An Enhanced Multi-Layered Security Framework for Context-Aware Mobile Web Services

P. Joseph Charles
Research Scholar,
Department of Computer Science,
St.Joseph's college,Trichy.

S. Britto Ramesh Kumar, PhD
Assistant Professor,
Department of Computer Science,

ABSTRACT
People seeking medical attention go in search of medical centers and specialists. For them time is vital as they search for resources, the information should be available with minimum latency. With the advent of wearable computing and ubiquitous computing Context -Aware Web services can be available with much ease, it enables users to retrieve information with relation to their context. While providing several benefits, although web services technology has been facing serious threats like prefix hijacking and interception in the Internet due to a man in-the-middle attack which compromises privacy of the user. The objective of this research work is to provide a secure framework for Context aware web services using access control mechanisms. It was found web services are prone to data theft and malicious attacks, Access Control Mechanism is introduced in the framework to provide a secured architecture where the privacy of the person accessing the web service will be preserved. The proposed architecture provides an end-to-end security by accomplishing the security properties such as user authentication, authorization of web services, message confidentiality, data integrity and non repudiation. Hence, there is a need that arises to design a security system for context-aware web services with the support of end-to-end security in business services between the service providers and service requesters thus providing a secure user experience

Keywords
Web Services, Web engineering, Context-aware, access control, security, privacy.

1. INTRODUCTION
The main objective of Web engineering is to establish and to use disciplined and systematic approaches to successfully develop, deploy, and maintain high quality web applications. Another dimension of Web Engineering is the Web services technology that offers a number of enterprise applications like online banking, e-shopping, and web portals. These domains have a greater demand in the software industry to urge the web developers and the software vendors for the design, development and deployment of numerous web applications for the diverse organizations. Such a situation has motivated us greatly to develop a security framework for health care related context aware mobile web services. The applications using web services have made the software vendors and the web developers to design, develop and deploy the complex web applications for the diverse organizations. However, a variety of the web developers and the researchers felt the need of providing the secured web services for the clients. Currently, most of the business organizations have initiated the design of their own web sites with the development as well as the deployment of their web services over the Internet. Such enterprise web applications are subject to man-in-the middle attack by intruders or malicious users which may cause severe financial and legal implications to any commercial organization. Hence there is a growing need for the concept of design and development of multi-layered security framework [1-2]. Subsequently, there is a lot of research carried out so far in the field of Web Services Security. However, each model has been proposed with its own limitations.

2. RELATED WORKS
Shen et al [3], presented intended a context aware role-based access control model (CGRBAC).This research presents global roles which can be used to map the local roles of other service providers. The access control model must arrest the security relevant contextual information such as location, time, and environmental state available at the time the access requests are made and incorporate it in its access control decisions. It will use the term global service, to refer to the concept of composite service and use local service to replace by atom service. The proposed CGRBAC model simplifies the role assignment and management in different system.

Shang et al [4] proposed a context based dynamic access control model (CDACM) for web service. By means of context constraint, they enhance the adaptability of web service access control mechanism. By means of defining permission hierarchies, we improve the efficiency of security strategy implementation.

Kenya et al [5] describes the implementation of an authentication and access control framework for context aware services. The system administrator easily can set/change security policies according to the user's preferences and context. To generate and control secure user environments, it consider the following security policies. Authentication level assignment (ID & password, smart card/security token, biometrics, multimodal), Authorization and access control level assignment (location restriction, time limit, duration limit) and Confidentiality level assignment (data encryption, data signature, virtual private network).

Shade et al. [6] describes web service controls the ubiquity of the internet to link applications, systems and resources within and among enterprises to enable stimulating, new business processes and relationship with clients, partners and providers around the world. It allows access to data that has been prior to protect within corporate networks and accessible only via specialized software. It demonstrates the new and existing security mechanism for securing web services at different security tiers and it presents general security framework of web service such as Authentication, Access Control, Authorization and Confidentially, Availability, Integrity of data.

Somesh et al [7] developed formal verification techniques for access control policies and formalized classes of security analysis problems in the context of Role Based Access Control (RBAC). Subsequently the formal RBAC models were developed by Sandhu et al [8].The second level of security in the model is the authorization of users to the web services.

Hwang et al [9] proposed an operational model for securing the Web services by fulfilling the essential security requirements such as authentication, confidentiality, data integrity with non-repudiation and by providing support for security mechanisms like encryption and digital signatures. This model still has the limitation of being not able to provide support for access control.

