A Context-Based Personalization for Mobile Applications' Network Access

Yaser Mowafi[1(✉)], Tareq Alaqarbeh[2], and Rami Alazrai[2]

[1] Department of Information Systems, Sultan Qaboos University, Muscat, Oman
mowafi@squ.edu.om
[2] School of Computer Engineering and Information Technology, German Jordanian University, Amman, Jordan
{tareq.alaqarbeh, rami.azrai}@gju.edu.jo

Abstract. In this paper, we propose a context-based framework for eliciting context information and adapting this information with mobile applications network access decision mechanism. The framework leverages the execution of mobile applications inside a sandbox to control the communication between mobile applications and mobile device resources. Applications' access requests are analyzed based on user's context information collected from the mobile device sensors and the application network access configuration. We validate our proposed framework in Android Operating System running on handheld smartphone devices. Preliminary results revealed the efficacy of our proposed context-based framework in providing network access control management based on users' context information at run-time.

Keywords: Context awareness · Mobile computing · Recommendation system · AHP

1 Introduction

Significant advancements in mobile technologies have shifted personal computing to pervasive and ubiquitous sphere. Many use their mobile devices for their most daily tasks such as emails, text messaging, documents viewing, mapping, as well as for entertainment. Such value-added services typically require collecting not only users' personal information, such as location or identification [1], but also gathering and transmitting trust sensitive information [2].

Today, nearly 70 % of the network usage actions generated by third party mobile applications' services have become invisible to the users [3]. According to [4], most of the current existing mobile platforms (i.e., Android, Apple and iOS) typically leave it to users to specify the permission of mobile applications' access to users' personal information. More critically, survey studies report a lack of users' awareness of privacy breach and security risks associated with installing third party mobile applications [5]. That said, ensuring users' awareness of trust and security controls needs to start from the mobile devices. For example, [6] proposes leveraging the level of privileges of mobile devices' owners in terms of trust and security controls, commonly set by default at low levels throughout the installation lifecycle of applications on these devices, to

M. Younas et al. (Eds.): MobiWIS 2016, LNCS 9847, pp. 406–415, 2016.
DOI: 10.1007/978-3-319-44215-0_34

protect users' information from malicious attacks and/or intrusions. In addition, [7] suggests a framework to shadow users' personal data in places that users wants to keep private to block network transmissions that contain such data. Similarly, [8, 9] propose just-in-time notifications that appear when users' personal data is subject to sharing and displays a visual summary of the shared subject data. However, such security control measures and much of the existing security management mechanisms do not take into account the nature of users' context in mobility.

As research and practice on context-based mobile computing have achieved remarkable success, context-based network access in mobility is still at infancy. The main challenge that renders context-based solutions of ubiquitous computing systems compared to traditional information access systems is that the later handles access threats based on set scenarios of specific protection needs and policies in accordance to those needs. In ubiquitous computing environments, network access alternatives should be supported in the situation where and when the decision is required. Hence, current context needs to be considered to effectively control a given situation. In order to address the aforementioned deterrents, we propose a context-based network access framework for eliciting context information and adapting this information with mobile applications' network access measure. The network access measure is determined based on both the context information collected from the mobile device sensors and the user's settings of the mobile application network access. The user settings provide a mechanism to prioritize the importance of contexts towards the network access control of each mobile application. We implement the proposed framework in the Android Operating System (OS) for mobile devices. The remainder of this paper is structured as follows. In Sect. 2, we describe the context-aware network access framework architecture. Section 3 presents the AHP method. In Sect. 4, we present a prototype and evaluation of our network access control mechanism. Section 5 reviews related work. We conclude the paper with final comments.

2 Architectural Design

Our proposed framework extends an earlier proposed architecture [10] that aims to control the communication among mobile applications and mobile device resources at run-time. The framework consists of a mobile application sandbox and a context shadow application. To avoid any changes to mobile OS, the framework component is implemented as a shadow application. The sandbox is built inside the mobile OS. Mobile application data, code execution, and network access are all concealed within the sandbox. Any network access can only go through the sandbox.

When a running mobile application attempts to get a network access, the application sends TCP SYN request as part of a TCP handshake. This triggers a checking request in the sandbox, which in turn triggers a request in the shadow application. The shadow application examines the request based on both the context information collected from the mobile device sensors, and the user configuration of the mobile application network access settings using the Analytic Hierarchy Process method, discussed in Sect. 3, to provide the appropriate network access of allow or restrict recommendation decision. This decision will then be returned to the sandbox.

