Recent Advanced Computing Methods Employed in Web Service Automation - A Survey

Chaitanya Raveendra[1] Dr.S. Manju Priya[2] Dr. M.Thiyagarajan[3]

1. Research Scholar, Department of Computer Science,Karpagam Academy of Higher Education,Coimbatore, Tamil Nadu, India - 641 008
2. Associate Professor , Department of Computer Science,Karpagam Academy of Higher Education,Coimbatore, Tamilnadu- 641 021
3. Professor Emeritus and Dean Research, Research Cell, Nehru Group of Institutions, Kuniamuthur, Coimbatore, Tamil Nadu - 641 008

Abstract

Web Service Automation gains momentum for the past two decades. So, various computational algorithms have been developed on different aspects of web service categorization and resource allocation. Research activities are more on comparing the algorithms over time and space complexity. Web designers and service providers make their contribution to enrich the IT products in this area. In this paper, a detail study is attempted on the above aspects of web service Automation. We open an area of web technology for implementation of newer algorithms.

Keywords - Web Service Allocation, Zero Knowledge Authentication, Logic Programming, Service Computing, Distributed Algorithms, Cloud computing.

I. Introduction

The users have the basic demand and browse the internet in their assumption that the network is reliable, latency is zero and further there is a single administrator. These fallacies are overcome by understanding the service and modeling it in a larger scenario of computational technology as automated services. In this paper, a survey and analysis of web services, composition and basic finite state models are explained.

II. User Categorisation and Resource Allocation

In operational research, resources are to be allocated to individuals depending upon the inventory level. These algorithms cannot be applied to web resources as content allocations are put in hyper texts and links [16]. The service accesses are of different orientation and execution of larger links to be serialized is put on a sequence. Different jobs enter the node of specific processors in various stages of implementation. This leads to the distributed computing environment and newer types of algorithms have to be designed. One such algorithm that are studied in detail is circular token Algorithm.

The execution and implementation of that algorithm was suggested by Nancy Lynch [4] through predicate calculus and needs a specialized language. Nancy Lynch and Jennifer [10] develop an automaton representing the resource allocation algorithm used to allocate the resources. A resource allocation algorithm decides which user gets which resources at which time; thus, it supplies the code for the trying and exit regions. A distributed resource allocation algorithm consists of one component for each user; the component communicates with each other by message passing. They develop an I/O model of the resource allocation module which is useful in stating the properties that concern the infinite behavior of the system, such as no-deadlock and no-lockout, and which supports modular algorithm design and verification.

These abstract commands should be transformed in to real time execution by converting these modules in to java API. The work on two basic models of resource allocation by Thiyagarajan [18] is given in java. They have given positive hit matrix, negative hit matrix and total hit matrix. So we conclude that service providers can increase the users from other categories to update the specialized service. The frequent access of the users may be inferred as an attempt as external non members attempting as users. This algorithm needs further improvement in applying security to multi users, multi access rights.

III. Authentication

According to William Stallings [19], the most efficient way to handle the intruders and the malicious software is the implementation of the trusted system technology. Trusted system deals with the protection of data or resources based on the basis of the permission of the user. This when implemented in the network can be called as trusted network security. Thus when applied in the web, we are having a set of users and the set of data that can be accessed by the users. Trusted system implements the authentication of the file a user handles. It is mainly handled using access control using access matrix or an access control list.

An alternative to the Man in the Middle Attack [MITM] is use of Zero Knowledge Proof Protocols (ZKP). Wang Huging and Sun Zhixin [5] published an article elaborating the concept, nature, mathematics theory, general proof process of the zero knowledge proof, focusing on the application research polynomial function root, graph isomorphism, cloud storage service, RFID, proxy digital signature and identity authentication. It is very important that proving to each other the identity of the user information in authentication and digital signatures.

If "zero-knowledge" means identify information, then zero-knowledge proof protocol can be applied to identity authentication. The common authentication requires transmission of password or personal secret information, which will give attackers loopholes to attack more or less. With zero-knowledge proof of identity, one can prove himself legal to the system without transferring above information. There are large protocol has great superiority and importance in the field of authentication is the first that had been proposed, while it is the most basic authentication scheme. The main idea of zero knowledge proofs is as follows: P (the Prover) had some secret information. P wanted to prove to V (the Verifier) by taking other proof process without revealing anything other than the fact that it knows in order to prevent the confidential information from leaking to anyone (including V or any other third party).

