CHAPTER 1

INTRODUCTION

1.1 PROBLEM STATEMENT

Generally in web services, services are accessed by multiple customers and they are expected to get consistent offered services with the stipulated period of time. In today's business environment, the accessibility of any particular service gets delayed to the customers depending on the service providers. To reduce the customer searching time, this thesis introduces a new method called Heterogeneous Offer Agreement Generation (HOAG) system. This system focuses on the problems addressing on security, accuracy and availability of services. The customers have their own choices to buy the requirement matched services. To buy any particular service, they should produce all necessary information to the provider. The credential information are obtained and executed for security analysis. To provide supplementary security for the credential information, the services are evaluated with the proposed Enforcer algorithm in this work. This will solve the problems that arise with the third party analysis and will prevent hacking. Secondly, measuring accurate data will reduce the load balancing and produce the best accuracy to the service providers. To measure accuracy, this system proposes an Efficient Trim Down (ETD) classification algorithm. This will measure and produce accurate results to the service providers. Finally, the availability of offer services is checked with the Decision Manager. It analyses the results with the help of User Requirements, User Oriented-Data Base and Expert

Advice. Once the customer is satisfied the approval is assigned by the Fuzzy Base Offer Agreement Generator where the offered services are exchanged to the required customers. All the focused problems of this work are solved with the proposed HOAG system in the form of layer formation with three layers namely Layer1: Analyzer and Security Originator, Layer 2: Classified Filter and Layer 3: Fuzzy Based Offer Agreement Generator.

1.2 PROJECT OBJECTIVES

In the recent years, online businesses are highly dependable on the valuable customers, where the service customers are too busy with their scheduled period of works and they like to limit their searching time to select the favored services. With reference to the customer point of view, the proposed HOAG system has been designed to reduce the customer searching time and to produce the offered services to the customers. The objective of the proposed HOAG system is to improve the security for the user credential information with the proposed Layer 1 called Analyzer and Security Originator and to provide load balancing of the secured credential information with the proposed Layer 2 Classified Filter. Finally, it checks the available status of preferred services to the customers in the proposed Layer 3 Fuzzy Based Offer Agreement Generator. With this layer formation execution, customers get their preferable services in a necessary period of time.

1.3 IMPORTANCE OF THIS RESEARCH

Some of the Challenges of this research area are:

1. What is the necessity to propose a new web services for the sales data?
2. How to improve the security for online sample data?
3. Why decision accuracy is important?

Current economic world is fully activated with the usage of Internet. Business people buy and sell their products through online web applications. In this work, applications are framed as services and efficiently accessed with the number of end users. From the service provider concern, they want to sell their products to the required customers and offer attractive offers to the customers. Once the customers satisfied with the offered service, they make a bondage to the provider. In present trend, multiple service providers are providing various offers to the customers. So, there is a necessity that the customer must be in a position to search their opted services which are correctly matching with their requirements. To avoid the inconvenience and condense the searching time of customer, this research proposed the HOAG system, which improves security, accuracy and availability of the customer selected services. Through this research work, the service customers get an idea about the selection of services in a required period of time.

1.4 WEB SECURITY AND SERVICE LEVEL AGREEMENT IN SOA

In business environment, web services identify threats and avoid vulnerabilities using different technologies. Among them, Service Oriented Architecture (SOA) is a loosely coupled architecture where all the services are distributed and accessed by multiple customers. In this loosely coupled architecture, attacks like Denial of Service (DoS), Extensible Markup Language (XML) injection and session hijacking majorly occur with the services, where the DoS attacks can crash the systems and affect the confidential information during business process. In XML injection, the attacks manipulate the contents of the business logic. In session hijacking attacks, the unauthorized information are hijacked from any resource. With these attacks, accessing of services are unsecured and they must be prevented

by applying various methodologies and techniques. These attacks also affect the service agreements for the period of business transaction. With secured composition of services, the Service Level Agreements (SLA) generated between the customers and service providers can be secured effectively. Moreover, SLA provides the binding between multiple customers and providers. With the service agreement, any client can access the required services based on the service quality, availability and prompt services. The service agreement has its advantages and disadvantages. Mostly, the advantages like customer binding, required timing transaction, accessing quality offered services are preferably utilized by the customers.