3 Analytic Hierarchical Process Method

Given that context dynamically combines a variety of heterogeneous context measures. While some measures are tangible and objectively measured, other measures are intangible and subjectively measured. To model the inherent interdependency of such various criteria measures of comprehended sub-problems into a single integrated decision problem, each of which can be evaluated independently. Hence, from a decision making perspective it will be necessary to consolidate these context measure into single integrated decision problem. Such consolidation allows for establishing a multi-criteria decision making (MCDM) [11]. A common methodology for dealing with MCDM problems is the Analytic Hierarchy Process (AHP) method [12]. One advantage of the AHP method that (a) it enables to breakdown unstructured complex decision problems into smaller constituent components in order to construct an integrative hierarchy, and (b) its capability of handling both tangible and intangible criteria that entails a systematic procedure in the thought process. AHP has been widely used in a variety of policy selection and decision making [13], adaptive learning [14], and recommendation and feedback systems [15].

When applied in decision problems, the AHP method assists in describing a general decision operation by decomposing the decision problem into a multi-level hierarchic structure. We apply the AHP method to perform a paired comparison among the contexts (i.e., location, time, and network) to determine the relative weights of the mobile application network access decision alternatives, secure and insecure network access (Fig. 1). The AHP structure represents the problem decision goal (context network access); the decision problem alternatives (secure and insecure) $A_1 \ldots A_i$; and the decision criteria (Location, Time, Network) C_i and Sub-criteria $C_{i,j}$. The weights ω_i and ω_{ij} are determined through a pair-wise comparison of C_i and $C_{i,j}$, respectively. In determining the relative weights of the decision problem alternatives, the AHP applies eigenvalue method to determine a ranking weight for each criterion and its sub-criteria variables using a pair-wise comparison among each alternative, and then consolidate the weighted values of the hierarchy alternatives to create an overall priority value for each alternative relative to the overall decision goal [16].

Consolidating the weighted values is performed via component measure priorities assigned by the decision maker to create an overall decision value for each alternative. For example, a pair-wise comparison of q elements' weights, $\omega_1, \omega_2, \ldots \omega_q$ is performed via composing the following comparison matrix, every element a_{ji} of each trial is the result of a paired comparison denoting the dominance of element i relative to element j. A comparison is also being made of the *j th* element with the *i th* element. This results in the comparison matrix being a reciprocal matrix satisfying $a_{ji} = 1/a_{ij}$. The matrix diagonal represents the self-comparisons on the matrix elements.

$$\begin{pmatrix} \frac{w_1}{w_1} & \frac{w_1}{w_2} & \frac{w_1}{w_3} & \cdots & \frac{w_1}{w_q} \\ \frac{w_2}{w_1} & \frac{w_2}{w_2} & \frac{w_2}{w_3} & \cdots & \frac{w_2}{w_q} \\ \cdots & & & & \\ \frac{w_q}{w_1} & \frac{w_q}{w_2} & \frac{w_q}{w_3} & \cdots & \frac{w_q}{w_q} \end{pmatrix}$$

