An Evaluation of Break-The-Glass Access Control Model for Medical Data in Wireless Sensor Networks

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

***Abstract*—Wireless Sensor Networks (WSNs) have recently attracted a lot of attention in the research community because it is easy to deploy them in the physical environment and collect and disseminate environmental data from them. The collected data from sensor nodes can vary based on what kind of application is used for WSNs. Data confidentiality and access control to that collected data are the most challenging issues in WSNs because the users are able to access data from the different location via ad-hoc manner. Access control is one of the critical requirements to prevent unauthorised access from users. The current access control models in information systems cannot be applied straightforwardly because of some limitations namely limited energy, resource and memory, and low computation capability. Based on the requirements of WSNs, we proposed the Break-The-Glass Access Control (BTG-AC) model which is the modified and redesigned version of Break-The-Glass Role-Based Access Control (BTG-RBAC) model. The several changes within the access control engine are made in BTG-RBAC to apply and fit in WSNs. We developed the BTG-AC model in Ponder2 package. Also a medical scenario was developed to evaluate the BTG-AC model for medical data in WSNs. In this paper, detail design, implementation phase, evaluation result and policies evaluation for the BTG-AC model are presented. Based on the evaluation result, the BTG-AC model can be used in WSNs after several modifications have been made under Ponder2 Package.**

I. Introduction

Wireless Sensor Networks (WSNs) have been an area of significant research for a decade because of the potential to change the way of living with applications in military surveillance, electronic medical record, medicine, disaster and emergency management, and many other areas. Recently, WSNs have become more widespread and more active in the research community. The nature of WSNs consist of a hundred or even a thousand of sensor nodes that have an ability to collect, store and transfer data between each other in the network. These days, the sensor nodes can even store and collect multimedia information themselves. A user, who has an appropriate permission, is able to access the collect data at the sensor nodes directly via ad-hoc manner. This means that the data security and control access to that data are essential to provide in WSNs when the users try to access collected data at the sensor nodes. Based on the requirements of application, the provision of security requirements can change. For the military and medical application, the data collected by sensor nodes need to be stored securely and allowed access only to the authorised users. Therefore, some kinds of security mechanism are required for WSNs to provide the security requirements such as confidentiality, integrity, authenticity, etc.

This paper focuses on an access control model in WSNs and Body Area Networks (BANs). The current access control models in information systems are not efficient enough to apply directly in WSNs and BSNs because of limitations such as limited memory, resource and power. These limitations impose unique security challenge. A new light-weight access control model is desired to provide the flexible making process of decision in WSNs. Towards addressing these requirements of WSNs, we developed a BTG-AC model. This is a modified and redesigned version of BTG-RBAC [1] to better fit for WSNs. It provides a flexible approach to the access control engine. The implementation results in Ponder2 framework [2] are also discussed. The remaining structure of this paper is explained as follows. Section 2 presents the related work. Section 3 discusses an overview of the BTG-AC model for WSNs. The development and implementation of the BTG-AC model can be seen in Section 4. Section 5 provides evaluation results based on a medial scenario. Section 6 concludes the paper with the suggestion for future work.

II. Related Work

An access control is a critical security service to prevent unauthorised access to certain network resources. In WSNs, users can enter a 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. Maw et al. [3] stated that a considerable number of access control models has been proposed for use in WSNs, though some of them are not yet implemented. Most of the current 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 are 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.

Yu et al. [4] proposed the Fine-grained Distributed Data Access Control (FDAC) model based on Attribute Based

Encryption. The main idea of their approach is to provide a distributed data access control which is able to support fine-grained access control over sensor data. A network controller, which stores access structures, acts like a central distribution centre and distributes keys to users in FDAC. Only users with the right access structure and the right key can access data at the sensor nodes. The access structures will be different for each user depending on the access privileges of users. If the network controller is compromised by a malicious user, there will be no security provisioning in the system anymore.

