International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 8 (2015) pp. 19967-19975

http://www.ripublication.com

Architectural Analysis for Improving Security using LBS with ATAM

Almas Begum[1] and V.Cyrilraj[2]

[1]*Research Scholar* [2]*Professor, Dept of CSE,*
Dr.MGR University, Maduravoyal, Chennai – 95, Tamil Nadu
almasbegum@drmgrdu.ac.in, cyrilraj@drmgrdu.ac.in

ABSTRACT:

An increasing number of smart phones and PDA's, allows people to use internet and often, store sensitive personal data, Mobile banking, Contact lists, information on Location (eg: GPS) and Sensor data. So smart phones need to protect data which is a challenging Security problem. Software architecture (evaluation) plays vital role in supporting the installation of multiple thirty party applications.

The objective of this paper is to propose an architecture for smart phones to provide security when using in LBS (Location Based Services) and analyzed above architecture with ATAM (Architectural Tradeoff Analysis Method).The main objective of ATAM is to make qualitative analysis on risks, sensitivity and trade-off points.

Keywords - Security, ATAM, LBS, Quality attributes, software architecture.

I. INTRODUCTION

In recent years, it is witnessed smart phones are universally used. These smart phones help the users to store personal data, do Mobile banking, access the Internet where ever they are and whenever they want and also to obtain information on social events as well as information on places, etc. Smart phones has the ability to do social communication with the help of internet service. Location Based Services (LBS) determines the location of a mobile device. Using LBS, every user can know who or what is near them, eg: nearest ATM, bank, etc,. With GPS, location of smart phones can be measured accurately. When user uses smart phones equipped with GPS and moves from place to place, location based transactions are possible[2].When user performs location based transactions, providing Security becomes challenging task. For all Mobile based transactions Security has to be provided to resist unauthorized usage.

"Software quality is the degree to which software possesses a desired combination of attributes"[IEEE 1061]. There are many scenario based software architectural evaluation methods, developed by SEI for risk identification of any software at the earliest along with quality attributes. They are SAAM (Software Architecture Analysis Method), ATAM (Architecture Trade-off Analysis Method), CBAM (Cost Benefit Architecture Method), ALMA (Architecture-Level Modifiability Analysis). In this paper, ATAM is the architectural analysis evaluation method used to evaluate our proposed architecture. ATAM is based on SAAM[5].

During every life cycle of software development process, identification of potential risks is the most important step. Using ATAM, architecture evaluation is performed to identify risks, trade-off points and sensitivity points. Risks are those substitutes that might generate issues for few quality attributes in future for an architecture. Sensitivity point is the criteria of an architecture to which a few of quality attributes are vastly relevant. Trade-off points are those whose criteria for an architecture affects numerous quality attributes in reverse order. ATAM is also designed to extract business goals and quality goals of any architecture. In this paper Security quality attribute is taken along with three main concerns and analyzed with ATAM. They are

(i) Integrity,
(ii) Confidentiality,
(iii) Availability.

II. ATAM (Architectural Tradeoff Analysis Method)

The ATAM is a scenario-based technique to do analysis of software architecture with respect to quality attributes. This method is used to identify possible risks in the architecture in the early software development life cycle. As ATAM is considered a mature approach, it has been validated in different domains. It has four phases and nine steps. Four phases are Presentation phase, Investigation and Analysis phase, Testing phase and Reporting phase[1]. The following are the steps used in evaluation of ATAM.

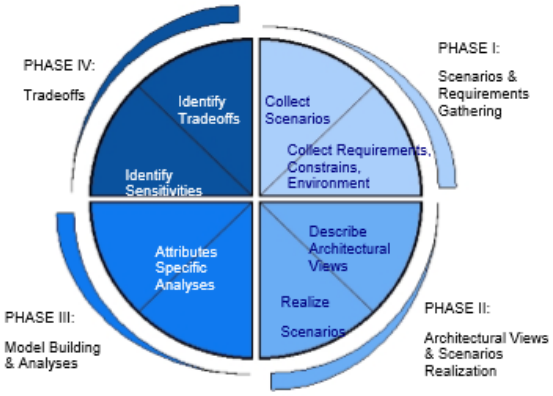

Figure 3. Architectural Tradeoff Analysis Method Steps & Phases[6]

Step 1: Present the ATAM:
The architecture team representatives are involved to describe the assessment method to the shareholders.

