International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

Secure Communication Algorithm in Web-Services

Mamidala Naveen Kumar[1], Shaik Khaja Hafeezuddin[2], G Kumari[3]

[1]Assistant Professor, TKRCET

[2]Assistant Professor, TKRCET, Consultant Web Developer, Pixel Designers

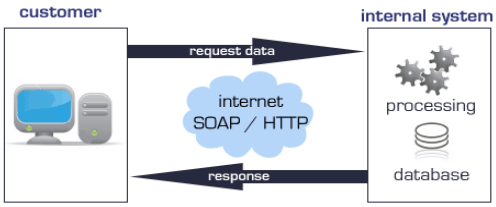
[3]Research Scholar, Department of CSE, Andhra University,

Abstract: ***A web service is a product framework that is intended to bolster machine to machine interoperable association of frameworks over a network. Web service give a structure to framework joining without relying upon programming dialect. It is currently widely deployed over a range of systems. The Web services have ended up more suitable now to integrate heterogeneous frameworks and are to a great extent encouraged through its broad utilization of the Extensible Markup Language (XML). Thus, the security of Web services is not limited to security of framework but also based on integrity of XML. Security of the web services is concentrated upon frameworks and as well as on the secrecy and respectability of the XML based SOAP messages that are utilized for correspondence. Now-days, Web services have created immense intrigues in sellers and specialists. A web service depends on existing Internet conventions and open guidelines, furthermore gives an adaptable answer for different issue of utilization reconciliation. This paper gives an outline of the web services, web administration security and the different calculations utilized for encryption of the SOAP messages.***

Keywords: HTTP, Web services, RSA Algorithm, Web service architecture & secure communication

1. Introduction

Web service[1] is basically a network accessible interface to various application functionalities build upon various emerging internet technologies[2] across the globe.



It can be stated that if an application is accessed by multiple client systems or machines over a geographical horizon over a network using standard protocols such as HTTP, XML, SMTP, or Jabber but not limited to, then it is a web service. A webs service can also be defined as an software system designated to support machine to machine interaction within & over a wide range of network. Web services provides a framework to integrate systems without directly depending upon programming or coding languages and operating systems thus making it flexible and enforceable over very large of systems which are using the above specified standard protocols.

A web service is an dialectical interface[3] that is positioned in between the application program and the user of that application .Web service acts as an intermediate abstraction layer, which separates the platform and the programming language specific details of how an application code is actually revoked by falling functions of the code, and this standardized layer shows that any programming language that supports the web service can also access the application's functionality. These days the basic web services that we see on the Internet are HTML sites. In these, the application services such as requesting data, processing and sending back the retrieved set of data to the user utilizes the protocols which follow strict standard data format, such as HTTP[4] and HTML which that are the instruments for distributed, overseeing, seeking, and recovering data substance. Customer applications (different web programs) that comprehend these measures can cooperate with the application administrations to perform different undertakings like requesting books, sending welcome cards, or perusing news and so forth. As this standard based interface gives reflection, it doesn't make a difference whether the applications and web service protocols are composed in Java and the program written in another dialect like C++, or the application services sent on a Unix box or some other framework while the program is conveyed on Windows. Web services additionally take into consideration cross stage interoperability[5] that makes the stage unimportant and is one of the key advantages picked up from executing web services. There is right now a progressing exertion inside of the Java group to characterize a precise construction modeling for executing web services inside of the structure of the Java 2 Enterprise Edition particular. Each of the significant Java innovation suppliers, for example, Sun, IBM, BEA, and so forth are all attempting to empower their stages for web service support and numerous critical application merchants, for example, IBM and Microsoft have totally grasped web services. Today IBM is coordinating web administrators to support all through their Web Sphere, Lotus, and DB2 items, and Microsoft's new .NET framework is built upon s web services that are an informing system. The necessity set on a web services is just that it must be equipped for sending and getting the messages utilizing some mix of different standard Internet conventions.

The Web services are in more utilization and are being suitable for coordinating over heterogeneous wide range of systems over a network and is encouraged through its broad utilization of the Extensible Markup Language (XML). The interface of a Web services is portrayed utilizing the XML

based Web Services Description Language (WSDL). The correspondence is performed utilizing XML based SOAP messages. Consequently, the security of a Web services construct framework depends with respect to the security of the administrations themselves and also on the classification and reliability of the XML based SOAP messages utilized for correspondence. The Organization for the Advancement of Structured Information Standards (OASIS) and the World Wide Web Consortium (W3C) has institutionalized a few determinations that are identified with security in Web administrations and XML.In this current decade Web services are rising as a precise and extensible system for application to application connection and are on top of existing Web conventions[6] and open XML principles. Web services are another class of Web applications and are independent, self-portraying, particular applications that can be distributed, found, and summoned over the Web.

