NAIST-IS-DD0961212

Doctoral Dissertation

Secure Trans-organizational Role-Based Access Control for the Internet of Things

Ramon Francisco Mejia

August 16, 2012

Department of Information Processing
Graduate School of Information Science
Nara Institute of Science and Technology

A Doctoral Dissertation
submitted to Graduate School of Information Science,
Nara Institute of Science and Technology
in partial fulfillment of the requirements for the degree of
Doctor of ENGINEERING

Ramon Francisco Mejia

Thesis Committee:

Professor Hiroyuki Seki	(Supervisor)
Professor Kotaro Minato	(Co-supervisor)
Professor Toru Fujiwara	(Osaka University)
Associate Professor Yuichi Kaji	(Co-supervisor)

Secure Trans-organizational Role-Based Access Control for the Internet of Things[*]

Ramon Francisco Mejia

Abstract

The “Internet of Things” (IoT) describes a convergence of technologies where physical objects are interconnected through a computer network. The digital representation of objects are not limited to basic data of the object; roles are assigned to an object in order to naturally depict its properties in an expressive way. Role-Based Access Control (RBAC) is therefore suitable for securing IoT systems. However, this presents new challenges in RBAC for IoT systems, where there is a need to support access control in a trans-organizational way. In a straight-forward approach, a trusted third party facilitates the authentication of role assignments secured through a public-key infrastructure (PKI). But in a trans-organizational setting, involvement of a trusted third party in role authentication introduces performance issues due to the high volume and distributed nature of Auto-IDs. Consequently, this thesis investigates the development of a secure scheme for Trans-organizational RBAC (ToRBAC) in IoT systems.

Traditional RBAC models are designed for scalability in a single organization, and these models have been extended to support multiple organizations. However, an RBAC model which explicitly supports trans-organizational scenarios has yet to be studied. Chapter 2 proposes a ToRBAC model within and across organizational domains but does not require user-role assignment lists to be shared. First, a family of ToRBAC models are formally defined: its base model, models for role hierarchies and constraints, and finally a consolidated ToRBAC model. The proposed models have several properties that address aspects of trans-organizational

[*] Doctoral Dissertation, Department of Information Processing, Graduate School of Information Science, Nara Institute of Science and Technology, NAIST-IS-DD0961212, August 16, 2012.

use cases, namely role administration structures, standardized roles, and identification of liability. Moreover, it is shown that the rate of increase in management complexity of ToRBAC is smaller compared to traditional RBAC models as the number of users, roles and organizations increase.

Balancing the security and functionality of ToRBAC systems requires designing a secure scheme with flexible key management and representation of roles. Chapter 3 proposes a secure scheme for ToRBAC based on a Hierarchical Identity-Based Encryption (HIBE) mechanism. Components of the scheme which support the ToRBAC models are discussed. Analysis shows that the proposed role authentication protocol is secure against adaptive and nonadaptive chosen ciphertext attacks based proper constructions of HIBE, and modifies the protocol to add security properties such as message freshness, two-way authentication, and entity authentication. Furthermore, it is shown that the scheme offers advantages over PKI in implementing ToRBAC systems.

To implement the proposed scheme, two-dimensional monochrome (2D) barcodes must be able to store cryptographic keys. Chapter 4 investigates error control for 2D barcodes with increased data density. It is shown that the communication channel model defined by printing and scanning 2D barcode images can be modeled as an additive white Gaussian noise channel, with the variance $\sigma = 0.5637$. Then, a reference symbology for encoding and decoding high-density 2D barcodes was designed with low-density parity-check codes and symbol interleaving. Tests show that 2D barcodes with an image quality ≥ 11.176 dB are robust against errors introduced by the channel ($< 0.05\%$ bit-error ratio). It is also shown that the symbology adapts to the irregularities caused by printers, scanners, and physical damage.

Keywords:

Internet of Things, Role-Based Access Control, Hierarchical ID-based Encryption, Two-dimensional Barcodes, Low-Density Parity-Check Codes

List of Publications

Peer-reviewed Journal Paper

1. R. F. Mejia, Y. Kaji and H. Seki. Error control for high-density monochrome two-dimensional barcodes. *IPSJ Transactions on Databases.* 5(2):17-25. Information Processing Society of Japan, June 2012.

Peer-reviewed International Conferences

1. R. F. Mejia, Y. Kaji and H. Seki. Trans-organizational role-based access control (Poster). In *Proceedings of the 18th ACM Conference on Computer and Communications Security*, CCS 2011. pages 817–820. ACM, October 2011.

2. R. F. Mejia, Y. Kaji and H. Seki. Low-density Parity Check Codes for High-Density 2D Barcode Symbology. In *The Sixth International Multi-Conference on Computing in the Global Information Technology*, ICCGI 2011. pages 43–48, June 2011. (Best Paper Award)

Contents

List of Figures

List of Tables

1. Introduction

In the advent of cheaper and more reliable *Automatic Identification and Data Capture* (Auto-ID) technologies including barcodes, smart cards and RFID tags, common objects can now be tagged for identification and management using computer systems. Auto-IDs allow digital data to be distributed in many physical locations in an ubiquitous way. They are used in many applications where data sources need to be decentralized, such as health care [27], government [7], e-commerce [9] and other large-scale data management systems.

The "*Internet of Things*" or IoT refers to the networked interconnection of everyday objects. It is an emerging area with a vision to link real-world "things" or objects – human beings, physical or smart objects, and services – with the virtual world through Auto-IDs and scanning technologies. This represents a spatio-temporal connectivity between objects with virtual data and environments though a computer network [23]. It is similar to *Cyber Physical Systems* [12], in which sensor networks are its key technology for object interconnection. IoT systems are realized through a convergence of technologies to form a new IT infrastructure, as shown in Figure 1.

As shown in the figure, IoT systems are a *trans-organizational*. One organization can allow another organization to access "things" under their control. However, these organizations are independent of each other, and thus cannot share data about their role assignments. For example, consider a common supply chain scenario. A delivery company's logistics application tags grocery items with barcodes and RFIDs. Upon receipt, a supermarket's company's ERP application uses the same Auto-IDs to track and account for the items within their store. In this scenario, the tags are supplied and read by separate companies which do not explicitly exchange information about the objects. Note that this is different from a multi-organizational setup (e.g., federations), where organizations are required to share sensitive information.

Furthermore, IoT systems require many Auto-IDs to be attached on "things" the system keeps track of. These systems track a large amount of objects, thus Auto-IDs must be easily accessible for quick and efficient scanning through hand-held readers or sensor networks. On the other hand, Auto-IDs may contain sensitive information about the object. The flexible and accessible nature of

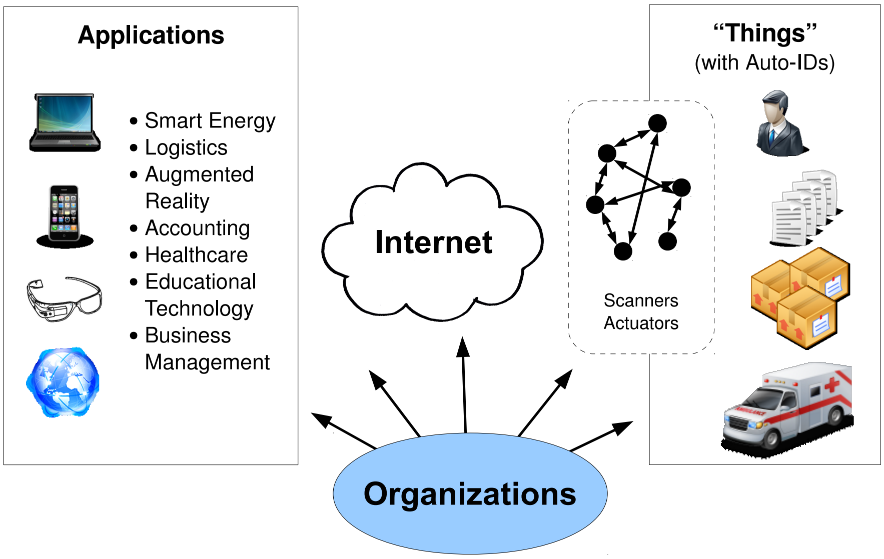


Figure 1. High-level infrastructure of the "Internet of Things".

Auto-IDs makes them susceptible to attacks by malicious users, and this has been regarded as a major issue in the adoption of IoT systems [25].

Another consideration is the capability of existing Auto-IDs to function under a secure scheme. While RFIDs remain a focal point in IoT research, 2D barcodes are a practical alternative to RFIDs in several applications. 2D barcodes must therefore be enhanced to accommodate the additional data overhead required to work with the secure scheme.

Therefore, one of the important aspects in an IoT system is to protect the privacy and confidentiality of existing Auto-ID technologies in trans-organizational settings. This thesis focuses on the following goals to address these issues:

1. Support trans-organizational use cases for IoT systems by extending *Role-Based Access Control* (RBAC) models.

2. Prevent unauthorized access to data stored in Auto-IDs by developing a security scheme using suitable cryptographic mechanisms.

3. Improve Auto-IDs – specifically *two-dimensional (2D) barcodes* – for storage of cryptographic keys and data needed for the security scheme.

Trans-organizational Role-Based Access Control

In information security, *access control* refers to features that manage user permissions to certain resources in a system. This protects the confidentiality, integrity and availability of those resources. “Things” in IoT systems can be treated as resources that require some form of access control each time a user tries to execute an action on the object. To facilitate this, objects are assigned with *roles* which naturally express their properties and capabilities. RBAC is then used as the management model for the objects and their roles. However, IoT systems must also be scalable since they can grow rapidly in terms of the number of objects, users or organizations. It is important to consider the management complexity of RBAC for IoT systems, as well as other issues that arise from its trans-organizational use cases.

A formal model for trans-organizational RBAC which supports IoT systems is presented in Chapter 2. First, an overview of trans-organizational use cases and their applications to IoT systems is presented to gain an appreciation of their benefits and challenges. The base model for traditional RBAC systems is then extended to support multiple organizations. A second model introduces role hierarchy constructions to the base model, which express natural relationships between roles in the real world. A third model then introduces constraints for the base model by setting rules on assignment relations to further control the integrity of an RBAC system. The final model combines all of these models, therefore having the ability to place constraints on role hierarchies. Finally, several properties of the model concerning management complexity and role administration are discussed.

Security Schemes for Trans-organizational RBAC

In implementing access control schemes for trans-organizational IoT systems, one must take into consideration some design decisions without significantly hindering its functionality, scalability or flexibility. For example, the task of data retrieval in an IoT system is decentralized, often distributed to offline terminals. This means we cannot deploy a scheme with conventional key authentication schemes because this would require an active connection to a trusted third party, thus affecting the efficiency of the data retrieval process. To find a balance between security and functionality, a security scheme for IoT systems should have the following properties:

- **Distributed Key Management**: IoT systems have deep role hierarchies, spanning many organizations, sub-systems and device domains. The scheme must be designed in such a way that the involvement of a trusted third party or certificate authority is minimized to avoid performance bottlenecks. This includes the key authentication protocol in data retrieval processes.

- **Dynamic Credentials**: There are cases where credentials for "things" are unknown at the time of encryption (e.g., a new user may wish to access data in Auto-IDs encrypted in the past). Thus, the system must be able to authenticate parties with credentials granted at different points in time.

- **Multi-Authority**: In trans-organizational applications, an Auto-ID may be accessible to users with roles issued by different organizations. The scheme must therefore be able to authenticate a key from an arbitrary authority.

- **Role Representation**: The scheme must use a flexible representation for roles that decreases the dependency on a trusted third party for certification. It should also be expressive, such that parties can exchange information about role in an unambiguous way.

Chapter 3 discusses a security scheme based on *Hierarchical ID-Based Encryption* (HIBE) for trans-organizational RBAC. The representation of trans-organizational roles using identity strings is defined, followed by protocols to setup the system, to register organizations and users, and to authenticate roles. The role authentication protocol of the scheme is then analyzed. It is shown that the protocol is secure to adaptive and non-adaptive chosen-ciphertext attacks over well-constructed bilinear groups of a HIBE scheme. Intruder models of challenge-response protocols are then described, and enhancements to role authentication that address the vulnerabilities are presented. Also, it is shown that the proposed scheme is more efficient compared to conventional public-key infrastructure schemes for trans-organizational systems.

High-Density Monochrome 2D Barcodes for IoT Systems

In data management systems, applications which use 2D barcodes mainly rely on its high data capacity (compared to 1D barcodes) and portability to provide better functionality. A printed barcode can also survive for a long time (possibly decades), even if no additional costs are paid for maintenance and conservation. Furthermore, 2D barcodes serve as a compliment to RFIDs in IoT systems because of their lower cost to print and distribute. Some examples are applications which require tags to be sent electronically (e.g., through email or fax), recyclable tags, and high-volume inventory (e.g., a batch is tagged with an RFID, but individual items are tagged with barcodes). People can also tag information to objects by using common printing devices. This is especially advantageous when we consider IoT systems in a home environment, where it is not realistic to assume that people have RFID readers and writers at home.

However, the data capacity of conventional 2D barcodes such as QR codes is around 2.9 kilobytes[1]. Due to the amount of data that maybe stored in tags (including its cryptographic overhead), this may limit the usefulness of 2D barcodes for IoT systems. Chapter 4 presents a novel 2D barcode symbology and error control techniques to increase the data density of 2D barcodes while retaining robustness against errors. The communication channel defined by high-density barcodes is studied, and the barcode is designed to convert the peculiar behavior of printing equipment to the well-studied model of additive white Gaussian (AWGN) model. The use of low-density parity check codes is also investigated, as they perform much better than conventional Reed-Solomon codes especially for AWGN channels. Through experimental evaluation, it is shown that the proposed error control techniques can be essential components in realizing high-density barcodes.

[1] QR codes by Denso Wave, Inc (http://www.qrcode.com/, last accessed: Jun 2012.)

2. Trans-organizational Role-Based Access Control Models

Traditional Role-Based Access Control models such as RBAC96 [20] and NIST-RBAC [6] are designed for use in a single organizational domain. However, the scope of IoT systems is very large in terms of the number of users, organizations, roles and permissions managed by a particular application. Use cases for access control are complicated, and are often not closed to one flat organization; sometimes, a role in one *identity-providing organization* (IdP) is referred by an independent *service-providing organization* (SP), and the role is granted with certain permissions by the SP. Management complexity and performance degradation of traditional RBAC mechanisms have therefore become problematic, and there is a need for more scalable access control models [11].

We say that an RBAC model is a *trans-organizational RBAC model* (ToR-BAC) if a) it can provide RBAC within and across organizational domains, and b) an SP can provide services to users who have roles managed by an IdP without knowledge of an IdPs role assignments. In general, an IdP assigns users with a *trans-organizational role* which serves as a role in the IdP's RBAC system. If an SP interprets the trans-organizational role as a valid role in their RBAC system, it grants permissions needed to access their services. That is, trans-organizational roles are valid roles within and across different RBAC systems.

There is a need for scalable RBAC systems which support trans-organizational use cases without creating federations. This chapter proposes a family of trans-organizational RBAC models. The base model $RBAC_0$ found in RBAC96 is extended to include multiple organizational domains. Components of $RBAC_0$ are likewise extended for each organization and additional components to support trans-organizational roles are developed.

2.1 Application to IoT Systems

IoT systems often contain such trans-organizational RBAC use cases. Figure 2 illustrates a real-world example, where SPs provide free or discounted services to students under educational licenses or student plans. The school `NAIST` (IdP) validates a user and issues the trans-organizational role `student`. This role can

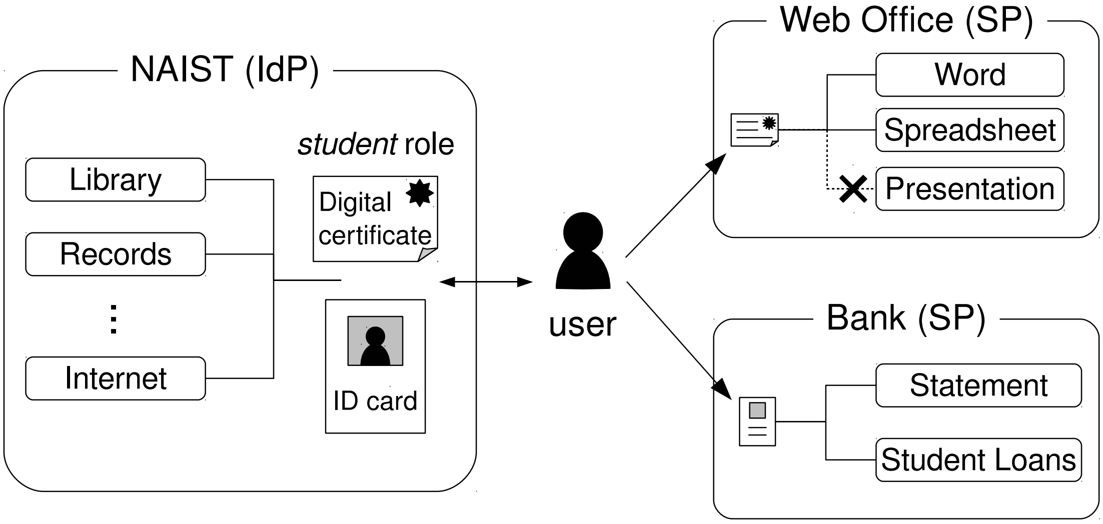


Figure 2. Example of a trans-organizational use case. The IdP `NAIST` assigns the role `student` to a user, and the user has access to `NAIST`'s services. SPs, even if not in a federation with `NAIST`, can provide students access to some of their services.

be used with services provided within `NAIST`'s system, and can be distributed in a number of ways (i.e., a single digital certificate stored offline in the user's computer and in a plastic card with an Auto-ID). In addition, the role can also be used in other organizations (SPs) such as an online office suite (using the offline certificate) or a bank (using the card). Note that the school does not prohibit its users from utilizing their `student` roles with SPs, but the school will not agree to provide their list of students to external organizations.