Yanjiang et al. [10] proposed a password based user authentication and key exchange system by employing two-server architecture. This system is a password-only system and requires no public key cryptosystem aiming to secure against the offline dictionary attacks. Since the password-based user authentication systems are inexpensive and user-friendly, a password-based user authentication is incorporated as the first level of security in the proposed model.

Richard [11] presents a research-in-progress study that incorporates context, in terms of application events, into a specific security framework and maps authorized events to adaptable Web services. These events are incorporated as XML attributes within an encrypted security token which is passed to a Web service for a response. The specific response behavior of the service to the event is restricted by a fine-grained access model as per pre-defined security policy.

Charles et al [12] proposed on the security requirements in context-aware service on the web. In the proposed solution some access control policies are created on the basis of the services available and that policies are taken in account during the services requestor login. It validates the user preferences based on the user role and it's the part of key to the actual data. This work can be used to provide authorization and role-based access control policies to context-aware web services.

Liu Hong-yue et al [13] discusses the conventional role-based access control model, does not take into account context factors before making access control decisions. It may not be suitable for distributed computing applications. Researcher proposed a context aware fine-grained access control model.

Based on the survey, in the web services scenario, there exists quite a lot of research activities, out of which some are essentially being carried out for the design and development of architectural framework models. Such proposals have been mostly intended for the secure enterprise web services but with some significant limitations.

The paper is organized as follows: chapter 3 presents the enhanced multi-layered security architecture and framework for context-aware web services related to health care industries. Chapter 4, describes the methods that have been built upon the framework. Section 5 provides summary and conclusions of the research proposal.,

3. ENHANCED MULTI-LAYERED SECURITY ARCHITECTURE AND FRAMEWORK FOR CONTEXT-AWARE MOBILE WEB SERVICES

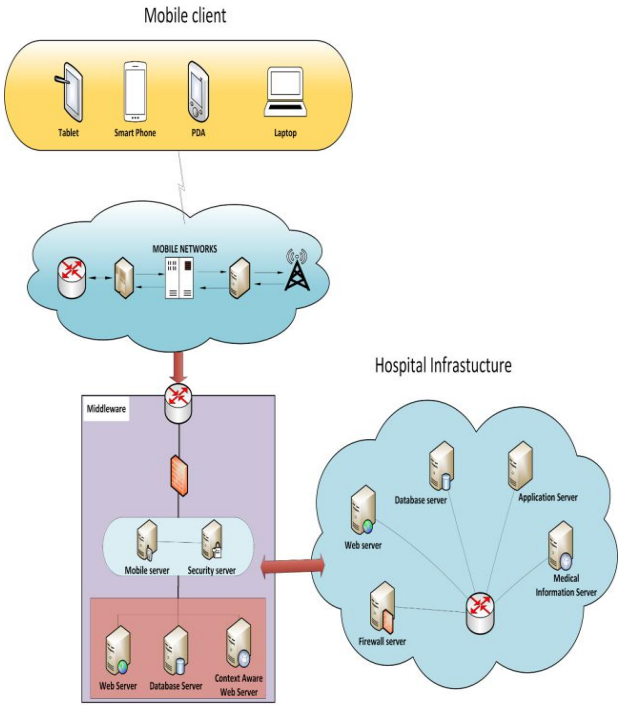

Fig 1. Security Architecture For Context-Aware Mobile Web Services

Figure 1 depicts the proposed security architecture for context aware mobile web services that consists of Mobile Client (MC), Mobile Network and Hospital Infrastructure . The proposed architecture provides the necessary technical infrastructure such as acquiring user information, connectivity, authentication, and communication to facilitate the necessary information about health care industries and mobile users which acts as an intermediary between the health care industries and the clients.

Also this architecture support for strong authentication and non-repudiation by employing digital signatures. Confidentiality and message integrity are also provided using digital signature. The proposed architecture for providing the various services in context aware web services and its functionalities, PKI based security algorithms and the performance of the model is proposed.

