CHAPTER II

SYSTEMATIC LITERATURE REVIEW

2.1 Introduction

This chapter presents systematic literature review (SLR) on bring your own device (BYOD) trend which is conducted based on academic and professional journal papers published from 2011-2015. This review summarizes the existing studies related to bring your own device security policies.

This chapter reviews systematically the previous studies related to bring your own device (BYOD) security policies. The systematic literature review has been undertaken using Kitchenham guidelines (2009) and it fulfilled the requirements of standard systematic literature review to be beneficial to researchers to have an overview of the current state of research trend in this area. The systematic literature review conducted using *"bring your own device"* AND *"security policy"* keyword from various available databases. The articles that have been gathered in this review are found in the IEEE xplore, ScienceDirect and Scopus as the most useful ones in computer science. In addition, Springerlink was chosen because it coordinates with the academicians and authors in the scientific community. The search for relevant articles and papers was limited to those published between the year 2011 until 2015, and the result was 10 papers which were analyzed. The review answers all the review questions defined in the review protocol to achieve the main objective of this research.

2.2 Results of the Literature Search

"Bring Your Own Device" is a new phenomenon in technology era and new concept in the field of researches, for this reason the number of articles returned in searching process through different databases was quite low. The following table gives an example of the number of articles returned during searching process for the following keywords:

Search Name	IEEE Xplore	ScienceDirect	Springerlink	Scopus
BYOD	78	354	492	268
Bring your own device	181	48,159	40,287	226
BYOD security policy	23	219	230	56
Bring your own device security policy	26	9,477	7,324	52

Table 2: Initial search results

Since the term of "Bring Your Own Device" is relatively new term, wherefore, to make the results more focused to the research topic the timescale of the search was narrowed to 2011-2015. By doing this narrow we can limit the results to peer-review journals. The number of articles returned during narrowing the search process as follow:

Search Name + (2011-2015)	IEEE Xplore	ScienceDirect	Springerlink	Scopus
BYOD	78	360	459	268
Bring your own device	123	48,063	13,733	224
BYOD security policy	23	224	227	56
Bring your own device security policy	24	2,520	2,792	52

Table 3: Key words search results from 2011-2015

Another way to make the result more relevant, there are three Boolean operators allow researcher to combine terms to narrow or broaden the search process such as AND, OR, NOT. In this search we used AND Boolean operator to combine between "Bring Your Own Device" AND "security policies" through searching process in there available databases which are IEEE Xplore, ScienceDirect, Scopus and SpringerLink since 2011 until 2015 using English language only and the results were as following:

Database Name	Number of articles (2011-2015)
IEEE Xplore	3
ScienceDirect	83
SpringerLink	71
Scopus	15
Total	172

Table 4: Search Result

172 articles returned during narrowing the search process by combining between "Bring Your Own Device" AND "security policies" terms in databases advanced mention. This number of articles was sent forward to screening stage to explicit which studies are selected for review and which studies should be discarded.

2.3 Articles Related Literature Screening

It was necessary to explicitly investigate the articles were found during searching process to see which ones should be put in the next stage. 18 articles and papers which had been identified during screening process based on inclusion criteria that have been mentioned in methodology chapter III. This selecting preformed through studying the title and abstract of the article. 154 articles were discarded based on exclusion criteria. The 18 articles which have been identified to be review must send forward to the next stage.

2.4 Articles Related Literature Quality Assessment

18 articles have been identified during screening stage. In the quality assessment stage, each paper was read and examined to see whether it should be included for final review or no. These articles were examined using quality assessment criteria mentioned early in methodology chapter. Only 10 articles which have been identified during this stage. Below is the quality assessment checklist of the 18 papers based on the quality assessment criteria mentioned in methodology chapter:

Title	Author &Year	Purpose (context/comments)	Intro	Method	Resluts	Concl (Y/N)
Towards Enforcing on The -Fly policies in BYOD Environments	Costantin o et al., (2013)	Proposed a framework by enforces on-the-fly policies. This framework apply a role-based access control system depend on user identity.	Y	N	Y	Y
Advanced Persistent Threat Mitigation Using Multi Level Security – Access Control Framework	Zulkefli et al., (2015)	Access control framework using multi-layer security	Y	N	Y	Y

