1-2015

Multidimensional Context Awareness in Mobile Devices

Zhuo WEI
Singapore Management University, zhuowei@smu.edu.sg

Robert H. DENG
Singapore Management University, robertdeng@smu.edu.sg

Jialie SHEN
Singapore Management University, jlshen@smu.edu.sg

Jixiang ZHU
Wuhan University

Kun OUYANG
Wuhan University

See next page for additional authors

DOI: https://doi.org/10.1007/978-3-319-14442-9_4

Citation

WEI, Zhuo; DENG, Robert H.; SHEN, Jialie; ZHU, Jixiang; OUYANG, Kun; and WU, Yongdong. Multidimensional Context Awareness in Mobile Devices. (2015). *MultiMedia Modeling: 21st International Conference, MMM 2015, Sydney, NSW, Australia, January 5-7, Proceedings*. 8936, 38-49. Research Collection School Of Information Systems.
Available at: https://ink.library.smu.edu.sg/sis_research/2600

Author
Zhuo WEI, Robert H. DENG, Jialie SHEN, Jixiang ZHU, Kun OUYANG, and Yongdong WU

Published in MultiMedia Modeling: 21st International Conference, MMM 2015,
Sydney, NSW, Australia, January 5-7, 2015: Proceedings, pp. 38-49.
http://doi.org/10.1007/978-3-319-14442-9_4

Multidimensional Context Awareness in Mobile Devices

Zhuo Wei[1], Robert H. Deng[1], Jialie Shen[1],
Jixiang Zhu[2], Kun Ouyang[2], and Yongdong Wu[3]

[1] Singapore Management University, Singapore
[2] Wuhan University, China
[3] Institute for Infocomm Research, Singapore
{zhuowei,robertdeng,jlshen}@smu.edu.sg
{jixiang.jason.zhu,oyk1115}@gmail.com
wydong@i2r.a-star.edu.sg

Abstract. With the increase of mobile computation ability and the development of wireless network transmission technology, mobile devices not only are the important tools of personal life (e.g., education and entertainment), but also emerge as indispensable ”secretary” of business activities (e.g., email and phone call). However, since mobile devices could work under complex and dynamic local and network conditions, they are vulnerable to local and remote security attacks. In real applications, different kinds of data protection are required by various local contexts. To provide appropriate protection, we propose a multidimensional context (***MContext***) scheme to comprehensively model and characterize the scene and activity of mobile users. Further, based on the scheme and RBAC, we also develop a novel access control system. Our experimental results indicate that it achieves promising performance comparing to traditional RBAC (Role-based Access Control).

Keywords: Mobile security, context awareness, access control.

1 Introduction

The growing pervasiveness of the mobile device has changed the way we go about our daily lives. With increasing computing and storage capabilities, mobile device emerges as dominant computing platform for end-users to access the Internet services and connect the people. Meanwhile, most mobile devices are equipped with a wide range of advanced sensors, such as cameras, speakers, microphone, and accelerometer. They can be used for various purposes and open up a wide range of opportunities to develop new applications for business. It comes as no surprise that more and more employees bring their own mobile devices to workplace and frequently access sensitive company information (named BYOD - Bring Your Own Device). While it has been proven that BYOD can improve productivity of employee and make the company look like a flexible and attractive

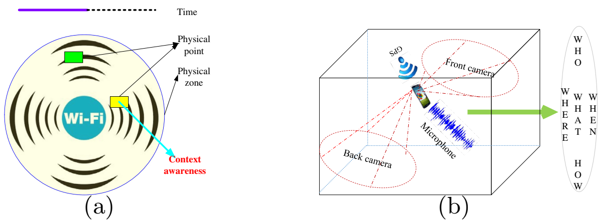


Fig. 1. (a) Existing access control model; (b) Multidimensional context aware model

employer, the practice could create various kinds of data security risks. For example, when users read confidential documents or have confidential discussion via phone lines, this can create high risk of information leak or loss.

