Towards A Quantitative Risk Evaluation Model for Risk-Aware Access Control In Pervasive Environment

Shefiu .O. Ganiyu
[1]Department of Information and Media Technology
School of Information and Communication Technology
Federal University of Technology Minna, Nigeria
shefiu.ganiyu@futminna.edu.ng
+2348061601131

R.G. Jimoh
[2]Department of Computer Science
Faculty of Information and Communication Sciences
University of Ilorin, Nigeria
jimoh_rasheed@unilorin.edu.ng
+2348168421369

ABSTRACT

The use mobile devices by employees to perform both official and personal tasks popularly referred to as Bring Your Own Device (BYOD) has manifested in many sectors of human endeavours, whether the devices are authorised by employers or otherwise. BYOD strategy increases employees productivity, improves employees work experience and enhance business agility. However the strategy exposes crucial organisation resources to various threats, culminating to risks which might jeopardise the benefits of BYOD. Thus there is need for risk evaluation model that could be used by risk-aware access control to grant or deny access request based on inherent risk factors surrounding the request. This paper presents a conceptual approach for modelling a quantitative risk evaluator to mitigate security risks of BYOD strategy. Thus, implementation of the model will enhance access control in BYOD environment and minimize the security risks associated with adopting the strategy.

Key words: Risk, Risk Evaluator, Risk-aware, Access Control, BYOD, Pervasive Environment.

1. BACKGROUND TO THE STUDY

In the past decades, deployment of Information and Communication Technology (ICT) has brought tremendous benefits to information storage and retrieval activities within organisations (Sanchez, 2013; Baker & Wallace, 2007). Also as a result of business convergence and agility, organisations offer critical information to employees and business partners on varieties of computing devices and platforms through Business-to-Business (B2B) or Process-to-Process (P2P) integrations (Ganguly & Mansouri, 2012; Bhattacharjee, Sengupta, Barik, & Mazumdar, 2012) in a pervasive environment. Likewise, organizations are striving to improve employees work experience and productivity by allowing workers to use personal device to store and process official data through a strategy in pervasive computing known as Bring Your Own Device (BYOD) (Reddy, 2012; Luo & Kang, 2011).

Thus pervasive environment like BYOD and cloud computing exposes resources to security threats which translate to security risks that could jeopardise the envisaged benefits of ICT implementation. In a bid to minimize the risks and ensure confidentiality, integrity and availability (CIA) of information, security experts implement security controls or countermeasures. The controls which are in form of policies, services, processes and products are designed to mitigate identified or envisaged threats in particular aspect of information security (Ponnam, Harrison, & Waston, 2009). In general term, access control is a component of authorization and it determines whether request from subjects should be granted or denied using access context data such as time of access, place of access, quantity, security label on objects and operations that subject can perform on object (Samuel, Masood, Ghafoor & Mathur, 2009).

However, the access control models offer varying level of fine-grained security controls on object, subject and actions performed by subject, hence, organizations can choose any model of choice from a list which includes - Access Control List (ACL), Role Based Access Control model (RBAC), Attribute Based Access Control model (ABAC) and Policy Based Access Control model (PBAC), and lately, Risk Adaptive Access Control (RAdAC) (Sahafizadeh & Parsa, 2010). The aspiration to manage access to organisation resources by using concepts and models from traditional risk management practice has been on for a while. Thus terms like "risk-aware" and "risk-based" are often used interchangeably in access control to mean a process of factoring quantified risk into access decision, thereby, managing trade-off between risk of allowing request to resources and the cost or consequence upon resource misuse (Bijon, Krishman, & Sandhu, 2012, 2013; Chen & Crampton, 2012). RAdAC is an access control model developed by United States Department of Defense (US DoD) with built-in risk management principles (Santos, Westphall & Westphall, 2014). However, RAdAC is yet to be adopted for commercial and civil implementation (Program Office, 2004; Luo & Kang, 2011). Likewise, non-technical concerns like law and policy to operate the model are yet to be addressed (Farroha & Farroha, 2012). So, studies have been conducted (Dimmock, Belokosztolszki, Eyers, Bacon, & Moody, 2004; Nissanke & Khayat, 2004), to incorporate risk components into traditional and well adopted access control models like RBAC (Aziz, Foley, Herbert, & Swart, 2009; Chen & Crampton, 2012) and ABAC (Kandala, Sandhu, & Bhamidipati, 2011) to them risk-aware.