High-Level Design for a Secure Mobile Device Management System	Keunwoo et al., (2013)	Mobile Device Management system composed of an agent and a device management server.	Y	N	N	N
Context Based Smart Access Control on BYOD Environments	Kang et al., (2015)	Security framework (Smart Access Control based on context)	Y	Y	N	Y
Modifying security policies towards BYOD	Vignesh & Asha (2015)	Proposed 3-tier enhanced policy architecture to modify the security policies for BYOD by suit the mobile devices.	Y	N	Y	Y
Corporate security solutions for BYOD: A novel user-centric and self-adaptive system.	Cuevas et al., (2015)	Proposed a taxonomy system to classify the features of BYOD systems. Describe a novel, adaptive and software system called (MUSES) to secure BYOD environments.	Y	N	Y	Y

BYOD security engineering a framework & its analysis	Zahadat et al., (2015)	Proposed BYOD security framework with three pillars: people, policy management, technology.	Y	Y	Y	Y
BYOD security challenges: control and protect your most sensitive data	Morrow (2012)	Presented a security challenges for BYOD and guidelines to secure sensitive data.	Y	N	N	N
BYOD - popular and problematic	Beckett (2014)	Data security implications that can arise via BYOD.	Y	N	N	N
Implement network security control solutions in BYOD environment	AlHarthy & Shawkat (2013)	Proposed Network security solution by create separate VLAN which specify rang of IP address and by using 802.1x encryption standard.	Y	N	Y	Y
Formal and Automatic Enforcement of Bring Your Own Device Policies.	Armando et al., (2014)	Proposed a framework by modeling the behavior of Android applications and verifying their compliance with	Y	N	Y	Y

		security policies.				
Remote Mobile Screen (RMS): an approach for secure BYOD environments	Ocano et al., (2015)	Propose BYOD security Framework to secure BYOD by using architecture consist of two sides, enterprise side and BYOD side.	Y	N	Y	Y
Techniques and real world experiences in mobile device security	Jaramillo et al., (2014)	Presented techniques and real world experiences to secure mobile device in organization.	Y	N	Y	Y
Bring your own device, securely	Armando et al., (2013)	Proposed a security framework for mobile devices that ensures that only applications complying with the organization security policy can be installed.	N	N	N	Y
Towards a user-friendly security-enhancing BYOD solution	Gessner et al., (2013)	Proposed a solution that enhances the security in BYOD scenario without compromising the usability and flexibility	Y	N	Y	N

		of the system				
Role of software product customer in Bring Your Own Device(BYOD)Trend: Empirical observations on software quality construction	Seth et al., (2014)	Identified the role of software customers in deciding about the quality of products and the impact in BYOD.	Y	N	N	N
Preserving dates and timestamps for incident handling in Android smartphones	Verma et al., (2014)	Proposed reactive approach gathers Kernl-generated timestamps of events and stores them in a secure location outside an Android smartphone	Y	N	N	N
Crossorer: secure and usable user interface for mobile devices with multiple isolated OS	Lange & Liebnerge ld (2013)	Designed an UI framework which provides the mechanisms to handle multiple environments on a mobile device.	Y	N	N	N

Table 5: Quality Assessment Checklist

After the quality assessment was completed, 10 papers related to BYOD security policies were put forward for the final literature review.

2.5 Overview of Studies

10 studies only on "Bring Your Own Device" security policies were identified using *"bring your own device" AND "security policy"* keyword, by searching from several available databases which are IEEE Xplore, ScienceDirect, Scopus and SpringerLink. Dated since 2011 until 2015 by English language only. These studies were identified to be reviewed by analyzing the context of each study, research questions and the result of each study. The studies covered different types of study areas such as survey, technical, literature review and system design.

Figure 2: Classification of papers reviewed

The studies that have been identified in this review covered a range of research topics related to bring your own device. These studies were categorized into following main topics:

- What is Bring Your Own Device?
- Bring Your Own Device benefits.
- Bring Your Own Device concerns.
- Bring Your Own Device policies.

