Web Services Security Architectures for Secure Service Oriented Analysis and Design

D.Shravani [#1], Dr.P.Suresh Varma[*2], Dr.B.Padmaja Rani [#3], K.Venkateswar Rao[*4] M.Upendra Kumar[#5]

[#1]Research Scholar CS Rayalaseema University Kurnool A.P. India

*[*2]Principal and Professor CS Adikavi Nannaya University A.P. India*

[#3] Professor CSE JNTU CEH Hyderabad A.P. India

*[*4] Associate Professor CSE JNTU CEH Hyderabad A.P. India*

[#1]Research Scholar CSE JNTU Hyderabad A.P. India

***Abstract*— This paper discusses the research methodology on Web Services Security Architectures for Secure Service Oriented Analysis and Design. Initially we discuss about the Research Methodology for Designing Dependable Agile Layered Security Architecture Solutions for Web Services Security Architectures. Finally we discuss an implementation case study of ensuring data security architecture on Web Services Cloud.**

***Keywords*— Web Services, Security Architectures, Agile Modeling, Dependability**

I. Introduction

Web Services: According to World Wide Web Consortium (W3C), "A Web Service is a software application identified by a URI (Uniform Resource Identifier), whose interface and bindings are capable of being identified, described and discovered by XML (eXtensible Markup Language) artifacts and supports direct interactions with other software applications using XML based messages via Internet-based protocols". Web Services are among the most important emerging technologies in the e-business, computer software and communication industries. The Web Services technologies will redefine the way that companies do business and exchange information in twenty-first century. They will enhance business efficiency by enabling dynamic provisioning of resources from a pool of distributed resources. Due to the importance of the field, there is a significant amount of ongoing research in the areas. In a parallel effort, standardizations organizations are actively developing standards for Web Services. The Web Services are creating what will become one of the most significant industries of the new century Web Services Computing is a diversified discipline suite that related to the technologies of Business Process Integration and management, Grid/Utility/Cloud computing paradigms, autonomic computing, as well as the business and scientific applications. It applies the theories of science and technology for bridging the gap between Business services and IT services.

Secure Software Architectures (Security Architectures) Software Engineering covers the definition of processes, techniques and models suitable for its environment to guarantee quality of results. An important design artifact in any software development project is the Software Architecture. Software Architecture's important part is the set of architectural design rules. A primary goal of the architecture is to capture the architecture design decisions. An important part of these design decisions consists of architectural design rules. In an MDA (Model-Driven Architecture) context, the design of the system architecture is captured in the models of the system. MDA is known to be layered approach for modeling the architectural design rules and uses design patterns to improve the quality of software system. And to include the security to the software system, security patterns are introduced that offer security at the architectural level. More over, agile software development methods are used to build secure systems. There are different methods defined in agile development as extreme programming (XP), scrum, feature driven development (FDD), test driven development (TDD), etc. Agile processing includes the phases like agile analysis, agile design and agile testing. These phases are defined in layers of MDA to provide security at the modeling level which ensures that "security at the system architecture stage will improve the requirements for that system".

Designing Solutions for Security and Dependable Privacy Requirements: The task of developing Information Technology Solutions that consistently and effectively apply security principles has many challenges, including: the complexity of integrating the specified security functions within the several underlying component architectures found in computing systems, the difficulty in developing a comprehensive set of baseline requirements for security, and a lack of widely accepted security design methods. With the formalization security evaluation criteria into an international standard known as Common criteria, one of the barriers to a common approach for developing extensible IT Security architectures has been lowered; however more work remains. In related literature survey we found description about a systematic approach for defining, modeling, and documenting security functions within a structured design process in order to facilitate greater trust in the operation of resulting IT Solutions.

Web Services Security The flow of today's market conditions is continuously changing. Competitive demands from traditional and non-traditional businesses, the rapid appearance and growth of new channels, the rising trend to outsource certain business processes, and the demand to comply with an ever-growing amount of new regulatory and legal requirements, are all creating an increasing demand for change. The effective and efficient management of organizational changes has traditionally been a real challenge.

Service-Oriented Architecture (SOA) is the main architectural style that IT departments are currently adopting to support the aforementioned business requirements owing to its capacity to enable the loose-coupling and dynamic integration of business services and applications, and their possible operations across trust limits. Just as organization's timely response to changes in the business environment is critical to their survival, so is the appropriate protection of their assets. In the field of IT Systems, the main assets are information and IT services, which support the implementation of the business services, and must therefore handle this information in a secure manner. Securing access to information is thus a critical factor for any business and security is even more critical for IT deployment based on SOA principles.

