An Adaptive Access Control Model for Medical Data in Wireless Sensor Networks

Htoo Aung Maw, Hannan Xiao and Bruce Christianson
School of Computer Science
University of Hertfordshire
Hatfield, United Kingdom
Email: (h.maw,h.xiao,b.christianson)@herts.ac.uk

***Abstract*—Wireless Sensor Networks (WSNs) have recently attracted a lot of interest in the research community. The security mechanism with large overhead of computation and communication, are infeasible to apply in WSNs due to many constraints such as limited energy, resource and memory, and low computation capability. Current access control models cannot make an effective access decision in many events because access decisions are based on predefined access policies and roles. Sometimes, users may need to access important data urgently but apart from those predefined access policies, other user request will not be granted. An adaptive access control model is proposed aiming to provide a flexible and an effective access decision on user access request at any time. The proposed model is developed in Ponder2 framework with additional extensions to adapt the unexpected events by using privilege overriding and also adjust its decision based on users' behaviour trust value. A medical scenario is used as an example application to develop and evaluate the proposed model in Body Sensor Networks (BSNs) and WSNs. In this paper, detailed design, implementation phase, evaluation result and policies testing for the proposed adaptive access control model are presented. Based on an evaluation result, all the modules in the proposed access control model are cooperated to make an effective access decision.**

I. Introduction

Wireless Sensor Networks (WSNs) technology has been the interest of researchers and scientists in many research areas because of their potential to change the way of living with applications in retail, medicine, emergency management and many other areas. WSNs consist of hundreds and even thousand of low-cost small sized sensor nodes each with sensing, processing and communicating capabilities to monitor the real world environment and collect information through infrastructureless ad-hoc wireless networks. Nowadays, a sensor node can capture multimedia data and store data locally as the distributed manner or transfer it to a central storage as the centralized manner. WSNs become popular and play an essential role in the medical or healthcare domain. Wireless sensor nodes become smaller and more powerful to use in a wide range of medical applications such as health monitoring, chronic disease management and measuring user vital signs. Garci-Morchon and Wehrle [1] mentioned that user's medical data lead to security and privacy concern. Therefore, collected and stored data are important and it should be kept secretly. Additionally access to that private data needs to protect unauthorized access from both legitimate and illegitimate users. Using security mechanism can provide the security properties such as confidentiality, authentication, integrity, etc. and can prevent abnormal access from the internal and external users.

This paper focuses on an access control model in WSNs and Body Sensor Network (BSN). There are many constraints such as limited memory and power, which impose unique security challenges and make innovative approaches desirable in WSNs. A new security mechanism and access control model are needed because existing security mechanisms are not efficient, adequate and suitable to use and apply in WSNs. Towards addressing these challenges, this paper discusses an adaptive access control model and its implementation result in Ponder2 framework. The remaining structure of this paper is explained as follows. Section 2 discusses the related work. Section 3 provides an overview of the proposed access control model. In section 4, the development and implementation of an adaptive access control model are discussed. Section 5 represents an evaluation result based on a medical scenario. Section 6 concludes the paper.

II. Related Work

Access control is a critical security service to prevent unauthorized access of network resources from the users. In WSNs, users can enter the sensor field directly to access data at the sensor nodes. Different users may have different access privileges to access data at the sensor nodes based on their roles and policies. Most of the access control models in WSNs and Wireless Medical Sensor Network (WMSN) are based on traditional Role-Based Access Control (RBAC), which has been widely accepted as a policy access control model. Cryptography-based access control is designed for the untrusted environment, where the lack of global knowledge and control is defining characteristics. Cryptography is relied upon to control data access and to ensure data confidentiality and integrity. Cryptography methods in WSNs should meet the constraints of sensor nodes.

