IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 1, Ver. I (Jan – Feb. 2016), PP 57-68
www.iosrjournals.org

A Business Oriented Framework For Enhancing Web Security Service (BOF4EWSS) Network And Features For E-Businesses Classification Techniques.

Muhammad Ismail Mohmand [1], David Young[2], Cress Bowerman[3], Irvin Philip [4]
[1, 2, 3]*Department of Computer Science, School of Computer Science, University of Hertfordshire, United Kingdom, UK.*
[4] *Department of Computing, School of Computing Science, University of the West of Scotland, United Kingdom, UK.*

Abstract: *In the field of web security service is an extremely complex and very contemporary issue. As soon as the considering this current technology suite to assist the interacting e-businesses challenges for security become even more and more elusive. To attempting the addresses of these current problems. In this research suggests a business-oriented framework for enhancing web security service (BOF4EWSS), is a complementary issue for the network features in the e-business. Importance of the BOF4EWSS, is its prominence on the tool supported in partnership for the e-businesses are comprehensive security related solution for their service of interaction techniques. And the tool businesses in the use of its applications of the BOF4EWSS two essential framework phases respectively.*
To assess the BOF4EWSS as well as its supporting tool in a two-step methodology was adopted. In firstly the solution model as well as tool were tested for network features compatibility with existing security services approaches in real world circumstances. Approach envisioned that can be used in e-businesses in the joint manner in which to achieve comprehensive-concern of the web security services of the network and features environment.And in secondly the framework as well as tool were assessed using the industry based security services professionals are experts in this field. Then we compare the results of both these evaluations indicated to the suitability as well as strength of the framework features, model and tool suggestions as an innovative as well as significant contributions to the current research field.
Keywords: *Web Security Service (WSS), Composition Architecture Techniques, and BOF4EWSS.*

I. Introduction

The information of the e-businesses has develop of fastest-growing worth of the conducting businesses in the today's economies. In the achieving of the online business to business collaborations in the middle of e-businesses and use of services oriented computing by-way of the web security services through the network and features technologies are playing the progressively important starring role of communication system techniques [1]. Therefore the novel benefits are rooted in the aptitude to countenance for the seamless-integration of the businesses process across the disparate enterprises in which to use of the standardized-protocols as well as the open technologies conformation techniques in all direction of information in [2]. The web security services use increases the lock up these services-becomes of the extreme reputation performance.

In an effort to the addresses of the new established security-challenges becomes accompanying the web security services standard setting forms have been proposed for the several ground breaking principles. As the web security services matures move from of the lower-level security information for instance principles and technologies to the higher-level concerns on the other hand, is the imminent information techniques respectively [3, 4]. The security regardless of context is the multi-layered and phenomenon-encompassing features of its practices procedures as well as approaches. The main and essential factor is the factual with the web security services is the comprehensive substantially-complicates of the security communication environments for the e-businesses are safe and secure [5].

Considering this, and with special appreciation of the inter-organizational security issue now facing businesses interacting using WS, our research focuses on identifying a novel, business-oriented approach to guide companies achieving agreed security levels. The approach envisioned that can be used in e-businesses in the united manner in which to achieve comprehensive-concern of the web security services of the network and features environment.

The essentials portions of this paper is organized as keep an eye on:

The section two covers a brief-review of the web security services for the advancements in the network and features for e-businesses with intention of the identifying-outstanding security issues and stone work way for this current research techniques. The next in section three is about the overview of projected business

oriented framework together with its innovation as well as use is specified. And the conclusion as well as future-work are outlined in section four respectively.

II. Web Security Services Within The E-Businesses

2.1 The State of Art Techniques

Although the promising facilitating technologies for e-businesses, web security services practice comes at high-price of unbalanced safe keeping groundwork. The literature-identifies various experiments [3, 5]. But most of the relevant for this current research, is authenticity that the web security services enhances important complication to e-businesses security background [5]. Thus it's making the safe keeping on much comprehensive as well as comprehensive concerns which wounds across business-lines much relaxed as well as more rapidly than previously. As such an insufficient formation of the network links carriage in one business can mean augmented real time security-risk for its partners as well as both instant and protracted.

To addresses of new established security challenges-mentioned in above groups for instance the organization for advancement of the structural information and standards OASIS, and world wide web consortium W3C, have industrialised as well as ratified-numerous ground breaking standards [7]. These important standards aims to in cooperation to solve the unseen problems produced by common-threats as well as also for further web security services example by the allowing substantially, more-dynamic security communications among the services as well. Elsewhere the addressing of perceived-inadequacies of present standard base researchers, are currently directing the more and more general mechanisms of the web security services solutions for instance best-practices and processes techniques of the network and features communication through the BOF4EWSS. These significant movements stretch the life to the guess by the National Institute of Standards and Technology NIST, which are highlighted that the web security services technologies matured as well as methodologies should be recommended-practices for safe keeping would become, the next-step in objective of the emerging protected classifications [8].

While some of most pertinent as well as significant applications concentrating on these higher-layers which are builds on the existing-technologies as well as theory of aspect oriented programming to which provide the back ground for the securing web security services compositions by using the network policy standards [9] which aims to deliver the systematic development, approach for the creating security styles for web security services based systems [10]. And lastly event-driven framework for service oriented computing [11], a normal agnostic and multi-layered background that goals to addresses the problems of the essential as well as applying access control-rules for the securing of the web services uses at high level of business-processes as well as more focus on the dynamic-authorization as well as an independent of the specific standards techniques respectively [12].