To provide appropriate data security protection under different real scenarios, accurate context modelling and detection becomes more and more important. Motivated by the observation, this research aims to design, develop and evaluate an automatic multidimensional context aware security techniques tailor-made for mobile device users. To support an effective user context modeling, we propose a novel and efficient scheme called ***MContext*** to characterize contextual information based on mobile users' scene and behaviours. By using raw signal from various sensors in mobile device, ***MContext*** can effectively model and infer mobile users' context including: ***Who***, ***When*** , ***Where***, ***What*** and ***How***.

The contextual information can be further applied to design security strategy of mobile device users when they use different applications. In this paper, based on the scheme and RBAC, we have developed and fully implemented a novel access control system. To validate the proposed scheme, we carry out large scale experimental study and our results show that ***MContext*** model is highly effective and can dynamically detect current situation. Meanwhile, ***MContext*** aware RBAC system demonstrates high efficiency and effectiveness while deployed in ubiquitous devices.

The rest of this paper is organized as follows. We introduce the related works in Section 2. Section 3 and Section 4 describe the multidimensional context aware model and access control system, respectively. Finally, we give experimental results and performance analysis in Section 5. Section 6 concludes the paper.

2 Related Works

Recently mobile device security attracts a lot of research attentions and the core research challenge is closely associated with the end node problem, wherein a device is used to access both sensitive and risky networks/services. Because of Internet-based risks, the very risk-averse organizations provide devices specifically for Internet use. Thus, it is very important for company to understand the behaviour of its own employees while using mobile devices. Previous literatures proposed several access control techniques for mobile device users, which are classified into three major categories: temporal, physical zone and physical point domains as shown in Figure 1(a).

The first category is related to temporal domain. In many practical scenarios, users may be restricted to assume roles only at predefined time periods. Furthermore, the roles may only be invoked on pre-specified intervals of time depending upon when certain actions are permitted. For example, Bertino et al. presented TRBAC (Temporal Role Based Access Control)) [1] and GTRBAC (Generalized Temporal Role Based Access Control) models [2]. Both proposed models can be used for the access control for mobile device users inside time interval.

Secondly, the information about where mobile user presents can be applied to characterize objects, user positions, and geographically bounded roles. Roles are activated based on the position of the user. Besides a physical position, obtained from a given mobile terminal or a cellular phone, users are also assigned a logical and device independent position, representing the feature (e.g., room, floor, region) in which they are located. For example, with GPS (Global Positioning System) and GIS (Geographic Information System) information, Bertino et al. propose the geometric-based RBAC [3,4]. Similarly, by taking use of WIFI information. In [5], Ray et al. design a location-aware RBAC. All of information can be used for the access control for mobile device users inside physical zones.

The third access control management of mobile device users depends on extra devices and can be used inside physical places (points). A user provides a service provider with role and location tokens, e.g., Radio-frequency identification, along with a request. The service provider consults with a role authority and a location authority to verify the tokens and evaluate the policy. The typical example of system in this category is the smartphone-based system developed by Gey [6]. Using the system, user can exercise her authority to gain access to rooms inside university building, and by which she can delegate that authority to other users.

More recently, a few more comprehensive access control schemes have been developed for mobile device users by combining temporal, physical zone/point analysis techniques, e.g., STARBAC [7]. However, the existing techniques are not good enough for BYOD. On the one hand, they are unable to identify the higher level contexts (e.g., meeting, leisure, travelling), which a user involves. Mobile device access control requires high-level visual information to analyse scene of employee or environment context and then invoke the appropriate security policy and measure. On the other hand, mobile device application is getting ubiquitous now. It cannot depend on extra devices for its access control, e.g., you cannot setup radio frequency identification devices at public places.

