A Study of Access Control Requirements for Healthcare Systems Based on Audit Trails from Access Logs

Lillian Røstad and Ole Edsberg
Norwegian University of Science and Technology (NTNU)
Department of Computer and Information Science
Trondheim, Norway
{lilliaro,edsberg}@idi.ntnu.no

Abstract

In healthcare, role-based access control systems are often extended with exception mechanisms to ensure access to needed information even when the needs don't follow the expected patterns. Exception mechanisms increase the threats to patient privacy, and therefore their use should be limited and subject to auditing. We have studied access logs from a hospital EPR system with extensive use of exception-based access control. We found that the uses of the exception mechanisms were too frequent and widespread to be considered exceptions. The huge size of the log and the use of predefined or uninformative reasons for access make it infeasible to audit the log for misuse. The informative reasons that were given provided starting points for requirements on how the usage needs should be accomplished without exception-based access. With more structured and fine-grained logging, analysis of access logs could be a very useful tool for learning how to reduce the need for exception-based access.

1 Introduction

Security is a key concern for healthcare systems that contain sensitive data, like the Electronic Patient Record (EPR). Access control is at the heart of this concern. While healthcare personnel need access to the right information at the right time to provide the best possible care, it is also important to ensure patient privacy.

Over the last few years, we have seen a development in access control research towards more dynamic, workflow-based and user-centered models [1]. However, the state of the art in existing healthcare systems appears to be the traditional Role-Based Access Control (RBAC) model [2], where roles correspond to job functions and administration is centralized. These systems are not well-suited for handling unplanned and dynamic events like patients being transferred between wards, doctors asking for second opinions from colleagues or simply unplanned patient arrivals. Consequently most such systems have exception mechanisms in place in addition to the normal role-based access control for handling these situations. Use of these exception mechanisms typically triggers additional logging of the user's actions. Including these mechanisms makes the systems much more convenient to use. However, from a security viewpoint the use of exceptions leads to added complexity and a need to perform regular auditing to ensure that the mechanism is not misused. With an exception mechanism in place that allows the users to override the normal access control mechanism, technical measures alone cannot ensure privacy and security. This increases the need for manual control mechanisms and awareness training for users to limit the use of the exception mechanisms. However, studying how these access control mechanisms are used - in what situations, to cover what needs - may teach us something about how normal access control mechanisms should be changed to better suit the needs of the users, thereby eliminating or at least minimizing the use of exception mechanisms. Also, it is interesting to investigate if the audit logs contain the necessary information to trace any misuse of such exception mechanisms, or if not - what information is lacking.

In this paper we will examine access logs from an installation of DocuLive EPR[1], a system with extensive use of exception-based access control. Doculive EPR is used by many of the largest hospitals in Norway. We have pulled information from the access logs from all eight hospitals in the Central Norway Health Region (CNHR). The aim of this work is to investigate if the audit trails may uncover information about the real user needs that will be helpful in designing better access control mechanisms for healthcare and also to examine if the logs contain the information needed

[1] DocuLive is a product of Siemens Medical Solutions

Proceedings of the 22nd Annual Computer Security Applications Conference (ACSAC'06)
0-7695-2716-7/06 $20.00 © 2006 IEEE

to uncover misuse. Additionally we aim to explore if any of the principles set forward in access control research in recent years may be applied to create better-suited access control mechanisms for healthcare systems.

2 Related work

To our knowledge there has been no previous work published on investigating audit trails from EPR systems to extract access control requirements for healthcare systems. However some work has been done on eliciting access control requirements for healthcare systems by other means. Evered and Bögeholz in 2004 published a paper [3] describing how they performed a detailed case study on a small aged-care facility in Australia that at the time of study only used paper-based records. The study illustrates that even for such a small example, the access control requirements are very complex. In a short (one page) paper from 1998 [4] Beznosov discusses requirements for access control in the US healthcare domain and states that it should be based on role, affiliation, location, time and relationship. It is however not clear from the one-page paper what these conclusions are based on. In a classic paper [5] from 1996 R. J. Anderson presents a general security policy model for clinical information systems, which includes access control. He bases the motivation for this policy on a number of identified threats towards healthcare systems. Based on his experience and involvement in international EPR architecture and security standards, Blobel in 2004 [6] published a paper describing a set of models for authorization and access control in healthcare systems.

