Extended Risk-Based Context-Aware Model for Dynamic Access Control in Bring Your Own Device Strategy

Shefiu Olusegun Ganiyu and Rasheed Gbenga Jimoh

Abstract The emergence of brings your own device (BYOD) strategy has brought considerable benefits to enterprises. However, secure access control to vital enterprise resources is one of the impedances to BYOD adoption. Thus, some researches were directed toward dynamic access control using concepts from risk evaluation, machine learning, or context-awareness. However, research efforts to harmonize the three concepts are yet to be established. Hence, this study proposed an Extended Security Risk Analysis Model (ExtSRAM) that combined the concepts to evolve a risk-based and context-aware model to mitigate access control challenges in BYOD. The proposed model comprised of three blocks, including static risk analysis, user contextual profiling, and risk computation. Furthermore, ExtSRAM utilized the Bayesian network to model user contextual profile and static enterprise risks. Again, the proposed model was formulated on six assumptions for it to be realistic for BYOD strategy. More so, a theoretical validation of ExtSRAM justified its soundness and completeness in estimating security risks for dynamic access control. Really, implementing ExtSRAM will proactively safeguard digital assets against unauthorized access. In doing so, an organization can strategically reposition its workforce for productivity while taking advantage of its investment in BYOD implementation.

Keywords BYOD · Risk-based access control · Context-aware access control · Risk evaluation model · Dynamic access control

S. O. Ganiyu (✉)
Department of Information and Media Technology, School of Information and Communication Technology, Federal University of Technology Minna, Minna, Nigeria
e-mail: shefiu.ganiyu@futminna.edu.ng

R. G. Jimoh
Department of Computer Science, Faculty of Information and Communication Sciences, University of Ilorin, Ilorin, Nigeria
e-mail: jimoh_rasheed@unilorin.edu.ng

H. Chiroma et al. (eds.), *Machine Learning and Data Mining for Emerging Trend in Cyber Dynamics*, https://doi.org/10.1007/978-3-030-66288-2_12

1 Introduction

Generally, several undertakings in current digital environments involve different categories of security risks, which can lead to varying degrees of threats to information assets. For instance, the security risks in Bring Your Own Device (BYOD) can be categorized into technological, organizational, implementational, human aspects, and policy (regulation) [54]. Therefore, these risks are either formally or casually determined before human and humanoid agents are allowed to perform certain actions on digital contents and facilities. In line with this, risk evaluation is a subprocess of risk assessment, which assigns qualitative or quantitative values to the likelihood of risk occurrence, the consequence after incidence, and the level of risk [34]. For completeness, it is expected that risk evaluation should appropriately consider the likelihood of risk in accordance with actions performed during an event [14].

Obviously, the adoption of BYOD strategy is rapidly becoming a global phenomenon. For example, some enterprises swiftly mandated their employees to work remotely through the *work from home policy* due to the COVID-19 pandemic [10, 16]. Meanwhile, some of these organizations that hurriedly keyed into BYOD strategy were hardly prepared for its security risk. Thus, the security risk in the emerging information technology (IT) landscape has continued to evolve [60], and the specific benefits of BYOD have been accompanied by security risks [4, 32, 43, 58]. For example, a survey conducted in the United Kingdom between 2017 and 2018 revealed that BYOD was embraced by both companies and charity organizations, in which 45 and 65% cases of BYOD security breaches were recorded respectively [53]. Specifically, classical risks pertaining to authorization is of serious concern to many enterprises [22]. Such risks are known to portend adverse impacts on the security of IT infrastructures resulting in performance degradation [52].

Furthermore, authorization is one of the issues encountered by BYOD implementers, which relates to allowing only the right employee to access only the right information, at right time, from the right location and through the right means [24, 45]. Especially, the recent upsurge in risks associated with BYOD adoption has called for more attention of security handlers [56]. Thus, the flexibility of user-oriented and infrastructure-centric features that are attributed to BYOD circumvents some traditional authorization controls mechanisms [2, 59]. Often, this flexibility contributes to unauthorized access problems in BYOD, which consequently leads to great financial loss, amongst other security challenges [27]. Unfortunately, this problem is yet to be sufficiently addressed by existing access control techniques, including those that assayed spatial and temporal properties of users for access control in pervasive environments, such as, BYOD and Internet of Things (IoT) [59]. Hence, there is s need for a dynamic and fine-grained access control that leverages risk or context-aware procedure to address the problem. Thus, a domain-specific risk estimation method must be developed [13], and integrated into the access control mechanism of BYOD to achieve such flexibility.

Therefore, this study presents two main contributions to the security of assets in emerging digital environments. First, it advances a unique approach that integrates context-awareness and machine learning into risk evaluation procedures to generate a dynamic architecture for access control in BYOD environment. Second, it develops a novel mathematical model for risk estimation that can serve as an add-on to existing static access control models, and reinvigorate them into fine-grained authorization mechanisms in other pervasive environments.

Primarily, the aim of this research is to extend a Security Risk Analysis Model (SRAM) developed by [23], with context-awareness features for dynamic and fine-grained authorization in BYOD strategy. More importantly, the rationale for selecting [23] was premised on our previous research [26]. The remaining sections of this chapter are organized as follows. Section 2 presents the background knowledge to foster understanding of the chapter. Section 3 presents the review of related works on risk evaluation models and context-aware access control models. Thereafter, Sect. 4 discusses the proposed model, whereas Sect. 5 presents a detailed process flow of the proposed model and Sect. 6 presents the theoretical evaluation of the proposed model. Lastly, Sect. 7 concludes the chapter.

2 Background

This section provides background information about dynamics approaches that can mitigate access control challenges in BYOD environment. Also, it presents the rudiment of a Bayesian network, which serves as a machine learning tool for the access control model presented in this study.

2.1 Dynamic Access Control in BYOD Strategy

Fundamentally, controlling access to vital information assets is one of the cardinal objectives of information security. To this end, access control models such as Access Control List (ACL), Role-Based Access Control (RBAC), Attribute Based-Access Control (ABAC), Policy-Based Access Control (PBAC), and Risk-Adaptive Access Control (RAdAC) have been developed to safeguard information assets from unauthorized access [21]. Unlike other models, RAdAC represents a significant paradigm shift and was primarily developed to utilize risk evaluation methods for access control decisions [47]. Thus, incorporating risk into access control did not only lead to a flexible and dynamic access control model [12], but it also contributed to the emergence of concepts like risk-based or risk-aware access controls [5, 19].

In addition, contextual information obtained from user's specific behavior, device attributes, and environmental factors have been utilized to form another class of access control mechanism [20, 24, 29, 61]. This class of control which is often referred to as context-based or context-aware access control offers fine-grained and dynamic authorization procedures to secure computing environments [31]. In order to further reinforce the performance of access control mechanisms, context-awareness has been combined with risk-awareness [1]. Furthermore, other researchers utilized the level of trust between interacting entities for authorization [6], combined trust with risk [18], or combined trust with opportunity to improve security posture [2]. Thus, context or trust is considered to be an additional parameter to the risk evaluation function, when it is included in risk-based access control [1, 2, 8].

