CHAPTER 2

LITERATURE SURVEY

2.1 SECURE LOGIC AND PREVENTING ATTACKS IN WEB SERVICES

Web services are the chaining actions between three components or modules called the provider, requestor and broker. The provider's services are requested by multiple requestors or clients. In such scenario, security is considered as an important factor while multiple requestors access the services. Researchers have discussed various secure logics to prevent such attacks. These are discussed in the following literature survey.

Selection of prompt services is a required study in distributed environment. As large number of services provided offer different functionality to the customers, they are in a position to select their preferred services. To do a rapid service selection Micheal pantazagolu & Aphrodite Tsalgatidou (2013) designed a web service query model called proteus to discover heterogeneous services in distributed systems. The system was planned with three types of documents to evaluate the query patterns they are Service Advertisement, Query and Query Response. Service Advertisement document are used to illustrate the properties of service operations and query documents detains the service operation based upon the services. While searching results, the query response document conveys the service discovery results. Evaluation of this service model enhances the service advertisement

and user requirements. Also, the generic proteus query model was used to find the unified discovery operation in heterogeneous services.

Sabrina De Capitani Di Vimercati et al (2012) proposed a trust model for web applications. In this model, the trust execution is interlinked with SQL query. Generally, web applications retrieve the data from multiple databases. Their paper discusses the evaluation of secure trust generation with three layer architecture called Integrated Trust Management Access Control Systems. The function of this trust model system is to verify the certification and authentication details sent to the database from the user. The processed certificates are sent to web servers through the web browser and the certifications are verified by cryptographic services. This trust model prevents the SQL injection attacks distributing multiple copies datasets to different databases and by verifying the policy generation. Certificate verification algorithm is generated with the attributes of cost and certification Id. This method prevents attacks that are caused by various resources.

Web service providers are accessed through multiple sources of networks. While accessing services different players may involve in tracking and analyzing the service transactions and availability. To classify and evaluate the players of different services Sanat Kumar Bista et al (2010) proposed an acquaintance based reputation business model. The major contribution of this model is collecting the feedback from multiple players and classifying the player's feedback according to the distribution of weights. Trust worthiness assessment is used to calculate the feedbacks. They are based on direct association or acquaintance, friendly association and opposition to friendly association. In this work, the comparative feedbacks are collected from the unknown buyer and seller. Their proposed model is similar to the Prisoner's Dilemma Game, as the buyer and seller are not known to each other and they are differentiated into different categories. Reward (R)

denotes mutual cooperation, (T) denotes cooperative move, (S) denotes for cooperating with a default player and finally (P) denotes punishment. Finally, the cooperative feedbacks are evaluated using a formula called cooperativeness Index which classifies the strongest and the weakest identity. This type of business model improves the trust worthiness while carrying out online transactions and unauthorized users are also prevented from accessing of quality offered services.

Generally, the web services are stored in a repository called Universal Description Discovery Interchange (UDDI). The stored services may be viewed either by accessing private registry or public registry. Pedro Furtado (2009) introduced a QoS (Quality of Services) broker storage system, that reduces the transactional workloads of the accessed services. QoS broker has multiple of components that are interconnected with web applications. The different components of QoS broker are namely, interceptor, request manager, contractor, actuator and monitor. User oriented applications are also connected with QoS broker. These user oriented applications link the database and QoSBrokerConfigGUI interface. Before monitoring the service applications, the target source is monitored and matched in the QoS broker system. Three things that are notified in the repository services are targets, service features and contracts. The main advantage of this system is providing QoS features to services and also defines how these services were managed through admission control process.

Today, web services need more security measures in place to protect the valuable transactions originating from multiple sources. One of the DoS attacks focus on application level which target on the HTTP protocol messages. Mudhakar srivatsa et al (2008) proposed a mechanism for handling DoS attacks at application level. The authors proposed a two step mechanism to detect and rectify DoS attacks at application level. The first mechanism is

defined with admission control and the second technique is about congestion control. The authenticator in the first mechanism evaluates the IP packets that are received from the client HTTP layer. It checks the 16 bit port field number and verifies the client IP address. If any unmatched or unauthorized client details are found then the accessed services are blocked from the user. The second mechanism focuses on congestion control which prioritizes the incoming requests. A scoring mechanism is used to filter the requests and neglect the concurrency of accessing services. Also a feedback mechanism is provided to filter the unwanted services from the inputs received. The improvement of this system is to neglect the application level attacks from accessing unauthenticated services and prevent the application level attacks.

