RESEARCH ARTICLE

SAware: Sensor-based Context Awareness for Smartphone Access Control

Minqiang Deng[1]
(Department of computer science , Jinan university,China)

---------------------------------------************************----------------------------------

Abstract:

In this paper, we proposed a sensor-based context aware-ness system for access control of smarphone, named SAware. With sensors analysis and inferring, such as Wi-Fi-based and GPS-based location,SAware system can locate the coarse locations of user holding the smartphone during identity verification or data/application access control.Based on predefined role-based access control policies, SAware grandsthe user with corresponding authorization, such as reading, writing orpriority. In order to evaluate proposed SAware system, we implementedour experiments on Android mobiles (i.e., Google Nexus 5X). Experimental results show that proposed SAware system is efficiency, security,and valuable for user access control.

Keywords **—Access Control, Context Aware, Smartphone, Cloud Computing.**

---------------------------------------************************----------------------------------

I. INTRODUCTION

As smartphones become more powerful in computing and communicationcapabilities, researchers are using these features to provide new or enhanced service applications. For example, in March 2013, Samsung introduced a GalaxyS4 device with eight CPU cores and nine sensors, which enriched the devicewith powerful resources[1]. As mobile devices continue to improve, mobile devices become the primary computing platform for end users to access Internet services.Not surprisingly, more and more employees bring their mobile devicesto the workplace and often access sensitive company information (named BYOD- Bring Your Own Device). However, it is insecure for employees to use mobiledevices at any time and anywhere to access the company's sensitive information.For example, the employee's mobile phone is lost and keeps the login information that can cause information to leak. More serious is the employee's login information is eavesdropped so the privacy information will be more serious threat.So only the account and password access control can not guarantee information security. Therefore, there is a need for a more flexible access control system, and now a powerful mobile device features for us to provide a possible.

In this paper, we proposed a sensor-based context awareness system for access control of smarphone, named SAware. In general, when making access control decisions, it is necessary to take into account the information about the changing environment, called context information [2]. In our SAware system, we use location context and time context for access control. The location scenario is divided into Wi-Fi and GPS scenarios according to indoor and outdoor. Wi-Fi-based scenario perception we use jaccard similarity coefficient. For GPS-based context awareness, we calculate the distance between two points. In order to reduce the burden on the resource server, we save the scenario information on the cloud server.

II. RELATEDWORKS

With the development of mobile devices, more and more people use mobiledevices to work. People can use their mobile gadgets to access private or confidential information.Theconvenience of mobile devices has also raised concernsabout privacy issues and information security. Several research work has adopted and extended role-based access control (RBAC) methods to access softwareservices [3],[4],[5]. Researchers have proposed several context-based access control methods to extend role-based access control(RBAC). For example, Bertinoet al. presented TRBAC (Temporal Role Based Access Control)) [6] and GTRBAC (Generalized Temporal Role Based Access Control) models [7]. GRBACand TRBAC are a way to incorporate the concept of environmental information (such as time) into access control. However, GRBAC may not be feasible in practice because a large number of environmental roles make the system very difficultto maintain. So the researchers proposed dynamic RBAC (DRBAC), accordingto the context of information to dynamically adjust the role and permissions[8].However, these models are conceptual and focus only on high-level abstractionsand do not specify how to deploy them in an actual implementation. In orderto apply these models to practical implementations, many researchers have proposed solutions that can be implemented, such as Sandhu et al.[9], Gupta etal.[10] and Zhuo Wei et al.[11].

III. SAWAREACCESS SYSTEM

The architecture of our proposed model consists of three sections (see Fig.1). For the first section, the scenario data is collected and preprocessed anduploaded to the cloud server. Second, the cloud server saves the scenario information of each user. When the user accesses the resource, the cloud servercalculates the current scenario of the user. The cloud server then configures theuser's access control policy through the current user context information. Forthe third section, the resource server receives the access control policy from thecloud server and then returns the resources that the user can access in the scenario based on the current access control policy. Our proposed model is a wayto separate scenarios and resource data to achieve effective context awarenessfor mobile device users. The storage and analysis of scenario information on thecloud server can greatly reduce the burden on the resource server to improvethe efficiency of the system. The goal of the proposed model is to tell who (useridentification), when (request time), where (where the request is made), andwhat the user uses to do with the mobile device.

