International Journal of Current Research in Life Sciences *Available online at http:// /www.wrpjournals.com/journals/V/IJCRLS*
Vol. 3, No.12, pp. 066-069, December 2014

Full Length Review Article

ON USER AUTHENTICATION FOR WEB RESOURCE ACCESS

[1,*]Thiyagarajan, M. and [2]Ms. Chaitanya Raveendra

[1]Nehru Institutes of Engineering and Technology, Coimbatore, Tamil Nadu – 641105, India
[2]Nehru Institute of Information Technology and Management, Coimbatore,
Tamil Nadu – 641105, India

Accepted 27th November, 2014; Published Online 31th December, 2014

We give the generalized Fiat-Shamir multi-party authentication algorithm for web resource allocation. The complexity on the use of classical algorithms can be reduced by zero knowledge protocol. We give the Java implementation of this protocol. Our approach is modification of isomorphism of graphs algorithm. We also give an alternative approach for this authentication through isomorphism of graphs.

Key words: Web 2.0 Multi_Party Authentication, Zero Knowledge Edge Proof, Graph Isomorphism, Web Services, PROLOG and XML, Java Programming.

INTRODUCTION

Almendros-Jiménez *et al*. (2008) have presented a proposal for the implementation of the X Path 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 X Path language. This evolves the specialization of the logic program with regard to the X Path 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, (2010) 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 *et al*. (2005) have studied web service based on PROLOG and XML. 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. While the traditional Web is concerned with the interaction between applications and humans,

Corresponding author: Thiyagarajan, M.,
Nehru Institutes of Engineering and Technology, Coimbatore, Tamil Nadu – 641105, India.

Web services technologies and standards aim at taking the Web one step further by enabling interaction between applications and thereby facilitating application integration.We conclude that it can be valuable components of many Distributed Information Systems, for example in an information broker to support complex information gathering and integration strategies or to control a multi-agent system. In their discussion on the Zero Knowledge Proof Protocol Wang Huqing *et al*. (2013) gave typical application and implementation of this protocol in multiparty authentication by generalization of fiat- Shamir authentication process. By implementing arithmetic on ECC over GF (2^5) Thiyagarajan and Rishivarman, (2012) the multiparty authentication protocol finds a different setup. Here we address the problem of the web resource allocation through XML documents processing and semantic outlook of authentication process without use of hard number-theoretic concepts. In section 1, we give the role of XML and PROLOG in logic programming. In section 2, java programming for the implementation of generalized FS authentication process is given. The use of isomorphism of graphs and Zero Knowledge Protocol is presented in the last section.

Section 1

The Role of XML and PROLOG in logic programming

XML Document

XML provides a standard way to define the structure of documents that is suitable for automatic processing. This enables the development of generic tools that parse documents and extract their content as well as their structure. Restrictions on the structure of a document can be specified by Document Type Definitions (DTDs) or XML SCHEMAs (however, neither of these provide any semantic information). XML has been widely adopted as the foundation for data representation and formats on the Web. Many parsers and toolkits exist for different programming environments, which implement the XML related standards.

Web Services

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”. Since every element in an XML document (except the root element) is nested into another element, we can consider XML documents term structures, which can be handled nicely by PROLOG, which can then be used to process those terms in a very compact and efficient way. SWI–PROLOG (Martin Zima and Karel Jazek, 2010) offers a package called Sgml2pl which contains a SGML/- XML parser. This parser can parse a document from a file and transform the content into a PROLOG data structure. The data structure used is a nested term of the function element with three arguments: the name of an XML element, the list of its attributes and the content of this element. The parser also uses some other kinds of functions to represent other constructs in an XML document (e.g. entities, a DTD or processing instructions). The parsing process can optionally be controlled, e.g. to influence the treatment of spaces.Libxml21 is the XML parser and toolkit that was developed for the Gnome project, but it can also be used standalone and outside of the Gnome platform. This library of C functions implements XML parsers and toolkits for a number of existing standards related to XML, e.g. XPATH (Thiagarajan and Rishivarman, 2012). Libxml2 contains functions to parse XML documents supporting validation against a (internal or external) DTD or an XML SCHEMA. It can also handle namespaces and different XML document encodings. The internal document representation follows the DOM interface. The library can also be used to evaluate XPATH expressions.

