CHAPTER – 5

Emergency Aware, Non-invasive, Personalized Access Control Framework for IMDs

Contribution

This chapter provides justification for the belief that during emergency condition if fail-open security is provided, it increases the security risks. It extends the CAAC [98] Access Control model for providing controlled access to IMDs during emergency situation. The access control logic is placed on a trusted external device like PDA or cell phone which can be carried easily by the patient.

5.1. Introduction

Emergency medical staff may need immediate access to patient data [16]. The security solution requires a fail open access in order to make IMD accessible during emergencies to the health care providers who lack credentials. Fail Open access is granted bypassing all security techniques. This feature introduces a new vulnerability as the patient is feeble and complete removal of security may be dangerous for the safety of the patient. A solution is provided to provision fine grained Access Control which also incorporates emergency condition. Personalized Emergency Aware role based Access Control (EAAC) framework which can work in collaboration with Authentication and Encryption mechanisms to provide a strong security solution.

Access Control is a security mechanism which restricts the actions of a legitimate entity on a given resource object [99]. Due to resource constraints in IMD, we place the Access Control logic onto a handheld device like a cell phone or PDA belonging to the patient. Access Control in normal scenarios can follow standard pre-defined Access Control policies such as Role-Based Access Control defined in (or used in) [28]. However, during emergency scenarios, such Access Control policies may prevent an unregistered practitioner to access the patient's IMD for administering emergency treatment. In conditions of emergency, Access Control policies need to be modified dynamically to allow prompt access and quick treatment. But such changes should be temporary and

regular policies should be reinstated once the emergency is over. The Access Control framework should not only prevent unauthorized access to the IMD but should also be sensitive to critical cases which may run to an Emergency. Criticality Aware Access Control (CAAC) [98] framework for specifying Access Control policies is extended to control access to IMDs with automated operation during emergencies. Such framework requires continuous monitoring of context, authentication and application of Access Control policy. Therefore, instead of placing the service on the IMD itself, we propose to put it on an external proxy device. This is also useful when a patient has multiple IMDs installed, a centralized rechargeable proxy can manage secure access. PDA or cell phone which has an Internet access can be used as a proxy device. This helps in reducing resource consumption of IMD. During normal scenarios, Proxy Device performs Role Based Access Control and in emergency scenarios if registered practitioner is not available, Proxy device gets connected to its localized, Virtual Space to give emergency access to another medical practitioner by providing him with a temporary credential to access the Patient IMD for immediate treatment instead of failing open and giving access to everybody. During emergency this security scheme will provide Non-repudiation service which will ensure once an external device sends commands to IMD it cannot not deny doing so. A diagrammatic representation of the model is presented below:

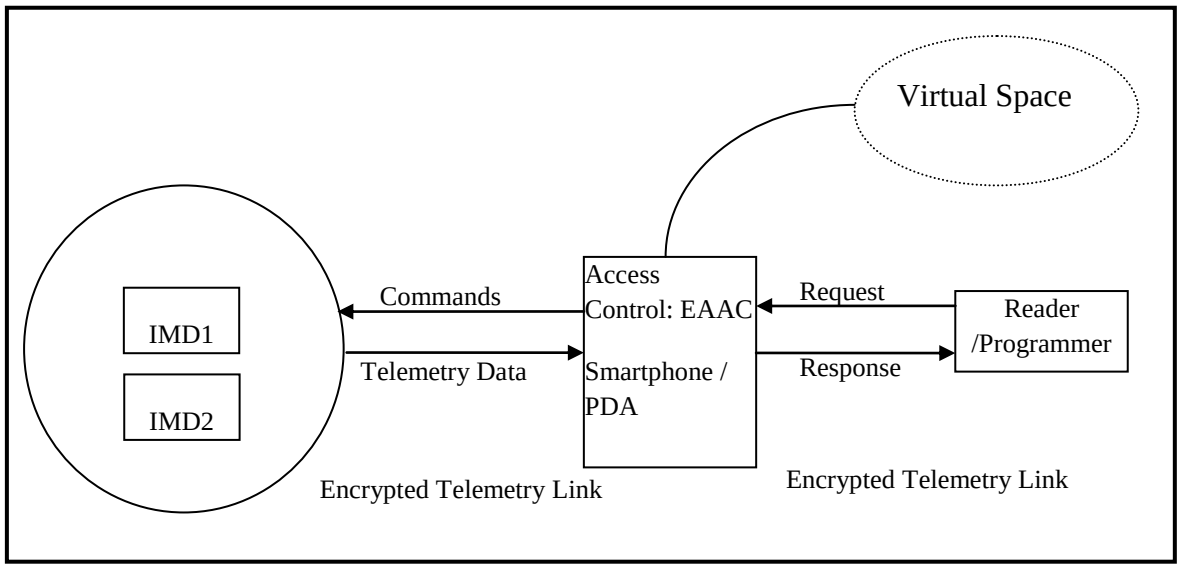

FIGURE 5.1 Block Diagram for Emergency Aware Access Control [124]

