Spring 3-2021

Towards Identity Relationship Management For Internet of Things

Mohammad Muntasir Nur

TOWARDS IDENTITY RELATIONSHIP MANAGEMENT FOR INTERNET OF THINGS

A dissertation submitted to Dakota State University in partial fulfillment of the requirements for the degree of

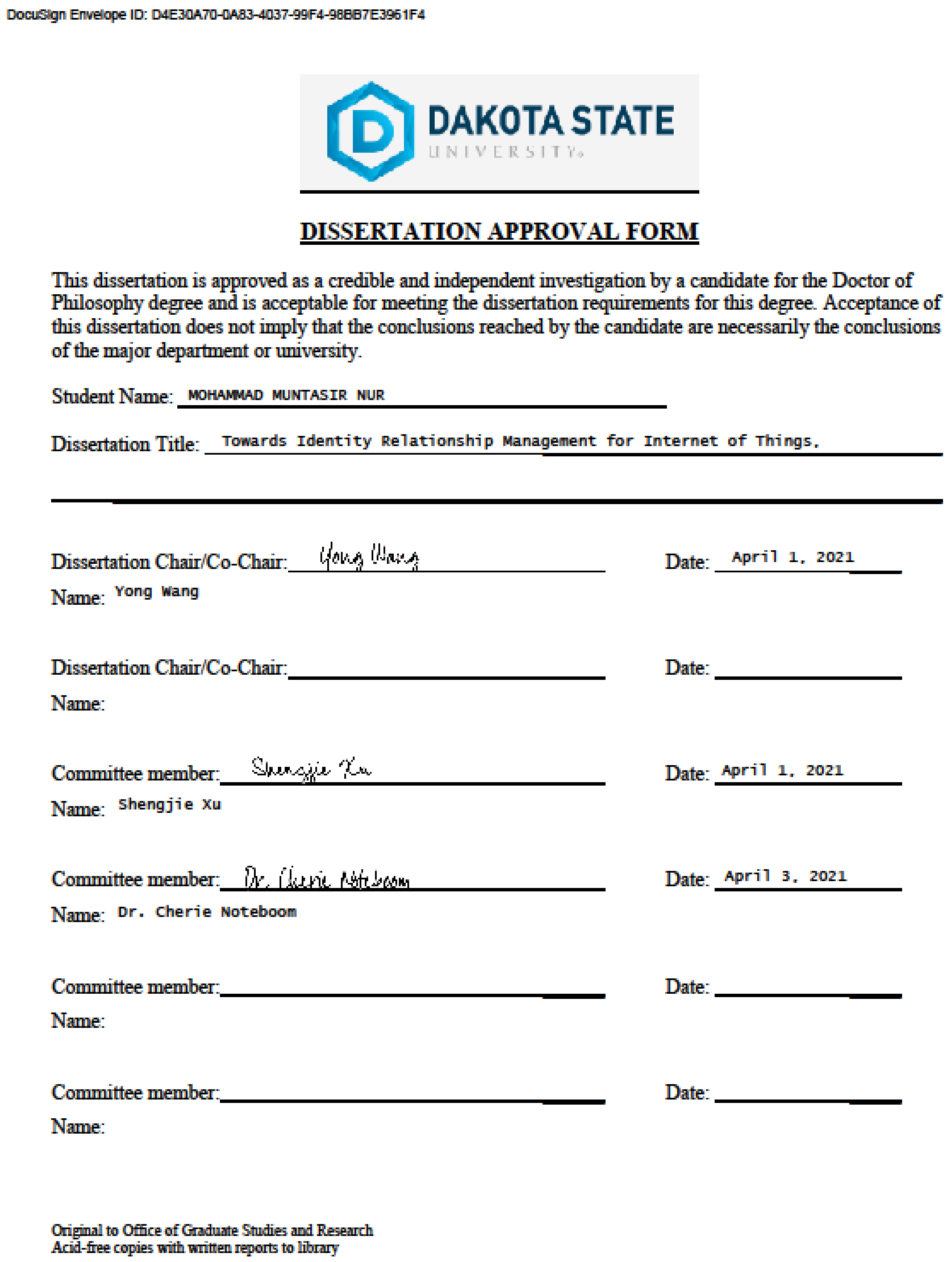
Doctor of Philosophy
in
Cyber Operations

March 2021

By
Mohammad Muntasir Nur

Dissertation Committee:

Dr. Yong Wang (Chair)
Dr. Shengjie Xu
Dr. Cherie Noteboom



DocuSign Envelope ID: D4E30A70-0A83-4037-99F4-98BB7E3961F4

DAKOTA STATE UNIVERSITY

DISSERTATION APPROVAL FORM

This dissertation is approved as a credible and independent investigation by a candidate for the Doctor of Philosophy degree and is acceptable for meeting the dissertation requirements for this degree. Acceptance of this dissertation does not imply that the conclusions reached by the candidate are necessarily the conclusions of the major department or university.

