



PDF Download
2832987.2833072.pdf
27 February 2026
Total Citations: 1
Total Downloads: 163

Latest updates: <https://dl.acm.org/doi/10.1145/2832987.2833072>

RESEARCH-ARTICLE

QoS web service Security Access Control case study using HTTP Secured Socket Layer Approach

M. SWAMI DAS, Malla Reddy Engineering College, Secunderabad, Medchal, TG, India

A. GOVARDHAN, Jawaharlal Nehru Technological University Hyderabad, Hyderabad, TG, India

D. VIJAYA LAKSHMI, Mahatma Gandhi Institute of Technology, Hyderabad, Hyderabad, TG, India

Open Access Support provided by:

Malla Reddy Engineering College, Secunderabad

Mahatma Gandhi Institute of Technology, Hyderabad

Jawaharlal Nehru Technological University Hyderabad

Published: 24 September 2015

Citation in BibTeX format

ICEMIS '15: The International
Conference on Engineering & MIS
2015

September 24 - 26, 2015
Istanbul, Turkey

QoS web service Security Access Control case study using HTTP Secured Socket Layer Approach

M.Swami Das
Faculty of CSE, MREC
Hyderabad,India, 500 100
msdas.520@gmail.com

A.Govardhan
Professor,SIT,JNTU Hyderabad
India, 500 085
govardhan_cse@yahoo.co.in

D.Vijaya lakshmi
Professor,Dept. of CSE
MGIT,Hyderabad
vijayadoddapaneni@yahoo.com

Abstract

Web services are expected to play significant role in message communications over internet applications. Most of the future work is web security. Online shopping and web services are increasing at rapid rate. In this paper, we have presented the fundamental concepts related to web security threats, web server architectures, and web server protocols. QoS web service security is important concern in network communications and firewalls security. we have discussed various issues and challenges of web security including the fundamental concepts of network security encryption, decryption processes and network security hierarchies. In this paper, we also address various issues related to secure communications, and handshake protocol using lossless compression technique to improve the speed of web services. As a case study, it is also about implementing message authentication code using using HTTP secured socket layer approach.

Categories and Subject Descriptors

C.2 [Computer-communication networks]: Security and protection, Data communication, OSI reference model, and firewalls.

General Terms

Web services, Security, Quality of web services, and Access control.

Keywords

Web Security, QoS web service, HTTP, Secure Socket Layer, Network Security, Network operations.

1 Introduction

Web services are loosely coupled, language neutral, platform independent, communication and coordination of messages passing between client and server processes. Web services are the functionalities offered by service providers to

end users. Web services are accessible using interfaces, applications over the web. Web services are self-contained, modular business applications that have internet oriented standard interfaces [1]. Web security is required for the organizations to communicate with the customers without any risk of data or information over transactions/web operations. The biggest on-line retailer is Amazon at USA with 44 million users using applications, and web services [5]. Recently attackers used man in the middle attack by changing DNS settings and redirecting information to other servers that affected 300,000 devices in countries like India, Italy and Thailand[4].

Cryptographic researchers proposed digital signatures procedures to protect digital data. Ron Riverst, Adi Shamir and L.Adleman created the first cryptographic algorithm named RSA cryptographic algorithm. The first digital web based certificate was introduced by International Telecommunication Unions Telecommunication standards in 1998, later secure socket layer technology was developed in 1990, and successor Transport layer security in 1999 [26].

It is essential and more significant to provide web security for financial web sites. Web services most widely in Government, Businesses and Individuals with use of internet, and some of the key terms used in web security/network security are: integrity, confidentiality, denial of service, and authentication integrity defined by the property that data has not been modified by non permitted users. Confidentiality means information not available to unauthorized users. Denial of service is a malicious attempt to make server or network not available to the user. Attack occurs when multiple systems flood the bandwidth or resources of under attack system, usually one or more web servers[14]. Authentication makes sure that a message is coming from true source[3]. Three major roles of web server architecture as Service provider that makes service available over Internet, Service requester is the end user requesting services over the Internet; Service registry is the logical centralized directory of services. This is used to provide/publish the services

1.1 Web service security by XML and SOAP

Web services security is provided by XML and SOAP specification. Three specific issues with the web services are Confidentiality, authentication and Network security

1.1.1 Confidentiality

Confidentiality is to make sure that private or confidential information is not accessible to unauthorized individuals.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from Permissions@acm.org.

ICEMIS '15, September 24-26, 2015, Istanbul, Turkey
©2015 ACM. ISBN 978-1-4503-3418-1/15/09...\$15.00
DOI: <http://dx.doi.org/10.1145/2832987.2833072>

1.1.2 Authentication

Authentication is a process of assurance that the communication is between true source and intended destination

1.1.3 Network security

Network security is the process of using cryptographic techniques in network protocols and network applications during data communications over web services[3].

1.2 Web service security protocol stacks

Web service protocol stack used for web security it has four major layers such as service transport, XML messaging, Service description and service discovery.

1.2.1 Service transport

Transport layer security (TLS) can make offered point to point security, but not end to end. It is required TLS ensures message reliability and confidentiality. This layer includes Hyper Text Transfer Protocol (HTTP), Simple Mail Transfer Protocol (SMTP), File Transfer Protocol (FTP), and Blocks Extensible Exchange Protocol.