Web Services Security Challenges are highly complex and technically advanced. On the one hand, the security challenges arising from this technology are: Risks that appear as a result of the publication on the Internet of a complete and well-documented interface to back office data and company's business logic. One of the main security problems associate with the WS is derived from the Internet publication of business interfaces through HTTP or HTTPS ports; Protecting the Semantic Web by ensuring that security is preserved at the semantic level; Context-aware and Context-based protection at the document level. Documents usually have information with different "degrees of sensitivity" which is necessary to protect at different levels of security. Access control policies that govern access to the different security parts of the documents, and an architecture enforcing these policies, currently constitute an extremely important area in the context of WS Security; Service trustworthiness, Dynamic discovery and the composition of services imply that a Web Service consumer may not know whether the services, either individually or as a whole, will behave as expected. How to select trustworthy Web Services consequently remains a challenge; the unstructured and overwhelming umber of WS Security related literature and approaches makes the developer's task of attaining a complete knowledge of all the potential WS Security issues, and standard means to address them, extremely difficult. On the other hand some of the main security objectives are: Management of Security policies in a large and distributed WS environment; Application-level, end-to-end and just-one-context-security communications.

Web Services Security Engineering Security Engineering into software development is one of the major security topics developed during the last few years. Applying security engineering throughout the different steps devised by the different software development methodologies has been a major topic in both scientific and industrial literature.

Web Services Security Architectures should define the highest level organization of the IT Security infrastructure necessary to meet the security requirements specified for the systems to be built by articulating the necessary security mechanisms in such a way that reusability, manageability and (internal / external) interoperability is guaranteed. Web Services Security Architectures have three layers, as provided by NIST standard: Web Service Layer, Web Services Framework Layer (.NET or J2EE), Web Server Layer. In services oriented web services architecture, business processes are executed as a composition of services, which can suffer from vulnerabilities pertaining to secure data access and protecting code of Web Services. The goal of the Web services security architecture is to summary out the details of message-level security from the mainstream business logic, with a focus on Web Service contract design and versioning for SOA. Service oriented web services architectures impose additional analysis complexity as they provide much flexibility and frequent changes with in orchestrated processes and services.

Service Orientation Engineering (SOE) (or Web Services) and *Agile modeling* software development presents promising solutions for contemporary software development projects to deal effectively with challenges in increasingly turbulent business environments typified by unpredictable markets, changing customer requirements, pressures of even shorter time to deliver, and rapidly advancing information technologies. Model-based agile security engineering is a promising approach that can help to fill the gap between vulnerabilities on the one hand and concrete protection mechanism on the other.

Adaptive Web Services for Modular and Reusable Software Development, Tactics and Solutions, means that Web Services provides a successful way to communicate distributed applications, in a platform independent and loosely coupled manner, providing systems with great flexibility and easier maintenance. In this sense, they are modular applications, which are self-descriptive and can be published, located and invoked from any point on the network. However, even though there are good procedures for the design, development and management of Web Services, there are scopes in which Web Services adaptation is required. Service adaptations should be implemented appropriately, so that the loosely coupled nature of Web Services is maintained, as well as allowing the implementations integration in the whole services lifecycle.

II. Objectives of the Research Work

Secure Service Oriented Analysis and Design and Secure Service modeling

Problem Statement

This research entitled "Designing Dependable Web Services Security Architecture Solutions" addresses the innovative idea of Web Services Security Engineering using Web Services Security Architectures with a research motivation of Secure

Service Oriented Analysis and Design. It deals with Web Services Security Architectures for Composition and Contract design in general, and Authentication and authorization (access control) in particular, using Agile Modeled Layered Security Architecture design, which eventually results in enhanced dependable privacy requirements, Secure Policies and Trust negotiations. All the above findings are validated with appropriate case studies of Web 2.0 Services, BPEL for Role Based Access Control, a secure stock market financial application, and their extension for spatial mobile application for cloud etc. All this research paves a way to Secure Web Engineering (or) Secure Web Science.

Research Questions addressed

1. How can Agile Modeled Layered Security Architectures design be used for Web Services Security Architectures, with a motivation of Dependable Privacy Requirements?

