J. Appl. Environ. Biol. Sci., 5(9)22-27, 2015

ISSN: 2090-4274
Journal of Applied Environmental and Biological Sciences
www.textroad.com

Analysis and Applications of Web Security Services through the Network Features

Muhammad Ismail Mohmand [1], David Young [2]

[1, 2]Department of Computer Science, School of Computer Science, University of Hertfordshire United Kingdom, UK.

Received: April 14, 2015
Accepted: July 30, 2015

ABSTRACT

In the field of computer networking the web security services (WSS) play very important rule in objects and the components highlight on the reusability by using the strategy apparatuses of the abstraction as well as separation of the trepidations. WSS has seemed as a preliminary impression to improve huge complicated and heterogeneous-distributed system effectively. Therefore they are combines the services-together to establish a system having a better impact power then other one. WSS are addresses need to standards based loosely-connected besides dispersed networking and that networking the protocol performance should be independent in all direction. But is not an easy task to ensure such secure-transaction of information in which is the crusade of information should be happens through the loosely-connected security services respectively.

Various numbers of methods have been projected to create a contemporary-literature in which is escorting the WSS implementation techniques in the disseminated systems. These important up to date methods offer the convinced benefits. However the posture of the some challenges-alongside for instance, use of Meta data as an outline as well as standard contract-documents of the security services designs and security-adviser. Therefore, some main objectives of this present up to date research work is deliver a comprehensive-analysis of the several methods are used to deliver the application-level security of the network features of the WSS. These methods have been likened based approaches on the integer parameters respectively. Furthermore we are critically analysis of various security services approaches are used in WSS. Study as well debates of the some future-directions are investigated.

***Index Terms*:** Application of the Network Security Services, Service-Oriented Architecture, and Cloud-Computing.

I. INTRODUCTION

Control systems engineering is well thought-out as one of most acute phase in web security services precisely in the network feature and development procedures. While in some cases if blunders are occurred in such requirement stages at that time they should be remain-undetected till the later-stages of the network establishment procedure [1]. Therefore the control systems engineering are addresses in the matters of the requirement-collection in which to plan as well as development of the desired networking policy. Control systems engineering has a direct-impact on the entirely and critical stages of the web security services in which are includes the design along with the implementation techniques have been proposed. Therefore the WSS architecture contracts with the requirement as well as expansion of abstract-level structure should be implemented. It contains of numerous architectural basics such as components as well as connectors. Which are collected in such technique that to be fulfil the serviceable and performance-requirements are described in [2]. Numerous architectural panaches are used in network features architects in which includes, layered data transmission systems, object oriented as well as implied supplication techniques respectively. Even though these such panaches is to deliver a sufficient-space of the architectural-choices. On the other hand posture challenges are architects that provide a realize trade-offs style of the particular-situation as well as environment procedures fully explain in [3].

Web security services (WSS), has been one of main absorbed parts of the recent research work, since in last three decade in which are provides the numerous clarifications by using such impression of amenities. Several scholars have been planned specific-models to modify such provision registry as well as configuration designed for its effective-working. Numerous microbes have been are investigated to the immovable all the way through life-cycle of the development produces. Furthermore novel approach on the bases of requirements is continuously shallow up to the completion process of the network features. The consequence in the sustaining of the significant-cost to the top of repairs of creation. Permissible to certify that the functionality and improvement performance of the security services should be satisfactory in in all domain to it to be integrated with the Web security services (WSS) is the solution of the problems in line for interoperable services-architecture respectively.

***Corresponding Author:** Muhammad Ismail Mohmand, Department of Computer Science, School of Computer Science, University of Hertfordshire United Kingdom, UK. muhammadismail1745@gmail.com.

Therefore, the improvement of the WSS request should be diverse in all from of the traditional network expansion in period of analysis as well as strategy techniques. WSS applications are involves the feeling analysis as well as design-phases. In the performance of the analysis phase the products amenities from of business-requirements in all directions. But in business psychoanalysts and service-architects are underline the convention of the standard refine services. The formal description of business-processes is significant in all respect with to the WSS. Testing and expansion phases of the WSS however they are alike to the network layers of the development processes are fully explain in [4].