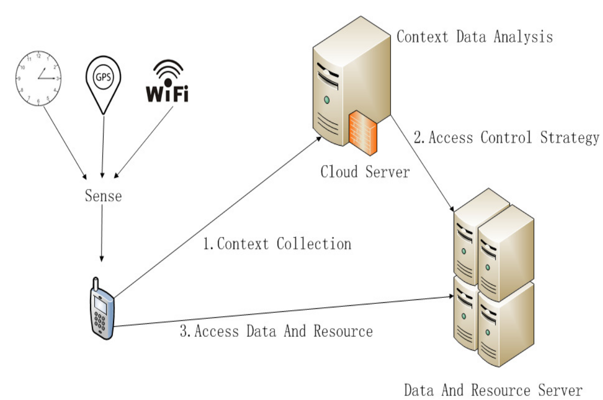


Fig. 1Architecture of the SAware access control model

IV. CONTEXT AWARENESS METHODS

In this paper, We divide the scenario into familiar Context and unfamiliarContext. With present technology, we can use the mobile device's sensors to infer the user's context. we rely on positioning techniques to identify devices thatare familiar with Context. In the outdoors, we collect location data from theGlobal Positioning System (GPS) to determine a familiar context. However, inthe interior, due to the complexity of the building structure, GPS-based positioning technology has low accuracy, we use Wi-Fi-based location technology forcontext-aware. Under normal circumstances, the receiver at least need to observefour GPS satellite signals to be able to carry out the normal three-dimensionalpositioning. Therefore, when we get more than four satellites, we use GPS toinfer the user's context. Assume that M1 is the first influencing factor in positioning decisions. if $num_{satellite}$>=4, M1= 1, otherwise, M1= 0. For Wi-Fi we can use the Wi-Fi access point signal strength to identify the indoor or outdoor. Wi-Fi APs signal strength greater than -50 is considered strong signal. If $num_{level>=-50}$>= 4, M2= 1, otherwise, M2= 0.Where λ is IOR decision.

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

$$\lambda = \begin{cases} \beta M1 + (1-\beta)M2, if \text{ Wi}Fi \text{ } and \text{ } GPS \text{ } is \text{ } accessable \\ 0, \qquad\qquad\qquad\qquad\qquad\qquad otherwise \end{cases}$$

When λ = (1- β) or 1, the user is in the indoor. When λ = β , the user is in the outdoor. However, when λ = 0, the location can not be configured for access control.

A. Wi-Fi-based Context Awareness

Many mobile devices now rely on Wi-Fi-based location technology becausethey effectively calculate the location of the device, especially where GPS andcellular signals are weak or unavailable[13]. These technologies are based on comparing the Wi-Fi access point received by the device with a database fingerprintthat contains a Wi-Fi access point with a known location [14]. Nowadays, WiFi-based positioning technology has been widely applied to a variety of scenarios such as intelligent space, location-based services, based on the positioning of access control[15],[16],[17].

In our work, mobile users will define their own Wi-Fi AP database, which contains only the familiar areas of the user. The resource data server also defineshis own Wi-Fi AP database, which applies to users with special access controlpermissions in the zone. For example, when a government employee accesses resources with mobile devices within a workplace, it is security in that context, sousers can access more resources. In order to identify the Wi-Fi-based context,each observation consists of the MAC address and signal strength of the detectedWi-Fi AP. Using the MAC address of the Wi-Fi AP to be able to identify a scene,but he can not handle the boundary problem, the recognition accuracy is low,in our case need to distinguish the higher precision sub-areas. Because differentsub-areas will have different access permissions. Whether the user-defined Wi-Fiaccess point database or the data server-defined Wi-Fi access point databaseneeds to be encrypted with the user's public key and then uploaded to the cloudserver.The user can capture several snapshots of location data in different areas, suchas at home and at work. Each snapshot captured by the user only saves the RSSI value for the top five Wi-Fi AP.When the WiFi APs fingerprint database is established, we use the machine learning similarity measure algorithm for context awareness.There are several similarity metrics, such as cosine,okapi [18], etc. Here we use the Jaccard similarity coefficient for similarity measure. The proportion of the intersection elements of the two sets A and B in the union of A and B is called the Jaccard similarity coefficient of the two sets, denoted by

$$JC(A,B)=\frac{|A\cap B|}{|A|+|B|-|A\cap B|}$$

B. GPS-based Context Awareness

GPS is the positioning tool in most mobile devices that uses data signalsfrom satellites to calculate the location of the device. The data received fromthe satellite contains the transmission timestamp, the orbital information andthe location of the satellite. Using at least three different satellite signals, theGPS uses a trilateral measurement method to calculate the position of the device by measuring the time difference of the satellite signal or the received signalstrength. Location information provided from GPS includes latitude, longitude,altitude, and time. The accuracy of the method is estimated to be in the rangeof 50 to 100 meters[19].