5.2. Threat Model for Fail Open Security

As discussed in [16], by bringing down the security to zero during emergencies means introducing vulnerability as IMD will communicate without using any cryptographic mechanism making the communication vulnerable to eavesdropping and alteration. This increases the risks of Insider and Outsider attacks like attacks on integrity, replay attacks, denial of service attacks. This can turn out to be a big loophole in the entire security framework and requires some amendment. This vulnerability may be exploited by an attacker by inducing false alarms to introduce a fake emergency situation and take control of the IMD.

5.2.1. Assumptions

As our concern is to provide Access Control, we assume a strong Authentication Mechanism available to authenticate user in Normal State similar to one suggested in chapter 7. We assume that Proxy device communicates with IMD via secure encrypted channel and it is capable of using an Internet connection to access Virtual Space which keeps a record of medical practitioners in proximity area of patient.

5.3. Security Mechanisms proposed to be Installed on Proxy Device

5.3.1. Authentication

For enforcing access control on IMD resources, external device needs to be authenticated first. During normal scenarios, authentication can be granted once authenticating party proves its legitimacy. This is typically brought into action by provisions like a password, or a physical key or biometrics like fingerprints, iris scan, signature and voice recognition or digital techniques (e-tokens, RFID, key fobs) [100]. Authentication is granted according to the principle of "least privilege", which withholds privilege unless need is established by a specific request, for example, even if a doctor(provider) logs in he should not be unanimously allowed to stop IMD as he may accidently do so. A user needs to be re-authenticated with high reliability to gain a new trust credential with aggravated trust level [100]. Authentication Service must reliably identify the user and issue a credential which can be subsequently used with every request for access that an external device makes, which is used by the Access Control Service to identify the requester [101]. Once assured that credentials are not tampered with or stolen, the Access Control system can reliably identify the requester.

5.3.2 Access Control

To ensure secure communication, an Access Control mechanism for IMD is a crucial need. A typical Access Control system consists of following entities [98]:

1. **Subject:** An entity like External Device that seeks access to a resource object like an IMD.
2. **Object:** An entity that is protected by the Access Control system for example an IMD.
3. **Permission:** It is the access right of a subject to access an object in controlled manner.
4. **Credentials:** It is a proof that subject possesses to prove its authenticity.

An emergency-aware Access Control model uses contextual information to provide controlled access to sensitive data of IMDs. Here we rely on the fact that during emergencies if IMD detects a weak pulse, low blood glucose, or if the patient is unconscious, IMD informs the proxy device immediately. In such circumstances, if authorized staff is not available in the vicinity, the proxy may switch from Normal to Emergency State of Access Control for patient safety.

Below given are the popular Access Control mechanisms along with discussion on the suitability of their application in provision of Access Control for IMDs.

5.3.2.1 Traditional rule based model

Discretionary Access Control (DAC) model makes use of Access Control Matrix (ACM) to store the access rights of each subject over a set of resource object [99]. It is a static solution where subjects and objects need to be pre-defined. Therefore additional constraints cannot be imposed easily. In Mandatory Access Control (MAC) model, access rights are determined by a central authority. It labels each resource object with a sensitivity level and each subject with a clearance level. In order to access a resource, subject must possess a valid clearance level. These models lack the dynamism and flexibility required for providing Access Control for wireless access of IMDs.

5.3.2.2 Role based access control model

In Role based access control model [102], subjects are assigned a role and access right are assigned to such roles. Subjects in the system are assigned roles when they register to the

system, and are allowed to access resources, based on the privileges associated with the assigned roles. Given a set of roles and privileges, RBAC maps subjects to roles and the roles to different sets of privileges. Even if administration and modification of the policies is easily achieved, this model fails in incorporating dynamic assess control as the mappings are static and not context aware. An authorization model based on semantic web technologies [103] which uses Common Information Model (CIM). For managing the authorization of resources, an authorization system should implement its semantics in a manner that they match with semantics of underlying data and resources to be protected. In [104] the RBAC model is extended to support more complex privacy-related policies, while considering features like purposes and obligations.

5.3.2.3 Context Aware Access Control Model

Context Aware Access Control Model (CA-RBAC) [105] extends RBAC model to incorporate context related data for controlling access to sensitive resource objects. While providing flexibility and dynamism, this scheme depends on combination of role of the user, context information and state of the system. Similar to CA-RBAC, a dynamic context aware Access Control scheme for distributed healthcare applications was presented in [100].