Distributed PRIvacy-preserving aCCESS control (PRICCESS) protocol [2] is proposed to provide privacy preserving distributed access control in WSNs. The PRICCESS model used Access Control List (ACL) to store the access permission of the group in the network controller. For ACL, roles need to be predefined in advance based on RBAC. Garci-Morchon et al [1] pointed out that RBAC model is not good enough to use in WSNs because in the traditional RBAC model, the roles and policies have to be predefined in advance. Based on that point of view, they proposed the Context-Aware RBAC [1] model for WMSNs. An access control decision will be based on the modular contextual information such as normal, emergency and critical, to ensure the users' safety. In normal situations, a user needs to verify his role to access the medical data of a healthy patient. The user can perform any action and can access data, when the system declares as critical and emergency case. One of the disadvantages of this model is, there is no prevention or detection mechanism and no verification process to check user's data access, when the critical situation occurs.

Ferreria et al [3] proposed the Break-the-Glass Role Based Access Control (BTG-RBAC). The main idea of this model is to gather necessary information from end users with their collaboration for usable access control policy that can perform BTG action in emergency cases. BTG extension is used for emergency and important cases whenever a user wants to access data urgently and immediately. When the user tries to perform BTG actions, the system will ask him if he really want to perform that action on specific object. If the user answers affirmatively, the system will activate the BTG operation and trigger the associated obligations like alarms, log file, etc. BTG-RBAC model is much more flexible than normal RBAC but one of the disadvantages is that human processes are needed in order to enforce the BTG rules.

Yu et al [4] proposed Fine-grained Data Access Control (FDAC) model which is based on Attribute-Based Encryption (ABE) [5]. The main idea of their approach is to provide a fine-grained access control over sensor data and is resilient against the attacks such as user colluding and node compromising. Their model is based on a centralized approach because only the network controller is managed for key management. If the network controller is compromised, there will be no security provisioning in the network. Therefore, a single point of failure can be occurred. In this approach, CP-ABE based selective broadcast is used for the user revocation and key revocation but there is no detailed information on how to use it.

To avoid a single point of failure, Ruj et al [6] proposed an access control scheme based on Multi-authority Attribute Based Encryption. Their objective is to provide fully distributed data access control by using several Distribution Centers (DCs). All the access structures from each DC, which need to satisfy the attributes from sensor nodes, are ANDed together to get a complete access for the single user. There is no detailed explanation of how to combine all the access structures together. Without the combining approach, the user has to store all the access structures in order to access different types of data from the sensor network.

From the above discussion, it is clear that achieving fine-grained data access control with flexibility is still an open challenge in WSNs. There is no protection for unauthorized usage from both legitimate and illegitimate users. A flexible access decision is needed because it is hard to predict and predefine data access policies for any unexpected and unanticipated events in the real world applications. Current access control models are not flexible enough to make an effective access decision at any time. Therefore, we proposed an adaptive access control model [7] to fill the gap in WSNs area. The proposed model has a similar structure like BTG access control model but the main difference is that no human effort is needed to override rules and policy for unexpected events because of the introduction of users' behaviour trust model, and prevention and detection mechanism.

III. Adaptive Access Control Model

Previously, we have proposed an adaptive access control model [7] to provide a flexible access decision in WSNs. The proposed model is incorporated the concept of possibility-with-override [8] into WSN for hard-to-define and unanticipated situations. Possibility-with-override means users might be able to override a denial of access, when unexpected events occur. The proposed model also uses user behaviour monitoring and trust model to check users' actions, location, time, etc. Whenever users try to access data at the sensor nodes, all user behaviour and user information will be kept by prevention and detection mechanism as an audit record to detect and prevent abnormal and unauthorized access. The detailed information of different modules inside the proposed adaptive access control model are explained in this section.

There are two main modules in the proposed access control model: Policy Enforcement Point (PEP) and Policy Decision Point (PDP). Whenever a user requests the access to an object, an access request will go through PEP for the authentication process and then it will forward a decision request to PDP for decision making process. PDP makes the access decision on user request based on defined policy. The decision response will be forwarded internally to the target. Also, PDP will forward the decision response to the users, whether they have the privileges to access data at the sensor nodes or not.