Information security services some fact standards such as credentials, verification, approval, and confidentiality, which is the same implication in WSS based-applications. However, agile application of the WSS, which makes very challenging to the ensure-secure WSS application within groups in [5]. Therefore a very lesser-possibility should be occur for the successful-implementation of the secure network policy makers of the WSS with a precise data security services strategies [6, 7]. The light of the above facts and figure there are some important principles in arrears in the agile philosophy includes,

• Highest main concern is allocated to fulfil the buyer to the primary and incessant distribution of network layers of information are releases in all circles.
• The varying in requirements smooth getting on the development-phase. Therefore the agile process should be very couple variation for the customers' competitive-advantages.
• The performance and development layers of network features should be integrated with each other to establish a secure connection between the transmissions and distributions in all direction of information.
• They are provides the favourable environment and necessary support actions are needed for secure data of integration strategy.
• These vital process encourage the sustainable-development techniques for the sponsors' designers and user should be able to preserve the constant-pace of the indefinite period of information.
• In some continuous-attention to the practical brilliance in addition to the good quality design improves nimbleness.
• In architectures requirements as well as design of the surface from self-behaviour information are very essential for connection development policy.

Therefore we can puts some extreme-programming techniques to accent on communication. In this techniques the all stakeholders principally user's information and developers should be in one bench to establish link wise collaborative-team. So the performance of the extreme-programming should be have similar outcome results as compared to the jigsaw puzzle in which the information is passes in very small pieces of date towards the destination points. However the exact form of the individual pieces have no any sense whenever the host to destination points are combined together. They should be play a complete describe image of plan respectively. Therefore, some important astonishing aspects of that extreme-programming is its artless rules. They maybe seem to be unstylish as well as conceivably even-naive in first place. However in information of these arguments should be passes all respect of data in sound standard form principles procedures. The extreme-programming methodology is to improve the network data projection in three main ways such as communication, feedback, and simplicity. As well there are three basic rules for the extreme-programming techniques such as planning, coding, and testing. They are further divided into very small number of chunks and guidelines. The main focus of this paper we are only planning of the data and managing-rules of the network features of the extreme-programming.

Furthermore the conservation of such system is too cut down to the great-extent. They are streamlines some various phases of security services lifecycle. In firstly, we necessity to the model-requirement documents, so we can analyse as well as take part of the host artefacts. The creators to make sure wholeness and constancy of provided system by the generating-models by the requirements brochures. However these vital methods are by as well as large-classified into main three categories such classic-techniques, cognitive-techniques, and group-elicitation techniques as well as contextual-techniques. Such of these three main classes contains a set of numerous techniques, in which grouped-together on source of their mutual distinctive and individualities respectively.

Such these requirements of data flow into the host by which create a secure connection of scope. Therefore, the requirements process security services play a very important role on it. The data link should be connected are broadly-categorized into two main classes such as the user information connected media. The user information are normally procedures of the requirements of the system and the host data flowing in the selected layers towards the improvement of the selected system. There are maybe the number of system in which the data are passes to the selected host of the network features respectively to the requirements of the psychoanalysts, creators, coders, testers, designers, and graphic-designers are usually well thought-out as destination point of the user.

In this paper are categorized as follows, such as literature review on the bases of the application-level security services in the web security services WSS is completely explain in section II. After the literature survey

a very critical-analysis of several techniques are discussed in section III. And after this we finally present a short summary/conclusion as well as future direction of the whole paper in section VI.

II. LITERATURE REVIEW

In [8] highlight that such current implements are used for an alignment of the network security services possessions to that web security services offerings a technology-aspect. Where the user should be fulfil the gap in the middle of the configuration as well as security need manually respectively. In such information to the misconfiguration problem as well as the extra configuration-costs.

