Strategic Techniques for Enhancing Web Services Security in Cloud Computing Model

Alo .U. Rita Nweke .F. Henry
Computer Science Department, Ebonyi State University, P.M.B 053 Abakaliki Nigeria

Abstract

The 21st century has witnessed an integration of enterprise business process with emerging techniques in a quest to maximize opportunities and organisational strength. In spite of these, vulnerabilities and risks still abound due to the integration for an effective operational mechanism. Mitigating against these requires strategic techniques for enhancing web services security. It is on this background that this paper has been presented. A critical study of web services architecture and cloud computing model as an emerging technology has been given a succinct digest. Furthermore, an evaluation of recent trends in web services and cloud computing model security issues were x-rayed. The threat to web services application deployed in cloud computing were identified hence presenting strategic techniques for enhancing web services security as a proactive measure to enhancing enterprise success. This paper concludes by re-iterating the need to understanding various security threats and proactively and dynamically reacting to them.

Keywords: Web Services, Cloud Computing, Cross Site Scripting, SQL Injection and Web Security

1 Introduction

Web services as a technology for creating distributed, integrated and interoperable solutions across the internet is the effective mechanism of data and applicative integration on the web. It provides first choice of emerging computing technologies such as grid computing, utility computing, and internet computing e.t.c for enterprise business processes. Web services have the characteristics of providing platform independent, dynamic, open and loosely coupled enterprise applications [21]. Cloud computing has helped to create avenue and enabling factors to position the web services as the foundation for the internet applications and businesses. The integration of web services architecture and cloud computing has been found to be of immense advantage. Some of these are data access openness and standardisation, autonomy of underlying supporting infrastructure and dynamic search and discovery using search engine optimisation. Web services have played a major role in high level implementation of cloud computing especially in platform as a service model [10]. The major problem faced by organisations adopting web services is to maintain security and data privacy. This may be inform of application or network security against attacks such as SQL injection, Cross site scripting, man in the middle attacks, denial of service to mention but a few.

To address these security problems, web service expert and organisations need to adopt proactive techniques and approaches to mitigate these attacks [23] and this is the basis of this research paper. We have critically discussed web services architecture and cloud computing model, evaluate the security issues hampering their implementation and outline practical and effective approaches to mitigate such security flaws

2 Overview of Web Services

The development of World Wide Web (WWW) has been a huge success enabling computer to human interaction at the internet scale. The Hypertext Transfer Protocol (HTTP) and Hypertext Markup Language (HTML) protocol stack used by web browsers has proven to be cost effective methods of presenting a user interface for connection of different devices. This feature was made possible by the simple nature of HTTP and HTML. The two protocols are mainly text based and can be implemented using wide ranges of operating system and programming environment. The ideas and principles of World Wide Web have been used to design web services to enable machine to machine or computer to computer interaction. Web services communicate using a set of foundation protocols that share common architecture and are meant to be released in a variety of independently developed and deployed systems. The main difference between World Wide Web and web services is while World Wide Web is designed for the purpose of browsing interactive contents that is often static or cacheable, web services architecture is designed for highly dynamic program to program interactions [18].

According to Erin Cavanaugh [13] Web services can be defined as "a software component that communicates using pervasive standard-based technology including hypertext transfer protocol (HTTP) and extensible mark-up language (XML) based messaging". The services are designed to be accessed by other application via web. The application may provide operations such as checking of account balance online, taking latest news from web service of a particular news agency, stock data, processing of customer relationship management and enterprise resources planning [13]. It can also be seen as an interface that describes a collection of operations that can be accessed over the network using standard XML messaging [19]. The major advantage of web services is the platform independence feature, application written in different programming languages can run in different machine, operating system and exchange information over the internet or intranet. The platform has become a distributed computing paradigm that allow application to be created from multiple web services dispersed across the web originating from various sources regardless of where they reside or how they are implemented [8].

Web services perform the functions of server in distributed application, that is, there are no clear differences except in underlying layer for performing the application logic and data manipulation. It provides the services needed and respond to the user request [14]. The interface provided by web services can communicate with other application using simple object access protocol (SOAP).

The architecture of web services consists of four components, and they are Extensible mark-up language, simple object access protocol, universal discovery and integration and web service description language [13], [8], [14].