1.5 NEED FOR WEB SERVICE SECURITY

Security is one of the issues to be discussed for web services. From the research survey, web service security is the extension standard retrieved from the Simple Object Accessing Protocol (SOAP). In web service security, parameters are defined based on the properties of authentication, confidentiality and integrity. The defined properties are discussed in the following paragraphs,

1.5.1 Authentication

Authentication is the process that verifies the personal details, when accessing the valid services (23). Also, authentication is used to check the unauthorized accessing of services with a genuine user details like user Id and password. It solves the attacks like masquerade attack, reply attack and identity interception. In services, these attacks could be reduced with the authentication methodologies, if applied effectively. It reduces the replay attacks with the reduction of unauthorized information from the third party source. The replay attacks are measured with the session tokens and timestamps. Session tokens are time tokens which are sent from the sender to

the receiver to measure the authenticated communication between dispatcher and recipient. Similarly, the receiver has the timestamp option to send a timing message from sender to receiver for authentication, so that the authorized user can securely utilize the services with the time stamp transformation. Secondly, identity interception is used to check the identity of the user when logged-on to the system. Using the single-sign on process, a user can access the system only once with the valid identity.

1.5.2 Confidentiality

When transmitting a message from source to target, the privacy of the message should be protected. In service transmissions, the encryption method is used to encrypt the plain text and transmit to the receiver, where the receiver can decrypt the messages and get the original plain text. To improve the confidentiality for business services, the XML encryption happens with the symmetric keys in web services. The other way of generating confidentiality is assigning digital signatures in the security header blocks. By way of assigning signatures, it will ensure that only valid user access the data reaching the destination.

1.5.3 Integrity

In service transmission, data is protected from modifications or any malicious attacks. The digital signatures are designed with the hashing techniques for the authenticated codes to provide secured transmission of messages. Integrity of Simple Object Access Protocol (SOAP) messages are generated with the methods like Canonicalization, Signature, Reference, Signature Value and KeyInfo methods. Canonicalization Method acts as a unique standard document forms that satisfies both the sender and receiver. Signature Method will create the signature using DSA and RSA algorithms. Here, the reference elements provide the signing option with the base64

encoded messages. Finally, the KeyInfo is verified with the validity of keys sent during data transmission.

While considering the security properties, the existing research work focuses on multiple security issues and solvable approaches for web services. Social networks are very popular and communicated applications used by multiple participants. In social networks, many individual users have an elaborated network with multiple logins. While accessing these networks, security is the major issue to be noted and the participant's details should be authenticated. Guanfeng Liu et al (2013) designed a novel complex network called Quality of Trust (QoT) to reduce the searching time of users to identify the identical social trust paths. Also, the novel multiple trust path selection algorithm called Multiple Foreseen Path Based (MFPB) algorithm – was designed by them to perform backward search procedure and Heuristic Optimal Social Trust Path (HOSTP) algorithm for forward search procedure. When compared to the existing Multi constrained Optimal Path Heuristic Multi constraint Optimal Path (H_MCOP), K node Multiple Constraint Social Path (MCSP_K) algorithms the MFPB - HOSTP algorithm produces better accuracy and makes easy to identify the shortest path.

Cloud computing is the emerging fielding that is used in all organizations focused on the development applications. In cloud environment, the services can be accessed from various sources to another destination. Cong Wang et al (2012) deliberated a cloud storage distributed architecture with which the client can easily audit and analyze the storage computation of a cloud environment. The designed architecture identifies the misbehaving server and clarifies the error correctness. Moreover, the architecture enhances the dependability and user can verify the correctness with light weight communication protocols. An error correcting code scheme is in their work to

reduce the errors and the explicit dynamic distributed scheme is used to easily update, delete and block the data in the cloud storage.

Service Oriented Architecture is a plug-in architecture that can be used by multiple service applications. Today, various companies developed their services with the SOA architecture and solve different consequences of business needs with SOA. Yang jun et al (2010) have proposed a novel authentication model that distributes the resources to produce the authenticated certificate according to the company requirements. The main advantage of this model is that it distributes the resources for companies and individual users effectively, so that the sharing of resources is made easy when they are distributed frequently at an available period of time. In this design, the certification was done with the Root Certificate Authentication function models. The model has three components known as Authentication Server (AS), Management Server (MS), Certificate Server (CS) and Information Database (IDB) to verify and produce certification based on the company requirements.

