XML Implementation of RBAC in Health Care Adhoc Networks

*Associate Professor, Department of Computer Science and Engineering, Bahria University, Pakistan
**Associate Professor, EE Department, UAE University, Al-Ain 17555, UAE

***Abstract* - As adhoc networks are becoming popular for a variety of applications, so are the issues engulfing their implementations. In this paper, we describe a health care application in an area where normal network connectivity is not available hence adhoc networking of small scale health care units and corresponding devices become necessary. We discuss how different roles of such units can be framed to facilitate RBAC conformant access. Further, we propose XML implementation of such access control within a typical health care environment .**

I. INTRODUCTION

A mobile adhoc network (MANET) [1-3] provides a communication environment that is characterized by dynamic changes in the topology and in the availability of resources. More research work has, recently, been reported in literature, which addresses issues of security across different aspects of adhoc networks. For example, the authors in [4-6] address the weaknesses of current routing protocols in adhoc networks with respect to security and highlight the robustness of the mechanisms proposed in their work. In [7], the authors have addressed security issues in an environment where devices remain in contact with each other for longer duration. For this purpose, a fully distributed approach has been proposed to secure long term communities of devices. Buchegger and Le Boudec [8] have proposed a technique called CONFIDANT (Cooperation of Nodes, Fairness In Demand Adhoc NeTworks) that primarily aims at detecting malicious nodes by means of combined monitoring and reporting and establishing routes by avoiding misbehaving nodes. The weakness lies in detection process where node identity is assumed to be persistent. This may lead to spoofing attacks. A related work can also be found in [9], where authors have addressed a subset of all threats in adhoc networks and have proposed short of a comprehensive answer to the security problem.

Typically, collaborations among the participants that form an adhoc network cannot be set up because they do not trust each other to use their respective services and resources [10-11]. Therefore, there is a need for explicit specification of policies for each activity. A large number of enterprises have recently started to explore Internet based workflow management systems to help improve their services and decision-making processes [12]. There has been a number of access control models discussed in literature for various objectives [13-14]. Among them, the RBAC model is gaining attention as a generalized approach and provides several advantages. Under the RBAC framework, users are granted membership into roles based on their responsibilities in the organization. User membership into roles can be revoked easily and new memberships established as job assignments dictate. Role-Based Access Control (RBAC) models [15-16] are receiving increasing attention as a generalized approach to access control. Thus, a role is a collection of permissions (or operations on a set of objects) determined by the system, based on the users organizational activities and responsibilities. Furthermore, RBAC has shown to be policy neutral [17] and supports security policy objectives, and static and dynamic separation of duty constraints [16]. Moreover, RBAC offers flexibility with respect to different security policies and in fact [18] shows that RBAC can be configured to enforce mandatory and discretionary access control policies.

The eXtensible Markup Language (XML) is regarded generally as having promise of becoming established as the general purpose framework for enabling transfer of data amongst heterogeneous environments. It is emerging as a useful platform-independent data representation language and is growing in proportion to the spreading speed of e-commerce, which requires a policy for providing a safer security service for exchanging e-documents within e-commerce. It is of interest therefore to analyze how suitable it may be once details of applications requirements and constraints are taken into account. Further, it becomes necessary to consider the issue of XML access control and document security in different network environments, for example adhoc network environment.

A lot of research work has been carried out in the area of XML, its specification development, and security features etc. For example in the area of XML, the authors in [19] propose a construct that locates related nodes in an instance of an XML data model, independent of a specific structure. High performance XML parsers can be prepared using parser generation and compilation techniques [20]. In that, parsing is integrated with Schema-based validation and deserialization, and the resulting validating parsers are shown to be as fast as or in many cases significantly faster than traditional non-validating parsers [20].