1.2.2 XML Messaging

This layer responsible for encoding messages in a common XML format. Messages can be understood at either end. For example XML RPC, and SOAP.

1.2.3 Service description

This layer is responsible for relating the public interface to a specific web service. Service handled by Web service Description Language (WSDL)

1.2.4 Service Discovery

This layer is responsible for centralizing the services into a common registry and providing functionality. For example UDDI [2]. The rest of this paper is organized as follows Section 2: Related work, Section: 3 Issues and challenges, Section 4: Web security and Network security, Section: 5 Discussions and Interpretations and Section 6. Conclusion.

2 RELATED WORK

Yang Kuihe etl, Proposed a VPN based SSL to provide data security in tunnel when data transferred between client and server. Intelligent IC card is used to authenticate identity, and cipher text is used to interpret the data. Introducing SSL proxy server behind the enterprise firewall. Internet security using SSN VPN system is discussed. Introducing SSL proxy server behind the enterprise firewall, provides Internet security over communication using SSL VPN system architecture technique[25].

The SOAP messages ensure integrity and authentication during the data transmission. Web services require partial signing of SOAP request which is achieved using XML signature by WSDL documents and operations as suggested by Padmanabhuni and Adarkar etl[9,12]. Web service security is critical task for message invocations by web servers. SOAP uses XML encryption, XML digital signature, and SSL/TLS methods.

Web service standards SOAP level security authentication and authorization management. Web security is defined as attach signature and encryption header to SOAP messages. it describes security tokens. Web security policy is defined as set of specifications that describe rules, constraints and other business policies on intermediaries and end points. (Example. Encryption algorithms). Web security trust describes a

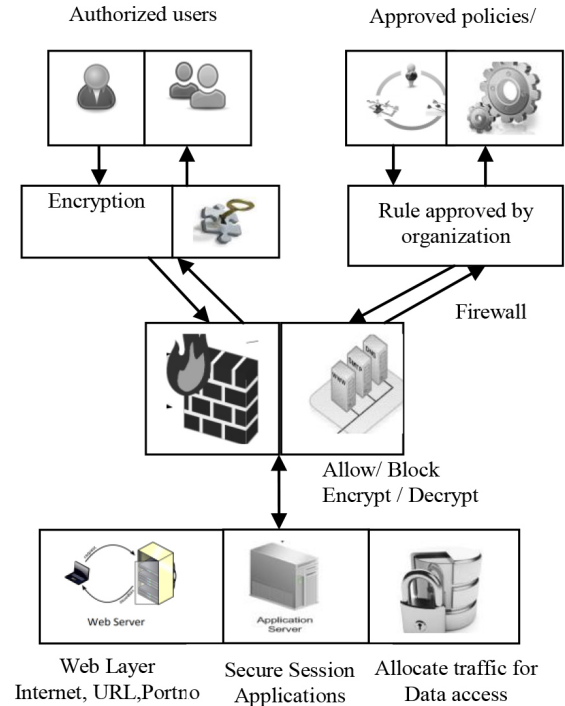


Figure 1. Firewall Architecture

frame work to design a model that enables web services to securely inter-operate request, issues, and exchange security operations.

Web security Privacy: A model web service and requesters state privacy preferences and organizational privacy instructions[9]. Web service securities by standards are firewalls, XML networks, EAR application Server technologies. Firewall is a network security system that monitors and controls the incoming and outgoing network traffic based on rule set/ policies. A firewall establishes a bridge between a trusted, secured internal network to other network[11]. Firewall architecture is shown in Figure.1.

2.1 XML Firewall

Web services environment, malicious attacks and DoS attacks are new challenges. Firewall allows Service providers residing in a network to be invoked from outside the network, keeping a high security[9]. HTTP protocol is not suitable for creating public key infrastructure. The prototype is used by application behind a firewall[10].

2.2 XML networks

Web service management vendors develop network based solution for web service applications that use peer to peer networks. (Blue Titan Network, Flamenco Network) provide better QoS web services by providing security to various networks endpoints service consumers and service providers. Extension of EAI and application Server Technologies: Enterprise application integration (EAI) product is enabling web based security (like SSL) security infrastructure by Vendors like Cisco, Dlink and others enterprise management vendors are meant for providing Web service standard

solutions to protect enterprise, financial, banking applications[10].

Fang Qi .etl, proposed Automatic Detecting Security Indicator (ADSI) for preventing Web spoofing on a confidential computer which is a harmless environment. if web browser is not trusted, attackers manipulate or steal user passwords, attack on web contents. web content to web server is authenticated with SSL protection. ADSI creates random indicator which is used to identify authenticated web page and detect bogus pages, with URL, screening data[23].

Fengying Wang, etl proposed web based information system that provides user identity and authentication. Web based system by digital certificate information service CA (center agent).After the authentication file is checked and considered correct, CA will send a user Digital certificate by using the RA (register agent). This certificate contains users personal information , public key information and Signature from CA. User needs to encrypt the certificate using the secret key and then send it to administrator,who uses users public key to decrypt and checks the identity. Web browsers and web services provide users authentication and encrypted channelSSL . SSL encryption technology and data package is supposed to achieve high secret communication[18].