2. How can we extend the above approach for Web 2.0 Services Security Architectures?

3. How can we validate this approach for Spatial Mobile Web Services Security Architectures for Cloud case study?

III. Implementations and Validations

Ensuring data storage security in cloud

Cloud computing (as an extension to web services) has been envisioned as the next-generation architecture of IT enterprise. In contrast to traditional solutions, where the IT services are under proper physical, logical and personnel controls, cloud computing moves the application software and databases to the large data centers, where the management of the data and services may not be fully trustworthy. This unique attribute, however, poses many new security challenges which have not been well understood. In this article, we focus on cloud data storage security, which has always been an important aspect of quality of service. To ensure the correctness of users' data in the cloud, we propose an effective and flexible distributed scheme with two salient features, opposing to its predecessors. By utilizing the homomorphic token with distributed verification of erasure-coded data, our scheme achieves the integration of storage correctness insurance and data error localization, i.e., the identification of misbehaving server (s). Unlike most prior works, the new scheme further supports secure and efficient dynamic operations on data blocks, including: data update, delete and append. Extensive security and performance analysis shows that the proposed scheme is highly efficient and resilient against Byzantine failure, malicious data modification attack, and even server colluding attacks.

Existing System: From the perspective of data security, which has always been an important aspect of quality of service, Cloud Computing inevitably poses new challenging security threats for number of reasons.

1 . Firstly, traditional cryptographic primitives for the purpose of data security protection can not be directly adopted due to the users' loss control of data under Cloud Computing. Therefore, verification of correct data storage in the cloud must be conducted without explicit knowledge of the whole data. Considering various kinds of data for each user stored in the cloud and the demand of long term continuous assurance of their data safety, the problem of verifying correctness of data storage in the cloud becomes even more challenging.

2 . Secondly, Cloud Computing is not just a third party data warehouse. The data stored in the cloud may be frequently updated by the users, including insertion, deletion, modification, appending, reordering, etc. To ensure storage correctness under dynamic data update is hence of paramount importance.

These techniques, while can be useful to ensure the storage correctness without having users possessing data, can not address all the security threats in cloud data storage, since they are all focusing on single server scenario and most of them do not consider dynamic data operations. As an complementary approach, researchers have also proposed distributed protocols for ensuring storage correctness across multiple servers or peers. Again, none of these distributed schemes is aware of dynamic data operations. As a result, their applicability in cloud data storage can be drastically limited.

Proposed System: In this implementation, we propose an effective and flexible distributed scheme with explicit dynamic data support to ensure the correctness of users' data in the cloud. We rely on erasure correcting code in the file distribution preparation to provide redundancies and guarantee the data dependability. This construction drastically reduces the communication and storage overhead as compared to the traditional replication-based file distribution techniques. By utilizing the homomorphic token with distributed verification of erasure-coded data, our scheme achieves the storage correctness insurance as well as data error localization: whenever data corruption has been detected during the storage correctness verification, our scheme can almost guarantee the simultaneous localization of data errors, i.e., the identification of the misbehaving server(s).

1. Compared to many of its predecessors, which only provide binary results about the storage state across the distributed servers, the challenge-response protocol in our work further provides the localization of data error.

2. Unlike most prior works for ensuring remote data integrity, the new scheme supports secure and efficient dynamic operations on data blocks, including: update, delete and append.

3. Extensive security and performance analysis shows that the proposed scheme is highly efficient and resilient against

Byzantine failure, malicious data modification attack, and even server colluding attacks.
Refer to Figure 1,2,3 below which provides the sequence diagram, application architecture and execution screen shot of this application respectively.