Another scenario is the flexibility of trans-organizational roles for Auto-IDs. Consider the system in Figure 3, where a hospital (IdP) issues `doctor` and `nurse` roles to medical personnel. Also, a healthcare provider and a manufacturer (IdPs) embed Auto-IDs in hospital items such as wrist tags (with a 2D barcode), medical cards (with IC chips) and wheelchairs (with an RFID), respectively. These Auto-IDs are tied to services which stores a particular patient's medical data and tracks their location – both of which are prominent healthcare management applications. The services are managed by other hospitals or clinics (SPs) depending on where a patient goes to.

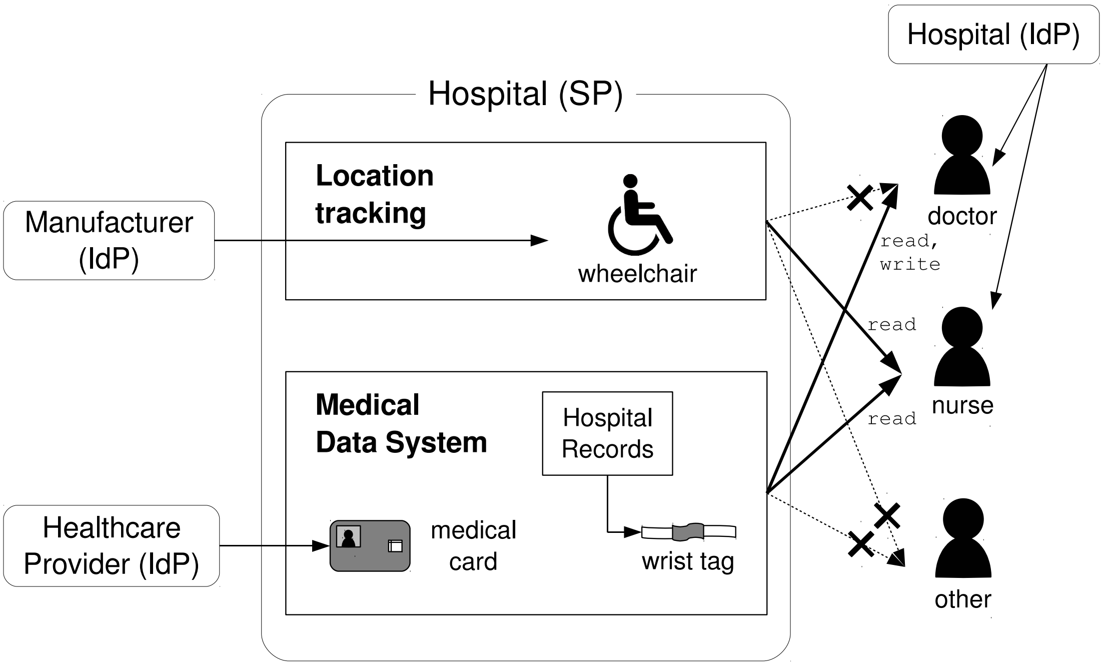


Figure 3. Example of a trans-organizational use case. IdPs assign roles to users and Auto-IDs in products. Data can be accessed only through a valid combination of roles determined by an SP.

Note two things in this example. First, this illustrates a scenario where an SP uses roles issued by multiple IdPs. SPs can validate Auto-IDs coming from different sources, and manage that data as a service to other users. Second, an organization in ToRBAC may be an IdP and SP at the same time. The hospital can be the same organization which has two functions: assign doctor and nurse identities as an IdP, and manage healthcare applications as an SP.

However, there is major concern to protect these Auto-IDs against unauthorized access. For example, medical cards and wrist tags contain sensitive information about the patient, thus users with a `doctor` role are granted read and write access, while users with a `nurse` role only have read access. Also, only `nurse` roles have read access to location data stored in wheelchair RFIDs. Other users and services who may possess scanning equipment but do not have a valid combination of roles should not be able to access Auto-IDs, whether or not they are registered SPs in the system. In general, users, services, and Auto-IDs must not be able to assert false roles in order to gain illegal permissions to these resources.

Finally, ToRBAC can be considered for large systems such as national identification numbers. In this kind of system, a government issues a unique number (and roles) to each of its citizens which can then acquire services provided by local or foreign governments. However, these can only be assigned after a rigorous check of a user's identity. This gives SPs a level of assurance that trans-organizational roles will be trustworthy (depending on the level of trust on the government). An existing problem in government IT infrastructures is their decentralized nature; computer systems are developed by multiple vendors or managed by separate administrators, which makes it difficult to centralize access control. ToRBAC systems by definition interconnect these organizations, and can therefore be a practical and cost-effective alternative for these systems as opposed to developing and maintaining a centralized system.

These examples serve to highlight the importance of trans-organizational use cases in IoT systems; however, note that trans-organizational RBAC can be used in many other systems, for different purposes other than illustrated above.

2.2 Related Work

In 1996, Sandhu, et. al introduced the RBAC96 models [20] for role-based access control. The aim of these models was to simplify the management of access control for computer systems through the expressive nature of roles. Figure 4 shows the family of models originally proposed in RBAC96. Here, the base model consists of the users U and permissions P. Access control from U to P is granted through the assignment of roles R. These roles can be arranged in a role hierarchy ($RBAC_1$), while constraints can be set in assignment relations ($RBAC_2$) and indicated in the figure with a star. The consolidated model of an RBAC system ($RBAC_3$) includes all aspects depicted in the figure.

Note that in this figure, it is assumed that all elements are within the domain of a single organization. With this centralized setup, administrators can flexibly control access to all resources within the organization according to their organizational tree (role hierarchy) and protection guidelines (constraints). As earlier noted however, this is not enough for trans-organizational systems because administration is distributed across multiple organizations. Additional components

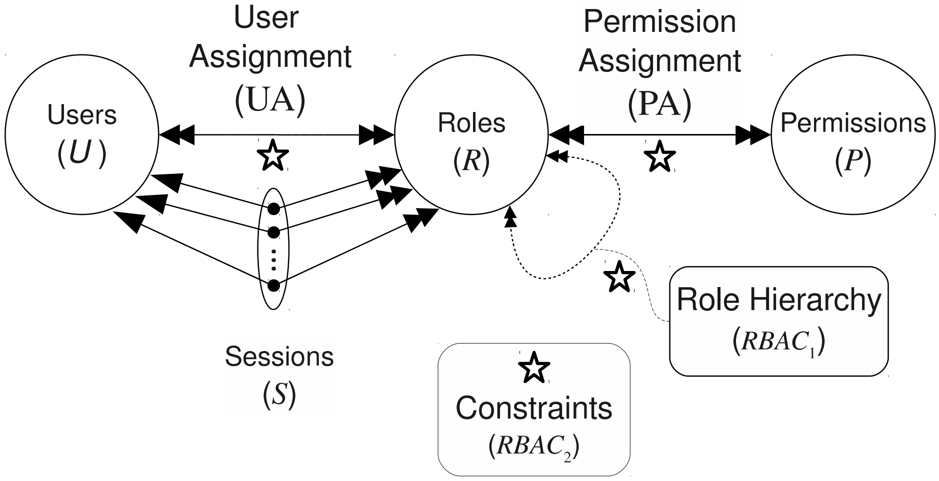


Figure 4. A family of RBAC models from RBAC96 [20].

must be added to the model in order to efficiently support one or more domains of control (e.g., different role hierarchies and constraints).

One solution to support trans-organizational use cases is to create a *federation* of organizations similar to single-sign on systems such as the Shibboleth System[2] such as user-role assignments to other organizations in the federation while retaining its autonomy [5]. On the other hand, an IdP might consider user-role assignments as critical and private information, and are unwilling to share this information with an SP. In such use cases, roles are issued and honored between independent organizations outside a federation. Support for trans-organizational use cases without requiring federations is therefore strongly needed for RBAC systems.

Zhang et al. [28] proposed another approach, where a family of *Role and Organization Based Access Control* (ROBAC) models take into account multiple organizational domains. In ROBAC, users are assigned role and organization pairs. Using this pair, access to an asset is restricted by two relations: the user's role must have the appropriate permissions to access the asset, and the asset must also be mapped to an organization. However, the authors of ROBAC note that there may be instances where the number of role and organization pairs may

[2] The Shibboleth System - Internet2 Middleware Initiative (http://shibboleth.net/, last accessed: Aug 2012).

become large as the number of organizations increase. As a result, management complexity issues related number of roles and permissions may arise in the long term. This can severely affect IoT systems given their large number of users, roles and organizations.

2.3 Trans-organizational RBAC Models

In this section, conceptual models for trans-organizational RBAC are presented. In the following discussion, the model is defined with respect to the components found in RBAC96 (Figure 4) to indicate additions and simplify comparisons between the two approaches. Four models are defined, starting with the base model $ToRBAC_0$ which serves as the minimum requirements for a trans-organizational RBAC system. $ToRBAC_1$ adds *role hierarchies* to the base model, and $ToRBAC_2$ adds *constraints* to the base model. Finally, $ToRBAC_3$ consolidates all additions to $ToRBAC_0$.

The models are introduced in a natural manner, where the $ToRBAC_0$ model defines a basic trans-organizational RBAC system. The subsequent models define additional features to a basic ToRBAC system, but these can be skipped depending on the use cases of the system. Also, for the sake of simplicity, our discussion assumes that IdPs and SPs are different sets of organizations (but this is not a requirement).

2.3.1 Base Model – $ToRBAC_0$

The characteristics of all models are presented in Figure 5, composed of the following entities:

Users. A user can be any “thing” that can access protected resources – a human being, a smart object, a service, an Auto-ID, etc.

Trans-organizational Roles. A trans-organizational role is a pre-defined name for a job function or an attribute recognized by an organization. An SP has the option to rename a role when used in their system, called an *interpreted role* (e.g., a digital library service may rename the roles `student` and `teacher` as the interpreted role `academic_member`).

Permissions. A permission is a combination of a resource and a list of

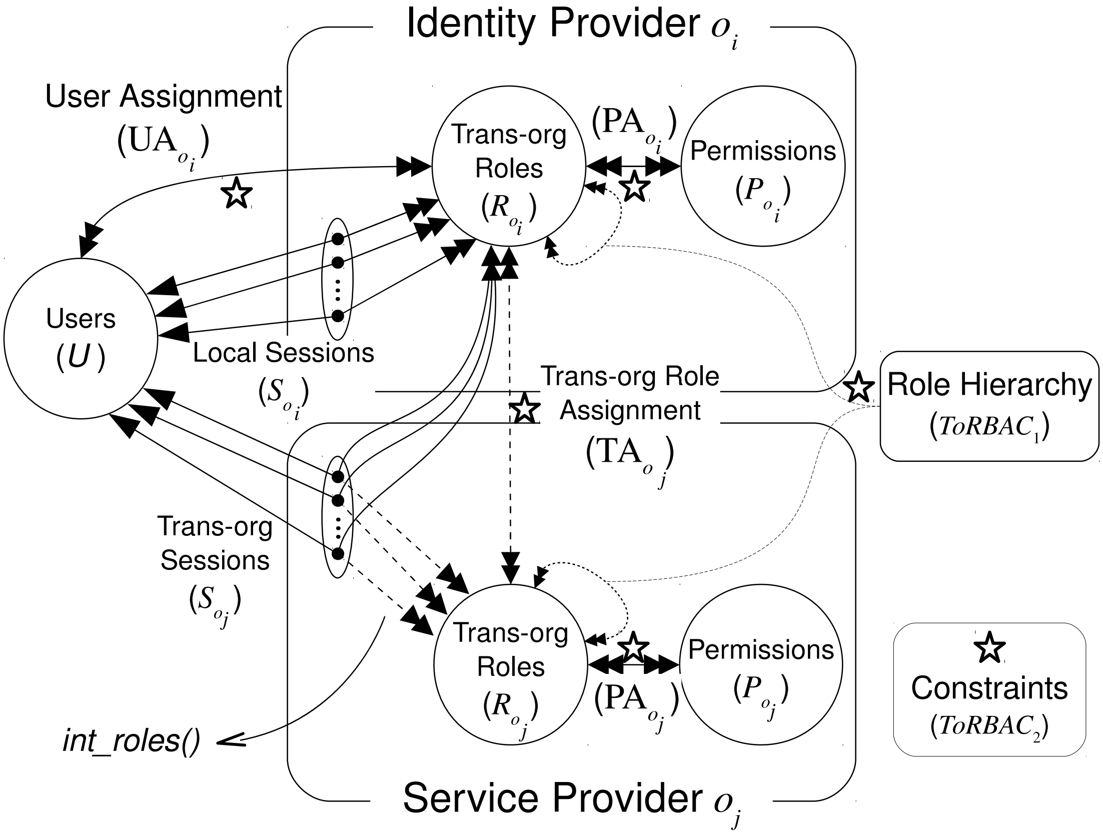


Figure 5. A family of trans-organizational RBAC models. $ToRBAC_1$ adds role hierarchies, while $ToRBAC_2$ adds constraints in assignment relations indicated with a star. The consolidated model $ToRBAC_3$ includes all components in the figure.

actions on the resource, such as read, write, execute, modify, etc. Permissions grant access rather than deny them; access denials are considered as constraints.

Sessions. When a user wishes to access a resource, it asserts some roles to gain the appropriate permissions. A session may either be a *local session* between a user and an IdP (where the roles being asserted are issued by the same IdP only), or a *trans-organization session* between a user and an SP (where the roles being asserted are issued by one or more IdPs).

$ToRBAC_0$ has the following components:

- U and O, the set of users and the set of organizations, respectively. An organization in O can be either an identity provider (IdP) or service provider (SP);

- R_o, P_o and S_o, the set of trans-organizational roles, permissions, and sessions managed by organization $o \in O$, respectively. To simplify the discussion, let us define $R_{\text{IdP}} = \cup_{o \in O, o \text{ is an IdP}} R_o$;

  In general, assume that for two different organizations o_i and o_j, $R_{o_i} \cap R_{o_j} = \emptyset$ and $P_{o_i} \cap P_{o_j} = \emptyset$; that is, each role or permission is managed exclusively by one organization. All organizations in O, however, share an identical set U of users. It follows that a user in U is allowed to have roles assigned by multiple IdPs, and acquire services from multiple SPs by asserting those roles.

- $\text{UA}_o \subseteq U \times R_o$ for each $o \in O$, a many-to-many *user-role assignment* relation in organization o;

- $\text{PA}_o \subseteq R_o \times P_o$ for each $o \in O$, a many-to-many *permission-role assignment* relation in organization o;

- $\text{TA}_o \subseteq R_o \times R_{\text{IdP}}$ for each $o \in O$ and o is an SP, a many-to-many relation of *trans-organizational role assignments* for roles in R_o (o is an SP) and roles in R_{IdP};

- $user : S \to U$, a function mapping each session s to a single user $user(s)$ (same as in $RBAC_0$);

- $org : S \to O$, a function mapping each session s to an organization (which should be an SP) $org(s)$ where the session is currently established;

- $roles : S \to 2^{R_{\text{IdP}}}$, a function mapping each session s to a set of roles $roles(s) = \{r \mid (user(s), r) \in \text{UA}_o, o \in O\}$. The function gives the roles asserted by $user(s)$ to $org(s)$ during the session (note that during a session, a user may assert any roles assigned from IdPs, hence the function range is $2^{R_{\text{IdP}}}$);

- $int\_roles : S \to 2^{R_{o_j}}$, a function mapping session s to the subset of interpreted roles defined by $int\_roles(s) = \{r' \mid (r', r) \in \text{TA}_{o_j}, o_j = org(s), r \in$

$roles(s)\}$. This function, present only in trans-organization sessions, gives the set of interpreted roles $r' \in R_{o_j}$ from the asserted roles $roles(s)$.

Note that many components of $ToRBAC_0$ are the same as in $RBAC_0$. The set of organizations O is introduced, while the sets R, P and relations UA, PA of $RBAC_0$ are modified to represent each component for a single organization. Similar to establishing a session in $RBAC_0$, users may activate a subset of roles when accessing the RBAC system of an SP. A key difference is when a user asserts a role r_{o_i} in a trans-organization session, the SP o_j looks for valid pairs of roles in TA_{o_j}. If there are some roles $r \subseteq R_{o_j}$ with $(r, r_{o_i}) \in \mathrm{TA}_{o_j}$, then the user is allowed to access o_j's RBAC system using permissions associated to the roles r. If there are none (i.e., if $(r, r_{o_i}) \notin \mathrm{TA}_{o_j}$ for any r) then no permissions are granted and the user is denied access. Note that in this process, the SP does not inquire the IdP about its user-role assignments.