Spam mails are unwanted mails sent to a large group of users. Numerous research work has been carried out in detecting spam among which web spam is a challenging research area to focused upon Luca becchetti et al, (2008) designed a web based link spam analysis using a collective group of web pages. Web spam is categorized with respect to content and link based analysis. Content spam is usually carried out by inserting a set of keywords into the web page, so that lot of keywords get merged in the title as well as hyperlinks of the page link spam is carried out by making changes in the link structure of a website. Web spam detection happens by linking multiple link pages using the concept of link forms. In this research work, link spam analysis is discussed which is used to detect web spam and classify hyperlinks. A link analysis algorithm hyperlink is web pages that are ranked and analyzed using web graphs. The semi streaming algorithm is also used to store the large data sets that relate to the web pages. By using ranking and prioritization, link spams are detected and are used in identifying the most possible correlated web page link sites.

Domain Name System (DNS) rebinding is an attack in which an attacker creates malicious web pages, which if an user visits unknowingly, a client side script gets executed and attacks the desired destination. Collin Jackson et al (2009) made a survey in the analysis of DNS rebinding attacks that used to represent how these attacks affect multiple destinations. These types of source attacks happen from any form of resources such as different browsers, flash players and live connect software's. In web browsers, binding attacks make issues with the client script of XMLHTTPrequest, the response received from the targeted URL and the content extracted from the attacker's server. With the flash player, it embeds the Shock Wave Flash (SWF) movies, through which it opens a TCP host to the targeted destination. Live Connect software's such as Java, Applets and Flash players connect service applications using DNS hosts. These hosts are attacked with multiple DNS binding attacks and their IP addresses. Various techniques are proposed to prevent such DNS binding attacks among which the author's research defines security policies and software plug-ins.

Social network is a network which enables users to connect with their friends in different location. Jennifer Golbeck et al (2009) carried out research analysis in the field of social networks of film trust in order to understand how the users connect with their friends. Trustworthiness can be checked in two ways. The first way is through the listed friends and second through the opted friends list. The trust rating of movies are assigned using stars ranging between half star and four star values. Mainly, the user profile lists are collected and matched with the group collections and finally the trust worthiness is evaluated. Rating of a movie is calculated using the formula of recommended rating, where it is compared with actual rating. Experiments are defined with three phases of maximum difference effects, extreme ratings, trust predicting trust. When compared with existing survey, the author's research concentrates on the study analysis of social networks with profile

matching concepts. The existing research defines the set of policies and rule matches.

Service Composition is one of the major research area in Service Oriented Architecture. Composing more number of services, improves the service accessibility from one service to another. Many web service applications typically use service composition. Wei She et al (2013) designed a three phase composition protocol that provides Information Flow Control (IFC) rules for access control in web service composition. Generally, the feasibility of access control is a challenging criterion in web service composition. Their work solves the information flow control and reduces policy evaluation cost in a grouped web services in three phases. The first phase rules solve the linkage break between two set of chained services using Likelihood Computation (LLC) rules. The second phase service composer solves the fraud detection in composed services by selecting the service attributes and policies of the services. The third phase security authority provides the security evaluation of services by identifying preferred service attributes. IFC provides the subsequent rules for securing services in a continuous chain. According to the secure information the risks are categorized as No Risk (NR), Low Risk (LR), Medium Risk (MR) and High Risk (HR). NR is impossible to gain the sensitive information from input or output, LR is somewhat difficult to gain the sensitive information from input or output, MR allows some sensitive information to be derived and finally HR can collect all the set of sensitive information's from the input or output. The main advantage of this research work is reduction in number of access control violations during execution time of services. Also, the risk information is tracked using dynamic information tracking analysis and hybrid information flow analysis approach.

