
WWJMRD 2018; 4(2): 168-172
*www.wwjmrd.com*
*International Journal*
*Peer Reviewed Journal*
*Refereed Journal*
*Indexed Journal*
*UGC Approved Journal*
*Impact Factor MJIF: 4.25*
*E-ISSN: 2454-6615*

**P. Joseph Charles,**
Assistant Professor,
Department of Information Technology, St. Joseph's College, Trichy-2, India

**S. Britto Ramesh Kumar**
Assistant Professor,
Department of Computer Science, St. Joseph's College, Trichy-2, India

**Correspondence**:
**P. Joseph Charles,**
Assistant Professor,
Department of Information Technology, St. Joseph's College, Trichy-2, India

# An Enhanced Multi-Layered Secured Architecture for Context-Aware Web Services

**P. Joseph Charles, S. Britto Ramesh Kumar**

**Abstract**
The Web services technologies change the software industry dramatically by developing and integrating enterprise Web services and applications so as to enable the users to access them. 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). Computing becomes increasingly mobile and pervasive today; these changes imply that applications and services must be aware and adapt to highly dynamic environments. Therefore in this paper a novel Security Framework for Context aware Mobile Web Services is proposed and developed for health care industries to share the important data to the mobile users through Web-enabled mobile devices. The proposed approach certainly proves to be advancement over the existing ones and has applicability to all related web services.

**Keywords:** HCIW, PKI

## 1. Introduction

A Web service is a piece of business logic, located on the internet that is accessible through standard based internet protocol such as HTTP or SMTP. Context aware Web services refers to an adaptive process of delivering contextually matched Web services to meet service requesters' needs at the moment. A context-aware system have many components, such as context sensor, context storage, context reasoner, context consumer, to name just a few. These components are logically separated from applications that they support. Context-awareness refers to the properties of a system that make it aware of the state and surroundings of its user, and help it adapt its behaviour accordingly [SAT, 2002] and [DEY, 2001]. 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). Since it was proposed about a decade ago, many researchers have studied this topic and built several context-aware applications to demonstrate the usefulness of this new technology. Context-aware applications, however, have never been widely available to everyday users.

## 2. Review of Literature

Major research efforts were undertaken in recent years to build secure context aware mobile applications. Security is an important requirement for these applications and for information exchange. However, it is difficult to authenticate the clients strongly and provide an adequate level of security. In this chapter, existing architecture, models and security frameworks of the context aware web services are evaluated and reviewed**.**

### A. Authentication

Kumar et al. [KUM, 2016] have proposed an enhanced Security of Internet Services through Continuous and Transparent using User Identity Verification. It addressed on explores promising alternatives offered by applying biometrics in the management of sessions. A secure protocol is defined for perpetual authentication through continuous user verification. Hayashi et al. [HAY, 2013] have Propounded Context-Aware Scalable Authentication.

This research work, context-aware scalable authentication (CASA) as a way of balancing security and usability for authentication provides a probabilistic framework for dynamically selecting an active authentication scheme that satisfies a specified security requirement.

**B. Access control**

Jagadamba et al. [JAG, 2015] have proposed an Adaptive Context-Aware Access Control Model for Ubiquitous Learning Environment. Context-Aware Access Control (CAAC) adapts itself to the varying environment by developing a proactive centralized monitoring system that acts as a context server through acquiring and managing the context information for analyzing user requirements. Bilal shebaro et al. [BIL, 2013] have Illustrated context based Access control system for mobile devices. This research work describes about personalized report of Android OS using Context-based access control policies. Of dimensions work life balance, Corporate social

**C. Confidentiality**

Danila et al. [DAN, 2014] have proposed a web-service based architecture for SCM that enables enterprises to develop context-awareness and to achieve interoperability at data, services, processes and business levels using event based web service notifications. Therefore in this paper a novel Security Framework for Context aware Mobile Web Services is proposed and developed for health care industries to share the important data to the mobile Users

**3. Security Architecture for Context Aware Mobile Web Services**

The proposed framework for Context Aware Mobile Web Services is envisaged to avail secure web services and applications anywhere, anytime through the mobile device with an end to end security. The proposed framework provides the necessary technical infrastructure such as acquiring user information, connectivity, authentication, and communication to facilitate the necessary health care services and mobile users. This proposed framework support strong authentication, Confidentiality, integrity and non-repudiation using digital signatures. The proposed framework consists of five major components namely Mobile Server (MS), Security Server (SS), Database Server (DBS), Web Server (WS) and Context Aware Web Server (CAWS). These five components are interconnected and interdependent which make the proposed framework more secure, and unique. The security framework provides well-defined and logical components and artifacts of the proposed system. This framework is explicitly developed for the health care industry-related web services for the mobile users in a secured manner. Figure 3.1 depicts the security architecture for Context Aware Mobile Web Services.