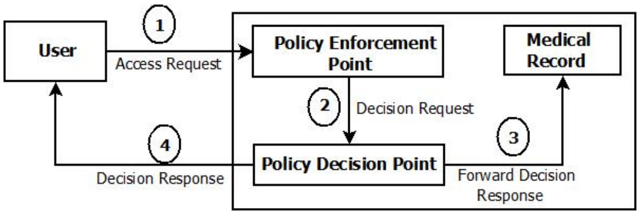


Fig. 1. An Overview of Implementation Framework

The proposed access control model is extended version of Ponder2 [9] by adding extra module and using additional information to provide flexibility. The proposed model is designed to make an effective access decision in both normal and emergency situations. Figure 1 shows the high level overview design of the proposed access control model. The detailed information of both PEP and PDP are explained in next sub section.

A. Policy Enforcement Point (PEP)

In the proposed framework, PEP is used as an authentication service provider between users and sensor nodes. The authentication service is an important security provisioning to provide in the system. Whenever PEP receives an access request from the user, it will check the user information like ID and cryptographic key for the authentication purpose. PEP checks the authenticity of the users, before it forwards the decision request to PDP. Currently, we assume that authentication service and key distribution are already provided in PEP. In future, we will work on the implementation of PEP by using Attribute-Base Encryption (ABE) [5] for data storage. Also Two-Tier Data Dissemination (TTDD) [10] protocol is considered to use for data transmission between users and nodes.

B. *Policy Decision Point (PDP)*

PDP is a main module in the proposed framework. There are three different modules inside the PDP as shown in Figure 2. These three modules are; the access control module, prevention and detection module, and user behaviour trust module. After PEP forwards the decision request to PDP, the information such as user, action, environment and context information will be forwarded to the access control module and the user behaviour trust module. The user behaviour trust module will calculate the trust value and forward that value to the access control module. The access control module will use the trust value from the user behaviour trust module and the other information, which is forwarded by PEP, to make access decisions on the user request. After the access control module makes a decision, it sends back a response message to the users and forwards internally to the target object. The three different modules of PDP are explained as follows.

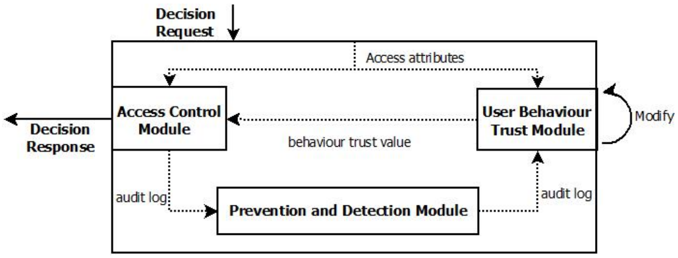


Fig. 2. Policy Decision Point

1) Access Control Module: The access control module is used to make an access decision based on access policies which are predefined in that module. In a normal access control model, there are two access decisions: permitted and denied access. If the user has the privileges to get data at the sensor nodes, his access will be permitted. If the user does not have rights to access data, his access will be rejected. In the proposed model, overriding access is introduced to provide flexibility and make access decisions effectively and efficiently, when the user needs to access data immediately. The access control module will only grant the overriding access to the user, when his trust value is high or trustworthiness enough to access data. Altogether, three access decisions are used in the proposed access control module: permitted access, denied access and overriding access.

In the access control module, there are several predefined authorization, obligation and overriding policies. In the proposed model, the permitted and denied access will be defined. By default, everything else is possible to override. The authorization policy will handle for normal permitted and denied access. The overriding and obligation policy will be used to make an effective access decision based on user behaviour trust value in unexpected events. The detailed definition of these three policies are explained as below.

- Authorization Policy
  An authorization policy is used to enforce the access control module to check whether a subject is authorized to execute an action on a target. In the authorization policy, subject, target, condition and action are used to define access role. Subject means a user, who is trying to access data from the target that stores information. Whenever the access control module receives a decision request, it will check the conditions i.e, location and time which are declared in the specific policy. If the decision request meets the criteria from a certain policy, the subject is allowed to do some actions at the target.

- Obligation policy
  An obligating policy expects zero or more conditions to be evaluated and one or more actions to be performed if the conditions are satisfied. One of the objectives of using an obligation policy is to provide finer-level access control than mere permitted and denied decisions. After a policy has been evaluated, specific obligations are sent along with the authorization decision. The obligation policies are used when the access control module is faced with abnormal user behaviour or overriding access.

