BTG-AC: Break-the-Glass Access Control Model for Medical Data in Wireless Sensor Networks

Htoo Aung Maw, Hannan Xiao, Bruce Christianson, and James A. Malcolm

***Abstract*—Wireless sensor networks (WSNs) have recently attracted much interest in the research community because of their wide range of applications. An emerging application for WSNs involves their use in healthcare where they are generally termed wireless medical sensor networks. In a hospital, outfitting every patient with tiny, wearable, wireless vital sign sensors would allow doctors, nurses, and other caregivers to continuously monitor the state of their patients. In such a scenario, patients are expected to be treated in reasonable time, so an access control model is needed, which will provide both real-time access to comprehensive medical records and detect unauthorized access to sensitive data. In emergency situations, a doctor or nurse needs to access data immediately. The loss in data availability can result in further decline in the patient's condition or can even lead to death. Therefore, the availability of data is more important than any security concern in emergency situations. To address that research issue for medical data in WSNs, we propose the break-the-glass access control (BTG-AC) model that is a modified and redesigned version of the break-the-glass role-based access control (BTG-RBAC) model to address data availability issue and to detect the security policy violations from both authorized and unauthorized users. Several changes within the access control engine are made in BTG-RBAC in order to make the new BTG-AC to apply and fit in WSNs. This paper presents the detailed design and development of the BTG-AC model based on a healthcare scenario. The evaluation results show that the concepts of BTG, prevention and detection mechanism, and obligation provide more flexible access than other current access control models in WSNs. Additionally, we compare the BTG-AC model with an adaptive access control (A^2C) model, which has similar properties, for further evaluation. Alongside with the comparison, the advantages and disadvantages of BTG-AC over current WSN access control models are presented.**

***Index Terms*—Access control, authorization, availability, body sensor networks, privacy, security, wireless sensor networks.**

I. Introduction

WIRELESS sensor networks (WSNs) have attracted much interest in the research community because of their wide range of applications. An emerging application for WSNs involves their use in healthcare where they are generally termed as wireless medical sensor networks (WMSNs). In a hospital, outfitting patients with tiny, wearable, wireless vital sign sensors would allow doctors, nurses, and other caregivers to monitor continuously the state of their patients. More importantly, in an emergency scenario, the same technology would enable medics to care more effectively for large numbers of casualties.

There are numerous applications like medical, battlefield, and environment monitoring in WSNs and security issue is important for many of them. Li and Gong [1] pointed out that WSNs suffer from many constraints like limited energy supply, limited memory, and low computation capability that impose unique security challenges and make innovative approaches desirable. Security techniques in other wireless technologies cannot be applied directly in WSNs because of its unique characteristic. As a result, existing security mechanisms are inadequate, inefficient, and new security approaches are desirable for WSNs.

In the healthcare industry, patients are expected to be treated in reasonable time. Therefore, an access control model should provide real-time access to comprehensive medical records. In emergency situations, a doctor or nurse needs to access data immediately. Any loss in data availability can result in further decline in the patient's condition or can even lead to death. Therefore, the availability of data is more important than security concerns. The overwhelming urgency is to take care of the patient; however, the privacy and confidentiality of that patient's medical records cannot be neglected. Thus, careful consideration in defining flexible policy is required to solve the conflict between data privacy and data availability in this real-world application. Additionally, it should also detect unauthorized information release of patient medical records from both authorized and unauthorized users because security breaches can happen at any time.

Security policy violations in multiuser systems were categorized by Anderson [2] into three categories: unauthorized information release, unauthorized information modification, and unauthorized denial of use. It is difficult to address the above violations in an access control policy for the healthcare application because an overly "loose" policy might permit access to inappropriate users, but an overly "tight" policy might prevent access from the appropriate users. To solve the problem of defining a flexible policy, we need a flexible approach in the access control engines to address all the possible access conditions.

The aim of this paper is to present new ways to provide a flexible approach to access control engine in WSNs and WMSNs. In addition, the other main issues we study concern the enforcement of access permissions dynamically across healthcare organizations. They are:

1) Who is designated to get access in emergency situations?
2) What happens after a restricted access is granted or not granted?

Manuscript received February 16, 2015; revised June 30, 2015 and October 14, 2015; accepted December 3, 2015. Date of publication; date of current version.

The authors are with the School of Computer Science, University of Hertfordshire, Hatfield AL10 9AB, U.K. (e-mail: h.maw@herts.ac.uk; h.xiao@herts.ac.uk; b.christianson@herts.ac.uk; j.a.malcolm@herts.ac.uk).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/JBHI.2015.2510403

[1]A restricted access means a data access request to sensitive or confidential data.

Let us consider the following example from a healthcare application to clarify the issues we aim to address in this paper. Alice is a doctor who takes care of a patient named Bob. Alice can access Bob's medical record but when she is away from work for some particular reason, such as sickness or on holiday, who has the right to access Bob's medical records in order to evaluate and treat him appropriately? Data availability is important: another doctor may need to access Bob's medical records to evaluate and treat his sickness. The healthcare system can provide data availability without security considerations but when patients are celebrities or high-profile people, how can we control and manage the privacy of these patients? The assumption is made that Bob is a celebrity who is in an emergency situation and Alice is not available at that time. The problem is who else has a designated access to Bob's medical records to give an effective treatment? Can other doctors or nurses from the emergency ward access Bob's medical record? If we consider the sickness of the patient, data availability is needed to give timely treatment, but what about the privacy of patient's medical record and information?

In the healthcare industry, the assumption cannot be made that all the users are trustworthy enough to access data even in emergency situations because security breaches can happen at any time due to inappropriate usage. Additionally, a prevention and detection mechanism is needed to detect security policy violations and to take courses of action for any access especially when a restricted access is granted or not granted. The question is: How can we design an access control model to provide privacy, confidentiality and availability at the same time?

To address the above issue, the break-the-glass role-based access control (BTG-RBAC) model [3], [4] proposed by Ferreira *et al.* is considered to apply in WSNs. The main reason of choosing the BTG-RBAC over other access control models is that it can address the conflict between data availability and data privacy in WSNs. The BTG-RBAC model is implemented in PREMIS [5] with MySQL [6] database, but it is not suitable to use in WSNs because PREMIS must be supplemented by metadata that can record detailed technical attributes of specific object types or media and hardware, and it is difficult to automate creation of metadata structures at present. Therefore, a modified version of BTG-RBAC is developed and implemented in order to fit in WSNs namely a break-the-glass access control (BTG-AC) model.

