Comparative Analysis of Risk Evaluation Models for Risk-aware Access Control in Bring Your Own Device Environment

Shefiu Olusegun Ganiyu, Rasheed Gbenga Jimoh
Federal University of Technology Minna, University of Ilorin
Nigeria

Abstract

Risk evaluation models are employed by individuals and organisations to determine the level of risk involved in a process. Specifically, such model could be employed in computing risk value for risk-aware access control in bring your own device (BYOD) environment. Remarkably, several of these models vary in their coverages of risk components, output rendering formalisms and areas of application; thereby, putting the burden of model selection on users. Worst still, attempts to compare these models by previous researchers are baffled by subjective criteria that are not well-founded and often based on old taxonomy that are incompatible with pervasive environments. Thus, the study purposely formulated eight comparison criteria from characteristics of BYOD risk factors and countermeasures. Thereafter, the criteria were ranked with Analytic Hierarchy Process (AHP). Then, the ranked criteria were used to compare twelve risk evaluation methods, which were selected through three selection criteria expressly crafted for the study. Specifically, the result was rendered as numeric value, which is easy to understand by non-technical user. In all, the comparison approach presented in this study will assist BYOD operators in selecting model that could safeguard vital information assets against unauthorised access.

1. Introduction

In reality, information technology (IT) has continued to transmute work environments irrespective of its area of application to human endeavours [1][2]. One of such transformation phenomena is Bring Your Own Device (BYOD), which is an emerging IT consumerisation policy that allows workforce to use privately owned portable devices to perform both official and personal tasks [3][4][5]. The policy offers numerous benefits to both organisations and employees in terms of reduced IT budgets for enterprise and job satisfaction to personnel amongst others [6][7]. Thus, staff can combine pleasure with work through their devices, whereas organisation processes could be repositioned to meet the ubiquitous challenges of contemporary business environments.

Risk modelling or methodology is an organised procedure to determine the value of risk. Hence, risk evaluation model is a quantitative, qualitative or semi-quantitative mathematical representation used by institutions or individuals to compute risk inherent in processes [8]. Really, performing risk evaluation either manually or automatically has proven to be challenging task [9] [10]. Again, there is nothing like “exact risk value” [11], which makes it difficult to have a unified model for risk evaluation in all situations. Therefore, several commercialised and free models have been developed to minimise the challenge depending on domain of knowledge and circumstances [12], [13]. Often, organisations have to choose one among existing risk evaluation models through set of criteria and under the guidance of experts.

Generally, access control models are formulated to restrict access to crucial assets. One of such initiatives is risk-aware (risk-adaptive) access control model, which estimates risk value allied with request for information asset [14]. Subsequently, access to organisation resources is regulated based on future risk possibilities estimated from underlaying request.

Analytic Hierarchy Process (AHP) was developed by Saaty [15], as a multicriteria decision-making (MCDM) tool for selecting an option from many alternatives. The selection is premised on criteria that are ranked using pairwise comparison provided by experts. Though, AHP is time consuming [16] and the matrix evolving from the comparison grows quickly [17], but it handles inconsistencies in experts’ judgements [18].

Interestingly, there are numerous and rigorously proven risk evaluation models and selecting one is a daunting challenge [17][18]. More so, most available criteria to compare risk evaluation models before selecting any for IT environments are based on old taxonomy which is not ideal for rapidly changing technologies and attacker know-how [19]. Aside that, the difference in approaches and methods of risk evaluation can be attributed to variations in risk evaluation practices, which cut across disciplines and industries [21]. Nonetheless, not all could be suitable for risk-aware access control in BYOD due to peculiar characteristics of risk factors and security controls of the strategy [22]. Therefore, the compelling issue which is yet to be sufficiently addressed by researchers is to identify the most appropriate risk evaluation model for implementation in risk-aware module of BYOD access control. Such research will contribute to risk mitigation efforts that can allow organisations to derive the full benefits of BYOD strategy. Above all, it will provide better understanding of the strengths and weaknesses of current risk evaluation models for adoption and further studies in domain of the strategy.

Accordingly, the purpose of this paper is to identify risk evaluation model that amongst others, considered the characteristics of risk factors and countermeasures that are peculiar to BYOD. In order to achieve this aim, a criteria-based comparative analysis was conducted on existing models to determine their appropriateness for risk-aware access control in BYOD. The remainder of this paper is structured as follows: the next section presents a review of related works. Then, the succeeding section details the methodology employed in this study. The next section, presents and discusses the results obtained by the researchers. The section on conclusion and recommendation for future studies ends the paper.

2. Related Works

Depending on context of usage and field of study, the task of qualifying or quantifying risk is often referred to as risk analysis [21][22], risk assessment [25] or risk evaluation [24][25][26]. For example, [29] used risk evaluation and risk estimation interchangeably. On the contrary, the meaning ascribed to the concepts sometimes cause confusion when improperly defined among stakeholders [30]. This study preferred to use risk evaluation for risk quantification or qualification.