If any particular web service is deployed once over the web, it can be discovered and invoked by the other applications or other Web services instantly by triggering the suitable functions. The advantage of using Web services is the ability to create applications through the use of loosely coupled and reusable software components, tools and protocols[7]; this has wide fundamental implications in technologies and business applications. The business services can be reorganized and distributed over the Internet and also can be accessed by a wide variety of communications devices using internet as a medium to access the remote resources. Businesses process applications and concentric Business application methodologies[8]can be released from the load of complex, low quality and costly software integration and focus instead on the value of their offerings. In this way, the Internet will become a universal and more generalized, flexible and highly customized platform where organizations and individuals converse with each other to carry out various commercial business activities to provide value added services to the clients sending requests. The fences to provide new offerings and entering new technological markets will be hand down to enable access for small and medium sized technical enterprises. Dynamic enterprises and dynamic chains might become reachable than now.

The Web services background is categorized into three spectral classes - communication protocols, service descriptions, and service discovery and specifications are being established for each. The following specifications are presently most stable in each of the above area:

1) The simple object access protocol (SOAP): This accessing protocol enables inter application process communications among the Web services over web. It is fundamentally a stateless protocol and a one way message exchange standard. The basic pattern is like request/response, request/multiple responses, etc.
2) The Web Services Description Language (WSDL): WSDL protocol provides a very formal and standard, computer-readable description of Web services. It provides a model and an XML data format for labeling Web services. WSDL defines services as groups of network endpoints or ports.
3) The Universal Description, Discovery and Integration (UDDI): UDDI protocol directory is a registry of Web services descriptions. It provides a methodology for clients to discover Web services and web applications.

2. Literature Survey

The amazon web services and Microsoft azure web services provided an overview of the various security processes and inter application communication they have used for providing security to web services.

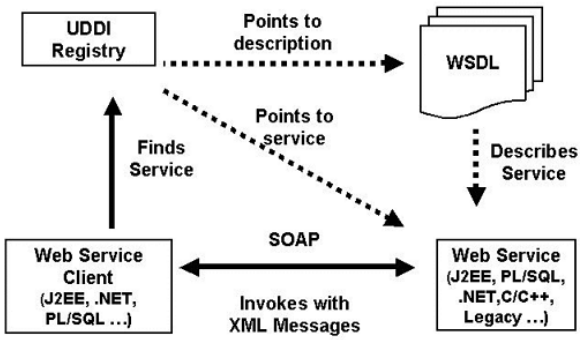
Joe M. Tekli, Ernesto Damiani, Richard Chbeir and Gabriele Gianini gave an brief overview of current research activities proceeding on SOAP processing performance enhancement that focused broadly on similarity based methodologies, as well as the web service Security optimization techniques, and XML parallel processing structural design protocols and frameworks. Most methods form on the observation that SOAP message exchange [9]usually includes highly identical messages.

[1]Nils Agne Nordbotten has provided an overview of latest security standards for XML and Web services. These standards provide a flexible framework for fulfilling the basic security requirements thus in turn enhancing confidentiality, integrity, and authentication, as well as more difficult requirements such as, authorization, and federated and unique identities. Various mechanisms such as those provided by Web Services Policy and the Web Services Description Language (WSDL) can handle the intruder's malicious messages or strings by utilizing the services of XML firewalls

[2]. Hongbing Wang,Joshua Zhexue Huang, Yuzhong Qu,Junyuan Xie have presented the basic idea on Web services and internet applications. They presented basicthree aspects of Web services they are the service composition, the service semantics and the service security.

3. Current System Overview

The Web Services building design is based upon the three parts that communicate with one another as service supplier, service registry and service requester. These cooperation's include distribute, discover and tie operations. These parts and operations together follow up on the Web Services antiquities that are the Web administration programming module and its portrayal. A web service provider has a system reachable programming module that is an execution of a particular Web service module. The web service provider depicts an administration portrayal for the Web services and distributes it to a service requester or service registry. The service requester makes utilization of the discover operation to recuperate[10] the depiction and uses the service portrayal to tie with the web service supplier and raise or cooperate with the Web service execution. Service supplier and service requester parts are the individual intelligent builds which interact with each other.



Roles in Architecture of Web services

1) **Web service provider:** Web service provider is a owner and host of a web service which is accessible over the web from the business and architectural point of view.
2) **Web service requestor:**From business and architectural point of view web service requestor is an entity waiting or requesting to initiate the communication channel to be established in order to invoke the web services and applications to cater various needs.
3) **Service Registry:** Services registry is a set of records where all the web service providers publish their services and their descriptions and are made available to service requestor.