Thus we conclude that XML documents can be handled to have semantic outlook through PROLOG and other parser.

Section 2

Java implementation of generalized FS algorithm

In this section we present multiparty authentication procedure for Web Resource Allocation.

- **Generalized authentication process**

The introduction of the parameters about Fiat-Shamir authentication process:

- $n = p \times q$, n is a random modulus, p and q are two large primes.
- s is the private key of the prover P. v is the public key of P. s and n are co- prime. $v = s^2 \bmod n$
- r, a committed random number, is a random integer, which $\in$ =[1,n-1]
- $e \in \{0,1\}$, a challenging bit.
- We can use this process to identify the resource allocation in web service. In addition, we give the Guillou-Quisquater authentication, a classic authentication process.

The introduction of related parameters

- J, v, n are public keys, n= $p \times q$ p and q are two large primes.
- B is the private key , which meets
- $J \times B^v = 1 \bmod n$.
- r, a committed random number, is a random integer, which $\in$ =[1,n-1].
- $d^{\in}$ = [0, v-1], a challenging bit.

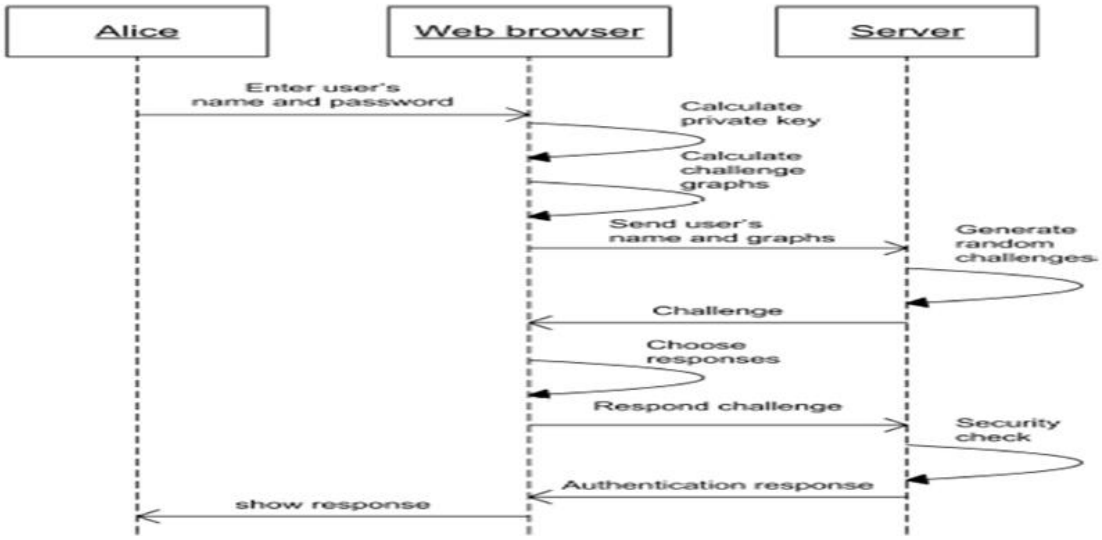
Zeroknolwedge.java

```
import.java.lang.*;
import.java.lang.*;
class Verifier {
Public void zeroProtocol ()
{
Double value, r=3, x, y, sA=4,v=5,n=35,e;
X = value %n;
e=2;
value=Math.pow(sA,e);
y=(r*value)%n;
System.out.println(“ The value a send for verification” +y);
Verification (e,v,n,y);
}
Public void Verification (double e, double v, double n, double y)
{
int iA=15,jA;
double value1, value2,z;
jA=2*ia+1;
Value1 = Math.pow(ja,e);
Value2 = Math.pow(y,v);
z=(Value1*Value2)%n;
System.out.println(“Calculated Z value is”+z);
If(z==0)
{
System.out.println(“wrong User”);
}
Else
{
System.out.println (“access Permission is granted”);
}
}
}
public class zeroknowledgege {
public  static void main (String[]args)
{
Verifier ABC= new Verifer();
ABC.zeroProtocol();
}
```

Authentication Procedure

ZKP implementation on the web

A sequence diagram presented above shows our approach in detail. Alice types her username and password, but the password never leaves her browser. In contrary to existing approaches like HTTP MD5 digest, the server does not have any information that would allow for impersonation Alice at another server.