Several studies were conducted to compare risk evaluation frameworks, methods or models. [31] derived a comparison technique that utilised classification matrix to compare risk assessment methods. The matrix utilised for the comparison depended on level of detail and approach to risk estimation of the analysed method. According to the authors, the 3 x 3 matrix could help user to make informed choice among compelling methods in non-quantitative terms. In another study, [32] used the same matrix to compare risk analysis methods for identity management systems. Similarly, [33] combined the matrix with an ontology that allowed identification of attributes relating to risk analysis process. Generally, [31][33] focused on risk analysis methods irrespective of domain of applications. However, the comparison technique might be too generic for certain systems [13]. Yet, the outcome of the comparison conducted by [33][32] were neither stated in quantitative nor qualitative term.

Prior to comparing risk analysis methods, criteria are often formulated to select methods that are relevant to the main objective of the comparison. Henceforth, this set of criteria is referred to as *selection criteria*. Surprisingly, out of the literatures reviewed on the subject matter, only [25][34][35] detailed the selection criteria used for comparison exercises. Then, *comparison criteria* are defined to compare the merit and demerit of methods against one another. So, [20] advanced a framework for comparing risk analysis that derived comparison criteria from methods analysed. Also, [21][35] adopted bottom-top approach, whereby comparison criteria were contrived from process task and specific issues that the selected methods were designed to address. One limitation of these studies is that the criteria could easily become large, especially when unrelated methods are included in the framework. Rather, criteria to compare methods could be crafted from specific need of risk evaluation in particular area of interest. For instance, [13] and [36] extracted criteria from cloud based systems and risk management principles respectively.

Generically, [19][25][31] compared risk analysis methods that are intended for wide-ranging domains of knowledge. Also, [20][37][38][39] concentred on risk analysis methods for securing generic information systems. Really, comparing risk analysis form general perspective allows many methods to be considered, but such exercise would have implications on the IT governance structure of organisations [20]. In addition, extra efforts would be required to excogitate the selection and comparison criteria. Certainly, these limitations could be minimised when comparison is trammelled to specific domain. Thus, [35][12] independently determined the appropriateness of some risk analysis methods for cloud system. Also, [40] compared risk assessment methods for IT project management, while [13] performed similar research on supervisory control and data acquisition (SCADA).

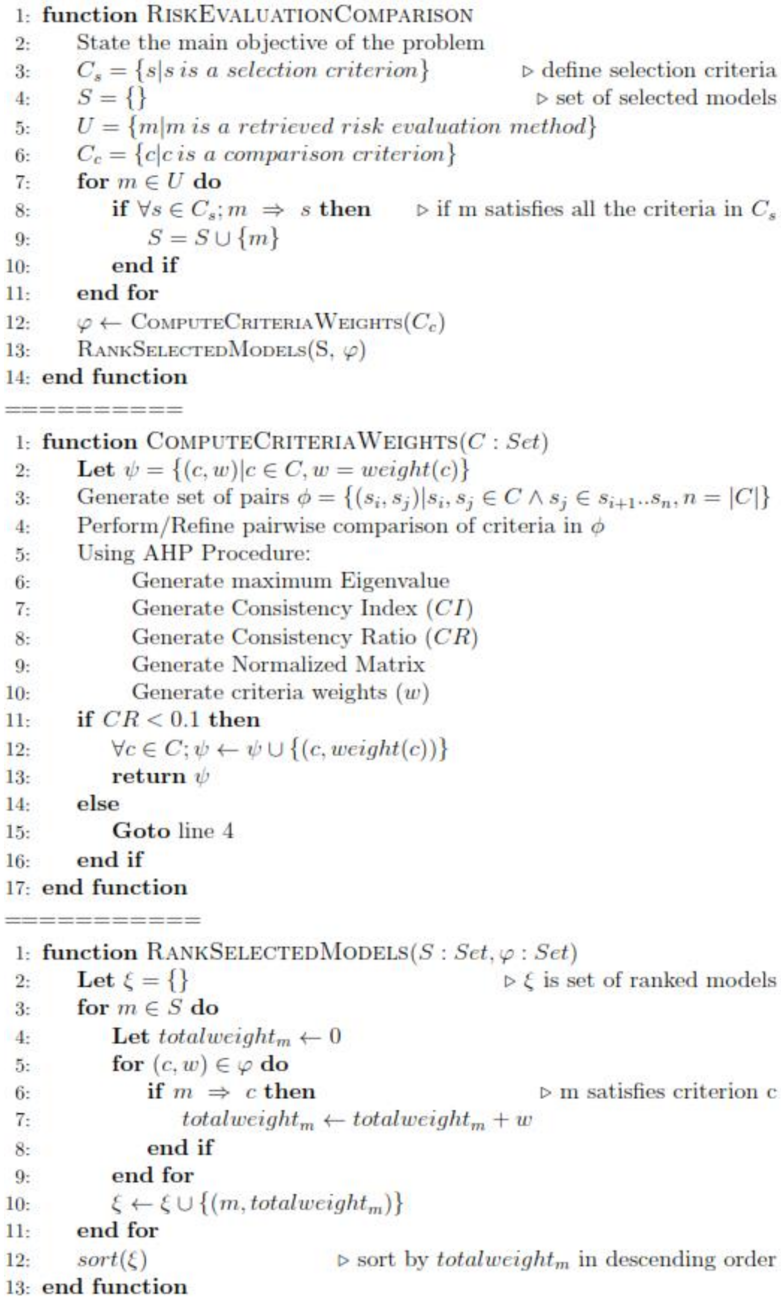
Majority of the reviewed works rendered the outcome of their comparisons in qualitative or quantitative terms to foster understanding of the results by non-technical users. However, [25][36] presented findings of their comparison in narrative terms which might not be easy to comprehend by non-experts.