The main difference is that the BTG-AC model is developed and implemented within the Ponder2 policy package to reduce memory and storage space by using the BTG policy for emergency and unexpected situations instead of defining access control policies for all situations in advance. Regarding limited resource and storage, the sensor nodes cannot store all the possibility of access control policies in practice. Therefore, the main contribution of this paper is the design and development of a lightweight BTG-AC model that considers the limited resource and storage by applying BTG concept for unexpected and emergency situations. In addition, the proposed model also addresses the conflict between data privacy and data availability issue and to detect the security policy violations from both authorized and unauthorized users in healthcare application.

The remaining structure of this paper is explained as follows. Section II presents the related work. Section III discusses an overview of the BTG-AC model for WSNs. The development and implementation of the BTG-AC model in Ponder2 framework [7] can be seen in Section IV. Section V evaluates BTG-AC based on a medical scenario. Section VI presents the frameworks of the adaptive access control (A^2C) model which was proposed by Maw *et al.* [8] to make a comparison with the proposed BTG-AC model in WSNs. Additionally, this section reviews the advantages and disadvantages of BTG-AC over current WSN access control models. Section VII concludes the paper with the suggestion for future work.

II. Related Work

Access control is a critical security service to prevent unauthorized access to 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.* [9] stated that a considerable number of access control models have been proposed for use in WSNs, though some of them are not yet implemented. The access control models such as trust and centrality-based access control model [10], Maerien's model [11], and Gaurkar's model [12] are aimed to prevent a malicious node from joining the sensor network.

The distributed PRIvacy-preserving aCCESS control (PRICCESS) protocol [13] 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 user groups in the network controller. For ACL, roles need to be predefined in advance based on RBAC. Garcia-Morchon *et al.* [14] 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. Instead they proposed the context-aware role-based access control (CA-RBAC) model [15] for WMSNs, in which an access control decision will be made based on the modular contextual information such as normal, emergency and critical, to ensure the users' safety. In this model, there is no prevention or detection mechanism and no verification process to check user's data access, when the critical situation occurs.

Yu *et al.* [16] proposed the fine-grained data access control (FDAC) model which is based on attribute-based encryption (ABE) [9]. The main idea of their approach is to provide fine-grained access control over sensor data and it is resilient against attacks such as user colluding and node compromising. However, their model is based on centralized approach because only the network controller can perform key management. If the network controller is compromised, there will be no security provisioning in the network, which is a single point of failure.

To avoid a single point of failure, Ruj *et al.* [17] proposed an access control scheme based on multiauthority ABE. 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.

Maw *et al.* [8], [14] proposed an A^2C model with privilege overriding and behavior monitoring to provide fine-grained access control for medical data in WSNs. In this model, no human effort is needed to override rules and policies because of the introduction of the users' behavior 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' behavior trust model is used to check the user's action, location, time, etc., but there is no detailed information about the behavior trust model. Without the behavior trust model, the access decisions cannot be made effectively.

Based on the above discussion, most of the current WSN access control models are based on traditional role-base access control (RBAC) model [18] to control data access based on roles and 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. The decision is binary: deny or permit access. The RBAC model has been widely accepted as a policy-based access control model but roles and policies need to be predefined before the system can make decisions. Some WSN access control models such as FDAC, A^2C, and Ruj's model used cryptographic methods for data storage and data access control but the systems still need to predefine attributes, roles, and policies before deployment. It is, however, difficult to determine in advance all the possible needs for access in real-world applications because there may be unexpected situations at any time.

There are many potential situations that cannot be defined in traditional RBAC and cryptography-based systems. For example, the roles and policies for emergency and unexpected situations cannot be defined in advance. When the system faces these kinds of situations, what will the system do? Does the system wait until the authorized user comes and logs in? Alternatively, in the medical scenario, does a nurse wait for a doctor who takes care of a patient, in order to retrieve that patient's medical record? In most of the emergency and urgent cases, the users cannot wait until someone comes in order to retrieve the necessary data. Given this, what is a possible method to provide a flexible approach in the access control engine? For real-world applications, the system needs to be flexible enough to make decisions regarding data access based on unusual situations in addition to normally defined situations.

Policy languages in support of emergency management have been already proposed for e-health application for wired and wireless networks in the literature. For instance, works [13], [19], [20], [21] use the concept of role-based access control with BTG policies to manage emergency situations in wireless networks but it cannot fulfill the requirements of real-world applications in WSNs because of the constraints such as limited power, resources, and memory shortage. Current WSN access control models that we explained in this section do not address the conflict between data privacy and data availability for emergency events and unanticipated events. Additionally, all of these models need to define access control policies in advance for both

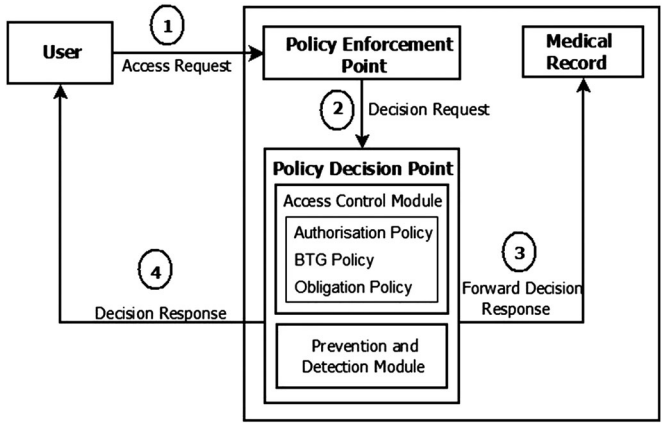

Fig. 1. Overview of BTG-AC.

expected and unexpected situations. In practice, it is very hard to define access control policy in advance. Therefore, a new BTG-AC model that considers the limited resource and storage by applying BTG concept for unexpected and emergency situations is proposed to provide a lightweight access control engine in sensor devices. Additionally, the BTG policy is introduced to provide a flexible policy to address the conflict between data availability and data privacy issue and to detect the security policy violations [2] such as unauthorized information release.

III. BTG-AC Model

The BTG-RBAC model proposed by Ferreira *et al.* [3] is considered to provide data availability in emergency situations and is also aimed at E-Health applications in general wireless and wired networks. Based on the limitations of WSNs such as memory size, CPU speed, battery life, network range, and changing connectivity, the BTG-RBAC model is not suitable to use in WSNs because it is implemented in PREMIS [5] with MySQL [6] database. Therefore, the BTG-RBAC model was modified and redesigned to function in WSNs; we call this BTG-AC, but it still has similar functions to those of the BTG-RBAC model. The main difference is that the BTG-AC model is developed and implemented within the Ponder2 policy package and it considers the requirements of WSNs.

Notwithstanding, an overview of BTG-AC can be seen in Fig. 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. The details of PEP and PDP are explained next.