2.6 The Current State of Security Policies on BYOD

Analysis based on publication years and the quantities of articles. As we mentioned earlier that the "Bring Your Own Device" term is relatively new concept, wherefore the results of articles returned in searching process during 2011 until 2015 shown that the number of articles in 2011 was quite low then it was slowly increasing in the last four years as it shown in Figure 3. This result actually is not a surprise as it is BYOD a recent phenomenon. This result of articles returned in BYOD was using "bring your own device" AND "security policies" keyword before screening process was done.

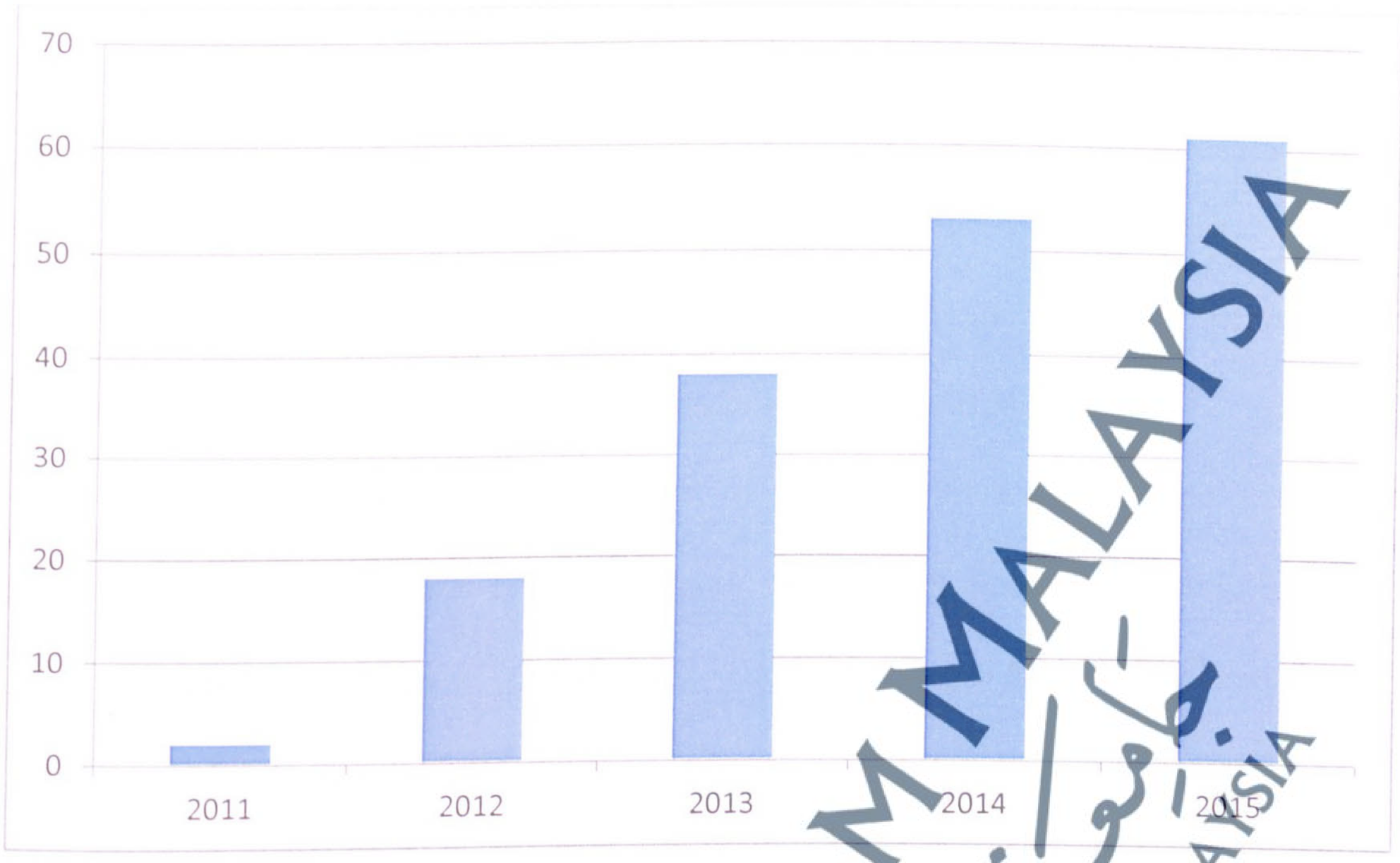

Figure 3: Number of publication papers from (2011-2015)

From Figure 3, we can note that BYOD is a growing filed in the last years. Most organizations are attracted by BYOD because it increases the productivity and efficiency of work. In addition, organizations who have adopted BYOD can save the purchasing and maintaining such assets (Alharthy & Shawkat, 2013; Vignesh & Asha, 2015).