The discussion above referred to IdPs and SPs as different sets of organizations. This is not a requirement in the model; SPs can also have user-role assignments and IdPs can have permission-role assignments. Regardless, an organization cannot view or assign trans-organizational roles and permissions for another organization. In Figure 5, for example, an IdP_{o_i} cannot view or define R_{o_j} or PA_{o_j} in SP o_j. This is in line with the fact that these organizations are not required to join a federation. On the other hand, trans-organizational roles, besides being used in an SP's RBAC system, can also be used in an IdP's RBAC system through local sessions. In Figure 5, IdP_{o_i} can define PA_{o_i} according to RBAC inside o_i by using trans-organizational roles R_{o_i}. These roles can be treated as regular roles of RBAC, thus the cost of adoption trans-organizational roles for IdPs are minimized.

Consider the simple example illustrated in Figure 2. Following the definition of the $ToRBAC_0$ model, let $O = \{\texttt{NAIST}, \texttt{WebOffice}, \texttt{Bank}\}$ be the set of all organizations where `NAIST` is an IdP (and SP at the same time), and `WebOffice` and `Bank` are SPs. Some roles in the system are $R_{IdP} = \{\texttt{student}\}$ and $R_o = \{\texttt{academic\_member}\}$ for $o = \texttt{WebOffice}$. For $o = \texttt{WebOffice}$ to grant services to users with the `student` role, they define:

1. $\mathrm{TA}_o = \{(\texttt{academic\_member}, \texttt{student})\}$ which declares the interpreted role

2. $\mathrm{PA}_o = \{(\texttt{academic\_member}, \texttt{Word}), (\texttt{academic\_member}, \texttt{Spreadsheet})\}$, for the set of permissions $P_o = \{\texttt{Word}, \texttt{Spreadsheet}, \texttt{Presentation}\}$

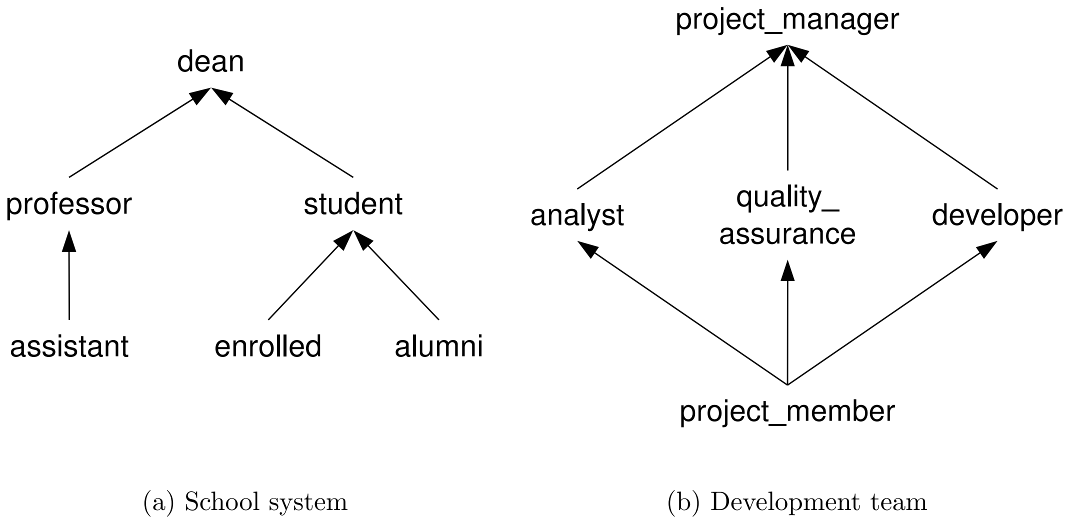
Assume that for a session s, $u = user(s)$ and $o = \texttt{WebOffice} = org(s)$. Also, assume $(u, student) \in UA_{NAIST}$; that is, u sends a service request to `WebOffice` with the role `student` $\in R_{NAIST}$. By the assumption, $roles(s) = \{student\}$ and hence $int\_roles(s) = \{\texttt{academic\_member}\}$ because of the trans-organizational role assignment $\mathrm{TA}_o = \{(\texttt{academic\_member}, \texttt{student})\}$. Therefore, u can use the `Word` and `Spreadsheet` permissions but cannot use the `Presentation` permission by PA_o. Services offered by `NAIST` and `Bank` can be constructed similarly.

2.3.2 Role Hierarchies – $ToRBAC_1$

In any organizational environment, it is common to define roles according to a hierarchy. This construct is a natural yet powerful way to describe structures of authority in real-world situations. To express this in our model, $ToRBAC_1$ adds role hierarchies to the base model. A role hierarchy is a partial order of roles, where *parent roles* (roles in a higher order) inherit permissions from *child roles* (roles in a lower order) if there is a binary relation between them. Figure 6 shows some examples of role hierarchies. Note that the arrowhead indicates the direction of permission inheritance.

Figure 6(a) shows a basic school system hierarchy. The `dean` role is the parent role of both `professor` and `student`, thereby inheriting permissions assigned to both roles. By transitivity, the `dean` role also inherits from the `assistant` role.

Role hierarchies are not trans-organizational because an organization cannot view user-role assignments of other organizations (and vice-versa). An SP may request the user to assert multiple roles, but the hierarchy structure is not explicitly revealed to the SP. This keeps role hierarchies hidden, which might be considered as private information by organizations. However, SPs can manage their own role hierarchies as well. When an SP interprets a trans-organizational role into another role in its ToRBAC system, it follows access control rules set by the role hierarchy defined by the SP.



(a) School system

(b) Development team

Figure 6. Examples of role hierarchies.

2.3.3 Constraints – *ToRBAC*$_2$

An important property of any flexible access control system is the implementation of constraints. These constraints are applied mainly to assignment relations in the system, as indicated in Figure 5. The *ToRBAC*$_2$ model places constraints on top of the base model in the following ways.

User-role assignments. Constraints can be applied to allow one user to be assigned to at most one role in a mutually exclusive set (*mutually exclusive roles*). This supports the security principle of *separation of duties*, where two or more different users (and roles) are required to accomplish a single task. Consider Figure 6(b) as an example, temporarily disregarding the hierarchy structure. A user in the same project cannot be assigned to both `developer` and `quality_assurance` to ensure unbiased QA testing. Similarly, one role can be assigned to at most one permission in a mutually exclusive set (*mutually exclusive permissions*), and different roles are required to accomplish a task.

Cardinality. Relations can be also limited by the number of assignments that can be done (e.g., the `project_manager` role can only be assigned to one user, or a user can only have a maximum of 5 roles at any given time).

Prerequisites. A system may require a user to have particular role before granting a new role. For example, a user can be required to have the `project_member` role first before being assigned the `analyst`, `developer`, or `quality_assurance` roles. Prerequisite permissions can be enforced as well.

Trans-organizational role assignments. IdPs can restrict some roles such that they can be interpreted by a subset of SPs only (i.e., a role cannot be part of a trans-organizational role assignment in some organizations). The model, therefore, can behave similar to a federation. A role that cannot be interpreted by any SP is called a *private role*; if all roles in the system are private roles, then the system becomes a regular RBAC system (trans-organizational use is prohibited).

On the other hand, SPs can restrict role interpretation in a straight-forward way. When a user asserts a trans-organizational role, it must contain information about the IdP that issued the role. The SP then checks this against a list of IdPs and grants or denies access accordingly.

2.3.4 Consolidated Model – $ToRBAC_3$

Finally, $ToRBAC_3$ puts both role hierarchies and constraints in a consolidated model. This implies that constraints can be further placed on role hierarchies to control role relations (role A cannot inherit a subset of permissions from role B), cardinality (a role has a maximum number of parent or child roles), and prerequisites (role A must have parent role B before assigning other child roles). Also, the system can prevent some roles from having common parent or child roles. This gives a central system administrator control over role hierarchies in systems where role administration is decentralized.

2.4 Discussion

As previously mentioned, trans-organizational RBAC extends the traditional model to make access control across different organizations possible. The RBAC system within each organization is still implemented according to any pre-existing RBAC model. Thus, organizations which have existing systems can adopt a trans-organizational RBAC system without changing their current business processes and system administration. However, the cryptographic representation of roles must be changed to support trans-organizational interpretation, which will be discussed in the next chapter.

2.4.1 Management Complexity

Related to this, the management complexity of an IoT system in terms of the number of roles and permissions must be considered, since applications may have many users and organizations. In trans-organizational RBAC, increasing the number of organizations does not increase management complexity in the IdP. This holds true because the RBAC system in an IdP's system is not changed. Management complexity in SPs increases when new trans-organizational role assignments need to be added (e.g., when services are made available to more roles). Furthermore, increasing the number of users does not increase the management complexity for both IdPs and SPs; it remains the same as if the system were a traditional RBAC system. However, one caveat of this is trans-organizational RBAC does not address scalability within a single organization – this must be addressed by the internal RBAC system the organization uses.

In addition, users also benefit from trans-organizational RBAC. If the user has M *role types* for N organizations, then the user needs to manage at most $N \times M$ *role instances* in RBAC96. On the other hand, since each type of role in ToRBAC can be shared across organizations, the user manages at most M instances of roles only. More concretely, assume that there are M role types. Each role type r^i $(1 \leq i \leq M)$ has a role instance, say $r^i_{o_j}$, for each SP o_j $(1 \leq j \leq N)$. In RBAC96, the user u needs to manage $N \times M$ role instances $r^i_{o_j}$ $(1 \leq i \leq M,\ 1 \leq j \leq N)$. On the other hand, in ToRBAC, if we let $(u, r^i) \in \text{UA}_o$ $(1 \leq i \leq M)$ for the user u and IdP o, and let $(r^i_{o_j}, r^i)$ *in* TA_{o_j} $(1 \leq j \leq N)$, then the user u needs to manage only $M \times N$ role types r^i $(1 \leq i \leq M)$ because the instantiation of r^i to $r^i_{o_j}$ can be automatically conducted by ToRBAC based on TA_{o_j} where o_j is the SP that the user u is requesting a service from.

An intuitive example of this is a passport issued by a government agency (IdP). A single passport book can be used to assert citizenship (role type) and subsequently acquire services from different organizations such as airports or financial institutions (SPs). Notice that the user only needs one passport to assert citizenship, thus minimizing the number of role instances issued by multiple government agencies that certify citizenship.

2.4.2 Standard Role Specifications

The management of trans-organizational roles can be made more efficient by defining a standard of role names and capabilities. A standard defines a list of common role names issued by a particular type of IdPs, including role hierarchies and constraints. If IdPs make roles available for interpretation, they must adhere to the standard in order for SPs to offer services without looking up roles names for each IdP. First, it decreases the total number of trans-organizational roles in the system. This also decreases confusion of which role names are used for classifying users. Furthermore, it gives a clear indication of trans-organizational interpretations available to all organizations in the school system, thus making trans-organizational RBAC more manageable.

To illustrate this, Table 1 defines a standard for a trans-organizational RBAC system used by schools nationwide. It first lists a column of categories, where roles can be classified to easily differentiate them. Next, role names in each category are defined. In this example, the role hierarchy in Figure 6(a) is partially represented (notice that the standard does not reveal the entire role hierarchy of the IdP). A right arrow $\rightarrow$ indicates that the role name is a child role of the preceding role (e.g., `BS` is a child role of `science`). The description column indicates the interpretation of an IdP for that role name. Mutually exclusive roles which are indicated here as well. SPs then refer to this table to understand what kind of trans-organizational role assignments are available to all IdPs.

For example, consider a school system that has two participating schools `NAIST` and `ADMU`. Using the standard, a library SP can offer their services to current students and teachers of `ADMU` using the role set $\{\{\texttt{ADMU, enrolled}\} \cup \{\texttt{ADMU, faculty}\}\}$. To offer the service to science students only (but regardless of specific discipline) in all universities, the set $\{\texttt{science, enrolled}\}$ can be used. Finally, to make a very specific service such as a loyalty card for Information Science graduates of NAIST who are not currently faculty members of any school, a service can use the set $\{\{\texttt{NAIST, IS, alumnus}\} \cap \neg\{\texttt{faculty}\}\}$, where $\neg\{\texttt{faculty}\}$ is an additional constraint.

Table 1. Example of a standard for a nationwide school system.

Category	Role Name	Description
Department	`science`	Science discipline
	→ `BS`	→ Biological Sciences
	→ `IS`	→ Information Science
	→ `MS`	→ Material Sciences
	`other`	Other discipline
Member	`student`	University student
	→ `enrolled`	→ currently studying*
	→ `alumnus`	→ graduated*
	`faculty`	University faculty member
	→ `professor`	→ Professor
	→→ `assistant`	→→ Assistant Professor

* Indicates roles which are mutually exclusive.

2.4.3 Role Administration

In trans-organizational RBAC, role administration structures can either be centralized or decentralized. Administration duties can be delegated by central authorities to lower authorities, thus improving the its efficiency when the number of users or roles is large. To enforce integrity and consistency across the structure, constraints are defined to keep centralized control over role administration. These constraints can be added at every level of authority and carried over to every subsequent level. In the previous example, the mutually exclusive roles `enrolled` and `alumnus` are set at the highest level of the school system; all schools therefore have the same constraint at every level of authority. Additional constraints (e.g., the `faculty` role is not trans-organizational) can be implemented at a lower level.

2.4.4 Identification of Liability

Finally, besides providing a secure mechanism to prevent unauthorized access, a concern with flexible RBAC systems with multiple organizations is the identification of liable parties when services are abused. If there is a dishonest party in the system, there must be a mechanism that allows administrators to identify the dishonest user or service. This scenario is different from unauthorized access – if a party gains authorized access to a service but misuses the privileges of that service, then this is also considered as a violation of trust. For example, if a user with role `student` fails to pay credit card dues within the allowable period, then the `bank` SP can suspend that user within its RBAC system. However, the SP must also be able to identify the user and `school` IdP that issued the role so that the nature of the violation can be determined. The SP can report the violation to the IdP for further sanctions, or the SP can investigate who are the parties responsible for the violation (the IdP can be at fault as well). Note that in general, the liable party in a trust violation case is not immediately clear. This is an administrative and legal issue, a discussion of which is out of the scope of this dissertation. Nevertheless, trans-organizational RBAC should provide such a mechanism to identify liable parties to address such scenarios.

2.5 Conclusion

This chapter proposed a trans-organizational RBAC model for applications that span multiple organizations without requiring federations to be created. Using RBAC96 as a basis, an extended family of models was proposed, centered on the definition of trans-organizational roles. A base model was formally defined; additions to this such as role hierarchies and constraints were explained.

Furthermore, it was shown that the proposed ToRBAC models provide benefits to access control for IoT systems. Example use cases of IoT systems were described, along with some of its performance and management problems. Several properties show that the models can address these problems; they are scalable with respect to the number of organizations in the system without increasing management complexity. Also, the efficiency and clarity in role management can be improved by defining a standard of role names, and designing either a centralized or decentralized administration structure. In addition, the issue of liability in trans-organizational trust violations was discussed, and it was established that ToRBAC systems must have mechanism to identify offending parties.

Finally, it was shown that the model can be designed to allow IdPs to protect roles from interpretation, or assign roles which can only be interpreted by certain

SPs. This constraint allows trans-organizational RBAC to create federations, or to completely protect their IDs from trans-organizational use; this gives the model the ability to support single organization, federation-based, and trans-organizational use cases.

3. Secure Scheme for Trans-organizational Role-Based Access Control

Properties and features of trans-organizational RBAC models may be implemented using conventional public-key cryptosystems. In *trust management* studies [19], credentials are granted to users using digital certificates based on a *Public-Key Infrastructure* (PKI). An important condition in using PKI is that it requires access to one or more external repositories managed by a trusted third party (TTP) for authenticating certificates. PKI schemes can easily be implemented within a single organization because the organization itself can serve as the TTP, making access control operations efficient and manageable. However, given that trans-organizational use cases for IoT systems are large and distributed over multiple organizations and levels, the involvement of a TTP for key authentication adds system administration and performance bottlenecks. For example, a large number of objects tagged with Auto-IDs may be distributed in various locations, and scanning them can be performed by many different users and SPs. In these cases, the volume of authentication requests to a TTP are high, which makes it impractical to implement for more than a few organizations.

Moreover, there are isolated instances where an active connection to the TTP is unavailable. The location of some Auto-IDs can be inaccessible to network-connected scanners, especially for objects that are constantly moved from one place to another. Also, in the aftermath of a natural disaster, scanners and their terminals may be physically unable to contact the TTP. This halts access control mechanisms for these systems, and therefore is undesirable in certain situations where IoT systems are used in critical applications. Connectivity to a TTP thus becomes a point of failure for such systems, and the cost of digital certificates and PKI outweigh the benefits of using ToRBAC systems for multiple organization scenarios.

In designing a scheme for ToRBAC models described in the previous chapter, there are several properties that must be considered including implementation of role hierarchies, constraints, role administration structures, and identification of liability. Furthermore, there is an inherent security issue in trans-organizational RBAC. When a user asserts a certain role to an SP, there is no guarantee that the role is indeed a valid role issued by an IdP. This is further compounded by the requirement that an SP cannot inquire IdPs about user-role assignments. Thus, there is a need for a role authentication protocol which allows an arbitrary SP to verify the user-role assignment of an arbitrary IdP. Also, the protocol must be secure against dishonest users that attempt to assert false roles to an SP, and dishonest SPs that attempt to deceive users about their authenticity and establish trusted communication. Given these drawbacks to conventional public-key schemes, improvements are needed specifically to support ToRBAC models.