A. Policy Enforcement Point

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 login process before forwarding request to PDP. In future, we will work on the implementation of the authentication service in PEP by using ABE [22].

B. Policy Decision Point

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—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.

1) Access Control Module: The access control module is used to enforce the policies for the decision-making process. In the access control module, there are three different policies, namely authorization, BTG, and obligation policy. These three policies are developed and designed under the access control module.

a) *Authorization policy:* An authorization 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 authorization policy, the subject, target, and action are checked to enforce the policy.
b) *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 administrator defines the BTG policy for each situation where users in an emergency situation require the BTG action.
c) *Obligation policy*: An obligation policy is used along with authorization 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. The obligation policy is linked with the prevention and detection module to store the user information and his access request as an audit log.

In normal access control models, the decision outcomes will be either permitted or denied access. If user's criteria satisfy 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. 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 follows:

1) (Permit, $\emptyset$) $\rightarrow$ A user has permission to access the targeted object.
2) (Permit, OBLGS) $\rightarrow$ A user is allowed to access the targeted object but an obligation is carried out when the access is given.
3) (Deny, $\emptyset$) $\rightarrow$ A user request to access the targeted object is denied.
4) (Deny, OBLGS) $\rightarrow$ Along side of a denied access, some obligations are performed.
5) (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 by extending the existing decision outcomes.

2) Prevention and Detection Module: The main idea of introducing a prevention and detection mechanism [23]–[25] is to protect the privacy and confidentiality of data by storing users' information, actions, etc., as an audit log for the purpose of detecting security violations. For an audit log to be usable, it should:

1) be available through a usable interface for the auditors or the administrators;
2) contain sufficiently detailed information to get a picture of what has happened.

Regarding the above facts, the audit log is to record the event and specify 1) when it occurred, 2) the user information associated with that event, and 3) the results of the decision-making process. An audit log can assist in detecting security violations and flaws in the system by detecting any suspicious access from users. In the audit log format, the subject is a user who tries to access a medical record from the targeted object with an authorization decision. In the audit log, the contextual information such as time and department are also recorded. The format of the audit record is shown as follows:

$$Auditlog := [Subject + Time + Target + Department + Decision\ Outcomes].$$

There are two different audit logs in the proposed model. These are the following.

1) *Access Log:* Every time a medical record is opened, an entry is created in the access log containing information about the users, the patient, and the document being accessed.
2) *Emergency Log:* An entry is created in this log whenever BTG operation is performed.

These two logs are stored as comma separated value (CSV) extension, so it can be easily checked and monitored by system administrators. Therefore, the prevention and detection module is used in the proposed model to keep a record of all the users access information as an audit log for detecting security policy violations.

IV. Development of The BTG-AC Model

Existing architectures for network and systems management are aimed at large-scale corporate environments, telecommunication networks, and do not cater for WSNs, although specific

techniques for policy-based management can be used to some degree. For WSNs, architectures are needed that scale down to small devices with local decision making. The limitations of WSNs such as memory size, CPU speed, battery life, network range, and changing connectivity require new techniques for optimizing resource usage and tailoring information within tight deadlines. Additionally, flexible techniques will be needed to filter information and perform access control, as well as defining and enforcing privacy. Therefore, the proposed BTG-AC model has been developed in Ponder2 [7] that is a popular lightweight policy language for BANs and WSNs.

Ponder2 has a high-level configuration and control language called PonderTalk and user-extensible managed objects that are programmed in Java. Ponder2 is implemented as self-managed cell (SMC) [26], which is a set of hardware and software components forming an administrative domain. An SMC manages a set of heterogeneous components (i.e., managed resources) such as those in body sensor network (BSN), WSN, or even a large-scale distributed application. Resource adapters are instantiated to provide a unified view for interaction with the resources as they may use different interfaces or communication protocols.

An SMC can load other components and services for detecting context changes, monitoring component behaviors, or for security (authentication and access control). However, the event bus, the policy service, and the discovery service work in conjunction with each other and form the core functionality of an SMC that must always be present. As most pervasive system are event driven, the services of a SMC interact using a common subscribe event bus, although we do not constrain all communication to be event based. The event bus can be used for both management and application data such as alarms indicating that threshold has been exceeded. The discovery service is used to discover new components which are capable of becoming members of the SMC, e.g., other SMCs in the vicinity.

The policy service implements a local feedback control loop to achieve adaption and self-management. It caters different types of policies, which specify what actions are permitted on which resources and services. The policy management is a main element that we modify and add extra function to develop a new access control model for BSN and WSNs. Therefore, Ponder2 is capable of self-management. The proposed model is implemented in the Ponder2 policy language. In practice, we envisage that sensor devices or nodes will be too primitive to run their own management agent, but will be capable of being managed by an external cell, such as a mobile phone, over a wireless link, such as bluetooth.

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 authorization, 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 are presented as follows.

A. Authorization Policy

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

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

The above authorization 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 authorization 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. BTG Policy

A BTG policy provides 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 authorization and BTG policies to prevent unauthorized 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 what is a course of action that 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 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 authorization, BTG, and obligation can be defined in Ponder2 for medical data

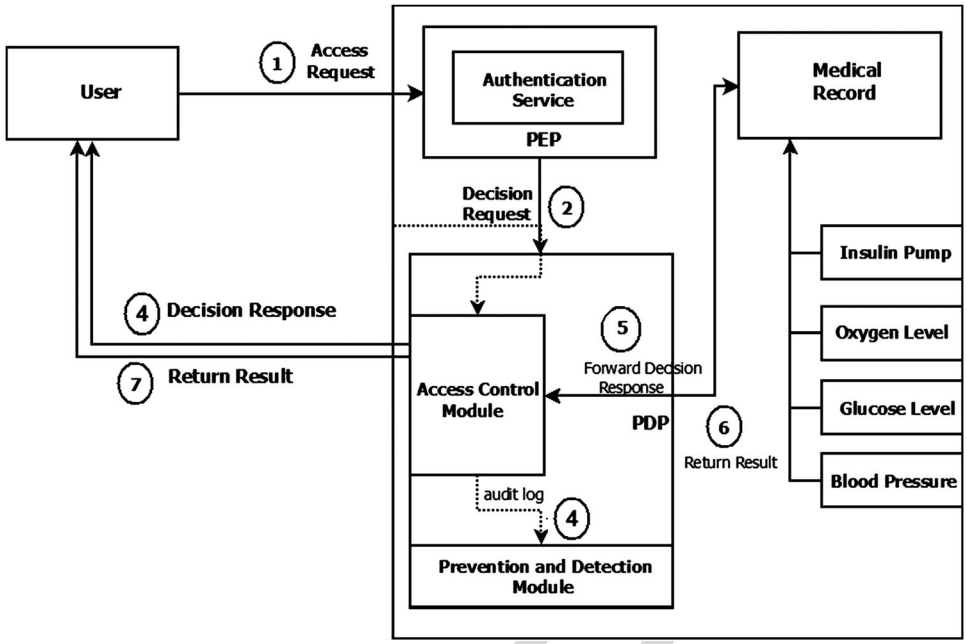

Fig. 2. Overview of BTG-AC with medical application in BSN.