Student Name: MOHAMMAD MUNTASIR NUR

Dissertation Title: Towards Identity Relationship Management for Internet of Things,

Dissertation Chair/Co-Chair: Yong Wang
Date: April 1, 2021
Name: Yong Wang

Dissertation Chair/Co-Chair: ____________________
Date: ____________
Name:

Committee member: Shengjie Xu
Date: April 1, 2021
Name: Shengjie Xu

Committee member: Dr. Cherie Noteboom
Date: April 3, 2021
Name: Dr. Cherie Noteboom

Committee member: ____________________
Date: ____________
Name:

Committee member: ____________________
Date: ____________
Name:

Original to Office of Graduate Studies and Research
Acid-free copies with written reports to library

ACKNOWLEDGEMENT

I would like to express my deepest appreciation to my committee chair, Dr. Yong Wang, for spending a lot of time with me on the dissertation, and for continuously providing guidance, ideas and assistance. Without his direction and partnership, this dissertation would not have been possible.

I would also like to thank the committee members, Dr. Shengjie Xu and Dr. Cherie Noteboom for their time and feedbacks to make this dissertation complete.

A special thank goes to my graduate advisor, Dr. Wayne Pauli, for his support and guidance during the course of study.

Finally, I would like to thank my family - my wife, my mom and dad, and my two daughters; without their support I would not have been here.

ABSTRACT

Identity and Access Management (IAM) is in the core of any information systems. Traditional IAM systems manage users, applications, and devices within organizational boundaries, and utilize static intelligence for authentication and access control. Identity federation has helped a lot to deal with boundary limitation, but still limited to static intelligence – users, applications and devices must be under known boundaries. However, today's IAM requirements are much more complex. Boundaries between enterprise and consumer space, on premises and cloud, personal devices and organization owned devices, and home, work and public places are fading away. These challenges get more complicated for Internet of Things (IoTs) due to their diverse use and portability nature. IoTs are being used in consumer space, healthcare, manufacturing, retails, entertainment, transportation, public sector, and many other places. Identity Relationship Management (IRM) can help in solving some of these challenges as it uses a more natural way of access management - a relationship-based access control methodology. IRM can perform identity and relationship management beyond home and organizational boundaries and can simplify authorization and authentication using dynamic intelligence based on relationship.

In this research, we studied the needs of IRM for the Internet of Things. We explored four fundamental questions in IRM: what relationships need to be supported in IRM, how relationships can be supported in IRM, how relationship can be used for access control, and finally what infrastructure is required to support IRM. Since relationship is globally spread out and perimeter-less in nature, we designed the IRM service with a global scalable, modular, and borderless architecture. Instead of building something from scratch, we slightly modified the UMA 2.0 protocol built on top of OAuth 2.0 to make the relationship-based access control feature easily pluggable with existing IAM frameworks. We implemented a proof-of-concept to demonstrate and analyze the results of this research. This dissertation serves as the foundation for future research and development in IRM domain.

DECLARATION

I hereby certify that this dissertation constitutes my own product, that where the language of others is set forth, quotation marks so indicate, and that appropriate credit is given where I have used the language, ideas, expressions, or writings of another.

I declare that the dissertation describes original work that has not previously been presented for the award of any other degree of any institution.

Signed,

4/6/2021

X Mohammad Nur

Mohammad Muntasir Nur

Signed by: *.myvisualiq.net

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

Identity and Access Management (IAM) is the security discipline of identifying users and controlling their access to resources through the processes of provisioning, authentication, authorization, delegation, revocation, expiration and deprovisioning. IAM is used everywhere - home, work, healthcare, public sector, entertainment, telecommunication, transportation, wherever a user needs to interact with an application or a device. This chapter discusses the need of a refined access control methodology for IoT devices, introduces the concept of Identity Relationship Management, and finally defines the objectives of this research.

