Multimed Tools Appl (2015) 74:2257–2271
DOI 10.1007/s11042-014-1938-x

Design of access control system for telemedicine secure XML documents

Sun-Moon Jo · Kyung-Yong Chung

Published online: 18 March 2014

Abstract XML can supply the standard data type in information exchange format on a lot of data generated in running database or applied programs for a company by using the advantage that it can describe meaningful information directly. Accordingly since there are increasing needs for the efficient management and telemedicine security of the massive volume of XML data, it is necessary to develop a secure access control mechanism for XML. The existing access control has not taken information structures and semantics into full consideration due to the fundamental limitations of HTML. In addition, access control for XML documents allows read operations only, and there are problems of slowing down the system performance due to the complex authorization evaluation process. To resolve this problem, this paper designs and builds a XACS (XML Access Control System), which is capable of making fined-grained access control. This only provides data corresponding to its users' authority levels by authorizing them to access only the specific items of XML documents when they are searching XML documents in telemedicine. To accomplish this, XACS eliminates certain parts of the documents that are inaccessible and transmits the parts accessible depending on the users' authority levels. In addition, it can be expanded to existing web servers because XML documents are used based on the normal web sites. The telemedicine secure and the guidelines are provided to enable quick and precise understanding of the information, and thus the safety enhancement gets improved. Ultimately, this paper suggests an empirical telemedicine application to confirm the adequacy and validity using the proposed method.

Keywords XML · Authorization · Policy · Access Control · Security · Telemedicine

This paper is significantly revised from an earlier version presented at [28].

S.-M. Jo
Department of Computer Information Technology Education, Paichai University, 155-40 Baejae-ro, Seo-Gu, Daejeon 302-735, South Korea
e-mail: sunmoon@pcu.ac.kr

K.-Y. Chung (✉)
School of Computer Information Engineering, Sangji University, Usan-dong, Wonju-si, Gangwon-do 220-702, South Korea
e-mail: dragonhci@hanmail.net

1 Introduction

XML (eXtended Markup Language) is a SGML-based, simple and very flexible text model, which is appearing as a new standard to express and exchange data on the Internet. Taking advantage of its capacity to describe meaningful information for itself, XML can provide a standard data type in the form of exchanging information on many datasets produced in an operating database or the application programs of a company. It is therefore quite suitable for component specifications or document management systems that require a definition and description of detailed information and meanings. As a large amount of XML-type information was provided on the web or telemedicine environment, developers and users became more concerned about the issues of telemedicine XML document security [2, 5, 11, 13, 14, 29, 34, 37 41]. XML documents should include information with diverse levels of sensitivity to support a level of access protection in a minute unit. In some cases, one access control policy can be applied to several documents. In other cases, different access control policies can be applied to parts of a document. Since XML documents are being used based on the websites, it should be possible to expand the access control system of XML documents to existing XML documents. XML documents are not always suitable for a predefined document type. Since an access control policy is quite likely to be specified in terms of the document type, it is essential to properly manage situations that failed to be dealt with using existing access control policy. Similar to models for XML, the existing access control models have considerable limitations because they fail to be based on a language that can structure data semantically. Therefore, it is very difficult to manage safe authorization. To access a part of the document, it was necessary to divide a page into several parts manually and provide different kinds of authority to them. XML document access control has complicated access control techniques according to the operations. It has another problem of reducing the system performance because it considerable memory space because of the repetitive searches of DOM (Document Object Model) [22] trees and parsing of XML documents during the process of authorization and DTD verification [8, 16, 23, 24]. For access control services on the Internet, XML-based access control should provide an authorization policy that can be applied consistently under different conditions and ensure interoperability under existing diverse conditions through the policy.