A. Security Mechanism in SFCAMWS

The SFCAMWS architecture is designed with the high level security using Public key Infrastructure (PKI). The PKI provides strong security services and facilitates the distribution and the use of public keys and certificates. The PKI offers a great deal of advantages with digital signature and standard encryption/decryption algorithms using asymmetric key cryptosystem. Both privacy and authentication are accomplished by using the combination of encryption and digital signature. The message digest algorithm ensures the message integrity effectively.The non-repudiation is supported by the use of digital signature. The standard encryption algorithm are used to affirm the strong data confidentiality. The proposed security architecture of SFCAMWS supports authentication mechanisms in five different levels and tested successfully. Five level Security for Context Aware Mobile Web Services could be possible. They are illustrated in the below sections.

1) Device Level

The process of identifying the user with their mobile device by Unique ID IMEI and user name and password. At every the time the any Internal user activates his/her device to perform the health care industry web service application, immediately the user's device can be validated and then if it matches with the server then they are allowed to perform the operations.

2) User Level (Authentication)

The process of identifying an individual is usually based on the username and password. Authentication ensures the individual who is claiming to be, but says nothing about the access rights of the individual. The credentials provided by the client are compared to those on file in a database of authorized user's information on a local operating system or within an authentication server. If the credentials match, the process is completed and the client is granted the system access.

3) Communication Level (Confidentiality)

Cryptography involves encryption and decryption of the messages. Encryption process is converting a plain text into cipher text by using an algorithm, while decryption process is getting back the encrypted message. A cryptography algorithm is the function used for encryption and decryption.

4) Service Level (Authorization)

Role-Based Access Control (RBAC) is a method of regulating access to a computer or network resources based on the roles of individual users within a community. In this context, access is the ability of an individual client to perform a specific task, such as view, create, or modify a file. Roles are defined according to job competency, authority, and responsibility within the industry. This framework provides each user, a flexible access control mechanism is used in a multi-user environment. It should allow multiple controllers, who are associated with the shared data, to specify access control policies.

5) Database Level (Integrity)

In order to provide secure the health care industries database with proper firewall server which is the database level security.