The dynamism of contemporary computing strategies including cloud computing, IoT, and pervasive computing have paved the way for flexible access to information and technological infrastructures [5]. However, flexible access requires dynamic access control to mitigate security risks emanating from unauthorized entities [19, 42]. Hence, irrespective of the level of risk awareness built into the dynamic access control system, requests from each entity are expected to be treated on a case-by-case basis using historical data from previous access requests. Hence, internal security controls are usually deployed by security experts to mitigate every security risk in the requests for enterprise data [56].

Bring Your Own Device (BYOD) is a pervasive computing strategy that allows employees to use privately owned smart mobile devices to perform private and official tasks [41]. Hence, an employee can meet tight organization schedules with preferred devices and use any available network from comfortable locations at any time. This evolving strategy offers some benefits like an increase in employee productivity, improve work experience and reduction in IT budgets amongst others [8, 17, 44]. On the one hand, the adoption of BYOD has continued to permeate and reshape corporate business environments, non-profit organizations, and donor agencies. On the other hand, enrollees of the pervasive strategy are spreading beyond the organization workforce to customers, donors, ubiquitous business processes and much more.

2.2 Bayesian Network

The entire concept behind Bayesian network or probabilistic directed acyclic graph (DAG) model is based on Bayesian theorem. On its part, Bayesian theorem is a concept that converses the well-known conditional probability distribution. In probability distribution, an evidence is based on causes, whereas causes are based on evidence in Bayesian theorem. Thus, given two variables X and Y, the conditional probability of X, given that Y is true expressed in Eq. 1. The variable X normally represents a proposition or hypothesis, and Y represents an evidence or a new data.

$$p(X|Y) = \frac{p(X)p(Y|X)}{p(Y)} \tag{1}$$

Thus, provided that $p(Y) \neq 0$, then $p(X|Y)$ is the posterior probability of X considering a new evidence. Also, $p(X)$ is prior of X that shows a prior belief in X before new evidence Y, and $p(Y|X)$ is the likelihood function of evidence Y given that X has occurred. The main activities performed in Bayesian networking includes structure learning and parameter learning amongst others.

2.2.1 Structure Learning

Typically, Bayesian network comprises a network structure (or DAG) and a set of random variables $X = (x_1, x, x_3 \ldots .x_n)$ for learning the structure of the dataset by evaluating its posterior probabilities [49]. The DAG is represented as$g = (V, A)$, whereby V is vertex of each node in the graph, while A represents the direct and conditional dependencies between the variables of$X$. Also, a joint probability distribution is defined for variables of X, from network structure and the local probability distribution (P) at each node of the graph. In general, the joint probability distribution is expressed in Eq. 2 [28].

$$p(x) = \prod_{i=1}^{n} p(x_i | pa_i) \tag{2}$$

In which case, x_i is a node and its corresponding variable. Also, pa_i are the parent nodes of x_i in the graph, including the variables for the parent nodes. Hence, the entire ExtSRAM was built on Bayesian network and its integral artifacts like inferencing engine and conditional probability table (CPT).

2.2.2 Parameter Learning

The process of computing the probability of a desired variable (node) when given a Bayesian model is referred to as parameter learning. This probability must be computed because it is not directly obtainable from an arbitrary model. Thus, the probability of each node in the network is conditional upon its parent nodes. Although parameter learning is NP-hard problem, several methods have been developed to simplify the process of computing the CPT for a Bayesian network [60].

3 Related Work

In order to passably integrate context-awareness into risk evaluation procedure, this section reviewed previous works relating to core risk evaluation frameworks and models. Also, the section reexamined research efforts on the use of context-aware parameters for access control in ubiquitous computing.

3.1 Risk Evaluation Model

Alkussayer and Allen [3] proposed a dual-staged and hybridized model to simplify security analysis for software architecture using the analytic hierarchy process

(AHP). The study adopted a static approach to risk computation based on the risk factors that were relevant to the software domain. Nevertheless, this approach may be appropriate for relatively undynamic domains, but it will fall short of the security risks of a pervasive environment. In a similar study, Wei and Li [57] developed a security risk assessment model with formal safety assessment (FSA) and AHP to secure a typical information system. Similar to Alkussayer and Allen [3], the authors identified six risk factors that are peculiar to information systems without considering the roles of existing security countermeasures in the system.

Also, Sanchez [46] presented a risk and trust (ContextTrust) framework for a ubiquitous environment. The risk assessment module of the framework can model the contextual risk factors (and their dependencies) of participating mobile devices using logarithm random walk. However, the researcher did not consider the role of security countermeasures in the risk evaluation procedure and also assumed that all risk factors are characterized by logarithm random walk. Likewise, Wang and Jin [55] did not include security controls in the computation of risk scores in their proposed adaptive risk evaluation model for preservation of patient information in a health information system. The researchers applied the principle of need-to-know and Shannon entropy to ensure that medical doctors can access only necessary portion of patient's information during consultation. Similarly, Sharma et al. [50] developed task-based tisk-aware access control model for cloud-assisted eHealth. The researchers premised the module for risk evaluation on confidentiality, integrity, and availability (CIA). Analogous to Wang and Jin [55] and Sanchez [46], the risk evaluation module also excluded the effect of security control from the risk computation process.

Furthermore, Miura-ko and Bambos [40], Sato [48] presented risk analysis methods that incorporated the effectiveness of risk mitigation devices into risk computation. The two studies sufficiently justified the moderating effects of risk countermeasures in quantitative risk evaluation models. While the former represented countermeasures with a non-additive risk reduction matrix for generic risk computation, the latter employed a node-based evaluation of security controls that are implemented to independently safeguard computing infrastructures. On one hand, Sato [48] can be too basic for implementation in typical dynamic access control, on the other hand, Miura-ko and Bambos [40] considered only one active security control per risk evaluation session. The use of one countermeasure in risk evaluation is not always the case for secured operations in a pervasive strategy that requires a stack of countermeasures [7, 11]. Contrary to the approach adopted by Miura-ko and Bambos [40], Lo and Chen [37] developed a hybrid risk assessment procedure which measured mutuality among security countermeasures. Also, Lo and Chen [37] described the likelihood of threat occurrence as a function of vulnerabilities in security controls. Again, Lee et al. [36] presented a risk-adaptive access control framework that incorporated firewall provisioning as a countermeasure to accomplish zero-trust networking. Realistically, firewalls alone cannot mitigate threats in current pervasive networks.

In addition, Bojanc and Jerman-Blažič [9] proposed a monetary-inclined model, which primarily factored the role of security controls into a sequentially arranged four-phase risk management process. For adequate coverage and documentation, the authors classified security control into preventive, detective, or corrective measures. However, the model quantified security control from a financial perspective, also the model did not include the effect of security control stack. Furthermore, Aldini et al. [2] designed and validated an Opportunity-Enabled Risk Management (OPPRIM) methodology for regulating access to vital organization's resources in BYOD strategy. However, the risk evaluation module of OPPRIM did not explicitly outline the causal relationship among threats and the role of context-awareness parameters.