Garcia-Morchon and Wehrle [5] proposed the Context-Aware Role-Based Access Control (CA-RBAC) model based on a modular context structure for WMSNs. The aim of the model is to provide context awareness and adapt its security properties to ensure the users' safety. Normally, an authorised doctor needs to verify his access control role in order to access the medical data of a patient but a nurse may not have the same level of privilege. When the system declares to be a critical or emergency case based on the modular context information, the doctor or nurse can take any action and can access data even though they may not be able to access that data in normal conditions. One of the disadvantages of this model is that there is no prevention or detection mechanism nor verification process to check a user's data access right, when the emergency occurs.

Maw et al. [6], [7] proposed an Adaptive Access Control (A2C) model with privilege overriding and behaviour monitoring to provide fine-grained access control for medical data in WSNs. This model has a similar structure to BTG-RBAC [1] but the main difference is that no human effort is needed to override rules and policies because of an introduction of the users' behaviour trust model, and the prevention and detection mechanism. In this model, the users may be able to override a denial of access, when unexpected events occur. In addition, the users' behaviour trust model is used to check the user's action, location, time, etc but there is no detailed information about the behaviour trust model. Without the behaviour trust model, the access decisions cannot be made effectively.

The current access control models in WSNs such as FDAC, CA-RBAC and A2C are mostly looking at how to avoid overly tight policy in the system. Sometimes, the overly tight access control policy might hold access for the appropriate users in unanticipated events. Ferreira et al introduced the BTG-RBAC engine [1], [8] to integrate BTG in the core RBAC model with obligations. They proposed to securely break access control in a controlled manner. The BTG-RBAC model was developed in Premis policy language with an Apache database and XML for Electronic Medical Records (EMRs). The BTG-RBAC model cannot be applied directly to WSNs because of limitations of WSNs. This means that the proposed access control model needs to be light-weight to apply in WSNs. Therefore, we redesigned and modified the BTG-RBAC model to become a light-weight access control model to fill the gaps of WSNs.

The proposed BTG-AC model has been developed in Ponder2 [2] that is a popular light-weight policy language for BANs and WSNs. Ponder2 is implemented as a Self Managed Cell (SMC) [9]. It is a set of hardware and software components forming an administrative domain. It is capable of self management. We assumed that SMC is performed and worked as the sensor node to evaluate the proposed BTG-AC with the example medical scenario. 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.

III. Break-The-Glass Access Control Model

Based on the requirements of WSNs, we modified and redesigned the framework of the BTG-RBAC model to fit in WSNs. Our model refer to as Break-The-Glass Access Control (BTG-AC) still has similar functions to those of the BTG-RBAC model. The main difference is that the BTG-AC model has been developed and implemented within the Ponder2 policy package for BANs and WSNs. The proposed BTG-AC model is to provide BTG action in access control engine for decision making process regarding access. It provides more flexible control of access to data in the event of emergency. The BTG action will perform within the users' traceability by extending the access control engine with obligations for auditing purposes.

Notwithstanding, an overview of BTG-AC in Ponder2 frame-work [2] can be seen in Figure 1. This shows that there are two main modules in the BTG-AC model: Policy Enforcement Point (PEP) and Policy Decision Point (PDP). The user requests will go through PEP and all the user formation will be forwarded to PDP for the decision making processes. There are limitations and issues for the BTG-AC model in Ponder2 language to fit in WSNs. These are discussed as follow:

- There is no BTG state variable in BTG-AC. This means that a fixed BTG state value is used.
- Initially the BTG state is set to FALSE but the state is set as TRUE if there is policy rule that allows a user to perform the BTG operation. The administrator can change the BTG state variable and create a new BTG state for the another or the same role.
- We have assumed that the authentication process is already provided for PEP in the BTG-AC model