In this section, a secure scheme for ToRBAC systems is studied. The key idea to support trans-organizational scenarios in a practical way is to represent the public key in a way that uses information that can be verified without a TTP. The approach considered in this thesis represents roles using *identity strings* (ID strings), which contain expressive information about the user. Through this design decision, roles contain information about the identity of the user, thus minimizing the need for a TTP during role authentication procedures. To secure ID strings, the scheme uses *Hierarchical Identity-Based Encryption* (HIBE) [10], a type of public-key encryption which uses identity strings as a public key. The steps of the basic scheme are designed based on HIBE, with emphasis on a role authentication protocol that is performed between the user and SP only. To analyze the scheme, security properties are defined and additional constructions are applied to the basic scheme.

3.1 Cryptographic Primitives

The idea of *Identity-Based Encryption* (IBE) cryptosystems was proposed by Shamir [21]. In a traditional public-key cryptosystem such as PKI, the encryption key is determined by some secret information unrelated to the user's identity. When another user wants to send a message, they must confirm the authenticity of the encryption key by contacting a certificate authority. In IBE, the encryption key is derived from some publicly known information about the user's identity instead (e.g., an ASCII string such as the user's email address). This ID string is well-associated to the user because an IdP such as an email service ensures that the string is unique and verified for that user. Thus, this eliminates the cost for PKI and certificate authorities for verifying digital certificates.

To setup an IBE system, a trusted third party called a *Private Key Generator* (PKG) first takes a set of security parameters to generate a master private key, which it keeps secret. Then, it publishes system parameters to all entities in the system. Given the system parameters, any party can compute a public key from an ID string. To read a message decrypted using an ID string, a user obtains the corresponding decryption key from the PKG using its master private key, system parameters and ID string. In this ID string registration process, the PKG must verify the identity of the user to minimize ambiguity in the system (i.e., messages encrypted using that ID string can be decrypted specifically by the intended recipient only).

3.1.1 Hierarchical Identity-Based Encryption

IBE can support a hierarchical tree of PKGs through Hierarchical Identity-Based Encryption similar to an organizational tree structure. The PKG at the top level of the tree (referred to as `root PKG`) manages a group of lower-level PKGs in order to delegate key management duties. These PKGs can have their own lower-level PKGs as well. An ID string S is composed of substrings called *ID-tuples*, where $S = (s_1, ..., s_t)$ and each ID-tuple represents a level in the tree. The PKG at level i of the tree is denoted by $\{(s_1, ..., s_i) : 1 \leq i < t\}$. The ID string of the root PKG (i.e., $t = 0$) is $S_0 = \epsilon$. Formally, there are five randomized algorithms which compose HIBE:

- *RootSetup*(K) – Given a security parameter K, the root PKG generates system parameters *params* and a master private key SK_{master}, which it keeps secret. The PKG publishes *params* to the public and it is available for the system's lifetime.

- *PKGSetup*$()$ – To setup a lower-level PKG, it obtains *params* from the root PKG. In addition, it may use its own secret value to generate keys for its children. However, it may not have its own system parameters to be used in their subtree of PKGs.

- *KeyGenerate*$(params, SK_{S_t}, s_{t+1})$ – A PKG with ID string S_t generates private keys as follows: given its private key SK_{S_t}, an ID-tuple s_{t+1}, and a secret value (if any), the PKG returns the private key $SK_{S_{t+1}}$ for the ID string $S_{t+1} = (S_t, s_{t+1})$.

- $\mathit{Encrypt}(params, m \in \mathcal{M}, S_t)$ – Encrypt message m using *params* and the ID string S_t.

- $\mathit{Decrypt}(params, c \in \mathcal{C}, SK_{S_t})$ – Decrypt ciphertext c using *params* and the private key SK_{S_t} of the ID string S_t.

The *Encrypt*() and *Decrypt*() algorithms must satisfy a standard consistency constraint. Let SK_S be the private key generated by $\mathit{Extract}(params, S)$. For all messages $m \in \mathcal{M}$,

$$\mathit{Decrypt}(params, c, SK_S) = m \text{ where } c = \mathit{Encrypt}(params, m, S).$$

Delegation of key management in HIBE is flexible. A PKG at level t can compute decryption keys at any level $i \geq t + 1$ of its subtree. This means that users can serve as PKGs, and generate their own subtree of ID strings. The implications of this are discussed in Section 3.4. However, a PKG cannot compute decryption keys for IDs outside of its subtree, including levels higher than t. Also, note that each level in the tree does not necessarily mean that there is a PKG at that level. An ID string at level t may designated for classification purposes only (e.g., employees at level $t + 1$ are grouped by department at level t, but the company PKG keeps the decryption keys at level t secret).

3.1.2 Challenge-Response Protocol

Challenge-response protocols are used when a party (*prover*) wishes to assert knowledge of secret value to another party (*verifier*) without revealing the secret itself. If we assume that the secret is a private decryption key in public-key encryption, then the protocol is straight-forward. The verifier encrypts a random message $m \in \mathcal{M}$ using an encryption key PK_i, and the resulting ciphertext $\{m\}_{PK_i}$ serves as the *challenge*. The challenge is then sent to the prover, who can obtain the original message $m = \{\{m\}_{PK_i}\}_{SK_i}$ if the prover indeed has the corresponding decryption key SK_i. The prover finally sends the decrypted ciphertext as the *response* to the verifier, and if the response and m match, this validates the prover's assertion. Note that the security of the protocol is based on the property that the chances of the prover obtaining m without knowledge of SK_i is sufficiently small to be ignored.

3.2 Proposed Scheme

The following subsections describe a basic scheme for ToRBAC based on HIBE. Additional components of the scheme that enhance its security are defined in the Section 3.3. In the following discussion, consider a simplified trans-organizational system where one root PKG manages all organizations in the system at level $t = 1$, and an organization can either be an IdP or SP only. Advanced use cases of trans-organizational systems are not discussed, but they are constructed from the components given below.

3.2.1 Representation of Trans-organizational Roles

In this scheme, trans-organizational roles are represented as the pair (S, SK_S), where S is the ID string describing the role, and SK_S is the corresponding decryption key generated through the $KeyGenerate()$ function of HIBE. An ID string is composed of a well-structured set of alphanumeric ID-tuples containing either the name of the IdP, the name of the role, or the category of the role. These are separated by a designated non-alphanumeric character (for the rest of this discussion, "." is used as the separator and not used in any ID-tuple).

To describe a role, ID-tuples are arranged according to the role hierarchy of the IdP. The name of the IdP is then prefixed to form a complete ID string. This is done for two reasons: the IdP which issued a role must be identified (identification of liability), and all ID strings in a ToRBAC system must be unique. For instance, valid constructions of ID strings in the school ToRBAC system given in Section 2.4.2 are `NAIST.faculty` and `ADMU.student.enrolled`.

3.2.2 System Setup

Setting up a ToRBAC system consists of two phases shown in Figure 7. First, HIBE is initialized for the ToRBAC system. The PKG calls the $RootSetup()$ function and the generated master private key and system parameters are kept

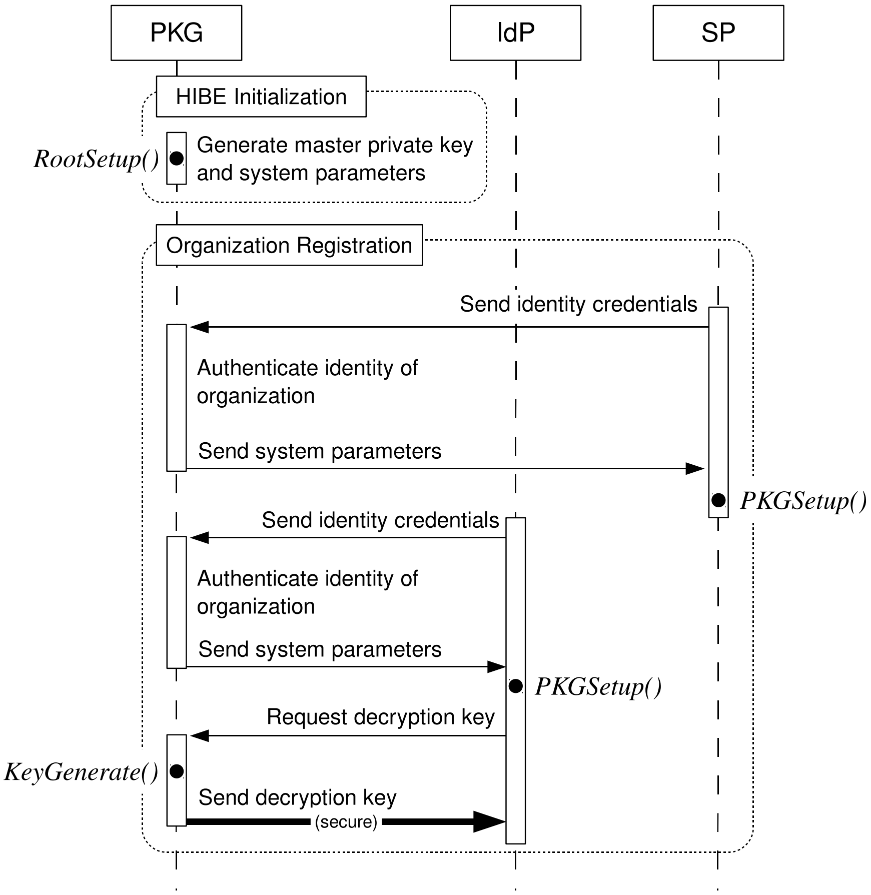

PKG
IdP
SP
HIBE Initialization
RootSetup()
Generate master private key and system parameters
Organization Registration
Send identity credentials
Authenticate identity of organization
Send system parameters
PKGSetup()
Send identity credentials
Authenticate identity of organization
Send system parameters
PKGSetup()
Request decryption key
KeyGenerate()
Send decryption key
(secure)

Figure 7. Sequence diagram of the two phases of system setup.

secret. Note that the system parameters are eventually shared with entities in the system, and knowledge of this does not compromise the security of the system. However, the master private key must be hidden by the PKG at all times.

In the second phase, organizations register with the PKG to participate in the ToRBAC system. An organization first sends its identity credentials. The PKG then authenticates the identity of the organization, the specifics of which are defined by the PKG. This procedure can be completed in various ways, including conventional document production or legal certification. If the organization's identity is verified, the PKG sends the system parameters to the organization. The organization has the option to generate a lower-level secret through the $PKGSetup()$ function. From here, the organization can set their ToRBAC system

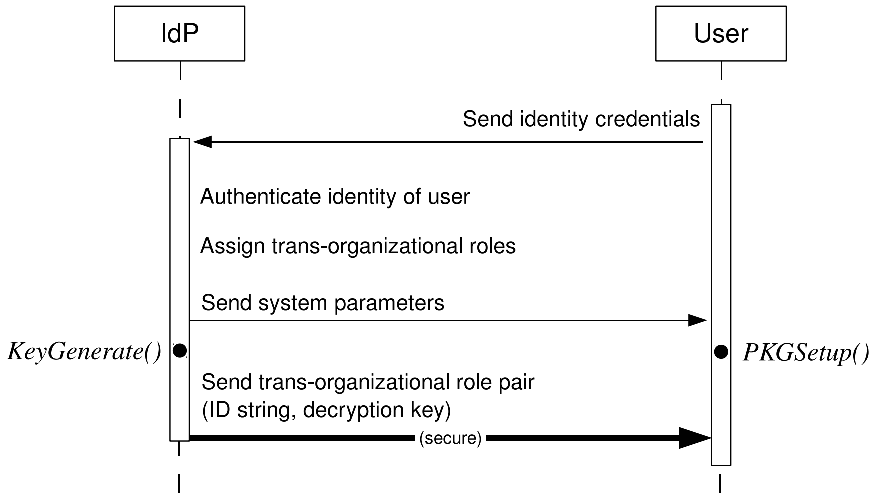

IdP
User
Send identity credentials
Authenticate identity of user
Assign trans-organizational roles
Send system parameters
KeyGenerate()
PKGSetup()
Send trans-organizational role pair
(ID string, decryption key)
(secure)

Figure 8. Sequence diagram of user registration between an IdP and a user.

rules such as role hierarchies and constraints.

IdPs who register with the PKG must perform additional steps. An IdP requests for a decryption key derived from their verified identity and agreed upon by both parties. The PKG generates this using the *KeyGenerate*() function and sends this to the IdP. Note that the process of sending the decryption key must be performed through a secure channel, emphasized in the figure by the bold arrow.

3.2.3 User Registration

User registration with an IdP is illustrated in Figure 8, and is similar to organization registration. A user sends its identity credentials to the IdP. The IdP decides the procedure to fully establish one's identity, and may be different to the PKG's procedure (e.g., additional requirements, examinations, etc.). Upon completion, the IdP then determines the appropriate trans-organizational roles for the user according to their ToRBAC policies. The IdP sends the system parameters to the user (and has the option run the *PKGSetup*() function). Finally, the trans-organizational role (ID string and corresponding decryption key using the *Decrypt*() function) is sent to the user over a secure channel.

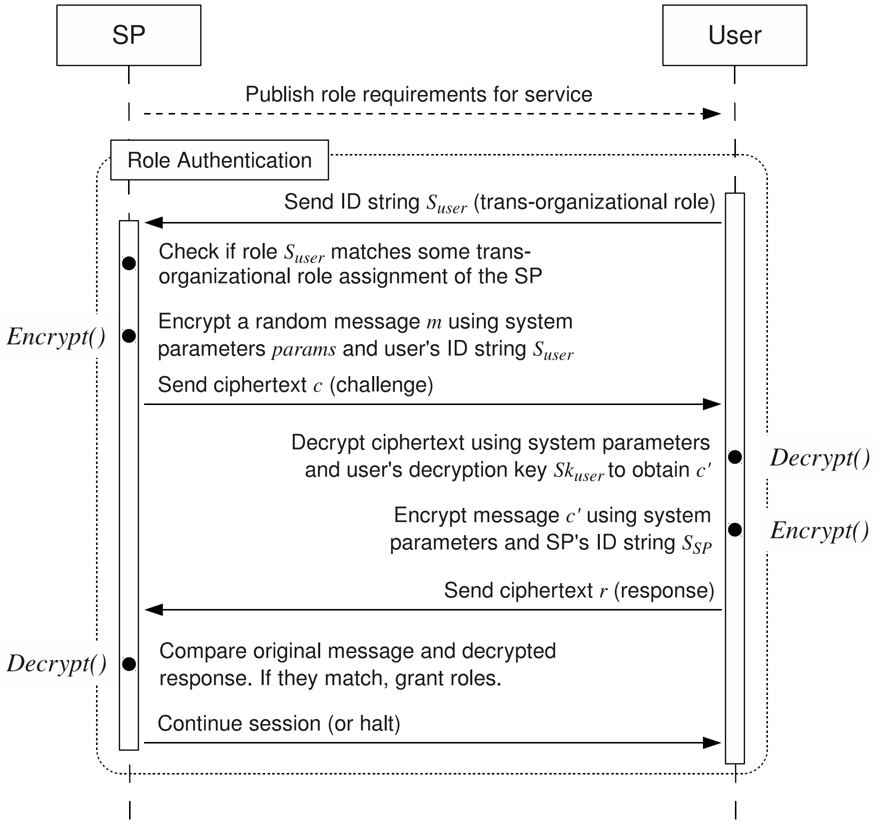

SP
User
Publish role requirements for service
Role Authentication
Send ID string S_{user} (trans-organizational role)
Check if role S_{user} matches some trans-organizational role assignment of the SP
Encrypt()
Encrypt a random message m using system parameters $params$ and user's ID string S_{user}
Send ciphertext c (challenge)
Decrypt ciphertext using system parameters and user's decryption key Sk_{user} to obtain c'
Decrypt()
Encrypt message c' using system parameters and SP's ID string S_{SP}
Encrypt()
Send ciphertext r (response)
Decrypt()
Compare original message and decrypted response. If they match, grant roles.
Continue session (or halt)

Figure 9. Sequence diagram of the challenge-response protocol between a user (prover) and an SP (verifier).

3.2.4 Role Authentication

A role authentication procedure is concerned with the verification of a user's asserted role. More specifically, it assures an SP that a role asserted by a user is indeed assigned by a particular IdP. In this scheme, role authentication is the challenge-response protocol illustrated in Figure 9. The protocol is the same in either local or trans-organizational sessions, but the following discussion uses notation for role authentication between an SP and a user. Also, SPs can have the choice of performing the protocol only once (user is permanently saved in the system, usually for recurring services) or each time the service is accessed (usually for one-time use cases, such as scanning Auto-IDs).

First, the SP publishes a list of its services and the roles required to access them. The user, wishing to access a specific service using a valid role, declares its role by sending the ID string S_{user}. The SP first checks the role against its list of trans-organizational role assignments if the SP interprets the role in their system. To complete the assertion a role using the ID string S_{user}, the user must prove its possession of the decryption key $SK_{S_{user}}$. The role authentication protocol is as follows:

1. The user sends the ID string S_{user} that satisfies the role requirements set forth by the SP.
2. SP checks if there is a valid pair in its list of trans-organizational role assignments that contains S_{user}, and continues the protocol if there is a match.
3. The SP generates a random message m and creates the challenge $c = Encrypt(params, m, S_{user})$. The challenge is sent to the user.
4. The user obtains the decrypted message $c' = Decrypt(params, c, SK_{S_{user}})$.
5. The decrypted message c' is then encrypted using the SP's ID to obtain the response $r = Encrypt(params, c', S_{SP})$. The response is sent to the SP.
6. The SP obtains the decrypted response $r' = Decrypt(params, r, SK_{SP})$. If $r' = m$, the user has proved possession of $SK_{S_{user}}$.