- Overriding Policy
  The proposed adaptive access control model introduces an overriding policy based on a user behaviour trust module. Overriding of access control is one way to handle such hard-to-define and unanticipated situations where availability is critical. An overriding policy is used to support flexibility of access control in the proposed model. The policy is designed especially for unpredictable and unexpected situations. Current access control models cannot make an effective access decision based on predefined policies and roles, when an unexpected event occurs. It is hard to predict all of the access control policies because unpredictable events can happen at any time. Comparing the proposed model with other access control models, it provides a flexible approach to make the effective access decisions.

2) Prevention and Detection Module: The privacy and confidentiality of data are still provided even in the emergency case because of the prevention and detection and user behaviour trust module. The prevention and detection module is introduced to prevent abnormal and unauthorized access from both legitimate and illegitimate users. The main idea is to keep the information from user access request as an audit record. The audit record maintains a record of user activities in the system. An audit record can assist to detect security violations and flaws in the system.

In the proposed model, an event-oriented log method is used. The purpose of an event-oriented log is to record an event and specify when it occurred, the user information associated with that event and the results of the decision-making process. The prevention and detection module is used to prevent any specious access from the users to protect confidentiality and privacy of data. An audit record will be used by the user behaviour trust module to predict and calculate the user behaviour trust value for the user's next attempt. We will use ABE based encryption which is already explained under PEP section, to provide confidentiality and integrity of the audit data. The TTDD protocol is considered to provide a secure communication channel for data transmission within BSN and WSN.

3) User Behaviour Trust Module: In current access control models, a user with right access privileges can access data. There is no way to prevent abnormal data access from the authorized user. The proposed model can be protected from these kind of situations by using both the prevention and detection module, and the user behaviour trust module together. In the proposed model, the users' behaviour trust value is calculated and evaluated based on the audit record from the prevention and detection module. The behaviour trust value will be forwarded to the access control module and stored in a database for another evaluation process. The overall structure of users' behaviour trust module is shown in Figure 3. To determine the user behaviour trust value, the previous, predicted and current value of user behaviour trust will be used. Current trust value will be calculated and evaluated based on the user information that is forwarded by the PEP. The previous trust value is stored in the trust module. For predicting user behaviour trust value, Naive-Bayes classification algorithm [11] will be used. The predicting user behaviour is important and significant in forming a trustworthy network. For the classification algorithm, the audit record from the prevention and detection module will be used. There might be more than two classifiers to predict the user behaviour trust value. Overall, the behaviour trust value of the user is calculated based on previous, predicted and current user trust value.

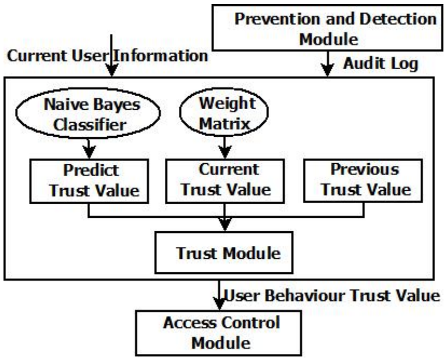


Fig. 3. A Framework of User Behaviour Trust Module

IV. Development of An Adaptive Access Control Model

The proposed adaptive access control model has been developed in Ponder2 [9] that is a popular policy language to use in BSN. Ponder2 comprises a self-contained, stand-alone, general-purpose object management system with message passing between objects. It incorporates an awareness of events and policies and implements a policy execution framework. It has a high-level configuration and control language called PonderTalk and user-extensible managed objects are programmed in Java.

Ponder2 is implemented as Self Managed Cell (SMC) [12] that is a set of hardware and software components forming an administrative domain. It is capable of self management. We assumed SMC as a sensor and try to implement access control model within the Ponder2. Everything in Ponder2 is a managed object. The managed object has to be loaded dynamically into the SMC from a library, thereby producing the factory managed object (Java class). The proposed model is an extended version of Ponder2 by applying possibility-with-override concept, user behaviour trust model and prevention, and detection mechanism together.