Step 2: Present Business Drivers:
The project manager describes what business goals are motivating the development effort and hence what will be the primary architectural drivers.

Step 3: Present Architecture:
The architect will describe the proposed architecture, focusing on how it addresses the business drivers.

Step 4: Identify architectural approaches:
Architectural approaches are identified by the architect, but are not analyzed.

Step 5: Generate quality attribute utility tree:
The quality factors that comprise system "utility" are extracted, specified down to the level of scenarios, annotated with stimuli and responses, and prioritized.

Step 6: Analyze architectural approaches:
Based upon the high-priority factors identified in Step 5, the architectural approaches that address those factors are elicited and analyzed. During this step architectural risks, sensitivity points, and tradeoff points are identified.

Step 7: Brainstorm and prioritize scenarios:
Based upon the scenarios generated in the utility tree (step 5), a larger set of scenarios is elicited and is prioritized via a voting process involving the entire shareholder group.

Step 8: Analyze architectural approaches:
This step reiterates step 6, and the highly ranked scenarios from Step 7 are considered to be test cases for the analysis of the architectural approaches. These test case scenarios may uncover additional architectural approaches, risks, sensitivity points, and tradeoff points which are then documented.

III. DESIGN &METHODOLOGY

The design and methodology for the proposed mobile architecture is shown in fig 1. All Smartphones are equipped with several applications by default. The frequent acceptance of using different applications in Smartphone, are always exposed to lack of security. When a user uses smartphone along with LBS application for any information retrieval, the information requested can be in disclosed in many ways. The information can be of geographic information, spatial information, temporal information or semantic information. When user tries to access sensitive information from a new location, the request is sent to location server, which in turn forwards the

request to the remote server. The sending of request and retrieval of reply through location server is done with “Push” and “Pull” service models of LBS application.