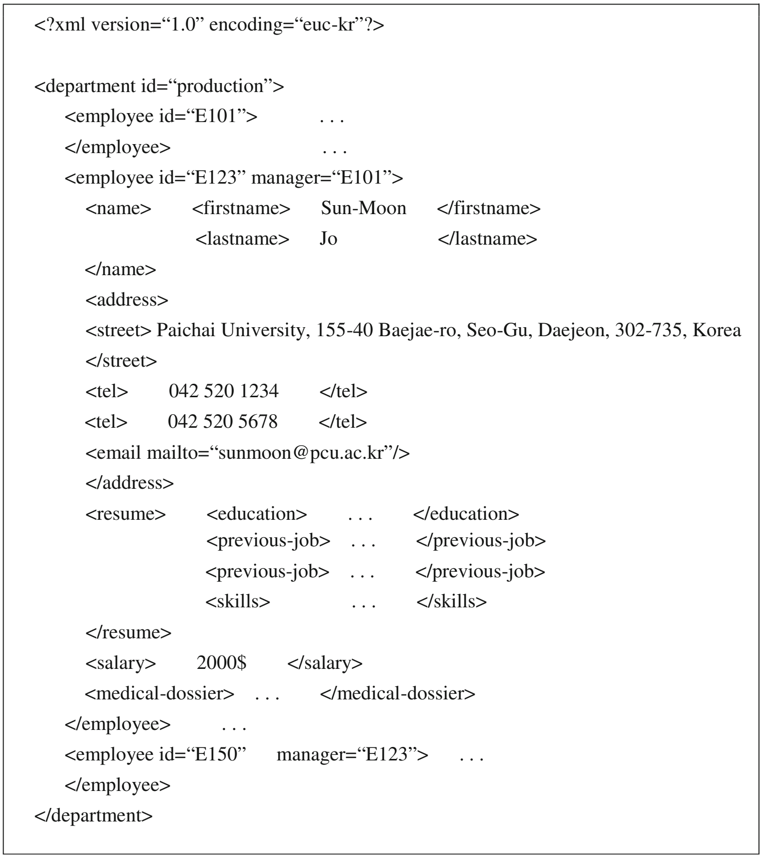
Problem of the conventional telemedicine lies on lack of combined system of a hospital linked medical service with the user oriented feedback service. User affinity lacks due to the development of a device/IT provider oriented medical service rather than the clinician or user oriented service. It is not reflecting the requirements of hospital specialist clinicians those are the core of the actual medical service feedback. Technical and institutional measures are insufficient on exposure of personal medical information, as it provides an individual's health history and biometrics through wired and wireless communication. It is not providing precise guidelines on acquisition and transmission of information considering infringement of human rights [31]. The telemedicine secure XML document technology which is based on information retrieval and convergence security technology needs a next generation wireless communication that executes communication between the devices by connecting the inside of the medical information with the outside region. This paper suggests the concept of fine-grained access control for telemedicine secure XML documents [28].

The paper is proposed as the following. In the chapter 2, the XML and access control would be reviewed. The access control for telemedicine XML documents would be described in the chapter 3 and the design of efficient XML access control system (XACS) in the chapter 4, and concluded in the chapter 5.

2 Related work

2.1 XML and access control review

The basis configuration of the XML document is element. The element can be embedded regardless of the depth and include sub-elements. The element contains the end part of the document in which a limit is determined by two tags. The start tag of <tag-name> type at the starting part of the element, the end tag of </tag-name> type at the ending part of the element and empty element of <tag-name/> type are also available. An example of the XML document that contains information about the company department is shown in Fig. 1. This document provides production department employee's name, address, resume, salary and medical records.



```
<?xml version="1.0" encoding="euc-kr"?>

<department id="production">
    <employee id="E101">          . . .
    </employee>                   . . .
    <employee id="E123" manager="E101">
       <name>      <firstname>    Sun-Moon     </firstname>
                   <lastname>     Jo           </lastname>
       </name>
       <address>
       <street> Paichai University, 155-40 Baejae-ro, Seo-Gu, Daejeon, 302-735, Korea
       </street>
       <tel>      042 520 1234      </tel>
       <tel>      042 520 5678      </tel>
       <email mailto="sunmoon@pcu.ac.kr"/>
       </address>
       <resume>      <education>       . . .      </education>
                     <previous-job>    . . .      </previous-job>
                     <previous-job>    . . .      </previous-job>
                     <skills>          . . .      </skills>
       </resume>
       <salary>      2000$      </salary>
       <medical-dossier>   . . .      </medical-dossier>
    </employee>         . . .
    <employee id="E150"     manager="E123">     . . .
    </employee>
</department>
```

Fig. 1 Example of XML document

The XML document and DTD need to be described according to the following format [7]. $\mathscr{L}$ is a set of element identifiers, *Label* a set of element tags and attribute name, and *Value* a set of attributes and element values [18, 28].

Definition 1 XML document

XML document is tuple d=(V$_d$, $\overline{v}_d$, E_d, ØE$_d$). Where in,

- $V_d = V_d^e \cup V_d^a$ is a set of nodes representing elements and attributes. Each $v \in v_d^e$ has the associated element identifier id$_v$ $\in \mathscr{L}_.$ Where in, each V $\in v_d^a$ has value $val \in V$ values in connection;
- $\overline{v}\ _d$ is a node that represents document elements(called from document root);
- $E_d = E_d^e \cup E_d^a \subseteq V_d \times V_d$ is a set of edges. Where in, e $\in E_d^e$ is linked between elements due to element-sub-element relationship or IDREF(s) attributes, and e $\in E_d^a$ represents element-attribute relationship by edges;
- ØE$_d$: E$_d$ → *Label* is a edge labeling function.

[Gabillon] composed the authorization rules with 4-tuple. The authorization rules are composed of a set of subjects, a set of objects, access and priority [23].

- <set-of-subjects, set-of-objects, access, priority>

The objects are XPath tree nodes represented by the location path of the subjects in relation to element subjects of XML subject sheet. This system does not provide the possibility of protect all kinds of nodes. Moreover, the conflict resolution policy is complex. In other words, it means that semantics will vary depending on the protected objects.