While [9, 15] are explained the requirements of the web security services should be all in fully control the levels of the network layers which is passing to the host to the destination point which are includes, monitoring, deploying, wrapping control, as well as discovering the fundamental programming of the checksum techniques some of the three most framework components which is fully describes on following.

(1) In web security services WSS specifications which are contains the functional as well as non-functional desires communication-style and it should be responsible for the its location on the web which used a language which is specified by web service definition language.

(2) While the performance of the web server is used for the requirements of the deploy web services respectively.

(3) They also specified the hidden layers of the network which are passing to the checksum development.

In [10, 2] are fully explained the data security-components for the web security services environments. Therefore these are based on the ISO/IEC 270022 2008 network security standard of the web security services design principles. Information security services are commands on the framework of the security control for web security services. Web security services follow the network layers principles which arrange for the developing-interoperable as well as agile service logic. While agile service logic are includes the performance composition of the discoverability and loose coupling abstraction. Therefore, some of the connected layers of the information security components are used to minimalize the network security methods.

While some contrast are found in [10, 11] which are state the flexibility as well as modularity of the network applications. However they underline the negative-impact of the security service procedures and the propose pattern approach is develop to the secure web security services applications respectively.

In [12] highlight the complex-nature of the security service policy which is lead the error prone and inefficient-creation of the web security services WSS. Some of these security configurations are used for the understanding of the security pattern techniques which is facilitates the fundamental framework work of the WSS. The security configurations is to cover such security services domain-expert information as well as local roots desired authentications of the system that gives the data about the relevant-security of fundamental structure. Therefore the information about the indigenous system direction as well gives a key storage-location and right to use criteria while web security services uses this facts for the creating enforceable-policy.

Software as a services and service oriented software engineering are explain the roots level of networking in [13] which is fully controls the checksum of the beginning points to the new models for the web security services WSS which is conveyed new security-challenges and perils of the entire structure of the systems. In this techniques the researchers are investigated the connection between in authenticates billing service and client in which is reduce the security peril of the encryption main algorithm performance.

In [14] preserve the wider-usages of the computer networking behaviour and its important performance demand for the motion based trust establishment along with the identity-exchange procedures. To establish this present up to date idea the researcher's draw an architectural patterns for the identity control system. They are able to share the information of the entire connection of host level to the service provider of the web security services and the identification confederation of the pattern centralize-administration and it should be responsible for secure data information in which to communicate identification information among the various security-domains respectively.

The researchers are explain in [15] that the performance and evaluations information of the security services backgrounds in which are based on the ISO/IEC 17798, 2005 standard in which is able to invention information of the security in WSS. In such assessment outcomes are shows the outlines are not capable to the information-security issues of the entire structure of the models.

In [16] the authors explain the unknown connected paths of the network which integrated to the web security services WSS and the security-vulnerabilities. They propose the background of the current-problems of web security services while such methods are pointed to element the implementation-structure as well as strategy of the WSS, both are play the importance behaviour to the network level configurations. While distributed denial of services and denial of services techniques should be qualify the performance of the WSS, at the application level to the design procedure of the network security service implementation.

In authors [17] confirm the current security planning are not well-matched with current-security approaches techniques. However they are responsible lead the redundant-development of the security examples

as well as it should give the applicable facts to such security performance process respectively. Such projected models are offerings the security facts to the related to various planning for the different opinions such as security integration techniques along with security services interpretations.

In [18, 24] the author is more emphasis on the improving such existing-approaches for the web security service within the applications of the e-businesses. Which delivered comprehensive and standard framework features of the networks such as business oriented framework for enhancing web services security (BOF4EWSS) approach [20, 23]. Therefore this current approach is mainly-concentrates on the appreciative and pointing the present inter an organizational complication which is get up due to the e-businesses.