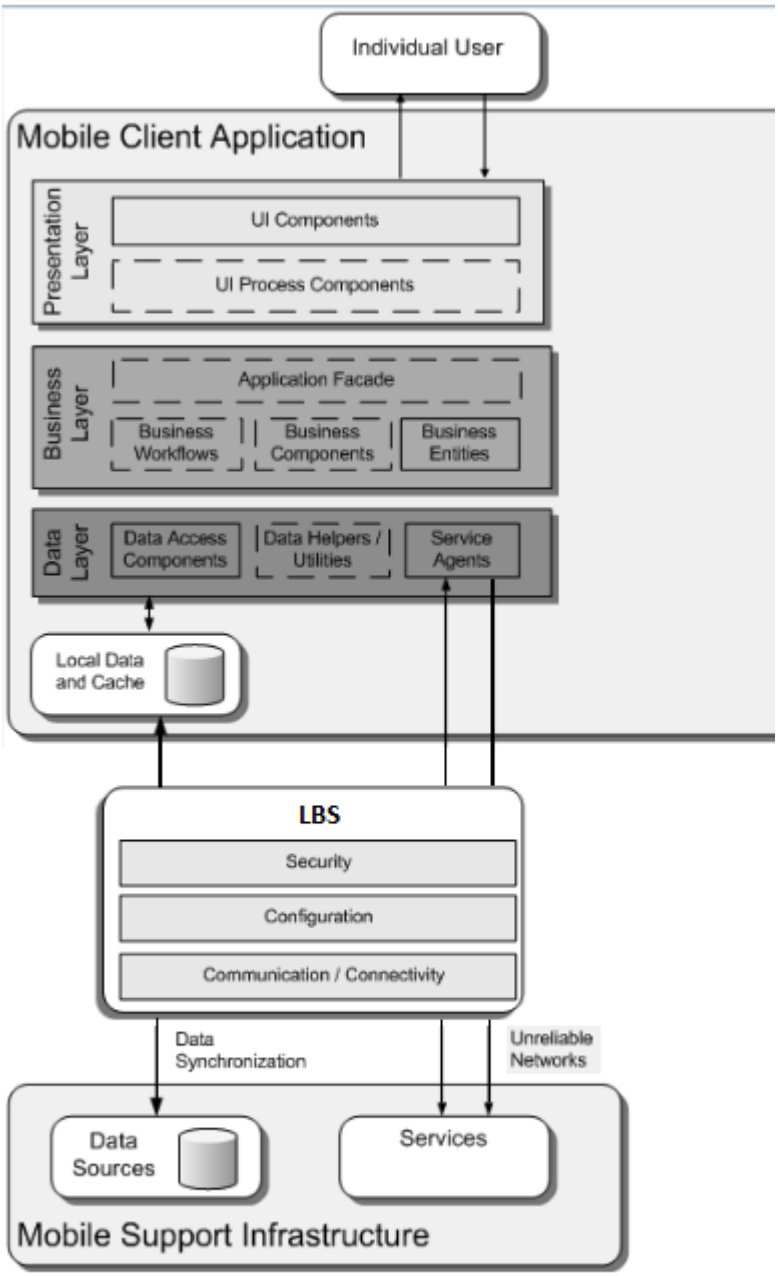

Fig 1. Proposed Architecture for Security with LBS Application

Fig 2 shows the architecture to strengthen the security of data when critical information is being accessed from unusual location

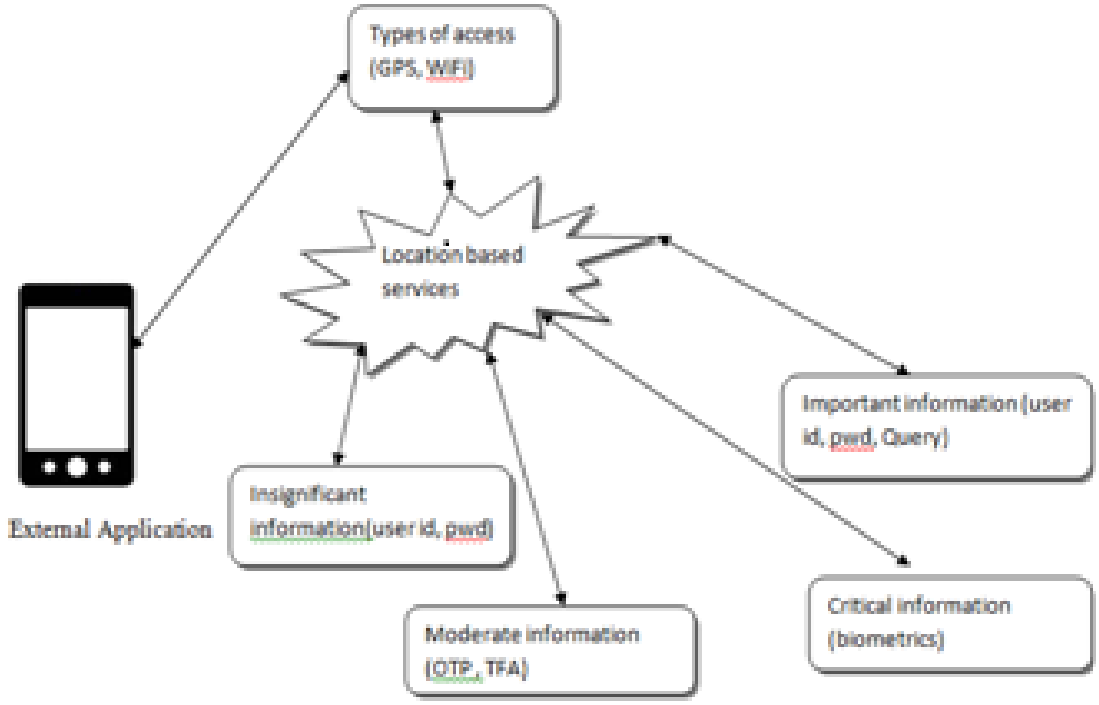

Fig 2.Architecture for mobile devices to access information from different locations[6]

When a user uses smartphone to access his/her personal data from an usual location, simple authentication is provided. When a user does the same from unusual location, authentication is provided based on the priority of information to be accessed from any of these securities stack levels. Once request is sent, Push service is enabled before the request is forwarded to the remote server. To provide security for the requested data, location estimation is made from where the user has pushed the request. [6]

IV. QUALITY ATTRIBUTES FOR SECURITY

Quality attributes are the cross-cutting concerns that affect run-time performance, system design, and user experience[7]. Quality attributes also serve as field of interest in identifying possible characteristics that are unique for an application. There are four individual areas where quality attributes are differentiated. They are Design, Run-time, System and User qualities. Every quality attribute is characterized in three categories[1]. They are

- *Stimuli* – an event that make architecture to respond or change.
- *Responses* – measurable answer for stimuli that is generated.
- *Architectural decisions* – are those conditions of an architecture that has an explicit impact on concluding attribute responses.

