A Survey of XML-based Security Standards for Handling Security Requirements of Grid and Cloud

Sarbjeet Singh, Jagpreet Sidhu
Computer Science and Engineering, UIET, Panjab University
Chandigarh, India
sarbjeet@pu.ac.in
jagpreetsidhu@gmail.com

***Abstract*— The purpose of this paper is to present a survey of XML-based security standards that can be used for handling security requirements of distributed computing systems like Grid and Cloud. Distributed systems are expanding and their growth is apparent from the advancements in the field of distributed computing technologies like Grid, Peer-to-peer, Cloud, Pervasive Systems etc. As a result of this expansion, security requirements are also increasing and becoming important. The expansion of Grid and Cloud demands new security standards for handling specialized security requirements and concerns of these systems. Different security standards are in use for handling security requirements of different systems. This paper presents a survey of important XML-based security standards, identifies general and specialized security requirements of Grid and Cloud like systems and then relates them to security standards. The paper also presents a general, security standards based view of distributed computing systems showing the applicability of XML-based security standards in handling security concerns of these systems.**

Keyword- Distributed computing systems, security standards, security requirements, Grid, Cloud

I. INTRODUCTION

A distributed system can be defined as a set of interconnected, autonomous computers that cooperatively solve large, single problem by facilitating parallel execution of separate but possibly related tasks [1]. Distributed technologies are expanding day by day and the computing technologies like Grid, Peer-to-peer, Pervasive and Cloud are becoming more prevalent. Many of these computing technologies share common goals and concerns e.g. sharing resources in an efficient way can be termed as common objective of these computing technologies. Similarly, security can be termed as common concern for these computing technologies. Security is a multidimensional problem. The real power of any computing technology can be harnessed only if it provides secure access to resources and services. A number of security issues need to be addressed to gain wide acceptance.

A lot of work has already been done in addressing traditional and basic security requirements like confidentiality, integrity, authentication, authorization and access control etc. But the newer computing technologies demand the support for specialized security requirements like single sign-on, delegation, trust, privacy, and policy based access in federated environment etc. Techniques are being proposed to handle additional security requirements of specialized distributed systems and number of standards are being developed.

This paper intends to present a comprehensive list of security requirements that a distributed computing technology may need to address, along with the discussion of various XML-based security standards that are becoming popular in addressing those requirements. This information can help security experts to select appropriate standards for handling the security concerns of their systems.

The paper is organized as follows: Section II presents a comprehensive list of security requirements that a distributed computing system like Grid and Cloud may need to address. Section III presents an overview of available XML-based security standards. Section IV relates security requirements with security standards. Section V gives a security standards based view of distributed computing systems and finally Section VI presents the summary.

II. SECURITY REQUIREMENTS OF GRID AND CLOUD LIKE SYSTEMS

The security requirements of distributed systems may be classified as basic and advanced. The basic security requirements include confidentiality, integrity, authentication and authorization whereas additional or advanced security requirements may include the support for single sign-on, delegation, credential renewal, non-repudiation, secure conversation, privacy, trust etc. A lot of literature like [2]-[12] exist which describe and justify these requirements in Grid and Cloud from various angles. Following table presents a brief description of these security requirements.

TABLE I. Security requirements/concerns of Grid and Cloud like Systems

Security Requirements/ Concerns	Brief Description
Authentication	Authentication basically deals with verifying the identity of the user.
Single Sign-on	Single sign-on enables a user to login once and access multiple services in heterogeneous domains with the same credentials.
Confidentiality	Confidentiality deals with the secrecy of the messages or information that flow over the communication channel.
Integrity	Integrity provides mechanisms to detect unauthorized changes to messages that flow over communication channel.
Delegation	Delegation feature enable a user to pass full or limited set of his/her authorization rights to other user(s).
Credential Renewal	Credential Renewal deals with the regeneration or re-issuing of expired credentials.
Non Repudiation	Non-repudiation guarantees that a user can't deny at a later stage that he/she has not performed a particular action, in case he/she has actually performed that particular action.
Secure Conversation	It deals with secure dialog exchange among communicating parties over a communication channel.
Privacy	Privacy security requirement deals with the protection of private/secret information.
Trust	Trust security requirement deals with trust related aspects like specifying trusted credentials, trust policies and determining trustworthiness of target service.
Policy	Policy security requirement deals with providing support for specification and enforcement of security policies. A security policy can be a rule/constraint/restriction that a system may want to enforce and may include aspects of privacy, trust, confidentiality, integrity etc.
Authorization	Authorization is concerned with what a user is permitted to do. It deals with issues like who can access what services and under what circumstances.
Assurance	Assurance provides the means to assure the quality of service that is expected or has already been agreed upon.
Manageability	Manageability security requirement deals with management related aspects of security services and requirements e.g. identity management, policy management, security key management etc.