Access control for web services is a required one because web services come under the distributed systems and hence use network communication. The systems fall on to the unauthorized access of services from unknown parties. The secured accessing and introduction of intelligent base access control techniques predict different attacks in services. Hany Yamany et al (2010) defined a methodology which is based on the extension of WS-standards. The authentication and authorization of services provided with two components namely Authentication and Security Service (NSS) and Authorization Service (AS). The NSS receives the user requests in the form of Simple Object Access Protocol (SOAP) messages. It is first verified in the authentication part and then validated by the intelligent security. The security component was designed with the intelligent security parser, which parses the

SOAP messages and stores the verified messages in a security database. From the database, it next passes to data mining engine and association mining rules are applied there to predict the attacks by classifying the customers based on their requirements. As a final point, the intelligent security generates a report to the service providers to either accept or reject the SOAP requests with the needed requirements. The discussed Authentication and Security Service (NSS) for Service Oriented Architecture was intended and implemented with .NET,ASP.NET and visual studio 2005. Based on the existing systems on data mining, new access control techniques are proposed in this research work and hence it reduces the disadvantages in security and the categorization of service.

Basically, web services are adopted to run on different platforms. Services are platform independent and they can share the resources to other independent services. Jinpeng Wei et al (2008) have designed an architecture called Information Service Oriented – Web Service Platform (ISO-WSP) for secure transmission of data from multiple platform services. Here, the ISO-WSP platform is divided into two components namely Trusted – Web Service Platform (T-WSP) and Untrusted- Web Service Platform (U-WSP). T-WSP represents the trusted web service platforms and U-WSP represents untrusted web service platforms. During the transactions secure data are transferred from client to the service provider services using the trusted platform. Whenever, it requires the authenticated credential information it get them from T-WSP and unauthorized data moves on to U-WSP. Compared to the existing systems, this proposed ISO-WSP filters the trusted and untrusted source, also it interconnects a link between trusted platforms to the untrusted platform and hence the proposed model is secure and robust.

SOA architecture represents a distributing network that have all interconnected services a paradigm. In the analysis of this loosely coupled architecture, security is a considerable factor to estimate the services. Marco Anisetti et al (2013) proposed a test based security certification for the selection of services. The new techniques provide security based on the non functional requirements. The model is based on a testing approach which is used to test the service requirements and to provide security certification. With this approach, it provides customer confidentiality for choosing best services. The certification was evaluated in the point of service provider, certification authority and accredited laboratory. The progressing starts with the service properties as input and performs the evaluation and produces the valued certification. The proposed conceptual framework executes the cyclic process with the security property. The service properties are analyzed and it prepares the service model. Here, the matched requirements are verified and validated. From that, the unmatched data are discarded. After making the certified verification, the services are put for modeling analysis and test case generation. Different models have been proposed in this work to describe the test case generation. They are test driver based generation, service based generation and attack based generation. Compared with the existing security models, the proposed model for security test generation produces requirement match services to customers with better executed results.

In this study, the first layer of proposed Heterogeneous Offer Agreement Generation (HOAG) is discussed based on the set of incoming requests. The secured layer provides two types of encryptions and two types of decryptions. By that, it prevents the third party from judging the credential information. According to the customer requests, the authenticated requirements are filtered from the ‘Analyzer Security Originator’ layer and it further moves onto the ‘Classified Filter’ layer to reduce the bulk transactions.

1.6 CLASSIFICATION OF ORCHESTRATED WEB SERVICES

Web services are accessed by multiple customers through internet. The classifications of services are the required one to analyze and filter the category of services. For example, if a customer wants to book air or flight ticket through online, the travel booking services offered by the various service providers are shown on the menu. From the listed services, the user can select the opted and satisfied services. The selected service providers are providing multiple services, so they need to be validated and evaluated. The classification of services majorly depends on the factors of quality and trustiness of services.

1.6.1 Improving Data Quality of Web Services

The composed web services depend on the input requirements from the users. Before transmission from source to destination, the collected requirements are evaluated and checked for quality standards. In majority cases, the Quality of Standards are applied to reduce the vulnerabilities, infrastructure failures and network failures. Web services qualities are improved with the factors of reliability, scalability, availability, integrity and accessibility. These are the general standards to improve the quality with the base protocols of Simple Object Accessing Protocol (SOAP) and Universal Description Discovery and Integration (UDDI). In SOAP protocols, the Quality of Service (QoS) mechanisms are included in the header and body content blocks. Similarly, for UDDI repository may extent its data structure by including the business service standards.

