IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 26, Issue 2, Ser. 4 (Mar. – Apr. 2024), PP 15-20
www.iosrjournals.org

Study Web Service Security And Implement It To Transmit And Receive Environmental Monitoring Data

Dung Vuong Quoc*, Loi Nguyen Tien, Nguyet Do Thi Minh, Thuy Tran Thi, Minh Nguyen Quang, Binh Nguyen Thi Thanh
Center Of Information Technology, Hanoi University Of Industry, Number 298, Cau Dien Street, Bac Tu Liem Distric, Ha Noi, Vietnam

Abstract:
This paper introduces an architecture and methodology for enhancing web service security. We utilize digital signatures and encryption to safeguard SOAP XML messages. Our approach is applied to the transmission and reception of environmental monitoring data between monitoring stations and the resources and environment department's server. By implementing this security protocol, our solution ensures data integrity and confidentiality. This stands in contrast to previous methods that transmit unencrypted and unsigned data, leaving it vulnerable to tampering by malicious actors during transmission.

Keywords: *Web service, digital signature, encrypt, environmental monitoring, SOAP XML.*

Date Of Submission: 11-04-2024 Date Of Acceptance: 21-04-2024

I. Introduction

The concept of web services emerged in the late 1990s and has since become the backbone of the IT industry. Nowadays, most business organizations rely on web services to achieve their goals. With the strong portability and customization offered by Extensible Markup Language (XML), it has become the language of choice for many web services [1, 2]. According to [3], XML web services are a successful model for many complex web applications. The interface of a web service is described using XML and is termed Web Services Description Language (WSDL). Information exchange with web services occurs through XML SOAP (Simple Object Access Protocol) messages. Therefore, web service security focuses on ensuring the integrity and confidentiality of XML SOAP messages. The World Wide Web Consortium (W3C) and the Organization for the Advancement of Structured Information Standards (OASIS) have proposed numerous standards for web service security. In [2] and [4], an overview is provided on improving the performance of SOAP message processing, optimizing web service security, and parallel processing of XML documents. The study [5] offers an overview of recent security standards for XML and web services. These standards lay the groundwork for meeting basic security requirements such as encryption, authentication, and data integrity, as well as more advanced requirements like authorization and identity federation.

In Vietnam, as per the Ministry of Natural Resources and Environment regulations, industrial parks discharging waste exceeding 1,000 m3 per day and night must install automatic monitoring stations for water indicators. Additionally, steel and cement factories are mandated to install automatic monitoring stations for emissions indicators and transmit the collected data to the respective servers of the natural resources and environment departments. To ensure accuracy, the Ministry stipulates the use of dataloggers to transmit sensor output data securely to these departments. Presently, dataloggers in our country primarily employ TCP/IP, UDP/IP, or FTP protocols for transmitting raw data, which lacks encryption and authentication, posing a security risk. This vulnerability allows hackers to intercept and modify packet contents, resulting in erroneous data transmission. In this article, we propose the adoption of web services coupled with web service security policies and SOAP XML for the secure transmission and reception of data between monitoring stations and the Department of Natural Resources and Environment servers, ensuring both precision and safety. Our proposed solution has already been successfully implemented at the Department of Natural Resources and Environment in Hai Duong province.

II. Methodology

Webservice
Introduction

According to the World Wide Web Consortium (W3C), a Web Service is a software system intended to facilitate interoperability between applications on different computers via the Internet, utilizing common

interfaces and communication protocols. Its structure and connection are delineated in XML. The architecture of the web service is depicted in Figure 1.

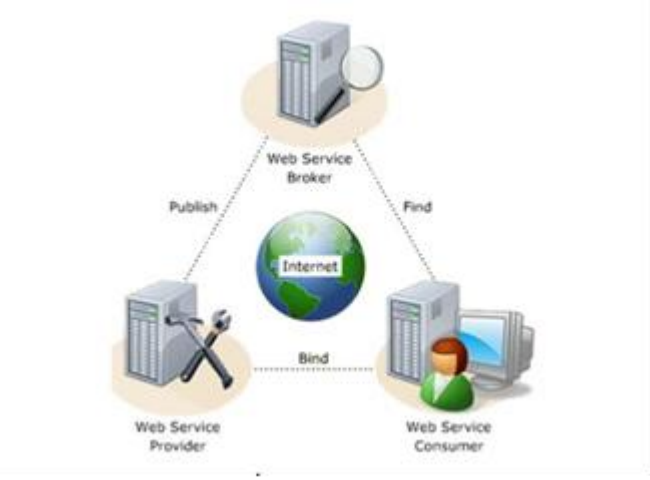

Figure 1. Architecture of web service [6]