In this role authentication protocol, the participation of the PKG or other trusted third parties is not required. This facilitates distributed key authentication, which is a requirement for ToRBAC systems. Also, the protocol does not require message exchange through secure channels, since all messages are encrypted apart from the initial role ID string. Finally, the protocol can be used in a hybrid cryptosystem to make subsequent data exchanges efficient. Hybrid cryptosystems use a public-key encryption scheme (such as HIBE) for session key exchange, where the session key is generated from a symmetric-key encryption scheme.

3.3 Security Analysis of Role Authentication

In this section, the security of the role authentication protocol is analyzed. An intruder (or adversary) in the protocol may either be a dishonest user or dishonest SP who directly attacks the cryptography of the protocol, or manipulates intercepted messages sent through an insecure communication channel to its advantage. We say that a role authentication protocol for ToRBAC is secure if no intruder may assert a trans-organizational role that is not assigned to it by a particular IdP (dishonest user), or may act as a legitimate SP to any user (dishonest SP). Intruders can be registered users or SPs in the system

The analysis is presented in two parts. The security of HIBE, in which the protocol is grounded upon, is briefly outlined. Then, additional security properties based on challenge-response protocol manipulation are discussed.

3.3.1 Security properties based on HIBE

The conventional definition of chosen-ciphertext attacks must be strengthened for IBE systems [3]. In addition to public key and decryption queries, an adversary is allowed to issue private key extraction queries, where it can obtain the private key associated with an ID string of its choice. Security is then provided when such an adversary cannot break the encryption of any ID string other than for ones issued through the extraction queries. Furthermore, an adversary can choose its target ID string adaptively or nonadaptively. In adaptive attacks, the target is chosen from all available ID strings after making extraction queries. Conversely, a specific ID string is targeted in nonadaptive attacks (e.g., ID string of a rival).

Gentry and Silverberg [10] showed that HIBE schemes are semantically secure against combinations of these attacks. In their construction, the HIBE scheme uses a bilinear, non-degenerate, and computable pairing $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ over two cyclic groups $\mathbb{G}_1$ and $\mathbb{G}_2$ of some large prime number q. These groups are generated using the security parameter K in *RootSetup*(). The security of the HIBE scheme is then based on the following Bilinear Diffie-Hellman (BDH) Assumption: Let $P \in \mathbb{G}_1$ and $a, b, c \in \mathbb{Z}/q\mathbb{Z}$ be randomly chosen elements. Given $\mathbb{G}_1$, $\mathbb{G}_2$, $\hat{e}$, P aP, bP, and cP, the advantage of an adversary in computing $\hat{e}(P, P)^{abc}$ is negligible.

3.3.2 Security properties based on challenge-response protocol attacks

Challenge-response protocols can also be broken when an intruder eavesdrops while messages are exchanged. By altering the flow of messages, the intruder can gain an advantage without breaking the cryptography itself. Furthermore, a system cannot depend solely on intrusion detection mechanisms; some attacks involve passively acquiring information, and therefore avoiding detection before the actively attacking the protocol. Thus, the role authentication protocol in the basic scheme is modified for the security properties defined below.

Message Freshness. In a *replay attack*, the intruder can monitor protocol runs between a user and SP and save the exchanged messages. At some protocol run at later time, the intruder can intercept a request and send a stale message as a response. If there is no mechanism to verify if a message is stale, then the party may assume that it is indeed a valid response by the other party to its request.

A way to prevent replay attacks is to use an unpredictable and unique random value called a *nonce*. Roughly speaking, nonces are used as a "marker" to differentiate messages. To protect the nonces, it is encrypted along side the message to be exchanged (or may be the message itself). Consider the following message exchange:

$$\begin{array}{lll}
\text{Message 1} & \text{user} \rightarrow \text{SP} & : \quad S_{user}.n_{user} \\
\text{Message 2} & \text{SP} \rightarrow \text{user} & : \quad \{m.n_{user}.n_{SP}\}_{S_{user}} \\
\text{Message 3} & \text{user} \rightarrow \text{SP} & : \quad \{m.n_{SP}\}_{S_{SP}}
\end{array}$$

The user generates the nonce n_{user} and appends this to the ID string in Message 1. The SP appends this to the message m and its own nonce n_{SP} and encrypts $m.n_{user}.n_{SP}$ using the ID string S_{user}. When the user receives Message 2, it checks if the n_{user} is intact. The SP also checks n_{SP} in Message 3. If any nonce is changed, it indicates message tampering and the protocol run is halted. Nonces are only used one-time, although they can be archived for future lookup if it is practical. Note that unique identifiers and timestamps for each run of the protocol may also be used in conjunction with nonces.

Also, the message space of all messages must be sufficiently large such that it is highly unlikely to randomly generate the same message $m \in \mathcal{M}$ for two or more protocol runs within a reasonable amount of time. Hence, the security parameter

K in *RootSetup*(), which determines the size of message space, must be chosen carefully.

Two-way Role Authentication. Note that the role authentication protocol is one-way; it authenticates the user's possession of a role, but the validity of the SP is not challenged. An intruder may disguise itself as a trusted SP and therefore deceive the user to exchange information.

To address this, a user can issue a second challenge to confirm the possession of SK_{SP} by the SP. The user encrypts a message m' using S_{SP} and appends this to Message 3 (its response to the SP's initial challenge). If the other party is indeed the SP intended for role authentication and has SK_{SP}, then it must be able to decrypt the challenge and send back $\{m'\}_{S_{user}}$ as Message 4.

Message 1	user → SP	:	S_{user}
Message 2	SP → user	:	$\{m\}_{S_{user}}$
Message 3	user → SP	:	$\{m\}_{S_{SP}}.\{m'\}_{S_{SP}}$
Message 4	SP → user	:	$\{m'\}_{S_{user}}$

However, an intruder can bypass this by performing an *interleave attack* similar to the attack on the Needham-Schroeder protocol [14]. Consider an intruder that is a registered entity in the system and possesses the role pair $(S_{intruder}, SK_{intruder})$. The attack is conducted across two protocol runs α (compromised run between user and SP) and β (valid run between intruder and SP).

Message $\alpha.1$	user → intruder	:	S_{user}
Message $\beta.1$	intruder → SP	:	$S_{intruder}$
Message $\beta.2$	SP → intruder	:	$\{m\}_{S_{intruder}}$
Message $\alpha.2$	intruder⟨SP⟩ → user	:	$\{m\}_{S_{user}}$
Message $\alpha.3$	user → intruder⟨SP⟩	:	$\{m\}_{S_{SP}}.\{m'\}_{S_{SP}}$
Message $\beta.3$	intruder → SP	:	$\{m\}_{S_{SP}}.\{m'\}_{S_{SP}}$
Message $\beta.4$	SP → intruder	:	$\{m'\}_{S_{intruder}}$
Message $\alpha.4$	intruder⟨SP⟩ → user	:	$\{m'\}_{S_{user}}$

The intruder intercepts a role authentication request intended for the trusted SP at Message $\alpha.1$. It then starts a valid protocol run with the SP by sending its ID string $S_{intruder}$ in Message $\beta.1$. The SP sends the corresponding challenge to the intruder, which then decrypts and re-encrypts the message using S_{user}. The intruder pretends to be SP (denoted as intruder⟨SP⟩) and sends the challenge to the user. The user decrypts the challenge and sends its response (with the additional challenge) to the intruder. The intruder simply passes this to the SP, which decrypts the user's challenge. The SP returns the response and the intruder passes it to the user. Upon receiving a response that seems to have come directly from the SP, the user was successfully deceived by the intruder.

Protecting against the described attack is done by embedding the user's identity itself in the response to the SP's challenge:

$$\text{Message } \beta.3 \quad \text{intruder} \rightarrow \text{SP} \quad : \quad \{m.\text{``}user''\}_{S_{SP}}.\{m'\}_{S_{SP}}$$

The intruder, assuming it is unable to break the cryptography and alter the message, cannot send it to the SP because it will reveal an interleaved run of the protocol with the user. The SP will halt the session, in which case the intruder will fail to send the correct response to the user's challenge.

The modified protocol is synonymous to *two-way role authentication* since we can view the pair (SP, SK_{SP}) as the SP's trans-organizational role issued by the root PKG at ToRBAC system setup. In order to receive a role pair, the organization registration phase for SPs must follow the same procedure (and level of identity verification) as IdPs in Figure 7.

Entity Authentication. Finally, while the protocol preserves the integrity of the message m and assures the possession of the role, it has a vulnerability since it does not assure the identity of the end entity. For example, consider the following *relay attack* performed by the intruder by hijacking the communication channel:

Message 1	user → intruder	:	S_{user}
Message 2	intruder → SP	:	S_{user}
Message 3	SP → intruder	:	$\{m\}_{S_{user}}$
Message 4	intruder → user	:	$\{m\}_{S_{user}}$
Message 5	user → intruder	:	$\{m\}_{S_{SP}}$
Message 6	intruder → SP	:	$\{m\}_{S_{SP}}$

The intruder intercepts a role authentication request intended for the SP at

Message 1, and simply relays messages between the user and SP (i.e., no message injection). In this case, the intruder does not make its presence known at any point of the protocol – both user and SP are led to believe that they are interacting with each other. SP authenticates the role S_{user} which does not belong to the intruder, and therefore violates the protocol's notion of security. To address this, *entity authentication* must be performed throughout the protocol. This can be achieved by pre-verifying identity of the user, or on the level of the device (e.g., Transport Layer Security).

3.4 Discussion

The construction of the proposed scheme is suitable for trans-organizational RBAC for IoT systems. Distributed key management is possible because the hierarchical nature of HIBE allows IdPs to delegate role assignment duties, and role assignments in ToRBAC can be authenticated between the user and SP only. Also, the authentication of credentials is dynamic and multi-authority because can they be verified regardless of which specific IdP issued the role or the point in time they were issued, i.e., the user must only prove that they possess a minimum set of valid roles.

The two-way role authentication property allows IdPs to implement constraints on trans-organizational roles. An SP is required to declare its ID string in a role authentication request, during which it can be checked against a list of organizations allowed to interpret a role (if any). Thus, the scheme supports ToRBAC for single, federated, or completely trans-organizational use cases.

The use of ID strings with a standard format offers several advantages to key design. Standard role specifications can be published using the aforementioned ID string construction rules. In addition, contextual access is enabled by appending additional ID-tuples to an ID string. IdPs can then designate the context that must be satisfied to decrypt objects. For example, an Auto-ID may only be accessed in a certain location (`IdP.auto-id.store`), time period (`IdP.auto-id.weekday`), or device (`IdP.auto-id.mobile`). Context checking is performed on the scanning device; however, this requires that the scanner be tamper-resistant to implement correct context information.

HIBE can be extended for anonymous authentication of ID strings, such that some ID-tuples are represented as *"wildcards"* [1]. Wildcards, denoted in an ID string using an asterisk, hide the ID-tuple during the role authentication process. A user may omit certain levels of a role from an SP who does not explicitly request the information, especially when role hierarchies are deep (e.g., `NAIST.*.*.student`). Note that the first ID-tuple must not be wildcarded (ID string of IdP) for liability identification.

Another advantage is that ID strings can contain role and organization pairs similar to that of ROBAC. Information about the pairing can be made available in the naming conventions of the ID string itself. In this case, management complexity of trans-organizational RBAC does not increase significantly when large number of role and organization pairs are needed, an issue which can arise in ROBAC.

3.5 Conclusion

This chapter presented a scheme for ToRBAC systems. It was first established that to efficiently support IoT systems that have a large number of entities, reliance on a TTP for authentication procedures must be minimized. Therefore, the scheme used ID strings to represent roles as opposed to digital certificates used in PKI. It was shown that through this, public keys are verifiable using the identity of the user only, thereby limiting interactions with a TTP. Furthermore, flexible constructions of such ID strings were described. Ways to embed contextual access information into ID strings and enabling anonymous authentication to hide unnecessary role data were shown.

To securely support ID strings, Hierarchical Identity-Based Encryption was used as the public-key cryptosystem to implement the scheme, such as to setup the system, register entities, and authenticate role assignments. Moreover, the role authentication protocol was shown to be secure against cryptographic attacks based on the semantic security of HIBE. Also, the scheme is enhanced to support message freshness, two-way role authentication and entity authentication to address intruder models that attack the challenge-response protocol. It was shown that while the scheme is secure, its hierarchical nature also offers features such as distributed key management, and dynamic multi-authority credential authentication for efficient ToRBAC administration.

Future work on this area involves providing mechanisms for key revocation and controlled key escrow. These mechanisms are important features of access control but are currently not present in HIBE schemes. In addition, the cryptographic representation of keys must be studied to combine decryption keys for a single user in order to minimizes the size of a decryption key for users with multiple roles. This is especially important in IoT systems, where the data capacity of Auto-IDs are limited.

4. Error Control for High-density Monochrome 2D Barcodes

To be able to implement the Internet of Things, Auto-ID technologies must be able to hold a considerable amount of data, including cryptographic keys used for secure IoT protocols. In this section, we examine error control techniques in order to improve the robustness of monochrome 2D barcodes with high data density. Particularly, the goal is to analyze the effectiveness of LDPC codes compared to RS codes. Understanding these factors can deepen our knowledge of high-density barcodes and lead to design improvements for symbologies and their applications. Note that the symbology constructed in this study is not a proposal for an independent 2D barcode standard, but rather a mechanism to develop and test fundamental techniques for reliable high-density barcodes.

The "communication channel" defined by a barcode system is not a simple binary digital channel. Transmission of data through the channel is handled through the physical process of printing and scanning barcodes, and interpreting the scanned image to obtain the original data. The transmission therefore introduces additional errors in a non-conventional way, and the quality of the scanned image directly influences the study for appropriate countermeasures. Thus, in order to understand how to protect data in barcodes using error control techniques, the *channel model* exhibited by the symbology must first be investigated.

To enhance reading robustness, 2D barcode symbologies use *Reed-Solomon* (RS) codes [18] to encode data prior to generating the symbol. In recent years, it has been shown that well-designed *low-density parity check* (LDPC) codes [8] perform well compared to RS codes in many communication channels. A remarkable aspect of LDPC codes is that we can perform *soft-decision decoding* for LDPC codes with almost linear-time complexity. Soft-decision decoding is an algorithm for error correction in which inputs to the algorithm can have continuous values. It is more powerful than *hard-decision decoding* algorithms in which inputs are quantized into two level, but requires very large computational complexity in general. Soft-decision decoding was considered to be impractical for many years, but the sparse nature of LDPC codes allow efficient algorithms of soft-decision decoding to be implemented. LDPC codes with soft-decision decoding show a much better performance than conventional error-correcting codes, including RS codes [2, 4]. To compare the performance of RS codes and LDPC codes in high-density barcodes, several experiments were conducted using different parameters directly related to image quality and data density. Furthermore, LDPC-encoded barcodes with different interleaving parameters were subjected to physical damage in order to evaluate their robustness in real-world environments.

4.1 Related Work

Past studies on barcode capacity mainly focused on improving the *symbology* of 2D barcodes, i.e., enhancing its structure and processing methods to increase data capacity while retaining its compact size and portability. Some technologies investigate colored data cell designs in order to increase the amount of data represented per cell [17, 24]. Using colored cells increases the density of barcodes, but high-quality color printers are expensive in general, and the degradation of colors over time can make it difficult to retrieve the original data. It will be more versatile and cost-efficient to develop *monochrome 2D barcodes*, because the equipment used to produce monochrome symbols are generally less expensive to acquire and operate (such as reasonably-priced printers and scanners found in office or home environments), and symbols can be kept in storage medium that are cheaper and easier to maintain (such as paper products).

Another approach to improve the symbology of 2D barcodes is through increasing the *data density* of a barcode symbol. Data density is defined as the amount of data stored per area of a symbol; for instance, the number of cells printed per square millimeter (assuming that cells represent binary values). Yet, while a number of high-density symbologies have been proposed so far[3], their technical details are not available for open review and improvement. Furthermore, an inherent issue in storing large amounts of data in a physical format is its decreased robustness against errors. Data stored in high-density monochrome barcodes are susceptible to errors caused by printing and scanning hardware, or physical damage inflicted on the symbol or its storage medium. To the author's knowledge,

[3] Optar by Twibright Labs. (http://ronja.twibright.com/optar/, last accessed: Jul 2012) and Paperdisk technology by Cobblestone Software (http://www.paperdisk.com/, last accessed: Aug 2012)

although there are some barcode products in the industry that address this, no existing research is available that provides an analysis of high-density 2D barcode channels and suitable error control techniques. Thus, advances in barcodes would benefit from open studies on these topics.

4.2 Channel Model of High-Density 2D Barcodes

The system diagram of our proposed high-density barcode system is shown in Figure 10, though several components which have little relation to error control are not shown in the figure. Given the data to be stored in a barcode symbol, we first perform an encoding process of an error-correcting code. In this study, LDPC codes considered for this process are discussed in Section 4.3.1. The result of the encoding is then passed to the image construction process. Basically, data bits are represented as solid squares called *data cells*, where a white cell signifies the bit value ‘0’ and a black cell signifies the bit value ‘1’. Additionally, several techniques discussed in Sections 4.3.2, 4.3.3 and 4.3.4 are employed to attain robustness in the printed image. The image construction process determines the barcode image which is given to the printing device such as a laser printer.