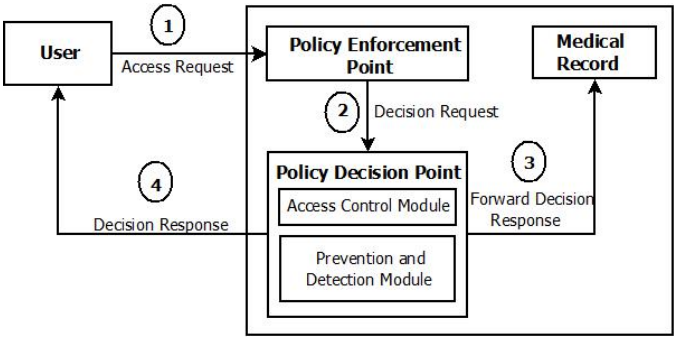

Fig. 1. Overview of the BTG-AC Model

The details information of PEP and PDP are explained next.

A. Policy Enforcement Point (PEP)

In BTG-AC, PEP performs as an authentication service provider between the users and sensor nodes. The authentication service is needed for the provision of security in the system especially when the access control model is allowing users to perform BTG action for data access in emergency situations. A user has to submit the information to PEP for the authentication process. When PEP receives the access request from the users, it will check the users' information such as their identity and cryptographic key. We assumed that the authentication service is provided through use of a users' normal log-in process before forwarding request to PDP. In future, we will work on the implementation of the authentication service in PEP by using Attribute-Based-Encryption (ABE) [10].

B. Policy Decision Point (PDP)

In BTG-AC, PDP is a main module. When PDP receives the decision request from PEP, the access control module will make an access decision. There are different predefined roles and policies in the access control module based on the users location and users' privileges. In the BTG-AC model, there is another module - a prevention and detection module - that keeps a record of all users' information for audit purposes. The two modules cooperate with each other to make the access decision with some flexibility but still within the required degree of prevention and detection. More details of the access control module, and prevention and detection module are explained next.

1) Access Control Module: The access control module is used to enforce the policies for the decision making process. The roles and policies are needed to predefine in advance. Whenever the decision request is forwarded by PEP, the access control module will check whether the information from that decision request is matched with predefined roles and policy. In the access control module, there are three different policies, namely authorisation, BTG and obligation policy. These three policies are developed and designed under the access control module that can be seen on Figure 2.

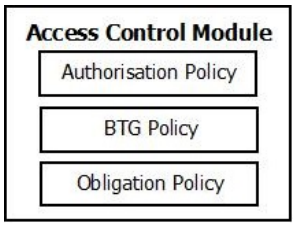

Fig. 2. The Access Control Module

If a user's criteria satisfies the access control policies, the access request will be granted. If they do not match, the access will be denied. In the BTG-AC model, BTG and the obligation policies are introduced to make access decisions in normal as well as emergency situations. A user can perform a BTG action for the targeted object - say, confidential medical record - in an emergency but some obligations will be triggered and performed at the same time. In normal access control models, the decision outcomes will be either permitted or denied access. The existing decision outcomes in the normal access control models are extended by introducing BTG and obligation policy in the access control engine. These decision outcomes are presented as follow:

- (Permit, $\emptyset$) $\rightarrow$ A user has permission to access the targeted object.
- (Permit, OBLGS) $\rightarrow$ A user is allowed to access the targeted object but an obligation is carried out when the access is given.
- (Deny, $\emptyset$) $\rightarrow$ A user request to access the targeted object is denied.
- (Deny, OBLGS) $\rightarrow$ Along side of a denied access, some obligations are performed.
- ($Permit^{(BTG)*(OBLGS)}$) $\rightarrow$ A user's request for access has been granted by performing BTG action and obligations such as "Write to Audit", " Trigger the Alarm" or "A Notification Message" are performed along with access decision.

Based on the above decision outcomes, it is clear that the introduction of BTG and obligation policy is beneficial for medical data in WSNs. The following section explains more details of the authorisation, BTG and obligation policy in that order.

