Proposed Multilevel Architecture for Securing Context Aware Mobile Web Services

DR. P. Joseph Charles, Ph.D

Abstract:

In Context Aware Computing, the application adapts not only to changes in the availability of computing and communication resources but also to the presence of situational information such as user context, environment context and computing context. There has been in these days a notable increase in consumer use of Context Aware Mobile Applications (CAMA). The consumer centric Context Aware Mobile Applications are realized as the next evolution of personal Mobile Computing[1]. Context aware computing devices and applications respond to changes in the environment in an intelligent manner to enhance the computing environment for the user. Context aware applications should be pre-emptive in obtaining contextual information and provide their response based on the collected information. Henceforth, context aware applications tend to be mobile applications. Smart Mobile devices are well suited for these applications to reach the customers through services.

Keywords: Context Aware Computing, Service Oriented Computing, Role Based Access Control, PKI

1.INTRODUCTION

The Mobile Distributed Computing and Service Oriented Computing (SOC) could be served as a good platform for the growth of Context Aware Mobile applications with the multi-functionality smart mobile devices. The other key drivers for the evolution of these location aware systems are ease-of-use, convenience, social interactions and anytime-anywhere availability. Additionally, the Context Aware Mobile Applications facilitates day-to-day activities such as search services, business, entertainment, advertising, marketing, shopping, ticket purchasing, payment and mobile banking live and smarter.

1.1 Context Awareness

The context aware system must provide mechanisms and capabilities to enable discovering a new context information using different forms of querying and lookup mechanisms. Context-Aware systems must offer facilities for storing and maintenance of a context history and the facilities to query historical context data.

Context-aware computing offers services or information that are to specific task, they facilitate in making tasks more effective and improving decision making through context driven approvals. Applications should possess some of the following experiences in order to be characterized as context-aware.

1.2 Mobile Context Awareness

Mobile web services are the application of web services technology to the mobile environment. Mobile web services are defined as web services that are deployed on mobile devices and are published over the Internet, wireless network or within the operators' network. The goal of mobile web services is to offer new personalized services to consumers on their mobile devices such as telephones, wireless-LAN enabled PDAs and laptop computers.

In mobile web services environment, users are mobile and typically access resources using mobile devices. Context of the user (i.e. time, location, network state, system resources, user's activity, devices, etc.) is highly dynamic, and grants access without taking the user's current context into account can compromise security as the user's access privileges not only depend on "who the user is" but also on "where the user is" and "what is the user's state and the state of the user's.

1.3 Context Aware Web Services

Context aware web services refer to an adaptive process of delivering contextually matched web services to meet service requesters' needs at the moment. Context can be defined in two perspectives such as one from service requesters and the other from web services. From the former perspective, context is defined as the surrounding environment affecting requesters' service discovery access such as requesters' preference, location, activities and accessible network devices. Context aware systems have many components such as context sensor, context storage, context reasoner, context consumer[8].

1.4 Context Aware Mobile Web Services

Context-aware computing is a mobile computing paradigm in which applications can discover and take advantage of contextual information such as user location, time of day, nearby people and devices, and user activity[9]. In the recent years many researchers have studied and built several context-aware applications to demonstrate the usefulness of this new technology.

1.5Security Limitations in Context Aware Mobile Web Services

Security in Context Aware Mobile Web services is critical to their wide scale adoption and integration in Web-based enterprise systems and software. While shifting from the traditional client/server architecture to Web services technology is seen as an ratification of the Internet community's faith in the promise of the Web services paradigm. The goals of interoperability and ubiquity as envisioned by the Context Aware Web services technology can only reasonably be realized if the unique security challenges posed by this paradigm are appropriately addressed. [10]. The uniqueness comes from the fact that Web-based enterprise resources being exposed via

Context Aware Web Services are typically dynamic and distributed in nature. Also which requires some integrity among the data sharing between the client and server.