Risk evaluation model is a common sub-model of risk-aware access control model and it quantitatively or qualitatively determines the risk value for subsequent use in decision making process of access control system (Ma, Adi, Mejri, & Logrippo, 2010). Although quantitative risk model is considered to be complex and difficult (Behnia, Abd Rashid, & Chaudhry, 2012; Bhattacharjee et al., 2012) to implement, however, it brings objectivity, flexibility, agility and dynamism to risk evaluation in access control system (Bijon, Krishman, & Sandhu, 2013; Kondo, Iwaihara, Yoshikawa, & Torato, 2008). Whether operating in qualitative or quantitative mode, risk evaluator computes risk value by evaluating values assigned to risk parameters like value of asset, threat and vulnerabilities for each identified risk factor (Ni, Bertino, & Lobo, 2010; Zhao, Liu, & Zhang, 2009). Thus risk evaluation models are mostly built on risk factors which are recognized as possessing the capacity to cause potential threat to situation being modelled (Schneidewind, 2005). Once risk evaluator computes monolithic risk value for access request, decision to either grant or deny a request is taken by comparing the risk value against an agreed risk threshold.

Research efforts to compare the accuracy and flexibility of existing quantitative risk analysis methods have been conducted (Behnia et al., 2012; Shukla & Kumar, 2012). Regrettably, risk evaluation has proven to be a challenging phase of risk management, because each risk scenario requires somewhat different or modified approach to address risk in that domain (Ni et al., 2010). Likewise, there no such statement like "exact risk value" in risk evaluation either when the evaluation is conducted manually or automated as the frequecny of risk evaluation varies among institutions (Bhattacharjee et al., 2012). Therefore organisation will need to select risk evaluation for its access control bearing in mind, the organisation specific functions and needs, in addition to risk factors or parameters that are peculiar to the functions and needs (Behnia et al., 2012).

Nevertheless, despite the much publicised benefits of BYOD (Brett, 2013; Nitin, 2013), unauthorized access to company data or systems accounts for 65% of security concerns related to BYOD according survey of IT Security Community on LinkedIn (Schulze, 2013). Obviously, such authorisation incidents often led to financial loss among others (Dimensional Research, 2013), and adversely affect BYOD implementation (Gartner, 2013a, 2013b). Thus, in order to alleviate the risk associated authorisation in BYOD environment, the need for risk evaluator that is relevant to context of application is presently recognized as vital component of risk-aware access control models (Behnia et al., 2012; Ponnam et al., 2009; Khambhammettu, Boulares, Kamel & Logrippo, 2013; Santos et al., 2014; Seigneur, Kölndorfer, Busch, & Hochleitner, 2013). The approximate risk value from the model could be used to grant or deny access request from mobile users after considering risk factors that are pertinent to BYOD.

Recent studies on quantified risk evaluation for dynamic risk-aware access control systems are limited to domains like cloud computing and health information systems (Fall, Blanc, Okuda, Kadobayashi, & Yamaguchi, 2011; Santos et al., 2014; Wang & Jin, 2011). However, research focusing on risk evaluation for risk-aware access control model in BYOD environment is yet to be conducted. This represents a gap, because risk evaluation model is not a one size fits all (Ni et al., 2010) and this research attempts to fill the identified gap to enable organizations realize the benefits of BYOD by conducting an experimental study. Therefore, the aim of this paper is to develop a quantitative risk evaluation model that minimizes the security risk and optimizes the benefits of BYOD implementation by improving the correctness of risk evaluator for risk-aware access control system. The remaining sections of this paper are structured as follows. Section 2 reviews related literatures. Section 3 access control models for BYOD. Sections 4 and 5 present the research direction and conclusion for the paper respectively.