Based on the model outlined above, web services are comprised of three main components: the Web Service Provider, the Web Service Consumer, and the Web Service Broker. The provider is responsible for creating web services and offering them to customer applications seeking to utilize their functionality. Clients, on the other hand, are applications seeking to utilize the services provided by web services. Meanwhile, the web service broker serves as an intermediary application, facilitating the discovery of registered web services by client applications. These three components interact with each other through the following mechanisms:

- Publish (release): The web service provider utilizes the program interface of the broker component to register information about its web service, including its address and available functions. This registration process enables customer applications to discover and effectively utilize the functionality provided by the web service.
- Find (search): Customer applications rely on the information of web services registered with the broker to locate the desired web service.
- Bind (invoke): To utilize the service, invocation is necessary. During this operation, the customer application, while executing, initiates an interaction with the service based on the information obtained from the service description. This information typically includes the service location, connection instructions, contact details, and interaction methods.

SOAP (Simple Object Access Protocol)

SOAP is a crucial protocol in Web services, constructed on XML. It serves as a communication protocol or format for transmitting messages, enabling applications to exchange information via HTTP. The structure of a SOAP message is depicted in Figure 2 [7]

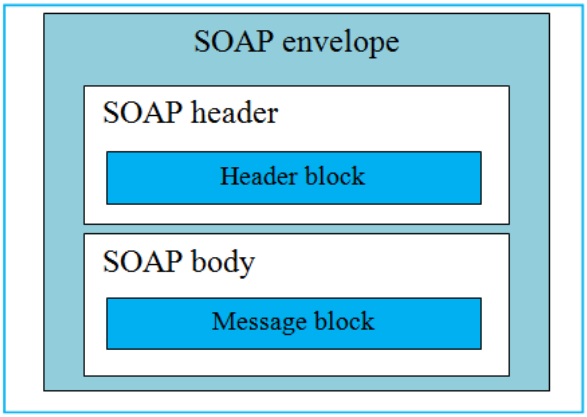

Figure 2. *Structure of SOAP messages*

WSDL (Web services description language)

A web service becomes inaccessible if it cannot be located. When a client program intends to invoke a web service, it must ascertain the location where the service is hosted. Additionally, the client program needs to understand the functionality of the web service to ensure accurate invocation. This task is facilitated by WSDL (Web Service Description Language), which is built on XML. WSDL provides crucial information to the client application, detailing the functionality of the web service and its location. Consequently, customer application programs can utilize the WSDL document to determine both the whereabouts and the method of employing the web service [8].

Universal Description, Discovery and Integration (UDDI)

UDDI, an XML-based standard, defines various elements enabling customer applications to retrieve requested information when consuming web services [9-15]. A UDDI comprises two primary components [16]:

- Registration of all Web Service metadata, including references to the WSDL document describing the service.
- The WSDL Port Type setting section, which delineates operations and facilitates searches for registration information.

Proposed model

Model

The proposed model for the data transmission and reception system between the data logger and the Department of Natural Resources and Environment server is depicted in Figure 3. The data logger will transmit notifications containing information about the environmental monitoring parameters of the station to the server of the Department of Natural Resources and Environment. On the server side, the integrity and structure of the transmitted data are checked. If the data passes the verification process, it is saved in the database. Additionally, the server will send a response back to the data logger indicating whether the data reception was successful or failed.