This section describes the Classical Zero Knowledge Protocol based on Fiat-Shamir, Guillou Quisquater [5] based on hard number theory and variation of zero knowledge using graphs. Zero-knowledge proof protocol can be applied for identity authentication. The common authentication requires transmission of password or personal secret information, which will give attackers loopholes to attack. With zero-knowledge proof of identity, one can prove himself legal to the system without transferring above information. There are large amounts of documents to show that zero-knowledge proof protocol has great superiority and importance in the field of authentication, Fiat-Shamir authentication is the first that had been proposed, while it is the most basic zero-knowledge authentication scheme. The process of Fiat-Shamir authentication is shown in Figure 1 [5].

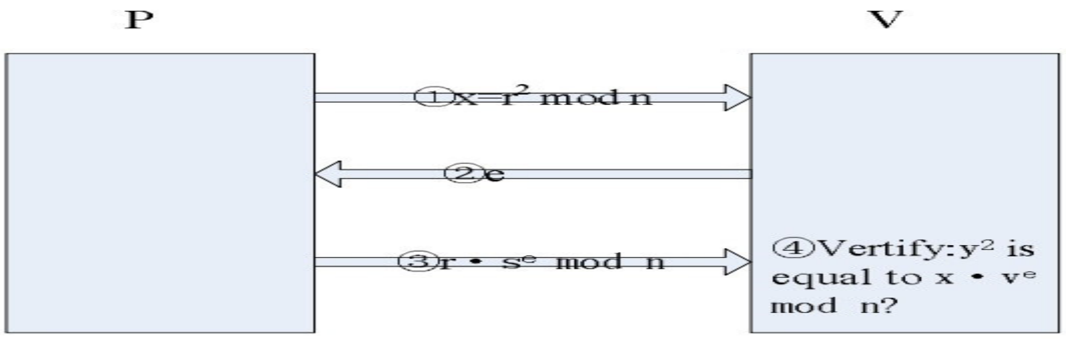

Fig. 1 Fiat Shamir Authentication Process

Guillou-Quisquater Algorithm is an extension of the Fiat-Shamir which uses the mathematical problem of the square root problem of modulo n. Given a positive integer n, a ∈ Z_n, if there exists x ∈ $Z_{n,}$ that makes $x^2 \equiv$ a (mod n), then x is called a square root of modulo n. The calculation problem of the discrete logarithm, given a prime number p and a, which is one of the primitive element on the finite field Zp. To p on Zp, looking for one and only integer c that makes a^c ≡ b(mod p).

Two Graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ that have the same sets of vertices $V_1 = V_2 = \{1,2,\ldots..n\}$ are isomorphic, if there exists a permutation π on vertices $\{1,2,..,n\}$ so that $(u, v) \in E_1 \leftrightarrow (\pi(u), \pi(v)) \in E_2$. Two graphs *G1* and *G2* are said to be isomorphic, if a one-to-one permutation or mapping exists between the set of vertices of *G1* and the set of vertices of G2, with the property that if two nodes of *G1* are adjacent, so are their images in *G2*. The graph isomorphism problem is therefore the problem of determining whether two given graphs are isomorphic. Figure 2 describes the isomorphic graph for 5 vertices. Graph (b) & (c) is generated by rearranging the vertices of graph (a) and the generated graph is an Isomorphic graph [20].

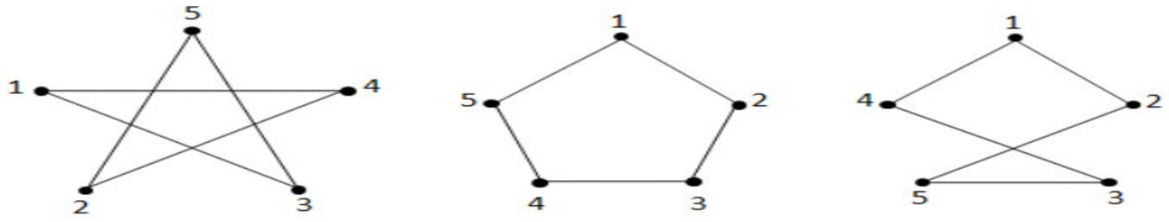

Fig. 2: Graph Isomorphism

Eric Ayeh [20] assess the graph Isomorphism based Zero Knowledge Proofs in his paper Graph Isomorphism based Zero Knowledge proofs. In order to effectively prevent unauthorized users impersonating legitimate users, one can use zero-knowledge proof protocol to authenticate. Both of the above two classical algorithms (Fiat Shamir and Guillou Quisquarter) on zero knowledge protocol is based on hard number theory and it involves the computation of large numbers. Thus a simple approach has to be developed using the Graph Isomorphism and basic zero knowledge proof protocol.

