Experimental Analysis Of Securing Context Aware Mobile Web Services

Dr. P Joseph Charles

Abstract: Service Computing is a cross-discipline that covers science and technology of bridging the gap between Business Services and IT Services. Service Computing technology suite includes Web services and Service Oriented Architecture (SOA), cloud computing, business consulting methodology and utilities, business process modeling, transformation and integration. The aim of Services Computing is to empower IT services and computing technology to perform business services more efficiently and effectively. The Context sensitive applications requires contextual information that must be obtained from various sources such as sensors that are embedded in the environment, devices that are carried by end users, repositories of historical data tracking use of the application, and information contained in user profiles. The rapid proliferation of mobile devices, wireless technologies and services, and the demand of user location awareness fueled by next generation mobile distributed computing research have ushered in the area of Context Aware Computing. Light weight portable computers, IP based appliances, and the popularity of Internet is strong forces to the service providers to support seamless user mobility. Realizing the change environment with new class of applications that are aware of the location in which they are run remains a research challenge. Although Research and Development on Context Aware Mobile Computing and Applications have attained a notable success in the past decade they are still in the infancy stage.
.

Keywords: Web Services, XML, SOAP, context-awareness, access-control, Confidentiality, Hit ratio

1 INTRODUCTION

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.

1.1 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.

1.2 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. In the recent years many researchers have studied and built several context-aware applications to demonstrate the usefulness of this new technology. Two technologies allow users to move about with computing power and network resources at hand like portable computers and wireless communications. Every day computers are becoming smaller and smaller to allow hand-held impressive computing power, whereas the bandwidth of wireless links keep increasing.

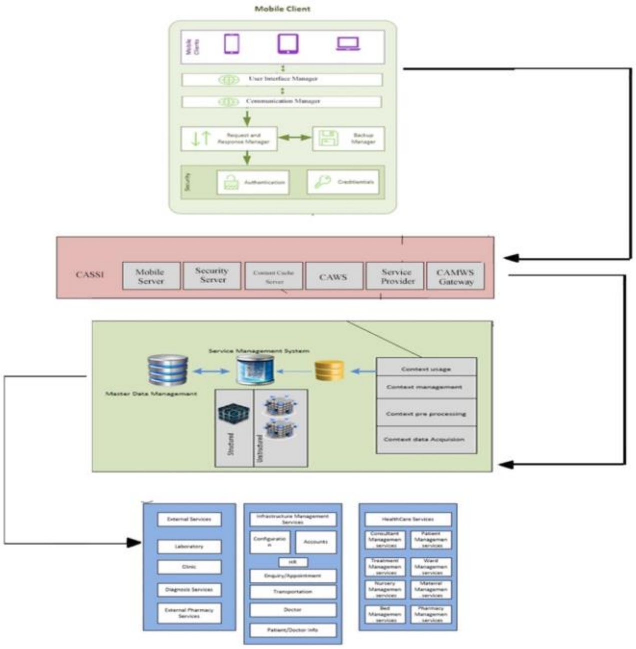
1.4 Security Limitations in Web Services

While providing several benefits, web services technology has been facing serious threats like Capture and Replay Attacks, Buffer Overflows, Denial-of-Service Attacks (DoS), Improper Error Handling, Eavesdropping, prefix hijacking and interception in the Internet due to a man-in-the-middle attack Therefore, security has become the key issue in the field of web services technology. There are many complexities in web services which complicate their security. Numerous threats can compromise the integrity, availability or confidentiality of a web service, that may expose the back-end systems of web service. Thus, the most important research thrust in web service technology is web services security. However, Web service security needs more attention in major security issues like authentication, authorization, confidentiality, integrity and non-repudiation.