Contexts can be either user-defined or automatically added by mobile devices,which can improve the user experience. When the user comes to a new location,the user can define the location as a familiar context. The mobile device marksthe GPS information for the context including longitude and latitude and theGPS information is encrypted and uploaded to the cloud server. Another contextdefinition method uses an automated detection method to improve user experience and security. To identify GPS-based Context Awareness, we adopt thenotions of stay points and stay regions as introduced by Zheng et al. [20]and developed further by Montoliu et al. [10]. When the user opens the GPS function,the device can always sense the user's GPS information. The GPS observationsequence is divided into GPS stay points, which represent the user's access todifferent places. The GPS observation sequence within 30 minutes is classified asthe same stay point during which the user stays within a radius of r_{sp}= 100mfrom the first GPS observation. In order to improve the performance of the system, we set the observation interval for each stay point to 1 hour. We calculate the average position of each stay point as the latitude and longitude of the position, i.e.,$pos_{sp}=(lat_{sp},lon_{sp})$,s.t. $lat_{sp}=\frac{\sum_{i=1}^{N} lat_i}{N}$,and $lon_{sp}=\frac{\sum_{i=1}^{N} lon_i}{N}$.If the user in the same place is long enough there will be a lot of stay points. These stay points are the mark of this place. There is only one stay point to stay in one place per day. If the distance of these stay points is less than 100 meters,

calculate the average of these points. We specify that a stay point appears four times in a week as a familiar context. For A, B two points we use the following formula to calculate their distance:

$$C=\sin(LatA)*\sin(LatB)*\cos(LonA-LonB)+\cos(LatA)*\cos(LatB)$$
$$Dis\tan ce=R*Arc\cos(C)*pi/180$$

V. ACCESS CONTROL POLICY

Most of the current access control models still rely on the allocation ofpermissions based on users, that is, user identities, and may not be able to guarantee that security-sensitive data relates to mobile devices. For example, whenthe user's device is lost and retains the login information will cause informationdisclosure. So only the role-based access control can not protect the information

disclosure. In other words, even in different cases, the same user should be assigned different permissions.

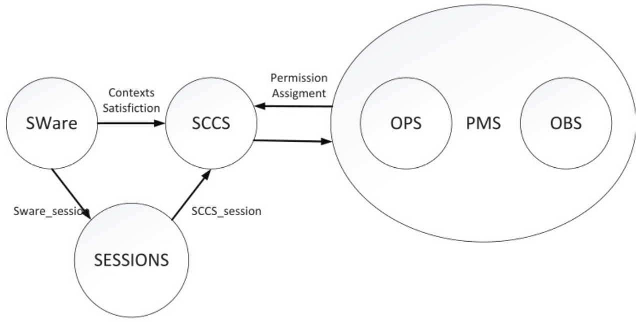


Fig. 2SAware access control model

Fig. 2 shows the basic architecture of our SAware. Our architecture consists offive basic elements: Sensors Aware(SAware), satisfied contextsconstraints(SCCS),objects(OBS), operations (OPS) and permissions (PMS). The model is definedbased on the context assigned to the roles and data access permissions assignedto the roles. In addition, the model also includes a set of sessions (SESSIONS),where each session is given a set of contexts to find the process to satisfy thecontext constraints. So the same user has different access rights in different contexts.

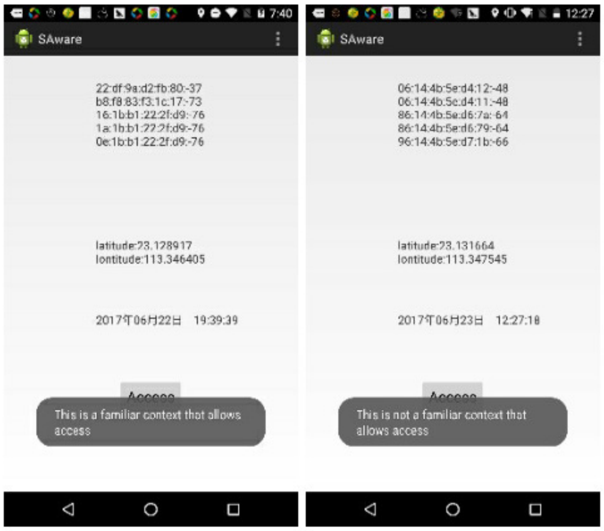
TABLE I
A SIMPLIFIED VERSION OF AN ACCESS POLICY

WHO	WHERE	WHEN	WHAT	READ	WRITE
R3	FC	WT	L2,L3	√	√
R3	FC	NT	L3	√	×
R3	UFC	NT	-	-	-
R2	FC	WT	L1,L2,L3	√	√
R2	FC	NT	L2,L3	√	√
R2	UFC	NT	L3	√	×
R1	FC	WT	L1,L2,L3	√	√
R1	FC	NT	L1,L2,L3	√	√
R1	UFC	NT	L2,L3	√	×