Extensible Mark-up language is the specification provided by the World Wide Web consortium (W3C), Meta language for describing data. The data to be described are "surrounded with customizable text based tags" which provides accurate information as well as the hierarchical structure of data. The component is both application independent, human readable, simple and interoperable, and has helped for its well acceptance as a standard for exchange of information between heterogeneous systems in different web applications. XML is the foundation of modern web services which use XML-based technologies to describe and encode their messages [13].

Web Service Description Language (WSDL) is another W3C specification that uses XML-based format to describe the clients that access the web services, read and interpret the WSDL files to learn the location of the services and operation they provide. The specification is the web service interface that provides the clients with the needed information to interact with other services in a standard way. The WSDL file is the contract between clients and the server, which when obeyed allow service providers and service consumers to exchange data in a standard way irrespective of the platform and application the services are operating [13].

To enable exchange of data over hypertext transfer protocol, *Simple Object Access Protocol* (SOAP) was developed. The protocol provides a standard based method for sending XML message between a service and its client. Simple Object Access Protocol can be sent between applications regardless of their platform or programming language. This has helped to enable efficient interoperability in web services [14].

Organisation can create XML based registry for listing information about their businesses using *Universal Description Discovery and Integration* (UDDI). UDDI specification is sponsored by organisations for advancement of structured information standard and is often described as the yellow page of web services [13]. The registry of the organisation's information can be private or public and linked behind organisation's corporate firewall. When the information about the organisation is needed, the application developer can query the registry for the services and can design the web services for automatic update and services change from the UDDI registry.

Heather Kreger [19] outlines different components that make-up the web services model. They include the service roles, operations and service artefacts. The web service roles define the interaction between service provider, service requestor and service registry.

- *Service provider* is the owner of the listed services or platforms. The service provider defines the service description for the web service and publishes it to service requestor.
- *Service requestor* is the business or applications that require certain functions to be classified. The application search for and invoke or imitate an interaction with service, this is done by a web browser driven by a person.
- *Service registry* is the registry where searchable service description by service provider is published and services requestors find services and obtain binding information.

Operations in web services architecture are the behaviours that must take place in web service. These operations are publication of web service description, finding of web service description and binding or invoking of services based on service description.

- *Publish*: Publication of service description that is accessible over the network and can be located by service requestor.
- *Find*: Service requestor retrieves the types service description required from the service registry.
- *Bind*: The service requestor invokes or initiates an interaction with services at run time using the binding details in the service description.

The artefacts of web service architecture are:

- *Service:* Service is the software module deployed on a network accessible platform provided by the service provider which can be invoked by service requestor.
- *Service description*: Service description is made up of detail interface and service implementation such as data types, operations binding information discussed before, network location, categorisation and

other metadata to ensure quick discovery and utilization by service request.

One may be forced to ask the benefits organisations stand to gain in adopting web services platform. Srinivas et al [8], Cavanaugh [13] and Kreger [19] discussed in details the advantages of web services adoption. Some of these advantages are:

- Web services have inherent interoperability that comes with using "vendor" and "language independent" XML technologies and ubiquitous HTTP as way of communicating with other applications. Organisations can interpret different applications and data formats with relative ease.
- Web services can be accessed by organisation through web based clients interface. Multiple data from web services can be combined to present application for accessing different services regardless of whether the services are compatible or not. Codes developed for implementing business requirement of organisation can be reused and tailored towards fulfilling different business objectives. This has eliminated the creation of custom code. Also, organisation can save huge amount of money, existing infrastructures and application can be utilised to increase saving.
- It is a technology for deploying and providing access to business functions over the web.
- Integration and application of web services can be done at incremental manner using organisations' language and platform.
- Helps to deploy solution faster and open up new opportunities.
- Allow application to be integrated more rapidly easily.
- Provide a unifying programming model so that application integration inside and outside the enterprise can be done using common approach with common infrastructure.

3 Cloud Computing Technologies

The quest to move computing and data from desktop portable PC into integrated data centre has lead to the development of cloud computing technology. Applications are delivered as a service over the internet using cloud infrastructure such as hardware and software in centralised location [7]. The advantage of this developing technology is the cost reduction of all computing infrastructures. Cloud computing also enables faster and effective means to store read document and "interface access to various web services." [2].