Nowadays, many systems use context aware mobile web services for health care industry. But, the security solutions adopted in each system does not consider all the above mentioned issues. Therefore, the development of secured framework for context aware mobile web services becomes a major research topic in the field of mobile computing and telecommunication industry.

2. REVIEW OF LITERATURE

Antorweep Chakravorty et al. [2] have proposed a framework for data security and privacy. The framework provides security and privacy through sensor data from smart homes, without compromising on data utility. However, the authors failed to include Role Based Access Control (RBAC) policies for authorization and the privacy levels are not be specified formally.

Theodore Patkos et al. [3] have proposed a Semantics-Based Framework for advanced location-based and context-aware services that integrates up-to-date technologies. It focused on modelling and representing context using Semantic Web technologies for efficient processing and dissemination of context-based knowledge in order to develop services for mobile users. Though, this framework has not handled continual, distributed planning.

Alexander Smirnov [4] have propounded a model of Context-Aware Access Control Model for Privacy in Mobile-Based Assisted Living.It supports virtualization mechanism which is a virtual private smart space, to authenticate the participants. After interaction of authenticated participants, the space is automatically destroyed. Information exchange in the smart space is implemented via HTTP using a uniform Resource identifier. The developed access control model is a combination of role based and Attribute Based Access Control (ABAC) mechanisms. The drawback of this model is, the connection information is transferred using single open key which leads to Man-In-The-Middle attack.

Hyun Jung La et al [5] have propounded framework for enabling context-aware mobile services. The framework enables tasks of capturing context, determining what context-specific adaptation is needed, tailoring candidate services for the context, and running the adapted service. Using the context information, Adapter Determiner is to analyze context information, look up candidate services, choose the most appropriate context-aware service adapter, and invoke an adapted service. Service Layer deploys multiple services such as CaaS and SaaS. A conceptual framework for enabling context-aware mobile services by dynamically adapting the service to the given contexts. However, the security mechanisms are missing in the proposed work that limits the scope of this architecture.

Having reviewed the literature, it is evident that several architectures, frameworks, models and security mechanisms exist. But each one has its own limitations. The literature review reveals

that the existing architectures, models and security mechanisms address only certain level of security issues and each one has its own limitations and security breaches. In addition, there is no end-to-end securing framework for context aware mobile web services adoptable by the health care industries to exchange their sensitive information.

Therefore, there is an urgent need to design a novel architecture for Context Aware Mobile Web Services related to Health-care Services[6][7].

3. Proposed Multilevel Architecture for Securing Context Aware Web Services

The proposed architecture for Context Aware Mobile Web Services (CAMWS) is envisaged to avail secure web services and applications anywhere, anytime through the mobile device with an end to end security[11]. The proposed architecture supports the necessary technical infrastructure such as acquiring user information, connectivity, authentication, and communication to facilitate the necessary health care services and mobile users.

The proposed architecture supports Confidentiality, authentication, integrity, non-repudiation and authorization. The proposed architecture offers various services in context aware web services and its functionalities, including PKI based security algorithms and the performance of the model is proposed.