3 The subject of study

Norway is divided into five health regions: north, south, east, west, and central. Each region has a regional health authority and several health enterprises. Each health enterprise encompasses one or more hospitals, and together the health enterprises in one region encompass all hospitals within the region. In the Central Norway Health Region (CNHR), which was the object of this study, there are four health enterprises and eight hospitals. All of these hospitals use DocuLive EPR. Norwegian laws prohibit sharing of medical records between health enterprises. Medical information may be transferred based on a specific request, but not shared in real-time, e.g. through a common EPR-system. As Figure 1 shows there are therefore separate installations of the EPR-system for each hospital. However, there is one common organization, CNHR IT, which is responsible for the daily operation and maintenance of the EPR-systems for all hospitals in the region. Because they all use the same EPR-system, DocuLive, it is possible to extract and compare log data across hospitals.

Figure 1 also illustrates how the EPR system for one hospital is divided into three domains: somatic, psychiatry and child and youth psychiatry. Information in the patient record is assigned to a domain. Domains are used to protect information that is considered "extra sensitive". This means that a user working on a ward in the somatic domain does not have access to parts of a patient's EPR that belong to any of the other two domains - even if the patient currently is at this user's ward. Only users working in psychiatry or child and youth psychiatry can access parts of the EPR that are assigned to these domains.

In DocuLive access decisions are based on a user's *role* (e.g. doctor, nurse, secretary), current place of work (ward) and the type of information being accessed. The role determines which documents in the EPR a user is allowed to access. At any given time a user has access permissions according to his or her role for the patients that are currently registered at the ward where he or she works. Note that a user may be assigned to several roles and places of work. In addition, there are two exception mechanisms for access:

- Actualization - allows a user to open the EPR of a patient that he/she does not have access to through the normal access control mechanism. The user is granted access to the EPR as though the patient was registered at the ward where he/she works. The permission to use the actualization mechanism is not part of a user's role, but is granted on an individual basis. When using actualization the user has to provide a reason for doing so, and the action is recorded in a separate log for use of actualization and emergency access. The EPR is then opened for a specific time period, which depends on the reason provided. In CNHR there are currently eight predefined reasons for using actualization which are shown in Table 1 with corresponding time intervals. There is also the option for entering a self-defined reason and time interval. Actualization is also used as an automatic mechanism by the system for opening EPRs for users who are assigned an approval-task (signing) for documents in the EPR and for opening the EPR of patients who are scheduled to arrive at the hospital soon, but have not been admitted yet. The time-period for automatic actualization is set to 7 days.

- Emergency access - allows a user to open a single document in a patient's EPR that he/she does not have access to through the normal access control mechanism. The emergency mechanism is stricter than actualization in that it has to be used on every single document that the user wants to open. In CNHR only some of the hospitals use emergency access - most make due with only actualization. However - where in use - emergency access is used to access EPR documents across

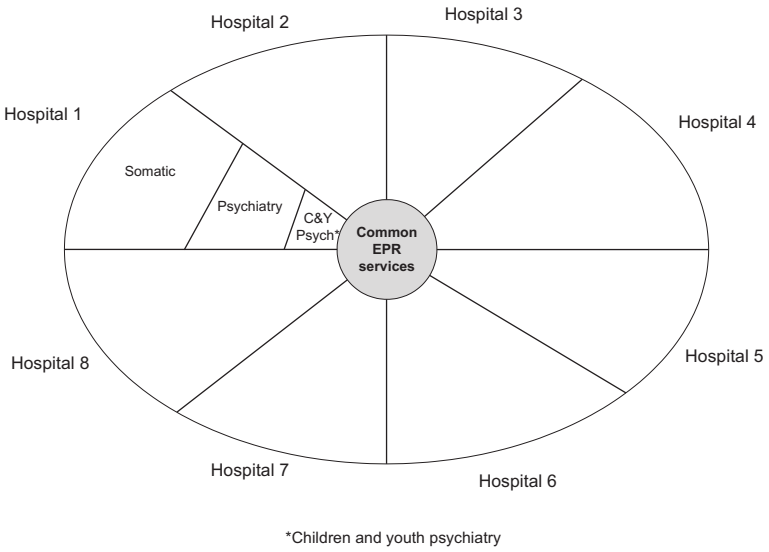

Figure 1. EPR Hospital model

domains within one hospital. That is: some use it as a way for users in the somatic domain to access information in the psychiatry and child and youth psychiatry domains. As for actualization, when using emergency access control the user has to provide a reason and the action is recorded in the same log as use of actualization log. Note that there are no predefined reasons for using emergency access; the user always has to manually provide a reason. Also note that the time interval where the document remains accessible after using emergency access is firm. In CNHR this time interval is set to 10 hours. Not all documents in the EPR are accessible through emergency access, only those specifically labeled so, and only some users have the permission to use emergency access. Emergency access is assigned to users much in the same way as roles - meaning that the permission to use emergency access is linked to a ward or hospital.