Rohit Bharadauria et al [2] defined cloud computing as "dynamically delivery of scalable, elastic, shared and virtualised resources as a service accessible over the web". Cloud computing can also be seen as a set of IT services provided to a customer over a network on leased basis and with the ability to scale up or down their services at will [3]. The technology offers innovative business model for organisation to adopt with upfront investment [3]. In cloud computing, the key elements are computing resources are wrapped up as a commodity for web access, extremely easy access to web resources for end users and business model based on "pay as use principles" [2]. Different services provided by cloud include ranges of free and paid services [20]. These services include free and paid services. Some of the free services are web based email services, search engine facilities, social networking and gaming services. While the major paid cloud services are business oriented services such as Google doc, Window Azure by Microsoft Corporation, Amazon Elastic Compute Cloud (EC2) to mention but a few.

3.1 Cloud Computing Deployment model

Cloud computing can be deployed in four ways. *Public cloud* where infrastructures are provided to customer by third party and the user can dynamically provision resources on fine grained, self services through the internet. Public cloud is based on a pay per use model and less secure. *Private cloud* infrastructures are designed and implemented by organisation for specific customers on private network. The deployment model is set up within an organisation's enterprise data centre where resources are available for use by the customer. It is more secure than public cloud due to the internal exposure, so it can only be accessed by designated stakeholder of the organisation. *Community cloud* infrastructures are shared, implemented and managed by several organisations for efficient service delivery. Finally, *hybrid cloud* combine the features of all the different types of cloud enumerated above and are linked in a way that data transfer takes place between them without affecting each other. The open architecture of this model allow it to be interfaced with other management systems, and provide more secure control on the data and application information over the internet[2], [20].

3.2 Cloud Computing Services Delivery Model

The technology can be implemented in any of the following models. *Software as a service* (SaaS) provides customizable and end user oriented packages and applications hosted on the infrastructure of the services providers and made available to customer over a network. Business software functionalities can be provided to enterprise customer at cheaper rate with same benefits of commercially licensed, internally operated software. Software as service architecture applications can support multi-tenancy at once and accessed using web browsers over the internet, providing security features for such web browser is very important. The enterprise customer is SaaS does not manage or control the underlying network server, operating system and storage but can access application stored on cloud providers' infrastructures. Examples of software as a services are Saleforce.com and Googledoc [10], [20]. *Infrastructure as a Service* (IaaS) provides shareable hardware resources for executing services using virtualised technology. Cloud customer can provision processing, storage, network server and other computing resources where the consumer can deploy and run different software. The user can manage and control the operating system, storage, deployment of application and some part of the network component but not the cloud infrastructure. Example of IaaS is the Joyent that provide series of virtualised servers on infrastructure demand. *Platform as a service* (PaaS) is the middle layer that provides platform oriented services besides providing the environment for hosting user applications. PaaS provides the input on implementation, design and also unique for web services development and deployment. That is, PaaS is a set of software tools hosted on a providers' server that offer developer can tap to build their application. Software developer can design, manage, plan build and test web based application without buying actual server and setting them up. The consumer does not manage or control the underlying cloud infrastructure such as network serve, operating system or storage but can deploy, configure and host built application on cloud provider's infrastructure. Example is the Google App Engine [2], [10], [20]. Figure 2 shows the structure of cloud computing model.