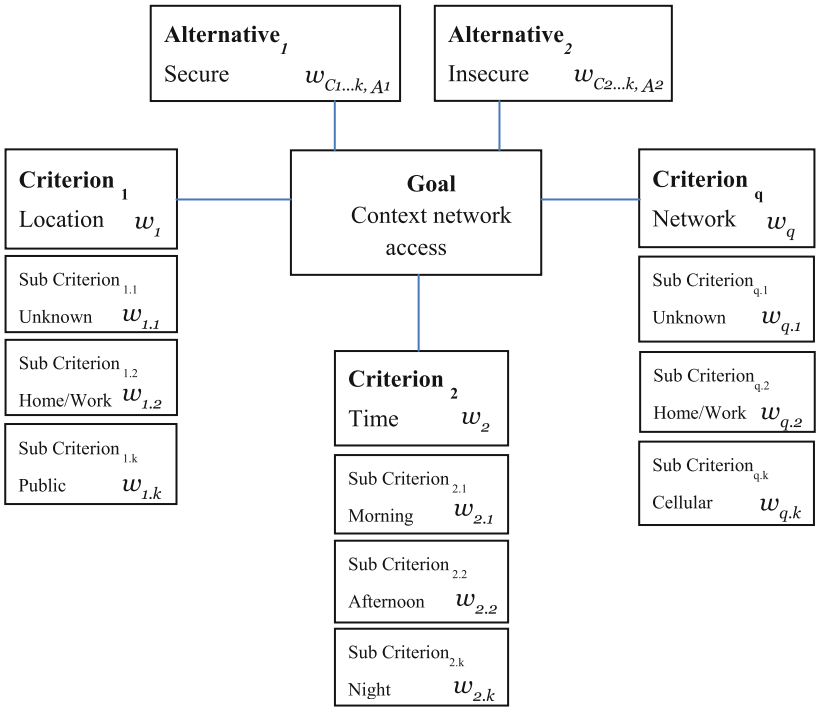


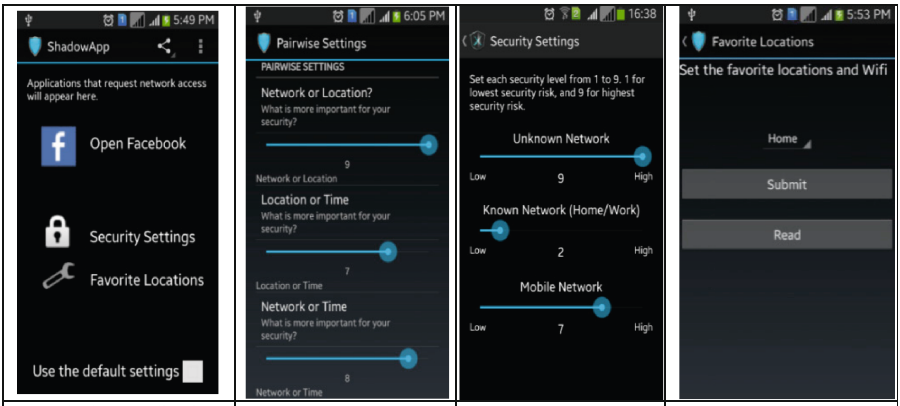
Fig. 1. The AHP structure

The association of the overall weighting for each element relative to its immediate above level is attained via priority vector (PV), which represents the eigenvector of the paired comparison matrices' components. The priorities assigned to the matrix elements reflect the order of their importance with respect to each alternative.

4 Implementation and Evaluation

We developed a prototype application of our proposed network access control mechanism in the Android OS on mobile devices. The application features prompt the execution of the mobile device applications inside a shadow application that controls the network access of these applications. The shadow application utilizes the AHP algorithm to determine the network access decision alternatives, namely secure or insecure. The calculated the AHP network access decision tallies the contexts' relative weights (location, network type, and time) with respect to the relative weights of their corresponding current states.

The application offers a network access setting interface for the users to prioritize the contexts towards the network access control of the running mobile application, such as Facebook that is used here for illustration (Fig. 2A). This is performed through a series of pair-wise comparisons among the contexts, as conferred in Sect. 2. The lowest



(A) Shadow application | (B) Context ranking setting | (C) Context states ranking setting | (D) Contexts definition setting

Fig. 2. Screenshot of the shadow application settings

network access control alternative is given a weight of 1, while the highest access control alternative is given a weight of 9 (Fig. 2B). These values will be used by the AHP analysis to provide eigenvector for the contexts. In addition, the application allows the users to prioritize the contexts' states with respect to the level of their network access control. The lowest alternative in terms of network access control is given a weight of 1, while the highest alternative is given a weight of 9 (Fig. 2C). The application settings allow users to add and/or to edit the definition of the contexts' states of their set locations and Wi-Fi networks (Fig. 2D).

Table 1. The pair-wise comparison matrix of the contexts criteria prioritization

Context	Location	Network	Time
Location	1	1/3	5
Network	3	1	7
Time	1/5	1/7	1

Table 1 illustrates the pair-wise comparison matrix of constructed contexts' security prioritization towards network access. These relative weights are then normalized and aggregated in order to calculate the priority weights defined from the AHP method (Table 2). Similar analysis is performed for the rest of the context sub-criteria states. For example, Table 3 presents the AHP matrix and the priorities for each alternative with respect to the different states of the Network criterion. Similar analysis is performed for the rest of the contexts' sub-criteria states.