4 Methods and materials

In this study we collected access log data from the EPR-system from all eight hospitals in CNHR for one month (March 2006). There are two separate logs:

- Access log - every time a document is opened an entry is created in the access log containing information about the user, the patient and the document being accessed.
- Actualization and emergency log - an entry is created in this log whenever an EPR is opened using actualization or a document is opened using emergency access. This record also contains information about the provided reason and time interval.

Note that it is only the action of actualization or emergency access that is recorded in a separate log. Any subsequent use of the EPR within the time interval is recorded in the normal access log. Therefore we had to extract and combine information from the two logs to get a complete view of use of EPRs within an actualization or emergency access period.

The IT-unit in CNHR was very helpful in creating anonymized versions of the logs - removing names of users and patients and replacing with anonymous, but unique indexes. In addition to the log-extracts, we also collected an anonymized listing of users in the region including their assigned access permissions. The log-extracts we received consisted of:

- All records:
  - Anonymous user ID
  - Users's place of work - hospital and ward
  - Anonymous patient ID
  - Patient location - hospital and ward
- Only in records from access log:
  - Time stamp
  - Document ID
  - Document type
  - Document code
- Only in records from actualization/emergency log:

Reason	*Time(hours)*
Healthcare - provide/plan/consider	48
User support	3
Research project	24
Write/complete EPR documents	48
Scan	2
Quality assurance - administrative/professional	48
Obliteration/editing/deletion/blocking/merging	1
Control committee	24
Other (self-defined)	-

Table 1. Predefined reasons and time intervals for use of actualization

- Start time
- End time
- Reason

4.1 Research questions

After reviewing the type of information available, we constructed a set of research questions to structure our work. The questions were selected to collect information that we hope will contribute to uncovering access control requirements for healthcare systems. The questions we aim to investigate and hopefully answer are:

- Q1: Is actualization/emergency access used sufficiently infrequent to be considered an exception?
- Q2: Which users (role) use actualization/emergency access the most?
- Q3: Which wards use actualization the most?
- Q4: What reasons are provided for using actualization/emergency access?
- Q5: What kind of information is most often accessed using actualization/emergency access?
- Q6: What information should be recorded in access logs to be able to investigate misuse?

5 Results

5.1 Some basic numbers

Table 2 contains an overview of basic user data: how many users in total, how many have actualization permission and how many have emergency access permission. The table shows that out of a total of 16723 DocuLive users in the health region, 74% have been assigned the permission to actualize EPRs, but only 0,25% have the permission to use emergency access. Note that emergency access is only used by two of the hospitals in the region. The others use only actualization.

	Count	%
No. users actualization perm.	12 298	74
No. users emergency access perm.	41	0.25
No. DocuLive users (total)	16 723	100

Table 2. Number of users and permissions

	Count	%
Actualized EPRs	54 095	54
EPRs accessed using emergency	67	0.07
Number of patients (total)	99 352	100

Table 3. Overall use of actualization

5.2 Q1: Is actualization/emergency access used sufficiently infrequent to be considered an exception?

As Table 3 illustrates, in March 2006 a total of 99 352 distinct patients were in contact (i.e. their EPR's were accessed in some way) with the hospitals in the region. Of these patients 54% had their EPR accessed using actualization. This fact combined with the fact that 74% of all users are assigned the permission to use actualization indicate that use of actualization is indeed not an exception. This motivates further investigations as to how actualization is used.

Emergency access is, by comparison, only used 67 times and only very few users are assigned this permission. The numbers are therefore so low that they are difficult to use as a basis for any reasoning. We will therefore focus on the use of actualization, and only return to emergency access in the discussion - as in the true meaning of it's name this mechanism will probably always need to be present. However the way this mechanism is used in the hospitals in this study, as we have explained earlier, does not really reflect on the name *emergency* access.