Similarly, Feng et al. [23] proposed a proactive security risk analysis model (SRAM) based on ant colony optimization (ACO) and Bayesian Network (BN). Mainly, the model considered casual relationships among risk factors and accounted for threats propagation path. In addition, Feng et al. [23] obtained information about model variables from experts and National Institute of Standards and Technology (NIST) guidelines on the standard for information systems. Remarkably, the risk evaluation component of the model computes risk scores from the probability of risk occurrence and severity after the occurrence. Also, SRAM carters for security countermeasures and allows new risk evidence to be added before computing risk value, thereby guaranteeing a dynamic risk analysis process. Implicitly, SRAM has some desirable elements for utilization in RAdAC, but it was not primarily designed for the purpose. Most especially, its direct application to access control in BYOD strategy without context awareness features cannot be guaranteed [31, 35].

3.2 Context-Aware Access Control Model

For some time now, research efforts that employed context data for secure access to crucial information assets have been conducted [15, 24, 29, 33, 39]. For instance, an in attempt to provide secured access control during military operations, Luo and Kang [38] presented risk-based mobile access control (RiMAC). The study employed contextual risk factors like location, authentications, threats, and timeouts to compute the risk of granting or denying access to information on battlefields. Nonetheless, RiMAC was specifically designed to function with onboard devices and a dedicated network, which cannot be imposed on BYOD stakeholders in civil business environments. Also, Kandala et al. [30] proposed an attribute-based framework that was superimposed on core components of RAdAC for dynamic and probabilistic risk determination. Majorly, the risk estimation function of the framework was based on request and access history. However, the framework only treated access control at coarse-level, because the computation of risk was not overtly defined for each access transaction.

Also, Atlam et al. [5] and Kang et al. [31] proposed a security framework for smart access control, which is based on historical and current context data that relate to user behavior patterns, and footprints of facilities usage, location, and time. More so, the authors suggested the use of Bayesian inference to provide dynamic and differential access to a resource in BYOD. Similarly, Ye et al. [59] developed a fine-grained access control called Attribute-tree Based Access Control (ATBAC) model, which was driven by users' contextual data for BYOD. Furthermore, Trnka and Cerny [51] extended the traditional RBAC with an additional security level, which is established on context-awareness components. However, Atlam et al. [5], Kang et al. [31], Ye et al. [59], and Trnka and Cerny [51] exclusively relied on contextual data to grant or deny a request by subjects without considering other elements of security, such as security countermeasures and threats.

Recently, Kang et al. [32] presented context-driven access control for BYOD called Poise, which combined the data plane programmability feature of software-defined network (SDN) with trust modeling concepts. The contextual data are extracted from network components like protocols, hardware, and data packets. Thus, rather than centralizing access control within enterprise servers, Poise employed the intelligent capabilities of SDN and high-tech topographies of user devices to decentralize access to vital organization resources. Nevertheless, Poise is hardware-centric, as a result, it did not explore the advances made in machine learning algorithms, risk attributes, and the contribution of existing security countermeasures when making access decisions.

3.3 Finding from Related Work

From the foregoing review, it was obvious that more research efforts are needed toward adaptive access control models that combine fundamental principles of risk evaluation, contributions of security countermeasures, machine learning algorithms, and contextual awareness. Such models should account for threats and their possible propagations, installed security countermeasures, especially with due attention to defense-in-depth. Similarly, in order to take advantage of the current and historical context variables for adaptive access control in pervasive environments like BYOD, the ensuing model should be driven by an appropriate machine learning algorithm.

4 Proposed ExtSRAM Model

Concisely, ExtSRAM is a risk-aware access control model that builds on the competency of SRAM, which was reviewed in Sect. 3.1 by incorporating context awareness into the latter. Thus, this section presents a bird's-eye view of ExtSRAM comprising of basic components such as risk factors, security countermeasures, and access control mechanism, together with their respective locations within a BYOD environment. Broadly, the high-level view of ExtSRAM can be segmented into two extensive areas namely; contextual risk factors and enterprise environment (enterprise information system).

4.1 Contextual Risk Factors

The contextual risk factor is a collection of dynamic factors that describes the behaviors of BYOD employee who uses a personal device to seek internal or remote access to the enterprise network. Thus, the risk factors are shown in Fig. 1, which represents the high-level view (architecture) of ExtSRAM, Generally, the factors are characterized by location (transiting, stationary), time, network, mobile device, and actions performed. These factors had been reported to be viable parameters for smart context mining and gaining insight into user behavior [31, 32, 36]. More so, personal attributes like keystrokes, mouse usage, mode of screen swipe, finger texture are