The browser uses the password to calculate her public-private key pairs and then executes the ZKP protocol. The browser is responsible for a number of new tasks: calculating private keys from passwords, generating challenge graphs, and responding to the challenge. A server has only one more responsibility: generating random challenges. There is also one more interaction between a browser and a server in comparison with classical approaches. Thus, the main question is if the new approach is feasible and will not require long waiting times for users.

Section 3

Zero Knowledge implementation of Isomorphism Graphs

In the authentication process discussed in section 2, demands for the computation of large primes and their powers. This is overcome to some extend the zero knowledge interactive protocol which minimizes the delay in computational process. The number theoretical competition can be minimized through graph isomorphism algorithm and zero knowledge proofs. We present the details of this alternative approach in this section.

Graph Isomorphism

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
$(u, v) \in E_1 \leftrightarrow (\pi(u), \pi(v)) \in E_2$.

An example is depicted on Figure. The problem is not likely to be NP-complete. But it is NP. There is no known polynomial time algorithm that solves it. If we apply this problem to ZKP, a public key is composed of two isomorphism graphs G_1 and G_2, where the permutation π_p

$G_2 = \pi_p (G_1)$

Figure An example of graph isomorphism G2 = (G1)

is a private key. A prover generates a random permututation π_R, and sends a graph $G_R = \pi_R (G_1)$ to the verifier. Then depending on the verifier's challenge, the prover sends back π_R or π_{R2} suchthat

$$\Pi_{R2} = \Pi_R \cdot \Pi_p^{-1}$$

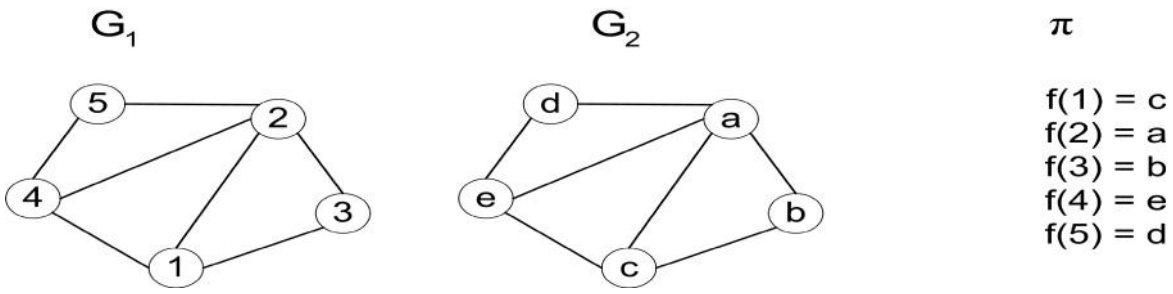
Thus, the verifier is able to check one of the conditions:

$G_R = \pi_R (G_1)$ or $G_R = \pi_{R2} (G_2)$

Knowledge about only one parameter π_{R1} or π_{R2} does not let the verifier compute the prover's private key

Zero –Knowledge Proof Protocol

The main idea of zero-knowledge proof 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). We call this technology which can achieve the purpose of proof without revealing anything "zero knowledge proof (ZKP) ".



Private-key algorithm

A user's private key is a permutation. Since we want to keep users using login and password pairs, we transform passwords to corresponding permutations using a one-way function. Such a transformation must always generate the same-size permutations.

Implementation and Evaluation

While implementing the graph isomorphism. We must take care of the various factorial arrangements of the permutation along with the multiplication table of these permutations. The transmission of public key and private key through server side and client side are done by Java Servlet and Ajax. Depending on the number of parties involve in the transaction specific no of vertices and edges can be assigned to the basic graph in question.

As a proof of the concept we implemented a prototype. Its server side was a Java servlet that was deployed on a Jakarta Tomcat server. The code was not platform specific to make it easily portable to other languages. The client side was implemented in Ajax. Such a choice, however, requires users to trust the server. We performed our evaluation on 6 different configurations

- Conf 1 - laptop, 1 CPU 2 GHz, 2 GB of RAM, Firefox 2
- Conf 1b - the same laptop with Internet Explorer 7
- Conf 1c - the same laptop with Opera 9
- Conf 2 - laptop Centrino 1.4GHz (1 CPU), 256 RAM,
- Firefox 2
- Conf 3 - desktop computer with 1 CPU 2.8 GHz, 2 GB
- RAM, Firefox 2
- Conf 4 - laptop with 1 CPU Xenon 1.4 GHz, 768 MB
- of RAM, Firefox 2