- **Authorisation Policy:** An authorisation policy is used in BTG-AC to enforce an access decision. It also checks whether a user should be allowed to access the targeted object. In authorisation policy, the subject, target and action are checked to enforce the policy. This means that a user, who wants to perform some action on the target object that stores both normal and confidential medical information, has to possess a right access privilege. The access control module will check whether a user's access request has possessed appropriate access right that the subject is allowed to do at the targeted object.
- **Break-the-Glass (BTG) Policy**: A BTG policy is used to perform a BTG operation on a targeted object. To perform the BTG operation, the new role that describes who is allowed to perform a certain action at the targeted object, is added. The obligation policy is used along with the BTG operation allowing an administrator to take actions when the "glass is broken". The new role can be added into the access control module to present how the BTG state variable is reset to FALSE. The BTG state of the permission can be set from TRUE to FALSE or from FALSE to TRUE. The administrator defines the BTG policy for each situation where the BTG action is required by users in an emergency situation.
- **Obligation Policy**: An obligation policy is used along with authorisation and BTG policy in some situations. The obligation policy checks whether one or more conditions have been evaluated and if they have, they carried out one or more actions to be performed. In the BTG-AC model, after the authorisation policy has made the evaluation, some obligations are performed along with the decisions. Similarly the same happened when the BTG policy is activated and made

its decision. The obligation policy is linked with the prevention and detection module to store the user information and his access request as an audit log.

2) Prevention and Detection Module: A prevention and detection module can be used for detecting security violations and flaws in the defined application. It is used to prevent an unauthorised access in the system. Whenever the obligation policy is activated, actions such as write to audit, trigger the alarm, send a notification message to administrator or auditor, etc are performed. There are various methods to store the users' information for the audit log but an event-oriented approach is used to keep a record of the event when it happened, and user information related to that event. Thus, the proposed model can prevent legitimate use by illegitimate users and detect illegitimate use by authorised users.

IV. Development of The Break-The-Glass Access Control Model

The proposed BTG-AC model is an extended version of Ponder2 in which the BTG concept, obligation policy and prevention and detection mechanism are applied together. The interface for all the users such as doctors, nurses and other member of staff is developed in Java based on managed objects in Ponder2. The Java class file is loaded dynamically into SMC. The PEP and PDP are already implemented for the proposed BTG-AC model but the policies definition and expression of authorisation, BTG and obligation policy can vary depend on the requirements of application. The definition and expression of these three policies for medical data in Ponder2 is presented as follow.

A. Authorisation Policy

The terms of the authorisation policy can be changed based on the requirements of the application. In the BTG-AC model, the predefined authorisation policies will be slightly different based on the privileges and roles of the users. An example policy is explained as below:

Def: Permit-Policy
subject A User
role Doctor or Nurse
action Read
target Normal Medical Record

The above authorisation policy defines that a user -a doctor or a nurse- has a right to perform an action called 'read' on a normal medical record. This means that the subject can only access the targeted object, when he meets the criteria of the authorisation policy unless the BTG state variable is TRUE to make a positive decision for access in an emergency situation. Otherwise, the user request will be denied.

B. Break-The-Glass (BTG) Policy

A BTG policy provides a flexibility on decision making process regarding access for the emergency or urgent data access. Thus, the BTG policy allows a user access to confidential data even if he does not have the access right. We assumed that the BTG policy is already defined in advance for these kinds of situations to perform BTG action at the targeted object. If there is no BTG policy for that object, the user request will not be granted. The example BTG policy can be seen as follows:

Def: BTG Policy
subject Nurse
action Read
BTG Yes
target Confidential Medical Record
do Call Obligation Policy

The above BTG policy defines that a user - a nurse - can perform the BTG action to the targeted object but the obligation policy will be activated when the access is given to that user.