Table 4 illustrates the proportions of use of actualization and emergency access compared to the total number of accesses in EPR. One access corresponds to opening of one

	Count	%
Accesses using actualization	297 742	17
Accesses using emergency	67	0.004
Total number of accesses	1 794 153	100

Table 4. Number of accesses in total and using actualization or emergency access

EPR or a folder or document inside an EPR. Based on these numbers we find that 17% of the accesses are based on actualization. On average there were registered 2.31 accesses in an EPR within one actualization period.

5.3 Q2: Which users (roles) use actualization access the most?

Table 5 presents an overview of defined roles, number of users assigned to this role in total, percentage of users within each role who are assigned actualization permission, and percentage of users within each role who have used actualization in the period. Note that we have removed the roles where no users are assigned actualization permission, which were a total of three roles: perfusionist, dental health secretary and acupuncturist.

If we assume that the percentage of actualization assignment for one role reflects the current perceived need or requirement for use of this functionality for users within this role (and possibly also a level of trust in users within this role) - then it is interesting to take a closer look at the differences between actualization assignment and use. DocuLive has been in use since 1998 (from 2002 for the entire region) so it is reasonable to assume that the distribution of roles and permissions are fairly stable now. We may then assume that the percentage of use of actualization reflects the actual needs or requirements of users within a role. If we examine Table 5 more closely we see that on average the actual percentage of use of actualization is significantly lower than the percentage of assignment of actualization. This may lead to the interpretation that actualization is in fact assigned to many users that do not need this functionality - at least not on a regular basis. For instance it seems to be the rule that all doctors should have permission to actualize - but only 52% of doctors did in fact need to do so within this period. Of the nurses, who represent the largest group of users by far, only 22% used actalization - while 61% has the permission to do so. Thus it would be interesting to further investigate who of these users, in what situations actually do require the functionality provided by actualization. However the log-data does not provide sufficient information, and would have to be supplemented with other information - possibly from questionaires, interviews, observations etc.

Role	*Count*	*%act*	*%use*
Nurse	9 234	61	22
Doctor	2 957	99	52
Health secretary	1 934	97	51
Enrolled nurse	799	31	5
Physiotherapist	411	93	52
Midwife	382	83	17
Psychologist	196	99	57
Ergonomist	150	84	38
Social worker	128	95	59
Educationist	101	96	47
Consultant	80	56	30
Social educator	79	84	28
blank/incompr.	48	75	25
Radiation therapist	34	100	44
Audiometrist	31	97	65
Radiologist	26	96	35
Speech therapist	25	80	40
Nutritionist	21	100	71
Bioengineer	16	94	6
Activator	15	67	7
Pharmacist	9	11	0
Welfare worker	9	44	11
Orthopaedy engineer	7	100	14
Dentist	7	100	14
Genetic advisor	4	100	100
Orthoptist	4	100	100
Occupational hygienist	2	100	0
Optician	2	100	100
Child welfare consultant	2	100	50
Ambulance personnel	1	100	0
Dental mechanic	1	100	100

Table 5. Overview of roles with % assigned and use of actualization permission.

Ward	*Users*	*%act*	*%use*
Medical ward (18)	2 834	86.9	49.8
Surgical ward (21)	2150	75.2	33.2
Anaesthesia ward (8)	629	99.5	30.3
Emergency ward (10)	482	71.1	27.6
Out-patient clinics (43)	473	99.7	62.6

Table 6. Overview of users employed at ward types with % assigned and use of actualization permission. The number of wards of a type is given in parentheses. Wards that were not covered by a major type were excluded.

5.4 Q3: Which wards use actualization the most?

From Table 6 we can see that actualization is used rather frequently at the medical ward[2]. According to [7], 90-95% of the patients who are admitted to the medical ward need immediate help. Only 5-10% are planned patient encounters. As such, the high number of actualizations for this ward is unsurprising. It is interesting to note that for the surgical, anaesthesia and emergency wards the percentage of users assigned actualization permission is significantly higher than the percentage of actual use. Out-patient clinics represent the wards with the highest count of actualization use. This is probably due to the fact that patients are not admitted to these wards, they are just there for a short time in the day, and as such it would make sense to have an access mechanism in place to handle this.

5.5 Q4: What reasons are provided for using actualization/emergency access?

Table 7 shows that out of all uses of the actualization functionality, a self-defined reason was only entered in 1.76 % of the cases. We investigated this number further and found that out of all the users who had used actualization functionality in the period only 8% had, at least one time, provided a self-defined reason for doing so. Actualization was used a total of 133 918 times, and a self-defined reason was only provided in 2 357 of these actualization occurrences. Several reasons were provided multiple times, so these 2 357 reasons again map to 730 unique reasons.