in WSNs. The audit log is kept as CSV extension in the BTG-AC model. The BTG-AC model considers to reduce storage space by an introduction of BTG policy in Ponder2 for WSNs. 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 BTG-AC Model

Sensor devices have limited computational capabilities and strict power consumption requirements. Their operation must, therefore, be optimized and must constantly adapt in order to minimize resource consumption. Users are by and large not technically knowledgeable, and user interaction must be minimized. Policy-based approaches are particularly suited to WSN's application as they offer simple, flexible, and dynamic technique for implementing adaptation. Therefore, the proposed BTG-AC is evaluated by developing a medical scenario in Ponder2.

A. Evaluation Scenario

A medical application is developed to show how the proposed model is fit and how the policy evaluation is done for decision-making processes. It was developed under the Ponder2 package to evaluate the BTG-AC model for BSNs and WMSNs. We assumed that an SMC [26] that manages a set of heterogeneous components (i.e., managed resources, policy management, context awareness, etc.) such as those in a BSN network is represented as a wearable sensor node. In practice, the high-end sensor nodes are considered to use. 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 BSNs. Users such as doctors and nurses were trying to access the medical record of the patients via mobile, personal digital assistant (PDA), or personal computer. For example, interactions with BSN nodes occur via IEEE 802.15.4 wireless links, while interactions with PDAs or mobile phones. Each SMC had managed its own policy. These policies were specified and could be performed by each SMC.

Fig. 2 expresses the overview diagram of how to apply the BTG-AC model in healthcare applications for BSNs and WMSNs. Based on Fig. 2, the step-by-step process of user access to the targeted object is explained as follows.

1) A user sends an access request to the targeted object in the system.
2) PEP authenticates the user. Simultaneously, it sends a decision request to PDP for decisions regarding data access.
3) PDP calls the access control engine and passes through the details (such as the requested operation, the targeted object, and the contextual information) to make decisions regarding data access.
4) The access control engine returns permitted access or permitted access with obligation or permitted access with BTGs and obligation (or denied access or denied access with overriding and obligation, in which case a denied message is sent from PDP to the user and the request terminates here).
5) PDP forwards the decision response to the targeted object.
6) The targeted object returns the results.
7) PDP returns the results to the user.

The following policies in Table I are identified and developed to evaluate the proposed model. In a medical scenario, there are two different types of data for each patient: confidential medical records (ob_1) and normal medical records (ob_2). The access policies for users' access to these medical records will be different based on the access privileges and roles of the users. In addition, different security levels are required in these medical

TABLE I
EXAMPLE OF BTG-RBAC POLICY

Policy	Role	Operation	Object	BTG State	Obligations
1	Doctor	read	ob_2	N.A.	N.A.
2	Doctor	read	ob_1	N.A.	oblg [Write to Audit]
3	Nurse	read	ob_2	N.A.	oblg [Write to Audit]
4	Nurse	$O^{\mathrm{BTG(read)}}$	ob_1	TRUE	oblg [Notify Manager; Write to Audit; Reset BTG to FALSE]
5	Admin	$\mathrm{reset}^{\mathrm{BTG}}$	ob_1	N.A.	N.A.
6	Admin	read	log	N.A.	N.A.

records. 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.

In Table I, policy 1 states that the doctor is allowed to read the normal medical record, i.e., object 2 (ob_2). In policy 2, the doctor is allowed to access the confidential medical record (ob_1) but an obligation such as "Write to Audit" is activated. Policy 3 allows a nurse to read the normal medical record ob_2, but it will trigger one obligation "Write to Audit". In policy 4, the nurse is not permitted to access the confidential medical record (ob_1) unless he or she performs the BTG action in that object for emergency data access, but the BTG variable needs to be TRUE meaning that BTG is enabled. Therefore, an extra BTG role is needed for the nurse. Additionally, some obligations such as "Write to Audit", "notify to manager", and "rest BTG variable to FALSE after 30 mins". This implies BTG = TRUE. Policy 5 is quite simple. It allows resetting the BTG variable from FALSE to TRUE or TRUE to FALSE. For policy 6, the administrator can easily check the audit log to monitor any legitimate use from authorized users and to prevent any misuse from unauthorized users.

Policy 4 demonstrates that if policy 3 is allowed, the system will perform three obligations such as "write to audit," "notify to manager," and "reset BTG variable to FALSE after 30 min." This implies BTG = TRUE, FALSE. Policy 5 is quite simple. It is allowed to reset the BTG variable to FALSE to TRUE or TRUE to FALSE. For policy 6, r_5 allows a user to read ob_1, but it will trigger one obligation that is "write to audit." The administrator or manager can easily check the audit log to detect any use from authorized users and to prevent any use from unauthorized users.

B. Threat Model

The attacker-centric-based threat model [27] is respected and commonly used. Defence strategy is of course improved if there is a reasonable understanding of how attackers think. By thinking like attackers and being aware of their likely tactics, the system can be more effective when applying countermeasures. Several threats that can be faced in the applications can be categorized based on the goals of the attacks. Knowledge of these threats can help to organize a security strategy and might be able to help plan responses to these threats. In this section, the threat model is categorized based on STRIDE [28]. We analyzed the STRIDE model in the medical scenario as follows.

1) *Spoofing*: Spoofing is attempting to gain access to a system by using a false identity. This can be accomplished using stolen user credentials or false information. After the attacker successfully gains access as a legitimate user, elevation of privileges can begin. *Example:* A nurse pretends to be a doctor.
2) *Tampering*: Tampering is the unauthorized modification of data, but we did not address it explicitly in this dissertation. Same considerations apply to write as to read.
   Example: A nurse or doctor edits the medical record of a patient illegitimately.
3) *Repudiation*: Repudiation is the ability of users to deny that they performed specific actions. Without adequate auditing, repudiation attacks are difficult to prove. The issue of repudiation is concerned with a user denying that he performed an action. The defence mechanism is needed in place to ensure that all user activity can be tracked and recorded. Lack of auditing and logging of changes made to data threatens the ability to identify when changes were made and who made those changes.
   Example: A nurse denies that he has edited the medical record.
4) *Information disclosure*: Information disclosure is the unwanted exposure of private data. Sensitive data need to be stored securely to prevent a malicious user from gaining access to and reading the data. The disclosure of confidential data can occur when sensitive data can be viewed by unauthorized users. Only authenticated and authorized users should be able to access the data that is specific to them. Access to data should be restricted to users.
   Example: Other staff members from the hospital try to read the medical record.
5) *Denial of service*: Denial of service is the process of making system resources unavailable.
   Example: A common application layer DoS attack will send multiple simultaneous requests for data access. These requests will most likely put the access control module under DoS condition and the user will likely be unable to access the medical record.
6) *Elevation of privileges*: Elevation of privilege occurs when a user with limited privileges uses the identity of a privileged user to gain access to a data resource.