2. RELATED WORKS

Review of literatures reveals that only few studies had been conducted to evolve specific risk factors for BYOD. Luo and Kang (2011), presents risk based mobile access control (RiMAC) as a policy framework that captures risk factor abstractions for access control systems to secure mobile devices access to information in during military operations. The study outlined standard fields comprising of location, authentication, timeouts, threats and conditions as risk factor abstractions.

However, Luo and Kang (2011) primarily cover mobile risk factors specific to military operations and it may not be suitable in civil business environment without modification. For instance, threats and conditions risk factors as defined in Luo and Kang (2011) are relevant to physically hostile environment and security of mobile devices and communication network are better controlled. Whereas, access control in BYOD environment is confronted with risk factors like, insider threat, unsecure network, heterogeneous mobile devices and platforms in addition to location and authentication factors (IRS, 2014; Schulze, 2013) which are not covered by RiMAC.

Still on BYOD risk factor, Kandala et al. (2011) proposed framework for risk-adaptive access control which identified six components for security risk including; user, device, object, operation, connection, attribute provider and lever of assurance. Conversely, the risk factors considered in the framework are specific to risk components in ABAC and also the suitability for BYOD was not mentioned. Likewise, Celikel et al. (2009) introduced a probability risk management model to handle permission abuse and misuse in database that deploys RBAC for access control to resources. The study defines two risk factors; permission misuse and permission abuse for components like user queries, user credentials, role history logs and expected utility with Failure Modes and Effects Analysis (FMEA). Although, Celikel et al. (2009) uses RBAC as the underlying access control model which is a widely deployed model (Nissanke & Khayat, 2004), the identified risk factors and domain of knowledge do not relate to BYOD.

The research efforts to build risk into access control models have continued to receive considerable attentions. The framework proposed by Kandala et al. (2011) defines a risk estimation function for the abstract model developed for the framework using request and accessory history of the user as input and returns a quantified risk value as output. Though, it does not provide any enforcement architectures and details about implementations of the risk estimation function. Rather it focuses on implementing the policy layer of information security. Also the function does not cover any of the security risk components stated in the research. Similarly, the research does not propose ways to calculate risk of each access transaction. However, this research work develops an extended model that is open for adoption to any access control model for implementation in BYOD environment.

Similarly, Celikel et al. (2009) evaluates risk posed by user's query to database system a model defined as product of three multiplicands. The model satisfies decision theory and as well as uses maximum utility function to calculate maximum utility for the model. However, the study focuses on risk evaluation of database query. Also computation of detector rating employs data mining technique (K-means) which does not utilize existing risk control mechanism and risk prevention control (prevention rating) is not included as parameter in the proposed model. In another research attempt to quantify access control risk for health sector, Wang and Jin (2011) propose a practical quantitative risk adaptive access control model for patient privacy protection in health information systems. The model adopts need-to-know principle of information security to mitigate the risk of over-accessing patients' records by authorized health workers otherwise referred to as doctors. The research computes risk using Shannon entropy to represent uncertainty, but risk and uncertainty are different concepts Peterson (2006). Also internal security controls are not considered in risk computation of the model.

Among the early studies to account for existing risk measure by risk evaluator component of access control is (Miura-Ko & Bambos, 2007). Markovian and non-Markovian risk mitigation models are presented by (Miura-Ko & Bambos, 2007) to dynamically assess security risk profile which accumulates at each node of computing infrastructures. In both models, security manager is assumed to be automated process that is capable of selecting appropriate security control to bring risk to de-risked state at each node. The models defined three ellipsoidal boxed zones namely; low, medium and high risks which are colour coded as green, yellow and red respectively. The low risk is the zone with most effective controls and nodes belongs to this zone is deemed to constitute least risk to computer infrastructures. However, both models require only one control to be active at any given time, in order to determine risk indicator for a node, nevertheless this approach may not be sufficient for dynamic risk evaluation in pervasive environment where multiple security controls are often stacked and their combined risk mitigating efforts determine the overall risk value (Bijon et al., 2013; Cabarcos, 2011). Also contrary to risk evaluation needs of risk-aware access control systems, the two models focused on generic classification of risk tolerance at computing nodes but not the inherent risk in request received by the node which is peculiar with evaluation requirement of access control models. Thus impact of risk shocks on nodes was not covered by the models.

