An Intelligent Agent Based Framework for Secure Web Services

N.Jaisankar
Research Scholar
Anna University
Chennai-600025, India
jaisasi_win@yahoo.com

A.Kannan
Professor
Anna University
Chennai-600025, India
jaisasi_win@yahoo.com

Abstract - Currently the characteristics of web services and the complexity of the distributed environment poses a great challenges for its security. Moreover, there is no complete Role Based Access Control (RBAC) model and RBAC framework for Web Services that has been reported in the current literature which considers spatio-temporal constraints in its model. So, in this work we propose a spatio-temporal RBAC model for providing effective access control for Web Services. In this model SOAP Proxy has been employed to send messages for Web Services and security mechanisms are provided using rules, temporal and spatial constraints. In the proposed model, users are restricted to assign the role and to access the service only when (s) he satisfies some predefined identity and spatio–temporal constraits in addition to the enforcement of usual security and integrity constraints which are used for providing additional security. Finally, we use intelligent agents to rpovide security through rules and constraints and hence multiple agents are deployed.

Keywords-Role Base Access Control (RABC), Spatio – Temporal constraints, Web Services, SOAP Proxx, WSDL, XML.

I. INTRODUCTION

Service-Oriented Computing (SOC) is the paradigm that uses services as fundamental elements for developing complex web applications. A service is well defined self contained function that does not depend on the context or state of other services in which independently developed services interoperate with each other via a well defined interface. Moreover, the services may be hetrogeneous and possibly be implemented in different languages. Web service systems are developed based on a set of XML standards, such as SOAP, WSDL and UDDI which are used for representation and communication across different security domains in the Internet. Compared to centralized system and client-server environments, the web services environment is much more dynamic and distributed. As a result of the character of Web Services, its business functions are to be separated into reusable components there by exposing interfaces beyond firewalls. They enable outsiders to invoke applications potentially for providing access to sensitive information. Compared with the existing distributed object technology Web Services security management and control ability are more weak currently because XML documents are encoded in text rather than in binary form. Therefore, Web Services face a lot of new security challenges. So, it is necessary to study the existing acess control technology carefully and to propose new access control models which reduce security threats for web services.

Role Based Access Control has been the subject of interest for many years and a considerable research has been carried out in the last decade[22,23] and is widely accepted as an alternative to traditional discretional and mandatory access controls.The emergence of distributed environment in Web Services poses new demands on access control mechanisms, because the decisions to grant access may depend on contextual information such as the location of the user and the time at which access requests are made. Several context based RBAC models have been defined in recent years and [16-17,19-21] each of these models introduced few extentions to the basic role based models in which components may be associated with general contextual constraints[18,20,21]. However none of these models are exactly suitable for web services because of the dynamic and distributed nature of data used in web services. Therefore it is necessary to enhance the existing RBAC models with spatio-temporal constraints and features.

In this paper, we propose a new Intelligent Spatio-Temporal Role Based Access Control model (ISTRBAC) that uses agents for rule management and for enforcing spatio-temporal constraints more suitable for web services that use hetrogenious environments and multi databases. In order to provide effective secure web services, first we propose this ISTRBAC model by adding integrity constraints and spatio-temporal constraints.Second, this system provides separate agents such as a spatial information agent, a temporal information agent and a rule management agent to check appropriate constraints. Finally, this work proposes new agents that are capable of providing rule matching and rule firing so that the accuracy level is increased to an optimal level of security.

II. RELATED WORK

Access control technology for Web Services is becoming the recent hot research topic.and hence a number of researchers have contributed their views and works in the recent literature, For example Damiani[6] first proposed the notion of a fine grained access control model on XML documents that uses SOAP messages. On the other hand many papers [6-8] focus on controlling access to XML documents. However, these works focused more on protecting XML documents rather than provinding web services. Hao He et al [25] proposed a RBAC model for XML information management where an access control scheme has been presented which is represented in XML itself, with Apath to specify the linkage between the access information and the actual data.The authors have claimed a few advantages of having RBAC in XML for XML information. However, they did not focus on the use of agents to tackle spatio-temporal aspects in contraint satisfaction which is crucial in the web services environment. Xianzhi Huang et al [26] have described the Access control policies for XML that typically uses regular path expressions such as Xpath for specifying the object for access control policies which are burden to the query engines for XML documents. To relive this burden they introduced static analysis for the Access Control subsystem. However a dynamic analysis is necessary for providing security in a web services environment. Miao Liu et.al.[27] based on the analysis of the access control requirements for web services, they point out the limitations of current access control models for web services and present an attribute and RBAC model for web services. Feng He.et.al.[28] have presented a web services security technology for implementing RBAC components for secure web services environment. Their work focuses on introducing RBAC to protect e-learning applications based on web services. Recently some authors [2,3] have considered the security of SOAP messages in their work on web services. However, no complete access control model architecture for web services has been proposed yet by the researchers in this area that includes rules, spatio constraints and temporal constraints that are intelligently handled by multiagents.