Jin-Ha Kim.,etl proposed (Round Robin, ssl with session and ssl with buffering (backend forward) to analyze the performance of SSL enabled application servers. A back end forwarding scheme for getting better server performance through load balancing using ssl with buffer scheme in user level communication, and minimizing intra-cluster communication overhead [19].

Jingli Zhou., etl proposed an Asymmetric SSL tunnel solution which improves VPN throughput. SSL tunnel is the overlay networking technique for creating a SSL VPN on top of Internet (or IP based network). Before passing SSL tunnel, IP packet is compressed and decrypted in advance using SSL/TLS protocol[20].

Seyed Hasan M., etl proposed Fuzzy Secure Socket layer (FSSL). This protocol is the combination of fuzzy controller and SSL protocol. Functionality is allotted to transport layer like TCP with FSSL protocol. This improves performance in SSL blocks in Cipher Block Chaining mode(CBC) after the MAC is generated. The data is fixed blocks of always eight bytes length. This will lead to vulnerability of cipher text length within easily discloses the length of plaintext. The cipher text is converted to Fuzzy by Fuzzy controller and cipher text length cannot disclose the length of fuzzy data[21].

Lin-Shung Huang., etc introduced a new method for detecting SSL man -in- the middle attacks against website users, feasibility detecting man-in-the middle attack mechanisms over of SSL connections at the top web sites by checking certificates as number of CA certificates. Trace of pervasive malware in the wild that intercepted SSL connections. Multiple available defenses for better protection [22].

S. Bregni, etl. proposed the Secure Socket Layer (SSL) protocol which provides applications by introducing SSL accelerating cards in network nodes security, confidentiality, message integrity and end to end SSL Security, performance improved by minimizing the total cost, end to end delay for completion of distribution[24]. Stefano Bregni.,etl proposed

a solution for SSL to minimize the cost by tabu search approach, which improves the confidentiality, method integration and Authentication [15].

3 ISSUES AND CHALLENGES

The following are the list of issues /challenges in Web security/network security. Digital certificates are designed to establish credentials of the people doing business or communicating in the web described in Table.1.

Table 1. Issues related to web security

Safety check or vulnerable attacks	Solution
Created fake certificates on trusted companies	Digital certificates authenticated by online checking
Installing Plug-in players Free softwares protected antivirus	Use firewall and Authorized or licensed antivirus software
Various attacks due to entrusted system	Provide security by authentication
Cryptographic methods not available in old browsers	Use new Browsers use SSL security protocols Monitor web site history

Web security developers provide secured connections with server digital certificates, that are useful for on-line transaction to identify the trusted systems.[26] Mal-ware, Denial of service attacks to modem routers against other systems by unknown users by stealing personal information and credentials to access certain web sites. Hackers used stolen laptops/equipment to hack web data where there is vulnerability like private wireless network or wireless network unsecured with no password is immediately accessible to hackers. Hacker used wireless antenna and software, nearby buildings and capture/ steal information like passwords, email-messages, and any data transmitted over the network when a network is not secured.[5]. Brute-force attack is the password cracking method, trying all the solutions seeking one that fits[11].Stealing the login password controlling the devices by malicious scripts and malicious DNS servers, attacked on DSL modems.

Manufactures of Modems/Routers are supposed (like D-Link, Cisco etc) to give a better solution to protect the information for Small offices, homes that use broadband connection devices. If the security devices are not configured properly, the people who want to connect the network and use it, lead to all sorts of issues such as attackers planting malicious DNS server in the device configuration in LAN, DHCP services.

Secure Session Layer: to request URL, XML format formatted router. This will extract the router hardware and firmware, and connect to portno, using SSL to request URL. Admin credentials are not checked by this script. Linsys

Table 2. Discussions and Interpretations of web security Hacker send phishing mails to web users

Web services	Solutions or
Problem in domain or threats	Safety precautions
Mail respond with Cyber attacks by phishing mails	Phishing and cyber Do not respond mails with personal data
Credentials stolen from email, accounts	Beware of web browsers environment network

router is aware of vulnerability of CGI script running on these routers [7].

In recent one used Wi-Fi network in traveling. Most virus to computers come from internet resources, internet access points, because wireless access point is least protected by encryption password. If virus are trying to propagate and looks access point, and strongly protected Wi-Fi point on locations as shops, airports. When router is effected malicious virus. Router firmware easily decodes the root password with target sites various domains targeted like face book, Ask, Bing,Google, LinkedIn,Slide Share. Solution is to disable SNMP, ASAP [7].

Routers are poorly protected by default password (Admin). If DNS is to be found malicious wires then that leads to change the DNS settings and cyber hackers steal credentials of personal data like credit card details. When web server applications run with brute force attack HTTP request to malicious DNS server IP address, except navigation temporary files, no files are created in virtual machines, no persistent techniques can be found. Modified DNS settings clone trusted websites. Network router is exposed to attack through mobile phones. Hackers try to send junk mails to the user to give feedback, when the user is trying to send the details of personal information/credentials. The hackers steal the user credentials. Example. Online banking services. The hackers send the junk mails asking the user to send personal details like credit card account no, cvv, pin etc..