A SAware access control Policy captures the who/where/when/whatdimensions. The access decision is based on the following policy constraints:who the user is (subject.s role), The location where the user accesses theresources(location context), When users access resources(time context), whatresource being requested(object.s privacy level). We divide the user into threedifferent ROLES {R1,R2,R3} and resource.s privacy LEVELS {L1,L2,L3} .Here R1 >R2 >R3 and L1 >L2 >L3. We divide the access resource sites into familiar context(FC) and unfamiliar context(UFC). For the visit time we simplydivided into working time(WT) and non-working time(NT). Let ’ s consider theaccess control policy for several scenarios. Now imagine the following situation:

- an ordinary employee accesses resources at workplace,
- an ordinary employee accesses resources at home,
- an ordinary employee accesses resources in the subway,
- a manager accesses resources at work,
- a manager accesses resources at home,
- a manager accesses resources in the subway

Obviously, the user under six different situations described above owns differentcontexts. The access policy is defined as TABLE II.

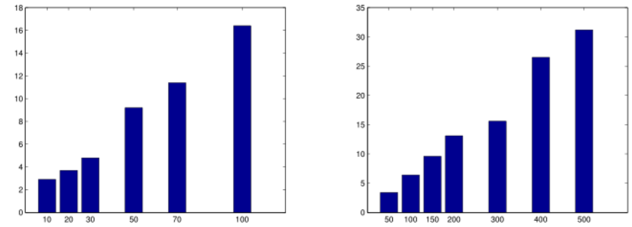


(a) (b)

Fig. 3Main interface

VI. EXPERIMENTAL

Our system is developed on Android 6.0.1 platform (Google Nexus 5X) andFigure 6 shows its main interface.Our system simulates the cloud environment onWindows7. All tests were performed on an Intel(R) Core(TM) i3-2330M runningat 2.20GHz with 4.00GB of RAM. We use the phone to collect Wi-Fi accesspoints and GPS information. In order to obtain reliable test results, we runthe test 10 times to get the accuracy of the time. Fig. 3(a) shows that the environment in which the phone is located meets the context constraints and can access the resources; Fig. 3(b) shows that the environment in which the phone is located does not satisfy the context constraints and can not access the resources. Fig. 4illustrates experimental results and demonstrates a set of promising performance. Fig. 4(a) shows the time required to calculate the Jaccard coefficients at different levels of the user's Wi-Fi fingerprint database;Fig. 4(b) shows the time required to calculate the distance at different orders of magnitude of the user's GPS fingerprint database.



(a) (b)

Fig. 4Experiments results

VII. PERFORMANCE ANALYSIS

Experimental results show that using Wi-Fi access points and GPS information to do context awareness has a very good performance. Fig. 4(a):Wi-Fi context detection. The purpose of this experiment is to evaluate the time-consuming use of the jaccard similarity coefficient algorithm in the SAwaremechanism. Experimental results show that time consumption is very small.When the user's Wi-Fi Fingerprint database contains 100 familiar context, ittakes about 17 milliseconds. Among them, each familiar context contains fiveWi-Fi access points. So the use of Wi-Fi to do context awareness is very efficient. Fig. 4(b):GPS context detection. The purpose of this experiment is toevaluate the time-consuming use of the GPS distance algorithm in the SAwaremechanism. The experimental results show that the time required to calculate500 GPS distances is no more than 33 milliseconds. Whether Wi-Fi-based context awareness or GPS-based context awareness is calculated on a cloud server, itdoes not affect the performance of the resource server, and the latency is almost.As the location information is important to the user's privacy information, inthe future we will use cryptography related technology to protect the privacy ofusers, in the encrypted conditions to do context awareness.