C. Obligation Policy

An obligation policy is used along with the authorisation and BTG policies to prevent unauthorised access and to detect security violations. The example of obligation policy is explained as follows:

Def: Audit-Log
on auditrecord
if BTG action is performed
do write.audit $<$ subject, Time, Target, User Role $>$

The above obligation policy defines that it will be activated when the "glass is broken" for urgent and emergency data access. Thereafter, the users' information such as subject, targeted object and user role is stored as comma separated value (csv) in an audit log for further security purposes.

From the above discussion, it can be seen how the proposed BTG-AC was developed and how the policies for authorisation, BTG and obligation can be defined in Ponder2 for medical data in WSNs. The audit log is kept as comma separate value (csv) extension in the BTG-AC model. The next section will explain how the BTG-AC was evaluated based on a medical scenario that was also developed under Ponder2 package.

V. Evaluation of Break-The-Glass Access Control Model

In this section, a medical scenario is explained. It was developed under the Ponder2 package to evaluate the BTG-AC model for BSNs and WMSNs. We assumed that a SMC [9] is represented as the wearable sensor node. In the example scenario, each patient had his own BSN, which consisted of several sensors. The sensor nodes sense and collect information such as glucose level, temperature, heart rate, etc. We assumed that collected data were stored as the medical record in BSN. Users such as doctors and nurses were trying to access the medical record of the patients via mobile, personal digital assistant or personal computer. For example, sensors are able to 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 had managed its own policy. These policies were specified and could be performed by each SMC.

In a medical scenario, there are two different types of data for each patient: normal medical records (ob^2) and

confidential medical records (ob^1). The access policies for users' access to these medical records will be different based on the access privileges and roles of the users. Also different security levels are required in these medical records. This means that the tight policies might be used for confidential medical records to provide data privacy. Nevertheless, the access to even confidential data can be essential in some circumstances. For example, the doctor should be able to access the confidential medical record of a patient when the nurse cannot but the decision can be changed to a positive decision if the nurse performs the BTG actions.

Subject	Role	Operation	Object	BTG	Obligations
Doctor	r^1	read	ob^1	-	oblg [Write to Audit]
Doctor	r^2	read	ob^2	-	-
Nurse	r^3	read	ob^1	BTG	-
Nurse	r^3	$O^{BTG(read)}$	ob^1	-	oblg [Notify Manager; Write to Audit; Trigger the alarm]
Nurse	r^4	read	ob^2	-	oblg [Write to Audit]
Staff	r^5	read	ob^2	BTG	-
Staff	r^5	$O^{BTG(read)}$	ob^2	-	oblg [Notify Manager; Write to Audit; Trigger the alarm]

TABLE I. EXAMPLE OF BTG-RBAC POLICY

Table 1 shows how the designed of BTG-AC model is developed for medical data in WSNs with predefined authorisation, BTG and obligation policies. In this table, the role (r^1) is related to a doctor. The doctor is allowed to access the confidential medical record (ob^1) of a patient but an obligation such as "Write to Audit" will be taken as an action when the decision has been made. This means that the management teams can check the audit log to detect security breaches of doctor. The role (r^2) allows access of the doctor to the normal medical record (ob^2) without obligation. This means that the stored data at the object (ob^2) is not as sensitive as object (ob^1). The roles and policies for other users such as nurses and other members of staff will be predefined differently.

In role (r^3), the nurse is not permitted to access the confidential data (ob^1) unless he performs the BTG action in that object for emergency data access but some obligations will be activated when "the glass is broken". This means that an extra BTG role is needed for the nurse. The role (r^4) allows the nurse to access the normal medical data (ob^2) but still one obligation action is triggered. The role (r^3) and (r^5) have a similar property. There is no way for other members of staff in the hospital to gain access to the confidential medical record (ob^1). There is a way for them to access the normal medical record (ob^2) but they have to "break the glass". The administrator or manager can easily check the audit log to detect illegitimate use from authorised users and to prevent legitimate use from unauthorised users.