4 WEB SECURITY NETWORK SECURITY

Web Service Security: Three types of digital certificate are domain validated certificate, organizational validation certificate and Extended validation certification.

Domain validated Certificate: trusted domain name of owner. Organizational Validation Certificate: validation of organization by DNS names. Extended validation certification: Certificate Agent must meet minimum validation criteria. Organizations, application vendors, Browser makers issue extended validation certificate[26]. Web services standards worked at w3C, OASIS, IETF and other bodies to enable faster inventions of web services and security. A web service provides a flexible set of mechanism to design a range of security protocols. It is essential to design a non-vulnerable protocols for web services security. Web services specifications goals are to provide multiple security token formats, multiple trust domains, multiple signature formats, multiple encryption methodologies, and end to end message

Table 3. Web service problems with Various attacks

Web services Problem or threats	Solutions or Safety precautions
Denial of service attack inserting body of the table Cyber attacks by	Use firewall and secured network Do not respond
domain vulnerability and weak security web sites	Provide security by Firewall and Authentication
NTP server Vulnerabilities if visited web site is malicious web site	Beware of web browsers environment network Use anti virus software with firewall
Due to cloud client leaks the sensitive information	Use Authentication by Encryption process
Attackers execute arbitrary weak secret key due to vulnerability	Provide firewall and use strong security policies
Request invocations Content stealing by hackers	provide more security with Secured session layer OTP passwords

content security[12].

4.1 Network Security Encryption and Decryption process

Cryptography is a method of converting plain text into cipher text. Encryption and decryption process shown in Figure.2. Cryptography classified into three types: Secret Key cryptography, Public Key Cryptography and Hash functions

Secret Key cryptography (SKC): It uses a single key for both encryption and decryption

Public Key Cryptography (PKC): It uses one key for encryption and another key for decryption.

Hash Functions: It uses a mathematical transformation function to encrypt the message

Plain text: Actual information is send to web server by files, mail, images, web data processing(i.e. sequence of character etc.).Example. Plain Text= X

EncryptionDecryption key: The number of bits used for encryption or decryption process. Depending on the application the Key is represented by Secret key, public key and Hash functions. For example in Banking transactions user authentication and by using this decryption key confirmed application authorized cleint. Ex. Encryption Key= Decryption key= K

Cipher text: The decoded information by encryption key. The information will be represented by encryption key. (This code is not understood by users) and this information will be transferred over the network to provide security 1 to

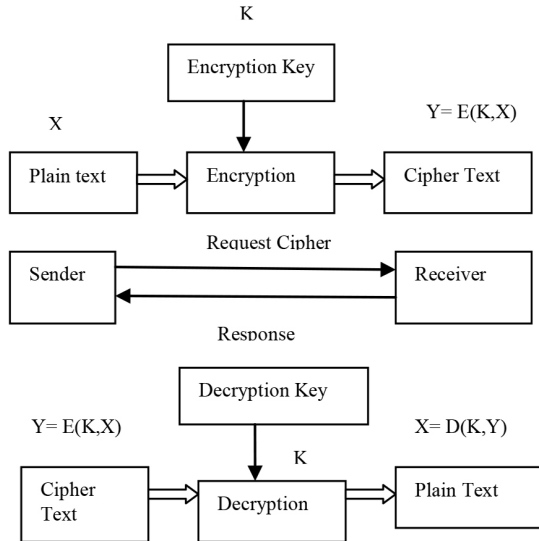


Figure 2. Encryption and decryption process in networked communication

the other end of web server/application server. Example. Cipher Text $Y = E(K, X)$

Sender: sender sends the information after encryption process that converts plain text into cipher text. This cipher text Sender will send cipher text $Y = E(K, X)$

Receiver: Receiver receives the cipher text (i.e. encoded information) and decrypts key the information that converts cipher text into plaintext. Example Plain Text $X = D(K, Y)$

4.2 ISO/OSI Reference model Fundamentals

ISO OSI (open system Interconnection) reference model. The reference model proposes the following layers (or abstractions) [27,28].

Physical Layer (Layer1): Transmits raw bits the physical link connecting to network nodes. Physical signal is transmitted over hardware. It deals with electrical, mechanical, frequency bandwidth etc. Example. Concerns with bit rate, point to point, multipoint, Network topology. Example Blue tooth.

Data link layer (Layer2): It recognizes the frame boundaries. It deals with framing, error control, and Flow control. Ex. Point to Point protocol.

Network layer (Layer3): Controls the operation on the subnet. Receives the frames from Data link layer and converts into packets. Example. Internet protocol, IPSec.

Transport Layer (Layer4): This Layer determines the type of service, transport connection, error free point to point channel the delivers the stream of bytes. It deals with reliability, flow controlling and multiplexing. Example TCP, UDP.

Session Layer (Layer 5): Allows establishing sessions between various services. Keeps track of token management and synchronization. Communication sessions, Request and response. Example. RPC.