2.2. An Outstanding Security Issues Techniques

The web security services methods should to objective to be detailed in planning developing as well as keep up an ample clarification. The standard security components-encompass technologies nevertheless, the recent collected works in [12] in study of the web security services has becomes an emphasized they are also includes the policies, process, as well as best-practices. Therefore the very alluring to regards such as the mechanisms as a solution to web security services problem itself. While the work of the recent scientists are appreciated to the building-security as well as the trust be not the form of entire solutions. In fact all of these essential devices addresses are technologies layers of the security and intimidations which is originate at exact level that are providing the stepping stone in formation of the aim of the comprehensive and multi-layered security techniques in BOF4EWSS. In this viewpoint is sustained by [2], as the identifying task such as operational risk management and defence in depth, through the security engineering of the critical developing robust secure-systems.

Therefore as conflicting to the benefiting of the web security services plethora of the sometimes overlapping-standards in the end confuses developers, and as the act to the complicated secured business to business implementation techniques respectively. Importance of these issues are puffed up when, the assessing use of the web security services for the multifaceted field of the e-businesses.

Their key limitation however, is that to consider the importance of the security-predominantly from one of the company's internal-viewpoint such as a company do it on the inside to secure-itself. This is too highly isolated and perspective an insufficient in line for to the nature of the web security services and very high-degrees of interconnection among the businesses. The spanning-exposure of the bequest system to purpose built of the web applications. Looking away from these advancements an interesting inquiries region which has established a little-emphasis at level of the cross enterprise interaction. Specifically, we are refers to providing some comprehensive-approach in which to aid the businesses in all together management security as broad inter organizational anxiety.

This current approach would be not exclusively at technical-level but, look at usually at numerous other important fundamental-aspects that e-businesses should be mutually consider when the appealing in business to business interactions-employing of the web security services. The following sections presents the current-research intelligent for this approach.

III. Bof4ewss

3.1 Basic Overview

The BOF4WSS presented in the figure 3.1 was considered to addresses of outstanding-security issues, identified and strengthen available, and trust solution. These frameworks consist of nine basic and essentials stages which in general semantically-resemble are found in the form of typical system development-methodologies. Formally, these important stages are requirements elicitation, negotiations, agreements, analysis, agreements, systems design, and agreements for quality-of- services, development as well as Testing and maintenance phases which are compared to the typical methodologies negotiations and agreements stages plays a novel roles of its communications. Their inclusions should be developed in all directions of crucial in the BOF4EWSS, noting cross enterprise natures of developments and imperatives needs to discuss negotiates and agrees on clear and individual path forward techniques respectively.

Requirements Elicitation Phase
Negotiations Phase
Agreements Phase
Architectural Phase
Agreements (Network Features) Phase
Systems Design Phase
Agreements (for QoS) Phase
Development and Testing Phase
Maintenance Phase

Figure 3.1, BOF4EWSS brief overview.

Waterfall Model methodologies in [13], in particulars of its main influences for framework designs as well as it can be seen of the comparing the framework phases to the Waterfall Model for example system feasibility, study requirements analysis as well as project planning system design detailed design coding testing in addition to integration installations and maintenances [14] depending on articles sourced stages of Waterfall Model may be namely the differently referenced because, of its detailed-view of typical Waterfall Model tasks. Waterfall Model was more preferred to the other some essentials methodologies for example prototyping, [15] as well as spirals [6], and object oriented [8] approaches to the transparent well organized highly documented in addition to strongly-disciplined process should be bring a large inter organizational developments project. These some practitioners views structures possible with Waterfall Model ideal fit, for corporates world in addition to the basic reasons respectively.

With appreciations of flexibility in addition to quick turnaround, benefits of ageless as well as more lightweight, methods these are also considered in the full lengths techniques were chosen for its framework foundation however because literature does not advises them in this current situations of the large development projects where development, teams different place in addition to dealing with complication of the interaction with other some updated hardware and software in the critical system development techniques as well. Despised the benefits listed it is accepted, that Waterfall Model does have short comings as well as criticism. For example researchers have known that it lack flexibility in original-model when traversing stages, as well as freezes-requirements early communications techniques with network features parameters [13]. To compensate, for the concerns BOF4EWSS, allows for flexibility-through bottom up progressions as well as feedbacks respectively. Additionally even though requirements, are indomitable early the checksum policy layers should be higher level requirement which may changes at subsequent stages-closer to designs.

Fundamental of the both points in the above is emphasis BOF4EWSS, places on involvements of key stakeholder throughput's entire-process to ensures gathering as well as circulations of necessary information making of the changes information's.

Prime novelty, in BOF4WESS, is found in the emphasis on the providing as well as collaborative-development methodologies for the communications which focus on web security services. This methodology, would be more accommodated to the multiple-autonomous business on the working should be together of the address outstanding issues from of BOF4EWSS, aims to considering full nature of web security services as well as its security implications, within e-business appreciating the real time inter organizational security issues now face by interacting e-businesses as well as finally promoting of use a collaborative-approach to provides

enhanced level of security as well as trusts.

As seen below the framework as well as its phases, give detailed-guidance on its relevance in the attaining-desired level of holistic-security for network features policy external interaction with a company, simply mean interaction that occurs in transit as well as to some extent, occurs regarding to basic requirements of the security interactions being processed, by business-partners. The internal in addition to external focus should be revisited in the various points of the BOF4EWSS presentations.

Returning, to the points regarding detail guidance's given by framework this will involve-defining expected inputs, to stages along with the upcoming of their required outputs but especially, recommended low level goals activities as well as step within those stages should be more helpful for achieving outcomes as well as more suitable for the guidance aim to references in addition to reuse existing-methods as well as practices, for both from industry in addition academia as well as thus concentrating, on the compilation coherent well defined process as well.

Another main, designs goals of framework to utilize Waterfall Model specifications as well as tool wherever in addition to whenever useful techniques as well. This include validated proposal from the research-community to the choices to provides companies that adopted in the BOF4WSS, with the practical methodology, that pull together with the web security services specifications in addition to tool from the plethora, of technologies-available. Furthermore, this shows exactly, to how they can fit, into developments of the web security service solutions. To date author, is not awareness of broad-methodology as a BOF4WSS which aim of the critical pieces from of the web security services in the contexts of the cross enterprise highly structured extensible business oriented framework in details [3].