[2]A countermeasure is an action or technique that can reduce a threat and an attack by eliminating or preventing it.

TABLE II
POSSIBLE THREATS AND COUNTERMEASURES

Threat	Countermeasure
Spoofing	Strong Authentication (ABE)
Tampering	Strong Authorization (ABE and Access Control)
Repudiation	Audit Trials (Audit Record or Log)
Information Disclosure	ABE and Access Control
Denial of Service	Access Control
Elevation of Privilege	Access Control

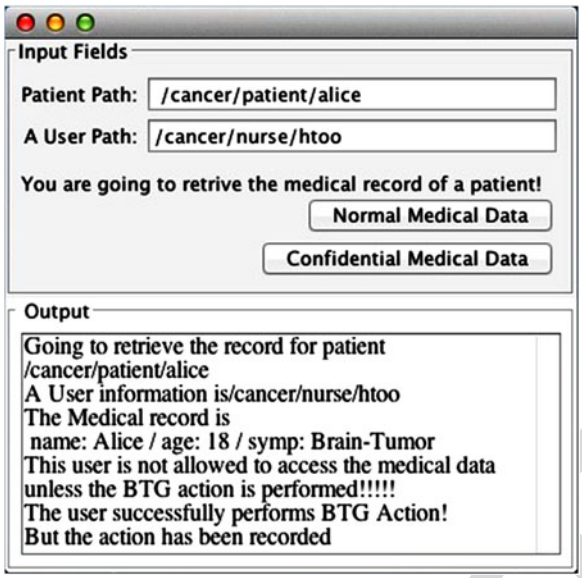

Fig. 3. User interface for a nurse.

Example: A nurse tries to access restricted data by using the fault identity.

Based on the above discussion, these threats and attacks are trying to violate the security services such as confidentiality, integrity, authenticity, repudiation, etc. These threats and attacks should be protected by using security mechanisms or countermeasures. A countermeasure is a safeguard that addresses a threat and mitigates risk. Table II lists the security threats that can violate the security services and the possible countermeasures to defend against them in the proposed BTG-AC model.

C. Evaluation Framework Based on Example Scenario

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

1) User Interface: To evaluate the BTG-AC model for medical data in WSNs, we developed the users' interfaces under Ponder2 package. Different access policies are applied to a nurse. Fig. 3 shows the interface of a nurse (Htoo). 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

Fig. 4. Interfaces for BTG.

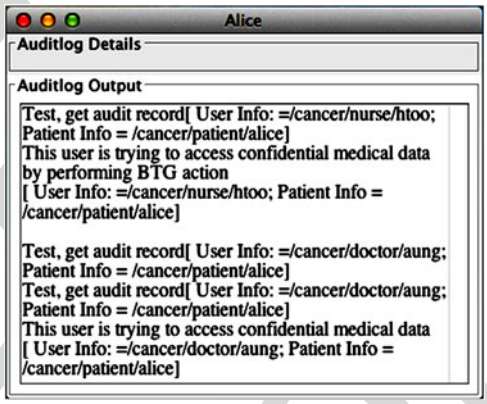

Fig. 5. Interface for audit log.

authorization decision 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: When a nurse wants to perform a BTG action to access patients' confidential data, a 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. The confirmation message will appear twice before the access is given to the nurse. Additionally, another simple authentication process is used to protect the privacy of patients' information by using normal log in process before the second confirmation box appears. The interfaces for BTG action are shown in Fig. 4.

3) Audit Log: We developed the audit framework based on managed objects in Ponder2 package. The interface of an audit log can be seen in Fig. 5. 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 be 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 every day is determined by the

TABLE III
CONCEPTS AND APPROACHES FOR A^2C AND BTG-AC

A^2C	BTG-AC
- Discretionary Overriding of Access Control	- Role-Based Access Control
- User Behavior Trust Model	- Break-The-Glass concept
- Prevention and Detection Mechanism	- Prevention and Detection Mechanism

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.

D. Summary

Based on the evaluation results with a medical scenario, the BTG-AC model 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 authorization, BTG and obligation cooperate with each other to make decisions about data access in the emergency situations.

VI. COMPARISON BETWEEN BTG-AC AND A^2C MODEL

To make a full comparison with the proposed BTG-AC model, an A^2C model is chose among current WSN access control model because it has similar properties as BTG-AC. As well, both models are developed in Ponder2 policy language. This section recapitulates both A^2C and BTG-AC models to make a comparison based on the evaluation criteria. First, the evaluation criteria are discussed for both A^2C and BTG-AC models. Additionally, a brief discussion of the A^2C model is explained. This is followed by an exploration of advantages and disadvantages of BTG-AC over current access control models in WSNs.

A. Evaluation Based on Features

In this section, the comparison of the A^2C and BTG-AC models is made based on the evaluation criteria including the network architecture model, the concepts and approaches, the decision outcomes, the access control policy and role, the data confidentiality and data privacy, and the data availability.

1) Network Architecture Model: Access control models can be different based on their network architecture model when the cryptographic keys, roles, policies, and attributes are distributed to users from the trusted authority or controller. The A^2C model is based on a distributed approach to make and adjust access decisions dynamically. This means that each sensor is deployed with the access control engine to make an effective local decision within itself based on the users' request and the sensor is required to store access policies. Unlike A^2C, the BTG-AC model is based on a centralized approach because each sensor node cannot store all the possible situations and BTG operations in the system. The disadvantage is that there might be a single point of failure in the BTG-AC model.

2) Concepts and Approaches: The A^2C and BTG-AC models use different concepts and approaches to fill the research gaps and the requirements of the application in WSNs. One similarity between these two WSN access control models is that both aim to provide data availability in emergency and unanticipated situations. An outline of the concepts and approaches for these two models can be seen in Table III.