3 Multidimensional Context Aware Model

It is not hard find that a conflict always exists between employee's flexibility and employer's management: employees can flexibly use mobile devices to access sensitive company data or important government documents at anytime and anywhere while employers need to protect data/documents in case of security risks. A possible way to help employers to perform the access control of mobile device users is to understand employees' context information (e.g., location and behaviours) and perform different access control policies.

Our proposed model is a systematic and comprehensive approach to achieve effective context awareness for mobile device users. It can effectively exploit both static and dynamic scene and event recognition to classify users' location and activity. The goal of proposed model is to tell a ***who*** (user identification), ***when*** (current time), ***where***, ***what*** and ***how*** story of mobile device users to employers. Figure 1(b) illustrates the multidimensional context awareness for mobile device users. ***Where*** and ***What*** are the location, scene and behaviours of mobile device users.

3.1 *Who*, *When* and *How* Verification

When a user wants to access a remote server database with his/her mobile device, it is necessary to supply user' profile (***When***, ***Who***, and ***How***) to the server in order to verify his/her validity. For example, when a businessman requires checking email outside company by own mobile, he must provide name and password, i.e., ***Who***, to the server. Meanwhile, his login/logout time log, i.e., ***When***, also are recorded by the server. In addition, user's network and device type, i.e., ***How***, can further be analysed by servers in order to verify the user authorities.

3.2 *Where*: Physical Location Recognition

Physical location are generally classified into two categories: indoor (e.g., bedroom or office) and outdoor (e.g., bus or square), which can be inferred from mobile devices sensors, e.g., GPS (out-door), 3G and WIFI (indoor). With present technology, we are able to recognize users location precisely and efficiently, thereby determining the IOR (Indoor or Outdoor) information of mobile users. In this paper, we exploit GPS signal information as well as hybrid location technology provided by third-party map API to determine IOR.

GPS: Nowadays, GPS (Global Positioning System) is widely applied for localization in smart device related application. Its signal differentiates obviously from indoor and outdoor, e.g., the acquisition speed of indoor is less than 10s with the accuracy of 10m to 20m; while the acquisition speed of outdoor is expected to be larger than 20s with the accuracy of more than 500m. Hence, by using the acquisition time T and the accuracy A, we can coarsely infer users' location. Assuming N_1 is the first impact factor for location decision, if $T < 10$ and $A < 50$, $N_1 = 1$, otherwise, $N_1 = 0$.

Hybrid Position: Most of the users are inside the architectural complexes in cities, where the GPS accuracy can not be guaranteed. It also takes a long time to locate the position, which can affect the accuracy as well. In this study, a third-party map SDK, the GOOGLEMAP SDK[1], is adopted for the hybrid

[1] `https://developers.google.com/maps/`

positioning solution which integrates WIFI, GPS, and base stations, in order to enhance the accuracy when users connect to WIFI or GPRS network. By using the relevant API, we can achieve more accurate locations and translate users coordinates into specific locations. We collect a set of building coordinates at advance, and set proximity alert based on the users current coordinates and the collected ones. When users are approaching the building, the proximity alert will be activated. The alert signal is recorded as the second impact factor N_2. When the proximity alert is activated, $N_2 = 1$, otherwise, $N_2 = 0$.

Algorithm: The algorithm to determine whether the user indoor or outdoor is as follows.

$$\mu = \begin{cases} (1-\alpha)N_1 + \alpha N_2, & if\ WIFI\ is\ accessable \\ N_1, & otherwise \end{cases} \tag{1}$$

Where μ is IOR decision. Under perfect circumstance, when $\mu = 1$, the user is in the indoor. However, in reality, since the accuracy of exiting positioning technology cannot reach 100, we can adjust the parameter α. By doing so, the accuracy is expected to exceed 80% when μ is larger than the threshold value, e.g., $\mu = 0.7$.

3.3 *What*

Although users' location (***Where***) is verified and recognized, it cannot decide if mobile users stay at a secure context. Hence, it is necessary to further know following context: **scene**, **situation** (e.g., are users' environment crowd, noise?), **behaviour** (e.g., are users static or moving?). By taking use of microphone, camera, accelerometer of mobile devices, robust temporal features (audio and accelerometer) and spatial features (images) are extracted and send to classifiers for sensing users' context.