Apart from [21][35] which involved relevant expert in the comparison process, other authors did not involve experts or did not sufficiently document contribution of such professionals to their researches. Thus, it might be difficult to discern researchers' subjectivisms from outcomes of their studies.

As revealed in this review, research that used ranked criteria for comparing risk evaluation methods has not been sufficiently carried out. Also, researchers' subjectivisms need to be properly managed at all stages of the comparison exercise. Though researches had been conducted in other aspects of computing systems or environments, the review indicated lack of research that compared risk evaluation models purposely for access control in BYOD environment.

3. Methodology

The algorithm presented in Figure 1 illustrates the formal representation of the methodology employed in this study.



```
1:  function RISKEVALUATIONCOMPARISON
2:      State the main objective of the problem
3:      $C_s = \{s | s\ is\ a\ selection\ criterion\}$          ▷ define selection criteria
4:      $S = \{\}$                                              ▷ set of selected models
5:      $U = \{m | m\ is\ a\ retrieved\ risk\ evaluation\ method\}$
6:      $C_c = \{c | c\ is\ a\ comparison\ criterion\}$
7:      for $m \in U$ do
8:          if $\forall s \in C_s; m \Rightarrow s$ then       ▷ if m satisfies all the criteria in $C_s$
9:              $S = S \cup \{m\}$
10:         end if
11:     end for
12:     $\varphi \leftarrow$ COMPUTECRITERIAWEIGHTS($C_c$)
13:     RANKSELECTEDMODELS(S, $\varphi$)
14: end function
==========
1:  function COMPUTECRITERIAWEIGHTS($C : Set$)
2:      Let $\psi = \{(c, w) | c \in C, w = weight(c)\}$
3:      Generate set of pairs $\phi = \{(s_i, s_j) | s_i, s_j \in C \wedge s_j \in s_{i+1}..s_n, n = |C|\}$
4:      Perform/Refine pairwise comparison of criteria in $\phi$
5:      Using AHP Procedure:
6:              Generate maximum Eigenvalue
7:              Generate Consistency Index ($CI$)
8:              Generate Consistency Ratio ($CR$)
9:              Generate Normalized Matrix
10:             Generate criteria weights ($w$)
11:     if $CR < 0.1$ then
12:         $\forall c \in C; \psi \leftarrow \psi \cup \{(c, weight(c))\}$
13:         return $\psi$
14:     else
15:         Goto line 4
16:     end if
17: end function
===========
1:  function RANKSELECTEDMODELS($S : Set, \varphi : Set$)
2:      Let $\xi = \{\}$                                        ▷ $\xi$ is set of ranked models
3:      for $m \in S$ do
4:          Let $totalweight_m \leftarrow 0$
5:          for $(c, w) \in \varphi$ do
6:              if $m \Rightarrow c$ then                       ▷ m satisfies criterion c
7:                  $totalweight_m \leftarrow totalweight_m + w$
8:              end if
9:          end for
10:         $\xi \leftarrow \xi \cup \{(m, totalweight_m)\}$
11:     end for
12:     $sort(\xi)$                           ▷ sort by $totalweight_m$ in descending order
13: end function
```

Figure 1. Algorithm for risk evolution models comparison

3.1. Selection of Risk Evaluation Models

The researchers searched for published academic and professional literatures on risk evaluation, risk analysis or risk assessment models (methods) from World Wide Web (WWW) and academic databases.

The retrieved documents were trimmed to relevant and sizeable number using the following criteria:

i. the model is founded on qualitative, quantitative or semi-quantitative technique;

ii. the model is formulated to address information security challenge in any IT related domains; and

iii. the risk evaluation algorithm or procedure implemented by such model should be freely available, which is not the case with enterprise editions [41].

3.2. Criteria to Compare Risk Evaluation Models

This paper evolved a set of comparison criteria, which were categorised into *core* and *complementary* criteria as captured in Tables 1 and 2 respectively. Meanwhile, four of the core criteria were derived from the five characteristics of BYOD risk factors and countermeasures [22], which are listed as follows:

i. Multiple risk factors may be considered for a given risk management scenario.

ii. Security controls differ in terms of efficacy to risk mitigation.

iii. Multiple controls are sometimes assembled to address loophole in a risk factor.

iv. Different risk factors including those belonging to same major factor might require differing controls.

v. Control can operate in specific modes, i.e. preventive or corrective, or detective.

The fifth criteria that was summarised as application domain of model, was arguably selected and categorised as core criteria due to its importance [20].