1.6.2 Trust Worthiness of Services

Web services are secured with WS-security standards and more trust worthy services are accessed with the extension of WS-trust. Trustworthiness of services can be improved with the token exchange

patterns. The token exchange patterns are used to transmit the messages from various trust domains using the token keys designed with the certificates of X509 and Data Encryption Standard (DES) algorithms. According to the security parameters, Liwei liu et al (2013) introduced a recommender based system to select the content based service from a group of services. The recommender base systems are the one from which the user can select the preferred services from the existing history of services, where it has a database to store all set of existing datasets. The authors proposed two types of approaches to find the preferred services namely content based method and context based method. The content based services select the user required contents and context based services select the services using ranking and priority base data. From this recommender system, users can quickly get the predicted or searched results within the stipulated period of time.

Service composition is a service orchestrated technology to connect more number of services. In service composition, the selection of services and grouping of services is a difficult factor. Composed services can be used by any number of applications. For example, travel services and Hotel services can be combined to provide single application services. Jong Myoung Ko et al (2008) proposed a composition planning architecture to solve the quality service standards for the customer requirements. In this architecture, the customers can choose the required services, and the services could be composed from the selection of UDDI broker repository. Finally, services are evaluated by the execution plan provided in the planning architecture. The composition plans are verified with the tabu search and annealing meta heuristics methods. Comparing with the previous analysis works, this planning architecture provides a stable analysis for composition and execution of the composed services.

Web page classification is one of the challenging issues in recent trends. The retrieval of URL according to the multiple contents is researched by the authors Eda Baykan et al (2011) they conducted an evaluation with the corpora tool to classify the multi combination of URL web pages. The four different types of methods are used by them to classify the web pages as tokens, n-grams for tokens, n-grams for URLs and encoding positional information. The classifications of these methods are compared with the four different types of algorithms namely Naive Bayes (NB), Support Vector Machines (SVM), Maximum Entropy (ME) and Boosting. From the comparative analysis, this work achieves a high macro averaged F-measure than the previous algorithms.

Service Oriented Architecture is used in various technologies to improvise their applications. Donglai Zhu et al (2009) designed a city portal service oriented framework for the public services. The services accessed in the city portal include public services, Information services, entertainment services and community services. In this model, composed set of layers are framed to execute the city framework. They are user oriented service layer, application oriented interface layer, data oriented layer, city oriented infrastructure layer and operation oriented policy layer. From the analysis, the designed work has been accessed by multiple users and more effective applications.

The Information Technology (IT) based business processes are nowadays executed with the Distributed Transaction Processing (DTP) systems. These DTP systems work without the help of human being interactions. In business processing, the service providers have to deal with more demand variation. The variations are caused because of the adaptive prioritization. Christian Markl et al (2010) analyzed the performance and capacity of the DTP systems. This work analyzes how the DTP system

improves queue processing and reduces the adaptive prioritization with queuing theory. This research work elaborates using the Queuing Network Model (QNM) and the arrived jobs are queued with the service stations. The stations have the single or parallel servers. The queuing networks are categorized as open queuing network, closed queuing network and mixed queuing network.

The QNM model was based on the mixed queuing model. In this model, the jobs can enter, leave and circulate in the closed network. An individual node in QNM model was designed with input station, server station and output station. The input station receives the input load and stores it for a particular period of time. Server station executes the arrived inputs and does the execution, within the period of time. After finishing server station execution the output next moves to the output station. This station finishes the jobs that are ordered in a sequential manner and are sent to the distribution. This adaptive workload prioritization reduces the workload in IT oriented business transactions. For example, the credit card transactions are used by many number of consumer applications. During purchase, the transactions are sequentially queued with the QNM model.

1.7 CREATION AND GENERATION OF SERVICE LEVEL AGREEMENT

Service Level Agreement (SLA) is necessary for web services. Generated agreements are valuable and confidential between service providers and consuming customers. Based on the agreement generation a restricted period of time is allotted for the customers to choose the preferred services. During agreement generation, the service providers may expect to rise with some problems. The agreement gets capriciously categorized based on the problems that arise like DoS attacks, Hardware failures, and credit transactions.