Similar to risk evaluation approach proposed by (Miura-Ko & Bambos, 2007) and Sato (2011) presents a risk evaluation model that accounts for risk improvement factors during risk computation process. The model incorporates risk reduction matrix to conventional risk evaluation model. According to Sato (2011), the matrix represents a significant factor in decision making, because it allows investment incurred on mitigation mechanism to be evaluated. One noticeable improvement of Sato (2011) over (Miura-Ko & Bambos, 2007) is the flexibility built into the model to account for more than one active risk controls at a time. Interestingly, such risk improvement approach will contribute to correctness of risk value of dynamic access control system of BYOD risk factors when combined with research outputs from Celikel et al. (2009), Kandala et al. (2011), Wang and Jin (2011). However the implementation and evaluation of the model was carried out without considering risk factors from specific industry.

It is therefore, evident from the review of related works that research to evolve risk factors for BYOD is yet to be covered. Also, the existing studies on risk-aware access control that explicitly account for existing risk controls have not covered for BYOD related case. These present research gaps which this study attempts to fill. Thus filling these gaps (serves as research outcome) will contribute to knowledge upon completion and other issues arising from the research will be opened to further researches.

3. ACCESS CONTROL MODELS FOR BYOD

Authorisation or access control can be described as the process by which an access request is validated by checking it against agreed and well-established rules (Santos, Westphall & Westphall, 2013). Access control principles are designed to complement other information security principles and ensure the confidentiality, integrity and availability of enterprise resources.

Access control mechanisms deployed in BYOD environment enable organisations to restrict access to only mobile users who are authorised to access certain resources after fulfilling authentication obligations (Samaras, Daskapan, Ahmad & Ray, 2014). So an important activity towards access regulation in BYOD involves the classifications of mobile device, communication channels, users (Ruebsamen & Reich, 2012) and other attributes. This is necessary to generate calibrated security levels for access control systems. Therefore, organisations with BYOD implementation mostly use two-tier security level (Chung, Chung, Escrig, Bai & Endicott-Popovsky, 2012). The first tier ensures security of data on mobile devices using mobile antivirus and data protection schemes (profile definition and encryption tools). The second tier is defined within the enterprise or cloud environment where other layers of security controls are put in place to control access for resources. Then access control policies are defined on existing access control models like ACL, RBAC, ABAC and PBAC (Ruebsamen & Reich, 2012). Typical two-tier architecture presented by (Chung et al., 2012) is shown in Figure 1.

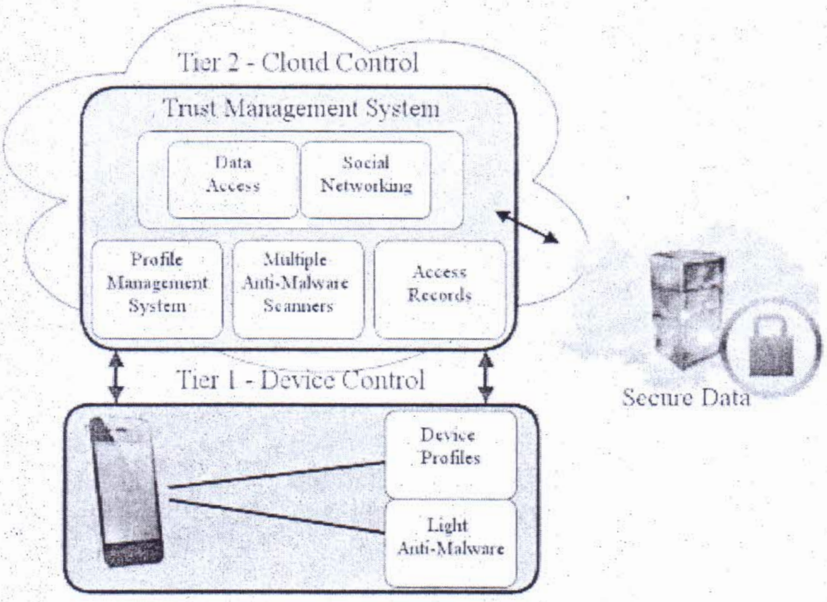

Figure 1: 2-Tier Access Control Architecture (Source: Chung et al., 2012)