To access the stored data, the printed barcode image is scanned using a flatbed scanner. Because the printed image is expected to be disturbed by several factors, which are discussed in Section 4.2.1, we first need to reconstruct the original image, and then need to estimate the value of each symbol (data bit) from the reconstructed image. In this study, the estimated value of a symbol is simply computed as the *ratio* of black pixels over the total number of pixels in an (estimated) cell area. These issues are addressed in the Section 4.4.1. The estimated symbols are given to the LDPC decoder (Section 4.4.2), and we finally obtain the estimated data. From the viewpoint of encoder/decoder of LDPC codes, these estimated values can be regarded as the output of the communication channel, while the binary (0 or 1) result of ECC encoder should be regarded as the channel input.

As Figure 10 shows, the error control mechanism consists of several components. To evaluate the effectiveness of each component, we focus on two empirical measures: *peak signal-to-noise ratio* (PSNR) for evaluating the image reconstruction process, and *bit-error ratio* (BER) [13] for evaluating the use of LDPC codes.

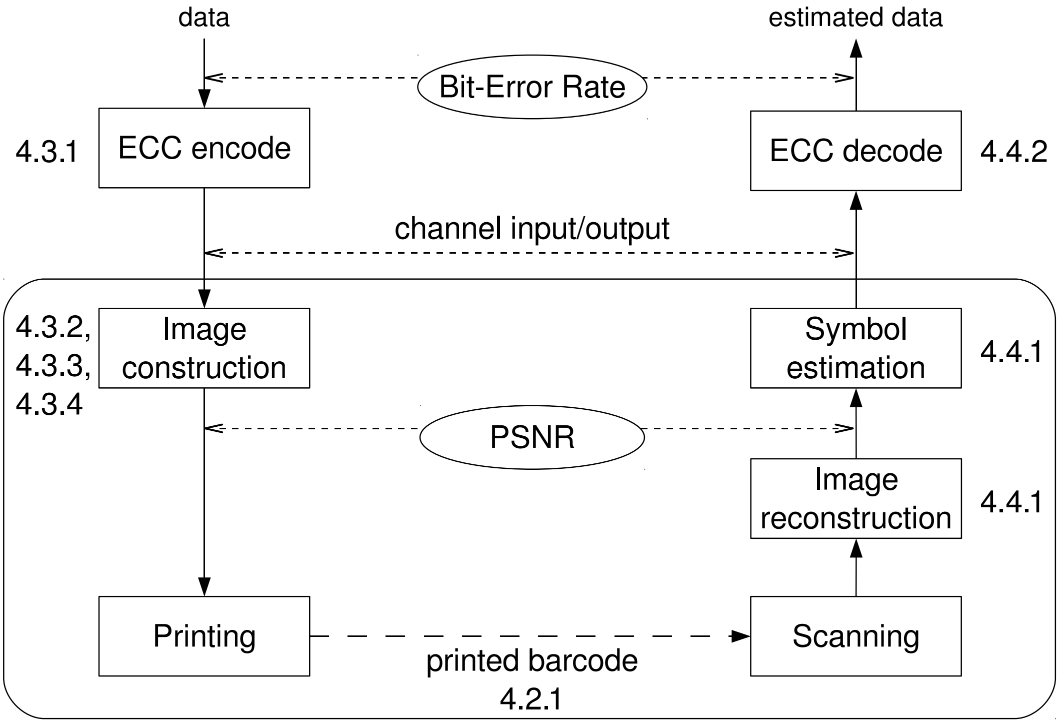


Figure 10. System diagram of the barcode system

1. Obviously, an LDPC code performs well if the input to the decoder is accurate. Because the input to the decoder is derived from the reconstructed image of the barcode, it is important to observe the quality of image reconstruction. To statistically measure quality of image reconstruction, we calculate the PSNR. First, the *mean squared error* (MSE), a statistical measure of error used to compare two $m \times n$ images, is computed. Given the image of data cells (channel input) and their corresponding scanned images (channel output), the MSE of data cell $c \in C$ is computed as the squared difference of the expected value $val(c)$ of the cell and each pixel of the sampling cell img_c; specifically, MSE is computed as

$$MSE(c) = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [val(c) - img_c(i,j)]^2 \qquad (1)$$

Given the MSE of all data cells in a symbol, the PSNR of the symbol is computed as

$$PSNR = 20 \cdot \log_{10}\left(\frac{MAX_{img}}{\sqrt{\sum_{i=0}^{|C|} MSE(i)}}\right) \tag{2}$$

where $MAX_{img} = 1.0$, the maximum value of ratio r.

2. The bit-error ratio or BER is a direct measure of the quality of data transmission, but we need to remark two things. First, the number of samples that can be generated through empirical testing (i.e., manual reproduction of barcodes) is limited versus the sample space of all barcodes that can be generated. Therefore, this paper appropriately uses the term "bit-error ratio" instead of bit-error rate, which measures the error probability of a communication channel. The rate can be obtained through a thorough simulation of the channel, which was not tested during this research.

   Second, the internal belief-propagation decoding algorithm for LDPC codes must be provided with the statistics of the communication channel. Through a preliminary experiment outlined in Appendix A, we found that the communication channel defined as above can be modeled as an *additive white Gaussian noise* (AWGN) channel, and the variance of the Gaussian distribution can be determined heuristically from the result of the preliminary experiment. In the preliminary experiment, we know the input and the output of the channel. We can collect samples O_{black} of ratios which corresponds to black cells and samples O_{white} of ratios which corresponds to white cells. The variance of each set is then calculated as

$$\sigma^2 = \int P(x)(x-\mu)^2 \,\mathrm{d}x \tag{3}$$

   where x is either in O_{black} or O_{white}, $P(x)$ is the probability distribution of x, and μ is the population mean of x.

4.2.1 Sources of Errors

We review the phenomena and factors which can cause problems in realizing a high-density barcode scheme. The factors can be classified into two types: *device-oriented factors* and *external factors*. Device-oriented factors are mainly caused

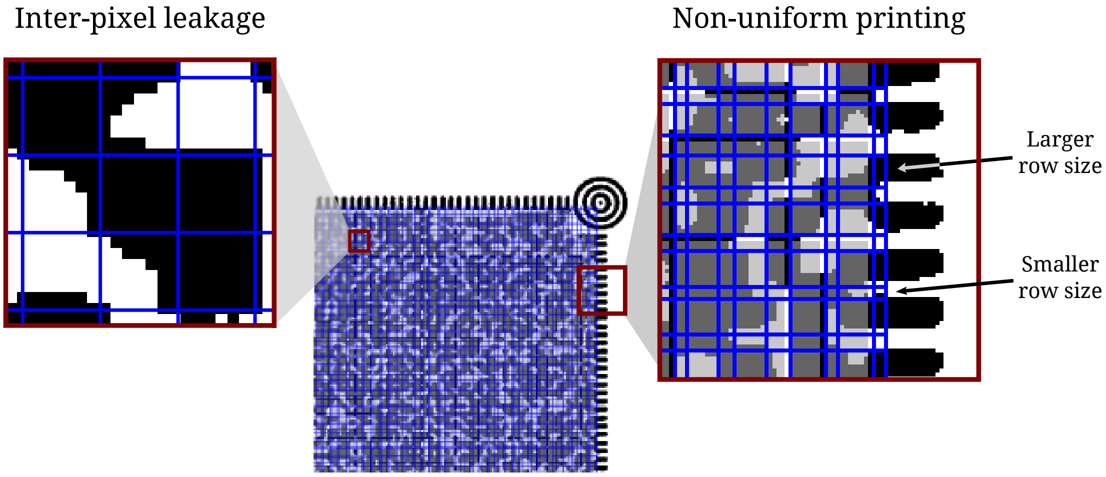


Figure 11. Example of a symbol containing inter-pixel leakage and non-uniform printing of rows.

by inaccuracies during printing and scanning barcodes using regular office equipment. These inaccuracies are not noticeable in regular use, but are significant if these devices are utilized to its performance limit. One such factor is called *inter-pixel leakage*. Data cells in high-density barcodes are printed in small sizes (less than 0.3×0.3 mm^2). As a result, the laser printer toner used to draw black cells splatter uncontrollably and blot neighboring white cells, thus becoming a major source of noise in the channel.

Another factor is called *non-uniform printing*, where cells along the same row were printed with similar heights, but cells in other rows were printed with different heights. This factor was also observed for the widths of columns. It is conjectured that this phenomenon is introduced by the mechanical constraints of the printer or scanner, and are not avoidable unless we use professional quality image setter. In the usual home and office environment, we need to expect that a printed barcode image is not as precise and uniform as stated in the specifications of the devices. Figure 11 shows an example of both factors.

External factors are caused by the environment where 2D barcodes are placed. Harsh conditions can introduce physical defects on printed symbols. For example, an ink blot or stain on the symbol affects a continuous sequence of data cells in neighboring rows and columns. Thus, if data is also stored in a sequential manner (e.g., left-to-right, top-to-bottom), a defect can introduce a consecutive stream of erroneous bits (known as a *burst error*). External factors are a problem for regular-sized barcode schemes, and it becomes more problematic if a scheme relies on higher resolutions of a scanned barcode image.

To mitigate these factors, we design a symbology that employs several error control techniques. Device-oriented factors are addressed using a margin factor parameter and a tweaked design of the timing pattern which surrounds data area. To cope with external factors, we developed a strategy for interleaving which stores data in a non-contiguous way. This creates a more uniform distribution of errors across codewords when a symbol is partially damaged. Details of these techniques are discussed in the next section.

Despite these countermeasures, it is still difficult to accurately determine whether a scanned data cell is black or white. To be able to maximize the robustness of a symbol, we investigate the use of powerful LDPC codes with soft-decision decoding, instead of the conventional RS codes with hard-decision decoding.

4.3 Encoding and Printing

Conventional 2D barcodes employ symbologies which are good for fast reading. However, because we are designing a symbology which increases data density, the focus is to safely accommodate as many data cells as possible in a given area. The following subsections describe the encoding and printing steps to create a symbol.

4.3.1 Encoding

First, the input data to be stored in a barcode symbol is encoded using error-correcting codes. Most 2D barcodes use RS codes for error correction, which are non-binary cyclic error-correcting codes. RS codes adds t check symbols to the original data, and upon decoding it can detect up to t random symbol errors or erasures, and correct up to $\lfloor t/2 \rfloor$ symbols.

For comparison, this study considers the family of LDPC codes designed for the IEEE 802.16e standard (also known as mobile WiMAX). Using these codes are advantageous since they have smaller complexity for encoding, compared to other classes of LDPC codes. In general, the encoding operation of an LDPC code requires quadratic-order complexity in the code length; however, the IEEE codes defined in the standard are designed so that they have *quasi-cyclic* structure, which enables the realization a linear-order encoding algorithm. Another advantage of these codes is that the code parameters can be changed in a flexible manner. The standard defines several classes of LDPC codes with code rates 1/2, 2/3, 3/4 and 5/6, and code length ranges from 576 to 2304 bits. These parameters have a strong relation to the efficiency and the error-correcting capability of the code [15]. We note however that we do not have to restrict ourselves to this family of LDPC codes. The techniques developed in this study can be used for any LDPC codes.

4.3.2 Data Cells and Data Area

A monochrome[4] 2D barcode stores codewords in data cells arranged inside a 25.4×25.4 mm^2 space or *data area*. We can consider larger data area spaces, though we fix the size in this study to make the following discussion simple and clear. Data cells inside the data area are arranged in a $dim \times dim$ matrix, where dim is an integer called the *dimension* parameter. Increasing the dimension parameter of a fixed-size data area has two effects on the symbol:

1. **Data capacity and density**: The number of data cells available in the data area[5] is increased. This is computed as slightly less than dim^2 because of the overhead introduced by the symbology. Because the size of the data area is fixed, data capacity can be regarded as the density of data: dim^2 cells per square inch or $(dim/25.4)^2$ cells per square mm.

2. **Cell size** or printing size: The cell size of a data cell must be reduced in order to increase the data density of the symbol. Cell size is computed $(25.4/dim) \times (25.4/dim)$ mm^2.

[4] The term "monochrome" means that barcodes are printed and scanned as black-and-white images. Although grayscale images contain more information that may assist in barcode detection, producing small data cells in grayscale generate too much noise in the channel.

[5] This definition does not take into account other techniques which would increase the total data capacity of a barcode symbol (such as data compression).

Table 2 lists the relation of dimension, data capacity and density, and cell size.

Table 2. Data capacity, density, and printing size of a cell for a symbol with dimension *dim*

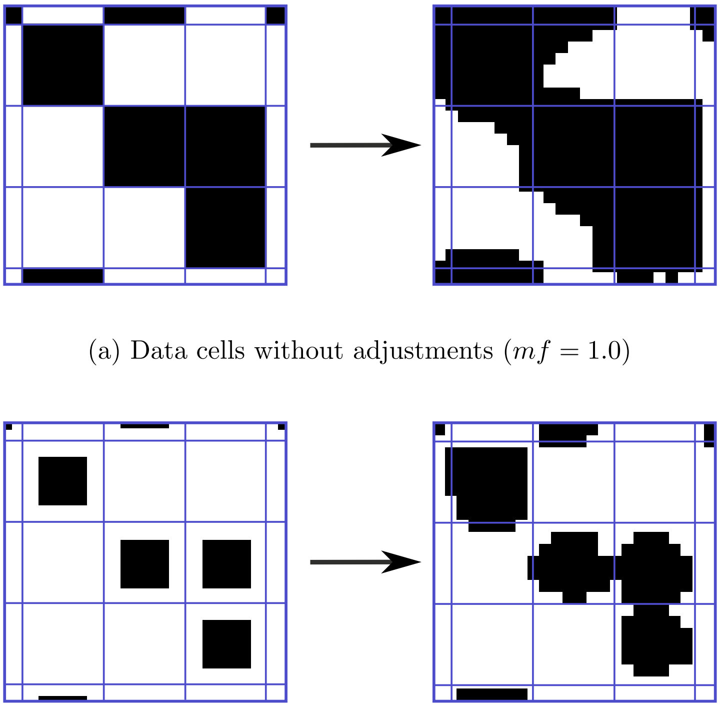
dim	Capacity (no. of cells)	Density (cells / mm^2)	Cell size (mm^2)
57	3,053	5.04	0.446
67	4,293	6.96	0.379
77	5,733	9.19	0.330
87	7,373	11.73	0.292
97	9,213	14.58	0.262
107	11,253	17.75	0.237
117	13,493	21.22	0.217

To cope with inter-pixel leakage, the printing size of black cells are reduced by a certain *margin factor* relative to the size of the data cell. Figure 12 shows data areas printed with a margin factor value of $mf = 1.0$ and $mf = 0.6$. Notice how black cells printed with $mf = 0.6$ contain a white border which acts as a buffer for inter-pixel leakage. The white cells in this case have less noise generated by adjacent black cells. Thus, the data area is more distinguishable than the data area printed with $mf = 1.0$. The optimum choice of margin factor depends on the size of the cells and the resolution of the printer. It is expected that the optimum margin factor is determined in advance for the environment where barcode images are produced.

4.3.3 Finder and Timing Patterns

A set of *finder patterns* is used to isolate the barcode symbol from a scanned image, and a set of *timing patterns* is used to estimate the size and location of data cells. Figure 13(a) shows the individual design elements of the high-density symbology.

Finder patterns are placed on the four corners of the data area. It consists of three black rings co-centric to the corner of the data area, marking the corner with a single black cell. A *quiet zone* of white cells is placed underneath the



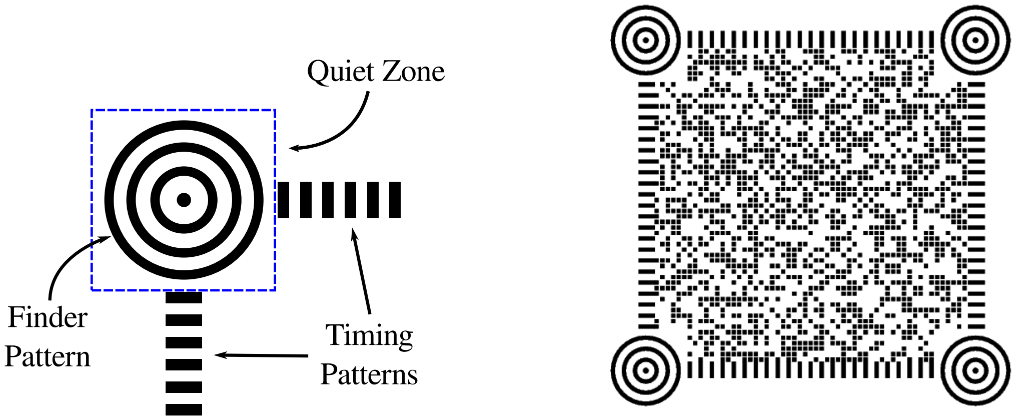
(a) Data cells without adjustments ($mf = 1.0$)

(b) Data cells with margin factor ($mf = 0.6$)

Figure 12. Effect of inter-pixel leakage on 0.237 × 0.237 mm^2 data cells.

finder pattern to improve detection accuracy.