Table 1. Core criteria for BYOD risk evaluation method

Description of Criterion	Related Characteristic [22]	Code
Caters for multiple threats from single threat source.	i	MT
Considers the effectiveness of implemented technical risk countermeasures.	ii	CE
Accounts for contribution of each security control in defence-in-depth.	iii and vi	DD
Categorises security control as either preventive or detective control.	v	CS
The domain of application of the model should be relevant to security of information system or any its allies [20].	-	AP

Correspondingly, three criteria which are basic to risk computation in dynamic computing environment like BYOD formed the complementary criteria. Consequently, a total of eight comparison criteria were used in this research.

Table 2. Complementary criteria for BYOD risk evaluation method

Description of Criterion	Code
Computes risk value from combination of impact of risk on enterprise system and likelihood of threat occurrence in addition to other parameters.	RP
Utilises simple computation procedure.	MS
Considers causal relationship among risk factors (e.g. relationship between network and mobile device).	CR

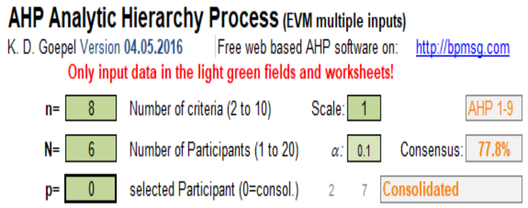
3.3. Data Gathering and Application Setup

In order to assign weight to each criterion by experts, this study used AHP and its corresponding rating scale. Hence, questionnaire comprising of parts A and B was developed and administered after initial validation by two experts. In parts A, demographic data of respondents were captured and parts B contained 28 items prepared from pairwise comparisons of the eight criteria using Equation 1.

$$C(n,k) = \frac{n(n-1)}{k} \qquad (1)$$

Where n is the number of criteria and constant $k = 2$. Also, purposive sampling method was adopted to select subject experts who served as respondents. Broadly, respondents are academics and professionals with interests in information security, risk management or system auditing (administration).

The data obtained in part B were analysed with AHP Application Package developed by Goepel [42], Version 04.05.2016. The configuration screen of AHP application is shown on Figure 2. Consolidated input ($p = 0$) from six participants were used ($N = 6$), together with the eight criteria ($n = 8$). Also, this study used standard nine points AHP rating scale ($Scale = 1$) and the threshold for acceptance of inconsistency (α) is set to 0.1 as recommended by [43].



AHP Analytic Hierarchy Process (EVM multiple inputs)
K. D. Goepel Version 04.05.2016 Free web based AHP software on: http://bpmsg.com
Only input data in the light green fields and worksheets!
n= 8 Number of criteria (2 to 10) Scale: 1 AHP 1-9
N= 6 Number of Participants (1 to 20) α: 0.1 Consensus: 77.8%
p= 0 selected Participant (0=consol.) 2 7 Consolidated

Figure 2. AHP configuration

3.4 Ranking of Risk Evaluation Models

The risk evaluation models selected in Section 3.1 were allocated weighted numerical value under each criterion, perhaps the method appropriately accounted for it. The values were assigned by the researchers, after thorough analysis of the model's documentation under each criterion. Subsequently, the values of each model were aggregated to obtain its overall score using the weight assigned by experts to each criterion as expressed in Equation (2).

$$s_j = \sum_{i=1}^{n} \omega_{ij} \qquad (2)$$

Where s_j is total weight of model j, ω_i is the weight of model s_j for i^{th} criteria, $i \geq 1$ and $n = 8$. Along the same line with AHP, the model with highest weight is the most relevant for BYOD environment. The consistency index (CI) of the ranking performed by experts is computed using Equation 3 in accordance with [15], where λ_{max} and n represent maximum Eigenvalue and order of the expert judgement matrix respectively.

$$CI = \frac{\lambda_{max} - n}{n - 1} \qquad (3)$$

Thus, the consistency ratio CR compares CI against consistency index (RI) of randomly generated pairwise comparison matrix as shown in Equation 4.

$$CR = \frac{CI}{RI} \qquad (4)$$

4. Result and Discussion

4.1. Respondents Demography

A total of six security or IT experts returned their completed questionnaires before six weeks earmarked for data collection.

Table 3. Respondent general information

Respondent Code	Designation	Experience	
		Years	Weight
ln1	Academic (cyber security)	6-10	2
ln2	Network Administrator	1-5	1
ln3	IT Manager/ Director	16-20	4
ln4	Academic	Above 20	5
ln5	Network Administrator	6-10	2
ln6	Academic (cyber security)	6-10	2

Therefore, general information about respondents extracted from part A of the questionnaire is presented in Table 3. For brevity, the respondents were assigned unique code and their years of experience were assigned specific weight. Next, the weights were considered in computation of weighted geometric mean (WGM) by the AHP package. Coincidentally, both academics and professionals have three respondents each and the respondents resided in five countries. Again, more than 83% of the participants possessed more than five years cognate working experience in areas relating to either IT management or information security.