What - Scene Recognition. In the scenario of scene recognition, mobile device is able to provide lots of information such as lighting, acceleration, temperature, audio and videos. The solution of context recognition based on those scenarios has been studied widely. Scene recognition based on audio has advantages like simplicity of data acquisition, abundant information amount and maturity of existing processing approaches. Considering the limitation of computing capability of mobile device and realizability of the model, our recognition scheme mainly takes use of audio as well as location information. The scheme consists of off-line training and real-time classifying. During the training process, classifiers are trained and built, which includes feature extraction, classifier construction, machine learning and model evaluation. In the real-time classifying process, the best performance classifier at last process is utilized and environment information such as audio and IOR from mobile device are extracted and sent as input to trained classifier to get predict values.

Recording Procedure: In order to reflect the characteristics of the scene, we have collected plenty of audio data[2]. Totally, there are 1350 audio records with no less than 10 seconds each in nine scenes: Indoor (Classroom, Quiet room and Market hall), Outdoor (Square, Park and Street), and Transportation (Bus, Metro, and Train). Audio are recorded in PCM standard with sampling rate of 41.1 KHz, 16 bit mono.

Feature Extraction: Currently, literatures proposed a variety of approaches for audio feature extraction, e.g., zero-crossing rate (ZRC), Mel Frequency Cepstral Coefficients (MFCC), spectral centroid and linear prediction coefficients (LPC), etc. Among these approaches, MFCC is often exploited in audio processing due to its accuracy and robustness properties, such as speech recognition, music genre and instrument categorization. In this paper, we also utilize MFCC as features for subsequent classification and prediction. Regardless of the accuracy of classification, the 13 dimensional MFCC vectors extracted from audio can be used as input data to train and build the classifier. To improve the performance, the IOR information obtained by location recognition scheme is added to feature vectors as the 14^{th} dimension of them.

Classification Method: Plenty of approaches designed for audio retrieval and classification have been proposed. Our main focus is on finding methods that are suitable for implementation on mobile devices. In this paper, we build and train our Bayesian network model as a classifier on PC, then download it to mobile devices for the inference procedure of Bayesian network which is much simpler than its building procedure.

Description of the Model: Let $U = \{x_1, x_2, ..., x_n\}$ be a set of variables. A Bayesian network consists of a network structure B_s, which is a directed acyclic graph over U, and a set of probability tables $B_p = p(u|pa(u)|u \varepsilon U)$, where $pa(u)$ is the set of parents of u in B_s. A Bayesian network represents a probability distributions:

$$P(U) = \prod_{u \varepsilon U} p(u|pa(u)) \tag{2}$$

The task of a Bayesian network classifier is to classify $y = \hat{y}$ called the class variable, given a $X = \{x_1, x_2, ..., x_n\}$ set of input variables called attribute variables. A classifier is actually a mapping function $h = X \rightarrow y$.

Learning Procedure: A classifier is built in this period given a training data set. The learning procedure consists of two stages: firstly learning a network structure B_s, then learning the probability tables B_p. There are various approaches to structure learning, such as *local score metrics*, *global score metrics*, *conditional independence tests*, and so on. Each kind of approach has corresponding search algorithms, e.g., hill climbing, simulated annealing, and tabu search. Considering the limitation of the calculating capacity of mobile devices, *local score*

[2] It is available at `http://1drv.ms/1sQ9Pxj`.

metrics and $K2$ algorithm [8] are exploited as the structure learning approach and search algorithm, respectively. For probability tables learning, we estimate the conditional probability tables by averaging all sub-structures of the network structures we have learned before. This is achieved by estimating the conditional probability table of a node x_i as a weighted average of all conditional probability tables of x_i given subsets of its parents $pa(x_i)$.