Today, distributed networks are widely used in many web oriented applications. Distributed network frameworks are entirely different from centralized network. Providing security and workflow traceability in distributed networks is a challenging issue. To avoid such circumstance, the author Frederic Montagut & Refik Molva (2008) designed onion encryption techniques and workflow execution models. When this technique is processed along with business partners, they can easily access the workflow instances and execute sensitive workflow execution paths. Also, onion encryption techniques are mostly used by the work flow based web applications. Business analysis execution was initiated along with workflow specifications and run time specifications, where workflow specifications had collaboration with business partners. Here, each set of messages are executed along with multiple structures and with respect to the execution plan, each messages are encrypted with public keys. Run time execution is based on Vertex execution, once these executions are complete, it builds the workflow messages. These messages are accessed with the onion workflow data. The execution of these workflows are then choreographed to trace by means of the business analysts and identified during run time execution. The main advantage of this run time workflow execution method is to prevent the vulnerabilities and avoid hacking in the distributed networks. Moreover, the proposed onion encryption technique is interlinked with workflows in business process. Once a business analyst starts the execution, the messages are grouped and encrypted. When compared with existing techniques, the author of this work introduces runtime execution of workflow messages in distributed network environment.

Providing security access multi service platforms is a recent research issue viewed and analyzed by many researchers. From the above survey, it can be seen that security can be even applied for multi service platforms.

2.2 LOAD BALANCING AND REDUTION OF RISK FACTORS FOR SERVICE INFORMATIONS

Using World Wide Web tools multiple source data contents are collected and used for web applications and this form of collection of data is called mashups. Rattapoom Tuchinda et al (2011) developed a framework called Karma that collects source content from various web applications. The Karma framework has been designed to extract the mashup data using data extraction, source modeling, data cleaning and data integration. This framework focuses on the enhancement of existing data bases and to consolidate or solve the problems while combining the mashups. The evaluation of Karma framework has been processed with the major factors known as users, tasks, procedures and set of data collections. With the user's involvement, it is categorized as programmer and non programmer. Based on the requirements for the programmer, user requirements are collected from M.S or PhD students of computer science and for non programmer, the administrative assistants or accounting students are considered. This tasks involved in the requirements collection include, collecting the mashup from a single resource. Building the mashup from a multiple web page query results and developing a mashup from multiple databases. The procedures involved needs a set of information defined for users. It is represented by three ways namely Familiarization, Practice and Test. Finally, the mashup has been formed by extraction, modeling, cleaning and integration. When compared to the existing Dapper/pipes, the proposed framework analyses better and work completes the task within the duration of time period with a faster factor ratio of 3.3.

Evgeniy Gabrilovich et al (2009) proposed a methodology for search based query classification from a source of web. In this method, the given query is classified according to the topic that matches with the query.

This type of classification is defined with pseudo relevance feedback technique and has been evaluated with empirical estimation. Two types of phases are used by the authors to construct the query classification. They are 1) document classifier 2) query classifier. In document classifier they classify the same taxonomy using the machine learning algorithms. The query classifier performs the classification with respect to the queries based on conditional probability. Different methodologies are applied to do the classifications namely classifications based on relevance model, voting method and generalized voting. Classification based relevance model is developed to classify only with the queries and document classes. Relevance model calculates the relevance using the formula

$$RC(d, q) = \sum_{Cj \in C} P(Cj \mid d)P(Cj \mid q) \quad (2.1)$$

where, RC(d, q) is the relevance of document for ‘d’ and query for ‘q’. P(Cj |d)P(Cj |q) is the estimated web search results of the ranked documents. Voting method is conducted based on the weightage of the documents. With the weightage of query and rank classification the voting method calculates P using the formula

$$P(Cj \mid q) = \frac{1}{2\lambda} \sum wi\ P(Cj \mid di(q)) \quad (2.2)$$

From the calculation of above formula, equal weight is calculated for multi source web documents. The generalized voting is the enhanced extension of second category of voting method, where the highest priority based queries are retrieved from the voting method. Query search results are beneficial for rare query identification. Compared to the existing research analysis, the web knowledge based query classification provides better search result and priority based ranking of web pages.