5.3.2.4 Criticality Aware Access Control Model (CAAC)

Criticality Aware Access Control Model (CAAC): [98] responds to occurrences of critical event and changes Access Control policies autonomously. Criticality which is the measure of urgency required to handle a critical event. CAAC classify system context information into Critical and Noncritical. Critical context indicates the occurrence of a critical event which requires immediate action and noncritical contexts indicate normal operations and require no special action. Critical event allows adjustments in Access Control policies by including notification and logging, our Access Control draws inspiration from CAAC.

5.4 Proposed EAAC Architectural Framework

Our solution, Emergency Aware Access Control (EAAC) framework is designed for granting wireless access to one or more IMDs implanted on the Patient's body. Our proposal extends Criticality Aware Access Control [98] by incorporating a number of design choices specific to the IMD context and proposes its placement on a proxy device for personal security. Also we make use of virtual spaces to dynamically assign credentials

to medical practitioners to allow access of a patient's IMD during emergencies. Parts of our framework are as follows:

5.4.1 Role Management

Access rules for IMDs are delineated and assigned to a medical staff when he becomes a part of an IMD system of the patient by undergoing the process of registration and is established in his actual position and permissible activities. The primary task then is to assign well defined and unambiguous roles to subjects (medical staff) and providing them appropriate privileges based on their access rights.

Emergency aware role management is done by the help of a Web Service using which a medical practitioner can join a particular virtual space depending on his current location and can be contacted for providing emergency treatment to a patient bearing IMD is case of medical emergency when the registered medical practitioner with access privileges is unavailable. The privileges are, nevertheless, given to those who are authorized medical staff and are available within a limited distance from the place of exigency. Therefore system roles are a subset of space roles. The proxy on sensing a medical emergency, will access the virtual space by exhibiting the form of service required for the IMD and its placement to produce a list of doctors who are available in the vicinity. With a doctor's consent it will grant admittance to the IMD for a limited period as explained below to only a doctor and not to all. The physician will be provided credential and a complete access log will be stored in proxy for non-repudiation.

Context information [100] is helpful in modifying the Access Control policies to ensure IMD access and thus patient safety.

5.4.2 Emergency State Management

For Emergency State, following points are considered:

1. Emergency State requires autonomous changes in access policies if registered staff is unavailable.
2. All policy changes with respect to Emergency State are temporary and rolled back once emergency is over.

5.4.3 Emergency Management

Criticality is an amount of level of responsiveness required in taking corrective actions to curb the effects of a critical event and is used to find out the severity of critical events. To quantify this attribute, the term Window-of-Opportunity (Wo)[100] is introduced, which is defined as the maximum delay that is allowed to take corrective action after the IMD informs of a critical event and varies from application to application. Window-of-Opportunity = 0 indicates maximum criticality which leads to an emergency condition while a Window-of-Opportunity = ∞ indicates no criticality which means normal state of IMD and of patient Access Control policies.

Here, access policies are modified during the onset of a critical event in order to control the emergency in best possible manner. However completely diluting access control polities during critical events may introduce security concerns; therefore duration of relaxation of Access Control policies needs to be managed carefully. During a critical event, the Proxy implements a new set of access policies to facilitate prompt action. When the critical event is controlled and the patient is no longer in an emergency, the system restores to regular Access Control policies.

Criteria used for managing the Emergency mode: 1) the Window of opportunity Wo, 2) the time instant when the criticality is controlled T_{EOC} and 3) the time instant when all necessary actions to handle criticality has been taken (T_{EU}). The maximum duration for which the system can be in Emergency mode $T_{Emergency}$ is given by: $T_{Emergency}$ =min (Wo, T_{EU}, T_{EOC}). The Proxy determines the criticality level and on observing a critical event changes the access policies to Emergency-Aware and enters the Emergency State. It accesses the Virtual Space and provides credentials to one or more medical staff who are in the vicinity and agree to visit the patient, once emergency is over, then the system checks if it is in the EAAP - mode, if so, it returns the system to its Normal State and enforces the regular policies. Figure 2 below is a state transition diagram showing the Proxy States and Fig. 3 shows the Proxy architecture.