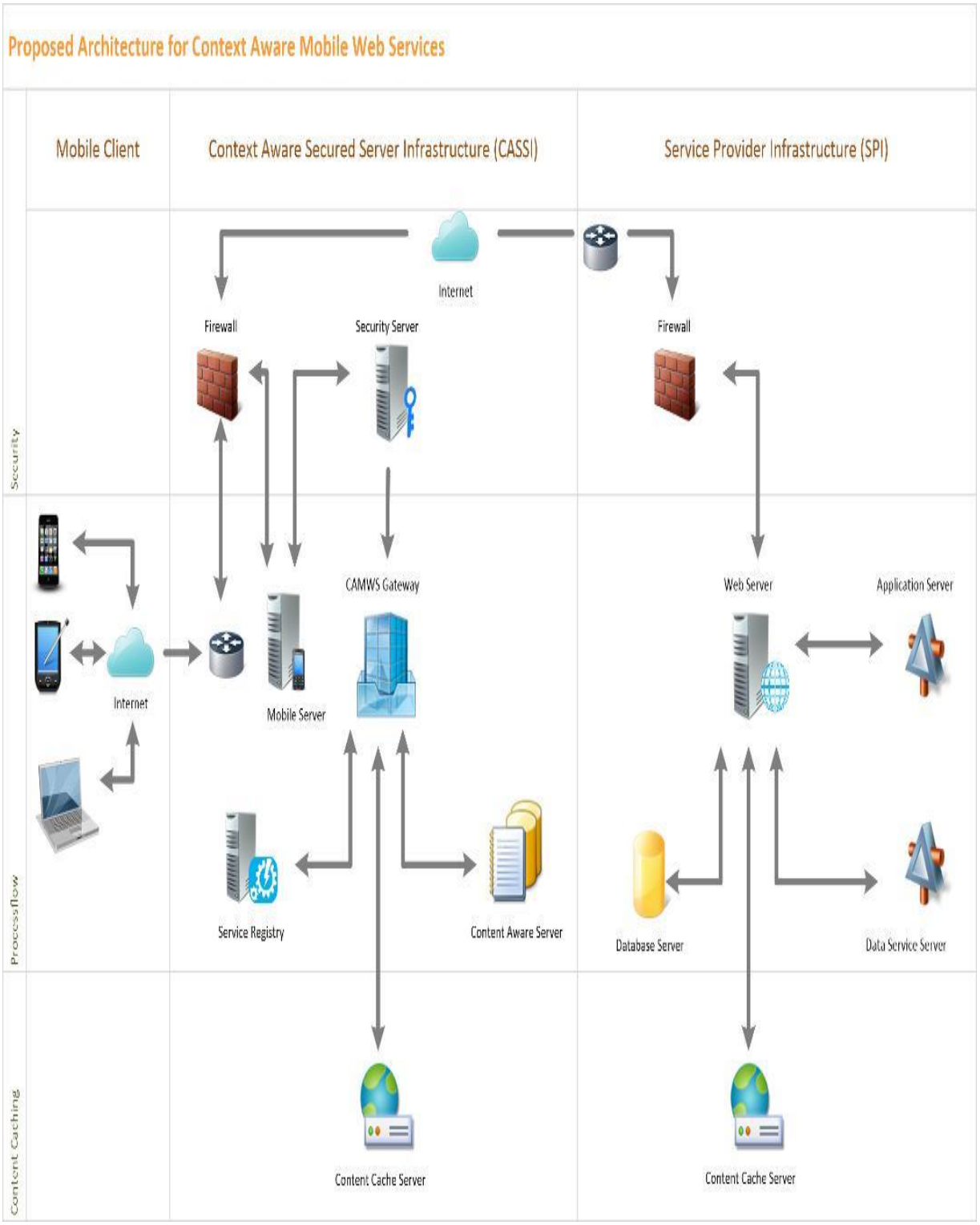

Figure 3.1: Proposed Architecture for Context Aware Mobile Web Services

The proposed architecture consists of five major components namely Mobile Server (MS), Security Server (SS), Service Registry (SD), Web Server (WS) and Context Aware Web Server (CAWS). These five components are interconnected and interdependent which make the proposed architecture more secure and unique.

3.1.1 Mobile Server (MS)
After the successful registration, the MS receives the service request from the mobile users and finds the user's context information such as, User's location, time of request received, etc. Then the MS decrypts the request and matches the service ID with the Service Registry (SD). The request is configured as service by Web Server. Once the service is configured, it is forwarded to the web server (WS) that match service ID with Service Registry.

3.1.2 Security Server (SS)
When IMU sends request to MS, the SS verifies the user credentials. After the authentication of IMU by the Security Server (SS) of CAMWS using their UId and PWd, the SS authorize the IMU's access privileges. Authorization of web services is accomplished by SS based on the Role-based Access Control (RBAC) technique using the Role (R) of the mobile user. Then suitable web services are provided to the mobile user through the Web Server.