IV. Finite State Automation Model

According to basic definition of finite state automata, it is one of the most significant developments has been the discovery of the model checking technique, that automatically allows to verify on-going behaviors of reactive systems. Hopcroft, Motwani and Ullman [3] defines an NFA as a finite set of states, a finite set of input symbols, on start state and a set of accepting states as its output. It has a transition function δ which takes a state and an input symbol as argument but returns a set of zero, one, or more state.

According to Johan Bengtsson and Wang Yi [9,11], A timed automaton is essentially a finite automaton (that is a graph containing a finite set of nodes or locations and a finite set of labeled edges) extended with real-valued variables. Such an automaton may be considered as an abstract model of a timed system. The variables model the logical clocks in the system that is initialized with zero when the system is started, and then increase synchronously with the same rate. Clock constraints *i.e.* guards on edges are used to restrict the behavior of the automaton.

Basic definition of PDA is, Pushdown automata is a finite automata with auxiliary storage devices called stacks. (A stack is merely a pile and symbols are normally placed on stacks rather than various colored discs.) The rules involving stacks and their contents are: a) Symbols must always be placed upon the top of the stack. b) Only the top symbol of a stack can be read. c) No symbol other than the top one can be removed.

Daniela BERARDI, Fabio DE ROSA, Luca DE SANTIS and Massimo MECELLA [6], each interaction of an eservice is described by the triple < input command, internal computation, output message >; however, by adopting a black box approach, we skip over internal computations and represent only the input/output behavior of e-Service from the client view point, i.e., that have some effects towards the client: each interaction is therefore described by the pair < input command, output message >only.

Web service Automation aims at reducing the time and space complexity in search and implementation process. We want finite state transition to complete our search techniques. The nodes of the search are mapped to the states of Finite State Automata introduced by Hopcroft in Noam Chomsky Hierarchy Language.

V. Semantic Outlook

Almendros-Jiménez et al [1] have presented a proposal for the implementation of the XPath language in logic programming. They described the representation of XML documents by means of a logic program. In this context, rules and facts are used for representing the document schema and the XML document itself. In particular, they described as to how to represent indexes of XML documents in logic programs. That is, rules are stored in many memories by using two kinds of indexes, one for each XML tag, and other for each group of terminal items. One can query a logic programs which represents an XML document by means of the XPath language. This evolves the specialization of the logic program with regard to the XPath expression. Finally, they explained as to how to combine the indexing and the top-down evaluation of the logic program.

Martin Zima and Karel Jezek [13] have provided information on how web documents written in the XML language can be rewritten into logic forms in terms of programs in Prolog. The XML language constitutes the basis of many semantic web languages and information in XML documents is usually retrieved with the help of procedural language called XQuery. Retrieving based on logic formulas gives us the chance to take advantage of logical deduction and in this way to gain new originally hidden information.

Bernd D. Heumesser, Andreas Ludwig and Dietmar Seipel [12] have studied web service based on Logic Programming and XML [21]. They have observed the series of new approaches for web services. The World Wide Web as we know it today was initially designed as a platform for information sharing. The core Web technologies i.e., HTTP, HTML, Web servers and Web browsers, enable the exchange of information in the form of documents.

Service has to be analyzed and action has to be performed based on the semantics of the request. Web documents are presented based on the request but not based on the meaning or semantics of the request. Thus there arises a need to develop a semantic outlook to the web service Automation.

VI. Web service composition

Web Service Architecture Working Group defining a Web service as “a software system identified by a URI, whose public interfaces and bindings are defined and described using XML. Its definition can be discovered by other software systems. These systems may then interact with the Web service in a manner prescribed by its definition using XML based messages conveyed by Internet protocols”. A Web service is a software system designed to support interoperable machine-to-machine interaction over a network. It has an interface described in a machine-processable format (specifically WSDL). Other systems interact with the Web service in a manner prescribed by its description using SOAP messages, typically conveyed using HTTP with an XML serialization in conjunction with other Web-related standards.