The application uses the relative weights of the contexts along with the current user's context states to calculate the decision values of the context network access at run time. The overall weight of the decision values of the context network access is obtained from the sum-product of the normalized priority weights of each context criterion (Table 2) and the corresponding normalized priority weights of the assessed

Table 2. The normalized weight values for each context criterion

Context	Location	Network	Time	Priority
Location	0.238	0.385	0.226	**0.283**
Network	0.714	0.538	0.677	**0.643**
Time	0.048	0.077	0.097	**0.074**
Total	1	1	1	1

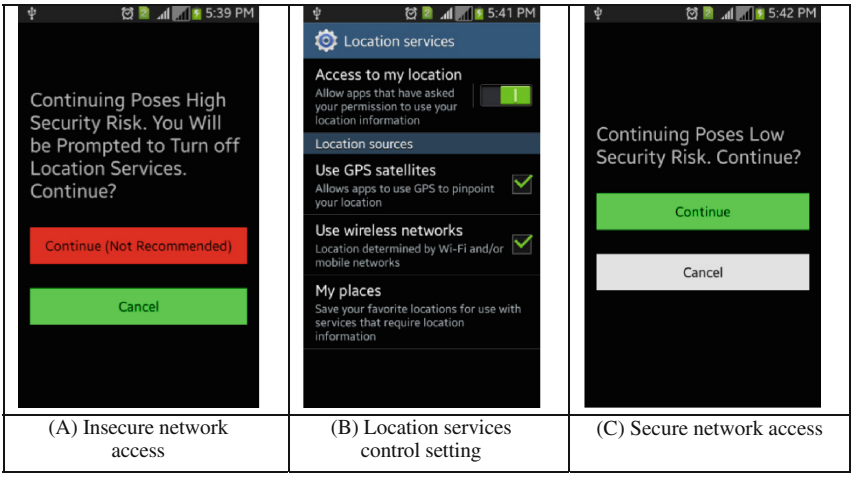
Table 3. The normalized weight values with respect to the network context states

Unknown	Priority	Home	Priority	Work	Priority	Cellular	Priority
Secure	**0.10**	Secure	**0.90**	Secure	**0.83**	Secure	**0.75**
Insecure	**0.90**	Insecure	**0.10**	Insecure	**0.17**	Insecure	**0.25**

context states (Table 3). Hence, the obtained higher priority value of each alternative of secure or insecure determines the recommended AHP network access level.

For example, Fig. 3A shows a scenario of a network access attempt of launching a mobile application, via the shadow application, at different context states. In this context, location is Public, Wi-Fi network type is Unknown, and time is Afternoon. The shadow application calculates the overall relative weight of the AHP context network access level. This yields a higher relative weight of an "insecure" network access that prompts the user, if decided to continue, to turn the mobile device location (geo-tracking) services off prior to launching the mobile application (Fig. 3B) — a feature that uses GPS along with crowd-sourced Wi-Fi hotspot and cell tower locations to determine user's approximate location.

Alternatively, Fig. 3C presents another scenario of network access attempt that is triggered with the launching a mobile application. The user's location is determined to be at Work, network type is Work, Wi-Fi, and time is Evening. The shadow application



(A) Insecure network access | (B) Location services control setting | (C) Secure network access

Fig. 3. Screenshots of the shadow application network access

recalculates the overall relative weight of the AHP context network access level. This yields a higher relative weight of "secure" network access in this case.

In order to examine our network access control framework performance, we used the general cross-validation evaluation technique to test the power of accuracy of the network access control mechanism alternatives and their associated contexts. The validation of our framework draws on a dataset of nine undergraduate university students affiliated participants (5 males and 4 females). Participants' age ranged from 19 to 22 years old with a mean age of 21. The participants have been considered as frequent mobile devices users who own the Android mobile devices for an average of more than two years, and considered themselves as frequent users of mobile applications. After installing the framework shadow application on their mobile devices, participants were informed about the shadow application functionality and the network access control mechanism setting. Participants were then instructed to run the logging application at various times and places over a week time period. The application logs this information, along with participants' feedback options of whether they think that the mobile application launching of network access is secure or not– relevant to the shadow application network access control mechanism recommendation.

The collected data resulted into 118 observations of network access of mobile applications launching attempts via the shadow application, with an average of eight different mobile application network access logged attempts per user per day. The collected data were divided into 80 % of training data, and the remaining 20 % for testing. Table 4 presents the cross validation confusion matrix of network access options accuracy, in pursuit of the context states. The rows present the generated case values and the columns present the predicted values. The results showed a classification accuracy of 91 % with an average Euclidian distance of 0.006. Euclidian distance ranges from 0 for the perfect classifier and square root of 2 for incorrect classification.