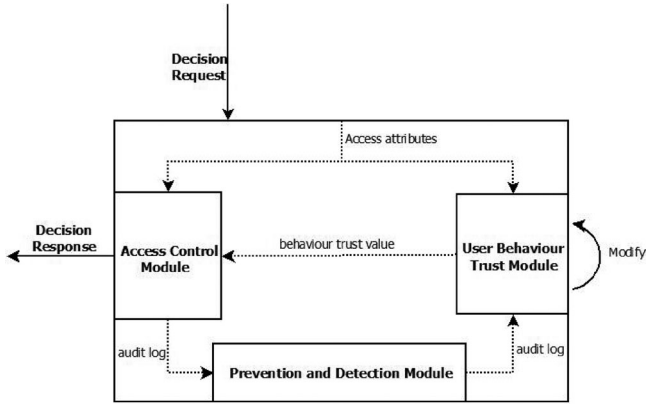

Fig. 6. Overview of A^2C.

The A^2C model was proposed by Maw *et al.* [14] to provide a flexible access decision in WSNs. This is incorporated the concept of possibility-with-override [29], [30] 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 A^2C model also uses user behavior monitoring and trust model to check users' actions, location, time, etc. Whenever users try to access data at the sensor nodes, all user behavior and users' information will be kept by prevention and detection mechanism as an audit record to detect and prevent abnormal and unauthorized access. The overview diagram of the A^2C model can be seen in Fig. 6.

The main difference between A^2C and BTG-AC models is that the user behavior trust module is introduced in PDP. Therefore, there are three modules inside PDP unlike BTG-AC (see Fig. 1). These modules are the access control module, prevention and detection module, and user behavior 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 behavior trust module. The user behavior trust module will calculate the trust value. To determine the user behavior trust value, the previous and current value of user behavior 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.

There is limited local decision-making capability in current WSN access control models because it is impossible to define the possibility of denied and permitted access for all situations, especially in WMSNs and WSNs. The A^2C model is based on the concept of discretionary overriding of access control by Rissanen *et al.* [29]. The system defines permitted and denied access policies for normal situations and leaves the possibility-with-override for emergency and unusual situations as the default to address the data availability issue. In the A^2C model, the behavior trust model is introduced to monitor the behavior information as well as to compare with previous and predefined users' behavior pattern. A prevention and detection mechanism

is used in both models to prevent the unauthorized information release and to detect security violations that can occur in the system anytime. The concepts of the A^2C model can provide both data availability and data privacy, but there is a lack of information for the behavior trust model.

Unlike A^2C, the BTG-AC model uses core RBAC with obligation and BTG concept to make decisions regarding access for emergency and unanticipated situations with details information for each components. The BTG-AC model needs predefined access roles and policies in advance for any situation. The authorization decision-making process is made within the core RBAC engine based on the inputs of the current section, the requested operation, and the target object. The main idea of the BTG concept is to allow the users emergency and urgent access to the system when a normal authentication process does not perform or work perfectly. In BTG-AC, BTG action is based on predefined user accounts. The system is managed in a manner that can make data access available in emergency situations with minimum of human interactions.

The BTG approach can be easily applied in the existing architectures and systems. It is very useful for existing systems because it does not involve additional automated technology. It is intended to cover unanticipated and emergency situations and it should not be used as a replacement for a helpdesk. BTG-AC can make decisions regarding data access quickly without unreasonable administrative involvements and delays. When an emergency or BTG account is activated in the system, it can alert the security administrator for that event for auditing purposes. This means that the monitoring process is required as an extra checkpoint to detect security violations. The proposed approach is well suited for the emergency decision-making process, but after an emergency in which a BTG account has been used, that account has to be deleted or disabled to prevent a replay attack. Therefore, human interactions are still involved in the system. The advantage of the BTG-AC model is that it can provide data availability service in emergency situations with a certain level of prevention and detection.

3) Access Control Policy: In this section, the access control policies defined in both A^2C and BTG-AC are presented. Similar access control policies are used from both models to make an effective comparison.

Table IV shows how the access control policies are defined in the A^2C model for the same medical scenario in Section V. In policy 1, a doctor is allowed to read the normal medical record (ob_2) without obligation. In policy 2, the doctor is allowed to read 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. Therefore, the management teams can check the audit log to detect security breaches that can occur by the authorized users. This means that the stored data at the ob_2 is not as sensitive as ob_1. The roles and policies for other users such as nurses and other members of staff will be predefined differently. Policy 1 and policy 2 are the same in Table I for BTG-AC.

In policy 3, the nurse is not allowed to access the confidential data (ob_1) unless the associated user overrides the access policy for emergency data access, but some obligations will be activated. Based on policy 3, the users (U* represents the group of nurses) can override access policy. If he or she overrides based on policy 3, his or her behavior trust value will be lower than normal data access. Access will only granted to that user when his behavior trust value is great than three. Otherwise, his or her access to the confidential data will be denied. Policy 4 allows the nurse to access the normal medical data (ob_2); however, one obligation action is triggered. Policies 5 and 3 have a similar property. There is a chance for member of staff from hospital to access the normal medical record (ob_2), but they have to override access policy. The administrator or manager can easily check the audit log to detect illegitimate use from authorized users and to prevent legitimate use from unauthorized users.

The complete BTG-AC policy can be seen in Table I and discussion in Section V. The policy definitions for both A^2C and BTG-AC have a similar structure. The weakness of the BTG-AC model is that an additional role for a BTG policy is needed for each user to perform BTG operation and an additional account is needed for emergency access. As a constraint, the BTG role needs to be considered in advance and predefined before the system is running in real time.

4) Decision Outcomes: In both A^2C and BTG-AC models, the existing decision outcomes in current access control models such as permitted access and denied access are extended into five different outcomes. The decision outcomes for the BTG-AC model are already discussed in the previous section. For the A^2C model, the decision outcomes are extended because of the discretionary overriding process with the user behavior trust value and the prevention, and detection mechanism. These decision outcomes are explained as follows:

1) *Permitted access:* A user access request has been permitted.
2) *Denied access:* A user access request has been denied. The user is not allowed to access the resources.
3) *Permitted access with obligation:* A user access request has been permitted but an obligation is executed when data access is given to that user especially for important and confidential information.
4) *Permitted access with overriding and obligation:* A user does not have privilege to access the resources but his or her request will be granted if he or she overrides policy within some constraints. The obligation policies are activated when access is granted to the user.
5) *Denied access with overriding and obligation:* A user access will be denied, if he or she tries to override the policy and does not satisfy some thresholds from that policy. At the same time, the obligations such as write to audit, etc., will be performed.

Based on the above decision outcomes, it is clear that the introduction of different concepts and approached can provide a flexible approach in the access control engine by extending the decision outcomes. Both A^2C and BTG-AC models add a finer grained level of control in access control engine for emergency situations.