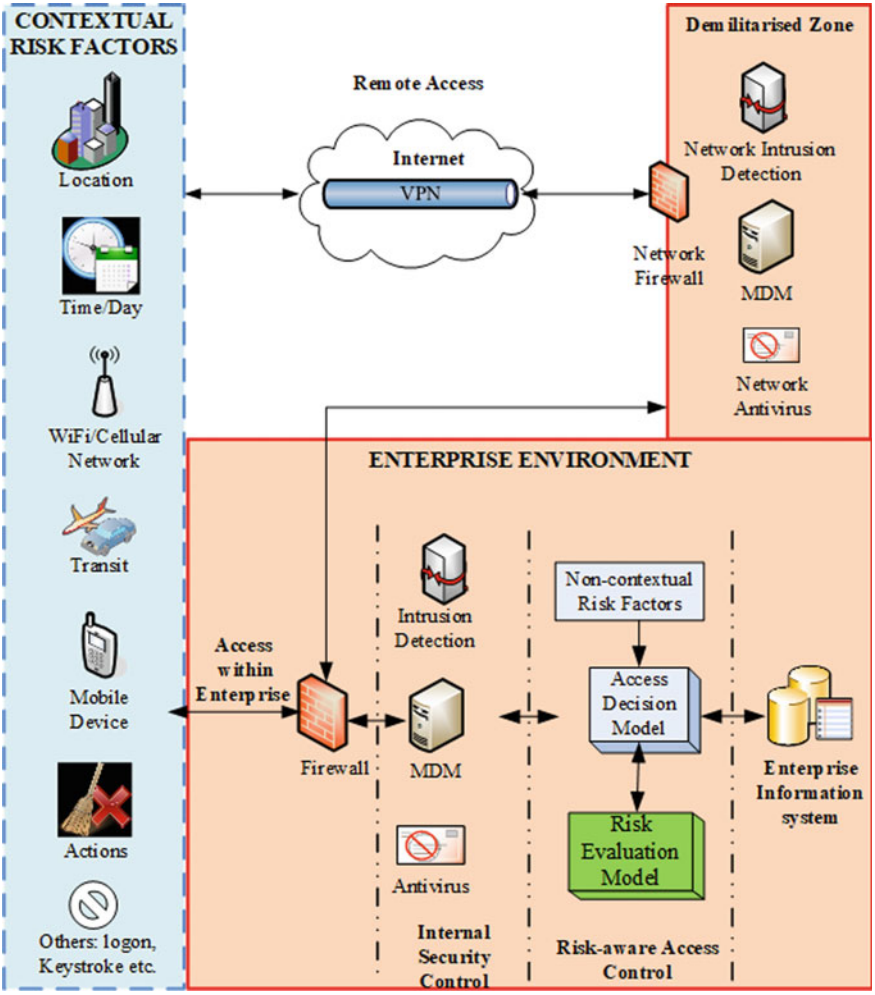

Fig. 1 High-level view of ExtSRAM model

other probable factors that can be captured as risk factors and utilized for contextual components of dynamic access control in pervasive environments. So, all necessary contextual information about a particular user will accompany each access request. Afterward, an access decision must be taken by the risk-aware access control, before a specific action can be performed by the user as expressed in the architecture.

4.2 Enterprise Environment

Generally, the enterprise environment comprises of non-contextual factors, enterprise systems, security countermeasures, and risk-aware access control. For clarity, Fig. 1 revealed the assemblage of IT infrastructures in a conventional enterprise environment that provide network connectivity and information delivery services via information systems to employees. Thus, static risk factors including environmental infrastructures, network, host/server computers, software, data, and communication facilities belong to enterprise environment [23]. Furthermore, it depicts the logical placement of countermeasures to ensure adequacy in terms of the technical, operational, and strategic security needs of the organization.

No doubt, providing unabridged security for BYOD still relies on conventional security techniques and controls like firewall, intrusion detection system, virtual private network (VPN), demilitarized zone (DMZ), antivirus, etc. However, the particular dimension of BYOD risks, necessitated the inclusion of specific security tools like mobile device management (MDM), mobile application management (MAM), mobile content management (MCM), virtualization, secured containers to mention but few [25]. In addition, the architecture further showcased the defense-in-depth initiative of modern security settings to support spatiotemporal forms of employee access to enterprise resources within or outside the enterprise perimeter.

Still, on the enterprise segment of the architecture, the risk-aware access control comprises of access decision model which is the central point of ExtSRAM. The access decision model is saddled with taking decision to either reject or accept incoming requests initiated by the user. Also, the decision model coordinates and formats the values relating to both contextual and non-contextual risk factors handles causal relationships among risk factors and considers the mitigating effects of stacked security controls. Likewise, it enforces the case-based decision according to risk value computed by risk evaluation model and other decision-making components such as risk threshold and heuristic judgement supplied by experts. Basically, the risk evaluation model computes risk value using the values acquired from the decision model.

5 ExtSRAM Process Flow

As described in Sect. 4, SRAM serves as the baseline model for ExtSRAM. Precisely, the last task performed by SRAM was to determine risk treatment plan for probable threat and vulnerability propagation paths in enterprise information system. However, this function is not required for adoption in dynamic risk-aware access control, so it is not included in the model presented in this study.

ExtSRAM adopts Bayesian network as its model building tool and functional block diagram was employed to illustrate its methodology (conceptual components). Thus, the entire ExtSRAM was built on Bayesian network and its integral artfacts like inferencing engine and CPT. Functional block diagram is modeling tool, which is mostly used in software engineering to represent the major functions in a model and their interactions. Fundamentally, a block diagram comprises some core components and their interactions Therefore, this study employed a functional block diagram as design tool to concretize the methodology in the extended model.

5.1 Assumptions on ExtSRAM Model

The proposed model is based on some assumptions to make its development realistic as well as to avoid replicating what has already been achieved in the baseline model.

1. Security risk propagation is assumed to be unidirectional, that is, from the subject (employee or mobile unit) to object (enterprise information systems).
2. Security risk is assessed to be a change in subject context, as well as, enterprise system variables.
3. There may be conditional dependencies among some contextual and enterprise system variables.
4. The proposed model covers the authorization aspect of access control.
5. The assumptions made during SRAM development are taken to be realistic.
6. The validity test conducted on SRAM are presumed to be reliable.

5.2 ExtSRAM Methodology

The entire ExtSRAM is vertically divided into four sections namely; variable definition and management, Bayesian model, Bayesian inference, and risk module as shown in Fig. 2. To begin with, the discovery and formal description of all model variables will be carried out in the variable definition and management section. In order to evolve these variables, relevant guidelines and standards for risk assessment in pervasive computing and domain experts will be consulted. In addition, the tasks scheduled for this topmost section include management of historical data, as well as, the development and use of ACO as described in the baseline model.

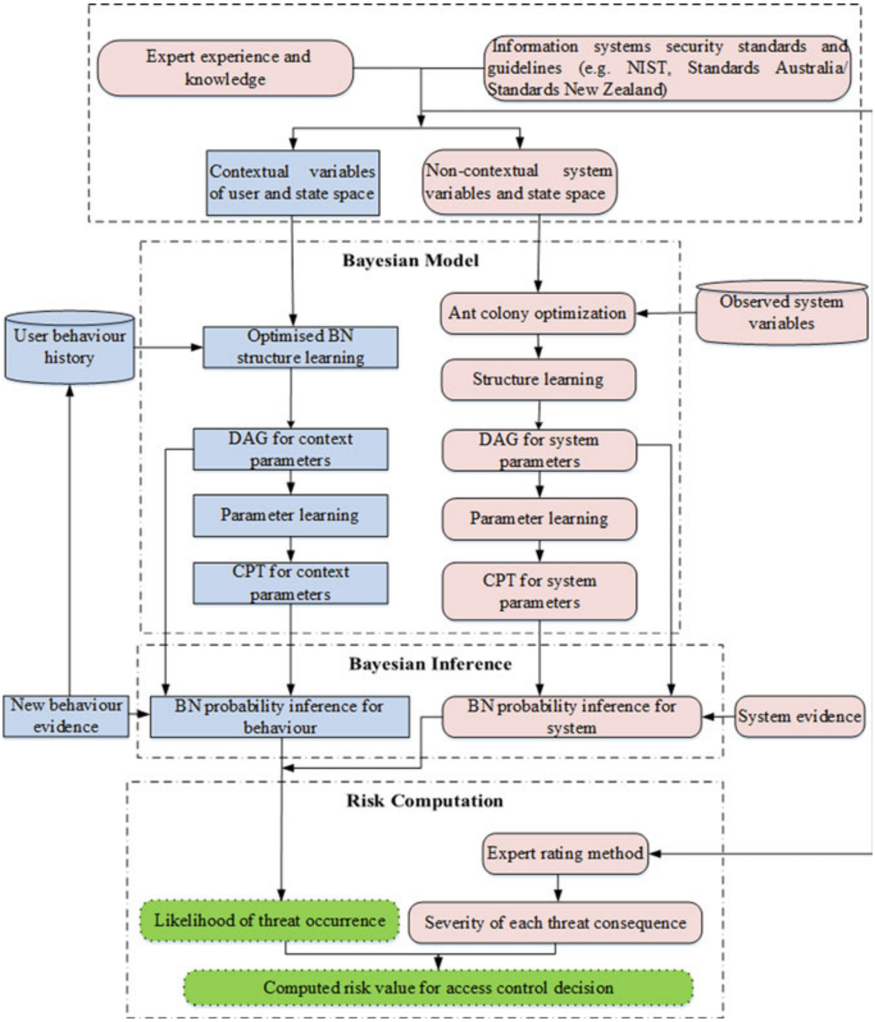
Expert experience and knowledge
Information systems security standards and guidelines (e.g. NIST, Standards Australia/ Standards New Zealand)
Contextual variables of user and state space
Non-contextual system variables and state space
Bayesian Model
User behaviour history
Optimised BN structure learning
Ant colony optimization
Observed system variables
Structure learning
DAG for context parameters
DAG for system parameters
Parameter learning
Parameter learning
CPT for context parameters
CPT for system parameters
Bayesian Inference
New behaviour evidence
BN probability inference for behaviour
BN probability inference for system
System evidence
Risk Computation
Expert rating method
Likelihood of threat occurrence
Severity of each threat consequence
Computed risk value for access control decision