In the area of security, XKMS (XML key management specification) is one of the XML's security specifications that define the protocol for distributing and registering public keys for verifying digital signatures and enciphering e-documents of e-commerce applications with various and complicated functions. The authors in [21] discuss XKMS-based key management system architecture and a service model using Java crypto technologies and XML security mechanisms. XML digital signature capability has also been discussed in [22], where authors describe a solution to add XML digital signature using a signature server implemented as a web service without modifying XML based systems. In [23], the authors explore eXtensible Stylesheet Language (XSL), whose document transformation component (XSLT) may well have sufficient functionality to perform all reasonable cryptographic transformations to deliver a desired level of document security. The authors in [24] describe developments in

semantic Web and then provide an overview of secure semantic Web. In particular XML security, RDF security, and secure information integration and trust on the semantic Web are addressed. Another work on Web and e-commerce applications security has been reported in [25], where authors discuss, in particular, access control policies, workflow security, XML security and federated database security issues pertaining to the Web and e-commerce applications. In emerging applications, a similar work is found in [26], where future directions for data and applications security that include secure semantic Web, XML security and applications such as bioinformatics, peer-to-peer computing, and stream information management are addressed. In [27], the authors discuss concept of cryptographically secured, XML based Security Labels using a guard prototype for file transfer and web services based applications. Another approach related to XML access control is reported in [28], where storage of the accessibility information is based on the compressed accessibility map (CAM), and further improved by integrating multiple CAMs into an integrated CAM (ICAM).

II. PROPOSED APPROACH

The formation of an adhoc network requires that authentication and server devices be present to initiate formation of an adhoc network. The joining of a device is to be authenticated by a server owned by the organization. Such network architecture is depicted in Figure 1. It consists of a group of devices forming an adhoc network through an authentication server. We propose a multi-channel model for accessing services and information interchange among users. The objective is to define and categorize types of data transfer pertaining to general and role specific use respectively for sake of easiness and simplicity. The universal description, discovery, and integration (UDDI) channel is proposed to include registry information about the groups, given by the central server and propagated by the coordinator device. Each entry in the UDDI channel is identified by Key_i, and information within the channel is customized to fit wireless environments. The session channel contains the description of each session, and information within the session channel is indexed with a service key to enable better access performance. The data channel is used to transfer data among network devices. Whenever a device enters an adhoc network, it downloads UDDI channels content to its device and store it for later use. Caching it avoids frequent access to the channel, and minimizes power consumption of the devices as well. Thus, the organizations need to empower mobile user devices with the ability to:

- Discover session and data channel(s)
- Find out the way to invoke the session (like which input parameters are required).

The impact of using a data buffer, as shown in Figure 1, is to improve cache retrieval. The objective of coordinator buffer is to share and cache those data frequently used by all mobile users. This reduces the amount of disk accesses in central databases. At the end of transaction execution, the device has to perform buffer write to store updated data. This in turn invalidates obsolete data in the buffer. The authentication server may be empowered to supervise many adhoc network(s). In case, if authentication device leaves and another takes over, a new broadcast from authentication server is to be initiated to let all devices know that there is a new authentication server. This however, will require all devices to re-authenticate.

Roles essentially partition database information into access contexts. Methods associated with a database object, also partition the object interface to provide windowed access to object information. By specifying that all database information is held in database objects and authorizing methods to roles, we achieve object interface distribution across roles. By authorizing different users to the different roles, we can enforce both the order of execution on the objects and separation of duty constraints on method execution. Because of space limitations in mobile devices (like laptops etc.), data is proposed to be at database server, where single or distributed databases can be placed, and then caching of events, registries and other services can be allowed on individual devices.