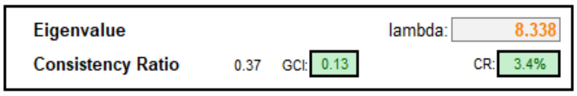
4.2. Criteria Ranking

The consistency ratio for individual respondent and weighted year of experience are shown in Table 4. Also, Figure 3 showed the principal Eigenvalue, lambda, consistency ratio Geometric Consistency Index (GCI) and Consistency Ratio (CR) computed for all respondents while taking their years of experience into cognisance. Specifically, the consolidated consistency ratio is calculated to be 3.4% or 0.034 which is less than 0.1 as suggested by [15]. Further analysis from the AHP package revealed that there was 77.8% consensus (see Figure 2) among the respondents in the pairwise comparisons.

Table 4. Respondent consistency ratio

	Respondent					
	ln1	ln2	ln3	ln4	ln5	ln6
Consistency Ratio	8%	9%	10%	7%	7%	9%
Weight	2	1	4	5	2	2

Above all, the ranking of the comparison criteria depended on consolidated matrix computed from the result of weighted geometric mean (WGM) for each pairwise comparison as shown in Figure 4.

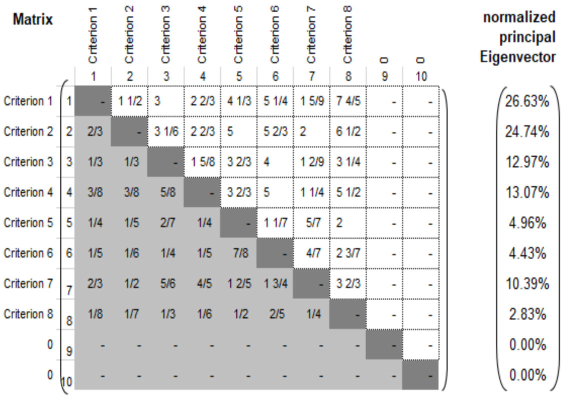


Eigenvalue lambda: 8.338
Consistency Ratio 0.37 GCI: 0.13 CR: 3.4%

Figure 3. Overall consistency ratio

Then, from the matrix, the AHP application generated the normalised principal Eigenvector next to the matrix which signified the weight of each criteria.

The AHP package also presented the ranking of criteria according to order of importance as shown in Table 5. By taking advantage of the potentials of AHP, respondents inconsistencies were computed as 3.4%.



Matrix		Criterion 1	Criterion 2	Criterion 3	Criterion 4	Criterion 5	Criterion 6	Criterion 7	Criterion 8	0	0	normalized principal Eigenvector
		1	2	3	4	5	6	7	8	9	10	
Criterion 1	1	-	1 1/2	3	2 2/3	4 1/3	5 1/4	1 5/9	7 4/5	-	-	26.63%
Criterion 2	2	2/3	-	3 1/6	2 2/3	5	5 2/3	2	6 1/2	-	-	24.74%
Criterion 3	3	1/3	1/3	-	1 5/8	3 2/3	4	1 2/9	3 1/4	-	-	12.97%
Criterion 4	4	3/8	3/8	5/8	-	3 2/3	5	1 1/4	5 1/2	-	-	13.07%
Criterion 5	5	1/4	1/5	2/7	1/4	-	1 1/7	5/7	2	-	-	4.96%
Criterion 6	6	1/5	1/6	1/4	1/5	7/8	-	4/7	2 3/7	-	-	4.43%
Criterion 7	7	2/3	1/2	5/6	4/5	1 2/5	1 3/4	-	3 2/3	-	-	10.39%
Criterion 8	8	1/8	1/7	1/3	1/6	1/2	2/5	1/4	-	-	-	2.83%
0	9	-	-	-	-	-	-	-	-	-	-	0.00%
0	10	-	-	-	-	-	-	-	-	-	-	0.00%

Figure 4. Consolidated matrix and normalised principal eigenvector

Unpredictably, criterion 1 has the highest weight of 26.6% and ranked first, whereas criterion 8 has the least weight of 2.8% and was last in the ranking.

Table 5. Criteria ranking

Criteria	Description	Weight	Rank	Code
1	Handles multiple threat from single source	26.6%	1	MT
2	Considers technical control effectiveness	24.7%	2	CE
3	Categorises control as preventive or detective	13.0%	3	CS
4	Accounts for contribution of control in defence-in-depth	13.1%	4	DD
5	Relevant to pervasive environment	5.0%	6	AP
6	Computes risk from impact, threat etc	4.4%	7	RP
7	Utilises simple computation procedure	10.4%	5	MS
8	Considers causal relationship among risk factors	2.8%	8	CR

4.3. Comparing the Models

Table 6 presents brief descriptions and risk evaluation techniques employed by 12 risk evaluation models that satisfied the selection criteria detailed in Section 3.1. Then for the comparison, the researchers put a checkmark under each criterion met by the model after thorough scrutiny as discussed in Section 3.4. For example, a model is deemed relevant to domain of application, if it is dedicated to access control in IT related field. Likewise, model is considered to be simple, if risk evaluation does not involve complex computation that rely on historical data [44].

Furthermore, assigning checkmark to criterion was guided by objectivity and this approach paved way for comparison of the models using weighted criteria as shown in Table 5. Therefore, the fact that some models met same number of criteria does not mean their total weight will be equal. For example, [45] and [46] got five criteria, but the total weights are significantly different.