Not all distributed computing technologies require the support for all security services. Different systems may demand different set of security requirements and functions depending upon the application and the context in hand. XML-based security standards are available and various are emerging to handle the security requirements described in Table I. It may be noted that most of the XML-based security standards do not provide a new technique or method to handle the security requirement in hand; instead they assist various stakeholders (managers, designers, programmers, users, security experts etc.) to specify and handle these requirements in an interoperable way. The prime concern and objective of XML-based security standards is to enable interoperability among different systems. Following Section presents a list of XML-based security standards along with their brief description.

III. SECURITY STANDARDS

The major reason behind the need of security standards is to address the security requirements and concerns of different parties in a uniform and interoperable way. Security standards are required to achieve interoperability among heterogeneous domains with respect to security requirements and concerns. In Grid and Cloud, the administrative domains and service providers are free to use any security mechanism of their choice. The security mechanisms deployed by one administrative domain or service provider may be different from

security mechanisms implemented by other administrative domains and service providers. If exchange of security related information is required among heterogeneous participating domains, then standards can provide us the required platform. Consortiums, Communities and Organizations like OASIS, W3C, OGF, Microsoft and IBM are taking initiatives in developing standards for specification and exchange of security related information in distributed environments. Following table lists the important XML-based security standards that address various aspects related to specification and exchange of security related information in an interoperable way.

TABLE II. XML-Based Security Standards

XML-based Security Standards	**Brief Description**
XML-Encryption [13]	XML Encryption is a W3C recommendation that deals with expressing encrypted data using XML. The information that can be expressed using XML Encryption include encryption method, encryption key, data type of encrypted document, etc.
XML-Signature [14]	XML-Signature is a building block for many security standards and provides integrity for data. XML-Signature can be thought of as a digital signature expressed in XML. Using XML signature selected portion of XML documents can be signed.
WS-Security [15]	WS-Security describes how signature and encryption headers are attached to SOAP messages. It also describes how to attach security tokens, including binary security tokens such as X.509 and Kerberos tickets to messages [11].
WS-Trust [16]	WS-Trust describes a framework for trust models that enables web services to securely interoperate. It provides a framework for requesting and issuing security tokens [16].
WS-Policy [17]	WS-Policy provides a general purpose model and corresponding syntax to describe the policies of a web service, e.g. required security tokens, supported encryption algorithms and privacy rules etc [17].
WS-SecureConversation [18]	WS-SecureConversation describes how to manage and authenticate message exchanges between parties including security context exchange and establishing and deriving session keys [11].
WS-Authorization [11]	WS-Authorization intends to describe how to manage authorization data and authorization policies.
WS-Privacy [11]	WS-Privacy intends to describe a model for how web services and requesters can state subject privacy preferences and organizational privacy practice statements.
WS-Federation [19]	WS-Federation describes how to manage and broker the trust relationships in a heterogeneous federated environment including support for federated identities [11].
SAML [20]	The OASIS SAML specification allow trust assertions to be specified using XML. These assertions can concern authorizations, authentications and attributes of specific entities.
XACML [21]	XACML provides a policy language which allows administrators to define the access control requirements for their resources in a standard and portable way. It also provides a mechanism that offers much finer granular access control than simply denying or granting access [29]. XACML architecture is tightly intertwined with SAML architecture.
XKMS [22]	XKMS (XML Key Management Specification) provides an interface to a PKI (Public Key Infrastructure). The XKMS specification defines two web services: The XML Key Registration Service and XML Key Information Service Specification (X-KISS).
ebXML [23]	The ebXML (electronic business XML) is a series of standards developed by OASIS and UN/CEFACT. The objective is to provide an open XML-based infrastructure enabling the global use of electronic business information in an interoperable, secure and consistent manner by all parties.
XrML [24]	XrML is Extensible Rights Markup Language. XrML enables users to specify rights and conditions with resources which are to be shared. XrML is XML-based document describing rights and conditions together with the message integrity and the entity authentication information.
EDXL [25]	EDXL (Emergency Data Exchange Language) is a suite of XML-based messaging