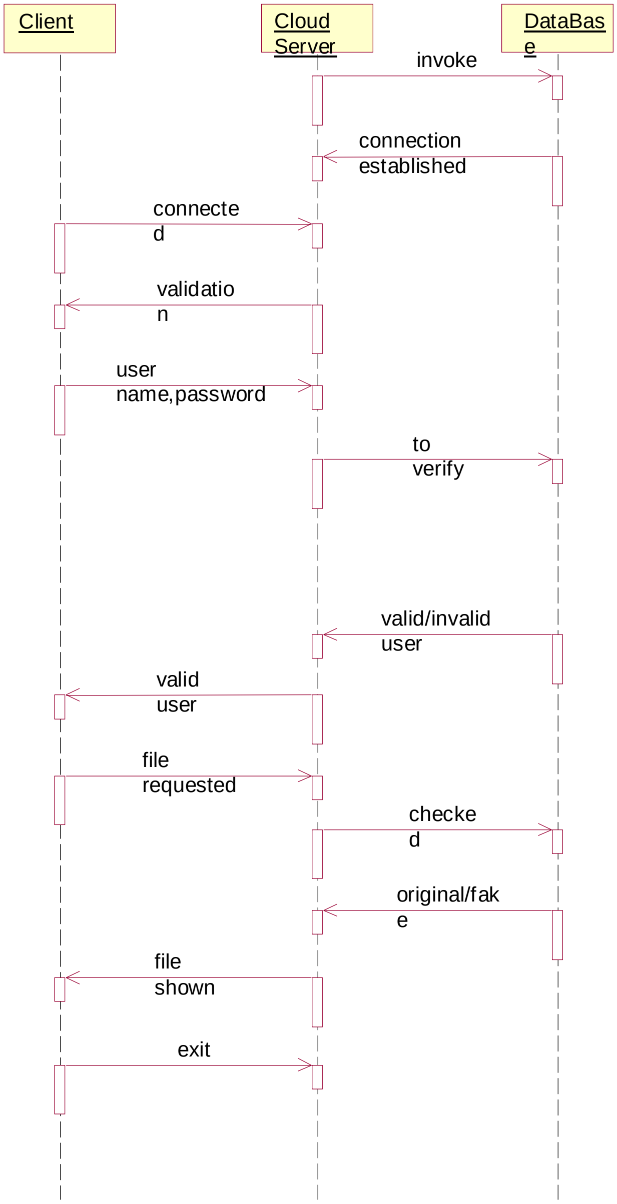


Fig. 1. Sequence diagram of the application

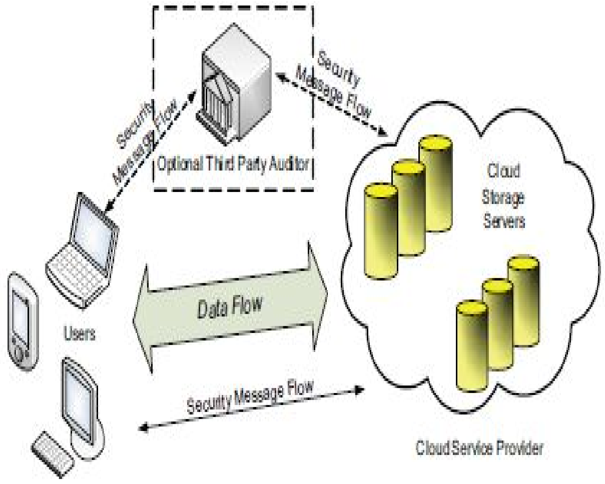
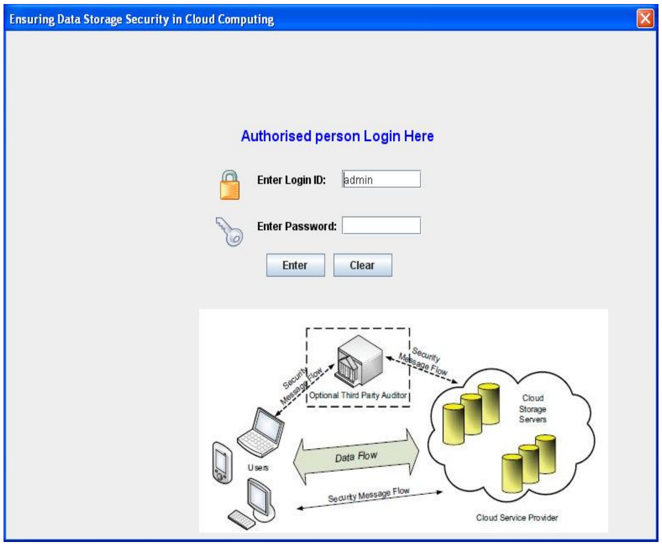


Fig. 2 Security Architecture of the application


Ensuring Data Storage Security in Cloud Computing

Authorised person Login Here

Enter Login ID: admin

Enter Password:

Fig. 3. Execution screen shot of the application

IV. CONCLUSIONS

This paper discussed about Research methodology on Web Services Security Architectures for Secure Service Oriented Analysis and Design, with a case study implementation of Ensuring Data Storage security on Web Services Cloud. Future work includes extending this approach for Spatial Web Services Security Architectures for Mobile Cloud.