Similarly, model's relevance should not be literarily adjudged based on year of development. Though, [47] could be considered to be among the oldest models, it ranked higher than seven recent models. Likewise, model suitability does not necessarily depend on domain for which it was developed. Evidently, [48] and [49] were developed for use in pervasive environment, the result exposed their respective gaps in addressing security characteristics of BYOD strategy. Once more, nine models were scored for their simplicity, but only two models accounted for defence-in-depth. It is also revealing that only three models accounted for causal relationships among risk factors, despite its importance to risk management in pervasive computing. Obviously, none of the models possessed all the eight criteria.

Based on this finding, the task of comparing set of risk evaluation criteria for adoption in risk evaluation model significantly depends on comparison criteria developed for the exercise. Clearly, this approach to comparing risk evaluation models presented its result in concise fashion for non-technical information security risk analysists. Importantly, the ranking does not in any way discredit any model, especially under different operating environments or other set of criteria outside risk-aware access control for BYOD. With this in mind, it only showed their relevance to the purpose of this research.

Table 6. Comparison of risk evaluation models

			Weighted Criteria (%)									
Author	Description	Risk Evaluation Technique	MT 26.6	CE 24.7	CS 13.0	DD 13.1	AP 5.0	RP 4.4	MS 10.4	CR 2.8	Total Weight (%)	Rank
[45]	Security risk evaluation for information system	Bayesian Network; Ant Colony Optimisation	✓	✓	✓			✓		✓	71.5	1
[46]	Information security assessment for health insurance company	Analytic Network Process; Decision Making Trial and Evaluation Laboratory, Fuzzy Linguistic Quantifiers-guided Maximum Entropy Order-Weighted averaging		✓		✓		✓	✓	✓	55.4	2
[50]	Risk evaluation for generic purpose	Conventional risk evaluation with improvement factor		✓		✓		✓	✓		52.6	3
[9]	Risk evaluation for generic information system	Financial loss and economic indicators of countermeasures		✓	✓			✓	✓		52.5	4
[47]	Access control for distributed database	Failure modes and effects analysis	✓				✓	✓	✓		46.4	5
[51]	Generic risk assessment model for information system	Formal Safety Assessment; Analytic Hierarchy Process	✓					✓	✓		41.4	6
[24]	Discovery of software security risk	Risk rating methodology; AHP		✓				✓	✓		39.5	7
[49]	Access control to data in pervasive environment	Random walk	✓				✓			✓	34.4	8
[52]	Analyse dynamic risk profile in computing infrastructures	Queueing modelling		✓							24.7	9
[48]	Access control for Ubiquitous environment	Risk evaluation using confidentiality, integrity and availability					✓	✓	✓		19.8	10
[53]	Access control for cloud-assisted eHealth	Risk evaluation using confidentiality, integrity and availability; HL7-based message transfer protocol					✓		✓		15.4	11
[54]	Access control for Health information system	Shannon entropy from information theory					✓		✓		15.4	11

MT=Caters for multiple threats from single threat source; **CE**= Considers the effectiveness of implemented technical risk countermeasures; **DD**=Accounts for contribution of each security control in defence-in-depth; **CS**=Categorises security control as either preventive or detective control; **AP**=The domain of application of the model should be relevant to security of information system or any its allies; **RP**=Computes risk value from combination of impact of risk on enterprise system and likelihood of threat occurrence in addition to other parameters; **MS**=Utilises simple computation procedure; **CR**=Considers causal relationship among risk factors (e.g. relationship between network and mobile device).

5. Conclusion and Future works

So, conducting comparative analysis on risk evaluation models is an essential task in realm of risk management in pervasive environments due proliferation of the models. No doubt, such task can only assist stakeholders in making informed decision, if the weighted criteria for the analysis relate to crucial components in domain of model's application, while analysts' subjectivisms and inconstancies are reduced to barest minimum. Likewise, result of the comparison ought to be presented in unambiguous and measurable terms. All things considered, ranking of models should neither depend on year of development nor number of criteria satisfied in the comparison. For the most part, the success of comparing existing risk evaluation models for implementation in any dynamic or security agonistic systems, including risk-aware access control for BYOD requires well-defined analysis.

Future researches could focus on how to reduce experts' subjectivisms when determining whether a model satisfies a criterion or not, especially, subjective criterion like model simplicity. In addition, the weaknesses identified in the risk evaluation models considered in this paper could be source of inspirations to other researchers.

6. Acknowledgement

We appreciate the time and efforts of all respondents who completed and returned our questionnaire.

7. References

[1] S. Deb, "Information technology, its impact on society and its future," *Advances in Computing*, vol. 4, no. 1, pp. 25–29, 2014.

[2] S. Ahmad, "Technology in organizations," *International Journal of Research in Business Management (IMPACT: IJRBM)*, vol. 2, no. 7, pp. 73–80, 2014.

[3] S. Köffer and E. Fielt, "IT consumerization and its effects on IT business value, IT capabilities, and the IT function," in *2015 Proceedings of Pacific Asia Conference on Information Systems*, 2015.

[4] M. N. O. Sadiku, S. R. Nelatury, and S. M. Musa, "Bring your own device," *Journal of Scientific and Engineering Research*, vol. 4, no. 4, pp. 163–165, 2017.