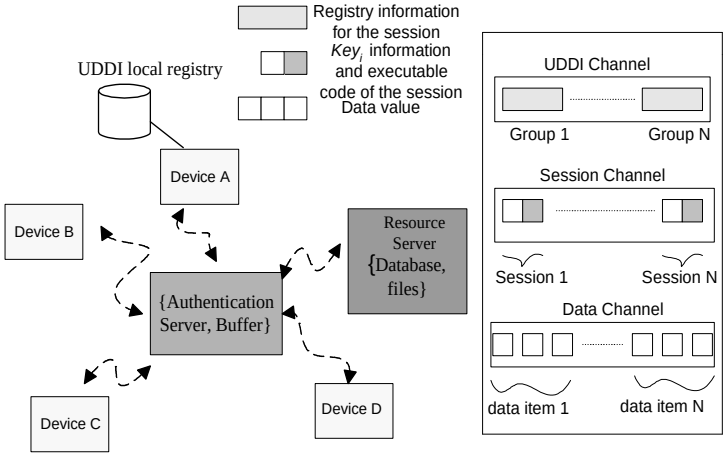

Figure 1: Adhoc Network Infrastructure with multi channels

A. Access Security for a Database Application

The database application we have chosen in this work is a rural health care center. The application is used by basic health unit manager, doctors, Mother and Child Care Unit Incharge to perform various transactions. It is also used by nurses, health visitor, and office assistant to post data. The accounting manager, accountant and internal auditor post, generate and verify accounting data. The process of developing RBAC-based access control for this application is stated below:

(i) *Role definition and functions identification:*

Based on the various categories of participants that will use this adhoc network application, the participating roles and functions required for each role can be defined as follows:

- Office Assistant: Input data in family folders regarding nutrition, and vaccination provided to respective family.
- Mother-Child unit Incharge: Create and delete family folders in addition to tasks defined for office assistant.

- Health visitor: Input/modify vaccination information of children under age 10; input and modify mother nutrition chart.
- Nurse: Input/modify in-patient record.
- Operation Theater (OT) Incharge: Input/modify OT record.
- Doctor: Create/modify/delete in-patient record; enter prescription; create/modify/delete OT record.
- Accountant: Input all health unit transactions and generate General Ledger Reports.
- Accounting Manager: In addition to accountant functions, the ability to modify Ledger Posting Rules.
- Internal Auditor: Verify all transactions and Ledger Posting Rules.
- Basic Health unit Incharge: Ability to perform any of the functions of other roles in times of emergency and to view all transactions, account statuses and validation flags.

(ii) Role Structural relationships

Based on the intended functionality and privilege assignments required for each role, a structural relationship emerges among roles, as shown in Figure 2. It is clear from the Figure that roles higher in hierarchy accumulate more privileges than the ones lower in hierarchy. The privileges set for any two roles which are not part of the same chain are disjoint.

(iii) Formulation of Constraints

a. The maximum number of users that can be assigned to Basic health unit Incharge and Internal auditor is ONE.
b. The following pair of roles can not be assigned to the same user ("Static separation of Duty (SSD) or Membership Mutual Exclusivity (MME)")
    1. MCC Incharge and Accounting Manager
    2. MCC Incharge and Internal Auditor
    3. Doctor and Accounting Manager
    4. Doctor and Internal Auditor
    5. Accounting Manager and Internal Auditor
    6. Nurse and Health visitor
    7. Nurse and Office Assistant
    8. OT Support staff and Office Assistant
    9. OT Support staff and Health visitor
    10. Nurse and Internal Auditor
    11. Nurse and Accounting Manager
    12. Office Assistant and Accounting Manager
    13. Office Assistant and Internal Auditor
    14. Health visitor and Accounting Manager
    15. Health visitor and Internal Auditor
c. The following pair of roles can not be activated or enabled at the same user session ("Dynamic separation of Duty (DSD) or Activation Mutual Exclusivity"):

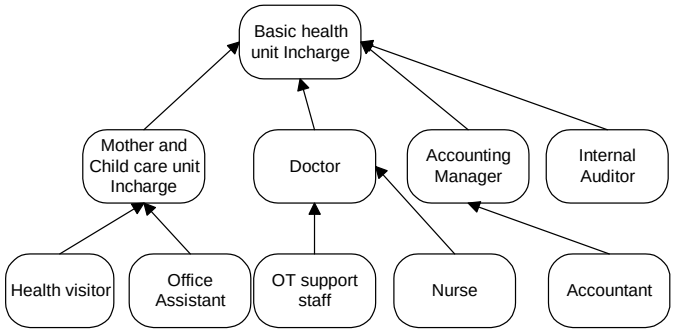

Figure 2: Role Structural relationships

B: Representation of RBAC-based Access Control Data in an XML Document

Our next task is to define a DTD that will represent the schema for the chosen RBAC Model for this application then to capture the actual data in a conforming XML document. Several issues to be considered to define a DTD include the following:

(a) Expressiveness: to capture the semantic of various RBAC model constructs.
(b) Flexibility: Generic DTD to describe most common RBAC models.
(c) Document Readability: That the conforming XML document is readable so that the logic of the RBAC implementation program that parses this document is not unduly complicated.

Since 'Expressiveness" and "Document Readability" have conflicting requirements, hence we have developed manually the following DTD for representing the RBAC model schema:

A fragment of the XML document that conforms to the above DTD which contains RBAC-based access control data relating to this application is given below:

Since we used a conceptual RBAC model for this application to create XML document, many commercial XML processors like in [ ] can be used to validate for conformance to the schema RBAC.dtd.

III. CONCLUSIONS

IV. REFERENCES

[1]. Y. Hu et al. Ariadne "A Secure On-demand Routing Protocol for Ad Hoc Networks". *Proceedings of the* 8th *ACM International Conference on Mobile Computing and Networking*, September 2002.

[2]. F. Stajano. "The Resurrecting Duckling –What Next?" *Proceedings of the 8th International Workshop on Security Protocols*, 2000.

[3]. F. Stajano and R. Anderson "The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks", *Proceedings of the 7th International Workshop on Security Protocols*, 1999.

[4]. P. Papadimitratos, Z. Haas, "Secure Routing for Mobile Adhoc Networks", in *Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference, CNDS* 2002.

[5]. S. Bhargava and D. P. Agrawal. "*Security enhancements in AODV protocol for wireless adhoc networks*", Vehicular Technology Conference, 2001.

[6]. S. Bhargava, D. Agrawal, "Scalable Security Schemes for Ad Hoc Networks", *IEEE Milcom 2002*, Anaheim, California, October 7-10, 2002.

[7]. N. Prigent, J.-P. Andreaux, C. Bidan, O. Heen, "Secure Long Term Communities in AdHoc Networks", 1st *ACM workshop on Security in Ad hoc and Sensor Networks* (SASN), Fairfax, North Virginia, U.S.A., 2003.

[8]. S. Buchegger and J-Y Le Boudec, "Performance Analysis of the CONFIDANT Protocol: Cooperation Of Nodes – Fairness In Distributed Adhoc NeTworks", In *Proceedings of IEEE/ACM Workshop on Mobile AdHoc Networking and Computing (MobiHOC)*, Lausanne, CH, June 2002.

[9]. Refik Molva, Pietro Michiardi, "Security in Ad Hoc Networks", *Personal Wireless Communications, IFIP-TC6 8th International Conference*, pp. 756-775, Italy, 2003.

[10]. Y. Zhang and W. Lee "An Integrated Environment for Testing Mobile Ad-Hoc Networks". In *3rd ACM Symp. on Mobile Ad Hoc Networking and Computing (MobiHoc)*, June 2002.

[11]. L. Zhou and Z. J. Haas. "Securing Ad-Hoc Networks". *IEEE Network Magazine*, Vol. 13, No. 6, November/December 1999.

[12]. Dan C. Marinescu, *Internet-Based Workflow Management: Toward a Semantic Web*, ISBN: 0-471-43962-2, Wiley Publishers, April 2002.

[13]. J. Doshi, W. Aref, A. Ghafoor, and E. Spafford, "Security Models for Web-Based Applications", *Communications of the ACM*, Vol. 44, No. 2, pp. 38-44, February 2001.

[14]. R. Sandhu, "Lattice based access control models", *IEEE Computer*, 26, 11, 1993.

[15]. Sandhu, R.S., Coyne, E.J., Feinstein, H.L., Youman, C.E. "Role-based access control models". *IEEE Computer*, 29 (1996) pp. 38-47.