In Service Oriented Architecture multiple services are combined to make the composition services. Many researchers have discussed the web service composition, Tao yu et al (2007) proposed two sets of algorithms for the selection of components for the service composition. They are combinatorial model and graph model. The two models define two types of algorithms called Multidimensional Multichoice Knapsack (MMKP) and Multi Constraint Optimal Path (MCOP). MMKP algorithm is based on two types of algorithms called Branch-and-Bound (BBLP) algorithm and Web Service Heuristic (WS-HEU) algorithm. In MMKP, a service candidate is selected from a service class and composed. The atomic services are grouped with the object and their quality attributes are matched with the required resources. BBLP selects the optimal solution path by finding utility upper bound and selects the node with largest hypothesis. WS-HEU algorithm is a heuristics algorithm where, it prunes the infeasible items and produces the feasible items.

Also the graph model is used to find the feasible paths from the unfeasible paths. This model has been designed with Multi Constraint Source Path (MCSP) algorithm to find the constraint requirement with Direct Acyclic Graph (DAG). In acyclic graph generation, the nodes are sorted and ordered in a topological way. Here, the ordering is based on QoS order constraints. By comparing with existing researches, this work invokes the service components using two models and performs the service composition. If the QoS parameters are not clearly defined with each service then, it is too difficult to make the service composition. This is the major disadvantage of this research work.

Barbara Poblete et al (2010) introduced the privacy preservation in query logs. In a business organization, the business process transmission of confidential information from one source to other source is a vital one since

attacks are possible. The attacks in the query log are categorized into three types called anonymized query log, search engine query results and web site log. In anonymized query log, institutions or organizations confidential information are anonymized using the anonymization scheme. In search engine query results, the results are obtained by the adversary agent by issuing queries to the online search engine. Web site log contains private information from where the adversary agent can access the private information. Vulnerabilities like anonymization, vulnerable queries, and attacks in anonymized query log may frequently occur in query log. The anonymization is defined by the structure

ANONuserId, query, timestamp, ANONclickedURL

When the user clicks the URL path, it gets anonymized and the user Id must be tracked. This is used through the parameters such as ANONuserId, query, timestamp, ANONsite.ANONclickedURLinSite. The different web sites are anonymized with the clicked URL web site and their contents are retrieved with the selected user Id. Vulnerable queries are based on the size and the amount of information of the published dataset. The attacks in anonymized query log are classified into two types. The first type is for exploiting a private web site log, and the second is for the attack to exploit the disclosed user data. To prevent the query log anonymization, heuristics methods are used. These methods select few nodes from multiple nodes. Here, the highest priority nodes are selected and the low density nodes are removed from the graph query format. This research is mainly used for web based companies that are fully oriented with web communication. Also, vulnerabilities attacks and anonymization are analyzed and are reduced with the heuristic method. If the business process data sets for IT companies make use of this concept, then they can make an easy way of confidential information transmission to any type of source platforms.

In this model, unemployment people who are seeking jobs have to fulfill their personal needs. Moreover, unemployed people are calculated or measured from the total number of people. Wei Xu et al (2012) proposed, a novel method framework which is used to evaluate the unemployment rate with the data mining tools using Neural Networks (NN) and Support Vector Regressions (SVR). By the novel method, this framework at first focuses on the general employment activities. Second based on the employment activities a query dimension model is designed. Third a genetic based data mining algorithm is used to refine or filter the activities. Finally, the finalized unemployment rate is forecasted to the customers. As per the process the query declaration is categorized as 'local jobs' and 'social/security jobs' also the Progression is evaluated by four steps. In step1, nearly 100 jobs are collected and put for analysis. Step 2 activities are evaluated with the calculation of Pearson function and step 3 modeling progress is carried out by genetic algorithm. Modeling is predicted with the set of chromosomes and the fitness is calculated by the fitness function. The unfitted chromosomes are dropped out and crossover chromosomes are exchanged with the matched genes. Neural networks are used to calculate the fitness function of chromosomes. Neural networks like Back Propagation Neural Network (BPNN), Radical Basis Function Neural Network (RBFNN), and Wavelet Activation Function (WNN) are used for testing the parameters of genetic chromosomes. Finally, the prediction results are estimated with the Root Mean Square Error (RMSE). The predicted results are calculated using the formula

$$RMSE = \sqrt{\sum (A_i - P_i)^2 / n} \qquad (2.3)$$

From the mean square estimation, the predicted results are progressed with the models of NN, Support Vector Regression of (linear SVR) and (polynomial SVR). In step 4, the comparative results from the

above mentioned models are estimated and the unemployment rate is predicted. With the major four steps, the unemployment rate is predicted which is to be utilized for various research fields or the online web based applications.