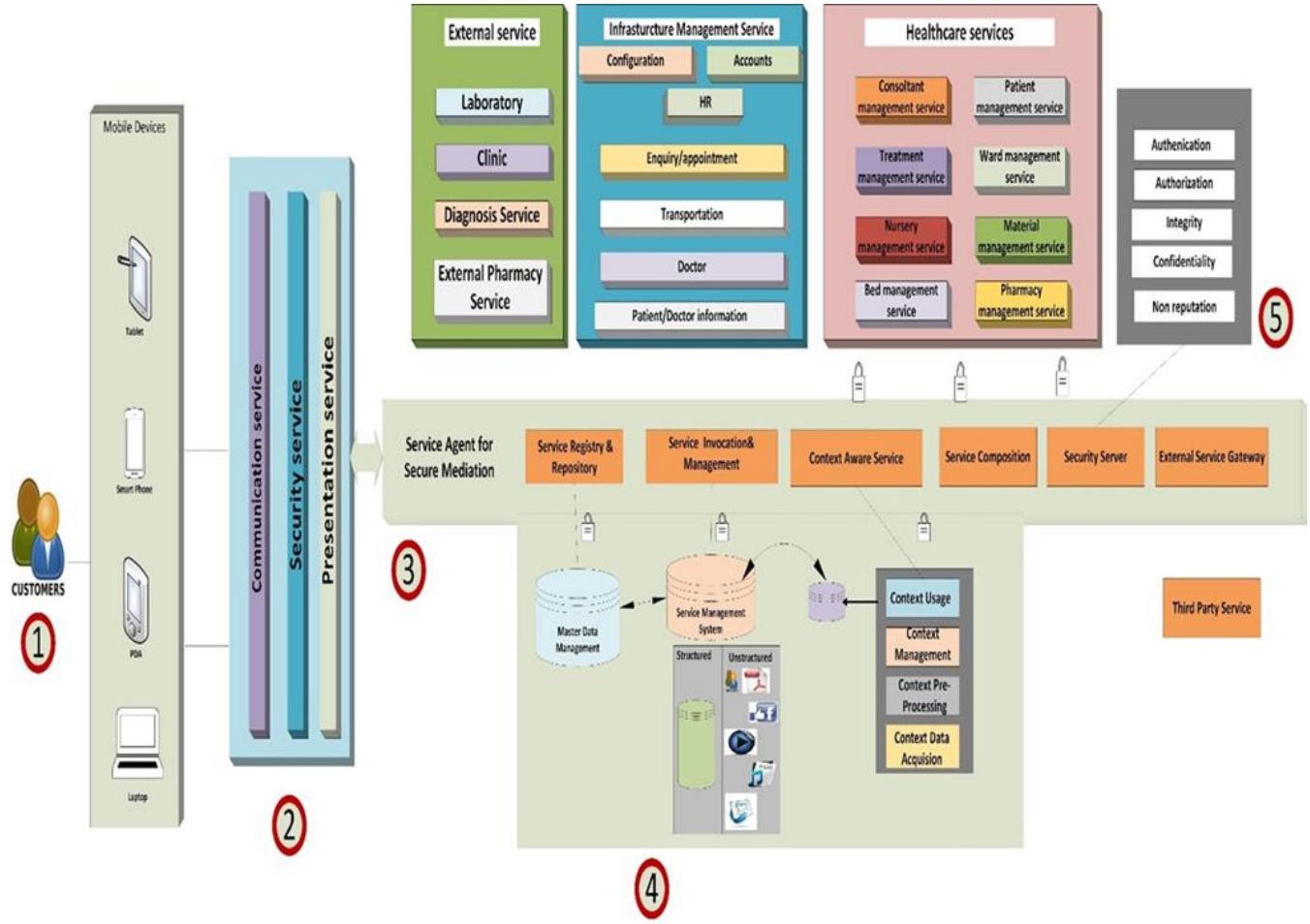


**Fig. 3.1:** Security Architecture for SFCAMWS

## 4 Experimental Study And Result Analysis

The core objective of the experimental study is to focus upon the measurement of the processing time for the encryption using RSA algorithm used by the Web-enabled client machine during client authentication and client/server authentication.

System Implementation and Testing

The SFCAMWS application system has been developed using PHP Language. The internal components of the architecture are different types of servers and workstations. The internal structure of the proposed system consists of various modules. The Graphical User Interface module, which can handles the creation of all the user interfaces and its related objects. The Communication module, that includes the creation of communication interfaces for all supported protocols between client and server. The third module is Business logic module has the responsibility for creating web service request messages and processing the web service responses messages.

Finally Security module, that implements the security elements to provide security features such as authentication, authorization, confidentiality, integrity and non-repudiation for the web service transactions and web service-oriented operations.

Implementation of SFCAMWS Application Software:

The SFCAWS application offers user interfaces for the following transactions:

1. The initial-level User Authentication to the SFCAMWS server based on the user profile.
2. The next-level Server Authentication to the user based on server certificate.
3. Authorization for the health care industry related web services using the Role (R) of the user.
4. Service Response to the user.

### A. Performance Analysis of Client/Server Authentication

The performance of secure communication between Client / Firewall Server authentication has been analysed for Mobile Users for their login session, two keys are generated in both

the client users and firewall Server such as public and private keys. Table 4.1 represents the response time of the client/ Firewall Server with respect to the time taken for key generation, encryption, decryption and the database validation. Figure 4.1. shows the performance result of client / Firewall Server Authentication by a plot between number of requests verses mean response time (ms).

**Table 4.1:** Results of the Mean Response Time for Client / Firewall Server Authentication

| Number of Requests | Mean Response Time(ms) |
|---|---|
| 1 | 5 |
| 10 | 6 |
| 20 | 7 |
| 30 | 11 |

| | |
|---|---|
| 40 | 26 |
| 50 | 32 |
| 100 | 75 |
| 200 | 234 |
| 300 | 356 |
| 400 | 368 |


**Fig 4.1**: The Performance Results for Client/ Server Authentication

**B. Performance Analysis of Secure Communication between Firewall Server / HCIW Server Authentication**

The communication between the Firewall Server and authorized industry server is again done with EECC algorithm. Hence, public and private keys are generated in both servers for securing the data transmission. Table 4.2 represents the response time of the Firewall Server with respect to the time taken for key generation, encryption/ decryption and the database validation. Figure 4.2 shows the performance result for Firewall Server / Health Care Industry Server Authentication by a plot between numbers of requests verses mean response time (ms).