VIII. CONCLUSIONS

With the popularity of mobile devices, more and more users use mobiledevices to access sensitive resources. Users who use mobile devices to access corporate or government data at any time and anywhere can be vulnerable. In thispaper, we have proposed SAware access control system to protect data security. The experimental results show that SAware model has high efficiency and practicability. In addition, the proposed access control system is fully compliant with the requirements of various practical applications. In the future, we plan to develop more advanced access control systems to improve the effectiveness of data protection and protect the privacy of users.

REFERENCES

[1] Wikipedia, (May 2013). Samsung galaxy s4 specifications. [Online]. Available:http ://en.wikipedia.org/wiki/SamsungGalaxyS4.

[2] Kayes, A.S.M., Han, J., Colman, A.: ICAF: A context-aware framework for accesscontrol. In: Susilo, W., Mu, Y., Seberry, J. (eds.) ACISP 2012. LNCS, vol. 7372, pp.442-449. Springer, Heidelberg (2012).

[3] Chandran, S.M., Joshi, J.B.D.: loT-RBAC: A location and time-based RBAC model.In: Ngu, A.H.H., Kitsuregawa, M., Neuhold, E.J., Chung, J.-Y., Sheng, Q.Z. (eds.)WISE 2005. LNCS, vol. 3806, pp. 361-375. Springer, Heidelberg (2005).

[4] He, Z., Wu, L., Li, H., Lai, H., Hong, Z.: Semantics-based access control approachfor web service. JCP 6(6), 1152-1161 (2011).

[5] Kulkarni, D., Tripathi, A.: Context-aware role-based access control in pervasivecomputing systems. In: SACMAT, pp. 113-122 (2008).

[6] Bonatti, P.A., Ferrari, E.: TRBAC: A Temporal Role-based Access Con-trol Model. ACM Transactions on Information and System Security 4(3), 191-233(2001).

[7] Joshi, J.B.D., Bertino, E., Ghafoor, A.: Temporal Hierarchies and Inheritance Semantics for GTRBAC. In: Proceedings of the Seventh ACM Symposium on AccessControl Models and Technologies, pp. 74-83 (2002).

[8] G. Zhang and M. Parashar, /Dynamic context-aware access control for grid applications,0in Proc. 4th Int. Workshop Grid Comput.,2003, pp. 101-108..

[9] R. Sandhu, K. Ranganathan, and X. Zhang, /Secure information sharing enabledby trusted computing and PEI models,0in Proc. ACM Symp. Inform., Comput.Commun. Security, 2006,pp. 2-12.

[10] A. Gupta, M. Miettinen, N. Asokan, and M. Nagy, /Intuitive security policyconfiguration in mobile devices using context profiling,0in Proc. IEEE Int. Conf.Soc. Comput., 2012, pp. 471-480..

[11] JZhuo Wei, Robert H. Deng, Jialie Shen.: Multidimensional Context Awareness inMobile Devices. International Conference on Multimedia Modeling (2014).

[12] J. LaMance, J. DeSalas, and J. Jarvinen, AGPS: A low-infrastructure approach.(2002). [Online]. Available: http ://www.gpsworld.com/innovation – assisted – gps – a – low – infrastructure – approach/.

[13] Sky hook. (2003). [Online]. Available: http ://www.skyhookwireless.com/.

[14] CD Flora,M Hermersdorf,0A practical implementation of indoor location-basedservices using simple WiFi positioning,0Journal of Location Based Services, 2008,2(2):87-111.

[15] PG Sun,H Zhao,DD Luo § XD Zhang,ZY Yin,0Research on RSSI-based Locationin Smart Space,0Acta Electronica Sinica, 2007, 35(7):1240-1245.

[16] B Shebaro,O Oluwatimi,E Bertino,0Context-Based Access Control Systems forMobile Devices,0IEEE Transactions on Dependable & Secure Computing, 2015,12(2):150-163.

[17] R. Baeza-Yates and B. Ribeiro-Neto, Modern Information Retrieval. AddisonWesley, 1999.

[18] B. Shebaro, O. Oluwatimi, E. Bertino, Context-based access control systems formobile devices, IEEE Trans. Dependable Secure Comput. 12 (2) (2015) 150-163.

[19] V. W. Zheng, Y. Zheng, X. Xie, and Q. Yang.Collaborative location and activityrecommendations with GPS history data. In M. Rappa, P. Jones,J. Freire, and S.Chakrabarti, editors, 19th International Conference on World Wide Web, pages1029-1038, New York, NY, USA, 2010. ACM.

[20] R. Montoliu, J. Blom, and D. Gatica-Perez.Discovering places of interest in everyday life fromsmartphone data. Multimedia Tools Appl.,62(1):179-207, 2013.