3.3 Benefits of Cloud Computing

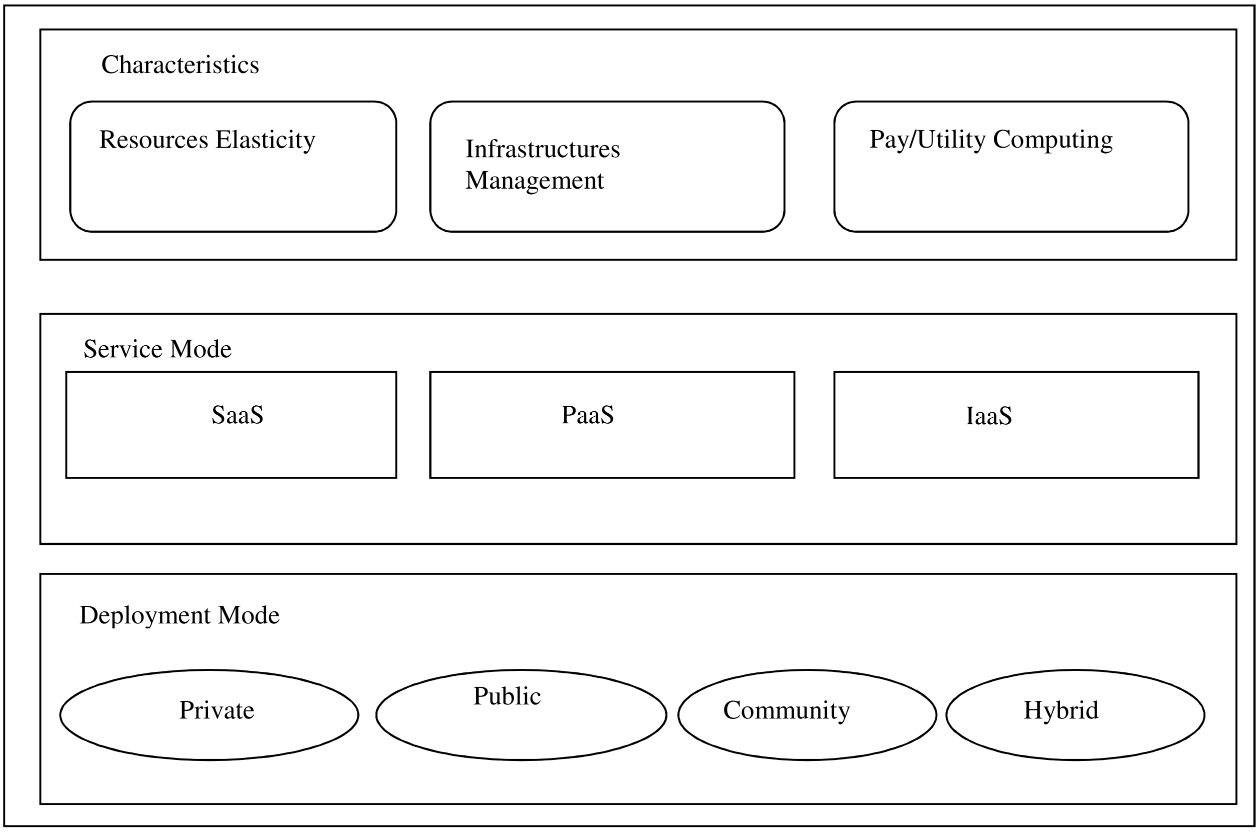
Cloud computing technology has many derivable benefits that can enhance the services of any organisation that adopt it as enumerated in [20]. These benefits are:

- Cost reduction on computing infrastructures and application;
- Immediacy of computing services;
- Availability of services;
- Helps to improve the pace of motivation for start up users to deploy new products quickly at low cost;
- Allow small user to compute favourably with big organisations;
- Provide internet based services allowing users to avoid upfront hardware and software investment
- Ensure rapid implementation of projects and service provision
- Ensure consistent service and limit network outage.

3.4 Characteristics of Cloud computing

For any computing technology to be termed cloud computing, it must exhibit any of these characteristics [20], [21].

- Dynamic provision of IT tools and capabilities from third party over an established network.
- Form of remote computer that can be accessed with the help of web based tools through web browsers as if it is locally available on end user's computer.
- Network resources through a standard mechanism using heterogeneous thin and thick client platform (e.g. mobile phones, laptop and Personal Digital Assistant).
- Provision of computing resources such as storage, processing, memory, network bandwidth and virtual machine from different organisation to multiple consumers using multi-tenancy model.
- Rapid and dynamic scaling of computing resources to meet the demand of end users.
- Cloud resources are automatically controlled and optimized thereby making cloud infrastructure available to the public on demand basis.



Cloud Computing Model [17]

4 Recent Trends in the Web Services and Cloud Computing Security

In recent years, there are number of on-going researches in the area of web services and cloud computing security and integration.

Hartwig Gunzer [14] presented a general overview of web services, advantages and problem associated with web services. He maintained that issues such as performance, scalability, failover and more importantly security are still areas of concern in web services implementation.

Gu Yue-Sheng; Ye Meng-Toa and Gan Yong [12] presented web services security based on XML signature and encryption. They noted that the current safety transmission mechanism used cannot meet the security challenges. The use of XML signatures and encryption was proposed. The process employs abstract algorithm such as MD5, SHA-1 etc to calculate hash value of primary data. XML signature can solve security problems such as falsification, spoofing and repudiation. XML encryption was used to solve security problems such as eavesdropping and the document is safe in transmission and storage status.

According to E. Uma et al [11], new architectural framework was developed for providing secured web services. The system splits existing software into three parts, highly trusted area that handle security sensitive information and a legacy. Untrusted part handles non-sensitive information without access restriction and medium-trusted part that handle information between the two. Bharat Prajapat et al [7] designed and developed web based document exploration using J2ME mobiles and cloud web services. The cloud based mobile computing architecture enables a faster and effective way to read any text documents.