As above said, all Smartphones equipped with several third party applications, are always exposed to lack of security. So we propose an architecture that provide security for applications to prevent unauthorized access of personal information. The quality attribute Security, in our architecture is based on run-time quality. To provide security for Smartphone applications, three common aspects of security are considered for any situation. They are Confidentiality, Integrity, Availability [8].

- *Confidentiality:* It refers to the measure taken to prevent unauthorized access of sensitive information.
- *Integrity:* It refers to the measure taken to prevent unauthorized modification of sensitive information.
- *Availability:* It refers to the measure taken to provide sensitive information to authorized users when needed with out interruption of services.

Now in our architecture, we take these aspects of security and are analyzed with ATAM.

V. ARCHITECTURE EVALUATION

Presentation Phase

Step 1:

Users of smartphone are allowed to do different processes, without changing the context and usage of applications.

Step 2 ~ Step 3:

To understand the evaluation of business drivers and architecture, different objectives are stated.

- Description on diverse Locations is provided where users tend to use their Smartphones
- Providing different evaluation constraints when user tries to use sensitive information (eg.personal banking) from new locations.
- Providing security based questions to the users when they access sensitive information.

\Table 1: quality attribute Security – Scenarios

Quality Attribute	Attribute concern	Scenarios
Security	Confidentiality	When a user is accessing smart phone from an unusual location, unauthorized access is denied (H, L)
		When a user makes some transactions, they are verified based on authentication provided. (H, L)
	Integrity	When an unusual user is accessing smart phone either from an usual or from an unusual location, unauthorized modification of information is denied (H, L)
		when a user is trying to make payment through a gateway and has not logged out, automatic timer has to be set to relock the transaction information (H, M)
	Availability	When a user is accessing sensitive information from a remote location, services are to be provided without interruption (M, M)

Investigation & Analysis Phase

Step 4:

There are number of events derived and prioritized based on two proportions such as

(i) importance of event to the success of system and

(ii) degree of recognized risk posed by achievement of the event.

The table in next page shows aspects of security quality attribute along with the scenarios.

Step 5:

In this step, Security quality attribute utility tree is extracted. The prioritized measures for Security utility tree is shown in fig.3. This step is still used to elevate attribute goals a step forward.

Step 6:

In this step, prioritized measures identified from step 5are analyzed to identify risks, sensitivity points and trade-off points. The architectural quality – Security, is important for users to use smartphone with Location based services. Some of the priorities used in utility tree are (H, L), (H, M), (M, M)as shown in figure3

Testing Phase

Step 7 ~ Step 8:

Based on the events generated from utility tree, analysis is done to extract more events by users which follows bottom-up approach[9]. Architectural approaches are

analyzed based on the events extracted. These events are used to discover few more other events for architectural approaches. Table 2 shows sample analysis of identifying risks, trade-off and sensitivity points.