1.1 Problem Statement

Due to the rapid growth of Internet of Things (IoTs) everywhere, IAM in IoT has been a key focus of research and engineering in past few years. IoT typically refers to small scale or embedded computing devices that have minimal or no user interfaces and are connected to the Internet. These devices need to be accessed and controlled remotely by users, administrators, and other devices. Many security issues and challenges have been reported to enable this requirement (Bhattarai, et al., 2008).

IAM is in the core of security and coming up with an effective IAM solution designed and developed for IoT use cases is the first step. The emerging IoT also raises new requirements for identity and access management. IAM needs are becoming more consumer oriented and dynamic. There are four changes in identity and access management in the IoT:

1) Change of entities: Traditional IAM systems focus on managing identities of users. IoTs require extending identity management to include devices. Identities of Things (IDoT), a general term describing the entities such as users and devices in the IoT, has been well adopted.

2) Change of perimeter: Traditional IAM systems focus on meeting demands within organizations and their partners. However, the users of IoTs or IoT devices may not be bound to organizational boundaries, and therefore IoTs require IAM to be perimeter-less. This is the biggest difference in access management for IoTs, which requires IAM frameworks to evaluate access privileges for entities that are not managed by them and yet the frameworks are responsible for granting those unknown entities access to the protected data.

3) Change of scale: Traditional IAM systems deal with one or more organizations, but to achieve a perimeter-less quality, an IAM framework needs to operate in Internet scale.

4) Change of intelligence: Traditional IAM systems manage a known set of users and devices, which are part of an organization or partner organizations. However, due to having a loosely coupled user base and due to the portable nature of IoTs, an IAM system for IoTs need to deal with dynamic user base and devices, and thus will require dynamic intelligence to identify users, devices and their relationship with each other.

Unfortunately, there is no well-defined and established standard for identity and access management in IoT. Different manufacturers have come up their own solutions to identify, provision, authenticate, authorize their devices, and manage relationships among devices, services and users. As a result, IoT systems from different manufacturers are not able to communicate with each other, and thus are not able to take advantage of capabilities already available in other devices. This results in duplication of the same set of capabilities in multiple IoT systems. For example, a smart thermostat and a security system both need a motion sensor to detect occupancy in a home. Unless they are from the same manufacturer, or sometime despite being from the same manufacturer, they must use their own motion sensors.

Many limitations of the traditional IAM systems are expected to be resolved by adopting Identity Relationship Management (IRM). IRM manages identities of users and devices as well as the relationships among these entities. IAM systems can use these relationships to control access to the IoT devices (Friese, 2014). Relationship, in fact, is the foundation of any access control mechanisms; it is the relationship that drives the access control decisions – employer-employee, computer-user, bank-customer, husband-wife, doctor-patient, car-driver, application-user and so on. These relationships are still either translated by human visually, or by issuing a token (e.g., a username/password, key, certificate, marriage certificate, birth certificate, passport, driving license, etc.) as a proof of the relationship, and then access control decisions are made based on the visual translations or the tokens. This research introduces and discusses the needs of IRM in the IoT, addresses the fundamental design challenges for building an IRM system, and finally provides future directions for IRM.

1.2 Research Objective & Research Questions

The purpose of this research is to build a borderless Identity Relationship Management framework for the Internet of Things that will simplify identification of users, devices and resources involved in the IoT ecosystem, streamline access management by replacing static resource-based policies with dynamic relationship-based policies, and finally facilitate interoperability in IoT devices from different manufacturers by providing a globally standardized framework. The four research questions pertaining to this research are stated below:

1) How do we define and characterize relationships?
2) How do relationships help with access control?
3) What infrastructure support an information system should have to support IRM?
4) How do we evaluate the effectiveness of the artifact?

The first research question attempts to identify the entities involved in the IRM framework and relationships among those entities. Since the relationship between an IoT device and the person who owns the device can qualify that person to manage the device, or the relationship between the owner of the device and a person living in the same household can qualify that person to access the IoT device to certain capacity, identifying the entities and their relationships is the foundation of this research.

The next research question seeks answers to how these relationships can be used for identity and access management in IoT domain. Relationship in an IRM framework is the key driving factor in determining who will be able to access an IoT device to what capacity, if an

IoT device will have access to another IoT device, or an IoT device will be allowed in a corporate network. In traditional IAM frameworks, the relationship factor is not present. As a result, all the accesses need to be manually granted and managed – there are no policies to automate that. For example, if hundred employees bring two personal IoT devices to use for the same purpose, IAM will require manually onboarding all those devices and granting access to necessary resources individually. Relationship can simplify the access management by defining a policy that automatically grants those accesses just because the IRM system knows the relationship between the employees and the IoT devices.