1.7.1 DoS Attacks in SLA Generation

Denial of Service (DoS) attacks are one of the curious attacks to infiltrate the network links, routers and firewalls. These attacks not only affect the networks, but also are helpful for cyber attackers to hack the informations. The attack happens based on stealing of packet data from the transmission protocols. By retrieving the protocol packets, the hackers may easily hack the provider information. Two types of attacks are represented with the DoS attacks namely bandwidth attacks and application attacks. Bandwidth attacks spoof the source address and track the IP address by Transmission Control Protocol (TCP) protocol and Internet Control Message Protocols (ICMP). Using these protocols, hackers affect the targeted resource and lacerate the targeted information.

The application attacks can hack the valuable resources of the service provider services. Hyper Text Transfer Protocol (HTTP) protocols are one of the protocols to be used to hack the provider resources. To prevent the DoS attacks for the agreement generation, various strategies are used. They are through routers, firewalls and Id. The router will block the unknown IP address accessing with service provider. Also it prevents the attacks from application layer of HTTP. In second way, firewalls provide the required security and control on the user accessing from unknown networks. During transmission, firewalls provide antispoofing technique to filter the affected packets from the transmission packets. Using the Id, signature can be verified for identification based on the verification of sender signature during message transmissions.

1.7.2 Hardware Failures

If the service agreements are not communicated successfully from source to destination it may be due to different criteria including hardware failure. Hardware failure may occur with the infrastructure, network timings

and server hardware replacement. The first reason may be defined with the infrastructure based on the power supplies, fault in Uninterrupted Power Supply (UPS) and cabling. Also, the availability of services is based on one of the criteria for these infrastructures. Second reason is with the network timing of services. The services are available and unavailable with the availability of internet connectivity. The service provider has the duration of timing services to be availed by the required clients. Third the hardware failure may occur due to the server hardware replacement. The failure may occur due to the replacement of components in the mother board and in hard disk.

Hardware failures can be rectified by notifying the storage capability and monitoring network performance. Storage capability gets varied from one service provider to other set of providers. Also, the storage problems can be rectified through the distributed networks.ie the resource data are shared in cloud storage with a schedule management is utilized by multiple clients. The other way of reducing hardware failures is to have the proper back up to store the required hardware components like RAM, Mother board and other essential elements.

1.7.3 Credit Transactions

Mostly credit transaction failure may occur during the payment transactions from customers. Services are to be monitored and activated based on the timings provided by concern providers. The credit transaction failures occur because of the improper internet connectivity and unauthorized customer details. In such scenario, credit transactions failures are rectified by allotment of timings to the service providers. The timing may be set as 8hours, 12 hours or 24 hours according to the availability of services. The discussed issues are defined for agreement generation and be rectified with various technologies and methods. Various research works in the past focus on agreement generation for the composed services. They are as follows,

The customers and service providers are bonded with the concept of Service Level Agreements. Here, the SLA plays an active role between two parties. Generation of offer agreement from a service provider was proposed by Azlan Ismail et al (2010) where providers provide the offer services to the customers. If the customers are satisfied with the offer agreement they can bond an agreement with the provider. In offer agreement generation, multiple customers who are accessing can be scheduled with the time slot scheduler and finally could be evaluated by the two types of evaluations namely constraint based and objective based evaluations. Compared to the previous research works on services, this work provides better facilities for customers and hence they can easily identify the quality of services.

Farhana et al (2011) designed a framework called negotiation broker for Service Level Agreement generation. This broker service performs the agreement generation between customers and providers. The bilateral accessing can be performed with the two concepts known as adaptive algorithm and intelligent algorithm. The first algorithm schedules the time slots with the arrival of user requests. Threshold value is set in this model to compare and check if the constraints of the offer exceed the given limit. The second algorithm provides the comparative analysis of multiple strategies with respect to the price and policy factors. The brokers usually act as the agent for negotiation and to gather the feedback from the negotiating parties. Finally, negotiated agreement gets validated by the three types of algorithms namely exponential, polynomial and sigmoid time based decision functions. This work mainly focuses on the bilateral decision making agreement between the two parties. So, that evaluation is processed easily and quickly than the other works for multilateral decisions.