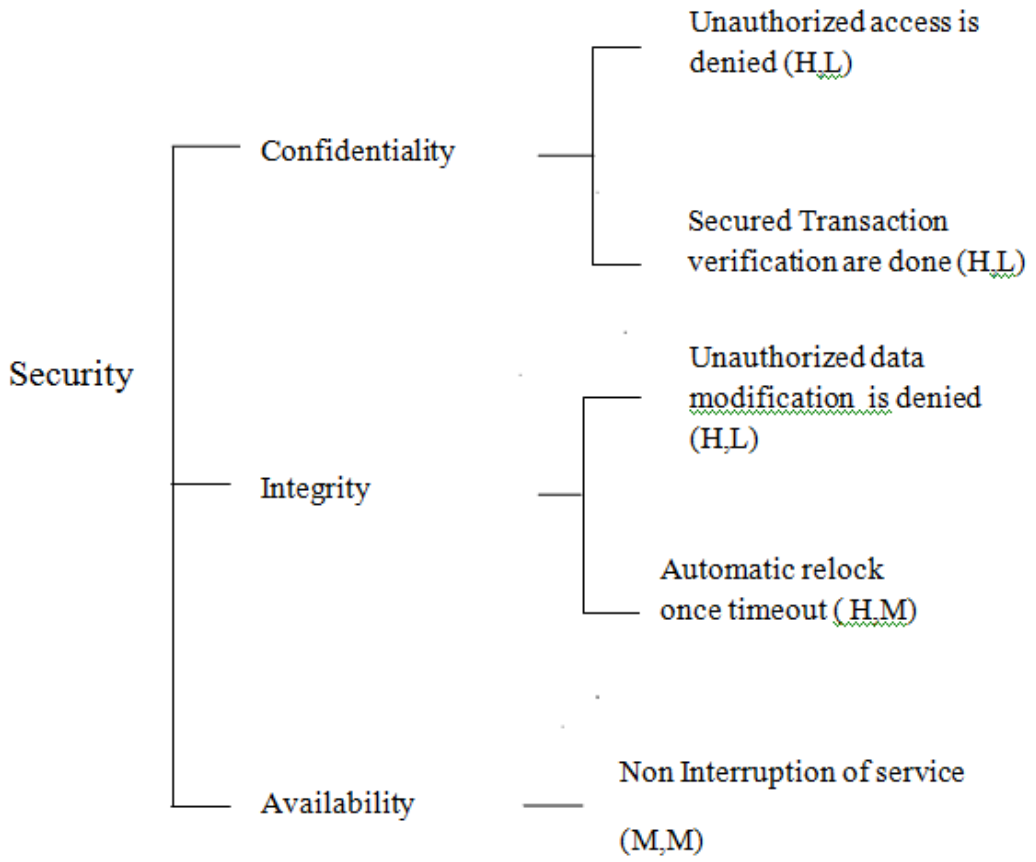

Fig 3.Security Utility tree

Table 2: sample analysis of Sensitivity, trade-off, risks points

Sensitivity points: • Sensitive data emission • Risky sensitive data storage • Risky sensitive data transmission **Trade-off points:** • While accessing sensitive information if location based service is not available **Risks:** • Risks is introduced if data integrity is lost • In case, confidentiality of passwords are lost risk is highly analyzed.

Reporting Phase

Step 9:

This is the last step used to create report based on the outcome of all information collected from all steps by applying ATAM. This step is also used to identify more strategies to reduce risks, trade-off and sensitivity points.

VI. CONCLUSION AND FUTURE WORK

In this paper, we have proposed an architecture for providing authentication and authorization to access sensitive information from usual or unusual location with LBS. To provide security, 4 different security stack levels are identified to access information. The proposed architecture is analyzed with ATAM and also used to identify sensitivity, risks, and trade-off points to determine more quality attribute requirements.

Future research will focus on further development of this architecture by identifying few more events for providing security and identify more risks, trade-off and sensitivity points.

REFERENCES:

[1] Rick Kazman, MarkKlein, Paul Clements, ATAM: Method for Architecture Evaluation, August 2000, Carnegie Mellon, SEI.

[2] Understanding Quality Attributes, Felix Bachmann, Mark Klein

[3] The essential components of software architecture design and analysisRickKazman, Len Bass, Mark Klein, 2006.

[4] Scenario based Software Architecture evaluation methods: An Overview, MugurelT.Ionita, Dieter K.Hammer, HenkObbink

[5] Architectural Quality in Development Processes: A Case Study, Anna Grimán and Maria Pérez, Journal Of Object Technology, Vol. 2, No. 2, March-April 2003.

[6] Novel Architecture For Improving Security Using LBS In Mobile Devices, Almas Begum, V.Cyrilraj, pp 602-606.

[7] https: //msdn.microsoft.com/en-in/library/ee658094.aspx

[8] "Quality Attributes – Technical report" Mario Barbacci Mark H. Klein Thomas A. Longstaff Charles B. Weinstock December 1995

[9] "Using ATAM to evaluate a game based Architecture", Ahmed BinSubaih, Steve Maddock.