Web service choreography is one way of composition of services, where each service acts as peers and one service interacts with other service without a unique control. Also the services are communicated with the XML based business process language. Zheng Wang et al (2010) designed a choreography tool called Choreography Description Language (CDL) checker for web services composition. Using the CDL checker, Web Service-Choreography Description Language (WS-CDL) is simulated and validated. Two types of simulation are processed namely static validation and dynamic validation. The process starts with inputting the WS-CDL documents to the simulator with their specified Web Service Description Language (WSDL) descriptions. After parsing the choreographed documents are assigned to the tree structures.

Two types of trees are used called choreography tree and activity tree. The choreographed documents are stored in the choreography tree and their related activities are stored in the activity tree. After the progression of tree assignment, the simulation algorithm is applied to the designed documents. It selects the execution path from the root and makes the choreography path. Then this simulated graph is next passed on to the validation. In this part, the relational calculus is applied to the choreographed graph. Two types of constraints are stated to select the variables namely static constraint and dynamic constraint. Static validation is based on the output from the simulator and dynamic validation relies on simulator. Both the simulator and validator are interconnected. Once the simulation is over, it send the results to the validation. Later, the services are choreographed and

they are parallelly validated in CDL checker. With the usage of this, a group of services are easily choreographed and applied for business process.

The Service Oriented Applications (SOA) is the plug-in architectures that are used with many IT oriented applications. Nowadays, SOA framework was popularly built for web applications, Automobile applications, and Medical applications. From that, the real time SOA is popularly built to reduce most complicated problems in web services. The real time services are distracted with the problems of composition, scheduling and time consumption. The service composition is based on more collaborative service linking where one service output is given as input to other services. During this composition, more collaborative services are matched and then put for comparison. In scheduling, the services are scheduled according to the tasks. If more number of tasks are assigned, they are categorized and based on that they are compared. In the time consumption, focused with the communication timing from one service to other services. During composition of services, the communication latencies are monitored and the measured frequencies are table viewed. Also with the cost estimation point, the service costs are estimated and the services are composed.

With the above three discussions, Hachem Moussa et al (2010) introduced a three phase composition approach for real time SOA applications. In three phase applications, the first phase has been designed with the Admission Control algorithm that manages the loads and assurance delay latency. From this algorithm, it states that the multi arrived service requests response time are monitored and their probability are calculated. From the calculated measurement, the delay requests are filtered and their latency was measured. By making such control focus to the services will reduce the delay latency time in a service group. Secondly, the second phase focused with the overloaded requests that mismatched in the first phase. Also

the second phase evaluates the concrete services and it timely admits the additional overloads. The second phase discusses about the admission and over loaded communication latency. In third phase, the real time admitted services are selected and composed. This composition satisfies all real time requirements of web applications. From this three phase composition, the services are monitored, latency is measured and executes filter composition. Compared to existing survey analysis, the three phase composition produces effective timing service composition for real time services.

The above discussion deals with the surveys and research focuses on web service classification. The survey analyzes how the services are classified according to the flow of information.

2.3 RULE GENERATION AND AGREEMENT MATCHING IN WEB SERVICES

Generation of agreement is the challenging one that is to be prepared or documented with providers and customers. Contract agreement generation is based on certain policies, security logics and meta data provided by the contracting providers. The provider is of any category, and hence may be related to IT industry or network service provider or application service provider. With respect to multi cultivate research, the Service Level Agreement (SLA) generation is based on multiple constraints with respect to the service providers. Some of the research works focused on service agreements are discussed below