3.1 Risk-Aware Access Control

In order to achieve a fine-grained control over resources, additional attributes like inherent risk in access request and level trust among participating entities are often included to access models (Sanchez, 2013). Hence, the primary goal of risk-aware access control is to provide flexible and permissible control on object by considering risk as major access determinant (Chen and Crampton, 2012). In addition, it is a vital tool for risk management, because it balances to need for users to get just right amount of resources to perform their functions against the overall organisation risk tolerance value (Cheng et al., 2007). Also decision to grant or deny access request made by mobile user may be taken after evaluating possible risk and comparing the risk value against a risk threshold, thereby leading to a risk-aware access control (JASON Program Office, 2004). Security risks represent the major concerns militating against present and future adoption of BYOD (Schulze, 2013). Thus leveraging and building risk concepts into access control management of BYOD will assist in minimizing the security risks. Moreover, existing risk management principles and standards could be ported into BYOD risk control paradigm.

3.2 Quantitative Risk Evaluation Models

Risk assessment process is an important requirement for risk-aware access control systems (JASON Program Office, 2004). The evaluation process will practically take vulnerabilities in risk factors and the probability of potential treat exercising the vulnerabilities into consideration. Therefore risk quantification process for risk-aware access control is domain specific task (Bijon et al., 2013). Specifically for risk evaluation to be realistic in BYOD environment there is need to take into cognizance role of existing risk controls or countermeasure as shown in risk evaluation models proposed by (Miura-Ko & Bambos, 2007; Sato, 2011) which are not related to BYOD.

4. RESEARCH DIRECTION

The primary objective of this research is to develop a risk evaluation model that takes risk factors of BYOD strategy into consideration. The model could serve as a plugin to any of the traditional access control models in order build risk-awareness into the traditional model so that inherent risk in a request could be used grant or deny access during decision making process.

To achieve the objective a study of the objects in the proposed architecture will be conducted to assemble a list of risk factors that a peculiar to BYOD. This will be followed by development of the quantitative risk evaluation model. Then a simulation of the risk evaluator will be conducted using the identified risk factors to generate a monolithic risk value that indicates inherent risk in a particular request. Lastly, performance evaluation of the risk model will be conducted.

The architecture of the proposed risk evaluation model is shown in Figure 2. As depicted in the model, a request from mobile device to enterprise information system could originate remotely via public wireless networks or virtual private network (VPN) through network security controls stationed within demilitarised zone (DMZ), to another security layer within the enterprise network and finally to the risk evaluator of risk-aware access control. Alternatively, request could be made by mobile device within the enterprise wireless networks via internal security controls and risk value will be computed by the risk evaluator to decide whether access request should be granted or denied. Typically, requests from the two sources would pose different risk values and could necessitate different risk thresholds.