3.1.3 Web Server (WS)
The Web Server (WS) of CAMWS is responsible for accepting the web service requests that arrive from the mobile users through Security Server (SS). It is also in turn responsible for providing the list of services which are registered with Service Registry.

3.1.4 Service Registry (SR)
The web service provider initially describes a web service and then publishes it to a service registry. When the mobile client requests a service, CAMWS Gateway finds the requested service from SR by matching the keywords.

3.1.5 Context Aware Server (CAS)
The CAS is responsible for identify and providing the context information such as user's location, time of request made, special services provided by the service providers and user preferences. These are the information is presented with the help of mobile user.

3.1.6 Content Cache Server (CCS)
The Content Cache Server is used to store the frequently accessed service requests for quick access that increases the performance of the system. Content Cache Server maintains the context for both the user-end and the service-end. On the client-end, it remembers the spatial and temporal context. On the service end it remembers the application and invocation context.

3.1.7 CAMWS Gateway
After mobile client and device authentication processes are completed, the service request is received by CAMWS gateway. This server acts as an intermediary between mobile client and SPI. Once the device request is received by CAMWS gateway, log is created and request is configured as services[12]. Then, the requested services are matched with Service Registry(SR).

Once the services are valid, the services are executed by service provider using service agent manager, where the services are implemented with service agents.

3.2 Significance of the Proposed Multilevel Architecture

The SFCAMWS security architecture addresses the security issues such as user authentication, authorization, data integrity and confidentiality, privacy and non-repudiation. Moreover, the prosed security architectureoffers complete security on both the ends from mobile client to SPI's web server and vice versa.

Authentication
Authentication is the process of verifying the identity and the relationship between the user and the system by validating user credentials. This security architectureverifies the identity of Internal Mobile User (IMU) and mobile server with each other, prior to information sharing. The mobile client authentication is established by verifying SS's public key using secret key which is created by using IMEI number. The entity authentication is completed using standard certificates based on X.509 between mobile client and SS of CASSI and between CAMWS gateway and SPI. Finally, the mobile client and CAMWS gateway is authenticated by verify UName and PWd using PKI.

Authorization
This security architecturerestricts unauthorized access to the services to the External Mobile user (EMU) and Internal Mobile user (IMU) as per the privileges. The design of SFCAMWS authorization implicates the Role Based Access Control (RBAC). Though, the IMU users get accesses to the system, the privileges of processing services are confined to the clients. The security architectureconfigures access policies to provide a controlled access according to the role of the client.

Confidentiality
The protection of IMU's request and response without disclosing them to others is called as Confidentiality. Confidentiality is obtained through PKI and standard cryptography algorithms.

Data Integrity
This security architecturehashes user message using SHA-1 message digest algorithm to ensure data integrity. This technique validates whether the data is interpreted, modified, injected or captured during the transmission. Hashing of decrypted data must match with received hash value for attaining data integrity. Change in the hash values implies that the message integrity has been comprised.

Non-Repudiation
In the proposed architecture, the mobile client, the CAMWS gateway and the Service Providers could not repudiate the service messages. The imperative security service of non-repudiation is achieved using digital signature. The digital signature only can generate by the private key of the communicating parties where the private key must be kept as secret. Authentication message, service request and service responses are sensitive information which are signed before

transmitting to the communicating party. Therefore, the mobile client, the CAMWS gateway and the Service Providers cannot deny the message sent by them.

Hence, the proposed security architecture for CAMWS is a novel one with end-to-end security using PKI to access the web services as well as data services. The experimental study has validated for the proposed security architecturein terms of Authentication, Latency, Throughput, Hit ratio and Response time.

4. CONCLUSION

Web services technology facilitates the building of more complex Web applications by composing elementary Web services. Since security plays a crucial role in the Context Aware Mobile Web services scenario, the design and development of security architecturefor complex web services, like health care services has become more promising research area. Furthermore, there has been considerable amount of research work carried out in the development and deployment of securing simple web services. Still there has been no concrete proposal offered so far to build a Context Aware Mobile Web Services.