We developed the proposed adaptive access control model based on Ponder2 framework. The interface for all the users are implemented in Java based on the managed objects in Ponder2. The Java class file will be loaded dynamically into SMC. The access control module is already implemented for the proposed model and defined the policies based on an application scenario. We designed and implemented the prevention and detection module in Ponder2. The interface for the audit log is implemented in Java. The audit log keeps all the information from user requests, whenever users try to access patient medical records from any location at any time. The audit log is stores as “Write.csv” file that will be used by the user behaviour module to evaluate the trust value of each user. For the users' behaviour trust module, a simple calculation is used and developed. In future, we need to do more work on the user behaviour trust module.

V. Evaluation of Adaptive Access Control Model

In this section, a medical scenario is used to develop the proposed model for BSNs and WMSNs. The policy specification for all scenarios is similar but an access policy for example medical scenario is discussed in this section. SMC [12] is represented as a BSN. In this example, each patient has his own BSN, which consists of several sensors. Sensors sense and collect information such as glucose level, temperature, heart rate, etc. We assumed that sensed data are stored as the medical record in BSN. Users such as doctors and nurses are trying to access medical record of the patient via mobile, personal digital assistant or personal computer. For example, sensors can interact with each other via IEEE 802.15.4 wireless links and interactions with other mobile phone and personal digital assistant from users via Wifi or Bluetooth. Each SMC has its own policy management. Policies are managed by each SMC specifying which actions can be performed. For doctor and nurse, context information will be used, when they try to interact with other SMC or request to join the patient's BSN for data access. The following example scenario will show and express how the proposed access control model is designed and developed for WSNs.

In an example scenario, users are doctors, nurses, patients, patient's family and administrative staff. We assumed that all the users in this scenario are in a “Hatfield” hospital. All the users will try to access the medical record of the patient. Based on their access privileges, the access to the patient medical record will be different. Therefore, access policies are based on the users responsibility, their role and context information such as location and time. A simple scenario of medical application will be used to express and state the policy clearly.

There are two departments in an example scenario: Heart and Cancer department. Nurses and patients will be assigned in one of the department. A doctor can be assigned in the same department as nurse and patient or he can be assigned in any other department. The doctor should be a physician of Heart or Cancer department or General Practitioner (GP) in

"Hatfield" hospital. The doctor and nurse can access patient medical records with a normal authorization policy when they are in the same department as the patient. But the nurse and doctor cannot access the medical record of another patient, who is not in the same department as they are. Otherwise, there might be a lack of data privacy for patient's medical record. For such a case, the overriding policy is used to override the denied access in urgent and emergency cases.

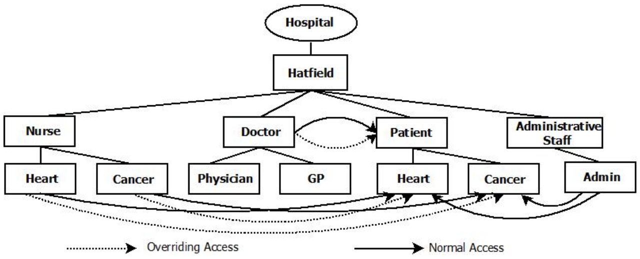


Fig. 4. Normal and Overriding Access

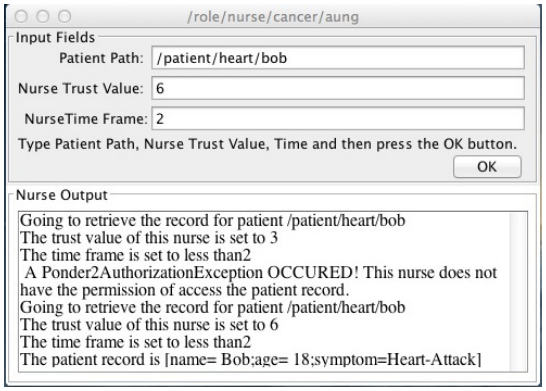
The patient's family might try to access data. They will have the access to the medical record but some important information will be hidden because of patient confidentiality and data security. It is the same for administrative staff. They can only access patient information like name, department and other general information, which means that they are not allowed to request the illness and prescription of the patient. Therefore, based on the role, responsibility of users and trust value, the access control model will make an effective access decision on user requests. Figure 4 explains the overview of normal and overriding access with an example scenario.