Sabah Mohammed et al [4] developed a service oriented architecture that securely managed scalable vector graphics (SGV) web services using the intermediary design pattern. They used signature/authentication and encryption/decryption security mechanism for security of web application and the prototype implemented in Apache Axis. Debalyoti mukhopadhayay et al [6] presented layer architectural framework for effective web services in cloud computing. Service consumer can discover the needed services using non-functional attribute of the web services. The proposed framework provided Quality of Service (QoS) requirement as part of service discovery query filter and rank services according to service consumer preferences.

Yogamangalam Y and Shankar V.S Sriram [9] reviewed various security issues in cloud computing, such as user authentication, open source provision, virtual infrastructure, service level agreement and data storage. They noted that security features such as privacy, authentication, application vulnerability, data integrity, access control, and confidentiality are of great importance in cloud implementation. Cloud providers maintain authentication to cloud service users' data from breeches using public cryptographic algorithm, where service level agreement (SLA) evaluates security for web services. Virtual infrastructure of the cloud should be secured against vulnerabilities. Hackers can introduce malicious codes to achieve Distributed denial of service (DOS), dynamically provisioned access control infrastructure (DDCI) architecture proposed are: use of partitioned clock cache (PLcache) and random permutation cache (RPcache) to defeat cache based side channel attacks, use of advanced cloud protection system (ACPS) to guarantee security to the resources in the virtualisation to monitor for integrity of guest and use of firewall, intrusion detection and prevention.

Catalin Strimbei [10] presented a framework for web services and cloud computing integration. The framework is a common services model of service oriented architecture (SOA), web services and cloud computing which could enhance the characteristics of its basic standards, specifications and platform to describe truly dynamic, agile and autonomous web services. Practical approaches like dynamic discovery and linking protocol to achieve dynamic interoperability between web services was proposed. Asfia Mubeen et al [5] proposed a new data integration architecture for web services and cloud computing. Web users' information were extracted, consolidated, linked and then populated into a single data store where user can have integrated access to their data objects from anywhere in the world through multiple devices. The proposed system was implemented in advanced Java technology and the results were tested on different dataset.

All the current research efforts addressed the security of web services, cloud computing or integration of web services and cloud computing. There are needed gaps to be filled when the security implications of such integration and the strategic techniques for enhancing the security of web services and cloud computing integration are presented in organisations' enterprise business process; this research focuses on the benefit of web services and cloud computing integration, security threats and strategic security techniques to eliminate these threats.

5 Threats to Web Services Applications Deployed In Cloud Computing

The rise in cloud computing implementation, design and deployment in organisation has increased the number of threats to security and privacy of services and data stored in cloud. Service users have to update their personal information online which can lead to identity theft [2]. Threat which is the potential risk launched by an attacker against system security weaknesses have become common in online application and services. Inaccurate vendor implementations, configuration problems and coding mistakes have led to exploitable vulnerabilities in web services. It is very important for developers and researchers to understand the risk these threats and vulnerabilities pose and consider mitigation before deploying for public use [15].

Research efforts by Information Assurance Directorate [15] and Rohit Bhadauria et al [2], enumerated different threats to web services securities, these threats pose serious security problems to web services application. Outlined are these threats.

- **SQL Injection**: The attacker gain unauthorised access to service database and accesses sensitive information by injecting malicious code into the SQL code. The web site sees the input data supplied by the attacker as legitimate data and therefore allows access and the attacker can compromise the integrity of some information.
- **Cross Site Scripting (XSS):** Most web sites and applications designed within web 2.0 technologies are dynamic in nature and therefore vulnerable to XSS attacks. Web site are injected with malicious script by attacker and displayed as popup link to hazardous site to the intruder third party where he/she takes control of the user information or hack their accounts after having known the information available to them.
- **Man in the Middle Attacks**: Attackers try to intrude in an ongoing conversation between sender and clients to inject false information and have knowledge of the important data transfer between them. Also attacker can steal or modify information if not protected using encryption algorithm while in transit.
- **Domain Name Server Attacks**: Domain name server helps to translate domain name to IP address. The use of domain will necessitate the routing of user packets to evil cloud instead of the intended one. This type of attack is common at the network level.
- **Denial of Service and Distributed Denial of Service:** The attacker attempts to make the services assigned to authorised users unable to be used by them. The network servers are flooded with service by attacker using bogus requests thereby making the service unavailable to the authorised user. Sometimes, when legitimate users try to access a site, we see that due to overloading of the server with request to access the site, we are unable to access the site and observe an error. These happen when the numbers of requests that can be handled by server exceed its capacity. The occurrence of denial of service (DoS) attacks increase the bandwidth making the services unavailable to the user. Distributed Denial of Services is the advanced version of denial of service in terms of denying the important services running on server by flooding the destination server with a bogus packet such that the target server is not able to handle it. The attacks are relayed from different dynamic network which have already been