5) Data Availability and Data Privacy: Both the A^2C and BTG-AC models are designed for making access decisions dynamically and efficiently in emergency and unanticipated situations. In the A^2C model, the decisions regarding access can be evaluated and adjusted dynamically, based on policies such

TABLE IV
EXAMPLE OF DEFINED POLICY FOR THE A^2C MODEL

Policy	Subject	Role	Operation	Object	Override	Obligations
1	U_1	Doctor	read	ob_2	-	-
2	U_1	Doctor	read	ob_1	-	oblg [Write to Audit]
3	U_*	Nurse	$\mathrm{Override}^{(\mathrm{read})}$ (if T $>$ 3)	ob_1	Override	oblg [Notify Manager; Write to Audit; Trigger the alarm]
4	U_2	Nurse	read	ob_2	-	oblg [Write to Audit]
5	U_*	Staff	$\mathrm{Override}^{(\mathrm{read})}$ (if T $>$ 3)	ob_2	Override	oblg [Notify Manager; Write to Audit; Trigger the alarm]

TABLE V
COMPARISON OF THE BTG-AC MODEL WITH RELATED MODELS

Access Control Model	Network Architecture	Decision Outcomes	Data Availability	Prevention and Detection Mechanism
BTG-AC	Centralized	5	Yes	Yes
A^2C [8]	Distributed	5	Yes	Yes
FDAC [16]	Centralized	2	No	No
CA-RBAC [15]	Centralized	2	Yes	No
DFG-AC [17]	Distributed	2	No	No

as authorization, obligation and overriding. Especially, in emergency situations, the user behavior trust value and the overriding policy are used to adjust access decisions to provide data availability in emergency and unanticipated situations. BTG-AC has similar properties to the A^2C model, but human interaction is still needed to define for BTG operation; the BTG role also needs to be predefined in advance for emergency situations. Users need extra roles for breaking the glass for unexpected situations and need an additional emergency account to do so for unexpected and unanticipated situations. Another advantage of the BTG-AC model over the A^2C model is that a simple user log in process is used as an additional security provisioning to protect the privacy of the patient information.

6) Summary: A comparison of the BTG-AC model with related works are expressed in Table V based on the evaluation criteria but only current WSN access control models are compared. The centralized access control management is used in BTG-AC, FDAC, and CA-RBAC, but for A^2C and DFG-AC, the distributed access control management is used. The existing decision outcomes such as permitted access and denied access are extended in both BTG-AC and A^2C and these are only two models that address data availability issue and detect security policy violation by using the prevention and detection mechanism. Based on the above discussion, Ponder2 policy language is a popular policy language for resource limited devices such as sensor nodes. Therefore, we assumed that the BTG-AC model is developed in Ponder2 based on limitations and requirements of WSNs. Additionally, the BTG-AC model addressed to solve the conflict between data availability and data privacy by using BTG approach and ABE-based authentication process.

B. Advantages and Disadvantages over Current WSN Access Control Models

The highlights for the advantages and disadvantages of BTG-AC over current WSN access control models are explained here. The BTG-AC model can manage policy such as creating a new role and editing an existing role and it can be used easily in existing systems and architectures. This model can provide data availability in normally defined situations as well as emergency situations; however, in the BTG-AC model, the BTG state and account need to be opened and defined in advance for emergency access. The BTG-AC model can provide data availability with certain constraints and limitations. Additionally, the BTG-AC model can detect security violations in the systems by checking the audit record in the prevention and detection mechanism. The main contribution of the BTG-AC model is that data availability and data privacy can be provided in both defined situations, and some emergency situations for effective treatment of patients in the real-time environment.

Alongside with the advantages, there are some drawbacks in the proposed BTG-AC model. Data availability is provided in BTG-AC, but some limitations apply for data access in emergency situations. A system administrator needs to open an emergency account for users in advance for BTG operation and emergency access. In addition, the BTG or emergency account can be used one time only to prevent replay attacks. The user needs to reopen the emergency account for another attempt. If this is not done, the system administrator needs to open and activate the emergency account for all users. This means that some kinds of administration processes are needed in BTG-AC for emergency situations. The storage might be costly because an additional role is needed for each user to use a BTG account. An alternative way is to use data aggregator as centralized access management to reduce the storage space in actual sensor nodes.

VII. CONCLUSION AND FUTURE WORK

The overall contributions of this paper is the design and development of a lightweight BTG-AC model that considers to reduce storage space for medical data in WSNs to address the data availability issue and to detect the security policy violations from both authorized and unauthorized users. The concepts of BTG, prevention and detection mechanism, and obligation provide more flexible access than other current WSN access control models. 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 to make access decisions and record a users' accountability to detect security violations from authorized users. Additionally, the A^2C framework, which has similar properties as BTG-AC, is briefly discussed to make a meaningful comparison with BTG-AC. One possible weakness of BTG-AC is that the human decision is needed to predefine BTG policy for each object. We

are considering to redesign the BTG-AC model to overcome that weakness in future work. We plan to develop the BTG-AC model within the actual sensor nodes for medical applications in WSNs. In addition, we will work on the implementation of the authentication service by using ABE.

REFERENCES

[1] Z. Li and G. Gong. (2008). "A survey on security in wireless sensor networks," University of Waterloo. [Online]. Available: http://cacr.uwaterloo.ca/techreports/2008/cacr2008-20.pdf.

[2] J. Anderson, "Information in a multi-user computer environment," *Adv. Comput.*, vol. 12, pp. 1–36, 1972.

[3] 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 *Proc. Annu. Comput. Security Appl. Conf.*, 2009, pp. 23–31.

[4] 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 *Proc. 19th IEEE Symp. Comput.-Based Med. Syst.*, 2006, pp. 847–854.

[5] PREMIS. (2015, June). "Premis data dictionary for preservation metadata, version 3.0. [Online]. Available: http://www.loc.gov/standards/premis/v3/premis-3-0-final.pdf

[6] M. Widenius and D. Axmark, *Mysql Reference Manual*, 1st ed. Sebastopol, CA, USA: O'Reilly & Associates, Inc., 2002.

[7] K. Twidle, E. Lupu, N. Dulay, and M. Sloman, "Ponder2—A policy environment for autonomous pervasive systems," in *Proc. IEEE Workshop Policies Distrib. Syst. Netw.*, 2008, pp. 245–246.

[8] H. Maw, H. Xiao, and B. Christianson, "An adaptive access control model for medical data in wireless sensor networks," presented at the IEEE 15th Int. Conf. e-Health Netw., Appl. Services, Lisbon, Portugal, Oct. 2013.