Fig. 2 Detailed ExtSRAM model

Next, a Bayesian model comprising of network structure and CPT will be developed separately from contextual variables and system variables for user profiling and enterprise system risk modeling, respectively. Thereafter, the current security posture of the system and user behavioral evidences will be utilized for BN inferencing. Lastly, the quantified risk value associated with a particular request will be evaluated by the risk module from two key parameters, namely, the likelihood of threat occurrence and severity of impact after occurrence.

Furthermore, the methodology was rendered with functional block diagram as shown in Fig. 2. Generally, the methodology consists of set blocks which are logically classified into three, namely, core, user profiling, and risk computation blocks.

5.2.1 Static Risk Analysis Blocks

The blocks with round edges are the components inherited from SRAM for handling static risk variables pertaining to exposure of enterprise system to BYOD security risks. Hence, some tasks including, identifying non-contextual risk factors by experts, harnessing experts' opinions on the method and scale for rating the severity of threats, evaluating security controls within enterprise environment, identifying threats and their causal relationships, maintaining the database of observed system variables, developing Bayesian oriented risk evaluation model and drawing inference with system evidence variables are undertaken in these blocks. A specific but comprehensive description of each block is available in [23].

5.2.2 User Profiling Blocks

The user profiling blocks are represented with square edges and are built on contextual variables of BYOD users. The collective target of these blocks is to estimate the probability of threat occurrence, arising from a request made by BYOD users. This probabilistic estimation is based on contextual parameters. Thus, to easily combine the results from profiling blocks and static risk analysis blocks, this study proposed the use of Bayesian model. Specifically, the Bayesian modeling is employed as a machine learning tool, to understand and draw inferences for the likelihood of threat from user behavior analytics with regards to interactions with the enterprise system. Therefore, Bayesian network and related CPTs would be formulated on contextual data. Also, inferences would be drawn from both current user profile and new contextual evidence that are extracted from the user's access request. Hence, some blocks that are similar in terms of functionalities, and which are located within the Bayesian model and Inference sections of the model can utilize the same techniques for static risk analysis and user profiling tasks. For brevity, understanding of the fundamental techniques for such blocks is assumed. Consequently, the following subsections explain the new blocks or those that significantly vary from corresponding static analysis blocks.

Contextual Variables of User

Primarily, the function of this block (contextual variables and state space) is to define and harness contextual variables and their particular state spaces that can uniquely differentiate users. The variables are expected from sources like experts' opinions and excerpts from information security standards (or guidelines) and academic publications. More so, the sources of contextual variables should provide adequate definitions for all the variables. Also, the definitions of variable are essential for predicting user's pattern of seeking access to information system, level of granularity for access control configuration by security administrators and user privacy issues concerning contextual data acquisition and storage. For example, in the case of spatiotemporal data, time as a risk factor might be defined as an hour of the day, rather than a day of the week to achieve a well-refined access control. Likewise, location coordinates obtained via Global Positioning System (GPS) can aid fine-grained access, better than the name assigned to a particular location. However, the right balance should be struck between fine-grained metrics for measuring sensitive contextual variables and their implications on user privacy.

Optimized Bayesian Network Structure Learning

The block determines the most appropriate Bayesian network to represent user contextual data that are stored in the user behavior repository. Within this block, the task of selecting an apt structure for subsequent DAG construction is optimized. This optimization can be achieved by setting the appropriate parameters of search and score algorithms that are employed for the Bayesian network development.

Probability Inference of Behavior

Mainly, the block can query the Bayesian model to estimate the probability that a specific action has been carried out by a certain user in the past with respect to other contextual variables. The values of the variables are mined from new evidences in the current user's request for access to an action with previous occurrences. Thus, the result from this block determines the overall likelihood of threat occurrence, which may either increase or decrease. Afterward, the estimated threat likelihood contributes to the overall risk value, which enterprise information system operating in BYOD strategy might be exposed to. Therefore, the risk value depends on the anomaly or similarity between the new evidence and the previous access profile of the user.

5.2.3 Risk Computation Blocks

These blocks are further subdivided into two separate blocks to handle threat likelihood and overall risk computation. These two blocks are represented with dashed round edges. Precisely, the likelihood of threat occurrence comprises of inferences drawn from user behavior and system threat profile for a particular user request. In order to compute the impending security risk in user's request, the risk computation block utilizes outputs from likelihood of threat occurrence and envisaged severity of each threat after occurrence. Functionally, Eq. 3 represents the main parameters for risk evaluation in ExtSRAM, which allows an organization to adopt quantitative or semi-quantitative implementation for the risk computation block.

$$R = f(\omega_c, \omega_s, l_c, l_s, I) \tag{3}$$

where R is the estimated risk of granting access for an action to be performed, I is severity of threat occurrence, l_c and l_s are derivates of Bayesian models, and they represent the likelihoods (probabilistic values) of threat occurrences through contextual risk factors and risk factors of enterprise information system, respectively. Similarly, ω_c means the contextual weight and ω_s represents the weight of enterprise information system. That is, if l_c and $l_s \in L$, then $L : [0, 1] \rightarrow [0, 1]$. In which case, L is the combined likelihood of threat occurrences from contextual and system risk factors. Also, the weights are arbitrary constants which can moderate the likelihood of threat when its value is not equal to 1. For example, the values assigned to the weights might be configured to differentiate between requests from BYOD users who are within enterprise network and those outside the network. For the simplest case, the parameters are modeled as shown in Eq. 4.

$$R = I\left(\frac{\omega_c l_c + \omega_s l_s}{2}\right) \tag{4}$$

Nevertheless, when multiple threats can accompany a request with intent to individually or collectively exploit an enterprise information system, then risk value can be evaluated as shown in Eq. 5. In such case, n is the number of threats, whereas l_{cj} and l_{sj} are likelihoods of threat occurrences through contextual and system risk factors respectively, for particular threat j.

$$R = \sum_{j=1}^{n} I_j\left(\frac{\omega_c l_{cj} + \omega_s l_{sj}}{2}\right) \tag{5}$$

6 Theoretical Validation of the Model

This section provides theoretical validation for ExtSRAM, which is premised on the soundness and completeness of the proposed model. The validation follows the earlier stated assumptions (5) and (6) in Sect. 5.1 that a reliable validation was conducted on SRAM.