In researchers are investigated in [19, 22] that e-business processes are examples in which clarify workflows at a very high-level in which support e-business predictors as well as verify e-business requests respectively. These replicas as well exemplify the fundamental-objects in which is relations and connected roots to network supplier's services oriented-architecture [21]. These current replicas are establishing members and contend grounded numerical individualities to describe and explain the hidden paths of the characteristics information. They establish a policy makers models are proposed in which association and join security requirements as well as plan the consequences of the various entities such as data-transfer and interactions in which is explain the aims of the web security services requirements [25, 15].

In the recent-technological improvement as well as expansion of the innovative standards have been information of creation of novel approaches for the conniving and expansion of web security services applications in all direction of information. The web security services some applications connected through the individualistically distributed web security mechanisms. A system in which propensity of the take part of the multiple WSS is mechanically is transparent in which are passes all data from the final destination points of the security service oriented-system.

III. CRITICAL EVALUATIONS

Critical evaluations of the various approaches such as framework techniques and its necessary policies that are projected for addressing of the security related issues in the WSS, is as long as in this piece of work. Therefore, behaviour of the critical evaluations which are based on some underline parameters which are following, proposed method, in which model used, key addressed and its listed benefits. Whole performance of the critical evaluations is presented in the following Table 1 respectively.

The critical evaluations of the Network security issue in web security services WSS.

References	Suggested Method	Model Used	Key Addressed	Excellence	Performance
[8, 20, 25]	Model-driven in security service configuration.	Network security and web security services viewpoints	Security requirements for gap among security requirements and configurations policy.	Configuration of the network security requirement for the WSS.	Fully command on the network layers to checksum policy.
[9, 10, 21]	Data framework	Web service definition language	Web security services development policy	Minimize the time and cost for web service.	Hidden path of the security service is initiated.
[11, 12, 7]	security comparison framework for ISO 27008 2005	ISO 27008 2005	Framework implementation control and developing guidelines for the effective data security issue	Protect the vulnerable	Implementation strategy are explain in all aspects.
[13, 14]	Web security service based approach	Checksum policy for network layers	Reduce the network security challenging's	Applied in all selected path	Reduce the security behaviour
[15,16]	Encryption data information algorithm	In Matlab, or other open resources	For avoid the uncertain change in the network	The common format for standard implementation security domain in the web service behaviour.	Data flow in the exact form to the host and destination points.
[17, 18]	Network layers of the ISO standard 17793 2005	ISO 17793 2005 controls	Evaluate the SOA governance framework.	Comparison of the hidden path and checksum security issues	The policy pattern for WS policy and WS-security.

IV. CONCLUSIONS

Web security service as a whole process is very complex process as well as on the top of it and some basic requirements is keep the varying throughout the network layers phase. Security service configuration-management are take place most acute part of its requirements doing the considerable-modification in the

hidden parts of the network layers and code technique. The web security services expansion procedure delivers a clarification to the changing-environment. Changing the requirements of the acute phase of the network layer is fully explain the entire process of the security service development process and the requirements of the open layers issue in collected works for the various periods.

Due to the nature of the web security services is quiet difficult to make certain the secure-implementation of web security services surrounded by the organization. In this paper we are fully concentrate for the exertion to make available a survey of concepts-related to the various techniques such as practices and WSS frameworks. Therefore on the fact and figure basis of this research work we are able to conclude the security-standard such as authentication, identifications, and authorization should be more and more challenging environments for the implementation level of the network identifications strategy. The most important techniques are proposed in literature survey which is focus on the security patterns that give some elementary concepts as well as understanding the secure network security domain. To facilitate the implementation performance of the network security patterns should be very successfully for the further-automation as well as enhancements in the model.

REFERENCES

[1] A.K, Khan, N. A., Khalida. Review of Requirements Management Issues in Software Development. International Journal of Modern Education and Computer Science, 4(3) August 2013.

[2] An active Endpoints. BPEL Open Source Engine. Active BPEL Community Edition for the updated theory of the BPEL Engine. Active Endpoints. Available online at http://www.activevos.com/community open source. php,

[3] H.L. Aguilar Savon. The business process modelling, Review and framework. International Journal of Production Economics, volume number 90(3)129-149.