Conclusion and Future Work

While dealing with multiple resources allocation over web services, we employ circular token algorithm. In this process, we met with the problem of multi-party authentication and semantic nature of a web documents. These problems are dealt with using PROLOG and XML programming and generalized Fiat-Shamir algorithm. The implementation details are given using ZKIP. However the complexity in implementation can be reduced using graph isomorphism protocols. This approach, we feel to be better than the earlier methods as we avoid the tough and complicated numerical calculations of larger bits.

As an improvement on this discussion we like to place the following computational procedure in each direction. Nowadays the zero knowledge interactive protocol is having further extension as zero knowledge non interactive protocol, statically zero knowledge protocol and statistical non interactive zero knowledge protocol. Also randomized algorithm play in important role in the improving techniques and implementation comes simpler. We have at present random graph theoretical algorithm for isomorphism of graphs. Such developments will wave way for the research in this direction. Our final aim is to develop an automated for web resource allocation process.

REFERENCES

Almendros-Jiménez, J.M., Becerra-Terón, A. and Enciso-Baños, F.J. 2008. "Querying XML Documents in Logic Programming", *Journal of Theory and Practice of Logic, programming*, Vol. 8, No. 3.

Bayer, Stephanic, Groth and Jens 2012. "Efficient Zero-Knowledge argument for correctness of a shuffle".31st annual International Conference on the theory and Application of Cryptographic Techniques, EUROCRYPT 2012.pp:263-280.

Bernd, D. Heumesser, Andrreas Ludwig and Dietmar Seipel 2005. Weeb Services Based on PROLOG and XML, Lecture Notes in Computer Science, Springer, Vol. 3392, pp. 245-257.

Chaitanya Ravendra 2013. "Web Crawling As Nonlinear Dynamics", Progress in Nonlinear Dynamics and Choas, vol.1, pp:1-7.

Garg, sanjam Jain, Abhishek, sahai and Amit 2011. "Leakage-resilient Zero knowledge". 31st Annual International cryptology Conference, CRYPTO 2011.

Goldreich, Micali, O. and Wigderson, S, 1986. A. Proofs that yield nothing but their validity and a methodology of cryptographic protocol design *J.FOCS*, 1986.174-187.

Gottschalk, K., Graham, S., Kreger, H. and Snell, J. 2002. "Introduction to web Services Architecture", IBM System *Journal*, Vol. 41 No. 2, pp. 170-177, 2002,

Grzonkowski, 2008. Zaremba, Zaremba, McDaniel. "Extending Web Application with a Lightweight Zero Knowledge Proof Authentication" ACM, 2008/10/28. pp: 65-70.

Gupta, A. Stahl, D.O. and Whinston, A.B. 1998. "Managing Computing Resources in Intranets: an Electronic Commerce Perspective," Decision Support System, Vol. 24, pp. 55-69.

Karpagaselvi, S. 2012. "Soft computing Techniques for web search Engines", Unpublished Ph.d thesis Anna University of Technology, Chennai June 2012.

Lin, Huijia, Pass, Rafel, Tseng, WeiLungDustin Venkitasubramaniam and muthuramkrishnan 2010. "Concurrent Nonmalleable Zero knowledge proofs"; 30th *Annual International cryptology conference*, CRYPTO 2010.pp:429-446.

Martin Zima and Karel Jazek, 2010. "Translation of XML documents into logic programs", in Proceedings of 14th International conference on electronic publishing, 2010. pp: 297-315.

Siba K.Udgata, 2011. Alefiah Mubeen and Samrat L. Sabat: "Wireless sensor network security model using Zero Knowledge Protocol"; IEEE Communication (ICC) 2011 Proceedings.pp:1-5.

Thiagarajan, M. and Rishivarman, A.R. 2012. An Arithmetic over GF (2^5) To Implement in ECC, *International Journal of Computer Applications*, (0975– 8887), Volume 39– No.11, February 2012.

Wang Huqing, Sun Zhixin and Nanjing, China, 2013. 'Research on Zero- Knowledge proof Protocol'; *IJCSI*., Vol.10,Issue 1,No1,January 2013.pp194-200.

****