[Hada] was designed to make a decision to grant authority more flexibly by integrating the concept of conditional action into traditional authorization semantics [24, 33, 36]. In this paper, XPath language is not fully utilized. The access control system poses its disadvantage in that the evaluation process of the authority is complex, and response time is slow. The reason is due to repeated search of the DOM tree and parsing of XML documents in the labeling process and DTD validation.

[Lim] defined XML update operators to propose a XML model to support update operations, and included them in the access control model. A new action type was defined to solve problems of performance that occur when update operators are added to the access control [35]. In this paper, a research was conducted by assuming environment. For example, there are no semantic dependencies between elements of the XML. The problem is that a lot of overhead occurs with respect to search queries.

XrML is comprehensive in that it can represent both simple and complicated rights in a variety of workflow steps in a direct manner [13–15, 25, 28, 29, 31, 32, 38]. XrML has problems when requirements for the access of XML document of this paper are taken into account. First, XrML has a difficulty express very simple characteristics such as group member of the subject in a transparent manner, and it has a restriction that the elements of the target document shall be consistent with specific properties of person who raise requirements. Second, XrML is better suited to deal with static resources such as e-books, audio and video files. On the other hand, it has a difficulty dealing with dynamic resources such as XML document that can be revised.

In the case of the existing web-based access control, small-unit level of protection is not accessible, like element and access based on the information meaning for processing according to the meaning of information characterized by the XML document. Requirements for access control of XML document can be summarized as follows [4, 7, 9, 20, 21, 28, 30, 32, 34, 39, 42, 43].

- Since XML document is generally used based on the web site, the access control system of the XML document should be able to be expanded in the existing web server.
- Due to the characteristics of XML, XML document can contain elements with different security levels, so the layer of security needs to be supported to meet this. To satisfy these requirements, the access control system for XML document should have the flexibility to apply the fine-grained security policy.
- Operation of the access control system should be performed transparently to users, and the reason that any one of the document among documents seen by requestors are rejected since it is not granted with authority should not be known.

Since XML document cannot be configured in the predefined type of document at all times, the document format to be returned depending on user's request requires the mechanism in which proper access control can be applied without prior definition and dynamic access control to support this.

3 Access control for telemedicine XML document

3.1 Authorization subjects and objects

For XML document to implement requirements of fine-grained level of protection, the authorization specification should support a wide range of protection objects ranging from a set of XML documents to a specific part of the documents. In the case of XML document, URI [6] can be expanded to path expressions, which are used to identify elements and attributes within the document. In this paper, XPath language to be proposed by W3C is used to identify the internal components of the telemedicine secure XML document [12]. The previous research of [28] is described more detail. The authorization can be specified in a single XML document (authorization of a document or instance level) or DTD (authorization of DTD or schema-level). The authorization specified in DTD is applied to all the XML documents, the instance of DTD. Figure 2 shows the example of Daejeon X university organization. For example, it is assumed that Daejeon X University consists of various departments, and each department is responsible for managing particular XML documents Fig. 2.

Here, general level of protection that should be met in all departments of Daejeon X University can be expressed through authorization of DTD level to the status of Daejeon X University organization. The requirements for special protection applied only to a single department can be expressed through authorization of DTD level. Similarly, requirement applied to specific documents are represented through authorization of instance level associated with the documents.

The subject can generally be mentioned based on the position of requests or identification number. In this paper, an IP address and a symbolic name are used. Therefore, the subject requesting access is composed of a user ID, IP address and symbolic address. The user ID refers to the user ID of the server with which the user is connected, and an IP address and symbolic address refer to the machine through which the user is connected to the server. User groups and position patterns are supported in this paper to permit authorization specifications

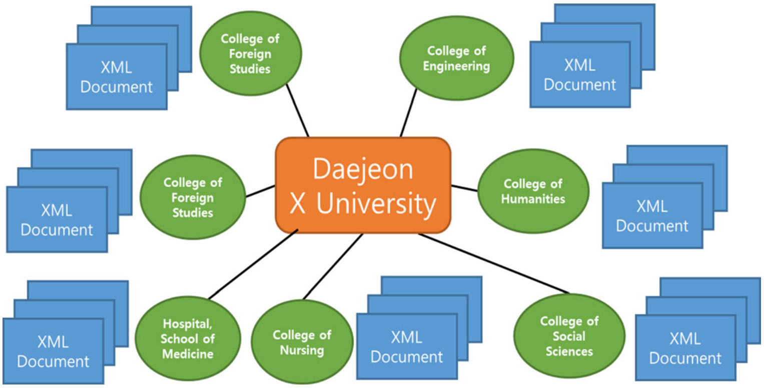


Fig. 2 Example of Daejeon X University Organization

applicable for users and machines. A user group is a set of users defined in the server. A position pattern expresses the physical positions identified in terms of symbolic or numerical identifiers. There are partially-ordered sets, such as a user and group with membership, an IP address with a pattern, and a symbolic name with a pattern. To treat the various components of the subject constantly, a hierarchy as in Definition 2 is suggested in this paper.