Concrete services are the services that are to be selected during run time of service composition. Also, the run time services are selected based on the Quality of Service parameters. Hiroshi Wada et al (2012) introduced an optimization framework called **E**volutionary multiobjective s**E**rvice composition optimiz**E**r (E^3) for service composition. The major contribution

of this work is the proposition of facilities to analyze multiple Service Level Agreement (SLA) using multi genetic algorithm and to apply the predicted results to Pareto principle. Finally, it produces quality parameters for the grouped concrete services. SLA oriented service composition deal with two issues 1) Complexity which discusses the much amount of time, cost and labor are required to make the composition of services. 2) It is the SLA-aware Service Composition (SSC) problem which is used to verify the mismatched QoS parameters for the multi grouped services. The two problems are analyzed and solved by E^3 framework. E^3 is used to solve the SSC problem with the two techniques called Service Deployment - Multi Objective Genetic Algorithm (E^3-MOGA) and Extreme-E^3 (X-E^3). E^3-MOGA is used to check whether the parameters are equally distributed between multiple constraints. Secondly, Extreme - E^3 is validating the tradeoff with respect to throughput and cost. With the composition, the users are categorized as platinum, silver and gold. The optimization with genetic algorithm is used to make the combination of composition with 36 genes. E^3-MOGA and X-E^3 share the gene structure and optimization process. The evaluation of this framework produces the stable composition of concrete services for a given application and produces an equality SLA generation.

Multiple computer resources that are composed and accessed for a common goal is known as grid computing. In this computing, multiple resources are shared and accessed from different service providers and customers. So, the workflow or transformations of informations are to be more effective. For example, a weather forecast may foretell the weather conditions periodically. The delay of reporting the weather conditions may confuse the people who are in need of the report. The timely information will help preventing loss during flood or disaster times. To view this problem, Dang Minh Quan & Laurence Yang (2011) prepared a parallel mapping algorithm to monitor the execution time of service providers and consumers

in a grid environment. Also, it resolves and maps the relevant components that match with Service Level Agreement (SLA) generation between the chosen application service providers and customers. The workflow mapping is based on condition of light communication, heavy communication and workflow within the grid work flow.

Mapping of services are executed with the algorithm called w-Tabu algorithm. It works with the conceptual idea of configuration space, construct reference configuration set, neighborhood structure and assign the workflow and also determine the timetable of the workflow. In configuration space, the resources requirements are selected based on the Resource Management System (RMS).First, the selection of resources are selected with the SQL commands. Secondly, the reference configuration set assigns number key for the selection of jobs. Third, the neighborhood structure presents a vector for the allotted sub jobs, also the selected vector to be matched with the candidate class. Fourth, the sequences of workflows are matched with the start and end time of sub jobs and the job transferring time accessed with the resources. Sequence workflows are parameters determined and workflow allocation is determined by conventional graph matching algorithm. At last the determinations of workflow based on the timetable. In Resource Management System processing the completion of one job is based on another job. Also, the process generation of this algorithm does not affect the quality parameters of the workflow. The study of this algorithm enhances the workflow transformations between a group of service providers and customers and improves the operation of SLA generation.

Scheduling of tasks in services is based on the compatibility of the particular services. To schedule a particular service may reduce the deadlocks, it is necessary to prevent resource sharing at particular time. Ivan Vermeulen et al (2007) introduced Multi-agent Pareto-improvement Appointment

Exchanging (MPAEX) algorithm for improving the scheduling of tasks for a grouped services. This paper proposes a scheduling algorithm for hospital patient scheduling system. This system is accessed by a set of patients and their appointments are scheduled with different allotted resources. Each patient may access the resources in different timings, where the scheduling of timings are planned by the doctors and allotted to various departments. During the allocation of timings, each department may sometime cause confusion to the patients, because a same patient may get appointment for various diseases. Exchanging of appointments is solved with allotments of software agents. Two types of agents are used to solve the allocation of scheduling in MPAEX 1) resource agents 2) patient agents.

Resource agent prefers resources with the fixed hours for scheduling. Here, the scheduling of hours is fixed based on the activities. Here, the scheduling is fixed by the doctors. The patient appointments are consulted with the doctors and patient preferences are noted. With availability of appointments, the timing is discussed with patients and schedule is drawn up. With the preferred types of agents in MPAEX the two types of algorithms are designed. In algorithm 1, the patient agent clarifies the availability of appointments with the resource agent. If the schedule is available, it fixes the timing for the patient. In algorithm 2, resource agent checks the availability with the chosen activity. If the activity is busy with selected time, the resource agent collects the feasible time slot for the required activity. Available slots are exchanged and the slots provided to the required patients. Compared to the existing scheduling algorithm, the MPAEX algorithm provides faster and short sequence schedule allotment of appointments to the patients. The main advantage of this algorithm provides ‘Theil’ index concept, from that a patient can refer the workloads for the allotted resources which require scheduling.