Inference: Assuming we have built a classifier through the learning procedure, $P(y|X)$ is calculated simply using the distribution $P(U)$ represented by the Bayesian network:

$$\begin{aligned} P(y|X) &= P(U)/P(X) \\ &\propto P(U) \\ &= \prod_{u \varepsilon U} p(u|pa(u)) \end{aligned} \tag{3}$$

Since all variables in X is known, no more extra complicated inference algorithms are needed. The output of the classifier is $\hat{y}$ where $P(\hat{y}|X) = argmax_y P(y|X)$.

What*: Environment Recognition.** When a user uses the phone with confidential operations, such as checking confidential document or talking on a confidential lines, there is information leak risk due to spy and eavesdropping. Therefore, estimating security level of surrounding environment becomes very important. In this paper, environment estimation refers to the number of people around and behind users. Generally, the more people around the user, the more congestion will be, the more insecure the environment will become, hence the risk of being watched is emerging. We exploits both front camera and microphone to analyze environments. Firstly, algorithm SC (Speaker Count) is used to determine number of people surrounding users, e.g., Crowd++ method [9]. SC algorithm splits audio file to equal length of speck slices, and extracts sound information and features in human voice frequency range. Eventually, SC algorithm will calculate the number people speaking based on unsupervised algorithm. Secondly, with the front camera, ***MContext model captures images as users access important/privacy data, and exploits face detection schemes (e.g., OpenCV[3]) to recognize human faces behind users.

What*: Activity Recognition.** As mobile users access important company or personal privacy data, above context awareness modules, e.g., ***Where, ***What (scene)***, will be activated once. However, context of users may be changed due to user activities (e.g., walking), hence the new location, scene or environment may require different security policies. In this paper, we use mobile sensors' signals, e.g., accelerometer and rotation sensors, to dynamically recognize users behaviours, such as walking speed and direction. Once those activities which

[3] `http://opencv.org/`

may hint that users' location, scene or environment are changed are recognized, ***MContext*** model will require processing static modules again, i.e., ***Where*** or ***What***, in order to apply the right security policies for new user context.

4 Context Aware Access Control

Most of the present access control models still resting on assigning permissions to users based on ***Who***, i.e., users identity, may cannot guarantee the security of sensitive data when it comes to mobile devices. The mobility of the device leads to the uncertainty of location, environment and other contexts. That is to say, even the same user should be assigned different permissions under difference circumstance. In this section, we propose a new access control model named ***MContext*** aware RBAC (MCARBAC), a modified model of RBAC[11]. An example of our model was implemented after that.

4.1 *MContext* Aware RBAC Model

The MCARBAC model consists of: a set of basic element sets; a set of RBAC relations involving those element sets (containing subsets of Cartesian products denoting valid assignments); and a set of mapping function that yield instances of members from one element set for a given instance from another element set.

Figure 2 shows basic architecture of ***MContext*** aware RBAC, which includes five basic data elements: MContexts (MCS), roles (ROLES), objects (OBS), operations (OPS) and permissions (PMS). The model is defined in terms of contexts assigned to roles and data access rights assigned to roles. Moreover, a set of sessions (SESSIONS) are also included in the model where each session is a mapping between a ***MContext*** and an activated subset of roles assigned to the ***MContext***. The most significant difference between RBAC and MCARBAC is that the element users (USERES) in the former is replaced by MContexts (MCS) in the latter.