	standards facilitating emergency information sharing between the participating entities. EDXL enable information about various life saving resources to be shared among communicating entities.
OVAL [26]	OVAL (Open Vulnerability and Assessment Language) is a security assessment language for checking security configuration of systems. The OVAL language is a collection of XML schemas which can be used for representing system information and expressing specific machine states and reporting the results of an assessment.

It is clear from the above table that many standards are available for addressing the security requirements of Grid and Cloud like systems. The usage of these standards facilitates the specification, exchange, interpretation and automatic processing of security related information. As distributed computing systems like Grid and Cloud are growing, the role of security standards will be very important for the wide acceptance and popularity of these systems. There are many attempts like [27] – [32] where XML-based security standards are being used to construct security models. The use of security standards will give inherent assurance and confidence to users to openly migrate to Grid and Cloud based systems. Next Section relates security requirements with security standards.

IV. THE APPLICABILITY OF XML-BASED SECURITY STANDARDS FOR HANDLING SECURITY REQUIREMENTS

This Section relates security requirements listed in Table I with the XML-based security standards described in Table II. The applicability of XML-based security standards in addressing security requirements and concerns in shown in the following table:

TABLE III. Table showing Applicability of XML-Based Security Standards in addressing Security Requirements and Concerns

Security Requirements/Concerns	**XML-based Security Standards**
Authentication	WS-Security, SAML
Single Sign-on	WS-Security, SAML
Confidentiality	XML-Encryption
Integrity	XML-Signature
Delegation	WS-Security, SAML
Credential Renewal	SOAP, WS-Security, SAML
Non Repudiation	XML Signature, WS-Security, SAML
Secure Conversation	WS-SecureConversation
Privacy	WS-Privacy, SAML
Trust	WS-Trust, WS-Federation, SAML
Policy	WS-Policy, SAML
Authorization	WS-Authorization, WS-Federation
Assurance	SAML
Manageability	XKMS
Digital Rights Management	XrML

As shown in Table III, WS-Security and SAML can be used to handle authentication, Single Sign-on and delegated related aspects e.g by using WS-Security, authentication tokens like X.509 certificates can be attached to SOAP messages. SAML can be used for making authentication assertions. The assertion defines several authentication elements such as the integrity of the issuer, the time at which the authentication is granted, and the valid authentication time period. The assertion can indicate that an entity was authenticated by a specific system at a specific time [9]. Similarly, XML-Encryption and XML-Signature can be used for specifying integrity and confidentiality related aspects. E.g. using XML-Encryption we can express the encryption method (RSA, AES etc.), type of encryption key (symmetric or asymmetric etc.) and the information about how the encrypted key was agreed upon (e.g. Diffie-Hellman). Using XML-Signature, resources of any type can be

signed. It supports detached signature (signing a resource outside the containing XML), enveloped signature (signing some part of the containing document) and enveloping signature (contains signed data within itself).

Similarly, the requirements and constraints of a service or resource can be expressed using WS-Policy. The concerns related to request and issue of security tokens to establish trust can be expressed using WS-Trust and WS-Federation. WS-Policy can also be used to express policies related to privacy, trust and authorization related aspects. SAML can be used to make authorization decision assertions and attribute assertions also in addition to authentication assertions. An authorization decision assertion involves making a decision about whether or not a principal can access a specific resource, given an authentication assertion and an attribute assertion. Attribute assertion asserts about attributes of a principal and along with policy information can determine the privilege of a principal.