Table 4. Confusion matrix of network access alternatives (TP, TN, FP, and FN represent true positive rate, true negative rate, false positive rate, and false negative rate, respectively)

		Predicted	
		Secure Network Access	Insecure Network Access
Actual	Secure Network Access	TP= 45.7%	FN= 4.1%
	Insecure Network Access	FP= 4.8%	TN= 45.4%

Finally, in order to test the possibility and the hypothesis of whether the difference in network access decision values could be resulted from random variation rather than from significant differences between the AHP decision alternatives; we use Analysis of Variance (ANOVA) to assess the differences among the decision values across the observations. Test results (Table 5) indicate that there is a statistically significant difference in the decision values (P-value <0.001).

Table 5. ANOVA test results ANOVA Test

ANOVA Test

Source of Variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*
Between Groups	0.928026	1	0.438053	1123.14	3.6E-96	2.8248
Within Groups	0.060813	116	0.000614			
Total	0.996156	117				

5 Related Work

The wide spread use of mobile devices and their integration with personal computing in different domains have shifted the paradigm of how security needs to be handled. For example, [17] proposes TaintDroid to provide real-time analysis of more than 20 mobile applications access to users' private information. The authors found considerable instances of potential misuse of such applications towards users' private information. Similarly, [18] investigates how permissions and privacy could play a role in users application selection decisions. The study found that presenting privacy information in a clearer fashion could assist users in choosing applications that request less permission. In addition, [19] proposes a real-time taint aware analysis to detect mobile applications' vulnerabilities of exchanging data between a single application or among several applications. Earlier, [20] explores retrofitting the Android permissions model to determine third party application extra permissions network access beyond the applications needs.

Various research initiatives have explored the use of security relevant context with focus on delegation of context-based access control rights. For example, [21] proposes an ontology-based frame work that utilizes context information to derive access control measures of mobile devices' assets, such as messages, based on the confidentiality level of these assets. Others focus efforts on context-based authentication and authorization policies for augmenting network access control in mobile environments. For example, [22] explores context-aware scalable authentication (CASA) as a way of balancing security and usability for authentication by enabling easy access in commonplace everyday situations, such as home; while requiring more secure authentication in less common unidentified places. In addition, [23] proposes a context profiling framework using location Wi-Fi and Bluetooth to infer appropriate access and sharing policies for sensitive data on the mobile device. In our proposed framework, the network type is included along with other contexts to continuously perform network access control measures. In addition, our framework provides a generalized infrastructure that can be configured for different applications.

Finally, [24] proposes a context-aware usage control that takes into account context information, such as the spatial and time data to enforce ongoing policy defined by users during runtime to data access (i.e., data and files) and resource usage (i.e., CPU utilization and battery power). Similarly, [25] explores an access control mechanism that allows users to set configuration policies over applications' usage of mobile device

resources and services when using the device at public places, and re-gain their original privileges when the device is used at private place. In addition, [26] proposes location-based access control mechanism among specified sub-areas via modifying the Android operating system to enforce access control restrictions within the specified locations.

6 Conclusions

In this paper, we proposed a context-based framework that incorporates users' context, collected from mobile device sensors, with network access control decisions. The framework applies the analytic hierarchy process (AHP) method to dynamically evaluate users' context, and to provide the appropriate network access control decision in run-time. We validate our proposed framework in the Android OS running on mobile devices. Evaluation results have illustrated the capability of our framework in providing network access control features based on real-time assessment of users' context.

References

1. 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: AVI 2012, Capri Island, Italy (2012)
2. Almuhimed, H., et al.: Your location has been shared 5,398 times! A field study on mobile app privacy nudging. In: Proceeding CHI 2015 Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems. ACM, New York (2015)
3. Tu, G.-H., et al.: Accounting for roaming users on mobile data access issues and root causes. In: Proceeding of the 11th Annual International Conference on Mobile Systems, Applications and Services. ACM (2013)
4. Fu, H., et al.: A field study of run-time location access disclosures on android smartphones. In: USEC 2014. Internet Society (2014)
5. Ferreira, D., et al.: Securacy: an empirical investigation of android applications' network usage, privacy and security. In: WiSec 2015, New York (2015)
6. Distefano, A., et al.: Securemydroid: enforcing security in the mobile devices lifecycle. In: Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research, ser. CSIIRW 2010. ACM, New York (2010)
7. Hornyack, P., et al.: These aren't the droids you're looking for: retrofitting android to protect data from imperious applications. In: Proceedings of the 18th ACM Conference on Computer and Communications Security, ser. CCS 2011. ACM, New York (2011)
8. Balebako, R., et al.: Little brothers watching you: raising awareness of data leaks on smartphones. In: Proceedings of the Ninth Symposium on Usable Privacy and Security, ser. SOUPS 2013. ACM – Association for Computing Machinery (2013)
9. Rastogi, V., Chen, Y., Enck, W.: Appsplayground: automatic security analysis of smartphone applications. In: Proceedings of the Third ACM Conference on Data and Application Security and Privacy. ACM (2013)
10. Mowafi, Y., et al.: A context-aware adaptive security framework for mobile computing applications. In: the 4th International Workshop on Context Aware Middleware for Ubiquitous Environments (PerCAM 2014), UAE, Dubai (2014)