Presentation layer (layer6): Concerned with syntax and

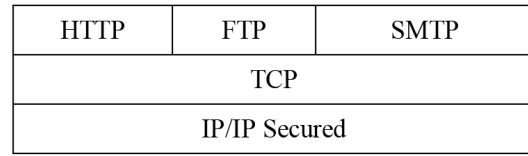


Figure 3. Network Level Security

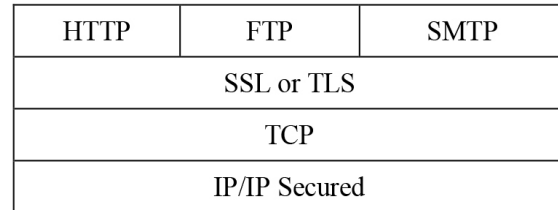


Figure 4. Transport Level Security

semantics of transmitted information. This gives data structures, delivery information to Application layer. ASCII code, Serializable, XML format, Data conversation, compression, Encryption and decryption are handled in this layer. Example. Telnet.

Application layer (Layer7): This layer is concerned with interface that is responsible for display information. Host communicate network interface responsible for display information. P2P, client server model. File transfer, Email, News, HTTP, and DNS.

4.3 Security in TCP/IP Protocol stack

Security provided in each layer of Network protocol hierarchies Network security provided in three levels as depicted in Figure.3., Figure.4 and Figure.5 We can extend the web security service by providing encryption that uses pre-images in poly to one trapdoor function methodology in web server. The disadvantage of earlier method is hard to invert decryption function in web server and not injunctive way of communication. The advantage proposed approach is easy to invert to recover for pre-images unique by injunctive trapdoor function, helps to ensure authentication. [29]

The standards for security in web services to be extended standard mechanism like encryption, digital signature, public key to handle XML and web services. W3C defines a set of services as software systems designed to support inter-operable system to system interactions over a network. W3C web services API implemented in web service and accessed over networks using internetwork.

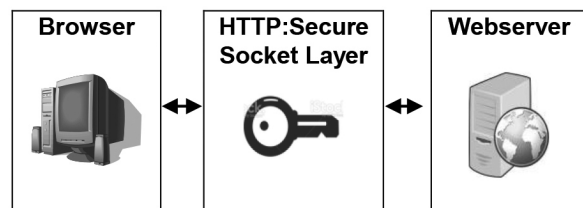


Figure 5. HTTP Secured Socket Layer Protocol

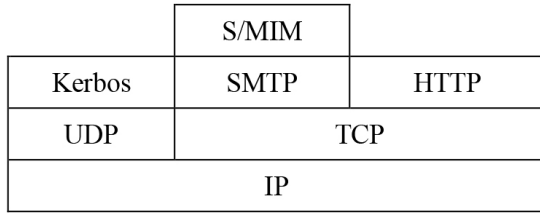


Figure 6. Transport Level Security

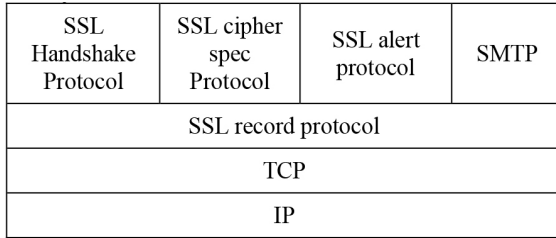


Figure 7. SSL Protocol stack

Web services are accessed by sending SOAP messages to endpoints. This is handled by transport layer security protocol such as HTTP, SSL, and TLS others. This ensures secured peer to peer messages. Web based security standards mapping to XML message security. All protocols are used to carry security data as part of XML document. The XML document is critical part of security requirement of web services.[9]

4.4 Secure Socket Layer and Transport Layer security

HTTP Secured Socket Layer Protocol: HTTP over Secured Socket Layer combination to secure communication between browser and web server systems is shown in Figure.6. SSL Secured Socket Layer Protocol is transient, peer to peer communication, SSL protocol stack described in Figure.7, link associated with SSL session Record Protocol operation is shown in figure 8. These SSL sessions are associations between client & server by handshake protocol, with defined set of cryptographic parameters that may be shared by multiple SSL connections[3,12,13]. HTTP protocol stack

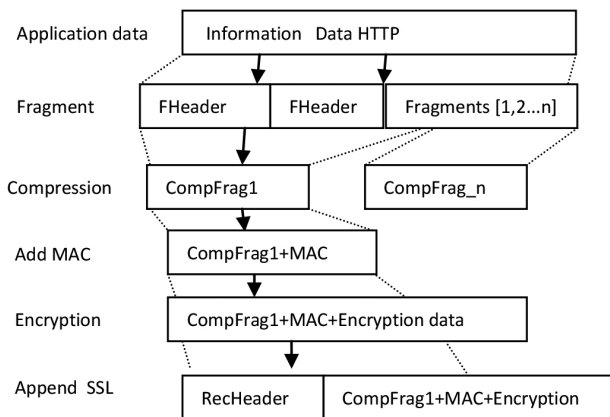


Figure 8. SSL Record Protocol Operation

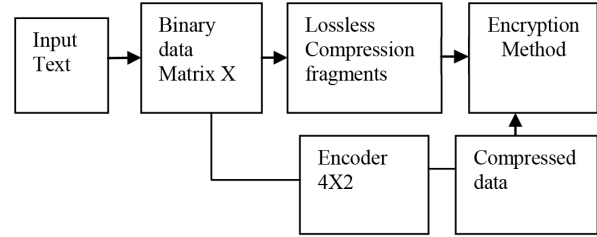


Figure 9. Lossless compression using ENCODER

provides transfer information for web services interaction which can operate on top of SSL. Three layers are defined as part of SSL such as Hand shake protocol, The change of cipher spec protocol and the Alert protocol. These protocols are used in management of SSL exchange.