XACML is an access control markup language and provides a policy language which allows administrators to define access control requirements for their resources in a standard and portable way. It also provides a mechanism that offers much finer granular access control than simply denying or granting access [29]. XACML architecture is tightly intertwined with SAML architecture. Similarly, WS-Privacy is intended for expressing subject privacy preferences and organizational privacy practice statements and WS-SecureConversation enable secure dialog exchange by describing how to manage and authenticate message exchanges between parties including security context exchange and establishing and deriving session keys. Similarly, XKMS, XrML and EDXL can be used for managing keys, managing digital rights of resources and for sharing emergency information respectively.

V. A VIEW OF DISTRIBUTED COMPUTING SYSTEMS MAKING USE OF XML-BASED SECURITY STANDARDS

This section presents a security standards based view of a distributed computing system. Figure 1 diagrammatically shows the placement of security standards in a distributed environment like Grid or Cloud.

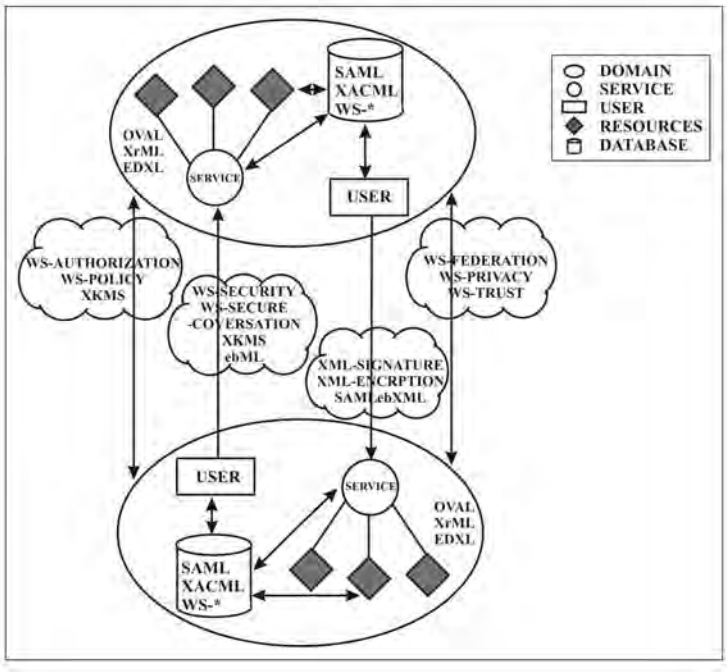

Fig. 1. Diagram showing placement of XML-based security standards in distributed environment which is representative of Grid or Cloud system

In Figure 1, ellipses represent distinct administrative domains or service providers' domains. Circles represent services, diamonds represent resources and rectangles represent users. The domain may have number of services and resources that it provides to service requesters (i.e. users) depending upon their authorization status. The information exchange takes place through SOAP messages among domains, services and users. The diagram is representative of Grid and Cloud systems. In case of Grid, the domain represents a different administrative organization and in case of Cloud, the domain is representative of a service provider.

Each user or service may have its own set of authentication, privacy, trust, confidentiality and integrity related requirements and users and services can express these requirements through WS-*, SAML, XACML and other related specifications and standards as shown in Figure 1. This information corresponding to each user and service is stored in the database which is maintained by every domain. While communication is taking place,

WS-* information is exchanged, which the both of the participating entities can understand, interpret and process and thus enable interoperability.

VI. SUMMARY

The paper identifies and relates key security requirements of Grid and Cloud like systems with available XML-based security standards and presents security standards based view of distributed computing systems. The information can help security experts to select appropriate standards for handling the security requirements of their particular systems. Though the XML-based security standards do not provide new solutions to satisfy the listed security requirements but their usage is important in an environment if we want to specify and address security related requirements and concerns in an interoperable way. So in our opinion the usage of XML-based security standards is very important, especially in Grid and Cloud like distributed computing systems where heterogeneous domains interact with each other to achieve a common goal and the user base is large and participating entities have different sets of security concerns.