These numbers tell us a couple of interesting things. First of all: the availability of predefined reasons means less specific information about why actualization was used. The predefined reasons are so broadly defined that they convey very little information about the user's needs. What we can see is that signing information in the EPR is a common task, that should be included in the normal access control regime.

Although the 730 unique reasons provided are too few to base any quantitative conclusions on, we nevertheless decided to take a closer look, working from the hypotheses that when users took the trouble to manually enter a reason they felt that the predefined reasons did not apply to their situation or did not describe their need accurately. If some of these manually entered reasons are recurring then this implies a need shared by several users. 730 entries are so few that it was possible to examine them one by one and attempt manual classification to see if we could create categories of recurring reasons or types of reasons. We found that the most commonly provided reasons are:

- Out-patient clinic patient encounters.
- Physician referrals.
- Hand over patient information to other hospital/health personnel on request.
- Request for information from a patient or next of kin.
- Release information to other external entity: insurance, legal, complaints.
- Patient not registered correctly in admin system (results in access denied, even though patient is physically present at ward).

As such, these should be considered as candidates for inclusion in the normal access control regime and constitute access control requirements that are not fulfilled.

5.6 Q5: What kind of information is most often accessed using actualization/emergency access?

Table 8 shows how the rate of actualization usage varies with the document category. The high rate of the top entry might be explained by the fact that it includes second opinions, where the provider of the opinion might often need access to the patient record across ward boundaries. The same type of need could also explain the high rate of the second entry, which covers reports from physiotherapists, psychologists and other non-physician specialists. The relatively low rate of the nursing-related entries might be due to the fact that nurses mostly work with the patients admitted to their working ward.

We also see that image-related lab results have almost twice the actualization rate of tissue and fluid-related lab results, perhaps because specialists from other wards are often called upon to interpret images.

With a more fine-grained and well-structured category hierarchy, we might have been able to construct a more

[2]The medical ward mainly offers internal medicinal treatment.

Reason	%
Healthcare - provide/plan/consider	32.87
User support	0.03
Research project	1.64
Write/complete EPR documents	41.27
Scan	2.02
Quality assurance - administrative/professional	2.83
Obliteration/editing/deletion/blocking/merging	0.88
Control committee	0.11
Automatic for signing	10.33
Automatic from planned patient list	6.26
Sum predefined and automatic reasons	98.24
Manually provided, self-defined reasons	1.76

Table 7. Actualization reasons: usage in percent.

Documentcategories	*Totalaccesses*	*%withactualization*
External correspondence	218381	32.80
Reports from other disciplines	60431	25.81
Lab results: Image diagnostics	24438	23.64
Physician's journal	503496	23.09
Declarations etc	13664	19.96
Summaries, not further classified	83810	18.49
Observation and treatment	22883	18.28
Lab results: Tissue and fluids	69046	13.09
Own discharge summaries	106968	12.50
Lab results: Organ function	26342	12.04
Nurses' summaries	10688	7.81
Nurses' documentation	482919	6.37
Other	154326	5.51
Patient orientation	12005	5.30

Table 8. Percentage of accesses performed within actualization periods, for different categories, as classified in the EPR system. The category *Other* collects accesses to documents without category or in categories with fewer than 10000 accesses.

informative chart of actualization rates. If a decision was made to reduce the usage of actualization, such a chart could be used to detect the best possibilities for reduction.

5.7 Q6: What information should be recorded in access logs to be able to investigate misuse?

Exception access in some form will always have to be present in healthcare systems to handle emergencies. Therefore it is important to have sufficient and usable mechanisms to trace any misuse.

It is clear from the work presented here that the DocuLive logs do not present sufficient information to effectively investigate suspicions of misuse. We had to combine data from two separate logs and the user database to be able to do this work, and still we believe that more information is required. The main shortcoming is the predefined reasons for using actualization that mask the real intent.

For an audit trail to be usable it should:

- be available through a usable interface for the administrators, and
- contain sufficiently detailed information to get a picture of what has happened.

6 Discussion

The system under study here in many ways conforms to the ideas of *optimistic security* put forward in [8]. However, this study illustrates how difficult it is to trace events in such a system. Being able to trace events is essential to provide adequate security for systems containing sensitive health information. Therefore we believe that healthcare systems require a stricter form of access control, where the usage of exceptions is minimized. Having examined the audit logs we have found some recurring events fulfilled with actualization, that should be candidates for inclusion in requirements for an access control model that is better suited for the real needs of the users. Thus this should aid in minimizing the use of actualization.