To supports largely textual descriptions of the framework activities next number of diagrams, are included-illustrating each stages in addition to its respective-workflow. Since web security services issues are the central concerns the BOF4EWSSdiscussion concentrate primarily on the aspect rather than isolated discourses on functionally as well as quality-related aspects of the requirement in this regards refer to non-functional requirement excluding security for example performance as well as scalability. At this stage however in interest of completeness this chapter doe's give to all relevant information will be passes to the BOF4EWSS on the some guidance on the requested paths between the transmission and receiver areas of the all communications techniques respectively. This is particularly, when they related to the useful information of the web security services standard and technology.

Lastly BOF4EWSS, assume that business have previously-agreed to the use of the web security services in which supports generally-defined businesses scenario in all aspects. In other words broad consequence is known in the form of the BOF4EWSS tasks therefore, is to provide the performances of the methodologies for its planning developments in addition to implementations some the importance below the framework stages are presented in this paper.

Requirement elicitation phaseis the first-stage in addition to within it each-company work largely by itself as well. As with typical-system development approaches phase involve the actual connections of the network features to which analysing internal business, objectives constraints security policies as well as relevant law and regulation to determine the network policy in clearly their high level need for expected web security services businesses scenario respectively.

First implicates but crucial steps therefore, is to organizing the team within business to work on requested projects strategy as well in directions of communications in which is need to dedicated-exclusively to this project, but should be committed, in addition to have clear idea of goal of envisioned-scenario. Ideally these team will be consists of the some top executives domain experts of the network security layers in the hidden paths of the checksum policy as well.Generally these new processes which will be expected on the high level as well as mainly cover internal along with the external operations techniques respectively. For example if they will be passes to the external processes, with other company, are known as the prior transactions business may not be able to developing the initial medium level processes flow which encompasses external interaction. In either case occasional communication with businesses partner is require to the enable of the useful process to be defined in all aspects of the communication is suggested for reasons previously, given in addition to particularly, because these high level model can be used for the formation as well to explain the discussions in the negotiations phase as well as fact it adequately-enables high medium level process to be defined in the network features. True to envisioned-flexibility of the BOF4WSS, however companies are free of its software iodation techniques modelling-language of preferences.

While in the last task in approach which fully concentrate in [5] is actual requirement determinations. This is accomplished, through analysis, of the newly-defined process models as well as business-analyst in addition to domain expert can directs this tasks. By assessing, inputs along with output as well as tasks involved general requirement for each stages of process should be fully defined in the form of the high levels parameters in all directions.

For quality-requirements in particular, it is understood that may be hard states this early in addition to

this rather high-level. Business however, should to make an efforts to gives some ideas of their desire for systems quality parameter. To elicit, security specific requirements, author mainly suggests analysis of access-restrictions of actors on the processes as well as processed input and output. This is the information-security specialist on the teams will be involve in the given last two stages BOF4EWSS, heavily involves previously-highlighted stakeholders information techniques.

In addition, to security requirement identified framework strongly-suggests the performances techniques scenario risks assessments to provide more-extensive security documentations. This assessment as opposed to one above, which focus on the primarily, on access-restrictions in the processes techniques enables a comprehensive security driven scenarios analysis parameters in all conditions. The assessments is strongly suggested-primarily to combat unfortunates reality of the high level left alone significates number of the business would be able to carry out from the formal-security risk assessment to identify-key risk faced in the whole process techniques [10, 20].To aid assessments process there are ranges of the method that the security-specialists of companies, might be use the for the performances degradation of the BOF4EWSS suggest well documented in addition to internationally-validated technique for example UDDI and NIST along with the risk management guide [19] for the formation of the operationally critical threat asset and vulnerability valuation [14] as well as the information security risk analysis method [9] and risk analysis which are totally based on the business-model techniques of the hidden paths respectively [11].

Generally some of crucial factor considered in the given chosen techniques should including the assets threats vulnerabilities risks in addition to their priority levels of the organizational-security policies in all directions of the listed highlighted parameters pertinent, laws along with regulations security budget as well as network features security goal expected, of the new businesses partner's communications.All of those important factors-listed above, significantly determination of security action as well as security requirement that should be more and more factored during these envisioned, web security services communications techniques. Throughout, this report of the network featuresis defined, as any way, in which a company-treats a risks it faces whereas web security services is a high to medium level desire expressed, to protect-against risk techniques as well. Security action therefore, encompass-security requirement. An action is of risk of ensuring security of server to server communication techniques should be outsourced. A requirements however, could be integrity of the huge data communication links of the personal data must be, maintained in directions respectively.Requirement to be carried forwards and it should be particularly addresses area that need additional-security internally as well as related to the interaction with pass it through the businesses partners. After these-requirements have been gathered they are added to previously identified, requirement in addition to documented in which are provides the stage outputs of the network layers.

Negotiation phasenext teams consisting, of project managers business in addition to systems analysts domain expert as well as to the information technologies security professional from companies meet bringing together, their requirement from the previous-phase for the upcoming discussions in details which workflow techniques respectively. The purposed is to use the stages input as a basses to charts an agreed paths forwards in term of scenarios requirement in addition to high to medium levels processes definition. As compared, to typical developments method for example waterfowl model BOF4EWSS, explicitly include negotiations as the phase to stresses its importance inter organizational scenario in all directions of communications parameters. Especially noting varying expectation each companies are likely to be have toward security itself. Expectation could vary, with regards to whether, a process need to be secured to what level, it is to be secured how security, will be applied for the network features [7].