[9] H. A. Maw, H. Xiao, B. Christianson, and J. A. Malcolm, "A survey of access control models in wireless sensor networks," *J. Sensor Actuator Netw.*, vol. 3, no. 2, pp. 150–180, 2014.

[10] J. Duan, D. Gao, C. H. Foh, and H. Zhang, "TC-BAC: A trust and centrality degree based access control model in wireless sensor networks," *Ad Hoc Netw.*, vol. 11, no. 8, pp. 2675–2692, Nov. 2013.

[11] J. Maerien, S. Michiels, C. Huygens, D. Hughes, and W. Joosen, " Access control in multi-party wireless sensor networks," in *Wireless Sensor Networks* (ser. Lecture Notes in Computer Science), vol. 7772, P. Demeester, I. Moerman, and A. Terzis, Eds. Berlin, Germany: Springer, 2013, pp. 34–49.

[12] S. Gaurkar and P. K. Ingole, "Access control and intrusion detection for security in wireless sensor network," *Internal J. Sci. Technol. Res.*, vol. 16, no. 2, pp. 63–67, Jun. 2013.

[13] C. A. Ardagna, S. De Capitani Di Vimercati, S. Foresti, and Grandison,, "Access control for smarter healthcare using policy spaces," *Comput. Security*, vol. 29, no. 8, pp. 848–858, 2010.

[14] H. A. Maw, H. Xiao, and B. Christianson, "An adaptive access control model with privileges overriding and behaviour monitoring in wireless sensor networks," presented at the 8th ACM Int. Symp. QoS Security Wireless Mobile Netw., Paphos, Cyprus, Oct. 2012.

[15] O. Garcia-Morchon and K. Wehrle, "Modular context-aware access control for medical sensor networks," in *Proc. 15th ACM Symp. Access Control Models Technol.*, 2010, pp. 129–138.

[16] 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.

[17] S. Ruj, A. Nayak, and I. Stojmenovic, "Distributed fine-grained access control in wireless sensor networks," in *Proc. IEEE Int. Parallel Distrib. Process. Symp.*, 2011, pp. 352–362.

[18] G. Zhao and D. W. Chadwick, "On the modeling of Bell-LaPadula security policies using RBAC," in *Proc. IEEE 17th Workshop Enabling Technol.: Infrastructure Collaborative Enterprises*, 2008, pp. 257–262.

[19] A. D. Brucker and H. Petritsch, "Extending access control models with break-glass," in *Proc. 14th ACM Symp. Access Control Models Technol.*, 2009, pp. 197–206.

[20] B. Carminati, E. Ferrari, and M. Guglielmi, "Secure information sharing on support of emergency management," in *Proc. IEEE 3rd Int. Conf. Privacy, Security, Risk Trust/IEEE 3rd Int. Conf. Soc. Comput.*, Oct. 2011, pp. 988–995.

[21] S. Marinovic, R. Craven, J. Ma, and N. Dulay, "Rumpole: A flexible break-glass access control model," in *Proc. 16th ACM Symp. Access Control Models Technol.*, 2011, pp. 73–82.

[22] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control for encrypted data, in *Proceedings of the 13th ACM Conference on Computer and Communications Security*, ser. CCS '06. New York, NY, USA: ACM, 2006, pp. 89–98. [Online]. Available: http://doi.acm.org/10.1145/1180405.1180418

[23] J. Blocki, N. Christin, A. Datta, and A. Sinha, "Audit mechanisms for privacy protection in healthcare environments," in *Proc. 2nd USENIX Conf. Health Security Privacy*, 2011, p. 10.

[24] E. Bertino and G. Ghinita, "Towards mechanisms for detection and prevention of data exfiltration by insiders: Keynote talk paper," in *Proc. 6th ACM Symp. Inf., Comput. Commun. Security*, 2011, pp. 10–19.

[25] L. Rostad and O. Edsberg, "A study of access control requirements for healthcare systems based on audit trails from access logs," in *Proc. 22nd Annu. Comput. Security Appl. Conf.*, Dec. 2006, pp. 175–186.

[26] 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," *Concurrency Comput.: Practics Exp.*, vol. 20, no. 3, pp. 277–295, Mar. 2008.

[27] D. Mirembe and M. Muyeba, "Threat modeling revisited: Improving expressiveness of attack," in *Proc. 2nd UKSIM Eur. Symp. Comput. Modeling Simul.*, 2008, pp. 93–98.

[28] J. Meier, A. Mackman, M. Dunner, S. Vasireddy, R. Escamillia, and A. Murukan. (2008, June). "Improving web application security: Threats and countermeasures," *Microsoft Corporation*. [Online]. Available: https://msdn.microsoft.com/en-us/library/ff648641.aspx

[29] E. Rissanen, B. Firozabadi, and M. Sergot, " Towards a mechanism for discretionary overriding of access control," in *Security Protocols* (ser. Lecture Notes in Computer Science), vol. 3957, B. Christianson, B. Crispo, J. Malcolm, and M. Roe, Eds. Berlin, Germany: Springer, 2006, pp. 312–319.

[30] R. Sandhu and Q. Munawer, "How to do discretionary access control using roles," in *Proc. 3rd ACM Workshop Role-Based Access Control*, 1998, pp. 47–54.

Htoo Aung Maw received the BCSc degree in computer science from University of Computer Studies (Yangon), Yangon, Myanmar, and the B.Sc. degree in computer science from Northumbria University, Newcastle upon Tyne, U.K. He received the M.Sc. and Ph.D. degrees in computer science from the University of Hertfordshire, Hatfield, U.K., in 2011 and 2015.

His research interests include security protocols, cyber security, and user behavior trust.

Hannan Xiao received the Ph.D. degree in electrical and computer engineering from the National University of Singapore, Singapore, in 2003, and the B.Eng. and M.Eng. degrees in electronics and information system engineering from the Huazhong University of Science & Technology, Hubei, China.

She has been with the University of Hertfordshire as a Lecturer since 2003. She proposed and developed one of the first Quality of Service models for mobile ad hoc networks (FQMM) which has been well cited in the literature. She has been actively involved in research and development in several areas of distributed systems and security.

Bruce Christianson received the B.Sc. and M.Sc. degrees in mathematics from the Victoria University of Wellington, Wellington, New Zealand, in 1978 and 1980, and the D.Phil. degree in mathematics from the University of Oxford, Oxford, U.K., in 1984.

He joined the University of Hertfordshire (then the Hatfield Polytechnic) in 1987 and has been Professor of Informatics since 1997. His research interests include security protocol design and the epistemology of trust.

Prof. Christianson is a Fellow of the New Zealand Mathematical Society.

James A. Malcolm's photograph and biography not available at the time of publication.