compromised unlike distributed denial of service. The attacker controls the flow of information by allowing some information available at certain times. The amount of and type of information available to the public usage is clearly under the control of the attacker. It is run by two functional units. A master slave that launches the attacks and slave is the network which acts as the launch pad for the master. It is operational in two ways such as intrusion phase where the master tries to compromise less important machine to support in flooding the more important one, and the installing DOS tools and attacking the victim server or machine.

- **Information Leakage:** Web services that generate verbose fault message are useful to developers and administrator. However, the message can give away too much information in operational environment. This issue also affects web services that use web services description language to provide a description of a services and its interface. Web services description language contains server directory information, internal IP address information available services and methods and other critical information valuable to attackers. Attacker can also replay leaked massage to a server to invoke actions multiple times.

Jiang Li et al [1] noted that the commonly used method of determining web services threats is by classifying them. They classify web services threats using the STRIDE acronym, which stand for spoofing, tempering, repudiation, denial of services, elevation of privileges and message disclosure.

Spoofing is the imitation of others on the computer and illegally access and use of other users' authentication message such as username and password. Tempering involves maliciously modifying the data, unauthorised altering the permanent data stored in database and altering data during transmission between two devices between unsecured networks. Repudiation occurs when user rejects activities and there is no way to prove that he is refusing to abide the agreement. Message disclosure means to disclose the content of a massage to the unauthorised user without access privilege or to let the intruder read the datum that transmitting between two computers. And elevation of privilege is when the users without using privilege can get access so there is no enough access privilege to damage or destroy the whole system.

6 Strategic Techniques for Enhancing Security of Web Services Application in Cloud Computing Model.

The security of Web services involves the use of software and hardware resources to provide security to applications hosted online such that attackers are not able to get control over the applications and make desirable changes to its form and formats. Because of the security threats experienced by web service applications in cloud computing, it is necessary to install high level security checks to minimise these threats which were mentioned in section four above. Most times, organisations employ traditional security methods such as device oriented, which handle specific security task but such security mechanism is ineffective due to the dynamism and adaptability of these threats in web services application [2].

Web service security provision need to be centred [1] on

- Testing and verifying web service effectiveness;
- Analysing the test to the vulnerability of web services security;
- Analysing the test to the reliability of web services;
- Authenticating the identity of the user access to the web service;
- And testing proposed framework of web service security.

They are many practical, conceptual and effective approaches developed to mitigate and enhance web services applications hosted in cloud computing environment. These approaches have been adopted and effectively utilised by most organizations in providing web services security [1]. These approaches are:

SQL injection attacks can be mitigated by avoiding the usage of dynamically generated SQL in the code, and the use of filtering techniques to sanitise the user input. Static analysis and run time analysis or combination of both to form hybrid techniques has been used extensively by researchers to prevent SQL injection (jalal et al, 2014; Perumalsamy et al, 2012). Jalal et al further outlined different steps such as database replication, creation of behavior database, redirection of SQL queries and virtual execution SQL queries implementation as an important prevent strategies. Cross site scripting attack(XSS) can be prevented using active content filtering, content based data leakage prevention technologies and web application vulnerabilities detection technology that adopt various methodologies to detect security flaws can be used.

Man-in -the-middle attacks that are common in wireless networks can be fixed by organisations, by adopting and implementing various tools such as strong encryption technologies like DSniff, Effercap, WSNiff and AirJack to safeguard against them. Other important methods are elevating software as service security in cloud computing, providing endpoint process and server security process, evaluating virtualisation at the endpoint, server access security and data privacy using encryption.

Domain Name System attacks can be mitigated using security measures such as Domain Name system security extension (DNSSEC). This is a suite of Internet Engineering Task Force (IETS) specification for securing certain kind of information provided by DNS. The technology provides origin authentication of DNS data, authenticate denial of existence of data integrity but cannot provide availability and confidentiality. It protects application from forged or manipulated DNS data such as data created by DNS cache poisoning [16].