REFERENCES

[1] J. M. Crichlow, An Introduction to Distributed and Parallel Computing. 2nd ed. Prentice-Hall of India Private Limited, 2003.

[2] Anirban Chakrabarti, Grid Computing Security. Springer, 2007.

[3] N. Nagaratnam, P. Janson, J. Dayka, A. Nadalin, F. Siebenlist, V. Welch, I. Foster and S. Tuecke, "Security Architecture for Open Grid Services", GGF OGSA Security Workgroup, 2003, Available: http://www.di.unipi.it/~coppola/GRIDsem/OGSA-SecArch-v1-07192002.pdf

[4] R. L. Krutz and R. D. Vines, Cloud Security: A Comprehensive Guide to Secure Cloud Computing.Wiley Publishing, Inc., 2010.

[5] T. Mather, S. Kumaraswamy and S. Latif, Cloud Security and Privacy. O'Reilly Media, Inc., 2009.

[6] S. Singh and S. Bawa, "A Framework for Handling Security Issues in Grid Environment using Web Services Security Specifications", in Second International Conference on Semantics, Knowledge and Grid, 2006, SKG'06, Guilin, China, Nov. 2006, pp. 68.

[7] F. Siebenlist, V. Welch, S. Tuecke, I. Foster, N. Nagaratnam, P. Janson J. Dayka and A. Nadalin, "OGSA Security Roadmap", 2002, Available: http://globus.org.eu/toolkit/security/ogsa/draft-ggf-ogsa-sec-roadmap-01.pdf

[8] J. Joseph and C. Fellenstein, Grid Computing. Pearson Education, 2004.

[9] M. O'Neill, P. Hallam-Baker, S. M. Cann, M. Shema, E. Simon, P. A. Watters and A.White, Web Services Security. Tata McGraw-Hill Publishing Company Limited, 2003.

[10] G. Singh and S. Singh, "A Comparative Study of Privacy Mechanisms and a Novel Privacy Mechanism [Short Paper]", in ICICS'09 Proceedings of the 11th International Conference on Information and Communication Security, Beijing, China, 14-17 Dec. 2009, pp. 346-358.

[11] "Security in a Web Services World: A Proposed Architecture and Roadmap", A Joint Security whitepaper from IBM Corporation and Microsoft Corporation, 2002, Available: http://www.ibm.com/developerworks/library/specification/ws-secmap

[12] S. Singh and S. Bawa, "Design of a Framework for Handling Security Issues in Grids", in International Conference on Information Technology, 2006, ICIT'06, 18-21 Dec. 2006, pp. 178-179.

[13] "XML Encryption Syntax and Processing", W3C Recommendation, 2002, Available: http://www.w3.org/TR/xmlenc-core/

[14] "XML Signature Syntax and Processing", W3C Recommendation, 2008, Available: http://www.w3.org/TR/xmldsig-core/

[15] B. Atkinson, G. Della-Libera, S. Hada, M. Hondo, P. Hallam-Baker, C. Kaler, J. Klein, B. LaMacchia, P. Leach, J. Manferdelli, H. Maruyama, A. Nadalin, N. Nagaratnam, H. Prafullchandra, J. Shewchuk and D. Simon, "Web Services Security (WS-Security)", 2002, Available: www.cgisecurity.com/ws/ws-secure.pdf

[16] S. Anderson, J. Bohren, T. Boubez, M. Chanliau, G. Della-Libera, B. Dixon, P. Garg, M. Gudgin, P. Hallam-Baker, M. Hondo, C. Kaler, H. Lockhart, R. Martherus, H. Maruyama, A. Nadalin, N. Nagaratnam, A. Nash, R.Philpott, D. Platt, H. Prafullchandra, M. Sahu, J. Shewchuk, D. Simon, D. Srinivas, E. Waingold, D. Waite, D. Walter and R. Zolfonoon, "Web Services Trust Language(WS-Trust)", 2005, Available: http://specs.xmlsoap.org/ws/2005/ 02/trust/WS-Trust.pdf