4.4.1 HTTP SSL record protocol architecture

Two important concepts are SSL session, and SSL connection. Connection: SSL connection that provides protocol suite is similar to ISO/OSI reference model. SSL connection is on peer to peer network, and sessions are created by the Handshake protocol. Each session is identified by session state, session id, compression method and cipher spec. HTTP secured socket layer approach is described in algorithm.2. Established connection between end to end communication is described in Algorithm.3. Web security access control algorithm is described in Algorithm.4.

The secret key that used in MAC operation on data sent by client client_write_mac: The secret key is used in MAC operation on data sent by server and decrypted by the client client_write_key. As a case study example Message Authentication Code is implemented in Java program and testing results tomcat web server. The corresponding outputs are shown in Figure.10, Figure.11 and Figure.12. The conventional encryption key for data encryption is decrypted by the client and server. initiation_vector: Block cipher in CBC model is used and initialization vector is the first initiated by SSL hand shake protocol. seq_number: each party maintains separated sequence number for transmitted of number for transmitted and received message.

4.4.2 HTTP SSL Message

Message: Message is information as sequence of bytes. Fragments: each message is fragmented into blocks of fixed size. Compress: High level protocol is used for this segment. Compression is done by various techniques SSL-V3, TLS. Encryption algorithm: High security encryption algorithm is used. Proposed compression algorithm is described in Algorithm.1. Final step is SSL record protocol. Is a header consists of the following fields. Content type: The higher layer protocol 8 bits are used to process the enclosed fragmentation. Major Version: Indicates major version of SSL consist of 8 bits in use for SSL-v. value 3 Minor version: Minor version consists of 8 bits SSL-v3 value is 0. Compression length: 16 bits length of plain text fragment or compressed fragment if compression is used. This is maximum value. The content type is defined by Change cipher spec protocol, Alert protocol and Hand shake protocol.

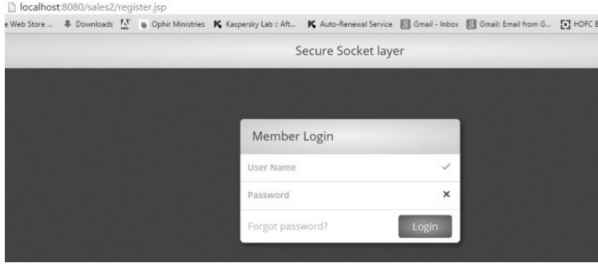


Figure 10. Client user name and password

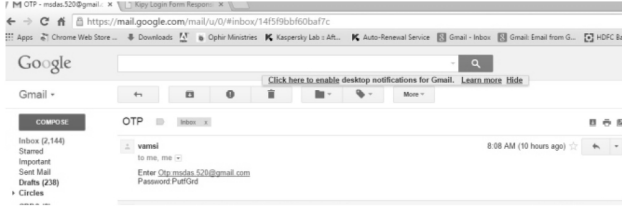


Figure 11. Server sends Random key to client

4.4.2.1 Change Cipherspec protocol

One of the SSL specification protocol that uses SSLrecord protocol. Message state with cipher suite to be used on each connection.

4.4.2.2 Alert protocol

This protocol is used for conveying SSL related alerts to peer entity. Application uses SSL to alert message is compressed and encrypted as specified with current state. Each message has two types of warning(1) or fatal_error(2) to convey security. Alert SSL specification has unexpected message in appropriate message received, bad_record_mac is incorrect MAC received, hand shake failure is security parameters unable to accept, illegal parameters are handshake message was out of range , notify, and certificate messages.

4.4.2.3 Handshake protocol

Most important part of SSL protocol is the hand shaking protocol. This allows the server and client to authenticate each other to negotiate an encryption and MAC algorithm. The cryptographic keys are to be used to protect data in an SSL record. The handshake protocol is invoked before any application data is transferred.

Phase 1: Establishes security, protocol versions, session_id, cipher_suite, compression_methods, initial random numbers. **Phase 2:** Server may send certificate key exchange and request certificate server signal of given message. **Phase 3:** Client sends certificate if requested client sends key exchanged. Client may send certificate verification. **Phase 4:** Change cipher suite and finish hand shake protocol [3].