Recently some organisations and company are devoting themselves to provivide effective security to web services. XrML[1] focuses on digital rights using an XML based framework for request response exchange of authentication and authorization information. Moreover, XACML [32] is another XML specification for expressing fine grained information policies in XML documents. Though XrML [1] is a general-purpose, XML-based condition, which can be used for expiration management, it overlaps with XACML where XACML is a more comprehensive and flexible specification. Nakamur [5] discusses how security information sent with SOAP message can be processed within enterprise environments and SOAP message filter approach has been reported in [4]. This approach realizes local component-based access control by translating a SOAP invocation into a RMC-based request. Because this system is constructed on the original system security architecture, it is a merely transition from the traditional application paradigm to Web Services.

Xiutao cui et.al.[29] presents a Ex-RBAC, an extension of the RBAC model adding identity constraints and spatio-temporal constraints in location aware mobile collaboration system and the author also proposes some assignment rules of previlege and interaction role by the analysis of different confilicts and their relationship. James B.D.Hoshi et.al.[30] proposed a generalised temporal role based access control model that allows specification of a comprehensive set of temporal constraints, particularly constraints on role enabling and activation and various temporal restrictions on user role,they hae also presented the time-based semantics of hierarchies and SoD constraints, here a notion of safeness has been introduced to generate a safe execution model for a GTRBAC system. Liang Chen and J.Crampton[31] constructed a number of spation-temporal role-based models based on RBAC96 and ERBAC07 using a simple extension of the syntax used for RBAC96. They also introduced a graph-based formalism to explain the semantics of RBAL96, and used this as a basis for defining the semantics of spatio-temporal models and also examined the difficulties that arise when enabling constraints are placed on roles in the presence of hierarchy.

Comparing with all these works, the access control model proposed and implemented in this paper is different in many ways. First, it considers the application of different type of rules dynamically using both forward chaining and backward chaining control flow for providing effective security using rule agent. Second, this work considers spatial and temporal constraints specially and hence can be applied on past, present and future data with geographically distributed locations which are handled by specific agents. Third, this system follows access control algebras based on first order predicate logic and hence inference can be made as and when it is required. Finally we consider dynamic analysis using agents that are capable of performing rule matching and rule firing that can work on hetrogeneous databases with multiple file formats.

III. AN INTELLIGENT AGENT FRAMEWORK

A. System Architecture

Based on SRBAC model proposed in [9], we have designed and implemented a spatio-temporal role-base access control system. The system architecture for Web Services (SAWS) is shown in Figure1. In this architecture, clientend is service requestor, UDDI registry is service registry, SOAP Proxy and Web Services are service providers [11-12]. In SAWS, SOAP Proxy is a proxy which can parse SOAP protocol. It publishes the service description in service registry. Service requests bind to SOAP Proxy, which enforces spatio temporal role-based access control. The SOAP Proxy is

the implementation point for access control. In SAWS, it gets subject information from client request, and then sends it to the ISTRBAC processor where it carries on identity certification and role judgment. Finally SOAP Proxy controls the invocation of Web Services based on the role of the requestor. As shown in Figure 1, among the Web services also each web services may call each other services. For example, when one Web service needs to call other service, it only sends the request to SOAP Proxy. The SOAP Proxy judges whether Web service invocated is in its jurisdiction range. If not in, SOAP Proxy will query the service registry for the type of service required.This system follows the web services process model proposed in [31] and additionally uses multiagents for providing intelligent constraints checking. Therefore, it uses five new componets namely temporal info_management agent, spatial info_management agent rule management agent,rule base and spatio-temporal database.

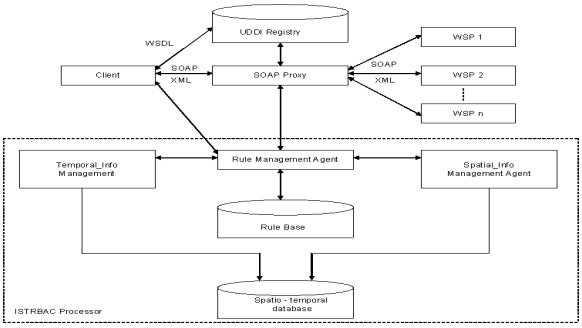


Figure 1. System Architecture

B. SOAP Message

To restrict the access to Web Services, the UserproxyrInfo (Up_info) recorded in the secure cookie [9] is transmitted to SOAP Proxy by SOAP message. Based on the WS-Security and XML Encryption [24] specification, the header of SOAP message is extended, Up_info element is appended behind web services security.Up_info is composed of five subelement (UserInfo, RoleInfo, Temporal_constraint, Spatia_constraint and Digital_Sign) corresponding to SOAPProxy_cookies.