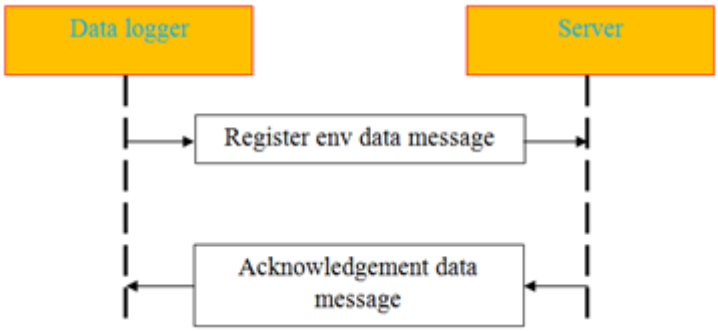

Figure 3. *Data transmission and reception model*

Structure of sent and response data

All sending and response data uses SOAP and is structured as shown in Figure 4.

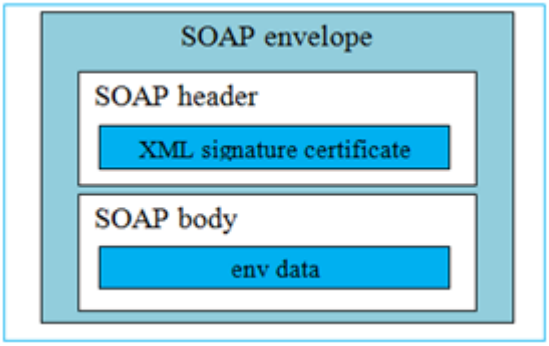

Figure 4. *General structure of sent and response data*

The XML format of the request message sent from the datalogger to the server of the Department of Natural Resources and Environment is as follows:

<report:env>

<env:Data attributes…/>

<env:Control>
values…
</env:Control>
</report:env>

Table 1. Describe in detail the attributes and values in the XML data structure

Data region	Item	Description	XML tag
Data	1	Station code	code
	2	Station name	name
	3	Monitoring time	date_time
	4	ph value	ph
	5	Cod value	Cod
	6	Tss value	Tss
	7	Color value	Color
	8	Temperature	Temp
	9	Flow value	Flow
	10	Total nitrogen	Nito
	11	Bod	Bod
Control	12	Station signature code	Ssic
	13	Station security code	ssec

where:
- Station code (code) consists of 3 digits from 001 - 999
- Station name has a maximum length of 100 characters including letters, numbers and spaces
- The monitoring time is in the format dd-mm-yyyyThh:mm:ss with dd being the 2-digit day, mm being the 2-digit month, yyyy being the 4-digit year, hh being the 2-digit hour, mm being the 2-digit minute digits, ss is a 2-digit second.
- Monitoring indicators are decimal numbers with 2 digits after the comma.
- The station's electronic signature is performed through the following steps:

Step 1: Select some information in the data section to be the signed data as follows: code| date_time|ph|cod|tss. In which the symbol '|' is used to separate data elements with ASCII code 124.
Step 2: The data selected in Step 1 will be digitally signed using the SHA256withRAS algorithm with the key and certificate used to sign all sent data.
Step 3: After being signed, the data will be encrypted using the Base64 algorithm.
- The station's security code is determined as follows:

Step 1: The data obtained in step 2 above will proceed to the next steps
Step 2: Use the SHA1 algorithm to create a message digest.
Step 3: The data obtained in Step 2 will be encrypted using the base16 algorithm.
Step 4: Insert the sign '–' with ASCII code 45 between positions 8 and 9; 16 and 17; 24 and 25; and 32 and 33.

The following example illustrates the structure of the sending data:

<env:Report>
<env:Data code="100" name="Tan truong"
date_time="10-11-2016T22:05:00" ph="7.00"
cod="34.27" tss="12.35" color="12.74"
temp="20.12" flow="40.79" nito="0.00"
bod="0.00" />
<env:Control>
<env:ssic digest="SHA256" cipher="RSA2048" encoding="base64">
Ca8sTbURReQjjgcy/znXBKjPOnZof3AxWK5WySpyMrUXF0o7cz1BP6adQzktODKh2d8s
oAhn1R/S07lVDTa/6r9xTuI3NBH/+7YfYz/t92eb5Y6aNvLm6tXfOdE3C94EQmT0SEEz
9rInGXXP1whIKYX7K0HgVrxjdxCFkZF8Lt12XbahhAzJ47LcPxuBZZp6U6wJ2sWI5os3
KY9u/ZChzAUaCec7H56QwkMnu3U3Ftwi/YrxSzQZTmPTpFYKXnYanrFaLDJm+1/yg+VQ
ntoByBM+HeDXigBK+SHaxx+Nd0sSmm1Im4v685BRVdUId+4CobcnSQ3CBsjAhqmIrtWT
GQ==
</env:ssic>
<env:ssec digest="SHA1" encoding="base16">
03ec1d0e-6d9f77fb-1d798ccb-f4739666-a4069bc3 </env:ssec>
</env:Control>
</env:Report>