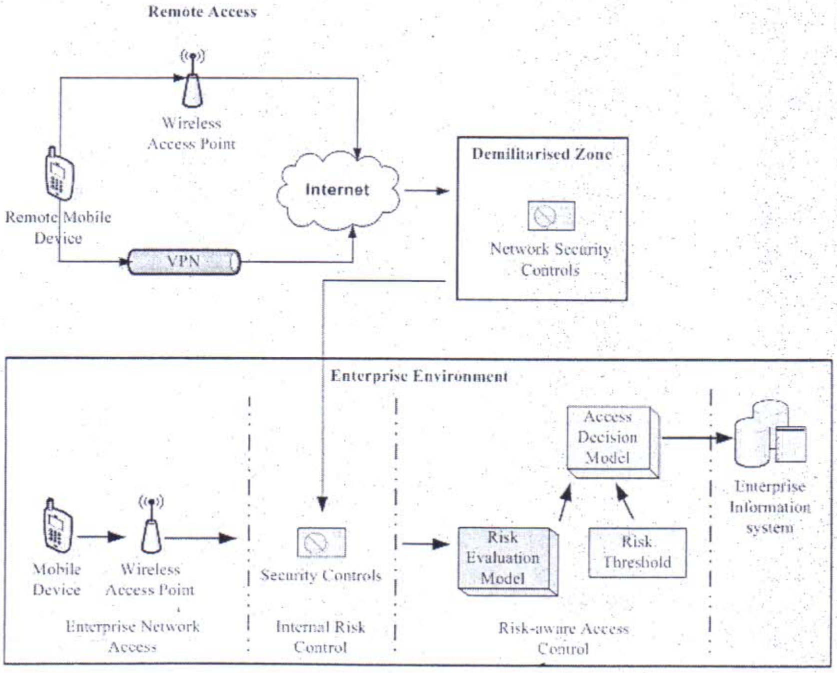

Figure 2: Architecture of the Proposed Risk Evaluation Model for BYOD

5. CONCLUSION

There is no premise to doubt the immense benefits accruing from BYOD implementation except security risks its adoption levied on enterprise information system. Any organisation that permits BYOD strategy must be prepared to mitigate the risks by implementing a risk-aware access control systems that grant or deny access request after considering risk factors that are peculiar to the strategy. Interestingly, central to such risk-aware access control model is risk evaluator which is required to computes approximate risk value relating to envisaged risk from the risk factors. The correctness of the monolithic risk value is essential in access control system to avoid wrongful denial or acceptance to request. In line with this, the paper presents a conceptual study of a quantitative model for risk evaluation in BYOD strategy to serve as plugin for traditional access control models like ACL, RBAC, ABAC and PBAC. Thus this research being the first in this direction will help to fill a research gap and its implementation will also assist enterprises to realised the full benefits of BYOD. Contributions and suggestions are welcome at this stage of the research.

REFERENCES

Aziz, B., Foley, S.N., Herbert, J., & Swart, G. (2006). Reconfiguring role-based access control policies using risk semantics. *Journal of High Speed Networks*, 15(3), 261-273.

Baker, W.H, & Wallace L. (2007). Is information security under control? Investigating quality in information security management. *IEEE Security & Privacy*, 5(1), 36-44.

Behnia, A., Abd Rashid, R., & Chaudhry, J. A. (2012). A survey of information security risk analysis methods. *Smart Computing Review, 2*, 79-94.

Bhattacharjee, J., Sengupta, A., Barik, M.S., & Mazumdar, C. (2012). A two-phase quantitative methodology for enterprise information security risk analysis. *CUBE '12 Proceedings of the CUBE International Information Technology Conference,* 809-815. Pune, India: ACM.

Bijon, K. Z., Krishman, R., & Sandhu, R. (2012). Risk-aware RBAC session. *8th International Conference, ICISS 2012*, 59-74. Guwahati, India: Springer.

Bijon, K. Z., Krishman, R., & Sandhu, R. (2013). A framework for risk-aware role based access control. *IEEE-CNS Symposium on Security Analytic and Automation (SAFECONFIG)*, 462-469. Washington: IEEE.

Brett, B. (2013). Money talks: Media takes note of recent BYOD financial impact study. Retrieved October 31, 2014, from Cisco Blogs website: http://blogs.cisco.com/wireless/money-talks-media-takes-note-of-recent-byod-financial-impact-study/

Cabarcos, P.A. (2011). Risk assessment for better identity management in pervasive environments. *Fourth Annual PhD Forum on Pervasive Computing and Communications*, 389-390. Seattle, WA: IEEE.

Celikel, E., Kantarcioglu, M., Thuraisingham, B.M., & Bertino, E. (2009). A risk management approach to RBAC. *Risk and Decision Analysis*, 1(1), 21-33.

Chen, L., & Crampton, J. (2012). Risk-aware role-based access control. In C. Meadows, & C. Fernandez-Gago (Eds), *Security and trust management*, 146-150. Verlang Berlin: Springer.

Cheng, P.C., Rohatgi, P., Wagner, G. M., & Reninger, A. S. (2007). Fuzzy multi-level security: An experiment on quantified risk-adaptive access control. *Security and Privacy, 2007, SP '07, IEEE Symposium on*, 222-230. Berkeely, CA: IEEE.