Definition 2 Sets are expressed in a capital letter, such as A, B, C, •••, X, Y, or Z.

Elements are expressed in a small letter, such as a, b, c, •••, x, y, or z.

If X and Y are optional sets, Optional subset R of X×Y is defined as relationship between X and Y.

Optional subset R of X×X, or R⊂X×X, is defined as relationship with X.

If Relationship R in Set X is reflexive, antisymmetric, and transitive relation, it is defined as partial-order relation.

If R is relationship in Set X, or R⊂X×X, R is defined as being reflexive when (x, x)∈R (here, x refers to all elements of X).

If R is relationship in Set X, or R⊂X×X, R is defined as antisymmetric when x=y with (x, y)∈R and (y, x)∈R.

If R is relationship in Set X, or R⊂X×X, R is defined as being transitive when (x, z) ∈R with (x, y)∈R and (y, z)∈R.

The access control system in this paper considers the following:

A user group is UG=(U, UG, ≤ UG).

If U is a set of user identifiers and G is a set of user group names, UG=U ∈ G. The two elements are given in x, y ∈ UG, x ≤ UG y.

IP (internet protocol) is IP=(I, IP, ≤ IP).

I is a set of addresses composed of completely-specified numbers. If each element of y is a wildcard character or identical with an appropriate element of x, the two elements are given in x, y ∈ IP, x ≤ IP y.

A symbolic name is SN=(S, SN, ≤ SN).

S is a complete symbolic name and SN is a set of symbolic name patterns. If each element of y is a wildcard character or identical to an appropriate element of x, the two elements are given in x, y ∈ SN, x ≤ SN y.

To meet the requirements at the level of minute protection for XML documents, the authorization specification should support a wide range of protected objects from a set of

XML documents to a certain part of the document. For XML documents, URI can be expanded to path expressions, which are used to identify the elements and attributes within a document. URI indicates the resources to protect the XML documents. XPath language suggested by W3C is used to identify the internal components of XML documents in this paper. The introduction of standard language has the following advantages. First, the users are well aware of the syntax and semantics of language. Second, it can easily be used again to make a function system. In addition, XPath provides many functions to manipulate the character strings, numbers, Boolean logic and node operation [1, 3, 10, 17, 19].

3.2 Authorization mechanism

Since XML has a hierarchic tree structure, authority of a parent node can affect that of a child node. Even the same user can have a different kind of authority according to his or her group, IP address and computer name. Conflict can occur between authorizations in that the subject has a different symbol but is given two types of authority for the same authority to the same protected object. The collision resolution policy to be implemented by the system in this study suggests rules that determine the priority of authorities based on the principles, as shown in Definition 3.

Definition 3

Step 1: Higher priority is given to the authority relevant to the subject described in greatest detail according to the partial order between subject relations.

Step 2: Higher priority is given to the authority described directly than to that which occurred through transmission.

Step 3: Priority is given to the authority described directly in XML documents rather than to that described in the DTD.

Step 4: Priority is given to authority on node rather than to its ancestor.

Labeling is a process of using information about access authority defined by security manager to set access authority on the nodes of DOM tree requested by user queries. If information on the authority is labeled on a DOM tree in the operator unit, labeling is treated repetitively as many times as the number of kinds of operators included in the query. This paper suggests an access control algorithm to remove such repetitive labeling. Figure 3 shows an XML access control algorithm for XML document security. The first step constructs a DOM tree for XML documents. The second step implements access control initialization labeling for a DOM tree. The third step sets the authority on each node and resolves the authority conflict. The final step is a process of removing documents with the final authorization information.

Figure 3 presents the input values that use a requester, XML document URI, DTD of XML and authorization policy. ap is composed of auth.dtd and xml.xas. In general access authorization information, xml.xas is used for the access authority relevant to telemedicine XML documents and auth.dtd is used for that relevant to DTD [27].

In Fig. 4, with a requester and DOM tree of XML document, ap first initializes Variable T into a tree showing the document and then initializes the root into T. The purpose of initialization relates to elements or attributes to a set authorization. Authorization of documents is not applied to all requesters. Authorization of the elements of a document and the setting of authorization by trees can vary according to the requestors. Therefore, the step, Initial_Label, is applied to requesters, setting the authority on document URI at the instance and schema level.

```
rq : Requester(subject, object, action, sign, type),
xml : XML Document URI,
dtd : DTD of XML,
ap : Authorization Policy(auth.dtd, xml.xas)
T : Dom Tree
begin
                T ← Build Dom Tree from xml
                T ← Initial_Label(T, rq, ap)
                T ← Label(T, rq, ap)
                T ← Prune(T)
end
```