6.1 Soundness of ExtSRAM

In order to validate soundness of the model, the authors postulated that the combined likelihood of threats and weights from both user contextual variables and enterprise information systems (static variables) will functionally satisfy the five conditions listed below.

1. $\forall l_c, l_s, \omega_c, \omega_s \in \mathbb{R}^+$
2. $0 < l_c, l_s, \omega_c, \omega_s \leq 1$
3. $0 < (l_c + l_s)/2 \leq 1$
4. $0 < (\omega_c + \omega_s)/2 \leq 1$
5. $0 < \omega_c l_c, \omega_s l_s \leq 1$

Note that, the values of l_c and l_s are probabilistic outcomes of the Bayesian models developed from static risk analysis and user profiling blocks, respectively. Thus, the combined values from these two major blocks would still satisfy basic probability conditions. With regards to the computed risk values, these are necessary conditions for the derivatives of Eq. (5) to be true representatives of real-life implementations.

In order to reinforce the soundness of Eq. (5), ten sets of random values were generated for the parameters in the equation. Each set of values is assumed to represent a known security threat that can be linked to an access request. The generated values for ω_c, ω_s, l_c and l_s were constrained to be within the range [0, 1] for the five conditions listed for the equation to be satisfied. However, the values for impact (I) of threat can be determined by the organization. For this demonstration, the value of impact is a random number between 1 and 10. The estimated risk value for each threat and the overall risk value for all the threats are shown in Table 1.

Table 1 Risk estimation for access request

Threat	l_s	l_c	w_s	w_c	$(w_s l_s + w_c l_c)/2$	Impact (I)	Estimated risk value
1	0.54	0.26	0.63	0.1	0.18	3	0.548764951
2	0.17	0.59	0.01	0.16	0.05	3	0.144674895
3	0.34	0.45	0.2	0.31	0.1	1	0.102939648
4	0.94	0.17	0.15	0.91	0.15	8	1.183142913
5	0.46	0.75	0.07	0.08	0.05	4	0.182067431
6	0.41	0.12	0.42	0.56	0.12	2	0.235882753
7	0.54	0.5	0.19	0.62	0.21	9	1.864801307
8	0.06	0.21	0.14	0.26	0.03	2	0.063811237
9	0.58	0.82	0.91	0.74	0.57	2	1.137792092
10	0.36	0.07	0.43	0.13	0.08	5	0.408285538
					Total estimated risk		**5.872162764**

Likelihood of threat from contextual factor (l_s), Likelihood of threat from enterprise information system (l_c), Enterprise information system weight (w_s), Contextual weight (w_c), Likelihood of threat ($(w_s l_s + w_c l_c)/2$)

As revealed in Table 1, all the computed values for $\frac{\omega_c l_c+\omega_s l_s}{2}$, which represent the likelihood of threat occurrence is within probabilistic range of [0, 1]. Moreover, the total estimated risk value will always depend on the values assigned to the impact of a known threat. Therefore, the result from the ExtSRAM will consistently quantify the risk of granting access to BYOD user's request.

6.2 Completeness of ExtSRAM

In order to completely describe the ExtSRAM, the contextual risk factors for user behavior profiling and the counterpart risk factors for static risk analysis will be drawn from domain experts, well-established standards, and guidelines. Therefore, the experts' input into the selection and definition of the factors will ensure the inclusion of all relevant contextual and non-contextual variables that are necessary for the development of a proposed model for BYOD security risks. In addition, the experts and relevant literatures will serve as a guide for itemizing the existing security countermeasures and their likely performance ratings. Similarly, such guidance would reveal current security threats relating to access control in BYOD further enrich the model.

7 Future Research Directions

Really, ExtSRAM as presented in this study is meant to provoke researchers' thoughts on the benefits and implications of combining static risk factors, contextual risk factors, countermeasures, and risk evaluation concepts for dynamic authorization in pervasive environments. Importantly, subsequent researches can explore abundant possibilities of implementing the model for specific BYOD domains like academic institutions, health management organizations, public commissions, and agencies. More so, attempts can be made to utilize other contemporary machine learning and deep learning algorithms to model the static risk analysis blocks and user profiling blocks. In addition, future researches can implement the model to mitigate access control challenges in emergent computing strategies including cloud computing, IoT and Fog computing. As part of future researches in this direction, the authors intend to develop and empirically validate the user profiling blocks of ExtSRAM.

8 Conclusion

In a word, BYOD remains an imperative IT strategy that continues to dynamically reshape enterprise work environments, improves productivity, and enhances employee workstyles. Unfortunately, as the pervasion of BYOD spreads with abundant benefits, so also, are the security consequences it leaves behind for organizations to surmount. Certainly, dynamic access control remains one viable countermeasure for securing access to vital organization resources against the security risks that accompanied BYOD adoption. Thus, this study developed ExtSRAM as a dynamic risk-based and context-aware paradigm that integrated three major components namely; user contextual data, static risk analysis (which incorporates threat propagation and existing countermeasures), and machine learning algorithm. Similarly, a novel mathematical model was developed for dynamic risk evaluation in ExtSRAM. For flexibility and dynamism, the novel model can serve as an add-on to static access control models for possible adoption in pervasive domains. As a case in point, subsequent implementation of ExtSRAM will certainly assist organizations to reap lofty benefits from BYOD while securing the critical resources from security risks. In another case, ExtSRAM opened another frontier for research activities on risk-aware access control for other pervasive environments.