<S:Envelope xmlns:S="http://www.w3.org/2001/12/soap-envelope">
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:wsse="http://schemas.xmlsoap.org/ws/2002/04/secext"
xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
<S: Header>
<wsse:Security> … </wsse:Security>
<Userproxyinfo>
< Userinfo> …. </Userinfo>
<Roleinfo> …. . </Roleinfo>
<Temporal_Constraints>
< Time_Interval> 23/04/09 from 9:00:30 to 4:35:30 </Time_Interval>
</Temporal_Constraints>
<Spatial_Constraints>
<Position> inarea(user,area) </Position>
</Spatial_Constraints>
<Digital_signature> ... . </Digital_signature>
</Userproxyinfo>
. . .
</S:Header>
<S:Body> . . . </S:Body>
</S:Envelope>
Fig.2. An Example of SOAP Message

When implementing, five kinds of key information (Encrypt_UserInfo,Encrypt_RoleInfo, Temporal_constraint, Spatial_Constraint, Digital_Sign) are taken out from SOAPProxy_cookie in the end-system. Then they are embedded into the Up_info in the header of SOAP message. There are extended dada items of Up_Info in the above SOAP message. In this, UserInfo and RoleInfo as encrypted data can be embedded into the corresponding data items and also can be recorded according to the XML Encryption [1] format. Figure 3 shows an example of encrypted UserInfo and RoleInfo recorded as the XML Encryption format. Similarly Temporal_Constraint and Spatial_Constraint are also encrypted.

< UserInfo>
<EncryptedData
Type='http://www.w3.org/2001/04/xmlenc#Content'
xmlns='http://www.w3.org/2001/04/xmlenc#'>
<CipherData>
<CipherValue>JS23P45S98….</CipherValue>
</CipherData>
</EncryptedData>
</ UserInfo>
< RoleInfo >
<EncryptedData
Type='http://www.w3.org/2001/04/xmlenc#Content'
xmlns='http://www.w3.org/2001/04/xmlenc#'>
<CipherData>
<CipherValue>B76C43D23….</CipherValue>
</CipherData>
</EncryptedData>
</ RoleInfo >
Fig.3. An Example of Encrypted UserInfo and RoleInfo using XML Encryption

IV. IMPLEMENTATION OF ISTRBAC

A. Algorithm

In the ISTRBAC system proposed in this work, SOAP Proxy is the key component as it has been followed in RBAC [9]. However, in this research work, intelligent rules are

applied to check the spatio temporal constraints. The steps of the ISTRBAC algorithm are as follows.

Step1. Parse the SOAP message to get information for the futher steps using SOAPproxy

Step2. Checking for the validity of the SOAP message using the time and position.

If client IP is a permitted IP and the interval time stamp is within permitted interval and if the spatial within permitted range then return true else return false

Utilizing these algorithm we can examine whether user's IP address is in the permission scope, get the Time_Stamp (t_1, t_2) from U_p _info and check if it is in the valid time interval and also check the distance range. Finally the validity of U_p _info Message from Digital_Sign, the signature of SOAP Proxy.

Step3. UserproxyInfo is processed as follows

SOAP agent exracts encrypted user information from <UserInfo> decrypt it with the private key of SOAP Proxy and examines its validity Similarly the SOAP agent extracts the role from <RoleInfo>, examines its validity. After the above examinations, it can be confirmed that the user and its role informations are valid.

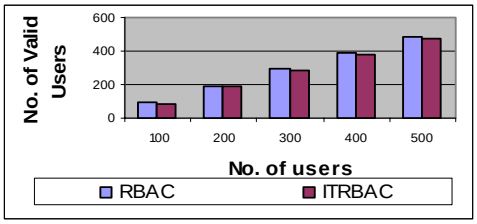
Step4. Executing ISTRBAC: If the user is valid and the called service is in scope of the role permission, the SOAP Proxy will retransmit this SOAP message to corresponding Web Service, and the respond of the Web Service will be retransmitted to the client, otherwise returns error message.