2 REVIEW OF LITERATURE

Hayashi et al. [HAY, 2013] have Proposed a probabilistic framework for Context-Aware Scalable Authentication (CASA). The probabilistic framework is dynamically selecting an active authentication scheme that satisfies a specified security requirement given passive factors. The prototypes could select active authentication factors based on passive factors which balancing security and usability of user authentication. The basic idea of CASA is the passive multi-factor data can be used to modulate the strength of active authentication needed to achieve a given level of security. Kayes et al. [KAY, 2015] have presented a framework for Purpose Oriented Situation-Aware Access Control (PO-SAAC) software services. This framework specifies purpose oriented situations and it's related to situation-specific access control policies. To achieve context-aware access control, the framework considers the states of the entities and the states of the relationships between entities. Kosala Yapa Bandara et al. [KOS, 2013] have proposed many consumption aspects and techniques to manage context constraints. It also proposes an ontology-based context model for service provisioning. The important objective of this model is to provide contextualization of dynamically relevant aspects of Web service processes. Antorweep Chakravorty et al. [ANT, 2013] have proposed a framework for data security and privacy. The framework provides security and privacy through sensor data from smart homes. Privacy is associated with collection, storage, use, processing, sharing or destruction of personally identifiable data. Storing the personally identifiable data as hashed values with holds identifiable information from any computing nodes.

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.



3.1Framework for Securing Context Aware Web Service

The multilevel security is adopted for the proposed framework sing PKI. Additionally, CAMWS gateway facilitates secure communication among the service requestors and SPs, via HTTPS. It also offers security services with the help of SS using digital signatures and standard encryption and decryption algorithms. The message confidentiality and IMU's authentication are accomplished by using RSA and digital signature. The digest algorithm known as SHA-1 ensures the integrity of the messages successfully. Another important security service, non-repudiation, is well supported by the digital signature. The security mechanisms are adopted in different levels and tested them successful. Hence, the proposed security framework for CAMWS is a novel one with end-to-end security using PKI to access the web services as well as data services.

4 EXPERIMENTAL STUDY AND PERFORMANCE ANALYSIS

The core objective of the experimental study is to focus upon the measurement of the processing time with respect to the latency for the security services like encryption using RSA algorithm and message digest using SHA 1during mobile client and MS authentication. The performance of the proposed architecture has been investigated on test bed with respect to hit ratio, throughput and the response time

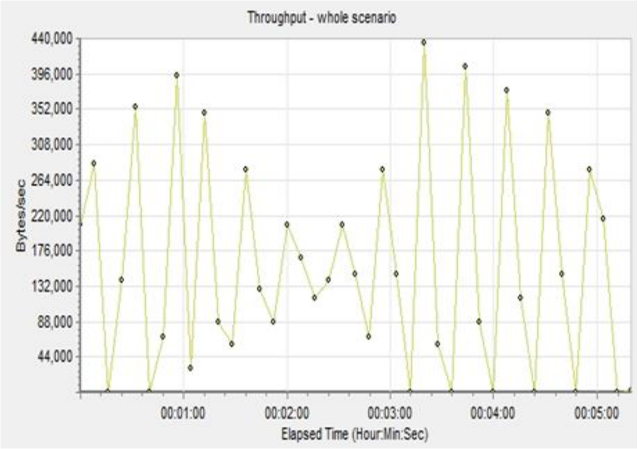
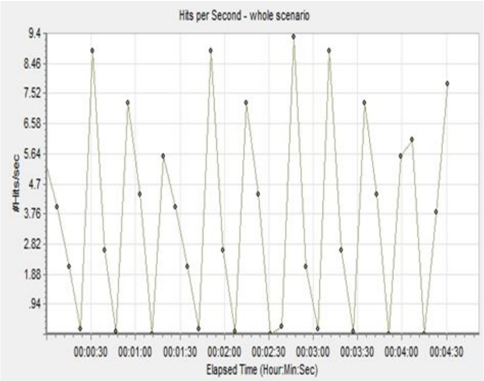


Figure 1 *Output screenshots for Response time per Seconds*

Tests are done to find out the response times with 1, 5, 10, 20, 30, 40, 50, 60, 70, 80, 90 and 100 successive internal users generating request to the proposed system simultaneously. 100 users are chosen to represent the test scenario. It is observed that even when there are 110 simultaneous service requesters, the graph does not produce a straight line, thus it is observed that the throughput of the proposed system is nonlinear. Hit Ratio on the serverThe number of hits made on the SFCAMWS by the users during each second of the load test is observed using the LoadRunner tool. Figures 2 displays the screenshots for two different loads on the SFCAMWS by creating 100 and 1000 virtual service requesters. This graph is useful for determining the number of users at any given amount of time.



color	scale	web resource	max	min	avg	std	last
🟩	*1*	*hits per second*	*n/a*	*n/a*	*3.650*	*n/a*	*7.800*

figure 2 *output screenshots for hit ratio per seconds*

figure 2 indicates that the service requesters are ramped up every 14 seconds at the arrival rate of 2 and this process continues until the number of service requesters reaches 1000. the service requester's load is continued up to 04:30 minute. the sample output screen shots to evaluate the amount of load generated by 100 and 1000 service requesters in terms of number of hits per second.the experimental study has validated for the proposed sfcamws in terms of authentication, latency, throughput, hit ratio and response time.