A. Evaluation Framework Based on Example Scenario

We evaluate the BTG-AC model based on an example scenario that was developed under Ponder2 package. In this section, user interface, BTG interface, audit log interface for prevention and detection module and how the access decision was made based on different access policies are presented with following screen shots.

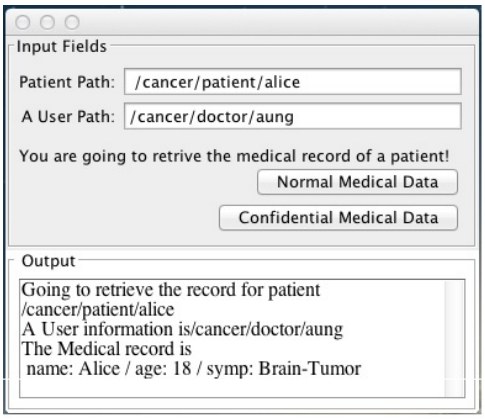

Fig. 3. User Interface for A Doctor

1) User Interface: To evaluated the BTG-AC model for medical data in WSNs, we developed the users' interfaces under Ponder2 package. Based on Figure 3, a doctor (Aung) tries to access the normal medical data of Alice. His access has been granted without any obligation. When he requests access to the confidential data, his requested information will be stored as an audit log to detect security breaches.

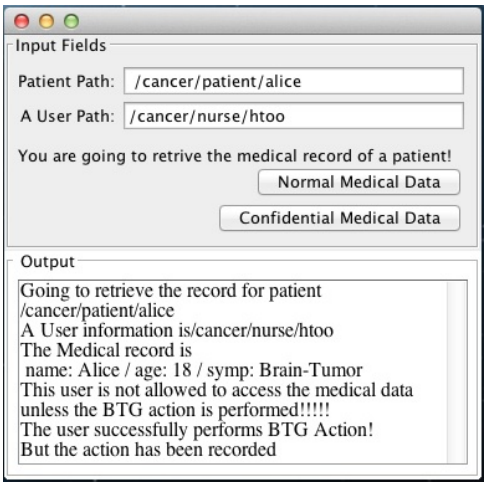

Fig. 4. User Interface for A Nurse

Different access policies are applied to a nurse. Figure 4 shows the interface of a nurse (Htoo). Based on Figure 4, the nurse can access the normal medical record of Alice but one obligation action is triggered and activated when the access is given. The nurse does not have access right regarding access to the confidential medical data unless the BTG policy is used to make an authorisation decision as in urgent and emergency circumstances. At the same time, obligations are triggered and activated. The management teams can check the audit log to prevent and detect security violations.

2) BTG Interface: We developed these simple interfaces for the BTG action. When a nurse wants to perform a BTG action

to access patients' confidential data, the BTG interface will appear. The user's attempt to gain access will be notified to the user and his/her management team and necessary actions will be taken for security. The confirmation message will appear twice before the access is given to the nurse. The interfaces for BTG action are shown in Figure 5.

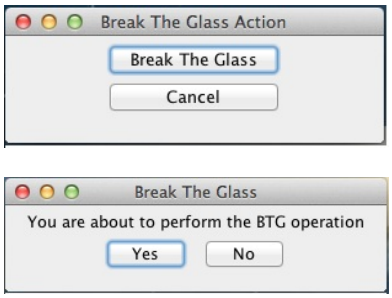

Fig. 5. Interfaces for BTG

3) Audit Log Interface: We developed the audit framework based on managed objects in Ponder2 package. The interface of an audit log can be seen in Figure 6. This Figure shows what kind of information and data are stored in the audit log. The first audit log shows that the nurse accessed the normal medical record of Alice. For the second log, the same nurse requested access to the confidential medical record by performing the BTG action and his or her access was granted. A doctor, who accessed a confidential medical record, was granted access as can be seen in the audit log of that patient. All the access requests to the medical records are recorded in which everyday is determine by the user' role. Based on the audit log, the management teams can check which users performed the BTG action and who among these will be granted access to the confidential medical records.