Web services are web applications that are accessed only through the internet. The services not only provide service functionalities but also are utilized as business collaborators. The Business to Business (B2B)

collaborations are interacted only with the web services. Li Guo (2010) introduced a web service based agent platform that solves the issues of B2B collaborations. The critical factors that affect the business of security, complexity and trust are analyzed and solved with this platform architecture. Agents that are used in this B2B collaboration use the Light Weight Coordination Calculus (LWCC) protocol and act as communication language between one agent to other agent. The collaborative business process is activated with this agent concept. This proposed multi agent platform solves the technical issues defined in the open distributed systems.

Generation of agreements for multi party customers and providers is a challenging field in agreement generation. Andreas Klenk et al (2012) invented a novel protocol to be applied to multi negotiation parties. The multiple requirements can be satisfied with this protocol in which the defined protocol is incorporated for service business process. The implementation of this concept provides the parties to choose the offered services from multiple providers. If the requirements have the accepted condition that matched with the defined novel protocol parameters then an agreement is generated and produced to the customers. Compared to the works on bilateral services this multi lateral service model provides a novel protocol to be accessed with multiple customers.

1.7.4 Fuzzy Approach for Service Agreement Generation

Fuzzy is a rule based logic that derives the true or false rate according to the defined condition. The fuzzy based conditions are applicable to all set of relevant fields to define their own basic knowledge. Slobodan Ribaric and Tomislav Hrkac (2012) proposed a fuzzy based temporal knowledge system called the Petri net with fuzzy spatio temporal tokens system for multi agent based systems. For such type of systems, the moving position has been noted as the spatial temporal relationships. The system was

designed and implemented with the help of petrinet and spatio temporal tokens. It uses a table format to represent temporal information that collected from spatial and temporal information modules. It stores 117 spatio temporal relationships for the test simulation process. By using this approach, it is easy to identify the moving position of an agent application in real time systems.

In web service composition, the input and output data are based on the retrieval or grouping of services. A new method for the ranking of service compositions was proposed by Karim Benouaret et al (2011) where the ranks of web services are performed using the logic of top k data service composition. Also the services are classified as “cheap”, “affordable” and “fairly expensive”. With the Resource Description Framework (RDF) a query language is framed to design a query algorithm to identify and rank the user defined query. Also, the ranking is stated with the fuzzy concept oriented pareto dominance method. To make the suitable service composition as the user design, the queries are provided in SPARQL query language. Therefore, the service ranking with fuzzy language identifies the best service from a group of services for composition effectively.

Ben Wang et al (2010) proposed a trust worthy evaluation model called Trustworthy Software Tools and Integration Environment (TRUSTIE-STE) for web services. The model has been designed with the combination of two methods called trust evidence framework and dynamic repudiation feedback. The model was framed with the measurable trust factors namely availability, reliability, security and maintainability. Fuzzy trust is designed by a map called Fuzzy Cognitive Map. In this map the graph has stated with the group of policies and events. Trust calculation is assessed with two phases called Initialization phase and Run time phase. In initialization phase, the static evidences are collected and applied during the deployment of services. Run time phase uses the dynamic evidences which are changeable during

deployment time. The resultant model was so efficient for measuring the trust worthiness of web services.

The web services are web based applications that are mostly accessed with the Internet. During accessing of service, many unauthorized controversies may occur in packet transmission. Autonomic self provisioning are the frequently occurring errors in internet which makes delay in transmission while communicating through multi tier systems. In multi tier system architecture, particular layer functionality was based on the next or previous layer functionality. To reduce the complex frequencies and to unbalance workloads in multi tier system architecture, Palden Lama & Xiaobo zhou (2013) introduced a new approach called Neural Fuzzy Control (NFC) independent model. Compared to the existing models, NFC control model produces high performance in unequalized workloads. This fuzzy controller mainly reduces and guarantees the 95^{th} percentile delays in multi tier architecture. The self adaptive neural fuzzy control was designed by the authors with online learning algorithm, multi tier server clusters and self adaptive neural fuzzy controller. Also, the adaptive controller was interlinked with the online learning algorithm and multi tier server clusters. The controller takes two inputs called ‘error denoted’ and ‘change in error denoted’. Mainly online learning algorithms were designed with the reference to machine learning algorithms. Moreover, the controller predicts the errors from the target source error rate with the measured value of the percentile calculation. The advantage of this fuzzy controller is that it reduces the dynamic workloads and improves the end to end delay assertion.