4. Web services & Security

In web services background and domain, security means that the recipient of a message/string must be able to validate the reliability and authenticity of a message. Web Service Security[11] defines the tool to include confidentiality, integrity, & single message authentication structures within a SOAP message. Web Service Security uses a unique XML Signature and XML Encryption specifications to include digital signatures, message digests, and encrypted data in a SOAP messages. Web Service Security is apprehensive with security for SOAP messages, and hence web service security very clearly builds on uppermost layer of SOAP. Web service security also makes use of XML Signature and XML Encryption. The Web Services Security mainly aim to provide an overview for building secure web services using SOAP.Here XML Encryption is being used to provide confidentiality, while message integrity is provided through the use of XML Signature through which the SOAP message body elements, selected headers or any combination may be signed or encrypted using unlike signatures. The functionality providing web service security is needed if confidentiality and integrity are required for such messages. A major performance traffic exist in SOAP message processing and the reason for SOAP performance criticality is because of two reasons as: On one side, SOAP communication creates network traffic, and causes higher potential than the other competing existing technologies. On the other side, and more importantly and predominantly, the generation and parsing of SOAP messages and their conversion to and from in application data can be computationally very expensive and resource consuming. As XML encryption doesn't provides any sort of security in web services and hence a new algorithm can be used to provide security to web services over web during inter application communication. However, the recent Web services architectures are antagonized with a few problems like security and hundreds of algorithms are currently used for performing cryptographic operations with symmetric key based security symbols and operators. Widely XML encryption used is symmetric key encryption where the authenticity of message can't be assured i.e identity of the sender cannot be verified. In this case the public key encryption allows the use of RSA algorithm which enables the recipient of a message to verify that the message is really from a particular authentic source. The recipient may receive a string or message privately so that any unauthorized listeners could not read and decode. Current web services do not meet minimum security specifications to the ever emerging security threats and vulnerabilities. Web services involve exchange of messages means that securing the message transmission is an important issue to consider when building and using Web services over the web. In the other scenario, because Web services allows all the internal systems as well as external systems to communicate on HTTP ports, using various standard protocols these application servers are vulnerable and opened up to application level attacks. Very few standards have been introduced to improve the activity of transmitting message securely, including web service security and various other enterprises towards enabling digital signatures on XML messages and the transactions.

5. Security Algorithms

Web Service security is big challenge for specialists as it requires a solid security calculation for the encryption of information. The xml encryption plan is being utilized in no time for scrambling the messages between the distinctive programming dialects running on diverse stages, however this xml encryption calculation is symmetric key encryption calculation creates correspondence overhead, and subsequently there is a need for asymmetric key encryption algorithm.

The more powerful version of DES is used for high security purpose where the data is encrypted thrice. Initially data is encrypted with first key and again it is encrypted with second key. In the third phase of encryption using the first key the data is encrypted for third time thus achieving the highest security. With the current computational power and code breaking techniques it is impossible to break the encrypted data stream. AES is a more up to date encryption standard and is currently the favored one to use for XML Encryption. AES is a substitution direct change system having 10, 12, or 14 rounds, contingent upon the different key sizes which are at present set at 128, 192, or 256 bits. The square size utilized as a part of AES is 16 bytes and the information piece to be handled is partitioned into a variety of bytes adding to a framework with lines and sections. AES and DES are symmetric figure that implies that both sides must know a mutual key. The issue of dispersing the key is not little, and there exist surely understood calculations for doing this. RSA calculation is a lopsided key encryption calculation and is generally known for its security strengthening. RSA includes an open key and a private key. General key can be known by everybody and is utilized for encoding messages. Messages encoded with the general population key must be unscrambled in a sensible measure of time utilizing the private key. In any case, RSA key size

is 1024 and this expands the correspondence overhead. Henceforth it can be actualized agreeing to the need of messages by utilizing the different key sizes of RSA. Bring down the need of messages lower will be the key size, higher the need of messages higher will be the key size.