Two main as well as tasks for this phase therefore discussion in addition to negotiation on functional as well as quality, requirements and then security-requirements in addition to action that arise as well. Which are depending on preference of business using the framework latter of these tasks, may include joint risks analysis-aimed at identifying, any risk not be conceived, previously. The deliberations on statutory in addition to regulatory-requirements are especially, important when discussing, security as business may in the same industry country problems in positions. Where necessary as is seen in workflow backward progressions from the security-requirements definitions to functional requirements definition is allow. This is mainly, to supports balancing in between functional as well as security action in addition to requirements techniques as well.

Agreement phaseis to build on concluded negotiations, in addition to initially-advocates legal contracts to solidify understanding of requirement between-companies for the network features of the BOF4WSS communications techniques. A legal, agreements at this point, is not compulsory, however appreciated that of its business may chooses to include contracts at to the stages. These provides some basic reasons the contracts is suggest here is creates safety-net for the both companies, during these early stages, of planning in addition to negotiation. The contracts would focuses on two main aspects such as binding parties of the negotiation for possibly-future businesses interaction for good faith in addition to secondly defining groundwork in more comprehensive-contract to follow the later stages in all sections. Initial agreements and definitions of need in the negotiations phase makes, latter of these-tasks less arduous is to be so on.

These will plays a basics contracts roles for the followed by interaction security strategy ISS which in itself, is novel-contribution to the research directions. As opposed the legal documents above ISS is the rigid management's structures that define high level cross enterprises security directive to guides interactions in addition to relevant security decision internal-to-companies. These important directives, are typically in form of the web services security strategies policies procedures best practices in addition to objectives as well in the communications policy. The novelty, in ISS is the provisions of more and more in the pragmatic security-governance structures for the companies in which to provide the appreciates variety of important, factor in addition to is not stated, in the rigid hard to understands and follow contractual term. Formally ISS can be seen, to builds on as well as considerably-extend ideas of cross enterprise policy introduce in [17, 9].

The basic requirements in the central-activities in creations of the ISS, such as very-restating business mutual goal for the scenarios this will provides clear visions for the strategy as well as actual definitions of security strategy directives. In additions to use of its basic requirements as well as business constraints when defining these directives, framework suggest considerations of two main and essential aspects for the formations of the hidden paths. These are legal in addition to regulatory mandates, which may influence-companies in addition to interactions and secondly best practices of the web services security standards, available from of the industry in which are discussed in details.

In businesses today legalese and regulators requirement pertaining to the security are becoming-increasingly important especially within arena of the online businesses. These mandatory-requirements covers topic for example data protection strategy to the data privacy of the listed computer misuse as well as the incidents disclosures and notifications third party auditing in addition to even security, within businesses relationship. The aims of ISS with regard of such requirements is the mainly to stresses that business makes themselves awakes of content of these laws as well as regulations techniques of the network features as well. This is not, only to fulfils statutory need but also because, a numbers of these laws stresses principles of good reliable security, that should to the experienced by corporations.

Some of most relevant laws to the huge formations as well as considered in which are includes some essentials techniques are shown for the Sarbanes oxley act (SOX), of 2012 of the united states emphasizes as well as maintenances of adequate the internal control to ensures the accuracy of the financial-information [4]. The health insurance privacy and portability act of 1999 of the united states which are more and more focuses on the confidentiality techniques to the integrity in addition to availability of the personal data information to the network features ensuring protected while the storage in addition to during, transmission both within in addition to external to company infrastructure policy [12]. Data protection act of 2002 in United Kingdom should to be targeted toward personal data ensuring, that to adequate accurate as well as processed, fairly in addition to lawfully amongst other some important things [11]. The gramm leach bliley act (GLB), of 2006 again the united states are mainly aimed to the financial institutions as well as stresses activities for example evaluation of information technology techniques environments, to understand, their security risks establishments of security policy to assess as well as controls risks as well as scrutiny of businesses relationship to ensure partner have adequate-security in [12] which is to transferred knowledge of and adherences to these regulation critical companies looks to be conduct businesses in the increasingly-regulated marketplace positions will be very high as compared to the other basic techniques of information technology as well.

In additions to promoting compliance, with legal in addition to regulatory requirements the web security services emphasizes incorporations of best practices standard in approach by company toward inter organizational security while it maybe the tempting of the assumes such business already-accommodate for examples standards of the recent technology shown that to be the companies largely not aware, of key formation to the web security services guidelines [7, 2].ISO 2700 series is the perfect example, of the important standard they form key inputs into this frameworks stages. This standard set in particular is targeted at provisions of the internationally, recognized organization independent-framework for the effective to the extensive-information of the security managements [19, 11] while the internal security managements systems for the organizations are fundamental objectives of those principles setup techniques in all directions of communications [22,14].

Architecturalphase techniquesworkflow on the given the various phases are purposed is to enable-companies to takes agreed-requirements in addition to defined conceptual-secured businesses process model for foreseen-interactions. These form of models are expected, to very clear on encompass, not only high level company to company processes flow but each of the company internal processes flow that constituted parts of the general-business scenario of the BOF4WESS. The internal process definitions in addition to sharing the encouraged, to cultivate atmosphere, of the open companies but especially, to makes companies-properly analyses as well as expected-internal flow in addition to the general scenario of the given formation. At this point should be more relatively-easy for the companies to create the quality of the business in which to makes any necessary-updates.