In web services, the service providers and service consumers or service providers to service providers are communicated with Simple Object Access Protocol (SOAP).Here the communication messages have some contracts between services to services. Constraints in service contracts are monitored with the research algorithm called Linear Temporal Logic-first order quantification (LTL-FO^{+}) proposed by Sylvain Halle & Roger Villemaire (2012). Amazon service and Google checkout service are taken for the experimental evaluation for message transmission. The Amazon service provides large service activities to customers. More than 3,00,000 customers access Amazon service and make more number of transactions with E-commerce services. Shopping can take place with the shopping cart and cart-Id. The customers entering online shopping cart in Amazon services need to make authenticated message transaction with the service providers. Similarly, the Google checkout is the commercial web-site provided by Google services. In Google check out, the registered users transfer amounts from their credit transactions to the nationalized or internationalized banks. So, here also the messages need to be securely transmitted and message constraints are monitored. The two experimental sets of service provider's message constraints are monitored with LTL-FO^{+} algorithm. Multi definitions are stated for this algorithm they are

Definition1: Syntax

Definition 2: Semantics

Definition 3: Watcher

Definition 4: Outcome function

Algorithm based on propositional logic and implemented in Java applet with the defined BEEP-BEEP algorithm. Java applet is used in client side web application and it verifies the transferred messages in that

application. With the improvement of this temporal logic to be experimented with Google checkout and Amazon service providers and nearly 10,000 messages are executed to produce the authenticated message transmission using LTL-FO^{+} algorithm.

Wireless Sensor Networks (WSN) distribute sovereign networks, where it gathers the physical data from surrounding environments. These sensors are built with individual nodes that connect to multiple sensor networks. Today, these networks are used for many customer oriented applications and military applications. While using such applications, the accessing nodes get complicated with the communication. Sometimes the nodes are tracked or interrupted with unacknowledged path of packet transmission. The Edgardo Aviles-Lopez & Antonio García-Macías (2009) designed a framework called TinySOA to make the users access the architecture with the service oriented API. The purpose of designing this framework is to reduce user's accessibility from any resource through SOA API with the choice of user preferred languages. TinySOA was designed with three components called Capture, Concentration and Application. The first one focuses on the WAN area. In the locality of WAN, it monitors how the messages are published and communicated to the outside entities. Here, the outside communications messages are passed through the gateway server.

Secondly, the concentration part designed with the gateway node and gateway server. This is the functionality area where the main execution is taken over here to execute the received data. Thirdly, application component receive the processed data from the concentration part where it distributes to the required customers. The three components all are mashed up with the internet to access different source accessibility in WAN network. Also, the components are classified with internal services and external services. The

internal services are defined with nodes and external services are defined with the gateway, registry and server. With the use of Service Oriented Architecture, the TinySOA framework was quickly designed and used by multiple customers with the choice of their own languages. By studying the various research works, it is found that the TinySOA provides quick transmission of messages and provide easy node accessibility in distributed networks.

For any buying and selling service products SLA agreement is the necessary requirement to be satisfied between customers and providers. Considering business environments, each business has its own service agreements. Carlos Muller, et al (2014) proposed a conceptual reference model called Service based system Aimed to Monitor QoS based web service on Agreement Document Analysis (SALMonADA) used to monitor the business agreements during run time for analysis. The models retrieves collection of service agreements as input and are executed with agent elements of client, configurator, monitor and analyser. The first element client acts as consumer or provider to collect SLA agreements and input to SALMonADA model. The second element configurator generates monitored SLA documents and decouples agreed SLA documents. Monitoring is executed by the processing called Monitoring Management Document (MMD) and the analyzer document executes the monitored SLA and produces the fulfilled agreement as Service Level Fulfillment (SLF). SALMonADA exhibits main features that operate with the protocols of SOAP and REST and easily interoperates the self adaptive service base frameworks such as cloud infrastructures. The framework model SALMonADA for the most part is enhanced with Agreement Document Analysis (ADA) framework and is used to extract the collective WS-Agreement documents and to chain the documents with the functionalities of logical expressions. Also the ADA framework was supported with the packages of Java library and OSGi service.