6. Proposed System

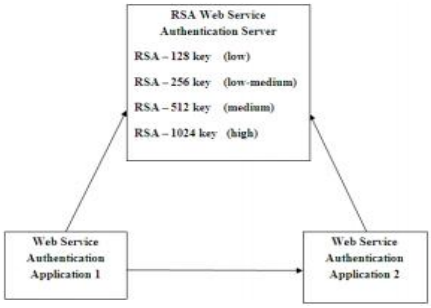


Figure 3: Proposed web service secure communication model

Since Web Service security is enormous test for specialists as it requires a solid security calculation for the encryption of information, the security calculations specified above can be utilized for key era and encryption of the messages. The RSA calculation is known for its security strengthening and subsequently it can be utilized for key era however as there are numerous difficulties in RSA usage for web benefits, the proposed framework will plan a security arrangement for RSA[12] execution as appeared in the figure 3. There are four sorts of keys that can be created with RSA calculation i.e. 128, 256, 512, 1024 piece key size. Key size will be picked relying on level of classification i.e. low, low-medium, medium and high. In the event that a message is not all that secret message then it will be encoded with 128 piece key. On the off chance that demand message is more private like checking equalization in bank then it will be scrambled with 256 or 512 piece key. In the event that demand message is most secret like moving cash in bank then it will be encoded with 1024 piece key. Separate outsider secure server will take care of for RSA key era. With this security approach correspondence overhead will diminish significantly. Though SHA-1 will be utilized for encryption and unscrambling of the messages as it gives more prominent imperviousness to the assaults.

7. Conclusion

In this paper we have introduced Web services, a rising innovation for the Web, The web administration review and the different security issues happened in the usage of the xml encryption of the messages. The security of web administrations is a vital angle and consequently a security calculation is required to execute in web administrations for key era and encryption decoding of the messages.The security calculation portrayed in this paper will be utilized together as a part of mix for key era and encryption unscrambling of the messages which will give solid security in web administrations.

References

[1] S. S. M. Chow, Y. J. He, L. C. K. Hui, and S.-M. Yiu, "SPICE - Simple Privacy-Preserving IdentityManagement for Cloud Environment," in Applied Cryptography and Network Security – ACNS 2012, ser. LNCS, vol. 7341. Springer, 2012, pp. 526–543

[2] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage," IEEE Trans.Computers, vol. 62, no. 2, pp. 362–375, 2013.

[3] B. Wang, S. S. M. Chow, M. Li, and H. Li, "Storing Shared Dataon the Cloud via Security-Mediator," in International Conference on Distributed Computing Systems - ICDCS 2013. IEEE, 2013.

[4] Cheng-Kang Chu, Sherman S.M. Chow, Wen-Guey Tzeng, Jianying Zhou, and Robert H. Deng,"KeyAggregate Cryptosystem for Scalable Data Sharing in Cloud Storage" IEEE Transactions On Parallel And Distributed System, Vol 25, No. 2 February 2014.

[5] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted data,"in Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS '06). ACM, 2006, pp. 89–98.

[6] Y. Sun and K. J. R. Liu, "Scalable Hierarchical Access Control in Secure Group Communications," in Proceedings of the 23th IEEE International Conference on Computer Communications (INFOCOM '04). IEEE, 2004.

[7] D. Boneh and M. K. Franklin, "Identity-Based Encryption from the Weil Pairing," in Proceedings of advances in cryptology – CRYPTO '01, ser.LNCS, vol.2139. Springer, 2001, pp. 213-229.

[8] M. Chase and S. S. M. Chow, "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption," in CM Conference on Computer and Communications Security, 2009, pp. 121–130.

[9] D. Kornack and P. Rakic, "Cell Proliferation without Neurogenesis in Adult Primate Neocortex," Science, vol. 294, Dec. 2001, pp. 2127-2130, doi:10.1126/science.1065467.

[10] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records," in Proceedings of ACM Workshop on Cloud Computing Security (CCSW '09). ACM, 2009, pp. 103–114.

[11] F. Guo, Y. Mu, Z. Chen, and L. Xu, "Multi-Identity Single-Key Decryption without Random Oracles," in Proceedings of Information Security and Cryptology (Inscrypt '07), ser. LNCS, vol. 4990. Springer, 2007, pp. 384–398.

[12] W.-G. Tzeng, "A Time-Bound Cryptographic Key Assignment Scheme for Access Control in a Hierarchy," IEEE Transactions on Knowledge and Data Engineering (TKDE), vol. 14, no. 1, pp. 182–188,2002site)

Authors Profile

Mamidala Naveen Kumar, working as an Assistant Professor at TKRCET. He has 9 Years of extensive teaching experience in various domains such as Data mining, machine learning and Big Data analytics including various cloud models.

Shaik Khaja Hafeezuddin, working as an Assistant Professor at TKRCET. He is a consultant web developer at 9Tree and Pixel Designers. He has real time experience on various cloud platforms such as Microsoft Azure. Worked on various projects in the domain of web development.

G Kumari, working as a research scholar at department of computer science in Andhra University. She has 9 Years of teaching experience in various areas such as Big Data mining, Artificial Intelligence and Data Analytics including using various cloud technologies such as Microsoft Azure, AWS, Heroku.