B Results and Discussion

Table1. Shows the number of users prevented by rule manager agent and temporalinfo management agent and from the corresponding graph it is observed that the use of intelligent temporal agent for temporal constraints checking decreases the number of users permitted to access the Web Services (WS) in all the experiments conducted int ehis work. Table2 shows the number of users prevented by rule manager agent and spatioinfo management agent, from the Graph2 it is observed that the use of intelligent spatio agent for saptial constraints checking further restricts the permission. Finally, the combination of temporal agents with spatial agents provides an effective security because of the combined management constraints.

TABLE 1. Authorised Access Control for IP Address and Time

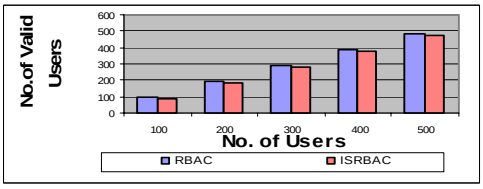
Exp No.	No of user agent tried	Users permitted after checking IP address by Rule Management agent	Users permitted after checking time by Temporal Management agent
Exp 1	100	95	86
Exp 2	200	192	186
Exp 3	300	290	282
Exp 4	400	389	380
Exp 5	500	486	478



Graph 1. Bar Chart Showing the Number of User Permitte-Checking IP Address and Time

TABLE 2. Authorized Access Control for IP Address and Position

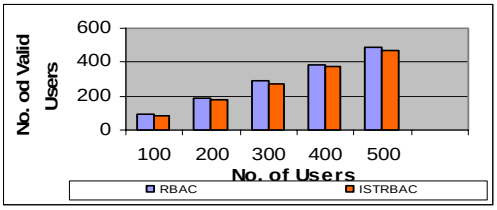
Exp No.	No of user agent tried	Users permited after checking IP address by Rule Management agent	Users permited after checking Position by Spatial Management agent
Exp 1	100	95	85
Exp 2	200	192	185
Exp 3	300	290	284
Exp 4	400	389	380
Exp 5	500	486	476



Graph 2. Bar Chart Showing the Number of Users Permitted after Checking IP Address and Position

TABLE 3. Access Control for IP Address and Spatio-Temporal Constraints

Exp No.	No of user agent tried	Users permitted after checking IP address by Rule Management agent	Users permitted after checking Time and Position by Spatio-Temporal Management agent
Exp 1	100	95	80
Exp 2	200	192	180
Exp 3	300	290	272
Exp 4	400	389	375
Exp 5	500	486	468



Graph 3. Bar Chart Showing the Number of Users Permitted after Checking IP Address and Spatio-Temporal Constraints

V. CONCLUSION

This paper presents An Intelligent Spatio Temporal Role-Based Access Control model and secure architecture model for Web Services. Compared with existing models this model provides additional security using agents for managing spatio and temporal constraints. Therefore, this system enhances the description ability for Web service, and shows intelligent behavior . From the implimentation carried out in this model, it is observed that there is 3% improvement in security with temporal constraints, 2% with spatial constraints and have a overall improvement of 5% security in comparison with the existing system that do not consider multiagents.Further works in this direction could be to carry out additional experiments with different types of agents to access various web services and to perform validation of the access control policies proposed in this paper.

REFERENCES

[1] ContentGuard, Inc. eXtensible Rights Markup Language, XrML 2.0, 2001. http://www.xrml.org.

[2] Web Services Security Core Specification Working Draft 01, 20 September 2002. http://lists.oasis-open.org /archives/wss/200209/pdf00000.pdf

[3] W3C NOTE. SOAP Security Extensions: Digital Signature. http://www.w3.org/TR/SOAP-dsig.

[4] E. G. Sirer and K. Wang, "An access control language for web services", In Proceedings of the ACM Symposium on Access Control Models and Technologies, ACM Press, pages 23–30 2002.

[5] Yuichi Nakamur, Satoshi Hada, and Ryo Neyama, "Towards the Integration of Web Services Security on Enterprise Environments", Symposium on Applications and the Internet Workshops, Narar City, Nara, Japan, 2002.

[6] Ernesto Damiani, Sabrina de Capitani di Vimercati, Stefano Paraboschi, Pierangela Samarati, "Design and implementation of an access control processor for XML documents", *Computer Networks*, Vol.33, No.1-6, pages 59-75,June 2000.

[7] E. Damiani, S. De Capitani di Vimercati, S. Paraboschi, and P. Samarati, "A Fine-Grained Access Control System for XML Documents", *ACM Transactions on Information and System Security*, Vol. 5, No. 2, pages 169-202, May 2002.

[8] R. Bhatti, J. B. D. Joshi, E. Bertino, A. Ghafoor, "Access Control in Dynamic XML-based Web-Services with XRBAC", In proceedings of The First International Conference on Web Services, Las Vegas, pages 23-26, June 2003.