Fig. 3 Access control algorithm

The predefined basic access authority value need to be set if the value of the union of auth.dtd and xml.xas that exists in ap is Ø when the present node is the root of the tree, or if there is no explicit access authority. Otherwise, it is necessary to set the authority with the highest priority among explicit ones. Default() sets the authority so that the security manager can provide the basic access document alone if there is no explicit authorization in a certain XML document. If the union of auth.dtd and xml.xas is not Ø, the decision_rule() sets the

```
Input:    T : Dom Tree,
  rq : requester,
          ap: Authorization Policy(auth.dtd, xml.xas)
Output:   T : Dom Tree
Procedure Initial_Label
begin
      if   T.root then
          if   ap.auth.dtd ∪ ap.xml.xas == Ø then
               T.root.label ← default()
          else
                T.root.label ← decision_rule (ap.auth.dtd, ap.xml.xas)
          fi
      fi
  end
```

Fig. 4 Initial labeling

authority with the highest priority using predefined conflict resolution rules when conflict occurs in an identical mode. In Fig. 5, the root node has no parent node, whereas the root nodes have a parent node. A label related to the nodes is transmitted to the sub-elements and attributes. There is local and reflexive authorization: local authorization is composed of details at the schema level and reflexive authorization is composed of details at the schema level. Ø relates to an absence of authorization. For each child, confirm ap.auth.dtd ∩ ap.xml.xas == Ø from AP if the type of c parent is L(local), R(recursive), LD(local DTD), or RD(recursive DTD); assign information about the label of the parent of c in the case of Ø. In Fig. 6, all sub-trees involving a rejection from documents or nodes attached with a non-authorized label are removed. The present node that is not '+' is removed on a visit to the trees through a post-search.

4 Design of efficient XML access control system

4.1 XACS structure

Our processor takes as input a valid telemedicine secure XML document requested by the user, together with its XAS(XML Access Sheet) listing the associated access authorizations at the instance level. The processor operation also involves the document's DTD and the associated

```
Input:   T : Dom Tree, rq : User_requester, ap : AP
Output: T : modified DOM Tree
Procedure Label
  begin
          for each c ∈ children(T.root)    do
          if c.parent.type in (L, R, LD, RD)    then
                    if auth.dtd ∩ xml.xas ==    Ø      then
                          c.label ← c.parent.label
                    else
                      c.label ← decision_rule(c.p.label, ap.auth.dtd, ap.xml.xas)
                    fi
                    else if ap.auth.dtd ∩ ap.xml.xas ==Ø then
                        c.label ← default()
                      else
                          c.label ← decision_rule(ap.auth.dtd, ap.xml.xas)
                    fi
              fi
        od
end
```

Fig. 5 Set authority and conflict resolution

```
Input:          T : Dom Tree
Output:         T : Pruned DOM Tree
Procedure Prune
  begin
    post ← Postorder(T)
      for each n∈ post do
      if    n.children ==Ø   & n.label   '+'   then
            remove n from T
      fi
od
end
```

Fig. 6 XML document remove

XAS specifying schema-level authorizations. Processor output is valid XML documents including only information a user can access. To provide a uniform representation of XASs and other XML-based information, the syntax of XASs is given by the XML DTD depicted in Fig. 7 [26].

In this study, a prototype was designed in Java using the DOM API Java implementation service that was developed into the Xalan tool of Apache. Figure 8 shows the structure of XML Access Control System (XACS). If a user requests telemedicine secure XML documents from a remote site, XACS at the remote site returns the telemedicine secure XML document according to the user's authority and request in the telemedicine medical center. The security processor uses as input the valid telemedicine XML document requested by the user and the

```
<!ELEMENT authorizations (authorization)+>
<!ELEMENT authorization (subject, object, action, sign, type)>
<!ELEMENT subject (#PCDATA)>
<!ELEMENT object (#PCDATA)>
<!ELEMENT action EMPTY>
<!ELEMENT sign EMPTY>
<!ELEMENT type EMPTY>
<!ATTLIST authorizations about CDATA #REQUIRED>
<!ATTLIST action value (read, write, create, delete) #REQUIRED>
<!ATTLIST sign value (+ | – ) #REQUIRED>
<!ATTLIST type value (L|R|LD|RD) #REQUIRED>
```

Fig. 7 XML access sheet [26]