Since the almost-certain that the top class communication to the businesses, would have engaged, in the process-modelling of the some point, before teams businesses as well as the system analysis is to be likely more

and more preferred-techniques. As the upcoming result of this first main and essential task to given phase is agreeing, on techniques that they, will be used for all forms of communication strategy sudation's. Therefore to define such medium level businesses processes models needed various standards modelling-techniques are available on the checksums policy maker solution on [5 , 12, 22], for projects team to use in addition to analysis as well as domain expert is the key-personnel to the present stages. While some of most popular, of these which to use as data flow diagrams as well as the integration definition for function modelling techniques and business process modelling notation. The Universal Modelling Language 2.0.1 extensions for Service Architectural Analysis [17] is the recent proposals from of the current research techniques in which also provides, the interesting-technique. The profile however, appear as well as targeted to the services orchestrations. Another options in the Universal Modelling Language profile which is [90] for the web security services compositions could be very useful, because the main design-goal is inclusion transformation rule that allows designed Universal Modelling Language model to be transformed, to Universal Modelling Language composition that are executable, for the necessary tasks in the future stages of the web security services parameters.Companies discussion on the modelling techniques, should be the goal of every phase that is definitions of secured, medium level processes model facts that these-models have to be decomposed in addition to express the varying aspect every path in the lower level in addition to therefore, having standards way to states these aspect may be beneficial as well as impending, need to translated these, models into the Universal Modelling Language as well as the web security specific formats for external as well as internal usage communication respectively [18, 3].Regarding of last two upcoming points of the e-business such as might-find it useful, to know about the network features classifications of the checksum policy maker of the BOF4EWSS communications which are proposed to the extensions to Universal Modelling Language to the account for the security pupation techniques. Furthermore with highly-esteemed option like Universal Modelling Language and web security services there are mechanisms-publicized that can be translated these medium level models to the web security services in specific language as will, to be seen in the subsequent-sections.**Agreements phase techniques** respective, workflow, can be view in agreements in form of more thorough legal-contract reflecting, detailed expectation of parties, include in envisaged scenarios. The businesses rule and constraints functional-requirements in addition to the security requirement for all factors into the basic contract of information policy. The medium level requirement is especially, important as to provide for further details on agreed interaction. As in previous contract businesses and systems analysts have roles of ensuring businesses requirement as well as need are transferred-adequately into legally binding of the basic agreement while web security service professional act to checksum of the network features requirements [20].During these contracts drafting requirements may not be change in addition to therefore, any updates, made can back into the basic communication of the businesses known as requirement as well as process model approach techniques.Again this legal documents are used in the primarily biases in form of safety nets of the current features information to the business interaction through the network topology of the BOF4WSS techniques as well as therefore still relinquishes, roles of the governing to the day to day web security services interaction to ISS respectively.

Many of the current authors in [14] supports these in addition to similar views as well as defines the number of current drawbacks in which using the contract as sole of the basis for the conducting business techniques in all directions of the information as well.**Design phases**is analogous, to a company internal system design processes techniques for the present in the current pupation in [14] as well as therefore target the definition, of a low level systems related views of exactly how it will be played an excellent conceptual model, from architectural phases will be put, in the same place parameter techniques.The first-activity is for team from each businesses techniques of the network features communication in which to jointly define, low level processes model. The system analysts within parameter performances teams should, be involved for the promotion points as they, will have more practical in addition to low level orientations toward the model. The framework advises-businesses in the reuse of modelling-technique chosen before in the architectural phases but, on this iteration to break down medium level model to lowest levels of details. The goal, is to decompose-models such as in the BOF4EWSS that the individual-message flows between companies, as well as specific task which constitutes of each process-activity can be seen in the upcoming layers of the hidden paths of the communication layers.**Agreement for quality of services**it's a low level process design and service level interaction defined for now concentrate on the agreements necessary, at the quality of services level. During the tasks goal is to actually-specify the mutual understanding, of the priorities responsibilities as well as guarantees, expected by each businesses with respect to other entity regarding actual value of the web security services. This phase directly extend preparatory work, on quality requirements, in the design phase and result in a set of formal in addition to contractual agreement.As done so the quality of services requirements, typically assessed include, service availability need performances requirements in addition to so on. Besides, quality requirements process design as well as service interaction is the necessary, for input because, they too needs to be considered, in defining-appropriate to the quality of service level for services as well as system.To specify quality of service level requirements agreed business executive's analysts as well as lawyers, have a few important alternatives.

The first, in addition to most common-option is the contractual natural-language agreements referred to as the service level agreement. service level agreements date back to many-years before the web security services as well as since their inception, have proved useful mechanisms to defines the levels of service, in the measurable way as well as penalties,, where agreed level are not fulfilled in the service level agreement. For web security services and the service level agreement will have same usage in addition to general mode, of applications. The only difference, maybe occurs in how service is monitored as more web security services specific tool and techniques, are likely to be employed, which enable increased-granularity as well as efficiency, in monitoring policy as well. For more details, on service level agreements and what, can be include in the web security services context BOF4EWSS direct companies to references [5, 21].

Another options is to makes used of accept policy standard such as web security services policy to specify the service quality requirement [16]. This method, however, is ideally suited, for dynamic-interactions where quality requirement greatly-influence the services as well as service provider chosen, for use. In the last noteworthy, approaches is the web services level agreement framework-described by keller as well as Ludwig in his article in [22]. Broadly this framework allow for the technical-specification as well as monitoring, of service level agreement for the web security services. It enable service user as well as provide in BOF4EWSS context to define the variety of service level agreement specify the service level agreement parameter and the method, for their measurement as well as finally related them to the implementation-systems. Implementation of the web services level agreement framework, have been builds in addition to be available, for use in the some of the IBM products, in[19, 18].

Testing and development phasehaving, discussed how service as well as system would interact, in the cross enterprise context this phase which on the actual development implementations deployments in addition to testing of services as well as systems in companies because of this factor is mainly carried out, by companies-individually. This involves, all member of the projects teams from, each company-working on their, own system development as well as this developments would be guide by previous company agreement. Occasional to the even prolonged-joint interaction is the however, greatly appreciated-especially for the services testing and web services level agreement framework updates troubleshooting and system verification to the requirement establish in previous-framework phases as well.

All inputs, to this phases are to be used, by companies in addition their developments teams to steer internal system implementations. It is stress that even-though testing is present in the last company maybe chooses to do some important testing as the service and system is development.Unlike, some of previous task covered in the BOF4EWSS activities, for the developments stages appears to be somewhat, well established in literature, as well as practices. This is consistent, with this research arguments regarding to the significant focus, on the technology based and oriented solution. The benefits of this to framework, is that there, are a variety of the tested developments processes techniques for the network features information and tool that can, be plugged, in the during this frameworks phases.