Denial of service which denies authorised user from accessing a service can be prevented by using intrusion detection system that will alert the administrators when there is any attack. To militate against distributed denial of service (DDOS), the following techniques and technologies can be adopted:

- Extensive modification of the underlying network;
- Use of swarm based logic for guarding against DDOS attacks. The logic provides a transparent transport layers through which common protocols such as HTTP, SMTP etc can pass easily;
- Implementing the intrusion detection system on all physical machines which contain the user's virtual machine.

Also, to ensure security of web services application, Jiang Li et al [1] emphasised that the following security objectives must be met. They include:

- **Confidentiality**: Ensure that the message cannot be stolen by unauthorised users of entity, prevention of illegal access by using encryption scheme to encrypt series of request and response of web services transmitted.
- **Integrity**: Ensure that the web services data can not be accidentally or deliberately be damaged and kept integral and uniform. It does not prevent message tempering but detect tempered message during transmission. This can be achieved using Hash algorithm.
- **Non-repudiation:** Ensure that a sender cannot deny or disaffirm sending a message and provide reliable entities during transmission. In online transaction, it ensures that a web site cannot deny it order request and response form sender and receiver. Non-repudiation is achieved using unsymmetrical key encryption algorithm especially digital signature.
- **Identity validation**: This provides suitable entity certificate to access enterprise application datum. Entity that cannot provide suitable certificate is denied access to the enterprise resources. Entity validation can be achieved using the following techniques:
  - Identity validation based on operation system;
  - Validation based on web server;
  - Validation based on order;
  - Validation based on single log on;
  - Client/server single log on;
  - And biometrics.
- **Authorisation:** Authorisation is the awarding of privilege and permission to entity to access web services resources and thereby provides access control. Authorisation is provided by limiting access to resources such as host computer, documents, web pages, and application interface and database records.

Table 1 below summarises the different web services threats and techniques adopted to militate against them.

Threats	Solution Techniques
SQL Injection attacks	▪ Avoiding the usage of dynamically generated SQL in codes ▪ Filtering
Cross site scripting (XSS)	▪ Active content based filtering ▪ Content based data leakage prevention.
Man-in-the-middle attacks	▪ Use of strong encryption techniques such as DSniff, AirJack etc.
DNS attacks	▪ Implementing Domain Name System Security Extension (DNSSEC) to reduce the effects
Sniffer attacks	▪ Implementing sniffer program through NIC. ▪ Malicious detection platform based on ARP and RTT.
DoS	▪ Using intrusion detection system (IDS)
Cookie poisoning	▪ Cookie clean up and strong encryption scheme.
DDoS	▪ Extensive modification of network infrastructure ▪ Swarm based logic ▪ Intrusion detection system

7 Conclusion

Technology has remained the central pivot for organisational success. The evolution and integration of emerging computing technology geared toward maximizing organisational opportunities and strength will continue to be on the increase. Realizing this has some security challenges. To mitigate against vulnerability and risks associated with this integration, there is need to be proactive and dynamically reacting to such organisation who want to deploy web services in cloud computing and still maintain a leading champion must be dynamic and proactive in its security check.

REFERENCES

[1]. Jiang Li, Chen Hao, Deng Fei and Zhong Qiusheng (2011) "A security Evaluation method Based on Threats Classification for Web Services". Journal of software, vol. 6, No.4, Pp 595-603.

[2]. Rohit Bhadauria, Rituparna Chaki, Nabendu Chaki and Sugata Sanyal (2011) "A Survey on Security Issues in Cloud Computing ". Online at www.arxiv.org (Accessed: 15/05/2013).

[3]. Kuyoro S.O, Ibikunle F., Awodele O (2011) "Cloud Computing Security Issues and Challenges". International Journal of Computer Networks (IJCN), Vol. 3, Issue 5, Pp 242-255.

[4]. Sabah Mohammed, Jinan Fiaidh, Hamada Ghenniwa and Marshal Hahn (2006) "Developing a Secured Web Services Architecture for SVG Image Delivery". Journal of Computer Science, Vol. 2, No. 2, Pp 171-179.

[5]. Asfia Mubeen, Mohd Murtuza Amed Khan and Sana Mubeen Zubedi (2012) "Web Services Integration using Cloud Data Store". International Journal of Computer Science and Networks (IJCSN), Volume 1, Issue 6, Pp 88-92.

[6]. Debajyoti Mukhopadhyay, Falguni J. Chathly, and Nagesh N. Jadhav (2012) "QOS Based Framework for Effective Web Services in Cloud Computing". Journal of Software Engineering and Applications, Volume 5, Issue 1, Pp 952- 960. Online at: http://www. sciRP.org/journal/jsca. (Accessed: 10/04/2013).