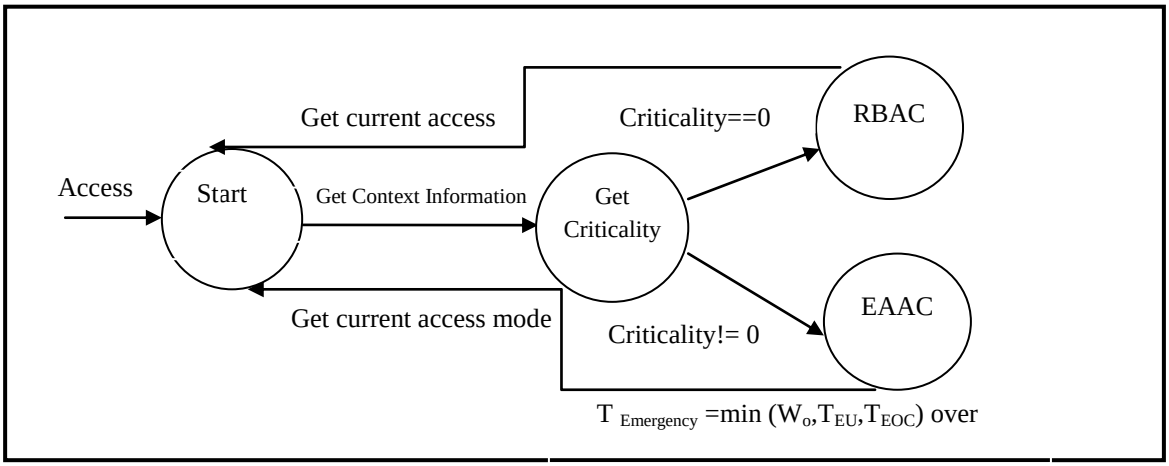

FIGURE 5.2 State Transition Diagram for Emergency Aware Access Control using Proxy Device [124]

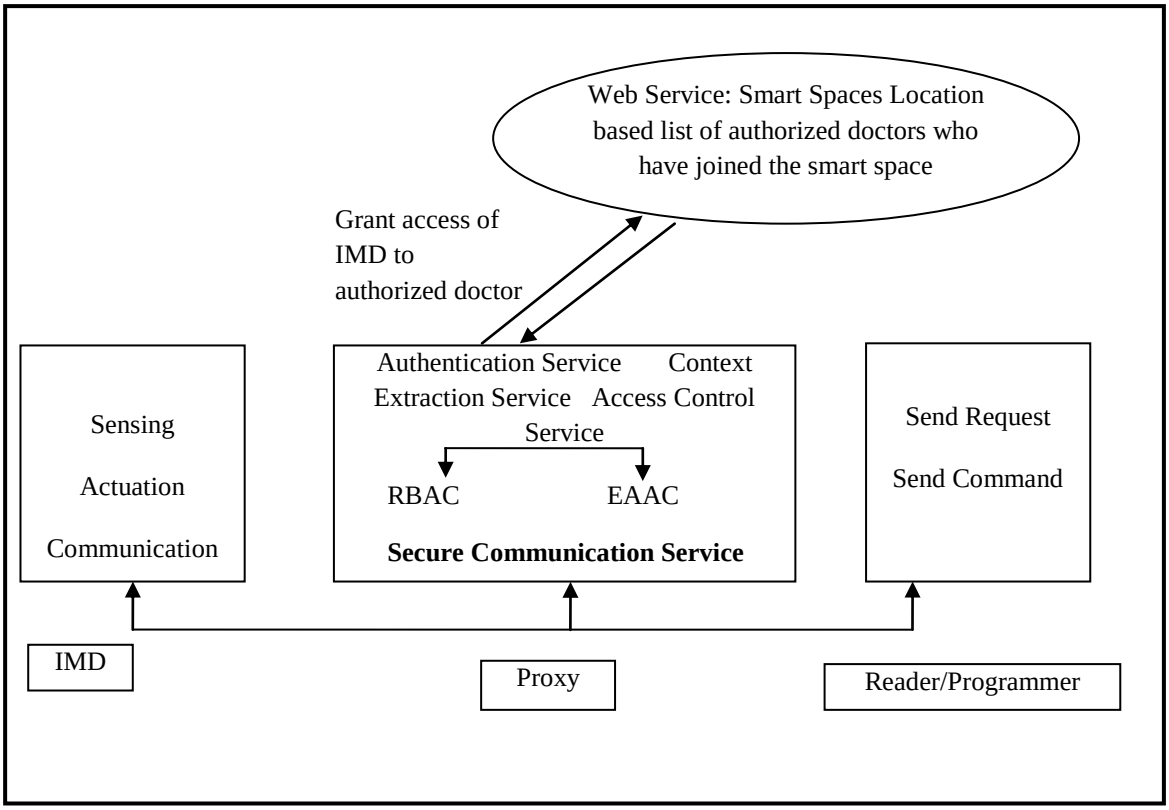

FIGURE 5.3 Proposed Proxy based Architecture [124]

The proxy implements RBAC [102] for Normal State and EAAC in Emergency State.

5.5 Conclusion

This system manages access control based on context information which allows it to provide controlled access during emergency which is beneficial for critical systems like IMDs.