[9] Xu Feng et.al. " Role Based Access Control For Web Services" IC on Computer Information, 2004,

[10] Ravi Sandhu, Edward Coyne, Hal Feinstein, and Charles Youman, "Role-Based Access Control Models", *IEEE Computer*, Vol. 29, No. 2, pages 38-47,February 1996.

[11] UDDI Version 3.0 Published Specification, 19 July 2002. http://uddi.org/pubs/uddi_v3.htm.

[12] W3CNote.WebServicesDescriptionLanguage (WSDL)1.1,15March2001.http://www.w3.org/TR/wsdl.

[13] Ray and M. Toahchoodee. A spatio-temporal role-based access control model. In Proceedings of the 21th Annual IFIP WG 11.3 Working Conference on Data and Applications Security,pages 211-226, 2007

[14] C. A. Ardagna, M. Cremonini, E. Damiani, S. D. C. di Vimercati, and P. Samarati. Supporting location-based conditions in access control policies. In *Proceedings of the 2006 ACM Symposium on Information, Computer and Communications Security*, pages 212-222, 2006.

[15] Ray and M. Kumar. Towards a location-based mandatory access control model. *Computers & Security*, Vol.25, No.1,pages 36-44, 2006.

[16] J. B. D. Joshi, E. Bertino, U. Latif, and A. Ghafoor. A generalized temporal role-based access control model. *IEEE Transactions on Knowledge and Data Engineering*, Vol.17, No.1,pages 4-23,2005.

[17] E. Bertino, B. Catania, M. L. Damiani, and P. Perlasca. GEO-RBAC: A spatially aware RBAC. In *Proceedings of the Tenth ACM Symposium on Access Control Models and Technologies*, pages 29-37, 2005,

[18] M. Strembeck and G. Neumann. An integrated approach to engineer and enforce context constraints in RBAC environments. *ACM Transactions on Information and System Security*, Vol.7, No.3 :pages 392-427, 2004.

[19] E. Bertino, P. A. Bonatti, and E. Ferrari. TRBAC: A temporal role-based access control model. *ACM Transactions on Information and System Security*, Vol.4, No.3:pages 191-233, 2001.

[20] M. J. Covington, W. Long, S. Srinivasan, A. K. Dev, M. Ahamad, and G. D. Abowd. Securing context-aware applications using environment roles. In *Proceedings of the Sixth ACM Symposium on Access Control Models and Technologies*, pages 10-20, 2001.

[21] C. K. Georgiadis, I. Mavridis, G. Pangalos, and R. K. Thomas. Flexible team-based access control using contexts. In *Proceedings of the Sixth ACM Symposium on Access Control Models and Technologies*, pages 21-27, 2001.

[22] M. Nyanchama and S. Osborn. The role graph model and con°ict of interest. *ACM Transactions on Information and System Security*, Vol.2, No.1:pages 3-33, 1999.

[23] R. Sandhu, E. Coyne, H. Feinstein, and C. Youman. Role-based access control models. *IEEE Computer*, Vol.29, No.2: pages 38-47, 1996.

[24] 24. W3C WorkingDraft.XML Encryption Syntaxand Processing,March2002.http://www.w3.org/ TR/xmldsigcore/

[25] Hao He et.al. " a Role Based Access Control Model for XML Repositories" IEEE, Pages: 138-145,2000.

[26] Xianzhi Huang et al " A Context Rule and Role Based Access Control Model In Enterprise Computing Environment, International Conference on PC and Applications,2006.

[27] Miao Liu et.al, " An Attribute Based Access Control Model for Web Services, Proceedings of the International Conference on Machine Learning and Cybernetics, Vol.18, No.21, pages: 1302-1306, 2005.

[28] Feng He.et.al, " Apply the Technology of RBAC and WS-Security for Secure Web services Environment in Campus", Proceedings of the IC on Machine Learning and Cybernetics, pages: 13-16,2006.

[29] Xiutao cui et.al, " EX-RBAC: An Extended Role Based Access Control Model for Location-aware Mobile Collaboration System".Second IC On

Internet Monitoring and Protection (ICIMP'07*), IEEE Computer Society*, 2007.

[30] James B.D.Hoshi et.al, " A Generalised Temporal Role Based Access Control Model", *IEEE Computer Society*, Vol.17,No.1, January-2005.

[31] Liang Chen and J.Crampton, " On Spatio Temporal Constraints and Inheritance in Role Base Access Control", ASIACCS'08, ACM, 2008.

[32] OASIS Standared. XACML 1.0 Specification Set. Feb. 2003. http://www.oasis open.org.