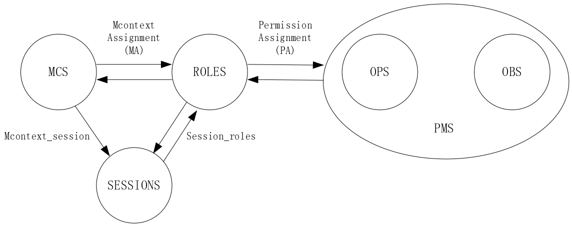


Fig. 2. ***MContext*** aware RBAC

4.2 Prototype Implementation of *MCRBAC*

A prototype of MCRBAC has been fully implemented using Android operating system. In our prototype, we define the element sets as ROLES $\{R1, R2, R3\}$ and PMS $\{P1, P2, P3\}$. We also assume that the elements in ROLES as well as PMS are hierarchical, which suggests all privileges of elements at low hierarchy are also privileges of elements at higher hierarchy. Here $R_1 < R_2 < R_3$ and $P_1 < P_2 < P_3$. Then we assign permissions to roles (PA) and ***MContext*** to ROLES (MA). The mapping function of PA is defined as $assigned\_permissions(R_i) = P_i$, where $R_i \in$ ROLES, $P_i \in$ PMS; and the mapping of MA is defined as Table 1. Less safe the ***MContext*** was, the lower its assigned role in the hierarchy would be.

Table 1. The mapping of MContext Assignment

Location		High crowd	Low crowd
Indoor	Classroom	R_2	R_3
	Quiet Room	R_3	R_3
	Market Hall	R_1	R_2
Outdoor	Square	R_2	R_3
	Park	R_2	R_3
	Street	R_1	R_2
Transpo-rtation	Bus	R_1	R_2
	Metro	R_1	R_2
	Train	R_1	R_3

Table 2. Categorization of OPS & OBS and the PMS each type requires

Source		Confid-ential	General
Files	Email	P_3	P_2
	Message	P_2	P_1
	Contact	P_2	P_1
Commu-nication	Phone Call	P_3	P_1
	Wechat	P_2	P_1
	Facetime	P_2	P_1
Money Apps	Bank account	P_3	\
	Amazon account	P_3	\
	Paypal account	P_3	\

”\”: resources are not considered as general.

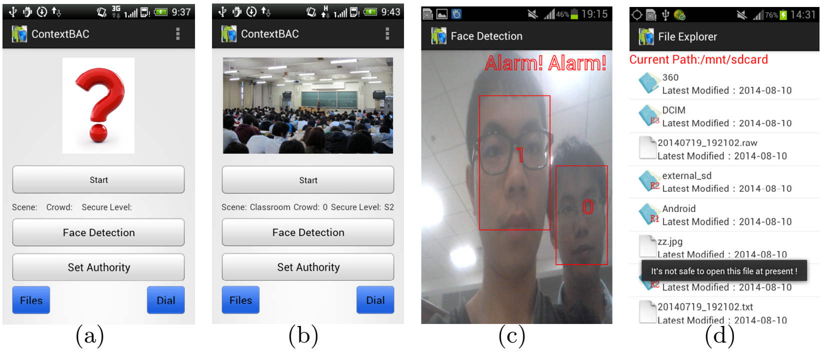
Since the accessible operations (OPS) and objects (OBS) on the mobile device are so complex and diverse, it is difficult to design an access control matrix (ACM) that contains all of them. Thus, for the sake of simplicity, OPS and OBS of mobile devices are categorized into three hierarchical types, and each type of OPS and OBS requires correspondent level of PMS, as shown in Table 2.

When the user attempts to execute some operations or access some objects of the mobile device, the ***MContext*** would be obtained through ***MContext*** model and a SESSION would be established during which a subset of activated roles will be assigned to the ***MContext***. If the roles possess required permissions assigned to them, then they can access correspondent operations and objects.Otherwise, access to those OPS and OBS are restricted as shown in Figure 3(d).