In this paper, the author has put on efforts to propose a Security architecture for Context Aware Mobile Web Services using Public Key Infrastructure to perform health care web services through Web-enabled mobile devices. The proposed architecturesatisfies the key elements of confidentiality and message integrity are proved by using strong encryption and decryption algorithms. Client and Server Authentication is performed in this algorithm when the mobile gateway and the internal mobile user are communicating.

The end-to-end security is strongly addressed. The secret values of the client such as Username and Password is encrypted, then hashed and later signed by the involving entities which ensures the strong authentication, integrity, confidentiality and non-repudiation. Also the the innovation of the proposed security framework is based on the lies on the fortification of the target network from various malicious attacks such as eavesdropping, replay, flood, phishing and brute force

Presently, the digital world is rapidly developing the web applications using web services with the context information for easy and free access to information while the mobile clients are looking for service provider’s information and data services such as health care services.

REFERENCES

[1] Alvin T.S. Chan, Member, IEEE, and Siu-Nam Chuang, “MobiPADS:A Reflective Middleware for Context-Aware Mobile Computing”,IEEE TRANSACTIONS ON SOFTWARE ENGINEERING, VOL.29, NO. 12, 2003.

[2] Antorweep Chakravorty, Tomasz Wlodarczyk, Chunming Rong,"Privacy Preserving Data Analytics for Smart Homes", IEEESecurity and Privacy Workshops, 2013.

[3] Theodore Patkos, AntonisBikakis, Grigoris Antoniou, MariaPapadopouli and DimitrisPlexousakis, "A Semantics-BasedFramework for Context-Aware Services: Lessons Learned and
Challenges" pp. 839–848, Springer-Verlag Berlin Heidelberg, 2007.

[4] Alexander Smirnov,"Towards Context-Aware Mobile Web 2.0 ServiceArchitecture", International Conference on Mobile UbiquitousComputing, Systems, Services and Technologies, IEEE, 2007.

[5] Hyun Jung La and Soo Dong Kim, "A Conceptual Framework forProvisioning Context-aware Mobile Cloud Services", IEEE 3rdInternational Conference on Cloud Computing, 2010.

[6] P. Joseph Charles and S. Britto Ramesh Kumar, "A Multi-LayeredSecured Framework for Context-Aware Web Services in HealthCare Industries", International Journal of Applied EngineeringResearch, ISSN 0973-4562 Vol. 10 No.82 , pp.554-560, India,2015.

[7] P. Joseph Charles, and S. Britto Ramesh Kumar, "An EnhancedMulti-Layered Security Framework for Context-Aware Mobile WebServices", International Journal of Computer Applications (IJCA),Volume: 146- No.15, ISSN: 0975-8887, pp. 1-4, 2016. (IF:3.12)

[8] [COV, 2002] Covington Y, Michael J., PrahladFogla, Zhiyuan Zhan, MustaqueAhamad, "A Context-Aware Security Architecture for EmergingApplications", Proceedings of the 18th Annual Computer Security Applications Conference (ACSACí02), IEEE, 2002.

[9] [JAG, 2015] Jagadamba G, B SathishBabu, "Adaptive Context-Aware Access Control Model for Ubiquitous Learning Environment", BIJIT -BVICAM's International Journal of Information Technology, NewDelhi, 2015.

[10] [KAP, 2013] Kapitsaki M. Georgia "Reflecting user privacy preferences incontext-aware Web Services", 20th International Conference on WebServices, IEEE, 2013.

[11] [JOS,2014] P. Joseph Charles and S. Britto Ramesh Kumar, "Design of ASecure Architecture for Context-Aware Web Services Using AccessControl Mechanism", International Conference on ContemporaryComputing and Informatics (IC3I), IEEE Xplore, pp.780-784, 2014.

[12] [JIA, 2012] Jianxin Liao and Jingyu Wang, "Toward a Multiplane Framework ofNGSON: A Required Guideline to Achieve Pervasive Services andEfficient Resource Utilization", IEEE Communications Magazine,2012.

******