The timing pattern is a consecutive series of modules located around the four edges of the data area. A timing pattern connects two finder patterns, with each module alternating between white and black cells. To increase the detection reliability, each timing pattern module is made up of three connected black or white cells. Timing patterns are also printed on the same row or column as data cells. Hence, timing pattern modules are also subject to non-uniform printing. This is advantageous because the separation of data cells (indicated by the blue lines in Figure 11) also adjusts to the non-uniform printing size of the rows and columns, and thus aiding the detection of data cells.



(a) Finder pattern, quiet zone and two timing patterns.

(b) Example of a symbol with a data area.

Figure 13. Design elements and a complete symbol generated by the symbology.

4.3.4 Interleaving

Finally, before a symbol is printed on a sheet of paper, the data cells inside the data area are interleaved. The interleaving technique designed for this symbology is illustrated in Figure 14. Given the *interleave level* (denoted as lvl) of the symbol, the data area is first partitioned into lvl^2 sub-divisions or *zones*. These zones contain an equal number of data cells except for zones which overlap quiet zones. The cell c_i, which represents the i-th bit of data, is then written in the $(i \bmod lvl^2) + 1$ zone. In other words, data cells are placed into zones one by one, starting from zone 1 to lvl^2. This process repeats until all data cells have been stored.

When data cells are inserted into zones, the interleave level affects the distance between the cells. When there is no interleaving, the distance between two cells is 1 since they are stored sequentially. For symbols with interleaving, data cells are stored apart from each other with a computed distance

$$dist(dim, lvl) = \lfloor dim/lvl \rfloor \tag{4}$$

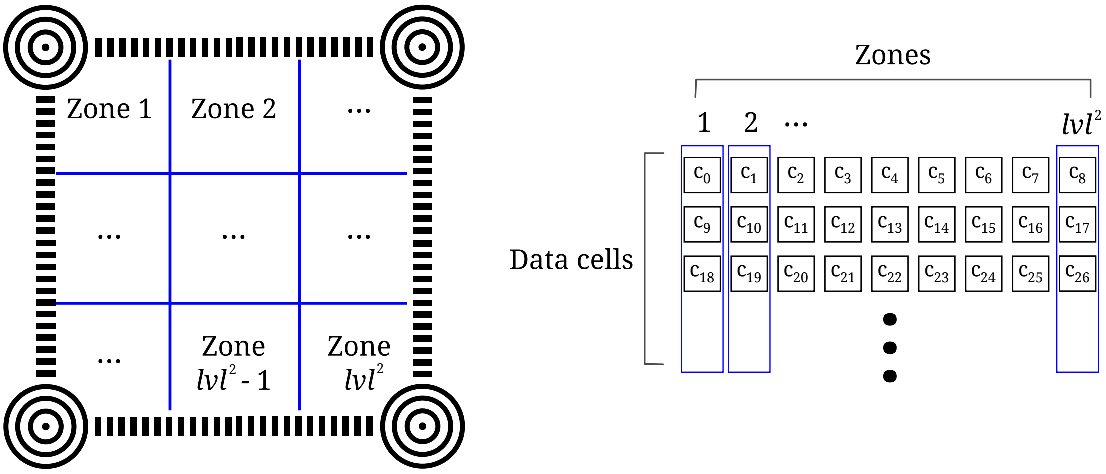

Zone 1
Zone 2
...
...
...
...
...
Zone lvl^2 - 1
Zone lvl^2
Zones
1
2
...
lvl^2
Data cells
c_0 c_1 c_2 c_3 c_4 c_5 c_6 c_7 c_8
c_9 c_{10} c_{11} c_{12} c_{13} c_{14} c_{15} c_{16} c_{17}
c_{18} c_{19} c_{20} c_{21} c_{22} c_{23} c_{24} c_{25} c_{26}

Figure 14. Example of interleaving using interleave level $lvl = 3$.

4.4 Scanning and Decoding

4.4.1 Symbol Processing

When data is needed from a barcode, the sheet of paper is scanned using a flatbed scanner and codewords are read from the symbol. We refer to this process as *symbol processing*, which involves the following steps:

1. Barcode symbols (if any) are searched in the scanned image. The finder patterns of a symbol are located using a basic template matching algorithm [22]. The centers of all finder patterns are then computed.

2. Lines connecting the centers of adjacent finder patterns are connected, and the resulting closed rectangle is masked. This enhances the detection of timing patterns in the following step.

3. The lines connecting adjacent finder patterns are scanned through pixel by pixel. The path each line passes through is also the location of a timing pattern. When the value of the pixel changes from white to black, this pixel is marked as a *transition point*.

4. Transition points from opposite timing patterns are connected, forming a grid of *sampling cells*.

5. The ratio r of black pixels in each cell is determined. From the grid of sampling cells computed in (4), we can determine the set P of pixels which are used to represent one particular cell. The ratio r of this cell is simply the number of black pixels in P over the total number of pixels in P.

6. The ratio r obtained from each sampling cell is mapped to a *soft value* using the function $f(r) = -(2r - 1)$. Soft values are de-interleaved and grouped into codewords.

Steps 1 to 4 constitute the "image reconstruction" process in Figure 10, while steps 5 and 6 constitute the "symbol estimation".

4.4.2 Decoding

Codewords obtained from symbol processing are then passed to a decoder program. If the data is encoded with RS codes, the soft values obtained from Step 6 of symbol processing are quantized into two level by straight-forward thresholding (e.g., '0' for soft values greater than 0, '1' otherwise). Afterwards, hard-decision decoding for RS codes [26] is performed on the discrete values.

If the data is encoded with LDPC codes, decoding is performed by using a belief-propagation algorithm [16]. In this algorithm, we consider representing the mathematical structure of the code with a bipartite graph whose incident matrix coincides with the check matrix of the code. The nodes of the bipartite graph are grouped to *variable nodes* and *check nodes*. A variable node receives information (the soft value) from neighbor check nodes, and it attempts to estimate which symbol ('0' or '1' bit) has been transmitted. During the estimation, the statistical information of the communication channel, such as the variance of the Gaussian channel, is considered to derive various probabilities. A check node receives the estimated symbols from neighbor variable nodes, monitors parity constraints, and gives variable nodes suggestions for the transmitted symbol. The accuracy of the estimation improves as nodes exchange messages iteratively. Refer to literature [16] for the detailed description of the belief-propagation decoding algorithm.

4.5 Evaluation and Results

The following experiments were designed to determine the effects of data density on the channel, and evaluate the performance of the error control mechanisms in the symbology. All experiments used the same office equipment and symbol processing steps for testing. In both the printing and scanning process, monochrome color settings were used. The general steps for experiments are as follows:

1. First, input data and parameters were passed to the ECC encoder followed by the image construction process, both written in the C programming language. The program then generated a sample set of symbols.
2. The sample set was printed on a sheet of plain white bond paper using a Canon LBP3410 laser printer with the default settings.
3. The sheet of paper was scanned using an Epson GT-F720 flatbed scanner at 720 dpi with monochrome settings.
4. Finally, the scanned image was passed to the image reconstruction process and subsequent modules, which are also written in C.

In the image reconstruction, we used conventional algorithms for image processing. Refinement of the image processing algorithms can improve the results, but this is not investigated in this study currently.

4.5.1 Test 1: Effect of Data Density on Channel

As noted earlier, the accuracy of estimating cell values is dependent on the data density of the barcode. To test this, 35 sets of symbols with different symbology parameters were processed. Each sample set consisted of five barcode symbols with random data cell values. The set was then printed with a combination of dimension and margin factor values listed in Table 3. After symbol processing, the PSNR of each combination of symbology parameters was graphed and analyzed to determine the overall accuracy of cell value estimations.

The PSNR results of the test are presented in Figure 15. PSNR values for $mf = 0.8$, 0.9 and 1.0 showed a decreasing trend as data density increased. This

Table 3. Input parameters used for Test 1.

Parameter	Value
Dimension dim	57, 67, 77, 87, 97, 107, 117
Margin factor mf	0.6, 0.7, 0.8, 0.9, 1.0
Encoding	None
Interleave level lvl	1

is in line with the fact that as data cells are printed closer to each other, inter-pixel leakage of black cells affect neighboring white cells and leads to reduced channel quality.

For data cells with lower data densities and $mf = 0.6$ or 0.7, the printing size of black cells were small compared to the actual cell size (e.g., 0.268 mm^2 and 0.446 mm^2, respectively for $dim = 57$, $mf = 0.6$). Hence, the effects of inter-pixel leakage were not enough to compensate for the remaining space in the data cell. This led to lower soft values for black cells and lower PSNR values overall. The PSNR values improved when data density was increased, since sampling cells were more densely packed. In this case, the soft values stabilized and became proportional relative to the expected values. PSNR values for densities beyond 370.4 showed a decreasing trend, due to the increased leakage of black cells on neighboring white cells.

4.5.2 Test 2: Performance of RS Codes and LDPC Codes

The second experiment evaluates the error correction performance of RS and LDPC codes in the symbology. A sample set without error-correcting codes was also tested to serve as a benchmark of performance. To measure error correction performance, the BER of each sample set was analyzed, where

$$BER = \frac{\text{*Number of erroneous bits after decoding}}{\text{*Total number of bits of input data}} \tag{5}$$

BER results for each sample set were then gathered and analyzed. Note that RS and LDPC decoder programs were modified to return the final state of the data word, whether or not the the received codeword was decoded correctly.

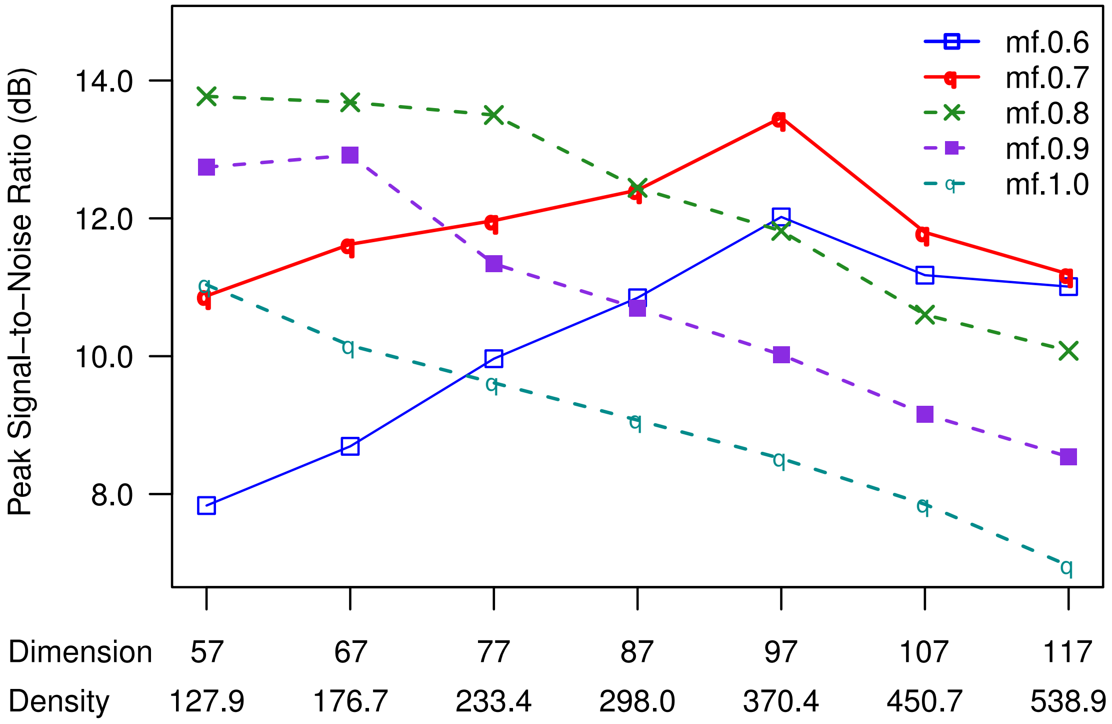


Figure 15. Peak signal-to-noise ratio of symbols using parameters listed in Table 3.

This modification allows for an accurate BER calculation. For symbols with not encoded using an error-correction code, BER is simply the number of erroneous bits after symbol processing over the total number of bits.

To conduct the experiment, 10 sets of symbols were generated using parameters listed in Table 4. Each set contained 24 barcode symbols with data obtained from an input file. The RS encoder used a $(255, 211)$ code, while the LDPC encoder used a $(6, 5)$ code. In this test, symbols were not subjected to physical damage in order to assess performance against errors caused by device-oriented factors only.

The preliminary experiment in Appendix A shows that symbol processing fails for parameter values above $dim = 127$ and $mf = 0.6$, and this seems to be the performance limit of the considered symbology. At this limit, the noise of our channel is well approximated as the AWGN channel with the variance value $\sigma^2 = 0.05637$. The variance can become slightly smaller for smaller choices of

Table 4. Input parameters used for Test 2.

Parameter	Value
Dimension dim	97, 107
Margin factor mf	0.6, 0.7, 0.8, 0.9, 1.0
Encoding	None, RS, LDPC
Interleave level lvl	1

dimension values, because the channel disturbance is mild if the dimension is small. It is ideal if we could estimate the variance from the scanned image in an adaptive manner, though, that kind of channel estimation is another challenging task. To get around this issue, we used the constant variance $\sigma^2 = 0.05637$ for all the evaluations in Test 2 and 3, because a barcode image may be subjected to external damage as well (as investigated in Test 3). Thus, assuming a worse channel model (with higher variance) than expected seems to be a reasonable direction to mitigate unpredictable external factors.

Table 6 shows the results of BER analysis for sample sets $dim = 97$ and $dim = 107$. The number of data bits tested are listed in Table 5. Overall, sample sets with error-correcting codes have lower BER values than for the set without encoding. This shows that both codes were effective in reducing the errors in this channel. Furthermore, the BER of symbols for $dim = 97$ were lower than for $dim = 107$. This was expected since the PSNR values for $dim = 107$ were lower. In general, all BER values exhibited the same trend as PSNR values with respect to the margin factor – this can be attributed to the decreased channel quality when margin factors are increased, as observed in Test 1.

Table 5. Number of data bits considered in BER analysis for Test 2.

Encoding	No. of data bits	
	$dim = 97$	$dim = 107$
None	221,112	270,072
RS codes	160,360	197,496
LDPC codes	136,320	180,480

Even though values in Table 6 are not very accurate due to limited number

Table 6. BER analysis of symbols using parameters listed in Table 4.

mf	$dim = 97$			$dim = 107$		
	None	RS	LDPC	None	RS	LDPC
0.6	34.971%	0.013%	0.000%	39.734%	0.094%	0.000%
0.7	34.931%	0.017%	0.000%	39.810%	0.069%	0.084%
0.8	34.931%	0.750%	0.000%	40.402%	2.447%	1.792%
0.9	35.222%	4.086%	1.513%	41.150%	5.021%	4.658%
1.0	35.571%	6.280%	6.916%	42.514%	10.549%	11.188%

of samples, LDPC codes generally yielded lower error ratios than RS codes in both dimensions. This is because the accuracy of the estimated data cell value deteriorated when thresholded from a soft value into a discrete value; thus RS codes were not able to perform as well as LDPC codes. LDPC codes reported low BER (less than 0.05%) when PSNR values were greater than 11.176 dB. Both coding schemes performed poorly (BER > 5.0%) when symbols had a PSNR value less than 9.158 dB.

Finally, Table 7 reports the word-error ratio (WER) for dim = 97 (with 95 codewords for RS codes and 71 codewords for LDPC codes) and dim = 107 (with 117 codewords for RS codes and 94 codewords for LDPC codes). To obtain the WER, codewords are decoded into datawords, which were then compared with the original data prior to encoding, where

$$WER = \frac{\text{*Number of erroneous datawords after decoding}}{\text{*Total number of datawords}} \tag{6}$$

From the results, we can conclude that bit errors were scattered across all codewords embedded in barcodes. This was expected because data cells in any part of the symbol are susceptible to inter-pixel leakage. Also note that in these tests, all codewords were successfully decoded. Thus, the reported errors indicate that some codewords were decoded to datawords different from the original input data, and the reported WER reflects codewords that were incorrectly decoded into another valid dataword.

Table 7. WER analysis of symbols using parameters listed in Table 4 (except non-encoded symbols).

mf	$dim = 97$		$dim = 107$	
	RS	LDPC	RS	LDPC
0.6	1.053%	0.000%	5.128%	0.000%
0.7	1.053%	0.000%	3.419%	2.128%
0.8	38.947%	0.000%	92.308%	46.809%
0.9	100.000%	67.606%	100.000%	95.745%
1.0	100.000%	100.000%	100.000%	100.000%

4.5.3 Test 3: Performance of Interleaving

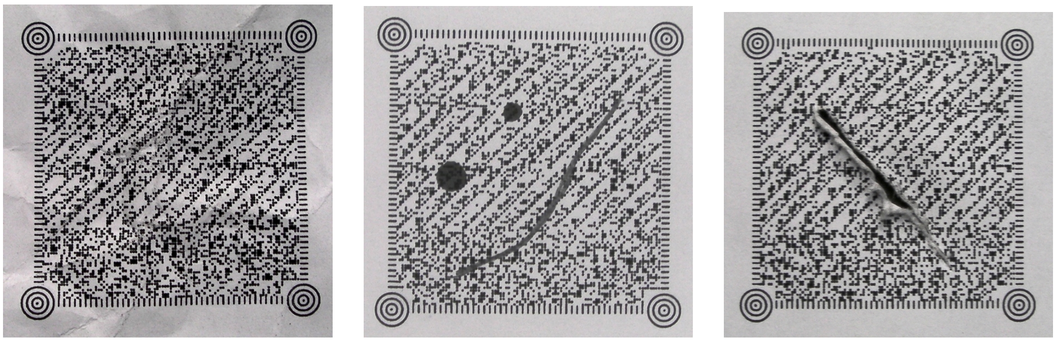
To evaluate the symbology's robustness against burst errors, 15 sets of symbols with different symbology parameters listed in Table 8 were printed. Interleave levels were varied to $lvl = 1$ (no interleaving), $lvl = 3$ and $lvl = 5$, while the dimension parameter was kept constant. Each symbol in a set was then subjected to one of three types of physical damage which normally occur to a sheet of paper in home and office environments, as shown in Figure 16. After symbol processing, the BER results were obtained and conclusions were derived from the results.