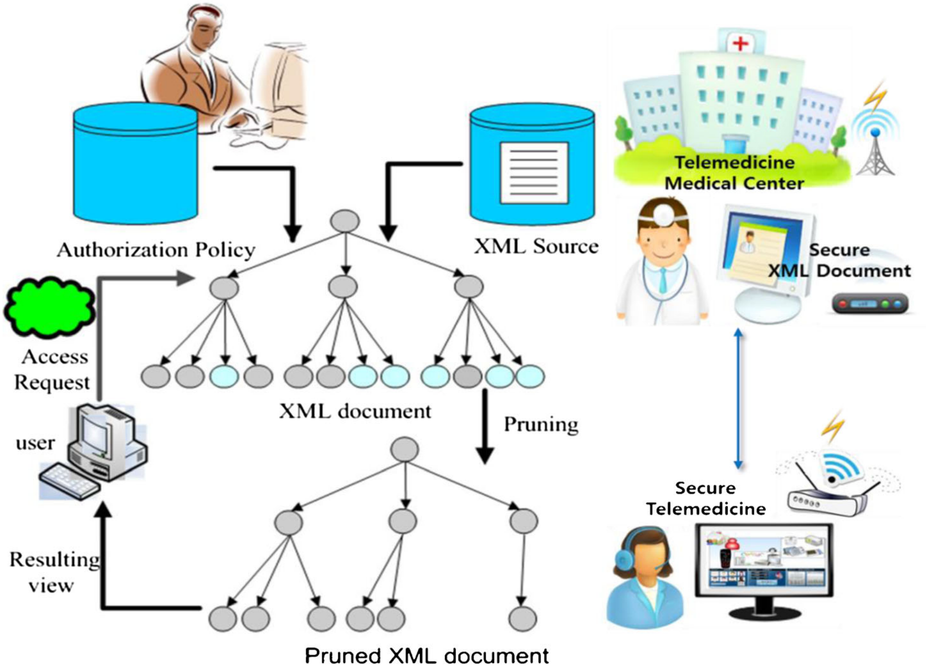


Fig. 8 XML Access Control System (XACS) structure [28]

access control list authorized at the instance level. Operation by the processor also includes the DTD of the document and the access control list described at the schema level. The output of the process is a valid telemedicine XML document just containing the information that a user is permitted to access. The proposed XML Access Control System plays the role of detecting and monitoring the secure information regardless the location, and transmitting it to the telemedicine medical center.

4.2 XACS performance evaluation

For a performance evaluation, comparison was made in the accessibility rate between XACS and XML access control techniques suggested in [23]. For the telemedicine secure XML

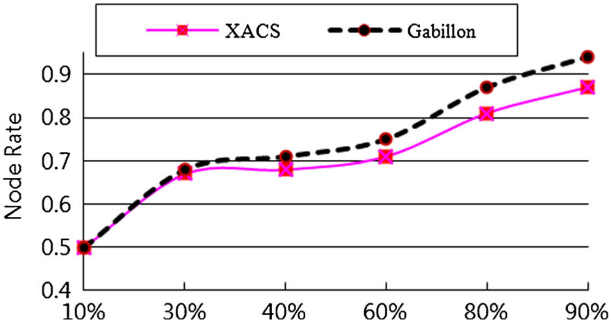


Fig. 9 Accessibility rate

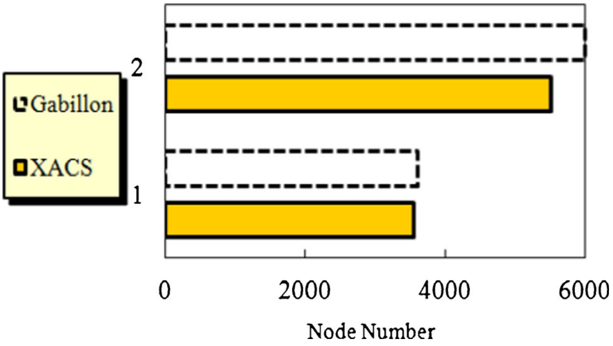


Fig. 10 Change note for the subject

document and DTD, the XML data and documents were used from the XML benchmark [40]. The first test selected several nodes randomly to document with the seed for the access control data and then labeled the seed as accessible or inaccessible to generate XML data access control with a user access mode merge. A comparison was made between XACS and Gabillon because Gabillon [23] is a labeled condition for access control. [40] The document was used for approximately 17,000 nodes in which merge access control was used at various accessibility rates. The criterion for measuring the performance in this study is the ratio of the number of Gabillon nodes to that of the XACS nodes. Figure 9 shows a comparison in terms of the accessibility ranging from 10 % to 90 %. A comparison of the access rate was made with these different levels of accessibility. The second test sampled many users for each of two read execution modes in Fig. 10 and constructed Gabillon and XACS for each single user. Figure 10 shows the ratio of the number of XACS labels to that of the Gabillon nodes for an average user. This is because it was assumed that a Gabillon node is identical to an XACS conversion node in size. On the other hand, an XACA is actually much smaller. This is because Gabillon stores the access authority separately in the data. Therefore, each Gabillon mode will not only include information about access control but also information about the children of nodes in Gabillon and document node reference. In contrast, XACS, which loads information access control in the document encoding, stores only one access control code per conversion node.