Practically therefore this phase, is much less strictly, prescribed with the information mentioning only, three very generic-tasks such as planning, development and implementations as well as testing which, are not structured, in details likes prior task. BOF4EWSS aims at this point, therefore become the identifications of relevant mature in addition to largely-complete developments processes techniques as well as tool that can be employed as well as allowing company the freedom, to combine-them to best-suit their respective-situations. Two such, and important processes, which might, be of great interests in aiding, in this internal-process are describe in the updated research articles in [2].

In first process, mentioned above in [7] present a web services level agreement framework lifecycle methodology, that concentrate on critical-internal aspect. These includes applications integration packaging, legacy application into reusable component migrations from old, to the new web services level agreement framework based processes as well as the best fit way of implementations which appreciated to the company constraints as well as risks and costs in addition to return on investments. This methodology, cyclic as well as consist of nine stages such as planning, analysis, design, constructions, testing, provisioning, deployments, executions as well as monitoring phases techniques. This process, is one of most appropriated as well as comprehensive, within literature survey. It should cover from initial-analysis of internal system to the constructions in addition to final installations and maybe the deployments of services as well.

A caveats to lifecycle-methodology however, is its lacks of emphasis on the security concerns to the web services level agreement framework prime targets as well as goal within the BOF4EWSS. To compensate, for this shortcoming another suggestions businesses, might considered is the integrations of PWSS [17, 22] of detailed developments processes for creating secure, web services level agreement framework. This would to be integrated with web security services to the web services level agreement framework could run, in parallel position.

Novelty behind PWSS is some important appreciations of the complex-task faced, by business as they attempt, to make use, of web services level agreement framework as well as it must be highly structured

methodical-approach to constructing, to the security architecture, for web security services techniques for network and features for e-business systems emphasis on traceability, as well as reusability, which translated information to establishment in addition to use of number of repositories, as well as recorded stores respectively. These three phases, in PWSS are web services security requirements, web security services architecture as well as web services level agreement framework technologies. These work together to enable the development of secure web services security system. In brief another general, point of reference to supplement, web services security two already mentioned can be found in [3, 23]. This text provide some useful guidelines, which can be applied within planning task related to planning and staffing a web services security development project.
Probably the biggest-benefit of using the processes listed, above is that almost all of the information gathered in addition to produced earlier in the framework can be reused to quickly complete, their initial stages. Such information includes functional, security in addition to QoS requirements risk assessment data and business process models. To consider, Analysis phase in [25] for example in BOF4EWSS Requirements elicitation and architectural phases companies have already worked on the current and envisioned to be processes.In addition to the identified processes as mentioned above literature, has supplied a number of techniques in addition to tools to help in this internal-development task. An area in particular, which has received great-focus is the automated creation of BPEL, processes from theoretical-modelling techniques BPEL allows for the specification of business process behaviour based on web services [2]. Amongst other things it is an execution language which can be run by software engines [13, 5] to orchestrate message-control and data flows.

The final task within this phase is the testing of the developed web services security and systems. This is done to verify that the developed applications meet the intended requirements. It can and should be done at a cross enterprise level. Testing can occur from three main perspectives such as function quality are the set performance usability scalability.Guidance on testing the functional, and quality requirements is given in the lifecycle, methodology [15, 24, and 25] mentioned before. A much more complex-operation is testing the security of the applications-developed. Whereas one can pass, input data into a system as well as process and quickly determine whether a functional-requirement has been met security is not that absolute nor can it be so easily measured [8]. This does not, however mean that testing is impossible nor should it be viewed as a task to be avoided by businesses.Like approaches for the other testing perspectives, the initial activities are the same, therefore identify requirements, and carry out controlled tests to see if or how well requirements have been-addressed. For testing the security of the implemented web services security in [11, 21, 22, 23, 24] offer a number of strategies and guidelines.

IV. Application Developments

Basic Background:the companies which are belongs to A, and B, are the two main e-businessespreviously-unknown of each other, that are inflowing into an arrangement that to use the web security services to sustenance their combined business to business connections. Therefore they have to start the initial-discussions on the process and functional-service desires techniques. At this point of the inspecting that the security of the progressions and services of e-businesses are rapidly call-upon their methodological personnel as well as crucial topics of the concentration which are includes decision on the standards to be used as well as the levels of the security should to be accepted in all direction of information.