The enhanced features of this conceptual model evaluates WS-agreements, monitors SLA documents, stores monitored results and executes the violated results with ‘push’ and ‘pull’ operations.

Web services are utilized in number of fields, from them geospatial web services are majorly used in environmental survivals to predict the data in case of floods, earth quakes and any natural calamities. The Open Geo Spatial web services use cache techniques to store the ecological data from the environment. Cache will improve the functionalities of temporary storage, reuse and regenerate the resultant data on certain time duration. To cache the data for the number of services at a time that overload Open Geo Spatial services. To reduce the overloaded data with respect to the number of cached services, Ruben Bejar, et al (2014) designed a protocol with a set of policies called machine readable Rights Expression Language (REL) along with harvesters. According to the authors, the harvesters are designed algorithms that will download and store the cached item. During caching process, the cached data are matched with the policies and they applied for the harvest algorithm. Algorithm1 checks the human requests with review Policy and obtainConsent policy. These two policies are confirmed by human requests. Algorithm2 checks the list of collected services from Algorithm1 and provides service caching. These REL policies are applied to the EuroGeoSource project that accesses the geographical information from mineral resources. In this model ten European countries are tested and the scheduled policies are made using REL concept. The advantages of these policies are that they are useful for the environmental community to monitor the cached data and to make the schedule accessing of data for user requests.

Service contracts are design principles agreed between the agreed service providers. In such contracts, the agreements are based on each active business events and activities. Xibin Gao & Munindar P.Singh (2014),

proposed a novel approach to enhance the business events using the set of patterns, parsing and classifications. Service contracts may differ with each service domains. The proposed a novel approach which makes the flow approach in hybrid workflows which are framed as collection of contracts, parsing and machine learning techniques. From this approach, initially raw contracts are collected, and then the filters unwanted HTML tags are filtered in order to remove the unmatched business events. Finally the matched business events and constraints are identified and are classified by the machine learning techniques. The discussed process are executed with three different tasks namely business event extractions, Business event topic discovery and Temporal constraints extraction. With this approach, the candidates or customer activity contracts are executed easily with their required needs.

2.4 PROPOSED WORK

From the study of above literature survey the proposed work Heterogeneous Offer Agreement Generation System (HOAG) developed in this study provides a better searching and offer quality services. Customers may get a quality based, acceptable price and availability based services from this proposed system. The system is modeled in three layers namely Layer1: Analyzer Security Originator, Layer 2: Classified Filter and Layer 3: Fuzzy Based Offer Agreement Generator. The first layer will receive and analyze the incoming requirements from the customers. More than that, number of customers can access the service providers and state their requirements of choosing service provider services. Such requirements are filtered and securely authenticated with this layer. To provide security, it acclimatized to the proposed Enforcer algorithm, that do the twice encryptions and decryptions. Secondly in Layer 2 Classified Filter will filter the requirement analysis received from Layer 1 and it reduce the bulk arrival of requests. The

authenticated informations are classified in the proposed Efficient Trim Down (ETD) classifier. This classifier will check the risk analysis and complexity of the bulk information. Finally, the customer required services are executed in the last layer of Fuzzy Based Agreement Generator. In this layer, services are matched with the requirements using Fuzzy rule based algorithm and the final fuzzy based agreement is sent for the customer approval. If the customer is satisfied with the agreement, they assign agreement with particular provider or they refuse the service.

The main advantage with the proposed HOAG system is that it reduces the searching time of the customers. Generally, if a customer wants to search the offer based services in a business environment, he faces more complications. In day to day business activity, multiple service providers deliver the optional services to the customers. From that the proposed HOAG system reduces the customer searching time and also provides secured accessing and balanced data to the customers. The formation of three layers to this functionality with the less period of time and produces the accurate data to the customers.