2.7 What is BYOD

Bring your own device (BYOD) is a policy of permitting employees to bring their own mobile devices such as, smartphones, laptops, and tablets to workplace and use them for work proposes (Costantino et al., 2013; Kang et al., 2015).

The BYOD refers to bring your own device to workplace to use for work purposes. This new phenomenon developed due to consumerization in IT.

The concept of consumerization indicates to the increasing rate of Information Technology that used in the beginning of consumer market and it shifted in the end to organizations and educational institutions. The objective of using BYOD is to use the mobile devices such as smartphones, tablets and laptops for both work and personal use (Vignesh & Asha, 2015).

BYOD is not a new phenomenon it has been introduced in the business world since the employees begun bringing their particular such as USB flash drive, installed some types of software in order to use for personal purposes (Zahadat et al., 2015).

2.8 BYOD Benefits

BYOD adopted in many of organizations has increased the productivity because the employees keep working from their personal mobile device at any place and anytime out of working hours. Furthermore, BYOD increases the speed and efficiency of work also customer's satisfaction because of good communications. Additional, organizations who have adopted BYOD save the costs of purchasing and maintaining such assets (Alharthy & Shawkat, 2013; Vignesh & Asha, 2015; Ocano et al., 2015; Costantino et al., 2013).

In fact, there are many reasons for why organizations allowing or adopting BYOD (Zahadat et al., 2015):

- BYOD increases productivity and efficiency when the employees are well known how to use their own devices, this is means that the burden of training is lowered.
- Employees who use their own devices in workplace providing more care to these devices than devices provided by the company.

- By using BYOD services can be provided to rural areas, for example, patient monitoring in remote locations. This service can be done using BYOD in very low cost.
- By using mobile devices via apps such as GoToMeeting, virtual conferences, can be setup from anywhere in fast and easy way.
- There are some organizations such as Harvard/MIT edX and Khan Academy provide online education ideal for BYOD learning experiences with little cost and high quality.
- BYOD provide communication and information sharing service from anywhere and anytime.

2.9 BYOD Concerns

There are many risks that can affect the security of BYOD such as device lost or stolen, in this case the device containing sensitive data about the company and customers who is serious issue. Also the employee leaves the company, the employee signed up for BOYD policies owned device supported by organization technically and financially may leave the company for various reasons. This will raise the question on the ownership of the device. Furthermore, in some cases, the employees prefer to bring their device that may not compliant with organization policies which lead to chances of network attacks such as eavesdropping, man in the middle attack when accessed from public networks (Vignesh & Asha, 2015).

Using personal mobile device in workplace can lack the employee's privacy, as companies may monitor the personal information saved in the devices. On the other hand, the worries of the companies become bigger as

mobile device connect to the company network, it gives more chances of cyber attacks, vulnerable to data leakage as well as unauthorized sharing of information between employee and company (Ocano et al., 2015).

2.10 BYOD Policies

There is an increasing pressure allow devices owned by individual, particular users get access to network, services, and corporate resources. These contexts must involve specific rules defining the legal behavior of the devices. This definition and enforcement called Bring Your Own Device (BYOD) Policies (Armando et al., 2014).

BYOD policies need to put specific restrictions on employees who are using their own devices in workplace. These restrictions involve using a strong password, using encryption technical to encrypt the sensitive data stored on the device, enabling automatic locking of the device after each period of time, monitor the wireless network as well as enable the remote locking in case of the device lose or stolen (Costantino et al., 2013).

2.11 The Existing BYOD Security Frameworks

As a result of the systematic review, it can be summarized that the previous studies that have been done to modeling the security policies for BYOD as well as improve the security of mobile devices as a whole.