G. Geetha and Rohit Dhand [2] presented a concept of Trust based System that can help in access control of different web services. Service Oriented Architecture has emerged as one of the main standards of writing software in the modern era. With the growing demand of cloud computing and ever increasing implementation of web services, problems of authorization control of these web services are also shooting up. With numerous web services hosted up, it would become a cumbersome process to manually provide access control to the users by the system administrators. The paper describes about a semi-intelligent system that works on the mechanism of Trust to automate the task of access control.

Service composition, its enhancement goals and advances is explained well by Munindr Singh [7]. Most of the applications touted for Web service are simple and straightforward client-server interactions. Service composition has been studied in the research literature for quite some time, but it is now becoming an important theme in practical Web system development. The basic idea behind service composition is simple. Web sites can be thought of as not only offering content, but also providing services. These services could be typically invoked by hand through a Web browser, but a program could invoke them directly. Service composition on the Web is about taking some existing services and building new customized services out of them. It needs to create a work flow over the existing services.

Business Process Execution Language for Web service (BPEL or BPEL4WS) is a language used for the definition and execution of business processes using Web service. BPEL enables the top-down realization of Service Oriented Architecture (SOA) through composition, orchestration, and coordination of Web service [14]. BPEL provides a relatively easy and straightforward way to compose several Web service into new composite services called business processes. BPEL builds on the foundation of XML and Web service; it uses an XML-based language that supports the Web service technology stack, including SOAP, WSDL (Web Service Description Language), UDDI (Universal Description, Discovery, and Integration), WS-Reliable Messaging, WS-Addressing, WS-Coordination, and WS-Transaction.Web service has to be composed and it has to be further extended to implement using J2EE for general application.

VII. Cloud Computing and Network Security Analysis

Gubbi, Marusic, Palaniswami [8] defines the internet of things for smart environment as the “Interconnection of sensing and actuating devices providing the ability to share information across platforms though a unified framework, developing a common operating picture for enabling innovative applications. This is achieved by seamless ubiquitous sensing, data analytics and information representation with cloud computing as the unifying framework”. The future lies in the ubiquitous sensing of devices in a communicating network. RFID and sensor technologies are used to sense the device in turn results in the huge data storage and each such service can be modeled in a reusable form. The traditional computing from the PC will move on to the machine to machine interactions.

For the realization of a complete IoT vision, an efficient, secure, scalable and market oriented computing and storage resourcing is essential. An integrated IoT and Cloud computing applications enabling the creation of smart environments such as Smart Cities need to be able to (a) combine services offered by multiple stakeholders and (b) scale to support a large number of users in a reliable and decentralized manner. They need to be able operate in both wired and wireless network environments and deal with constraints such as access devices or data sources with limited power and unreliable connectivity. The Cloud application platforms need to be enhanced to support (a) the rapid creation of applications by providing domain specific programming tools and environments and (b) seamless execution of applications harnessing capabilities of multiple dynamic and heterogeneous resources to meet quality of service requirements of diverse users. The Cloud resource management and scheduling system should be able to dynamically prioritize requests and provision resources such that critical requests are served in real time.

Christina Turc, Cornel Turc and Vasile Gaitan [17] explain on the communication Technology for data identification and security aspects. Radio frequency identification (RFID) is an Automatic Identification and Data Capture (AIDC) technology that uses radio waves to automatically identify entities (people or objects), allowing the collection of data about them and storing that data into computer systems. Thus, RFID technology enables various entities to be uniquely identified in the Internet of Things. There are a number of characteristics particular to RFID which make this technology superior to former technology like barcodes in terms of

(1) non-optical proximity communication,
(2) information density,
(3) two-way communication ability and
(4) multiple simultaneous reading (the reading of more than one item at a time).

The basic RFID system architecture has three major components: contactless electronic tags to store unique identification data and other specific information, an RFID reader (to read and write these tags) and processing elements (application components).

Security will be a major concern wherever networks are deployed at large scale [15]. There can be many ways the system could be attacked—disabling the network availability; pushing erroneous data into the network; accessing personal information; etc. The three physical components of IoT—RFID, WSN and cloud are vulnerable to such attacks. Security is critical to any network and the first line of defense against data corruption is cryptography. Security in the cloud is another important area of research which will need more attention. Along with the presence of the data and tools, cloud also handles economics of IoT which will make it a bigger threat from attackers. Security and identity protection becomes critical in hybrid clouds where private as well as public clouds will be used by businesses.