5 Experiments and Performance Analysis

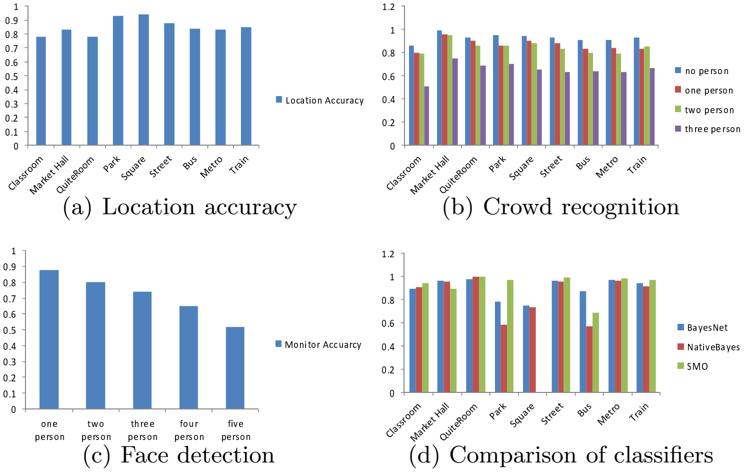
5.1 Experiments

Our system is developed on Android 4.0 platform and Figure 3 shows its main interface. To gain reliable test result, we run test 100 times in each of 9 scenes to


ContextBAC
Start
Scene: Crowd: Secure Level:
Face Detection
Set Authority
Files
Dial
(a)
ContextBAC
Start
Scene: Classroom Crowd: 0 Secure Level: S2
Face Detection
Set Authority
Files
Dial
(b)
Face Detection
Alarm! Alarm!
1
0
(c)
File Explorer
Current Path:/mnt/sdcard
360
Latest Modified : 2014-08-10
DCIM
Latest Modified : 2014-08-10
20140719_192102.raw
Latest Modified : 2014-08-10
external_sd
Latest Modified : 2014-08-10
Android
Latest Modified : 2014-08-10
zz.jpg
Latest Modified : 2014-08-10
Latest Modified : 2014-08-10
20140719_192102.txt
Latest Modified : 2014-08-10
(d)

It's not safe to open this file at present !

Fig. 3. The interface of ***MContext*** aware access control system. (a) Interface; (b) Classroom example; (c) Face detection; (d) File control.



(a) Location accuracy

(b) Crowd recognition

(c) Face detection

(d) Comparison of classifiers

Fig. 4. Experiments results

obtain the accuracy of location recognition scheme. 1350 recordings of 9 scenes are split into two data sets at the proportion of 66% to train and test the classifiers. Random division of recordings into the training and tests sets is done 100 times. As for comparison, two classification models SMO[12] and Naive Bayes[13] are implemented as the counterparts of our Bayes Net Model. Also, environment recognition scheme is also evaluated 100 times each scene on the condition that different number of persons (ranging from 0 to 3) speak respectively. Figure 4 illustrates experimental results and demonstrates a set of promising performance. Figure 4(a) shows that the recognition rate of location is about 85.1% for nine scenes; Figure 4(b) illustrates the recognition rates of crowd with SC methods; Figure 4(c) shows that accuracy rate of the faces detection is about

71.8%; Figure 4(d) illustrates the accuracy rate comparison among proposed scheme (90.2%), Native Bayesian (84.4%) and SMO (82.7%).

5.2 Performance Analysis

As mobile device users take their devices to access sensitive data, presented model can automatically and friendly perform context awareness. That is, all operations are transparent to mobile device users, e.g., image/audio capturing, features extraction. ***MContext*** aware model consists of static and dynamic context aware models. Static context aware model integrates scene and environment categorizations once; while dynamic context aware model takes use of temporal information (e.g., accelerometer) to percept users' context changing.

Good recognition that can be used for supporting real applications, largely depends on a major factors: 1) size of training dataset and 2) classification scheme. There is a trade-off between accuracy and efficiency. When more learning examples are consider, classifier can achieve better accuracy but needs more hours to complete training time. Since proposed model considers both spatial and temporal features, it guarantees nice accuracy rate. Experimental results show that the recognition the accuracy rate of Bayesian network is about 90.2%. It is better than Native Bayesian 84.4% and SMO 82.7%. The delay of ***MContext*** is about 2.358 second. In the future, we may try to leverage the computational and storage capability of cloud computing which improves the efficiency, i.e., performing light-weight feature extraction at mobile device while performing computational expensive classification in the cloud.