4.4.3 Proposed Model

The problems with SSL in Handshake protocol Encryption and Decryption in Figure.2 are they have slow communication. And another issue is to Monitor every router with any malware/suspicious attacks. To give solution for these problems the proposed architecture as described in Figure. 9. As a case study Message Authentication code in Handshake protocol Phase 3.(key exchange) we implemented sample

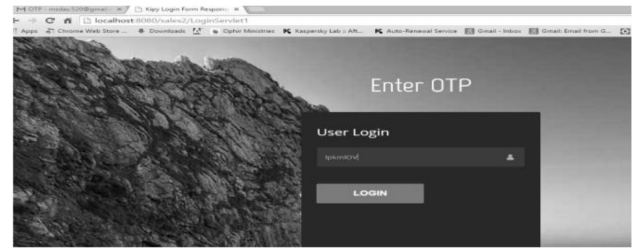


Figure 12. Client open the application using random key mailed to client

program in Java/J2EE language and executed tomcat web server, and results shown in Figure.10, Client gives user name and password, Server receives the client request and sends Random key to client mail id for validation authentication described in Figure.11, and finally client process to access web services by open secret key is shown in Figure.12

Algorithm 1 Compression algorithm

```

1: procedure ENCODING_DECODING
2:   begin
3:   Read Initialization variable Plaintext(binary)=X
4:   i, n, k, Xreduct(n,k), Xoriginal(n,m)
5:   Read plain text of binary data
6:   X= where X is a matrix hold binary data
7:   x =

$$\begin{pmatrix} a_{11} & a_{21} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{k1} & a_{k2} & \dots & a_{kn} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nm} \end{pmatrix}$$

8:   Divide binary data 8 fragments with each fragment
9:   Apply reduction by Encoder 4 bits into 2bits
10:  output Xreduction(n,m)
11:  Apply Encryption algorithm
12:  Convert the information into cipher text
13:  This cipher text transmitted by using HTTP SSL
14:  Receiver receives the cipher text
15:  Use Decoder input 2 bits into 4 bits output
16:  verify the Matrix X
17:  with each block of binary 8 bits with check sum.
18:  This decoded data same as Xoriginal data
19:  end

```

5 DISCUSSIONS AND INTERPRETATIONS

Secure Socket Layer provides security services between TCP and applications that use TCP. Internet standards TLS, SSL/TLS provide confidentiality using symmetric encryption and message integrity and Authentication code. This protocol as a case study will be used to Secure Electronic Transactions (SET) to protect credit card transactions on web service applications. We have implemented message authentication code by random message to client from Server. The

Algorithm 2 HTTP Secure socket layer

```
1: procedure HTTP_SSL
2: SSL required to make to use of TCP , reliable end to end
  secure services
3: input :Web service URL request
4: Ouput : Secured HTTP Session layer
5: Read request of web service
6:   begin
7: Invoke HandShake Protocol
8: Connect: logical link between peer to peer network
9: Session: Created by handshake protocol. Set of crypto-
  graphic parameters
10: Session multiple secured connections are not used.
11: Session established with both read and write.
12: During handshaking protocol session is created success-
  fully
13: pending the new state if already the state is running.
14: With both read and write Session identified with state.
15: Compress data prior encryption
16: Invoke Encryption algorithm
17: Flag is used indicate new connection.
18:   end
```

Algorithm 3 To Establish connection

```
1: procedure CONNECTION
2: A connection state is defined by the following Parame-
  ters:
3: Connection(clientid,clientMAC,ClientSecretKey,serverid)
4:   begin
5: Client sends request to Web server Invoke HandShake
  Protocol.
6: Each connection creates secure session layer and sets the
  flag.
7: If already connection is established in read/write mode
  do not open new connection else
8: Invoke Handshake protocol Sequence of each request is
  encrypted
9: Decrypt messages at receiver
10: Change CipherSpecProtocol: signal for coordinating
  client server.
11: Alert protocol: Application is allotting compression and
  close_notify alert for each message.
12:   end
```

Algorithm 4 Web Security by access control to Encryption

```
1: procedure WS_ACESSCONTROL
2: HTTP protocol is used for web transactions into appli-
  cation passed to SSL.
3: HTTP: connection initiation
4: Input: web service request message
5: Output: Secure access control by encryption
6:   begin
7: read HTTP request by SSL to Authorized web server by
  invoking HandShake Protocol
8: Data is encrypted with user details
9: send the request to Web server
10: User data is verified with the data with existing data of
  concerned web server.
11: If(HTTPrequest is successful) then connection is estab-
  lished under service access policy else connection is
  closed with notification
12: if connection is established enable decryption of data at
  the web server
13: Message communication is accomplished by SSL en-
  cryption method.
14: close the connection
15: Connection closure if connection is closed in HTTP
  record
16: TLS level exchange close_notify alert then close TCP
  connection
17: handle TCP close before alert exchange send or com-
  pleted
18:   end
```

discussions and interpretations for web securities, precautions and remedies are described in table.2. and table.3. The table provides the information related to web security or network security problems and proposed solutions/precautions to meet network securities QoS parameters such as confidentiality, integrity, data authentication, and availability of information to trusted users from web service systems by merchants by digital certificates and required policy constraints.

6 CONCLUSION

Web services are expected to play increasingly important role for message communications over internet applications. Most of future work is web security. Online shopping and web services are increasing in the world. In this paper we described the fundamental concepts related to web security threats, web server architectures, Encryption, decryption and web server protocols. QoS web service security is important concern in network communications. Firewalls security, various issues and challenges of web security. As a case study we presented comprehensive study of HTTP Secured Socket Layer Protocol. In this paper we address the issue of secure communications in web services using HTTP secure socket layer approach. The key issue of communications handshake protocol is using lossless compression technique by encoder to improve the speed of web services during SSL communications between client and server. As a case study using HTTP secured socket layer approach implemented Message Authentication code implemented in Java/J2EE and tomcat

web server results are shown from Figure.10, Figure.11 and Figure 12. In future we propose to extend this paper to E-Commerce, On-line financial transactions, and this security concepts used for designing and developing firewalls which will protect web services applications.