A. Evaluation Framework Based on Example Scenario

We evaluate and test the proposed adaptive access control model based on an example scenario. In this section user interface, policies definition of authorization, obligation and overriding, and audit log interface are explained based on the example scenario.

1) User Interface: The Interfaces for all the users in an example scenario have more or less the same feature but the information from the patient medical record will be changed based on their roles and access privileges. Consequently, the access decision will be different for each user. The interface of the nurse is shown in Figure 5.

In Figure 5, a user needs to give input of the patient path that includes the name and location of the patient. For example, Bob is a patient from the Heart department. The path of "Bob" is expressed as /patient/heart/bob. Aung is a nurse from Cancer department by looking at his path; /role/nurse/cancer/aung in above figure. All the trust values for the nurse and doctor are initialized as 5 that is average trust value. The range of the trust value is from 0 to 10. The user needs to fill the time framework, which is between one to twenty-four represented as twenty-four hours in a day. Time framework can be used to check time constraint, e.g a nurse can have access to the patient medical record only at a certain period of time. It is also part of information that will be used to predict the trust value of users.


/role/nurse/cancer/aung

Input Fields

Patient Path: /patient/heart/bob

Nurse Trust Value: 6

NurseTime Frame: 2

Type Patient Path, Nurse Trust Value, Time and then press the OK button.

Nurse Output

```
Going to retrieve the record for patient /patient/heart/bob
The trust value of this nurse is set to 3
The time frame is set to less than2
 A Ponder2AuthorizationException OCCURED! This nurse does not
have the permission of access the patient record.
Going to retrieve the record for patient /patient/heart/bob
The trust value of this nurse is set to 6
The time frame is set to less than2
The patient record is [name= Bob;age= 18;symptom=Heart-Attack]
```

Fig. 5. Interface of A Nurse

Figure 5 also shows the access results of the decision-making process and medical record of the patient. The first result shows that, the nurse from Cancer department cannot access the medical record of the patient from Heart department. Therefore, his access request has been denied because he does not meet any criteria from the authorization policy. The second result shows that if a nurse's trust value is higher than average trust value, he can get the patient medical record from Heart department by overriding his denied access. The access control module assumes that he is trustworthy to access the medical record based on previous interaction between other patients and behaviour trust values. All the permitted, denied and overriding access of the users are kept as an audit record that is used to predict trust value of the users.

2) Authorization Policy: Authorization policy is used for normal permitted and denied access in the proposed model. For example, a nurse sends the access request to a target. The access control module will respond to access request based on the access policy, which is defined in that module for decision making process. The authorization policy can be changed based on the requirements of the application. There might be several authorization policies based on the users' level and access privileges. An example authorization policy is expressed as below:

Def: Permit-Policy
subject nurse **or** doctor
action getrecord
target patient from which department
condition location **or** time
focus target **or** subject

The above permit-policy defines that who has a right to access the medical record from a target object. Subject can only access the target object, when it meets the criteria from the permit policy such as condition. The authorization policy can be handled based on predefined policies, apart from that all the access requests will be denied. For example, the nurse from the Heart department can access medical record of patients from the same department.

3) Obligation Policy: Obligation policy is used in some events to prevent a certain condition. For example, if a nurse meets the criteria to override access policy, the obligation policy will be used and sent along with the overriding policy. Obligation policy is used for triggering an alarm and kept the audit record for further investigation. For example, if the nurse's trust value is less than 5, his access will be denied. At the same time, the obligation policy will become active and keep the audit record based on user information and access request. Additionally, the security alarm will be triggered at the patient side. The format of obligation policy is shown as below.