[4] D, Albert and A. Doro fee. Managing of Information Security Risks, The OCTAVE Approach *Addison* Wesley, and Boston May, 2003.

[5] J, Alonso, F. Cassata, K. Kino, and U. Maharaja. Web security Services and important Concepts, and Applications. Springer Verilog Berlin, August, 2004.

[6] Anonymous, For WSS-CDL Eclipse Network security theory actions and its application. Available online the http://wscdleclipse.sourceforge.net/main.htm

[7] H. Baker, E. Smith, and N. Watson. The Information security risks in networks in the e-supply chain. Pages 44-55. Idea Group Inc. Hershey PA, 2007.

[8] C.G, Baldwin, Y. Bares, S. Shia, and L. Kearney. A model based approach to trust security and assurance. BT Technology Journal, 25(3), 44-70, 2008.

[9] B. Barbie, D. Hobbs, F. Bettino, L. Hirsch, and M. Martino. Challenges of testing web services and security in soak implementation. In L. Barresi and E. Dinettes, editor, *Test and Analysis of Web Services,* pages 278-342. Springer Heidelberg 2009.

[10] BE Systems, BMC Software, IBM, Layer 7 Technologies Microsoft, Novell, and VeriSign. Web security services implementation and its federation of instructions language, 2008. http://www.ibm.com/developerworks/library/specification/ws-fed/

[11] R. Beady, H. Sabra, S. El-Kansas, Y. Hanna, and Y. Youssef. Nudity. Web services firewall. In *IEEE International Conference on Web Services,* pages 598-610, Orlando, Florida, 2006.

[12] V. Belton and T. J. Stewart. *Multiple Criteria Decision Analysis: An Integrated Approach.* Kluwer Academic Publishers, Boston, 2003.

[13] D, G. Berg. *Qualitative research methods for the social sciences.* Pearson International Education, London, fifth edition, 2003.

[14] E. Beckman. B2B PARTNERSHIPS SECURITY - How to Practice Safe

B2B. Available online. http://www.cso.com.au/article/80707/howpractismsafmb2b

[15] L. Beznosovy, K. J. Flynn, L. Kawamoto, and C. Hartman. Introduction to web services and their security. *Information Security Technical Report,* 9(4), 3-20, 2005.

[16] K. Bhargava, R. Coring, C. Fount, and A. D. Gordon. Secure sessions for web services *ACM Transactions on Information and System Security,* 9(3) , 2007.

[17] B. W. Boehm. A spiral model of software development and enhancement. *Computer,* 21(4), 71-74, June, 2000.

[18] R. J. Bandello. Web services and web services security. *Communications of the Association for Information Systems,* 10(22), 322-340, 2005.

[19] H.-J. Bollinger, K.-P. Fahnricsh, and T. Mirren. Service engineering, methodical development of new service products. *International Journal of Production Economics,* 76(2), 273-284, 2004.

[20] A, Calder and S, Watkins. *IT Governance: A Manager's Guide to Data Security and ISO 27001/ISO/IFC 27002.* Kegan Page Limited London fourth edition March 2009.

[21] L. Camborne, J. Diaz, G. Pardo, and V. Valero. Using UML diagrams to model real time web security services. In *Second International Conference on Internet and Web Applications and Services,* 2008.

[22] M. Cambornee, G. Diaaz, J. Parado, V. Valearo, and F. L. Playa. RT- UML for modelling real-time web services. In *IEEE Services Computing Workshops,* pages 133-145, 2009.

[23] E. Ceramic. *Web Services Essentials.* O'Reilly, Farnham, July, 2004.

[24] M. Crepe and G. Varner. Prototyping: some new results. *Information and Software Technology,* 39(22), 654-674, 2006.

[25] CERT Coordination Centre CERT. OCTAVE information security risk evaluation. Available online at: http://www.cert.org/octave/.