[5] O. Oluwatimi and E. Bertino, "An application restriction system for bring-your-own-device scenarios," in *Proceedings of the 21st ACM on Symposium on Access Control Models and Technologies (SACMAT '16)*, 2016, pp. 25–36.

[6] C. Rose, "BYOD: An examination of bring your own device in business," *Review of Business Information Systems*, vol. 17, no. Second Quarter, pp. 65–70, 2013.

[7] H. Romer, "Best practices for BYOD security," *Computer Fraud and Security*, vol. 2014, no. 1, pp. 13–15, 2014.

[8] A. Klinke and O. Renn, "A new approach to risk evaluation and management : Risk-based, precaution-based, and discourse-based strategies," *Risk Analysis*, vol. 12, no. 6, pp. 1071–1094, 2002.

[9] R. Bojanc and B. Jerman-Blažič, "A quantitative model for information security risk management," *Engineering Management Journal*, vol. 25, no. 2, pp. 25–37, 2013.

[10] Q. Ni, E. Bertino, and J. Lobo, "Risk-based access contol systems built on fuzzy inferences," in *ASIACC'10*, 2010, pp. 250–260.

[11] J. Bhattacharjee, A. Sengupta, C. Mazumdar, and M. S. Barik, "A two-phase quantitative methodology for enterprise information security risk analysis," in *Proceedings of the CUBE International Information Technology Conference*, 2012, pp. 809–815.

[12] M. Alnuem, H. Alrumaih, and H. Al-Alshaikh, "A comparison study of information security risk management frameworks in cloud computing," in *CLOUD COMPUTING 2015 : The Sixth International Conference on Cloud Computing, GRIDs, and Virtualization*, 2015, pp. 103–109.

[13] Y. Cherdantseva, P. Burnap, A. Blyth, P. Eden, K. Jones, H. Soulsby, and K. Stoddart, "A review of cyber security risk assessment methods for SCADA systems," *Computer & Security*, vol. 56, no. 2016, pp. 1–27, 2016.

[14] J. Ma, K. Adi, M. Mejri, and L. Logrippo, "Risk analysis in access control systems," in *2010 Eighth Annual International Conference on Privacy, Security and Trust*, 2010, pp. 160–166.

[15] T. L. Saaty, *The analytic hierarchy process*. New York: McGraw-Hill, 1980.

[16] N. J. Mamat and J. K. Daniel, "Statistical analyses on time complexity and rank consistency between singular value decomposition and the duality approach in AHP: A case study of faculty member selection," *Mathematical and Computer Modelling*, vol. 46, no. 2007, pp. 1099–1106, 2007.

[17] F. J. Carmone, A. Kara, and S. H. Zanakis, "A Monte Carlo investigation of incomplete pairwise comparison matrices in AHP," *European Journal of Operational Research*, vol. 102, no. 3, pp. 538–553, 1997.

[18] L. V. de Freitas, A. P. B. R. de Freitas, E. V. Veraszto, F. A. S. Marins, and M. B. Silva, "Decision-making with multiple criteria using AHP and MAUT : An industrial application," *European International Journal of Science and Technology*, vol. 2, no. 9, pp. 93–100, 2013.

[19] A. Shameli-sendi, R. Aghababaei-barzegar, and M. Cheriet, "Taxonomy of information security risk assessment (ISRA)," *Computers & Security*, vol. 57, pp. 14–30, 2016.

[20] A. Vorster and L. Labuschagne, "A Framework for Comparing Different Information Security Risk Analysis Methodologies," in *SAICSIT 2005*, 2005, pp. 95–103.

[21] G. Wangen, "Information security risk assessment: A method comparison," *Computer* , vol. 50, no. 4, pp. 52–61, 2017.

[22] S. O. Ganiyu and R. G. Jimoh, "Characterising risk factors and countermeasures for risk evaluation of

bring your own device strategy," *International Journal of Information Security Science*, vol. 7, no. 1, pp. 49–59, 2018.

[23] M. Lee, "Information security risk analysis methods and research trends : AHP and fuzzy comprehensive method," *International Journal of Computer Science and Information Technology*, vol. 6, no. 1, pp. 29–45, 2014.

[24] A. Alkussayer and W. H. Allen, "Security risk analysis of software architecture based on AHP," in *7th International Conference on Networked Computing*, 2011, pp. 60–67.

[25] K. V. D. Kiran, S. Mukkamala, A. Katragadda, and L. S. S. Reddy, "Performance and analysis of risk assessment methodologies in information security," *International Journal of Computer Trends and Technology (IJCTT)*, vol. 4, no. 10, pp. 3685–3692, 2013.

[26] D. Zhao, J. Liu, and Z. Zhang, "Method of risk evaluation of information security based on neural networks," in *Proceedings of the Eighth International Conference on Machine Learning and Cybernetic*, 2009, pp. 12–15.

[27] S. Kondo, M. Iwaihara, and M. Yoshikawa, "Extending RBAC for large enterprises and its quantitative risk evaluation," in *8th International Federation for Information Processing Conference on e-Business, e-Services, and e-Society*, 2008, vol. 286, pp. 99–112.