The service composition has a group of collective services, where one service output is used as an input to other service. During composition of services, multiple work flows are organized and produce significant outputs. From the survey analysis of workflow, Shrija Rajbhandari et al (2008)

proposed a workflow trust model for the grouped services. This model takes the workflow data as input and analyzes with fuzzy inference rules and produces the trusted outputs. Normally, the workflow generation was categorized as ‘abstract’ and ‘physical’ workflow descriptions. The abstract descriptions have overall view of the activated services. The physical descriptions elaborate the instance services that interlinked in a group service. The authors elaborated this work with a trust model and it represents the work with the provenance data.

The workflow trust model was designed with the elements of decision tree process, fuzzy reasoning tool and analysis tool. The process was initiated with the evaluated workflow. Initially, the decision tree process was executed with the provenance data. The provenance storage have the collection of provenance set of data that are utilized for the workflow analysis. At first, the scientist will manually analyze the workflow and then sent them to the decision tree process. The tree analysis makes the finalized decisions for the intake services. The logically matched workflows are framed as tree format and sent to the provenance data store. The store data was mapped with the service actors and client actors. They can manage the services according to the workloads and then forward them to the analysis tool. Here the workflow patterns are analyzed and if any unmatched pattern is found, the data is again sent to the storage. Finally, the matched workflow patterns are executed using fuzzy rules that are mapped using the fuzzy reasoning tool. The rules are used to execute the work flows and to produce trustable finalized output to the linked service. While comparing with the existing works, this fuzzy work flow analysis provides a trustable output to the activated services.

The fuzzy logics and rules are used in various types of applications. The information summarization and information retrieval are some of the research areas that use fuzzy rules. Han Saem Park et al (2011) proposed a

framework for modeling the video life logs with the concept of indoor multi camera system. This video life logs model was designed for an office environment and summarizes all events by using a fuzzy rule based system. Summarization represents events and sequence of actions. The fuzzy rule based system calculates all summaries based on the annotations, events and objects involved in the sequence. The camera captured clicks are stored in the database and domain knowledge component have the domain knowledgeable views from the customers. Once the domain has been fixed, the user information from the domain are passed to the view selection mode. Here, the rules for event selection, transition and duration are monitored. From the monitored rule, it next moves onto the summarization to frame or design the fuzzy rules with respect to the captured life logs. The users can quickly update and execute the life log events through the analysis logs.

1.8 PROPOSED WORK

This research work focuses on the heterogeneous agreement generation for the multi level customers. In web service business process, more number of services are offered to the customers. The customers can choose the opted services that satisfy their requirements and match with their requirements. To reduce the searching time and to get a quality in offered service, this research work proposes a framework called Heterogeneous Offer Agreement Generation (HOAG). Through this framework, the customer can search the offered services that are listed. From the list, the customers can choose the preferred services and acknowledge with a service agreement.

While searching the preferred services, initially the requirements are collected from various customers. Requirements are validated with three layers known as Analyzer Security Originator, Classified Filter and Fuzzy Based Agreement Generator. Layer 1 provides security, Layer 2 provides filtering and Layer 3 provides agreement generation. Finally, the generated

agreement is sent for customer approval. From that, the customer selects the required services. The advantage of using this proposed system is that it will reduces the search time of customers to choose preferred services based on their requirements.

1.9 MAJOR CONTRIBUTIONS OF THE THESIS

This thesis focuses on the three types of contributions proposed to solve the problem of search time optimization. The first contribution discusses the process in which the incoming requests are filtered and securely generated in the first layer. The second contribution discusses about the techniques used for the classification of secured data to reduce the bulk arrival of requests in the second layer. The third contribution finalizes the fuzzy based agreement generation techniques used for handling multiple customers in the third layer. Here, the defined requirements are matched and if satisfied, the agreement is sent for the customer approval.

1.9.1 Contributions in Security

Security is an important issue in web services. In the proposed framework called Heterogeneous Offer Agreement Generation (HOAG) framework, the parameters of security, classification and agreement generation are the three functionalities that are defined clearly. In the layer 1 named ‘Analyzer Security Originator’ the evaluation of the security process is carried out. The purpose of providing security is to analyze the incoming requests and to validate the credentials. The main contribution of this Analyzer Security Originator is that it evaluates the security process using the sub components of Information Package (IP), Password Transaction – Secure Identity (PT-SI) records, Extracted Database, Enforcer algorithms, Arbitrator and Centralizer.