11. Dyer, J.S., et al.: Multiple criteria decision making, multiattribute utility theory: the next ten years. Manag. Sci. **38**(5), 645–654 (1992)
12. Rosenbloom, E.S.: A probabilistic interpretation of the final rankings in AHP. Eur. J. Oper. Res. **96**(2), 371–378 (1997)
13. Koumoto, Y., Nonaka, H., Yanagida, T.: A proposal of context-aware service composition method based on analytic hierarchy process. In: Nakamatsu, K., Phillips-Wren, G., Jain, L. C., Howlett, R.J. (eds.) New Advances in Intelligent Decision Technologies. SCI, vol. 199, pp. 65–71. Springer, Heidelberg (2009)
14. Cocea, M., Magoulas, G.: Context-dependent personalised feedback prioritisation in exploratory learning for mathematical generalisation. In: Houben, G.-J., McCalla, G., Pianesi, F., Zancanaro, M. (eds.) UMAP 2009. LNCS, vol. 5535, pp. 271–282. Springer, Heidelberg (2009)
15. Chen, D.-N., et al.: A Web-based personalized recommendation system for mobile phone selection: design, implementation, and evaluation. Expert Syst. Appl. **37**(12), 8201–8210 (2010)
16. Saaty, T.L.: Decision Making for Leaders: The Analytic Hierarchy Process for Decisions in a Complex World. RWS Publications, Pittsburgh (1999)
17. Enck, W., et al.: Taintdroid: an information-flow tracking system for realtime privacy monitoring on smartphones. In: Proceedings of the 9th USENIX Conference on Operating Systems Design and Implementation, ser. OSDI 2010. USENIX Association, Berkeley (2010)
18. Kelley, P.G., Cranor, L.F., Sadeh, N.: Privacy as part of the app decision-making process. In: CHI 2013 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM, New York (2013)
19. Arzt, S., et al.: Flowdroid: precise context, flow, field, object-sensitive and lifecycle-aware taint analysis for android apps. In: Proceedings of the 35th Annual ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI 2014) (2014)
20. Felt, A., et al.: Android permissions: user attention, comprehension, and behavior. In: SOUPS 2012 Proceedings of the Eighth Symposium on Usable Privacy and Security. ACM, New York (2012)
21. Fischer, K., Karsch, S.: Modelling security relevant context an approach towards adaptive security in volatile mobile web environments. In: International Conference on Web Science, Germany, Koblenz (2011)
22. Hayashi, E., et al.: CASA: context-aware scalable authentication. In: Proceedings of the Ninth Symposium on Usable Privacy and Security, ser. SOUPS 2013. ACM, New York (2013)
23. Gupta, A., et al.: Intuitive security policy configuration in mobile devices using context profiling. In: Proceedings of the 2012 ASE/IEEE International Conference on Social Computing and 2012 ASE/IEEE International Conference on Privacy, Security, Risk and Trust, ser. SOCIALCOM-PASSAT 2012. IEEE Computer Society, Washington (2012)
24. Bai, G., Gu, L., Feng, T., Guo, Y., Chen, X.: Context-aware usage control for android. In: Jajodia, S., Zhou, J. (eds.) SecureComm 2010. LNICST, vol. 50, pp. 326–343. Springer, Heidelberg (2010)
25. Prakash, S., et al.: A proposed approach for mobile devices with context based access control mechanism. Int. J. Adv. Res. Comput. Sci. Technol. (IJARCST) **3**(1–2), 149–150 (2015)
26. Shebaro, B., Oluwatimi, O., Bertino, E.: Context-based access control systems for mobile devices. IEEE Trans. Dependable Secure Comput. **12**(2), 150–163 (2015)