5 Conclusions

Telemedicine refers to the remote medical service system which hospitals and clinicians share medical information and medical technology. It is a concept of health management and prevention medical service which can be used anytime anywhere using the wired and wireless networking technology of the fusion of IT and welfare medical service. The information on the telemedicine environment is distributed and shared on a public network. For this reason, it is not stable from attracts such as the access of users without authority on the sensitive information and information counterfeiting. The existing access controls on a web cannot take full account of information structure and semantics due to the basic limitations of HTML. In addition, the access control only provides read-operation and allows changes of very limited values in the case of write-operation. In a search with a telemedicine secure XML document as target, there is a need to provide data applicable to the range of user's authority by granting authority so that users can have an access only to specific items of the XML document. To do this, user's right to access should be managed, and control based on the authority needs to be done when users have access to the XML document. In this paper, method to utilize the capacity of XML itself is described by defining and designing the authorization for access to documents and access control mechanism for efficient document management. The use of authorization sheet related to each XML document and DTD was introduced, along with the suggestion of fine-grained access control XACS for the telemedicine secure XML documents. Through this, a security administrator sets user's rights to read the information in the element, or add, modify and correct the element links. In addition, the security markup of this paper was designed to express various security requirements, supporting exceptions. The execution of requirements described in the authorization allows users to see documents, which include the only information that can be open to the service requestor. The concept of the subjects in this paper consists of identification number and location. In the identification number, information about the group or organization membership can be contained. This paper includes data-dependent conditions, and it is open and possible to expand so that other execution conditions such as restrictive conditions can be easily added.

For future work, it is required to study the control access to reflect each characteristic in other applications that use the telemedicine secure XML document, methods to set authorization automatically on a semantic web and access control policies through more simplified procedures.

Acknowledgments This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2013R1A1A2059964).

References

1. Adler S, Berglund A, Caruso J, Deach S, Graham T, Grosso P, Gutentag E, Milowski A, Parnell S, Richman J, Zilles S (2001) "Extensible stylesheet language (XSL) version 1.0," World Wide Web Consortium (W3C), Available at http://www.w3.org/TR/xsl
2. Agostino Ardagna C, Damiani E, De Capitani di Vimercati S, Samarati P (2005) "A Web Service Architecture for Enforcing Access Control Policies," Elsevier B.V,
3. Apache Software Foundation (2001) "Xalan-J version," 2.2.d14. Available at http://xml.apache.org/xalan-j/
4. Baek SJ, Han JS, Chung KY (2013) Dynamic reconfiguration based on goal-scenario by adaptation strategy. Wirel Pers Commun 73(2):309–318
5. Bartel M, Boyer J, Fox B, LaMacchia B, Simon E (2002) "XML Signature Syntax and Processing," http://www.w3.org/TR/xmldsig-core/
6. Berners-Lee T, Fielding R, Irvine UC, Masinter L (1998) "Uniform resource identifiers (URI): Generic syntax", Available at http://www.isi.edu/in-notes/rfc2396.txt
7. Bertino E, Braun M, Castano S, Ferrari E, Mesiti M (2000) "Author-X: a java-based system for XML data protection," Technical report, Dipartimento di Scienze dell' Informazione, University of Milano, submitted for publication
8. Bertino E, Castano S, Ferrari E (2001) Securing XML documents with author-x. IEEE Internet Comput 5(3): 21–31
9. Bertino E, Ferrari E (2002) Secure and selective dissemination of XML documents. J ACM Trans Inf Syst Secur 5(3):290–331
10. Biron P, Malhotra A (2001) "XML schema part 2: Datatypes", World Wide Web Consortium (W3C), Available at http://www.w3.org/TR/xmlschema-2
11. Bray T, Paoli J, Sperbera-Gcqueen C, Maler E (2000) "Extensible markup language (XML) 1.0 (second edition)," World Wide Web Consortium (W3C), Available at http://www.w3.org/TR/REC-xml
12. Bray T et al (2000) "Extensible Markup Language (XML) 1.0," World Wide Web Consortium (W3C), http://www.w3c.org/TR/REC-xml, October 2000
13. Chung KY (2013) Recent trends on convergence and ubiquitous computing. Pers Ubiquit Comput. doi:10.1007/s00779-013-0743-2