Initially, credential information are gathered in the Information packages. The package is the collective package, where it collects the credential information like shop code (service Id), bill no, card no, password and transaction Id. After collecting these, authenticated details are further passed to the Password Transaction – Service Identity (PT-SI) records to filter the authenticated data like password, transaction Id and service Id. Two packages are defined here namely the Password Transaction known as 'PT' and Service Identity 'SI'. PT is used to collect the password and transaction Id's and SI collects the service identity. Before doing the transmission, the PT-SI records are once again rechecked with the Extracted Database.

From the verification, it finally moves to the secured generation of proposed Enforcer component. Here, the sub components included are Enforcer E1, Enforcer E2, Enforcer D3 and Enforcer D4. The first two sub components perform the processing of encryptions and second two components perform decryptions. The purpose of providing such encryption and decryption is that the hacker cannot judge the secret keys easily and hence it is not possible for him to collect data from the credential information. Finally, the encrypted and decrypted keys are stored in the repository as a temporary copy and it is interlinked with the Arbitrator.

1.9.2 Contributions in Requirement Classification

The incoming requests from security layer are next processed with the 'Classified Filter'. The major aim of requirement classification is to diminish the bulk arrival of requests from the security layer. In HOAG, the Classified Filter has different sub components namely Multi Classifier Mixture (MCM), Collective Group-Efficient Trim Down (CG-ETD) classifier, Accuracy Analyzer and Request Recognizer.

The classification starts from the Multi Classifier Mixture which is used to collect the secured credential information from the secured layer. This mixture has been designed to collect all the incoming filtered requirements from layer 1. After collecting them, the secured information are classified using the Collective Group – Efficient Trim Down (CG-ETD) classifiers. This classifier has the comparative collection of four classifiers called Collective Group (CG) classifiers and the proposed Efficient Trim Down (ETD) classifier. The proposed ETD classifier provides better classification accuracy when compared to the existing classifier. The data that are classified accuracy moves to the Accuracy Analyzer.

The Analyzer has the finalized comparison parameters of accurate data and moves on to the bank progression module. The bank progression module validates the data using the sub component called Request Recognizer. The Recognizer sends the queued data to the particular service provider services. Therefore the, requirement classification reduces the overloading of incoming requirements and executes the accurate data for the service providers.

1.9.3 Contributions in Fuzzy Based Service Agreement Generation

'Fuzzy Based Agreement Generator' is the final agreement generation layer to the customers. From the execution of layer 1 and layer 2, it next moves on to the Fuzzy Based Agreement Generator. The contribution of this layer is to generate the fuzzy agreement for the required customers.

The components designed with this fuzzy based agreement generation layers are Service providers, Multi Negotiation Broker, Decision Manager, Expert Advice, User Requirements, Fuzzy Support - SLA and Consumer Approval. The execution starts using the received requirements from the Service providers. The Multi Negotiation Broker has the temporary

copies to store the collective services from the Service providers. The broker has the interconnectivity to the Decision Manager since the manager is the deciding authority to generate the final fuzzy based agreement. The Decision Manager will make the decisions from the concluded analysis from existing User Oriented Database, Expert Advice and User Requirements. Based on the arrival of user requirements, the required data get matched from the service provider list and are analyzed with the Decision Manager. If the customers are satisfied with the agreement generation, they accept to buy the services or they may discard it.

The purpose of designing the third layer is to reduce the searching time of the customers who search the opted and available services based on their requirements.

1.10 ORGANIZATION OF THE THESIS

The reminder of the thesis organized as follows

Chapter 2 provides a review of literature survey carried out on security logic, prevention of attacks in web services, reduction of risk factors in services, rule generation and agreement matching of services.

Chapter 3 presents the overall architecture of the system developed for web service called Heterogeneous Offer Agreement Generation (HOAG) system

Chapter 4 describes the techniques used in layer 1 called Analyzer and Security Originator of web services and the proposed Enforcer algorithms.

Chapters 5 explain the layer 2 technique used for Classified Filtering of the authenticated services by using the proposed Efficient Trim Down classifier.

Chapter 6 details the layer 3 technique agreement generation process using the proposed algorithm present in Fuzzy Based Offer Agreement Generator.

Chapter 7 gives the conclusion of this work and suggests some possible future enhancements.