We would also like to point out that when exception mechanisms are introduced, it is important to have regulations on who should be assigned this permission and to ensure that these regulations are followed. It should be easy to obtain an overview over which users, or roles, have the permission to use exception mechanisms. Minimizing risk includes minimizing the user base that has the potential for exploiting exception mechanisms.

Based on this study, we have not been able to conclude on a firm set of requirements for access control in healthcare systems. However, we have identified some initial requirements that we intend to explore further. Most of what we have seen indicates the need for a more dynamic and user-controlled access control solution. We believe that RBAC should be the foundation, but with added ability for handling dynamic events, workflow and collaboration. Several papers, including [9] [10] [11] have been written on the concept of *role delegation* which allows a user to delegate his/her role to another user. This may be used as a mechanism to handle referrals, second opinions and transfer of patients. To be able to do this we should introduce the notion of health personnel-patient *relationship*, meaning that they are linked by something more than just a common ward.

We also think the notion of Team-Access Control [12] centered around a cooperating team seems promising. Based on our findings of provided reason, we believe that the notion of *tasks* and related *responsibilities and duties* provides a promising platform for access control decisions in healthcare systems.

7 Conclusion and future work

Although we have been able to identify some requirements, or initial requirements, in this study, more work needs to be done. We intend to continue our investigation by supplementing with data from other systems from the same period (including admission/discharge dates) to see when actualization is primarily used. In addition we hope also to be able to observe healthcare personnel's information needs in situations where common tasks need to be performed. For that purpose, interviews are another possibility we hope to explore.

Acknowledgements

The authors would like to thank the people at Central Norway Health Region who helped make this study possible. We would also like to thank our advisors Øystein Nytrø and Svein Johan Knapskog, as well as our fellow PhD-student Thomas Brox Røst, for valuable input and help.

References

[1] W. Tolone, G.-J. Ahn, T. Pai, and S.-P. Hong. Access control in collaborative systems. *ACM Comput. Surv.*, 37(1):29–41, 2005.

[2] D. F. Ferraiolo, D. R. Kuhn, and R. Chandramouli. *Role-Based Access Control*. Computer Security Series. Artech House Publishers, Boston, 1 edition, 2003. ISBN: 1580533701.

[3] M. Evered and S. Bögeholz. *A case study in access control requirements for a Health Information System*. Proceedings of the second workshop on Australasian information security, Data Mining and Web

Intelligence, and Software Internationalisation - Volume 32. Australian Computer Society, Inc., Dunedin, New Zealand, 2004.

[4] K. Beznosov. *Requirements for access control: US Healthcare domain*. Proceedings of the third ACM workshop on Role-based access control. ACM Press, Fairfax, Virginia, United States, 1998. ISBN: 1581131135.

[5] R. J. Anderson. *A security policy model for clinical information systems*. Proceedings of the 1996 IEEE Symposium on Security and Privacy. IEEE Computer Society, 1996.

[6] B. Blobel. Authorisation and access control for electronic health record systems. *International Journal of Medical Informatics*, 73(3):251–257, 2004. ISSN: 1386-5056.

[7] St. Olavs Hospital - medical ward. URL: http://www.stolav.no/stolav/Virksomhet/behandling/medisin/index.htm. Last accessed: May 28th 2006.

[8] D. Povey. *Optimistic security: a new access control paradigm*. Proceedings of the 1999 workshop on New security paradigms. ACM Press, Caledon Hills, Ontario, Canada, 2000. ISBN: 1581131496.

[9] L. Zhang, G.-J. Ahn, and B.-T. Chu. *A role-based delegation framework for healthcare information systems*. Proceedings of the seventh ACM symposium on Access control models and technologies. ACM Press, Monterey, California, USA, 2002.

[10] S. Na and S. Cheon. *Role delegation in role-based access control*. Proceedings of the fifth ACM workshop on Role-based access control. ACM Press, Berlin, Germany, 2000.

[11] E. Barka and R. Sandhu. Framework for role-based delegation models. In *Annual Computer Security Applications Conference (ACSAC)*, pages 168–176, 2000.

[12] R. K. Thomas. *Team-based access control (TMAC): a primitive for applying role-based access controls in collaborative environments*. Proceedings of the second ACM workshop on Role-based access control. ACM Press, Fairfax, Virginia, United States, 1997.