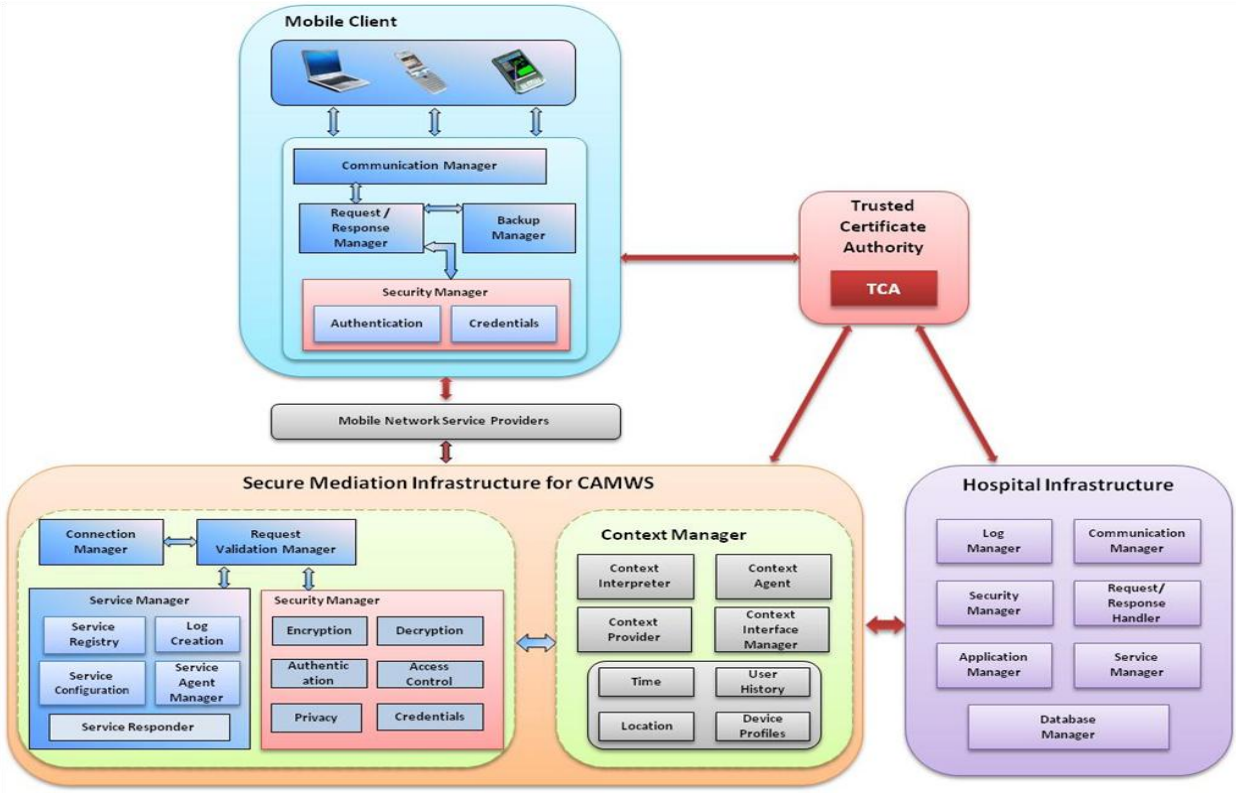

Fig 2. Enhanced Security Framework for Context-Aware Mobile Web Services

Figure 2 depicts the proposed Multi-Layered Security Framework for Context-aware mobile web services, which provides essential infrastructure for various significant operations such as acquiring user information, connectivity, authentication and communication to facilitate secure web services for multiple users. The framework that consists of the following major components: mobile client, secure mediationinfrastructure for Context Aware Mobile Web Services that includes Context Manager (CM), and a Hospital Infrastructure.

The mobile client starts to communicate with the IS by entering AcCode at mobile device. The User Interface Manager handles various interfaces such as authentication interface and payment authorization interface. The Security Manager is also responsible for authentication, signing the request, certificate management, secret key management and distribution etc. The Backup Manager supports atomic transaction in case of network disconnection. When the network is disconnected, the failed transaction is picked up from the restore point and resumes the data, instead of restart again.

The Context-aware Web Services Manager (CAWSM) acts as an intermediary between the clients and the Health Care industry Service Manager (HCSM). When the client makes the request i.e. CReq, it is customized by the Request Interceptor according to CAWSM format. The Request Handler maintains the queue of requests and handles them in sequential order. The CM sends the CReq to Security Manager of CM (SMCM) which authenticates and authorizes CReq with the User Identification Code (UIC) to avail the web services. CM forwards CReq to the Service Manager (SM) of CAWSM. The Request Validation Manager of SM filters CReq for spam or virus. Then SM sends CReq to Service Configuration Manager (SCM). Otherwise, CReq is returned to CM.