Def: Audit-Log
on auditrecord
if policy type is override
or trust value is < 5
do write.audit $<$ subject, Time, Target, Behaviour Trust Value, Context Value $>$

4) Overriding Policy: The proposed model extends the Ponder2 by adding an overriding policy. The overriding policy will check one or more one conditions for decision making process at the access control module. A user should be a nurse or a doctor and he can access data from anywhere at any-time. The nurse or doctor needs to meet at least two criteria to override the denied policy. The important factor is the user behaviour trust value which has to be over five to override the policy. If the trust value is set to zero, the person is untrustworthy but if it is set to ten, the person is trustworthy. To override the access policy, the subject have to meet more than one condition that are described as follow:

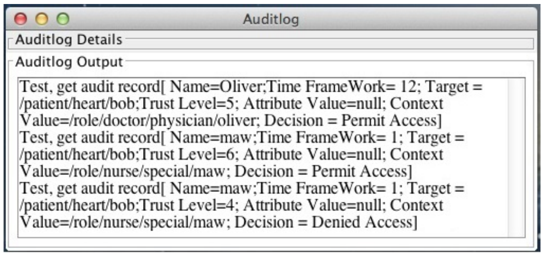
Def: Overriding-Policy
subject nurse **or** doctor
target patient $<$medical record$>$
if trust value is > 5
and location = Hatfield
or time is between 8am to 10am
or nurse **or** doctor is staff
do Set-alarm **and** Audit-Log
action getrecord

For example, if a nurse wants to override his access policy in an emergency or urgent case, his user behaviour trust value has to be more than 5 and at least two of the above conditions need to be trued.

5) Prevention and Detection Mechanism: The prevention and detection mechanism keeps all the information from the user requests as an audit log, whenever users try to access patient medical records from any location at any time. The audit log can be seen on Figure 6. In the audit log format, the subject is a user, who tries to access medical record from the target. In the audit log, time, user behaviour trust value and context information such as location are also recorded. For example from Figure 6, "Doctor Oliver", who works as a "Physician" in "Hatfield" hospital, tried to access the medical record of "Bob" from "Heart" department at "12am" with his trust value "5" and his access request has been permitted.

Auditlog := [Subject + Time + Target + Trust Value + Context Value]

6) User Behaviour Trust Module: The user behaviour trust module used all the information from the audit log to evaluate and calculate the current and predicted user behaviour trust value. When the application is started, the trust value of all the users is initialized as five which is an average trust value. The trust value will be set between zero and ten based on the trust level of the users. The proposed user behaviour module is not finished yet. The overriding policy is tested by giving the user trust value manually. Currently, the simple calculation is used for user behaviour trust value. Whenever the user access request has been permitted, his trust value will be increased by one. If it is a denied access, his trust value will be decreased by one. The user behaviour trust value is forwarded to the access control module. The computation effort of trust model will be evaluated after it is finished completely. The trust model needs to be analyzed and implemented carefully to meet the requirements of WSNs.



```
Test, get audit record[ Name=Oliver;Time FrameWork= 12; Target =
/patient/heart/bob;Trust Level=5; Attribute Value=null; Context
Value=/role/doctor/physician/oliver; Decision = Permit Access]
Test, get audit record[ Name=maw;Time FrameWork= 1; Target =
/patient/heart/bob;Trust Level=6; Attribute Value=null; Context
Value=/role/nurse/special/maw; Decision = Permit Access]
Test, get audit record[ Name=maw;Time FrameWork= 1; Target =
/patient/heart/bob;Trust Level=4; Attribute Value=null; Context
Value=/role/nurse/special/maw; Decision = Denied Access]
```

Fig. 6. Audit Log

B. Summary

Based on the evaluation result with an example medical scenario, the access control module is cooperated with the user behaviour trust module, which worked together with prevention and detection mechanism to evaluate and calculate a trust value of users, to make an effective access decision. All policies are predefined in the access control module, which can adjust its decision based on trust value at any time. Based on the previous discussion, the overriding policy is useful to handle unanticipated situations. Therefore, all the modules in the proposed access model are worked together to make the effective access decision.