Table 8. Input parameters used for Test 3.

Parameter	Value
Dimension dim	97
Margin factor mf	0.6, 0.7, 0.8, 0.9, 1.0
Encoding	LDPC
Interleave level lvl	1, 3, 5

The BER analysis for damaged symbols are shown in Table 9. Overall, the number of errors detected in this test were higher than in Test 2 because of the introduction of burst errors. Also, the trend of BER for all interleave levels performed similar to the results in Test 2, where increasing the margin factor (hence, decreasing PSNR) had a negative effect on the performance.

For comparison, consider symbols which did not use interleaving (i.e., $lvl = 1$)



(a) Folding / Crumpling (b) Markings (c) Tearing

Figure 16. Types of damage to a symbol.

Table 9. BER analysis of damaged symbols using parameters listed in Table 8 with varying interleave levels.

mf	Interleave level lvl		
	1	3	5
0.6	1.070%	0.344%	3.736%
0.7	3.238%	1.673%	1.681%
0.8	4.382%	3.397%	4.093%
0.9	8.298%	6.147%	8.128%
1.0	11.845%	11.988%	14.594%

as a benchmark of performance. Based on this, the BER results improved when the interleave level was increased to $lvl = 3$. In these symbols, data was stored in a non-contiguous way and therefore the burst errors due to damage was decreased. Intuitively, the performance should further increase when the interleave level is also increased, but the BER results for $lvl = 5$ show that this is not the case. This is because the distance between cells was decreased from $dist(97, 3) = 32$ to $dist(97, 5) = 19$ (Equation 4). If the distance between two sequential data cells is lower, there is a higher chance that physical damage affects more sequential data cells.

Finally, note that this test focuses on the robustness of the high-density channel, hence physical damage was inflicted on the data area only and not to the finder pattern and timing patterns of the symbol. This is due to the fact that the current version of the symbology implements error correction mechanisms for the data cells only. Therefore, finder and timing patterns are sensitive to damage.

4.6 Conclusion

In this chapter, we investigated techniques for error control in a high-density 2D monochrome barcode. A high-density symbology was defined, and its communication channel was modelled. The performance of error correction mechanisms were then tested with different symbology parameters.

The study showed that some characteristics of laser printing technology introduce inaccuracies to high-density barcodes. The communication channel of the symbology is an AWGN channel, where the channel quality of a symbol can be evaluated based on its PSNR value. Some symbology elements such as margin factor and timing pattern design are effective for controlling errors. Also, LDPC codes show a better error correction performance compared to Reed-Solomon codes. Finally, the interleaving strategy of the symbology is a useful technique to mitigate burst errors caused by physical damage. These symbology improvements and error control techniques showed possible directions to design 2D barcodes with increased data density compared to conventional symbologies, which can then be used for as an alternative to RFIDs for IoT systems.

Future work for this study includes improving of the robustness of finder patterns and timing patterns, and the dynamic computation of AWGN variance for LDPC decoding; that is, the variance of a symbol is computed upon scanning the symbol - thereby taking into account the physical condition of the symbol - to improve decoding performance.

5. Conclusion

This dissertation introduced access control models with a secure scheme and improvements to Auto-IDs to realize Trans-organizational RBAC for the "Internet of Things". A family of models were formalized using a traditional RBAC model as reference. The models, in addition to role hierarchy and constraint properties, support trans-organizational role authentication within and across organizations which can be performed sans joining federations. It was shown that the models are scalable with respect to the number of participating organizations.

A scheme for ToRBAC was designed using arbitrary identity strings to represent trans-organizational roles. Identity strings used Hierarchical Identity-Based Encryption as its security mechanism, and steps of the scheme were described. The role authentication protocol was shown to be secure against attacks on its cryptography, and additional security properties were constructed to address various vulnerabilities of a challenge-response protocol. By combining the flexibility of identity strings with the security properties, it was shown that the scheme based on HIBE can be used to implement efficient ToRBAC systems as opposed to conventional PKI structures.

Finally, the data density and robustness of 2D monochrome barcodes were enhanced in order to store cryptographic keys required for the ToRBAC scheme. It was shown that the communication channel of 2D barcodes can be modeled as an additive white Gaussian noise channel with the variance $\sigma = 0.5637$ at the performance limit of the symbology. Error control techniques were then investigated alongside the physical design of 2D barcodes to produce a symbology that adapts to irregularities caused by regular printing and scanning technology. Tests showed that the image quality of 2D barcodes are dependent on the density of data cells, and barcodes with equivalent image quality of ≥ 11.176 dB and protected by Low-Density Parity-Check codes are robust against errors introduced by the channel and physical damage ($< 0.05\%$ bit-error ratio).

References

[1] M. Abdalla, J. Birkett, D. Catalano, A. W. Dent, J. Malone-Lee, G. Neven, J. C. N. Schuldt, and N. P. Smart. Wildcarded identity-based encryption. *Journal of Cryptology*, 24(1):42–82, February 2011.

[2] N. Andreadou, C. Assimakopoulos, and F. N. Pavlidou. Performance evaluation of LDPC codes on PLC channel compared to other coding schemes. In *IEEE International Symposium on Power Line Communications and Its Applications (ISPLC '07).*, pages 296–301, March 2007.

[3] D. Boneh and M. Franklin. Identity-based encryption from the Weil pairing. In J. Kilian, editor, *Advances in Cryptology – CRYPTO 2001*, volume 2139 of *Lecture Notes in Computer Science*, pages 213–229. Springer, 2001.

[4] J. Chen, L. Wang, and Y. Li. Performance comparison between non-binary LDPC codes and Reed-Solomon codes over noise bursts channels. In *Proceedings of the 2005 International Conference on Communications, Circuits and Systems*, volume 1, pages 1–4, May 2005.

[5] S. De Capitani di Vimercati and P. Samarati. Access control in federated systems. In *Proceedings of the 1996 Workshop on New Security Paradigms*, pages 87–99, New York, NY, USA, 1996. ACM.

[6] D. F. Ferraiolo, R. Sandhu, S. Gavrila, D. R. Kuhn, and R. Chandramouli. Proposed NIST standard for role-based access control. *ACM Transactions on Information and System Security (TISSEC)*, 4(3):224–274, August 2001.

[7] J. R. Fu, C. K. Farn, and W. P. Chao. Acceptance of electronic tax filing: A study of taxpayer intentions. *Information & Management*, 43(1):109–126, 2006.

[8] R. Gallager. Low-density parity-check codes. *IEEE Transactions on Information Theory*, 8(1):21–28, January 1962.

[9] J. Gao, V. Kulkarni, H. Ranavat, L. Chang, and H. Mei. A 2D barcode-based mobile payment system. In *Proceedings of the 2009 Third International*

Conference on Multimedia and Ubiquitous Engineering, MUE '09, pages 320–329. IEEE Computer Society, 2009.

[10] C. Gentry and A. Silverberg. Hierarchical id-based cryptography. In Yuliang Zheng, editor, *Advances in Cryptology - ASIACRYPT 2002*, volume 2501 of *Lecture Notes in Computer Science*, pages 149–155. Springer, 2002.

[11] A. D. Keromytis and J. M. Smith. Requirements for scalable access control and security management architectures. *ACM Transactions on Internet Technology (TOIT)*, 7(2), May 2007.

[12] E. A. Lee. CPS foundations. In S. Sapatnekar, editor, *Proceedings of the 47th Design Automation Conference*, DAC '10, pages 737–742, New York, NY, USA, 2010. ACM.

[13] S. Lin and D. J. Costello. *Error Control Coding: Fundamentals and Applications*. Prentice Hall, Upper Saddle River, 2nd edition, 2003.

[14] G. Lowe. Breaking and fixing the Needham-Schroeder public-key protocol using FDR. In T. Margaria and B. Steffen, editors, *Tools and Algorithms for the Construction and Analysis of Systems - TACAS '96*, volume 1055 of *Lecture Notes in Computer Science*, pages 147–166. Springer, 1996.

[15] M. G. Luby, M. Mitzenmacher, M. A. Shokrollahi, and D. A. Spielman. Improved low-density parity-check codes using irregular graphs. *IEEE Transactions on Information Theory*, 47(2):585–598, February 2001.

[16] D. J. C. MacKay. Good error correcting codes based on very sparse matrices. *IEEE Transactions on Information Theory*, 45(2):399–431, 1999.

[17] Sala P. and G. Jancke. Robust segmentation, registration, and decoding of tri-2D high density color barcode. Technical Report MSR-TR-2006-119, Microsoft Research, Redmond, WA, September 2006.

[18] I. S. Reed and G. Solomon. Polynomial codes over certain finite fields. *Journal of the Society for Industrial and Applied Mathematics*, 8(2):300–304, 1960.

[19] S. Ruohomaa and L. Kutvonen. Trust Management Survey. In P. Herrmann, V. Issarny, and S. Shiu, editors, *Trust Management – iTrust 2005*, volume 3477 of *Lecture Notes in Computer Science*, pages 77–92. Springer, 2005.

[20] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman. Role-based access control models. *Computer*, 29(2):38–47, 1996.

[21] A. Shamir. Identity-based cryptosystems and signature schemes. In G. Blakley and D. Chaum, editors, *Advances in Cryptology – CRYPTO 1985*, volume 196 of *Lecture Notes in Computer Science*, pages 47–53. Springer, 1985.

[22] M. Sonka, V. Hlavac, and R. Boyle. *Image Processing, Analysis, and Machine Vision.* PWS Publishing, Pacific Grove, 2nd edition, 1999.

[23] H. Sundmaeker, P. Guillemin, P. Friess, and S. Woelfflé. *Vision and challenges for realising the Internet of Things.* European Commission – Information Society and Media, March 2010.

[24] K. Tan, D. Chai, and H. Kato. *Barcodes for Mobile Devices.* Cambridge University Press, New York, 1st edition, 2010.

[25] R. H. Weber. Internet of things – new security and privacy challenges. *Computer Law & Security Review*, 26(1):23–30, January 2010.

[26] S. B. Wicker and V. K. Bhargava. *Reed-Solomon Codes and their Applications.* Wiley-IEEE Press, 1999.

[27] Y. L. Yeh, J. C. You, and G. J. Jong. The 2D bar-code technology applications in medical information management. *International Conference on Intelligent Systems Design and Applications*, 3:484–487, 2008.

[28] Z. Zhang, X. Zhang, and R. Sandhu. ROBAC: Scalable role and organization based access control models. *Collaborative Computing: Networking, Applications and Worksharing, 2006*, pages 1–9, November 2006.

Appendix

A. Preliminary Analysis of Channel Characteristics for High-Density 2D Monochrome Barcodes

To evaluate the characteristics of the communication channel with respect to symbol processing, a preliminary experiment was conducted on samples of barcode symbols. The experiment used the same equipment and symbol processing steps for testing. First, a set of 24 barcode symbols was generated using an encoder program written in the C programming language. The symbols were then printed on plain white bond paper using a Canon LBP3410 laser printer with the default settings. Next, symbols were scanned using an Epson GT-F720 flatbed scanner at 720dpi. In both the printing and scanning process, monochrome color settings were used. Finally, each symbol was read using an image processing and decoding program, also written in C.

First, a set of symbols with dimension $dim = 117$ and margin factor $mf = 0.6$ were generated and sampling cells were scanned. The computed ratios (before mapping to a soft value) were separated into two groups, based on the expected value (white or black) of the cell. Histograms for both groups were then plotted to infer observations on the channel model. From the distribution, we can observe how the values in the sampling cells match the encoded data bits after they have gone through symbol processing.

The generated histograms for black and white cells are presented in Figure 17. Statistical analysis of the distribution showed that the channel can be modeled as an *additive white Gaussian noise* (AWGN) channel, which is suitable for the soft-decision decoding of LDPC codes. Also, by analyzing the distribution, the AWGN variance which will be used for the LDPC decoder in subsequent tests was determined to be 0.05637.

Then, the dimension and code rate parameters for sample sets were varied and the BER for each set was analyzed. The results of the BER analysis for are presented in Table 10. From the results, it can be concluded that LDPC

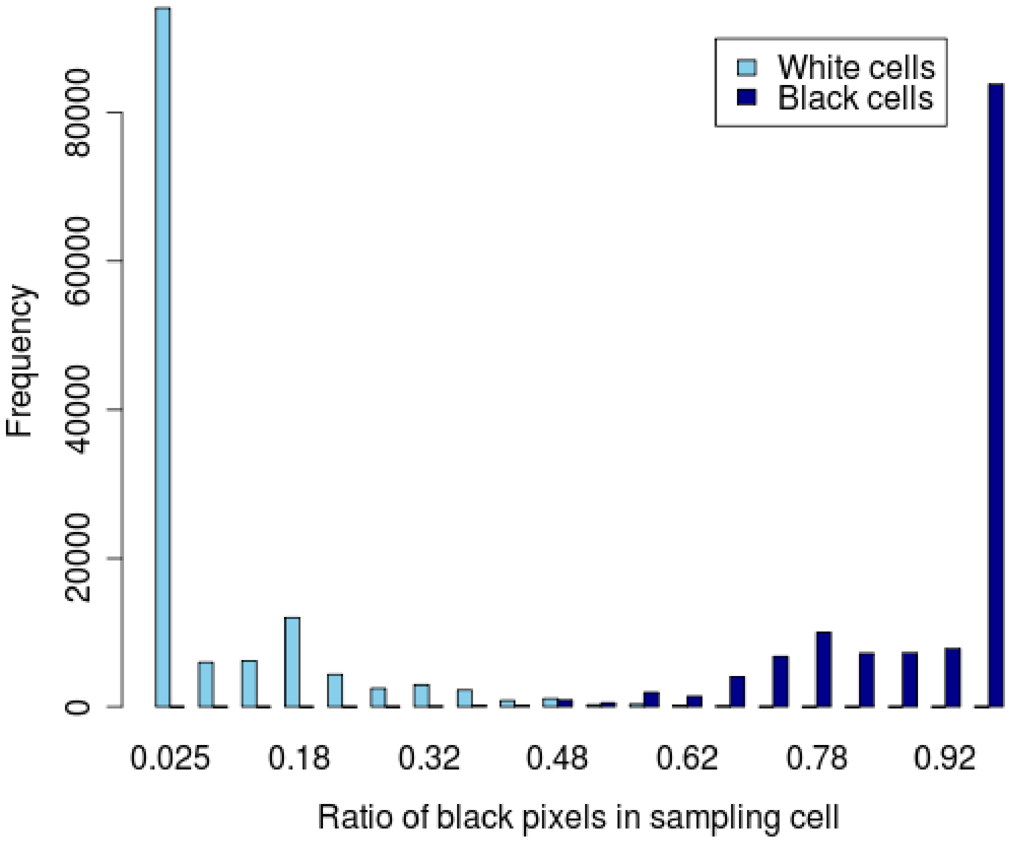


Figure 17. Histogram of ratios for black cells and white cells for symbols with dimension $dim = 127$ and margin factor $mf = 0.6$

codes with different code rates have similar performance for lower dimensions of the symbol. All codewords from the set of symbols were decoded correctly. For $dim = 117$, errors appeared for the symbols with LDPC code rate 5/6. This was expected, as this code rate has the weakest error-correcting capability.

However, there is a rapid increase of bit-errors for $dim = 127$. Inter-pixel leakage of black cells caused timing patterns to become too close to each other, thus the sampling cells formed were too small and there were not enough pixels to compute accurate soft values. This generated BER results that were inconsis-

Table 10. BER for symbols with margin factor $mf = 0.6$ and increasing dimensions

	Code rate			
d	1/2	2/3	3/4	5/6
97	0.000%	0.000%	0.000%	0.000%
107	0.000%	0.000%	0.000%	0.000%
117	0.000%	0.000%	0.000%	0.847%
127	0.709%	2.143%	5.674%	1.429%
137	Undetermined			

tent to the strength of LDPC codes, which indicated an unstable performance. Moreover, note that the BER for $dim = 137$ is "Undetermined". Due to the high density of cells in the symbol, some images were distorted by inter-pixel leakage in such a way that transition points for adjacent timing patterns could not be detected by the image processing algorithms, and the creation of sampling cells failed. Therefore, symbols with dimension parameter $dim = 117$ was deemed as the performance limit of the symbology.

Finally, note that the reported ratios have small "peaks", where white cell ratios increase unexpectedly at 0.18 and black cell ratios at 0.78. In general, barcodes scanned at a given resolution result in sampling cells having an constant number of pixels (this is to be expected, as these cells were printed using squares). However, because of interpixel leakage on timing patterns, there are cases when the sizes of sampling cells change (i.e., the number of pixels sampled are not constant). Therefore, there are round-off errors for some ratios, which are represented by these peaks.