Chung, S., Chung, S., Escrig, T., Bai, Y., & Endicott-Popovsky, B. (2012). 2TAC: Distributed Access Control Architecture for "Bring Your Own Device" Security. *2012 ASE/IEEE International Conference on BioMedical Computing*, 123-126. Washington, DC: IEEE.

Dimensional Research. (2013). *The impact of mobile devices on information security: A survey of IT professionals.* Technical Report. Retrieved November 12, 2014, from http://www.checkpoint.com/capsule/check-point-capsule-2014-mobile-security-survey-report.pdf.

Dimmock, N., Belokosztolszki, A., Eyers, D.M., Bacon, J., & Moody, K. (2004). Using trust and risk in role-based access control policies. *Proceedings of the 9th ACM Symposium on Access Control Models and Technologies*, pp. 554-563, Yorktown Heights, NY: ACM.

Fall, D., Blanc, G., Okuda, T., Kadobayashi, Y., & Yamaguchi, S. (2011). Toward Quantified Risk-Adaptive Access Control for Multi-tenant Cloud Computing. *The 6th Joint Workshop on Information Security.* 5-6. Kaohsiung: JWIS.

Farroha, B., Farroha, D. (2012). Challenges of operationalizing dynamic system access control: Transitioning form abac to radac. *Systems Conference (SysCon), 2012 IEEE International*, 1-7. Vancouver, BC: IEEE.

Ganguly, A., & Mansouri, M. (2012). Evaluating risks associated with extended enterprise systems (EES). *IEE A&E Systems Magazine*, 4-11.

Gartner. (2013a). How to take video mobile with enterprise video content management. Retrieved October 31, 2014, from https://www.gartner.com/doc/2516615?ref=SiteSearch&sthkw=BYOD&fnl=search&srcId=1-347892225

Gartner. (2013b). Gartner predicts by 2017, half of employers will require employees to supply their own device for work purposes. Retrieved October 31, 2014, from http://www.gartner.com/newsroom/id/2466615

IRS. (2014). Safeguards technical assistance memorandum protecting federal tax information (FTI) within a mobile device environment. Retrieved February 09, 2015, from http://www.irs.gov/uac/Safeguards-Technical-Assistance-Memorandum-Protecting-Federal-Tax-Information-FTI-within-a-Mobile-Device-Environment

JASON Program Office. (2004). *Horinzontal integration: Broader access models for realizing information dominance*. Technical Report JSR-04-132: MITRE Corporation.

Kandala, S., Sandhu, R., & Bhamidipati, V. (2011). An attribute base framework for risk-adaptive access control models. *ARES '11 Proceedings of the 2011 Sixth International Conference on Availability, Reliability and Security,* 236-241. Vienna: IEEE Computer Society.

Khambhammettu, H., Boulares, S., Kamel, A., & Logrippo, L. (2013). A framework for risk assessment in access control systems. *Computer & Security*, 86-103.

Kondo, S., Iwaihara, M., Yoshikawa, M., & Torato, M. (2008). Extending RBAC for large enterprises and its quantitative risk evaluation. *IFIP International Federation for Information Processing*, 99-112, Boston: Springer.

Luo, J., & Kang, M. (2011). Risk based mobile access control (RiBMAC) policy framework. *The 2011 Military Communicatio Conference-Track 3- Cyber Security and Network Operations. U.S. Government*, 1448-1453. Baltimore, MD: IEEE.

Ma, J., Adi, K., Mejri, M., & Logrippo, L. (2010). Risk analysis in access control systems. *2010 Eighth Annual International Conference on Privacy, Security and Trust*. Ottawa, ON: IEEE.

Miura-Ko, R.A., & Bambos, N. (2007). Dynamic risk mitigation in computing infrastructures. *Third International Symposium on Information Assurance ans Security*, 325-328. Manchester: IEEE.

Ni, Q., Bertino, E., & Lobo, J. (2010). Risk-based access contol systems built on fuzzy inferences. *ASIACC'10*. Beijin: ACM.

Nissanke, N., & Khayat, E.J. (2004). Risk based security analysis of permissions in RBAC. *Proceedings of the 2nd International Workshop on Security in Information Systems*, 332-341. Porto, Portugal: INSTICC Press.