VI. Conclusion and Future Work

The overall contribution of this paper is to design and develop an adaptive access control model for medical data in BSNs and WSNs. In this paper, the interface of the example application, the development of possibility-with-override, and the prevention and detection mechanism are developed in Ponder2. The proposed model is developed in Ponder2 framework with additional extensions to adapt the unexpected events by using privilege overriding and also adjust its decision based on users' behaviour trust value. All the modules in the proposed access control are cooperated to make an effective access decision. In this paper, detailed design, implementation result and policy testing for the proposed adaptive access control model are discussed.

Currently, we are working on the user behaviour trust module. A classification algorithm will be used to predict the user behaviour trust value. The previous, current and predicted user trust value are needed to calculate the overall trust value of the user. It is also important to clean up the data from the audit log to use it for the classification algorithm. Further research is needed for how Naive-Bayes and weight metric algorithm can be applied in the user behaviour trust module. In future, we plan to implement the proposed adaptive access control model within the sensor nodes. IRIS version of sensor motes, IRIS

Processor Radio Modules and Lotus motes are considered for the implementation of the proposed model.

Acknowledgement

The authors would like to thank Kevin P. Twidle who helped and gave a source code of the whole Ponder2 project.

References

[1] O. Garcia-Morchon and K. Wehrle, "Modular context-aware access control for medical sensor networks," in *Proceedings of the 15th ACM symposium on Access control models and technologies*, ser. SACMAT '10. New York, NY, USA: ACM, 2010, pp. 129–138.

[2] D. He, J. Bu, S. Zhu, S. Chan, and C. Chen, "Distributed access control with privacy support in wireless sensor network," *IEEE Transactions on wireless communications*, 2011.

[3] A. Ferreria, R. Correia, H. Monterio, M. Brito, and L. Antunes, "Usable access control policy and model for healthcare," *Computer Based Medical System(CBMS)*, 2011.

[4] S. Yu, K. Ren, and W. Lou, "Fdac toward fine-grained distributed data access control in wireless sensor networks," *IEEE Transaction on Parallel and Distributed Network*, 2011.

[5] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proceedings of the 2007 IEEE Symposium on Security and Privacy*, ser. SP '07. Washington, DC, USA: IEEE Computer Society, 2007, pp. 321–334.

[6] S. Ruj, A. Nayak, and I. Stojmenovic, "Distributed fine-grained access control in wireless sensor networks," in *IPDPS*, 2011, pp. 352–362.

[7] H. A. Maw, H. Xiao, and B. Christianson, "An adaptive access control model with privileges overriding and behaviour monitoring in wireless sensor networks," in *Proceedings of the 8h ACM symposium on QoS and security for wireless and mobile networks*, ser. Q2SWinet '12. New York, NY, USA: ACM, 2012, pp. 81–84.

[8] E. Rissanen, B. Sadighi, and M. Sergot, "Towards a mechanism for discretionary overriding of access control," *International Association for Cryptographic Research*, 2004.

[9] K. Twidle, E. Lupu, N. Dulay, and M. Sloman, "Ponder2 - a policy environment for autonomous pervasive systems," in *Proceedings of the 2008 IEEE Workshop on Policies for Distributed Systems and Networks*, ser. POLICY '08. Washington, DC, USA: IEEE Computer Society, 2008, pp. 245–246.

[10] H. Luo, F. Ye, J. Cheng, S. Lu, and L. Zhang, "Ttdd: A two-tier data dissemination model for large-scale wireless sensor networks," in *In Proceedings of International Conference on Mobile Computing and Networking (MobiCom*, 2003.

[11] C. K. I. Williams and D. Barber, "Bayesian classification with gaussian processes," *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, vol. 20, no. 12, pp. 1342–1351, 1998.

[12] E. Lupu, N. Dulay, M. Sloman, J. Sventek, S. Heeps, S. Strowes, K. Twidle, S.-L. Keoh, and A. Schaeffer-Filho, "Amuse: autonomic management of ubiquitous e-health systems," *Concurr. Comput. : Pract. Exper.*, vol. 20, no. 3, pp. 277–295, Mar. 2008.