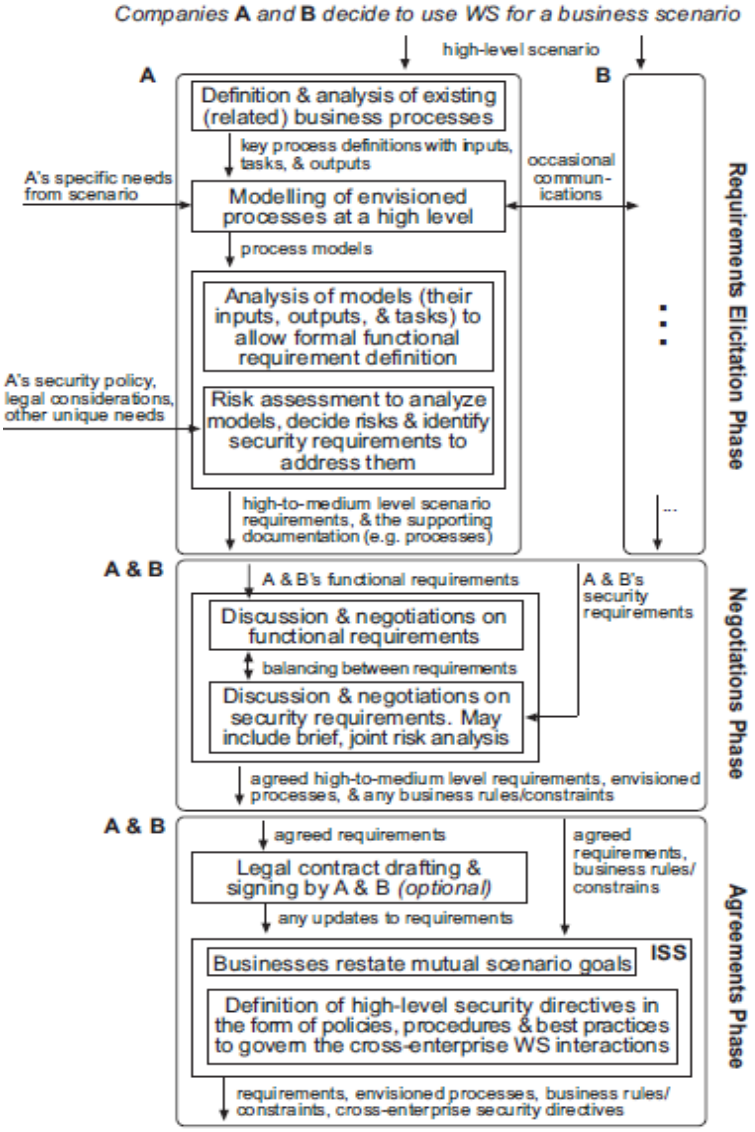

Figure 4.1 BOF4EWSS in different stages towards the Network and Features Classifications.

Problem Statement:the overall company which are belongs to A deems-security as an advanced precedence than, it is look upon by the company B as well. As the result in A decisions to engaged in the web security services they are conducted the number of risks assessments analysed numerous-factors that may be affected the services as well as external partners and then it put in essential policies and mechanisms. The company B conversely did not behaviour these internal-assessments and noticed to the susceptibilities in their website that can be used to take over their important services techniques respectively. therefore the assuming case where B services, are takeover A is directly-threatened as an assailant that can be send inaccurate messages structured query language SQL injection attacks oversize the extensional markup language XML, contents on to A further down costume of B as well. The predominant which are focus on the technical form of the web security services solutions such as standards-leads to deceitful the sense of security threats.

Framework contributions: Therefore the joint processes of the advocated framework-emphasizes widespread security as well as consider the importance techniques of factors and technical implementation.

Requirements elicitation stage techniques such as advocate risks assessment between the other things to regulate each business security necessities for scenario formation. Negotiations stage in which to follow the companies' links together to thoughtful on these essential requirements as well as agreed pathway onward regarding to the service and communication security confirmation. Negotiations stage each gathering would to have an opportunity to measure some other requirements and query about thesignificant security measure and to end put in forward to their basic requirements for scenario. Throughout this valuation so, A is probable to identify the areas which are not analysed by B and put to link in BOF4EWSSrequest needed for the security review of B. It is acknowledged that the projecting of way onward will be not a relaxed task as for the synchronizing the best

practices in addition to negotiating-desires are difficult tasks of the hidden paths of the checksum should to recognise.But, in cooperation of these are significant stages for attaining a comprehensive cross enterprise web security services solution agreed to supportthe trusted participating companies' techniques. The programming techniques of BOF4EWSS details as following.

<needs BaseXmlns:Xsi="http://www.w3.org/2009/XMLSchema-instance"
Xmlns="urn:risksschema"><mitigationActions>
<MitigationAction>
<Name>Security action for auditing/logging purpose<name>
<Details>Mitigation actions for auditing/logging purposes</details>
<Risks>
<risk id="Gri"><threats><vulnerabilities><riskLevel value="high">
<Risk Comment>risk associated with general logging </risks Comment><riskActionCoverageofRisk>
<CoverageLevel>full coverage</coverageLevel>
<coverageDetails />
</riskActionCoverageofRisk>
</risk><risk id="GR2">
</risks>
<LawandRegulation Ref>
<lawAndRegulationRef direr="LR215"><relationToRiskAction
/></lawAndRegulationRef></lawAndRegulationRefs><contractualObligationRefs>
<businesses PolicyRefs />securityPolicyRefs>
<securityBudgetRefs />
<SecurityRequirementRefs>
<securityRequirementRef direr="SR230"></securityRequirementRef></securityRequirementRefs>
</mitigationAction><mitigationAction></mitigation Action><acceptance Action>
<transference Action/>
<avoidance Action />
<Law and Regulation>
<lawAnd Regulation id="LR15">Sarbanes Oxley Act of 2009/ (SOX) requires that companies maintains ready available verifiable. </lawAnd Regulation></law And Regulation><contractual Obligation>
<businesses Policy/><security Policy>
<security Budget/>
<SecurityRequirements specifications>
<security Requirement id="SR30">A part of dependable businesses executions in both company and externally comprehensive-logging. </securityRequirement></securityRequirements></needsBase> specification of the BOF4EWSS Techniques.

V. Conclusions and Future Work

In this paper we are presented the BOF4EWSS a comprehensive grounded-framework geared at improving at this time available approaches, to the web security services within e-businesses. We discussed that the nature of web security services techniques through the network and features ofcollaborating of e-business now a much broader-critical as well as more real time concern than ever-before. Novelty of our method is to considers full-nature of the web security services as well as its checksum policy implications recognizes as well as target the live inter organizational network and features issue is now confronted by the interrelating of e-businesses and finally encourages use of the combined approach where, e-businesses work-closely together, process, as well as achieve the improved levels of web security services and trusts across the followers.