REFERENCES

[1] Athula Ginge and San Murugesan, “Web Engineering: A Methodology for Developing Scalable, Maintainable Web Applications”, Cutter IT Journal Vol.14, No.7 pp. 24-35, July 2001

[2] Cenzic Inc., “Web Application Security Trend Reports”, 2009.

[3] David Geer, “Taking Steps to Secure Web Services”, IEEE, October 2003.

[4] D.K.Smetters, R.E.Grinter, “Moving from the design of usable security technologies to the design of useful secure applications”, ACM New Security paradigms workshop September 2002 pp 82 – 89

[5] Durai Pandian M et.al., “Information Security Architecture – Context aware Access control model for Educational applications”, International Journal of Computer Science and Network Security, December 2006

[6] Ferda Tartanoglu et al, ”Dependability in the Web Services Architecture”, Architecting Dependable Systems, LNCS 2677, pp. 90 – 109, 2003

[7] Gunnar Peterson, “Security Architecture Blueprint”, Arctec Group, LLC, 2007

[8] Halvard Skogsrud,” Modeling Trust Negotiation for Web Services”, IEEE February 2009

[9] Heiko Tillwick, Martin S Olivier, “A Layered Security Architecture: Design Issues”, in Proceedings of the Fourth Annual Information Security South Africa Conference (ISSA 2004), July 2004.

[10] Jim Highsmith, Alistair Cockburn “Agile Software Development: The Business of Innovation”, IEEE Computer September’2001 pp: 120:122

[11] J.J.Whitmore,”A method for designing secure solutions”, IBM systems Journal, Vol 40 No 3 2001 pp. 747-768

[12] John Hunt, “Agile Software Construction”, Springer Verlag publishers 2006

[13] Lorenzo D Martino, Elisa Bertino, “ Security for Web Services: Standards and Research Issues”, International Journal of Web Services Research, Oct-Dec 2009, pp. 48-74, Idea Group Publishing USA 2009

[14] Mark Harman, Afshin Mansouri,”Search based Software Engineering: Introduction to the special issue of the IEEE Transactions on Software Engineering”, November December 2010, pp. 737 – 741

[15] Martin Naedele, “Standards for XML and Web Services Security”, IEEE April 2003

[16] Massimo Barloletti, et. al.” Semantics-Based Design for Secure Web Services”, IEEE Transactions on Software Engineering, Vol 34, No.1, January 2008

[17] Matt Bishop, “Computer Security: Art and Science”, Pearson Education, 2003

[18] NIST Draft, “ Guide to Secure Web Services”, September 2006

[19] Ross Anderson,” Security Engineering: A guide to building Dependable Distributed Systems”, Wiley publishers, 2003.

[20] Satoshi Makino, Takeshi Imamura, Yuichi Nakamura. ”Implementation and Performance of WS-Security”, International Journal of Web Services Research, Jan-March 2004, pp. 58-72, Idea Group Publishing USA 2004

[21] Sasikanth Avancha, “A Framework for Trustworthy Service Oriented Computing”, ICISS 2008, pp. 124 – 132.

[22] Sandeep Chatterjee,” Developing Enterprises Web Services an Architects Guide”, Pearson, 2004

[23] Sarah Spiekermann, Lorrie Cranor,”Engineering Privacy”, IEEE Transactions on Software Engineering”, Vol 35 No 1 January February 2009 pp. 67 – 82

[24] Spyros T Halkidis et. al., “Architecture Risk Analysis of Software Systems based on Security Patterns”, IEEE Transactions on Dependable and Secure Computing Vol 5 No. 3, July – September 2008, pp. 129 – 142

[25] Vipul Gupta, et. al., “Sizzle: A standards-based end-to-end security architecture for the embedded Internet”, Elsevier, Pervasive and Mobile Computing, 2005

[26] Wei She, et. al. ,”Enhancing Security Modeling for Web Services using Delegation and Pass-on”, International Journal of Web Services Research, Jan-March 2010, pp. 1-21, Idea Group Publishing USA 2010

[27] Wembo Mao, “Modern Cryptography: Theory and Practice”, Pearson education, 2004