Nitin, B. (2013). BYOD: Bring-your-own-device-or-demise? Retrieved October 31, 2014, from ComputerWeekly: www.computerweekly.com/opinion/BYOD-Bring-your-own-device-or-demise.

Peterson, G. (2006). Introduction to identity management risk metrics. *IEEE Security and Privacy*, 4(4), 88-91.

Ponnam, A., Harrison, B., & Waston, E. (2009). Information systems risk management: An audit and control approach. In J. Gupta, & S. Sharma(Eds), *Handbook of Research on Information Security and Assurance*, 68-83. Hershey, New York: Information Science Reference.

Reddy, A.S. (2012). Making BYOD work for your organization. Retrieved March 9, 2014, from http://www.cognizant.com/RecentHighlights/Making-BYOD-Work-for-Your-Organization.pdf

Ruebsamen, T., & Reich, C. (2012). Enhancing Mobile Device Security by Security Level Integration in a Cloud Proxy. *CLOUD COMPUTING 2012 : The Third International Conference on Cloud Computing, GRIDs, and Virtualization*, 159-168. Nice, France: IARIA.

Sahafizadeh, E., & Parsa, S. (2010). Survey on access control models. *Future Computer and Communication (ICFCC), 2010 2nd International Conference on,* V1-1 - V1-3. Wuhan: IEEE.

Samaras, V., Daskapan, S., Ahmad, R., & Ray, K.S. (2014). An Enterprise Security Architecture for Accessing SaaS Cloud Services with BYOD. *2014 Australasian Telecommunication Networks and Applications Conference (ATNAC)*, 129-134. Southbank, VIC: IEEE.

Samuel, A., Masood, A., Ghafoor, A., & Mathur, A. (2009). Enterprise access control policy engineering framework. In J. Gupta, & S. Sharma (Eds), *Handbook of Research on Information Security and Assurance* (311-337). Hershey, New York: Information Science Reference.

Sanchez, C.A. (2013). *A risk and trust security framework for the pervasive mobile environment.* PhD Thesis. University of Oklahoma. Retrieved May 04, 2014, from http://idea.cs.ou.edu/pubs/sanchez_dissertation.pdf.

Santos, D.R., Westphall, C.M., & Westphall, C.B. (2014). A dynamic risk-based access control architecture for cloud computing. *Network Operations and Management Symposium (NOMS),* 1-9. Krakwo, Poland: IEEE.

Sato, H. (2011). A new formula of information security risk analysis that takes risk improvement factor into account. *International Conference on Privacy, Security, Risk, and Trust, and IEEE International Conference on Social Computing*. 1243–1248. Boston: IEEE.

Schneidewind, N.F. (2005). Predicting risk as a function of risk factors. *Proceedings of the 2005 29th Annual IEEE/NASA Software Engineering Workshop (SEW'05)*, 131-141, Greenbelt, MD: IEEE.

Schulze, H. (2013). *2013 BYOD & mobile security report!* Retrieved January 12, 2015, from https://www.lumension.com/Media_Files/Documents/Marketing---Sales/Others/BYOD-and-Mobile-Security-Report-2013.aspx.

Seigneur, J., Kölndorfer, P., Busch, M., & Hochleitner, C. (2013). A survey of trust and risk metrics for a BYOD mobile worker world. *SOTICS 2013 : The Third International Conference on Social Eco-Informatics*, 82-91. Lisbon, Portugal: IARIA.

Shukla, N., & Kumar, S. (2012). A comparative study on information security risk analysis practices. *Sepcial Issue of International Journal of Computer Applicatons*, 28-33.

Wang, Q., & Jin H. (2011). Quantified risk-adaptive access control for patient privacy protection in health information systems. *ASIACCS '11,* 406-410. Hong Kong: ACM.

Zhao, D., Liu, J., & Zhang, Z. (2009). Method of risk evaluation of information security based on neural networks. *Proceedings of the Eighth International Conference on Machine Learning and Cybernetic*, 1127-1132. Baoding, China: IEEE.