[16]. Ferraiolo, D.F., Sandhu, R., Gavrila, S., Kuhn, D.R., Chandramouli, R. "Proposed NIST standard for role-based access control". *ACM Transactions on Information and System Security* (TISSEC) 4 (2001) pp. 224-274.

[17]. Bertino, E., Bonatti, P.A., Ferrari, E. "TRBAC: A temporal role-based access control model". *ACM Transactions on Information and System Security* 4 (2001) pp. 191-223.

[18]. Osborn, S., Sandhu, R., Munawer, Q. "Configuring role-based access control to enforce mandatory and discretionary access control policies". *ACM Transactions on Information and System Security* (TISSEC) 3 (2000), pp. 85-106.

[19]. S. Zhang, C. Dyreson, Symmetrically exploiting XML, Proceedings of the 15th International Conference on Word Wide Web (WWW '06), May 23-26, 2006, pp. 103-111.

[20]. Kostoulas, M. G., Matsa, M., Mendelsohn, N., Perkins, E., Heifets, A., and Mercaldi, M., XML Screamer: An Integrated Approach to High Performance XML Parsing, Validation and Deserialization, Proceedings of the 15th International Conference on World Wide Web (WWW '06). pp. 93-102.

[21]. N. Park, K. Moon, and Sungwon Sohn, XML Key Management System for Web-Based Business Applications, IEEE/IFIP Network Operations and Management Symposium (NMOS 2004), 19-23 April, 2004, Vol. 1, pp. 903-904.

[22]. Takase, T. Uramoto, N. Baba, K., XML Digital Signature System Independent of Existing Applications, Proceedings of Symposium on Applications and the Internet (SAINT) Workshops, Jan. 28- Feb. 01, 2002, pp. 150-157.

[23]. Bartlett, R.G. Cook, M.W., XML Security using XSLT, Proceedings of the 36th Annual Hawaii International Conference on Systems Sciences, 6-9 Jan 2003, 6 pp. on CDROM.

[24]. Thuraisingham, B., Security Issues for the Semantic Web, Proceedings of 27th Annual International Computer Software and Applications Conference (COMPSAC 2003), 3-6 Nov. 2003, pp. 633 – 638.

[25]. Thuraisingham, B. Clifton, C. Gupta, A. Bertino, E. Ferrari, E., Directions for Web and e-commerce Applications Security, Proceedings of Tenth IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WET ICE 2001), 20-22 June 2001, Cambridge, MA, pp. 200 – 204.

[26]. Thuraisingham, B., Data and Applications Security: Developments and Directions, Proceedings of 26th Annual International Computer Software and Applications Conference, (COMPSAC 2002), 26-29 Aug. 2002, pp. 963 – 965.

[27]. Thummel, A. Eckstein, K, Design and Implementation of a File Transfer and Web Services Guard Employing Cryptographically Secured XML Security Labels, IEEE Information Assurance Workshop, June 21-23, 2006, pp. 26 – 33.

[28]. Mingfei, J., Ada, F., Integration and Efficient Lookup of Compressed XML Accessibility Maps, *IEEE Transactions on Knowledge and Data Engineering*, Vol. 17, Issue 7, July 2005, pp. 939 – 953.

[29]. http://lists.w3.org/Archives/Public/xml-encryption/

[30]. IETF/W3C XML-DSig Working Group, http://www.w3.org/TR/xmldsig-core/:


```
<element name="KeyInfo" type="ds:KeyInfoType"/>
  <complexType name="KeyInfoType" mixed="true">
    <choice maxOccurs="unbounded">
      <element ref="ds:KeyName"/>
      <element ref="ds:KeyValue"/>
      <element ref="ds:RetrievalMethod"/>
      <element ref="ds:X509Data"/>
      <element ref="ds:PGPData"/>
      <element ref="ds:SPKIData"/>
      <element ref="ds:MgmtData"/>
    </choice>
    <attribute name="Id" type="ID" use="optional"/>
  </complexType>
```

Figure 7: Key Info Component