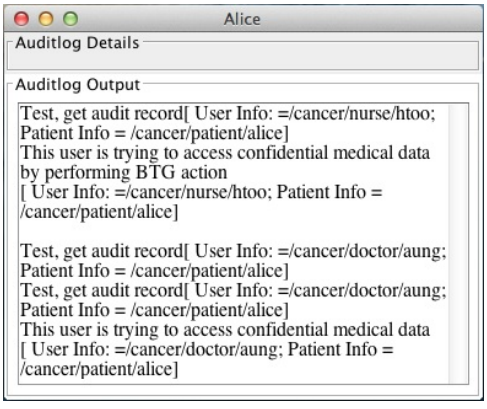

Fig. 6. Interface for Audit Log

B. Summary

Based on the evaluation results with a medical scenario, the BTG-RBAC model proposed by Ferreira et al [1] can be applied for medical data in WSNs after the framework and several changes within the access control engine are made. The BTG-AC model provides flexibility of decision making processes regarding access to medical records. The three policies such as authorisation, BTG and obligation cooperate with each other to make decisions about data access in the emergency situations. Based on the overall outcomes, the BTG-AC model can be applied in BSN and WSNs.

VI. Conclusion and Future Work

The overall contributions of this paper are the design and development of BTG-AC model for medical data in WSNs. The concepts of BTG, prevention and detection mechanism, and obligation provide more flexible access than other current access control models in WSNs. The BTG-AC model has been developed under Ponder2 package. All the modules - access control module and prevention and detection module - have been found to cooperate together to make an access decision and recorded a users' accountability to illegitimate data usage from authorised users as well as excluding illegitimate users for data access. One possible weakness of BTG-AC is that the human decision is needed to predefine BTG policy for each object. We are considered to redesign the BTG-AC model based on that weakness as future work. In addition, we will plan to develop the BTG-AC model within the actual sensor nodes for medical applications in WSNs.

References

[1] A. Ferreira, D. Chadwick, P. Farinha, R. Correia, G. Zao, R. Chilro, and L. Antunes, "How to securely break into rbac: The btg-rbac model," in *Proceedings of the 2009 Annual Computer Security Applications Conference*, ser. ACSAC '09. Washington, DC, USA: IEEE Computer Society, 2009, pp. 23–31.

[2] 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.

[3] H. A. Maw, H. Xiao, B. Christianson, and J. A. Malcolm, "A survey of access control models in wireless sensor networks," *Journal of Sensor and Actuator Networks*, vol. 3, no. 2, pp. 150–180, 2014. [Online]. Available: http://www.mdpi.com/2224-2708/3/2/150

[4] S. Yu, K. Ren, and W. Lou, "Fdac: Toward fine-grained distributed data access control in wireless sensor networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 22, no. 4, pp. 673–686, Apr. 2011.

[5] 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.

[6] H. Maw, H. Xiao, and B. Christianson, "An adaptive access control model for medical data in wireless sensor networks," in *2013 IEEE 15th International Conference on e-Health Networking, Applications and Services (Healthcom) (IEEE Healthcom 2013)*, Lisbon, Portugal, Oct. 2013.

[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] A. Ferreira, R. Cruz-Correia, L. Antunes, P. Farinha, E. Oliveira-Palhares, D. W. Chadwick, and A. Costa-Pereira, "How to break access control in a controlled manner," in *Proceedings of the 19th IEEE Symposium on Computer-Based Medical Systems*, ser. CBMS '06. Washington, DC, USA: IEEE Computer Society, 2006, pp. 847–854.

[9] 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.

[10] V. Goyal, A. Sahai, O. Pandey, and B. Waters, "Attribute-based encryption for fine-grained access control for encrypted data," *Wireless Network, IEEE*, 2006.