The SCM configures CReq with the help of Service Initiator (SI) and creates web services. If CReq is available in Service Registry then log is created. Otherwise,, "No Service" message is sent to CM. The SM make some group of Context Aware Web Service (CAWS) and sends it to Security Manager for SM (SMSM). The CAWS is encrypted as ECWS by SMSM. The CAWSM sends ECWS to Health care Industry Service Manager(HCSM) through Load Balancer. A connection is established between CAWSM and HCSM. The HCSM authenticates and authorizes CAWSM with a shared secret key. The HCSM decrypts the set of services and makes service classification. The SMHCSM maps CAWS with application services available at Service Subscriber (SS) and executes the services. If CAWS requires data access, then the connection is established with Health Care Industry Database Security Manager (HCIDBSM). The HCIDBSM validates the access privileges of CAWS and returns the data with data service. If CAWS does not require data access, then the service is executed if the mapping fails, then the error message is sent to SM of CAWSM. The HCSM returns the encrypted service response (ESR) to Service Responder through Load Balancer. The SMSM of CAWSM decrypts ESR, terminates the log for the service response and forwards it to CM of CAWSM. The CM encrypts the service response using UIC and sends the encrypted CWS to the client

4. RESULT AND DISCUSSION

Results and Discussions The proposed framework provides an end to-end security by accomplishing the security properties such as user authentication, authorization of web services, message confidentiality, data integrity and non repudiation. In this paper, proposes a enhanced Multilayered Security Framework for Context Aware Mobile Web services in health

care industry related services. The proposed architecture satisfies the key elements such as confidentiality and message integrity are proved by using strong encryption and decryption algorithms. The framework consists of four different security levels such as Level-1 (User Authentication), Level-2 (Service Authorization), Level-3 (Message Protection) and Level-4 (Server Authentication).

5. CONCLUSION

Still there has been no concrete proposal offered so far to build a secure health care related web applications. This situation has led to the design and development of security architecture for health-care related Web application. It is designed primarily for secure health care industry web services such as a finding hospital location service, doctor service, specialty hospital service, other services, etc. for the patients and the public from any where This framework provides the secured context-aware mobile web services for the mobile/web users through the proposed model that acts as an intermediary between the users and the various health care industries located in different geographical area. This model has also been designed to provide the security at multilevel such as user level, web services level, health care industry level and database level.

6. REFERENCES

[1] Timothy E. Levin, Cynthia E. Irvine, Clark Weissman and Thuy D. Nguyen "Analysis of Three Multilevel Security Architectures",CSAW'07,Fairfax, Virginia, USA, ACM, November 2007.

[2] SHENHaibo, HONG Fan, A Context-Aware Role-BasedAccess Control Model for Web Services", Proceedings of the2005 IEEE International Conference on e-Business Engineering(ICEBE'05), 5 IEEE, 2006.

[3] Chaowang Shang, Zongkai Yang, Qingtang Liu, ChenglingZhao, A Context Based Dynamic Access Control Model forWeb Service", International Conference on Embedded And Ubiquitous Computing, IEEE, 2008.

[4] Kenya Nishiki and Erika Tanaka, "Authentication and AccessControl Agent Framework for Context-Aware Sannella, M. J. 1994 Constraint Satisfaction and Services", Proceedings of the Symposium on Applications and the Internet Workshops, IEEE, 2005.

[5] Forman, G. 2003. An extensive empirical study of Kuyoro Shade O.Ibikunle Frank Awodele O. and Okolie Samuel O."Security Issues in Web Services", IJCSNS International Journal of Computer Science and Network Security, Vol.12 No.1, 2012.

[6] SomeshJha, Mahesh Tripunitara, Qihua Wang, and William H. Winsborough, "Toward Formal Verification of Role-Based Access Control Policies", IEEE Transactions on Dependable and Secure Computing, Vol. 5, No. 4, 2008.

[7] Ravi S. Sandhu, Edward J. Coyne, Hal L. Feinstein and Charles E. Youman, "Role-Based Access Control Models", IEEE Communications Magazine, Vol. 29, No. 2, pp. 38-47, 1994.

[8] G. H. Hwang, Y. H.Chang and T. K.Chang, "An Operational Model and Language Support for Securing Web Services", IEEE International Conference on Web Services (ICWS), 2007.

[9] Yanjiang Yang, Robert H. DengandFengBao, "A Practical Password-Based Two-Server Authentication and Key Exchange System", IEEE Transactions on Dependable and Secure Computing, Vol. 3, No. 2, April-June2006.

[10] Richard Millham, "Creating Context Aware and AdaptableWebServices within a Security Framework", IEEE, 2013

[11] Joseph Charles P, Britto Ramesh Kumar S, "Design of a Secure Architecture for Context Aware Web Services using Access control mechanism", IEEE, 2014.

[12] Liu Hong-yue, Deng Miao-lei, Yang Weidong, "A Context Aware Fine-grained Access Control Model", InternationalConference on Computer Science and Service System, IEEE,2012.