[28] S. Dorri Nogoorani and R. Jalili, "TIRIAC: A trust-driven risk-aware access control framework for Grid environments," *Future Generation Computer Systems*, vol. 55, pp. 238–254, 2016.

[29] J.-M. Seigneur, C. B. Lafuente, X. Titi, and J. Guislain, "Report OPPRIM : Opportunity-enabled risk management for trust and risk-aware asset access decision-making," Geneva, 2015.

[30] L. Pan and A. Tomlinson, "A systematic review of information security risk assessment," *International Journal of Safety and Security Engineering*, vol. 6, no. 2, pp. 270–281, 2016.

[31] P. L. Campbell and J. E. Stamp, "A classification scheme for risk assessment methods," California, 2004.

[32] E. Paintsil, "Risk methods and tools for identity management systems," Oslo, Norway, 2014.

[33] V. Agrawal, "A comparative study on information security risk analysis methods," *Journal of Computers*, vol. 12, no. 1, pp. 57–67, 2017.

[34] ENISA, "Inventory of risk assessment and risk management methods," 2006.

[35] G. Wangen, C. Hallstensen, and E. Snekkenes, "A framework for estimating information security risk assessment method completeness," *International Journal of Information Security*, 2017.

[36] M. Jouini and L. B. A. Rabai, "Comparative study of information security risk assessment models for cloud computing systems," *Procedia Computer Science*, vol. 83, no. 2016, pp. 1084–1089, 2016.

[37] A. Behnia, R. A. Rashid, and J. A. Chaudhry, "A survey of information security risk analysis methods," *Smart Comput. Rev.*, vol. 2, no. 1, pp. 79–94, 2012.

[38] N. Shukla and S. Kumar, "A comparative study on information security risk analysis practices," *International Journal of Computer Applications*, vol. Special Issue, pp. 975–8887, 2012.

[39] T. Dong and S. B. Yadav, "A comprehensive framework for comparing system security risk assessment methods," in *Twentieth Americas Conference on Information Systems*, 2014, pp. 1–8.

[40] J. Winiarski, "Comparative analysis of risk assessment methods in IT project," *Management and Finance*, vol. 11, no. 3/1, pp. 179–190, 2013.

[41] M. A. Khan, "Efficacy of OCTAVE risk assessment methodology in information systems organizations," *International Journal of Computer Applications Technology and Research*, vol. 6, no. 6, pp. 242–244, 2017.

[42] K. D. Goepel, "Implementing the analytic hierarchy process as a standard method for multi-criteria decision making in corporate enterprises – A new AHP excel template with multiple inputs," in *Proceedings of the international symposium on the analytic hierarchy process 2013*, 2013, no. June, pp. 1–10.

[43] K. D. Goepel, "BPMSG AHP Excel Template with multiple Inputs," 2013.

[44] J. Trajkovski and L. Antovski, "Risk management framework for IT-centric micro and small companies," in *ICT Innovations 2012*, 2012, pp. 271–280.

[45] N. Feng, H. J. Wang, and M. Li, "A security risk analysis model for information systems: Causal celationships of risk factors and vulnerability propagation analysis," *Information Sciences*, vol. 256, no. 2014, pp. 57–73, 2014.

[46] C. Lo and W. Chen, "A hybrid information security risk assessment procedure considering interdependences between controls," *Expert Systems with Applications*, vol. 39, no. 2012, pp. 247–257, 2012.

[47] E. Celikel, M. Kantarcioglu, B. Thuraisingham, and E. Bertino, "A risk management approach to RBAC," *Risk and Decision Analysis*, vol. 1, no. 1, pp. 21–33, 2009.

[48] N. N. Diep, L. X. Hung, Y. Zhung, S. Lee, Y. Lee, and H. Lee, "Enforcing access control using risk assessment," in *Proceedings of the Fourth European Conference on Universal Multiservice Networks (ECUMN'07)*, 2007, pp. 419–424.

[49] C. A. Sanchez, "A risk and trust security framework for the pervasive mobile environment," University of Oklahome, 2013.

[50] H. Sato, "A new formula of information security risk analysis that takes risk improvement factor into account," in *International Conference on Privacy, Security, Risk, and Trust, and IEEE International Conference on Social Computing*, 2011, no. V, pp. 1243–1248.

[51] Z. Wei and M. Li, "Information security risk assessment model base on FSA and AHP," in *Proceedings of the Ninth International Conference on Machine Learning and Cybernetics*, 2010, pp. 11–14.

[52] R. A. Miura-ko and N. Bambos, "Dynamic risk mitigation in computing infrastructures," in *Third International Symposium on Information Assurance and Security*, 2007, pp. 325–328.

[53] M. Sharma, Y. Bai, S. Chung, and L. Dai, "Using risk in access control for cloud-assisted eHealth," in *Proceedings of the 14th IEEE International*

Conference on High Performance Computing and Communications, HPCC-2012, 2012, pp. 1047–1052.

[54] Q. Wang and H. Jin, “Quantified risk-adaptive access control for patient privacy protection in health information systems,” in *ASIACCS ’11*, 2011, pp. 406–410.