7 References

- [1] Gustavo Alonso, Fabio Casati, Harumi Kuno: Web Services: Concepts, Architectures and Applications and Springer publications, 2003, 124-130
- [2] Sanjiva Weerawarana, Francisco Curbera, ony Storey: Web Services Platform Architecture: SOAP, WSDL, WS-Policy, WS-Addressing, WS-BPEL, WS-Reliable Messaging and O'Reilly Publications, 2005
- [3] William Stallings: Cryptography and Network Security, 5th Edition and Prentice Hall India
- [4] www.livehacking.com
- [5] <http://www.cnet.com/news/the-unvarnished-truth-about-unsecured-wi-fi>
- [6] <http://www.cnet.com/news>
- [7] <https://forums.spybot.info>
- [8] <http://www.cisco.com>
- [9] Khaled M Khan: Managing Web Service Quality: Measuring Outcomes and Effectiveness and Information Science Reference, 290-292
- [10] Zoran Stojanovic and Ajantha Dahanayake: Service Oriented Software System Engineering Challenges and Practice
- [11] <https://en.wikipedia.org>
- [12] www.cs.ucsb.edu
- [13] mercury.webster.edu
- [14] www.incapsula.com/ddos/ddos-attacks/denial-of-service.html
- [15] S.Bregni, P.Giacomazzi, A. Poli: Cost-Performance Optimization of SSL-Based Secure Distributed Infrastructures. IEEE Latin America Transactions, Vol. 9, No. 4, July 2011, 550-556, DOI: 10.1109/TLA.2011.5993742
- [16] <http://homepages.uel.ac.uk/>
- [17] Mohammed A. Alnatheer: Secure Socket Layer (SSL) Impact on Web Server Performance, Journal of Advances in Computer Networks, Vol. 2, No. 3, September 2014, 211-217. DOI: 10.7763/JACN.2014.V2.114
- [18] Fengying Wang, Caihong Li, Lei Zhao, Xiumei Li :A comprehensive security policy research on web information system Automation and Logistics, 2009. IEEE International Conference ICAL2009. 1776 - 1780, DOI: 10.1109/ICAL.2009.5262671
- [19] Jin-Ha Kim, Gyu Sang Choi, Das, C.R.: A Load Balancing Scheme for Cluster-based Secure Network Servers IEEE International Cluster Computing 2005. 1 - 10, DOI: 10.1109/CLUSTER.2005.347056
- [20] Jingli Zhou, Hongtao Xia, Xiaofeng Wang, Jifeng Yu :A New VPN Solution Based on Asymmetrical SSL Tunnels FCST '06. Japan-China Joint Workshop on Frontier of Computer Science and Technology, 2006. 71-78, DOI: 10.1109/FCST.2006.4
- [21] Mortazavi S.H., Yazdani. M., Jalilzadeh F., Avadhani. P.S : A novel secure protocol called FSSL using fuzzy controller for Web security IEEE International Conference on Systems, Man and Cybernetics (SMC), 2014, 1192 - 1197, DOI: 10.1109/SMC.2014.6974076
- [22] Lin Shung Huang, Rice.A., Ellingsen.E., Jackson.C.: Analyzing Forged SSL Certificates in the Wild IEEE Symposium on Security and Privacy (SP), 2014, 83 - 97, DOI: 10.1109/SP.2014.13
- [23] Fang Qi; Zhe Tang; Guojun Wang : Attacks vs. Countermeasures of SSL Protected Trust Model The 9th International Conference for Young Computer Scientists, 2008. ICYCS 2008. 1986 - 1991, DOI: 10.1109/ICYCS.2008.433
- [24] Bregni.S., Giacomazzi. P., Poli. A. :Cost-Performance Optimization of SSL-Based Secure Distributed Infrastructures IEEE (Revista IEEE America Latina), 2011, Volume: 9, Issue: 4, 550 - 556, DOI: 10.1109/TLA.2011.5993742
- [25] Yang Kuihe; Chu Xin: Implementation of Improved VPN Based on SSL, 8th International Conference on Electronic Measurement and Instruments, 2007. ICEMI '07, 2-15 - 2-19, DOI: 10.1109/ICEMI.2007.4350641
- [26] Leavitt, N. Computer: Internet Security under Attack: The Undermining of Digital Certificates Volume: 44, Issue: 12 Pages: 17 - 20, DOI: 10.1109/MC.2011.367
- [27] .A.S.Tanenbaum: Introduction to Computer Networks Computer Networks, 3rd Edition, Pearson publications., 2005, 41-45
- [28] Tanenbaum, and Wetherall: Computer Networks 5th Edition, Pearson publications, 2010, 12-15
- [29] Mihir Bellare, Shai Halevi, Amit Sahai, and Salil Vadhan: Many-to-One Trapdoor Functions and Their Relation to Public-Key Cryptosystems, CRYPTO98, Springer-Verlag Berlin Heidelberg 1998, 283-299