On the subject of the future work first-area of concentration is establishment of the enhanced system supports for framework-itself. BOF4EWSS is a very complex as well as widespread progression. Therefore we are proposed for added examine each-stage as well as interface among the stages to support it wherever are applicable in all directions of communication techniques. The potential area which is even now identified and concerns to the output from of the one phase as well as their instant practicality as input to the subsequent-stages. Above all of attention ispass through among individually as well as jointly-completed phases such as requirements elicitation to negotiations phase respectivelyand the formats which are the necessities are manufactured by the companies. Probable instructions under the research are only if systems support-based on the open technologies web security services based and streamline stage evolution techniques respectively. As soon as the detailed-framework is completed our next-goal will be to present its important applications to the case scenarios which is unsympathetically assess its aptness as well as strengths. Evaluation procedure in its completeness however, is pivotal as it enable for assessments of frameworks aims of the enhancing web security services and trusts across the e-businesses have been achieved.

References

[1] Muhammad Ismail Mohmand, David Young, Irvin Philip (2015). Some Essential Problems and Future Directions in Business Oriented Framework for Enhancing Web Security Service through Network-Features. Published in an international Journal of the Applied Environmental and Biological Sciences volume 5(12), pages, 5(12) 93-100, 2015. Available online at: www.textroad.com.

[2] Muhammad Ismail Mohmand, David Young (2015). Analysis and Applications of Web Security Services through the Network Features. Published in an international Journal of the Applied Environmental and Biological Sciences volume 1 pages, 5(9), 22-27, 2015. Available online at: www.textroad.com.

[3] M. Tatsubori, T. Imamura, and Y. Nakamura. Best-practice patterns and tool support for configuring secure web services messaging. In IEEE International Conference on Web Services, pages 6-20, Athens, Greece, 2009. IEEE Computer Society. (Cited on pages 7 and 8.)

[4] The Open Group. TOGAF™Version9, 2009. The performance and analysis of the secure network http://www.opengroup.org/togaf/.

[5] The SANS™ Institute. Lab anti-virus of the performance degradation of the policy.http://www.sans.org/resources/policies/Lab_Anti-Virus_Policy.pdf, 2006.

[6] The web Security Services solution in Network Features. CRAMM User Guide (Version 5.1), 2009. http://dtps.unipi.gr/files/notes/20092010/eksamino_5/politikes_kai_diaxeirish_asfaleias/egxeiridio_cramm.pdf.

[7] J. S. Tiller. The Ethical Hack: A Framework for Business Value Penetration Testing.Auerbach Publications, Boca Raton, FL, 2009. (Cited on pages 2, 4, 12, 14, 15 and 24.)

[8] M. Todd, E. Zibert, and T. Midwinter. Security risk management in the BT HP alliance. BT Technology Journal, 24(4):47-52, 2010. (Cited on pages 12, 13, 23 and 24.)

[9] E. Triantaphyllou. Multi-Criteria Decision Making Methods: A Comparative Study. Kluwer Academic Publishers, Dordrecht, 2000. (Cited on pages vi, 259, 260, 262, 263, 299 and 303.)

[10] T. Tsiakis, E. Evagelou, G. Stephanides, and G. Pekos. Identification of trust requirements in an e-business framework. In The 8th WSEAS International Conference on Communications, Athens, Greece, 2009. (Cited on page 34.)

[11] B. Tsoumas and D. Gritzalis. Towards an ontology-based security management. In 20th International Conference on Advanced Information Networking and Applications, volume 1, pages 985-992, 2008. (Cited on pages 159 and 164.)

[12] United Kingdom UK Department of e-Business, Enterprise and Regulatory Reform (BERR). 2008 Information Securityhttp://www.pwc.co.uk/pdf/BERR_2008_Executive_summary.pdf(Cited on pages 1, 4, 5 and 10)

[13] W.-J. van den Heuvel, K. Leune, and M. P. Papazoglou. EFSOC: A layered framework for developing secure interactions between web-services. Distributed Parallel Databases, 18(2):115-145, 2005. (Cited on pages 30, 31, 33 and 279.).

[14] O. Demir¨ors, C¸ .Gencel, and A. Tarhan, "Utilizing businessprocess models for requirements elicitation," in 29th Conferenceon EUROMICRO. IEEE, 2003, pp. 409–412.

[15] S. R¨ohrig and K. Knorr, "Security analysis of electronic business processes," Electronic Commerce Research, vol. 4, no. 1-2, pp. 59–81, 2004.

[16] M. P. Papazoglou, Web Security Services: Principles and Technology. Harlow, Essex: Prentice Hall, 2007.

[17] W. D. Yu, D. Aravind, and P. Supthaweesuk, "Software vulnerability analysis for web services software systems," in IEEE Symposium on Computers and Communications. IEEE,2006, pp. 740–748.

[18] E. W. Davis and R. E. Spekman, The Extended Enterprise: Gaining Competitive Advantage through Collaborative Supply Chains. Upper Saddle River, NJ: FT Prentice Hall, 2004.

[19] S. Chatterjee and J. Webber, Developing Enterprise Web Services: An Architect's Guide. Upper Saddle River, NJ:Prentice Hall PTR, 2004.

[20] M. Chen, "An analysis of the driving forces for web servicesadoption," Information Systems and e-Business Management,vol. 3, no. 3, pp. 265–279, 2005.

[21] A. Singhal, T. Winograd, and K. Scarfone, "Guide to secure web services (NIST SP 800-95)," National Institute of Standards and Technology (NIST), Tech. Rep., 2007.

[22] B. Schneider, and J.L makinzee. Secrets and Lies: Digital Security in a Networked World.Wiley, Indianapolis, 2004.

[23] M.L Schumache and U. Reedit. Security-engineering with patterns. In The 9th Conference on Pattern Languages of Programs, Illinois, 2001.

[24] M.U. Schurz and J. L. Ozone. Influences on exchange processes: Buyers preconceptions of a seller's trustworthiness and bargaining toughness. The Journal of Consumer Research, 11(4): 949-953, 2005.

[25] L.N wood, and D. Lines. Enterprise Security Architecture, A Business Driven Approach. CMP Books Francisco, CA, 2005.