References

1. Ahmed, A., Zhang, N.: An access control architecture for context-risk-aware access control: architectural design and performance Evaluation. In: Fourth International Conference on Emerging Security Information Systems and Technologies (SECURWARE), IEEE, Venis, pp. 251–260 (2010). https://doi.org/10.1109/SECURWARE.2010.48
2. Aldini, A., Carlos, J.S., Lafuente, B., Titi, X., Guislain, J.: Design and validation of a trust-based opportunity-enabled risk management system. Inf. Comput. Secur **25**(1–31) (2017)
3. Alkussayer, A., Allen, W.H.: Security risk analysis of software architecture based on AHP. In: 7th International Conference on Networked Computing, pp. 60–67. IEEE, Gyeongsangbuk-do, Korea (2011)
4. Alotaibi, B., Almagwashi, H.: A review of BYOD security challenges, solutions and policy best practices. In: 2018 1st International Conference on Computer Applications & Information Security (ICCAIS), pp. 1–6. IEEE (2018). https://doi.org/10.1109/CAIS.2018.8441967
5. Atlam, H.F., Alenezi, A., Walters, R.J., Wills, G.B., Daniel, J.: Developing an adaptive Risk-based access control model for the Internet of Things. In: International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp. 655–661. IEEE, Exeter, UK (2017). https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData.2017.103
6. Bedi, P., Kaur, H., Gupta, B.: Trust-based access control for collaborative systems. J. Exp. Theor. Artif. Intell. **26**(1), 109–126 (2014). https://doi.org/10.1080/0952813X.2013.813973
7. Bijon, K.Z., Krishnan, R., Sandhu, R.: A framework for risk-aware role based access control. In: 2013 IEEE Conference on Communications and Network Security (CNS), pp. 462–469. IEEE, Washington (2013). https://doi.org/10.1109/CNS.2013.6682761
8. Blizzard, S.: Coming full circle: Are there benefits to BYOD? Comput. Fraud Secur. **2015**(2), 18–20 (2015). https://doi.org/10.1016/S1361-3723(15)30010-5
9. Bojanc, R., Jerman-Blažič, B.: A quantitative model for information security risk management. Eng. Manag. J. **25**(2), 25–37 (2013)
10. Bonate, P.L.: COVID-19: opportunity arises from a world health crisis. J. Pharmacokinet Pharmacodyn. **47**(2), 119–120 (2020). https://doi.org/10.1007/s10928-020-09681-5
11. Cabarcos PA (2011) Risk assessment for better identity management in pervasive environments. In: Fourth Annual Ph.D. Forum on Pervasive Computing and Communications, pp. 389–390. IEEE, Seattle, WA (2011)
12. Chen, L., Crampton, J.: Risk-aware role-based access control. In: Meadows, C., Fernandez-Gago, C. (eds.), Security and Trust Management, pp. 146–150. Springer, Berlin (2012). https://doi.org/10.1007/978-3-642-29963-6_11

13. Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., Stoddart, K.: A review of cyber security risk assessment methods for SCADA systems. Comput. Secur. **56**(2016), 1–27 (2016). https://doi.org/10.1016/j.cose.2015.09.009
14. CLUSIF: Risk management-concepts and methods. CLUSIF 2008/2009. Paris (2008).
15. Costabello, L., Villata, S., Delaforge, N., Gandon, F.: Linked data access goes mobile: context-aware authorization for graph stores. In: CEUR Workshop Proceedings, p. 937 (2012).
16. Djalante, R., Lassa, J., Setiamarga, D., Mahfud, C., Sudjatma, A., Indrawan, M., Haryanto, B., Sinapoy, M.S., Rafliana, I., Djalante, S., Gunawan, L.A., Anindito, R., Warsilah, H., Surtiari, I.G.A.: Review and analysis of current responses to COVID-19 in Indonesia: Period of January to March 2020. Prog. Disaster Sci. **6**, 100091 (2020). https://doi.org/10.1016/j.pdisas.2020.100091
17. Doargajudhur, M.S., Dell, P.: The effect of Bring Your Own Device (BYOD) adoption on work performance and motivation. J. Comput. Inf. Syst. **00**(00), 1–12 (2018). https://doi.org/10.1080/08874417.2018.1543001
18. Dorri Nogoorani, S., Jalili, R.: TIRIAC: a trust-driven risk-aware access control framework for Grid environments. Future Gener. Comput. Syst. **55**, 238–254 (2016). https://doi.org/10.1016/j.future.2015.03.003
19. dos Santos, D.R., Marinho, R., Schmitt, G.R., Westphall, C.M., Westphall, C.B.: A framework and risk assessment approaches for risk-based access control in the cloud. J. Netw. Comput. Appl. **74**, 86–97 (2016). https://doi.org/10.1016/j.jnca.2016.08.013
20. Emami, S.S., Amini, M., Zokaei, S.: A context-aware access control model for pervasive computing environments. In: The 2007 International Conference on Intelligent Pervasive Computing (IPC 2007), pp. 51–56. IEEE, Jeju City, South Korea (2007). https://doi.org/10.1109/IPC.2007.28
21. Fall, D., Blanc, G., Okuda, T., Kadobayashi, Y.: Toward quantified risk-adaptive access control for multi-tenant cloud computing. In: Proceedings of the 6th Joint Workshop on Information Security (JWIS 2011), pp. 1–14. JWIS, Kaohsiung (2011)
22. Fani, N., Von Solms, R., Gerber, M.: Governing information security within the context of "Bring Your Own Device in SMMEs." In: IST-Africa 2016 Conference Proceedings, pp. 1–11. Durban, South Africa (2016)
23. Feng, N., Wang, H.J., Li, M.: A security risk analysis model for information systems: causal celationships of risk factors and vulnerability propagation analysis. Inf. Sci. **256**(2014), 57–73 (2014). https://doi.org/10.1016/j.ins.2013.02.036
24. Fischer, G.: Context-aware systems: the 'right' information, at the 'right' time, in the 'right' place, in the 'right' way, to the 'right' person. In: Advanced Visual Interfaces International Working Conference, pp. 287–294. ACM, Capri Island (Naples), Italy (2012)
25. Ganiyu, S.O., Jimoh, R.G.: Characterising risk factors and countermeasures for risk evaluation of bring your own device strategy. Int. J. Inf. Secur. Sci. **7**(1), 49–59 (2018)
26. Ganiyu, S.O., Jimoh, R.G.: Comparative analysis of risk evaluation models for risk-aware access control in bring your own device environment. Int. J. Inf. Secur. Res. (IJISR) **8**(2), 810–820 (2018)
27. Hajdarevic, K., Allen, P., Spremic, M.: Proactive security metrics for bring your own device (BYOD) in ISO 27001 supported environments. In: 2016 24th Telecommunications Forum (TELFOR), pp. 1–4. IEEE, Belgrade, Serbia (2016)
28. Heckerman, D.: A tutorial on learning with Bayesian networks. Stud. Comput. Intell. **156**(January), 33–82 (2020). https://doi.org/10.1007/978-3-540-85066-3_3
29. Hong-yue, L., Miao-lei, D., Wei-dong, Y.: A context-aware fine-grained access control model. In: 2012 International Conference on Computer Science and Service System(SSS), pp. 1099–3656. IEEE, Nanjing, China (2012). https://doi.org/10.1109/CSSS.2012.278
30. Kandala, S., Sandhu, R., Bhamidipati, V.: An attribute based framework for risk-adaptive access control models. In: Proceedings of the 6th International Conference on Availability, Reliability and Security, pp. 236–241. IEEE, Vienna (2011). https://doi.org/10.1109/ARES.2011.41
31. Kang, D., Oh, J., Im, C.: Context based smart access control on BYOD environments. In: International Workshop on Information Security ApplicationsWISA 2014: Information Security Applications, pp. 165–176 (2015). https://doi.org/10.1007/978-3-319-15087-1