[17] S. Bajaj, D. Box, D. Chappel, F. Curbera, G. Daniels, P. Hallm-Baker, M. Hondo, C. Kaler, D. Langworthy, A. Nadalin, N. Nagaratnam, H. Prafullchandra, C. von Riegen, D. Roth, J. Schlimmer, C. Sharp, J. Shewchuk, A. Vedamuthu, U. Yalcinalp and D. Orchard, "Web Services Policy Framework (WS-Policy)", 2006, Available: http://download.boulder.ibm.com/ibmdl/pub/software/dw/specs/ws-polfram/ws-policy-2006-03-01.pdf

[18] S. Anderson, J. Bohren, T. Boubez, M. Chanliau, G. Della-Libera, B. Dixon, P. Garg, M. Gudgin, S. Hada, P. Hallam-Baker, M. Hondo, C. Kaler, H. Lockhart, R. Martherus, H. Maruyama, A. Nadalin, N. Nagaratnam, A. Nash, R.Philpott, D. Platt, H. Prafullchandra, M. Sahu, J. Shewchuk, D. Simon, D. Srinivas, E. Waingold, D. Waite, D. Walter and R. Zolfonoon, "Web Services Secure Conversation Language(WS-SecureConversation)", 2005, Available: http://specs.xmlsoap.org/ws/2005/02/sc/WS-SecureConversation.pdf

[19] H. Lockhart, S. Andersen, J. Bohren, Y. Sverdlov, M. Hondo, H. Maruyama, A. Nadalin, N. Nagaratnam, T. Boubez, K. S. Morrison, C. Kaler, A. Nanda, D. Schmidt, D. Walters, H. Wilson, L. Burch, D. Earl, S. Bajaj and H. Prafullchandra, "Web Services Federation Language (WS-Federation)", 2006, Available: http://download.boulder.ibm.com/ibmdl/pub/software/dw/specs/ws-fed/WS-Federation-V1-1B.pdf

[20] Security Assertion Markup Language (SAML), Available: http://xml.coverpages.org/saml.html

[21] eXtensible Access Control Markup Language (XACML) Version 2.0, 2005, Available: http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf

[22] XML Key Management Specification (XKMS), 2001, Available: http://www.w3.org/TR/xkms/

[23] Electronic Business XML Initiative (ebXML), Available: http://xml.coverpages.org/ebXML.html

[24] Extensible Rights Markup Language (XrML), Available: http://xml.coverpages.org/xrml.html

[25] Emergency Data Exchange Language (EDXL), Available: http://xml.coverpages.org/edxl.html

[26] Open Vulnerability and Assessment language, Available: http://oval.mitre.org/

[27] S. Singh and S. Bawa, "A Privacy, Trust and Policy based Authorization Framework for Services in Distributed Environments", International Journal of Computer Science, vol. 2, no. 1, pp. 85-92, 2007.

[28] S. Singh and S. Bawa, "A Privacy Policy Framework for Grid and Web Services", Information Technology Journal (6), pp. 809-817, 2007.

[29] M. Verma, "Control information access with XACML", 2004, Available: http://www.ibm.com/developerworks/xml/library/x-xacml

[30] V. Welch, F. Siebenlist, I. Foster, J. Bresnahan, K. Czajkowski, J. Gawor, C. Kesselman, S. Meder, L. Pearlman and S. Tuecke, "Security for Grid Services", 12th International Symposium on High Performance Distributed Computing, Seattle, WA, USA, June 22-24, 2003, pp. 48-57.

[31] D. Jana, A. Chaudhuri, A. Datta and B. B. Bhaumik, "Framework for Handling Security Issues in Interoperable Grid Services", IEEE Indicon Conference, Chennai, India, December 13, 2005, pp. 280-285.

[32] R. Bhatti, D. Sanz, E. Bertino and A. Ghafoor, "A Policy-Based Authorization Framework for Web Services: Integrating X-GTRBAC and WS-Policy", IEEE International Conference on Web Services, 2007, pp.447-454.