14. Chung KY, Na YJ, Lee JH (2013) Interactive design recommendation using sensor based smart wear and weather WebBot. Wirel Pers Commun 73(2):243–256
15. Content Guard (2001) "eXtensible Rights Markup Language (XrML) 2.0," Available at http://www.xrml.org
16. Damiani E, Vimercati S, Paraboschi S, Samarati P (2000) "Design and implementation of an access control processor for xml documents," in proceedings of the 9th International WWW conference, Amsterdam, pp 55–75
17. Derose S, Maler E, Orchard D (2001) "XML linking language (XLink) version 1.0.," World Wide Web Consortium (W3C), Available at http://www.w3.org/TR/xlink
18. Deutsch A, Fernandez M, Florescu D, Levy A, Suciu D (1999) "A Query Language for XML," In International Conference on World Wide Web, http://www8.org/
19. Deutsch A, Tannen V (2001) "Containment and integrity constraints for xpath," In Proceedings of the Eighth InternationalWorkshop on Knowledge Representation Meets Databases (Rome), September 2001
20. Devanbu P, Gertz M, Kwong A, Martel C, Nuckolls G, Tubblebine S (2001) "Flexible authentication of XML documents," In Proceedings of the Eighth ACM Conference on Computer and Communications Security (Philadelphia), November 2001
21. Sabrina De Capitani di Vimercati (2002) "An authorization model for temporal XML documents," Proceedings of the 2002 ACM Symposium on Applied computing (SAC'02), pp 1088–1093, March 2002
22. Document Object Model (DOM) (2002) Avaiable at http://www.w3.org/DOM/
23. Gabillon A, Bruno E (2001) "Regulating access to XML documents," In Proc. of the Fifteenth Annual IFIP WG 11.3 Working Conference on Database Security
24. Hada S, Kudo M (2002) "XML access control language: provisional authorization for XML documents," www.trl.ibm.com/projects/, pp 1–28
25. Han JS, Chung KY, Kim GJ (2013) Policy on literature content based on software as service. Multimedia Tools Appl. doi:10.1007/s11042-013-1664-9
26. Jo SM, Chung KY (2008) Policy system of data access control for web service. J Korea Contents Assoc 8(11):25–32
27. Jo SM, Chung KY (2009) Efficient authorization method for XML document security. J Korea Contents Assoc 9(8):113–120
28. Jo SM, Chung KY (2011) "Access Control Mechanism for XML Document", In Proc. of the International Conference IT Convergence and Security, LNEE 120, pp 81–90, Springer
29. Jung H, Chung KY (2013) Mining based associative image filtering using harmonic mean. Clust Comput. doi:10.1007/s10586-013-0318-z
30. Jung YG, Han MS, Chung KY, Lee SJ (2011) A study of a valid frequency range using correlation analysis of throat signal. Inf Int Interdiscip J 14(11):3791–3799
31. Jung EY, Kim JH, Chung KY, Park DK (2013) Home health gateway based healthcare services through U-health platform. Wirel Pers Commun 73(2):207–218
32. Kim JH, Chung KY (2013) Ontology-based healthcare context information model to implement ubiquitous environment. Multimedia Tools Appl. doi:10.1007/s11042-011-0919-6
33. Kudoh M, Hirayama Y, Hada S, Vollschwitz A (2000) "Access control specification based on policy evaluation and enforcement model and specification language," In Symposium on Cryptograpy and Information Security, SCIS
34. Lee KD, Nam MY, Chung KY, Lee YH, Kang UG (2013) Context and profile based cascade classifier for efficient people detection and safety care system. Multimedia Tools Appl 63(1):27–44
35. Lim HC, Park S, Son HH (2003) "Access Control of XML documents Considering Update Operations," In Proc. of the 10th ACM Workshop on XML Security, Fairfax USA
36. Murat M, Tozawa A, Kudo M, Hada S (2006) Xml access control using static analysis. J ACM Trans Inf Syst Secur
37. OASIS, "OASIS eXtensible Access Control Markup Language (XACML)," Working Draft 14, http://www.oasis-open.org/committees/xacml/docs/, June 2002
38. Park RC, Jung H, Chung KY (2014) "Picocell based Telemedicine Health Platform for Human UX/UI", Multimedia Tools and Applications
39. Samarati P, De Capitani di Vimercati S (2001) "Access control: Policies, models, and mechanisms," In Foundations of Security Analysis and Design, R. Focardi and R. Gorrieri, Eds., Lecture Notes in Computer Science, vol. 2171. Springer-Verlag, New York
40. Schmidt A, Waas F, Kersten M, Florescu L, Manolescu D, Carey MJ, Busse R (2001) "The XML Benchmark Project," Technical Report INS-R0103, CWI, Amsterdam, the Netherlands
41. Sriram M, Arijit S, Yuqing W (2006) A Framework for access control for XML. J ACM Trans Syst Inf Secur 1–38

42. Yu T, Srivastava D, Lakshmanan LVS, Jagadish HV (2004) A compressed accessibility map for XML. ACM Trans Database Syst 29(2):363–402
43. Zhang N, Kacholia V, Ozsu MT (2004) "A succient physical storage scheme for efficient evaluation of path queries in XML," in proc. 20th int. Conf. on Data Engineering, pp 54–65

Sun-Moon Jo received the Ph.D. degrees from the Inha University, Korea, in 2007. He has worked for Seven System Korea. He is currently a professor in the Department of Computer Information Technology Education, Paichai University, Korea. His research interests include XML, Security, Knowledge System, HCI, and Recommendation.

Kyung-Yong Chung has received B.S., M.S., and Ph.D. degrees in 2000, 2002, and 2005, respectively, all from the Department of Computer Information Engineering, Inha University, Korea. He has worked for Software Technology Leading Department, Korea IT Industry Promotion Agency (KIPA). He is currently a professor in the School of Computer Information Engineering, Sangji University, Korea. His research interests include Medical Data Mining, Healthcare, Knowledge System, HCI, and Recommendation.