Costantino et al., (2013) in their study, they proposed a framework that enforces on-the-fly instantiated policies. This framework describes using a

role-based access control system based upon user identity and his context. Each user receives set of policy from a server, based on his role and current context. The effective user identity is confirmed using OAuth2.0 and device integrity is ensured by means of TPM installed on each device.

Zahadat et al., (2015), the BYOD security framework was presented in this study have seven stages including the BYOD security lifecycle. This lifecycle determine the stages of mobile device during its participation within a BYOD program. These stages include Plan, Identify, Protect, Detect, Respond, Recover, and Monitor. The BYOD security lifecycle is introduced to address structure and context to the steps presented in BYOD security framework.

Vignesh & Asha (2015) introduced multilevel security policy model consist of three levels which are organization level, applications level and device level. The organization level considered as a checklist to see before implementing BYOD in the organization. Access control should be restricted to the user based on user role. Application level provides security in the form of mobile device application known as Mobile Device Management include Mobile Content Management used to protect the data in smartphones. In the device level, the Certificate Authority CA credentials and encryption applications are provided.

Ocano et al., (2015), in this study the researchers presented Remote Mobile Screen (RMS) which consist of two sides which are enterprise side and BYOD side. RMS modifies BSF via moving the enterprise space inside the corporate network, using a new element named Corporate Space Manager

(CSM) employing VNC protocol to allow the employee to access the corporate space.

Zulkefli et al., (2015), presented multi layer security system based on Access Control and context aware Multi Level Security (MLS). Layer one MSRA architecture, allow admin to manage, monitor the activities that can be done by employees through MDM, MAM and DLP. Layer two Antivirus/malware Scanner, in this layer the employee's device should subject to device scans based on employee's level in the organization. Layer three Access Control, each employee should to pass this layer to ensure the privacy of the data. Layer four Multi Level Security, MLS divided into traditional MLS and MLS and the employee needs to choose one of them based on the suitability of the organization. Layer five Policies, based on the integration of layer 1 to layer 4 the security policies are created.

MUSES system by Cuevas et al., (2015) created a self-adaptive user-centric end-to-end system. This system applied Machine Learning and Computational Intelligence techniques based on users' behavior to adapt, improve and help to increase the setting of security rules. This security rules defined as specifications of the enterprise security policies.

Armando et al., (2014), designed a system that modeling the behavior of Android applications and verifying their compliance with security policies. This model applied in a corporate context for allowing the company to define and enforce the security policies for BYOD on employees' mobile device.

Kang et al., (2015), the researchers in this study presented smart access control framework which defines context based on context. This security framework can transform the information from low level into an intuitively meaningful context. Furthermore, this framework allows enterprises to create context-based, a flexible security policies by using access objects, and create security policies based on context.

AlHarthy & Shawkat (2013), they implemented BYOD security solution through presented network security solution by create separate VLAN to increase the security level using specify rang of IP address. 802.1x encryption standard and AES over CCMP used to increase the network security and protect it against several attacks.

Jaramillo et al., (2014), presented several factors and considerations. This factors involved techniques and real world experiences to secure mobile devices in an organization.

Table 6: Summary of studies related to BYOD security policies

	Title	Author	Year	Method	Mechanisms/Applications
1	Towards Enforcing On-The-Fly Policies in BYOD Environments	Costantino., et al	(2013)	Qualitative	Framework implements a role-based access control based on user role and his context.

2	Modifying Security Policies Towards BYOD	Vignesh & Asha	(2015)	Qualitative	Multilevel security policy model (organization level, application level, device level)
3	Corporate security solutions for BYOD: A novel user-centric and self-adaptive system	Cuevas., et al	(2015)	Qualitative	A self-adaptive user-centric end-to-end system named MUSES system. It applied machine learning and computational intelligence techniques.
4	BYOD security engineering: A framework and its analysis	Zahadat., et al	(2015)	Interview + Survey	BYOD security framework with three pillars: people, policy management, technology.
5	Advanced Persistent Threat Mitigation Using Multi Level Security-Access Control Framework	Zulkefli., et al	(2015)	Qualitative	Access control framework using multi-layer security based on context aware Multi-level