6 Conclusions

With increasing computing and storage capabilities, smart mobile devices are changing our lives and emerge as dominant computing platform for different kinds of end-users. BYOD users can access important company or government data at anytime and anywhere, however, they are vulnerable to local and remote attacks. In this paper, ***MContext*** aware access control system was proposed in order to protect local/remote data security. Experimental results indicate that ***MContext*** model enjoy high accuracy and good robustness. In addition, proposed access control system perfectly matches the requirement provided by various real applications (such as BYOD). In future, we plan to develop more advanced access control algorithm to improve effectiveness of data protection.

Acknowledgements. This work was partly supported by National Natural Science Funds of China (Grant No. 61402199). Jialie Shen was supported by Singapore Ministry of Education Academic Research Fund Tier 2 (MOE2013-T2-2-156), Singapore.

References

1. Bertino, E., Bonatti, P.A., Ferrari, E.: TRBAC: A Temporal Role-based Access Control Model. ACM Transactions on Information and System Security 4(3), 191–233 (2001)
2. Joshi, J.B.D., Bertino, E., Ghafoor, A.: Temporal Hierarchies and Inheritance Semantics for GTRBAC. In: Proceedings of the Seventh ACM Symposium on Access Control Models and Technologies, pp. 74–83 (2002)
3. Bertino, E., Catania, B., Damiani, M.L., Perlasca, P.: Geo-rbac: A spatially aware rbac. In: Proceedings of the Tenth ACM Symposium on Access Control Models and Technologies, pp. 29–37. ACM (2005)
4. Damiani, M.L., Bertino, E., Catania, B., Perlasca, P.: Geo-rbac: A Spatially Aware RBAC. ACM Transactions on Information and System Security 10(1) (2007)
5. Ray, I., Kumar, M., Yu, L.: LRBAC: A Location-aware Role-based Access Control Model. In: Bagchi, A., Atluri, V. (eds.) ICISS 2006. LNCS, vol. 4332, pp. 147–161. Springer, Heidelberg (2006)
6. Bauer, L., Cranor, L.F., Reiter, M.K., Vaniea, K.: Lessons Learned from the Deployment of a Smartphone-based Access-Control System. In: Proceedings of the 3rd Symposium on Usable Privacy and Security, pp. 64–75 (2007)
7. Aich, S., Sural, S., Majumdar, A.: STARBAC: Spatiotemporal Role Based Access Control. In: Meersman, R. (ed.) OTM 2007, Part II. LNCS, vol. 4804, pp. 1567–1582. Springer, Heidelberg (2007)
8. Cooper, G., Herskovits, E.: A Bayesian Method for the Induction of Proba-bilistic Networks from Data. Machine Learning 9, 309–347 (1992)
9. Xu, C., Li, S., Liu, G., Zhang, Y.: Crowd++: Unsupervised Speaker Count with Smartphones. In: Proceedings of the 2013 ACM International Joint Conference on Pervasive and Ubiquitous Computing, pp. 43–52 (2013)
10. Cheveigne, A.D., Kawahara, H.: YIN, a Fundamental Frequency Estimator for Speech and Music. The Journal of the Acoustical Society of America 111(4), 1917–1930 (2002)
11. Ferraiolo, D.F., Sandhu, R., Gavrila, S.: Proposed NIST Standard for Role-based Access Control. ACM Transactions on Information and System Security 4(3), 224–274 (2001)
12. Platt, J.: Sequetial minimal optimization: A Fast Algorithm for Training Support Vector Machines, Technical Report MST-TR-98-14, Microsoft Research (1998)
13. Langley, P., Iba, W., Thompson, K.: An Analysis of Bayesian Classifiers. In: The Tenth National Conference on Artificial Intelligence, pp. 223–228. AAAI Press and MIT Press (1992)