5 CONCLUSION

Propose a security framework for context aware mobile web services (sfcamws) using public key infrastructure to perform health care web services through web-enabled mobile devices. The proposed framework satisfies the key elements of confidentiality and message integrity are proved by using strong encryption and decryption algorithms. 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.

6. FUTURE DIRECTIONS

- This Framework can be extendable Service-Oriented Infrastructure following the Cloud Computing Paradigm that Will Provide Services for Mobile Semantic Web Services.
- This Work can be extended to Semantic Web Based Context-Aware Web Services, where Healthcare Related requests can be handled In a more Intelligent and Secure way to overcome Fraudulent Intruders.
- This Framework can further be Extended to Biometric Authentication with The Combination of Pki.
- It would be reasonable to extend the Encryption And Decryption Mechanisms using Elliptic Curve Cryptography. That solution would significantly increase the security level of the Services.
- In Recent New Communication Technology, such as Near Field Communication (Nfc), the Mobile Phones can be used like a Contactless Card that pose New Challenges while Accessing Context Aware Mobile Services.

7 REFERENCES

[1] Hayashi Eiji, Sauvik Das, ShahriyarAmini, Jason Hong, Ian Oakley, “CASA: Context-Aware Scalable Authentication”, Symposium on Usable Privacy and Security (SOUPS) 2013, Newcastle, UK.

[2] A.S.M. Kayes, Jun Han and Alan Colman, “OntCAAC: An Ontology-Based Approach to Context-Aware Access Control for Software Services”, Computer Science Theory, Methods and Tools, The Computer Journal, Vol. 58 No. 11, 2015.

[3] Kosala YapaBandara,• MingXue Wang, and Claus Pahl, “An extended ontology-based context model and manipulation calculus for dynamic Web service processes”, Springer-Verlag London 2013.

[4] Antorweep Chakravorty, Tomasz Wlodarczyk, Chunming Rong, “Privacy Preserving Data Analytics for Smart Homes”, IEEE Security and Privacy Workshops, 2013.

[5] M..Madden and K. Zickuhr. (2011), Online adults use social networking sites(Online) Available: http://www. pewinternet .org

[6] Boshmaf, I. Muslukhov, K. Beznosov, and M. Ripeanu, “The socialbot network: when bots socialize for fame and money (Published Conference Proceedings style),” in proc. 27th Annu. ACM Conf. Computer Security Applications; 2011, pp. 93–102.

[7] M. Egele, A. Moser, C. Kruegel, and E. Kirda, “Pox: Protecting users from malicious Facebook applications in Pervasive Computing and Communications (Presented Conference Paper style),” presented at the IEEE Conf.2011, pp. 288–294.

[8] Y. Liu, K. Gummadi, B. Krishnamurthy, and A. Mislove, “Analyzing Facebook privacy settings: User expectations vs. Reality (Published Conference Proceedings style),” in Proc. ACM SIGCOMM conf. Internet Meaurement; 2011, pp.61–70.

[9] G. Stringhini, C. Kruegel, and G. Vigna, “Detecting spammers on social networks(Published Conference Proceedings),” in Proc. 26th Annu. ACM Conf. Computer Security Applications; 2010, pp. 1–9.

[10] S. Nelson, J. Simek, and J. Foltin, The legal implications of social networking(Book style), Regent UL Rev., 2009,vol. 22, pp. 1–481.

[11] J. Kuzma, “Account creation security of social network sites (Book style),” in International Journal of Applied Science and Technology, vol. 1, no. 3, pp. 8–13, 2011.

[12] S. Mahmood and Y. Desmedt, “Poster: preliminary analysis of google+’s privacy (Published Conference Proceedings style),” in Proc. 18th Annu. ACM Conf. Computer and Communications Security: 2011, pp809—812.