					security (MLS) And access control.
6	Context Based Smart Access Control on BYOD Environments	Kang., et al	(2015)	Qualitative	Smart access control framework which defines context based on context.
7	Formal modeling and automatic enforcement of Bring Your Own Device policies	Armando., et al	(2014)	Qualitative	Framework modeling the behavior of Android applications and verifying their compliance with security policies.
8	Remote Mobile Screen (RMS): an approach for secure BYOD environments	Ocano., et al	(2015)	Qualitative	BYOD security framework using two sides: enterprise side and BYOD side.
9	Techniques and Real World Experiences in Mobile Device Security	Jaramillo., et al	(2014)	Qualitative	Presented techniques and real world experiences.

1 0	Implement Network Securiy Control Solutions in BYOD Environment	AlHarthy & Shawkat	(2013)	(Interview +Survey)	Network security solution by create separate VLAN which specify rang of IP address and using 802.1x encryption standard.

2.12 Critical Analysis

Through the previous approaches that have been done to modeling BYOD security policies and to enhances the security in BYOD scenario without compromising the usability and flexibility of the system, we can noted that the access control is the most important factors in organizations to mitigate the security risks associated with BYOD system and to protect of any organization activities that can be data, applications and services or any other type of information from unauthorized access (Vincent et al., 2014). There are various specific roadblocks to having a secure mobile devices and appropriate access control such as, more attacks and malware are being created constantly, the limitations of device resources such as processing power and battery life. Table 7 shows the list of above mentioned approaches which are modeled based on access control and the most relevant attributes.

	Profiles	User Role	RBAC	Device	Context	AV
Advanced Persistent Threat Mitigation Using Multi Level Security-Access Control Framework (Zulkefli et al., 2015)			Y		Y	Y
Towards Enforcing On-The-Fly Policies in BYOD Environments (Cosantino et al., 2013)		Y	Y		Y	
Modifying security policies towards BYOD (Vignesh & Asha, 2015)		Y		Y	Y	
Formal modeling and automatic enforcement of Bring Your Own Device policies (Armando et al., 2014)	Y			Y	Y	
Context Based Smart Access Control on BYOD Environments (Kang et al., 2015)			Y		Y	

1-AV: Anti-virus/malware

2-RBAC: Role Based Access Control

Table 7: Previous BYOD Approaches and their Attributes

While each method in these studies addresses a solution to a single and specific problem, none of these approaches are able to fully addressing the issue of BYOD security. However, through the evaluation of each solution shown in Table 7 we have found that each solution in these studies has a specific beneficial an attribute. From (Zulkefli et al,. 2015) we find a security system using multi layer security based on context and access control. On-The-Fly policies (Cosantino et al., 2013) also implemented a role based access control based on user role and his context by receiving the user a specific policy from a server based on current role and his context. (Vignesh & Asha, 2015) introduced multilevel security policy and suggest specific classifications based on user role and profiles. On the other hand, (Armando et al., 2014) modeled the behavior of android applications and verifying their compliance with security policies in corporate context. Lastly, (Kang et al., 2015) also implemented smart access control defines context based on context.

To address the roadblocks associated with securing mobile devices from attacks and malware as well as the limitations of device resources such as processing power and battery life. We can combine the concepts in previously methods in BYOD security framework.

2.13 Summary

This chapter presented a systematic literature review related to bring your own device security policies. In this chapter the primary articles related to research area are summarized and presented. The systematic literature review has been undertaken using Kitchenham guidelines. The systematic literature

review conducted from several available databases using *"bring your own device"* AND *"security policy"* keyword. The articles that have been gathered in this review are found in the IEEE xplore, ScienceDirect, Scopus and Springerlink. The search for relevant articles and papers was limited to those published between the year 2011 until 2015, and the result was 10 papers which were analyzed. The review revealed that the "Bring Your Own Device" term is relatively a new concept; therefore the result of articles returned in searching process from 2011unitl 2015 showed that the number of articles was quite low then it was slowly increasing in the last four years. This result is because of BYOD a recent phenomenon. The review answered all the review questions defined in the review protocol to achieve the main aim of this research.