III. Results

We have applied the data transmission and reception model as proposed above to transmit data from wastewater and emissions monitoring stations at industrial parks and factories in Hai Duong province. On the server of the Department of Natural Resources and Environment of Hai Duong province, we built a web service that receives and checks the authenticity and integrity of data sent from monitoring stations. If the data is accurate, it will be recorded in the database to facilitate future querying and display. The datalogger side will structure the sent data according to the required format and then use the web service from the server side to transmit the data. Figures 5 and 6 below illustrate the results we receive from wastewater and emissions monitoring stations of factories and industrial parks.

Figure 5. *Illustration of data transmission and reception results from automatic wastewater monitoring stations*

Figure 6. *Illustration of data transmission and reception results from automatic emissions monitoring stations*

IV. Conclusions

In this article, we have proposed a model for transmitting and receiving data from automatic environmental monitoring stations to the servers of provincial departments of natural resources and environment using secure web services. Our proposed model is simple and easy to process data on the server without needing to install any other software. In addition, our proposed model is also more secure than current data transmission models because data transmitted on the network according to our proposed model is encrypted and authenticated while another current model data transmission is raw (text files or text messages), so it is easy for hackers to capture and change the content of packets, leading to the received data being wrong compared to the original data. The data transmission and reception model we proposed has been successfully applied to transmit and receive data from wastewater and emissions environmental monitoring stations in industrial parks and factories in Hai Duong province. Positive. The data we transmit and receive is the same as the monitoring data at the factory. However, the RSA 2048 encryption method we use will be quickly decrypted when quantum computers become available. Therefore, shortly we will research other stronger encryption methods such as quantum encryption to encrypt and authenticate information.

References

[1] Amazon Web Services: Overview Of Security Processes, June 2013.
[2] Joe M. Tekli, Ernesto Damiani, Richard Chbeir And Gabriele Gianini, "Soap Processing Performance And Enhancement" Ieee Transactions On Services Computing, Vol. 5, No. 3, July-September 2012.
[3] Nils Agne Nordbotten, "Xml And Web Services Security Standards", Ieee Communications Surveys & Tutorials, Vol. 11, No. 3, Third Quarter 2009.
[4] Hongbing Wang, Joshua Zhexue Huang, Yuzhong Qu, Junyuan Xie, "Web Services: Problems And Future Directions", 2005.
[5] Doug Tidwell, James Snell, Pavel Kulchenko "Programming Web Services With Soap", First Edition, December 2001.
[6] Heather Kreger, "Web Services Conceptual Architecture" Ibm Software Group, 2001.
[7] Locktyukhin, Max; Farrel, Kathy (2010-03-31), "Improving The Performance Of The Secure Hash Algorithm (Sha-1)", Intel Software Knowledge Base (Intel), Retrieved 2010-04-02
[8] Http://Aws.Amazon.Com/Security.
[9] Xml Digital Signature – Recommendation, Http://Www.W3.Org/Tr/2002/Recxmldsig-Core-20020212/
[10] Xml Digital Signature, Http://Www.W3.Org/Tr/Xmldsig-Core/
[11] Xml Encryption Requirement, Http://Www.W3.Org/Tr/Xml-Encryption-Req
[12] Xml Encryption, Http://En.Wikipedia.Org/Wiki/Xml_Encryption
[13] Xml Encryption, Http://Www.W3.Org/Tr/Xmlenc-Core/
[14] Xml For Dummies. Wiley Publications. 4th Edition
[15] Xml Signature, Http://En.Wikipedia.Org/Wiki/Xml_Signature
[16] Ibm Corporation And Microsoft Corporation. (2002) 'Security In Web Service World: A Proposed Architecture And Roadmap', A Joint White Paper, Http://Schemas.Xmlsoap.Org/Specs/Ws-Security/Wssecurity-Roadmap.Htm.