**Table 4.2:** Results of Mean Response Time Firewall Server / Health Care Industry Server Authentication

| Number of Requests | Response Time(ms) |
|---|---|
| 1 | 5 |
| 10 | 6 |
| 20 | 11 |
| 30 | 15 |
| 40 | 26 |
| 50 | 39 |
| 100 | 215 |
| 200 | 387 |
| 300 | 655 |
| 400 | 689 |

The experimental study has revealed that the public key algorithm thus provides low response time at mobile phone compared with symmetric. However, it achieves high level security in terms of confidentiality and non-repudiation over symmetric algorithms. The proposed framework supports end –to- end secure communication between and within the internal users.

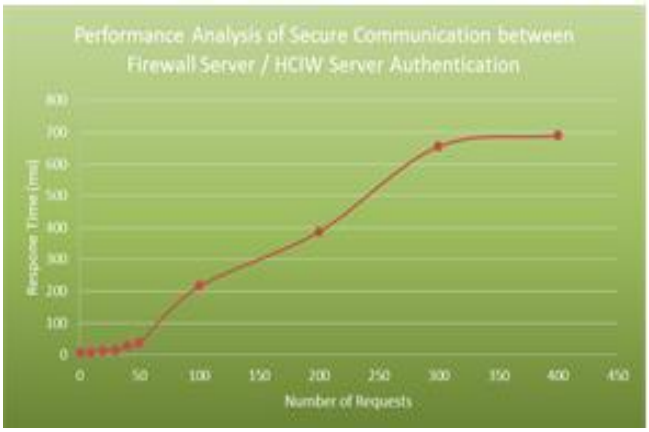


**Fig 4.2:** Performance result for Firewall Server / Health Care Industry Server Authentication

**Conclusion**

Since security plays a crucial role in the Context Aware Mobile Web services scenario, the design and development of security framework for complex Web application, like health care industry has become more promising research area. Furthermore, there has been considerable amount of research work carried out in the development and deployment of secure enterprise web applications. The proposed framework satisfies the key elements of confidentiality and message integrity are proved by using strong encryption and decryption algorithms. This includes the algorithm for Client and Server Authentication while communication between client machine and Firewall Server. As a result of this approach, health care -related transactions are transmitted over the Internet with confidentiality and authentication taking place in bi-direction which includes both the client and server. The novelty of the proposed techniques lies on the protection of network from malignant attacks such as replay, brute force, Man-In-The-Middle and eavesdropping.

**References**

1. Satyanarayanan, M. “Pervasive Computing: Vision and Challenges”, IEEE Personal Communications, pp. 10-17, August 2002.
2. Dey, A.K., Salber, D. and Abowd, G.D. “A conceptual framework and a toolkit for supporting the rapid prototyping of context-aware applications”, Human-Computer Interaction, Vol.16, pp.97-166, 2001.
3. Kumar G C, Rajesh S, Surya K, “Enhanced Security of Internet Services through Continuous and Transparent using User Identity Verification”, IJSRSET Volume 2 - Issue 2, 2016.
4. Eiji Hayashi, Sauvik Das, Shahriyar Amini, Jason Hong, Ian Oakley, “CASA: Context-Aware Scalable Authentication” Symposium on Usable Privacy and Security (SOUPS) 2013, Newcastle, UK.
5. Jagadamba G, B Sathish Babu, “Adaptive Context-Aware Access Control Model for Ubiquitous Learning Environment”, BIJIT - BVICAM’s International Journal of Information Technology, New Delhi, 2015.

6. Bilal Shebaro, Oyindamola Oluwatimi, Elisa Bertino, "Context-based Access Control Systems for Mobile Devices", IEEE Transactions on Dependable and Secure Computing, 2014.
7. Cristian Danila, Georgiana Stegaru, Aurelian Mihai Stanescu and Cristina Serbanescu, "Web-service based architecture to support SCM context-awareness and interoperability", Springer Science+Business Media, New York, 2014.