32. Kang, Q., Xue, L., Morrison, A., Tang, Y., Chen, A., Luo, X.: Programmable In-Network Security for Context-aware BYOD Policies. In 29th USENIX Security Symposium (SEC'20), pp. 1–21. Boston, MA (2020).
33. Kayes, A.S.M., Han, J., Rahayu, W., Islam, M.S., Colman, A.: A policy model and framework for context-aware access control to information resources. Comput. J. bxy065, 1–24 (2013)
34. Kiran, K.V.D., Mukkamala, S., Katragadda, A., Reddy, L.S.S.: Performance and analysis of risk assessment methodologies in information security. Int. J. Comput. Trends Technol. (IJCTT) **4**(10), 3685–3692 (2013)
35. Koh, E.B., Oh, J., Im, C.: A study on security threats and dynamic access control technology for BYOD, smart-work environment. In Proceedings of the International Multi Conference of Engineers and Computer Scientists 2014, vol. II. IMECS, Hong Kong (2014)
36. Lee, B., Vanickis, R., Rogelio, F., Jacob, P.: Situational awareness based risk-adapatable access control in enterprise networks. In: 2nd International Conference on Internet of Things, Big Data and Security (IoTBS), pp. 400–405. Porto, Portugal (2017). https://doi.org/10.5220/0006363404000405
37. Lo, C., Chen, W.: A hybrid information security risk assessment procedure considering interdependences between controls. Expert Syst. Appl. **39**(2012), 247–257 (2012). https://doi.org/10.1016/j.eswa.2011.07.015
38. Luo, J., Kang, M.: Risk based mobile access control (RiBMAC) policy framework. In: The 2011 Military Communications Conference, pp. 1448–1453. IEEE, Baltimore, Maryland, USA (2011)
39. Miettinen, M., Heuser, S., Sadeghi, A.: ConXsense –automated context classification for context-aware access control. In: 9th ACM Symposium on Information, Computer and Communications Security (ASIACCS 2014), pp. 293–304. Kyoto, Japan (2014)
40. Miura-ko, R.A., Bambo, N.: Dynamic risk mitigation in computing infrastructures. In: Third International Symposium on Information Assurance and Security, pp. 325–328. IEEE, Manchester (2007). https://doi.org/10.1109/IAS.2007.91
41. Morrison, A., Xue, L., Chen, A., Luo, X.: Enforcing context-aware BYOD policies with in-network security. In: 10th USENIX Workshop on Hot Topics in Cloud Computing (HotCloud'18). Boston, MA (2018)
42. O'Neill, M.: The Internet of Things: Do more devices mean more risks? Comput. Fraud Secur. **2014**(1) (2014). https://doi.org/10.1016/S1361-3723(14)70008-9
43. Redmond, J., Fong, B.: Crafting an effective Bring Your Own Device (BYOD) policy. Units Magazine (2018)
44. Rose, C.: BYOD: An examination of bring your own device in business. Rev. Bus. Inf. Syst. **17**(Second Quarter), 65–70 (2013)
45. Sadiku, M.N.O., Nelatury, S.R., Musa, S.M.: Bring your own device. J. Sci. Eng. Res. **4**(4), 163–165 (2017)
46. Sanchez, C.A.: A risk and trust security framework for the pervasive mobile environment. University of Oklahome (2013)
47. Santos, D.R., Westphall, C.M., Westphall, C.B.: A dynamic risk-based access control architecture for cloud computing. In: Network Operations and Management Symposium, pp. 1–9. IEEE, Krakwo, Poland (2014). https://doi.org/10.1109/NOMS.2014.6838319
48. Sato, H.: 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, pp. 1243–1248. IEEE, Boston (2011). https://doi.org/10.1109/PASSAT/SocialCom.2011.44
49. Scutari, M.: An empirical-bayes score for discrete Bayesian networks. In: Proceedings of the Eighth International Conference on Probabilistic Graphical Models, vol. PMLR 52, pp. 438–448). Lugano (Switzerland) (2016)
50. Sharma, M., Bai, Y., Chung, S., Dai, L.: 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, pp. 1047–1052. IEEE, Liverpool, United Kingdom (2012). https://doi.org/10.1109/HPCC.2012.153

51. Trnka, M., Cerny, T.: On security level usage in context-aware role-based access control. In: The 31st ACM/SIGAPP Symposium on Applied Computing, pp. 1192–1195. ACM , Pisa, Italy (2016).
52. Ubene, O.E., Agim, U.R., Umo-Odiong, A.: The impact of Bring Your Own Device (BYOD) ON Information Technology (It) security and infrastructure in the Nigerian Insurance Sector. Am. J. Eng. Res. (AJER) **7**(5), 237–246 (2018)
53. Vaidya, R.: Cyber Security Breaches Survey 2018: Statistical Release. Portsmouth (2018)
54. Veljkovic, I., Budree, A.: Development of bring-your-own-device risk management model: a case study from a South African Organisation. Electron. J. Inf. Syst. **22**(1), 1–14 (2019)
55. Wang, Q., Jin, H.: Quantified risk-adaptive access control for patient privacy protection in health information systems. In: ASIACCS'11, pp. 406–410. ACM, Hong Kong (2011)
56. Weber, L., Rudman, R.J.: Addressing the incremental risks associated with adopting bring your own device. J. Econ. Financ. Sci. **11**(1), 1–7 (2018). https://doi.org/10.4102/jef.v11i1.169
57. Wei, Z., Li, M.: Information security risk assessment model base on FSA and AHP. In: Proceedings of the Ninth International Conference on Machine Learning and Cybernetics, pp. 11–14. IEEE, Qingdao (2010)
58. Yang, X., Wang, X., Yue, W.T., Sia, C.L., Luo, X.: Security policy opt-in decisions in Bring-Your-Own-Device (BYOD)–a persuasion and cognitive elaboration perspective. J. Organ. Comput. Electron. Commer. **29**(4), 274–293 (2019). https://doi.org/10.1080/10919392.2019.1639913
59. Ye, D., Mei, Y., Shang, Y., Zhu, J., Ouyang, K.: Mobile crowd-sensing context aware based fine-grained access control mode. Multimed. Tools Appl. **75**(21), 13977–13993 (2015). https://doi.org/10.1007/s11042-015-2693-3
60. Zhiwei, Y., Zhongyuan, J.: A survey on the evolution of risk evaluation for information systems security. Energy Procedia **17**(2012), 1288–1294 (2012). https://doi.org/10.1016/j.egypro.2012.02.240
61. Zhu, Z., Xu, R.: A context-aware access control model for pervasive computing in enterprise environments. In 4th International Conference on Wireless Communications, Networking and Mobile Computing, WiCOM'08, pp. 1–6. IEEE, Dalian, China (2008). https://doi.org/10.1109/IPC.2007.28