[7]. Bharat Prajapat and Manish Chrisvastava (2012) " Mobile Cloud Computing through J2ME Application: Cloud Enabled Web Services". International Journal of Advanced Computer Research, Volume 2, No.4, Issue 6, Pp 475-480.

[8]. K. Srinivas, P.V.S Srinivas and A. Govardhan (2011) "Web service Architecture for Meta Search Engine". International Journal of Advanced Computer Science and Applications (IJACSA), Vol.2, No.10, Pp 31-36.

[9]. Yogamangalam R and Shankar Sriram V.S (2013) "Review on Security Issues on Cloud computing". Journal of Artificial Intelligence, Volume 6, No.1 Pp 2-7.

[10]. Catalin Strimbei (2012) "Smart Data Web Services". Journal of Information Economica, Vol. 6, No.4, Pp 74-85.

[11]. E. Uma, A. Kannan and R. Ramesh (2011) "Design of New Architecture for Providing Secured Web Services". Proceedings of the world congress on Engineering and Computer Services 2011, Volume1, WCECS 2011, October 19-21, 2011.

[12]. Gu Yue-Sheng, Ye Meng-tao, Gan Yong (2010) "Web Services Security Based on XMLSignature and XML Encryption". Journal of Networks, Volume 5, No.9, Pp 1092-1097.

[13]. Erin Cavanaugh (2006) "Web Services: Benefits, Challenges, and a Unique, Visual development solution". A white paper. Online at www.altova.com/web services.pdf (Accessed: 22/03/2013).

[14]. Hartwig Gunzer (2002) "Introduction to Web Services". Online at www.edn.embacarden.com/introduction-to-webservices.pdf. (Accessed: 22/03/2013)

[15]. Service Oriented Architecture Security Vulnerabilities-Web Services". System and Network Assurance Directorate. Online at http://www.nsa.gov/oa/~files/fastsheet/SOA-security-vulnerabilities-web.pdf (Accessed: 02/06/2013).

[16]. "Domain Name System Security Extension". Online at www.wikipedia.org/wiki/Domain_Name_System_Security_extension. (Accessed: 30/06/2013).

[17] www.blogs.msdn.com/b/jmae~/archive/2010/02/11/visual-model-of-cloud- computing.aspx. (Accessed: 20/06/2013).

[18] Luis Felipe Carbrera; Christopher Kurt and Don Box (2004) "An Introduction to web services Architecture and its Specification". Online at http://msdn.Microsoft.com/en- us/library/ms996441.aspx.(Accessed: 13/02/2014

[19] Heather Kreger (2001) "Web services Conceptual Architecture (WSCA1.0)". Online at http://www.csd.uoc.gr/~hy565/newpage/docs/pdfs/papers/wsca.pdf. (Accessed: 30/01/2014).

[20] Ghasura R.S, Patel H.B, Dudhatra G.B and Chaudhary G.M (2012) "Cloud computing: Future Buzz for Rural India". Wayamba |Journal of Animal Science. Online at http://www.wayabajournal .com (Accessed: 10/01/2014).

[21] Ahmed S. Al-Masah and Ali M. Al-Sharafi (2013) "Benefits of Cloud Computing For Network Infrastructure Monitoring Service". International Journal of Advances in Engineering and Technology. Vol. 5, Issue 2. Pp 46-51.

[22] Shujun Pei, Deyun Chen, Yuyuan Chu, Qingfeng Xu and Shi Xi (20112) " Research of web services security model base on SOAP information". Information Technology Journal, Vol. 11, No2. Pp 241-247.

[23] Hougbing Wang, Joshua Zhexue Huang, Yuzhong Qu and Junyuan Xie (2004) "Web Services: Problems and Future directions". Journal of Web Semantics, Vol. 1, Issue 1. Pp 309-320. Online at www.elsevier.com/locate/websem.

[24] Jalal Omer Atoun and Amer Jibril Qoralleh (2014) " A hybrid Techniques for SQL Injection Attacks Detection and Prevention". International Journal of Database Management System (IJDMS). Vol. 6, No. 1. Pp 21-28.

[25] Perumalsamy Ramasamy (2012) "SQL Injection Attacks Detection and Prevention". International Journal of Engineering Science and Technology. Vol.4, No. 4. Pp1396-14401.