VIII. Conclusion

Web service Automation has become very important component in web Technology. The web search is in demand from both academicians and e Service providers. Various aspects in bringing together the industrial and research group implements recent computational technologies with the advent of sophisticated computing machines. Distributed computing environment embraces various computing techniques such as service computing, distributed computing and ubiquitous computing.

IX. References

[1] Almendros-Jiménez, J.M., Becerra A-Terón and Enciso F.J. -Baños, “Querying XML Documents in Logic Programming”, Journal of Theory and Practice of Logic, programming , TPLP 323-361, Vol.8 No.3, pp.323-361, 2008.

[2] Geetha G, RohithDhand, "Controlling Web Services through a Trust Based System”, International Conference on Information and Computer Applications, (ICICA 2012), Vol.24, pp.48-51, 2012

[3] John E.Hopcraft, Rajeev Motwani, Jeffrey.D. Ullmann, “Introduction to Automata Theory, Languages and Computation”, (3rd Ed.) Pearson Education, New Delhi 2013

[4] Nancy Lynch, “Distributed Algorithms”, Harcourt Asia Pvt Ltd, Morgan Kaufmann, India, (2000)

[5] Wang Huqing and Sun Zhixin : ‘Research on Zero-Knowledge proof Protocol’, IJCSI - International Journal of Computer Science Issues, Vol.10, No.1, pp.194-200, January 2013

[6] Daniela Berardi, Fabio De Rosa, Luca De Santis & Massimo Mecella, “ Finite State Automata As Conceptual Model For E-Services”, Journal of Integrated Design & Process Science, Vol.8, No.2, pp.105-121, 2004

[7] S.P.Munindr, H.N.Michael, “Service-Oriented Computing Semantics, Processes, Agents”, John Wiley Sons, INC, UK, 2005

[8] Jayavardhana Gubbi, Rajkumar Buyya, bSlaven Marusic, Marimuthu Palaniswami, “Internet of Things (IoT): A vision, architectural elements, and future directions”, Future Generation Computer Systems, pp: 759-760, September 2013

[9] Johan Bengtsson and Wang Yi, Timed Automata: Semantics, Algorithms and Tools, Lectures on Concurrency and PetriNets pp: 87-124 2004

[10]Nancy Lynch, Jennifer L. Welch, “Synthesis of Efficient Drinking Philosophers Algorithm”, Technical Report, MIT/LCS/TM-417, MIT Laboratory for Computer Science, January 1990

[11] Rajeev Alur, David L. Dill, “Theory of Timed Automata Theoretical Computer Science” Vol.126, No.2, pp.183-235; April 1994

[12] Bernd D. Heumesser, Andreas Ludwig and Dietmar Seipel, "Web Services Based on PROLOG and XML", Vol.3392, pp.245-257, 2005.

[13]Martin Zima and Karel Jazek, “Translation of XML documents into logic programs”, Publishing in the networked world: transforming the nature of communication, 14th International conference on electronic publishing, pp.350-362, Finland, June 2010.

[14] Yuhong Yan, Philippe Dague, Yannick Pencole and Marie-Odile Cordier, “A Model based Approach for Diagnosing Faults in Web Service Processes”, National Research Council, 46, Dineen Drive, Fredericton, France

[15] Philip Levis, “Secure Internet of Things”, Secure Internet of Things Workshop, Standford University, pp. 1-34, August 2014

[16] Alok Gupta, Dale. O. Stahl and Andrew. B. Whinston, Managing Computing Resources in Intranets: an Electronic Commerce Perspective”, Decision Support System, Vol.24, No.1, pp:55-69, November 1998

[17] Christina Turc, Cornel Turc, Vasile Gaitan, “Merging the Internet of Things and Robotics”, Recent Researches in Circuits and Systems, pp.499-504, 2012

[18] M.Thiyagarajan, V. Thiagarasu, “Two basic models of web resource Allocation methods”, Icici Budca, Bharathiar University, PP.75-78, March 2014

[19] William Stallings, “Cryptography and Network Security:”, Pearson Education, 4th Edition USA 2002.
[20] http://nsl.cse.unt.edu/dantu/cae/attachments/Eric_Ayeh_MS_thesis.pdf
[21] www.ccunix.ccu.edu.tw/~lngwujs/Courses/.../NLP_prolog_Blackburn.pdf