The third research question studies the architecture and infrastructure aspect for developing a borderless Identity Relationship Management framework. This question is very important for this research. How do we build an IRM framework on a global scale? What kind of hardware and software support will be needed to support IRM infrastructure? Which organization will be responsible for maintaining and supporting such an infrastructure? All these questions will be considered here.

The fourth research question is to evaluate the effectiveness of the borderless IRM framework, the artifact designed and developed by this research. This includes identifying the evaluation metrics for this research as well as the evaluation of the artifact against existing similar solutions.

1.3 Dissertation Outline

The rest of the dissertation is organized as follows: Chapter 2 perform a literate review of different IAM methodologies, their evolution, IAM technologies available for IoT domain, Identity Relationship Management, and current knowledge of IRM in IoT. Chapter 3 discusses the research methodology used by this research. Chapter 4 identifies the characteristics of relationship in IoT space and outlines the relationship design for IRM. Chapter 5 explores how relationship can be used in access-control of IoT devices using IRM, both from authentication and authorization perspective. Chapter 6 discusses the architecture design of the IRM system. Chapter 7 evaluates the outcome of the IRM framework from the artifact designed as part of this research. It also performs a few case studies to understand the results and the effectiveness of the framework. Chapter 8 summarizes and concludes the dissertation.

1.4 Chapter Summary

This chapter discussed why traditional IAM technologies are not the best for managing access of IoT devices due to their boundary limitation and static knowledge about users and devices. We also introduced the concept of Identity Relationship Management, and finally defined the objectives of this research to apply IRM in IoT space.

CHAPTER 2

LITERATURE REVIEW

This chapter discusses different IAM methodologies, their evolution, IAM technologies available for IoT domain, Identity Relationship Management, and current knowledge of IRM in IoT.

2.1 Evolution of IAM Frameworks

Identity and Access Management is the security discipline of identifying users in an enterprise network and controlling their access to resources, applications, and services through processes such as provisioning/deprovisioning, authentication, authorization and delegation. IAM is essential and a core of any information system in enterprise networks. The development of IAM originally started from enterprise use cases based on the need to manage users' access to corporate resources such as computers, applications, services, and facilities. Figure 1 shows the evolution of IAM technologies from 1980s.

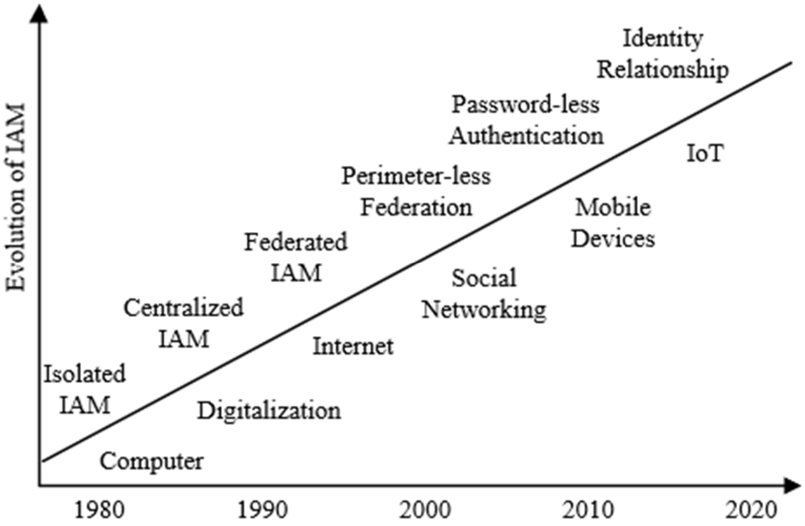


Figure 1. Evolution of IAM Technologies

Initially IAM architecture was based on an isolated model where service provider also worked as an identity provider. In the isolated model, a unique identity is issued to a user from each service provider. With the increasing adaption of digitalization, isolated IDM architecture fell short and a centralized model evolved. Microsoft Active Directory (AD) is an example of this model where all the systems in the corporation are connected to the AD. This helps the enterprise to maintain only a single username and password for each user accessing all the service providers in the company. It also adds convenience and improves security (Da, 2018). Federated IDM architecture came next. In the federated model, service providers come up with an arrangement for exchanging authentication and authorization data by delegating authentication to an identity provider. Federated IAM, e.g., SAML, simplifies identity management to a great extent. Features like Single Sign-On (SSO) add convenience to users and improve security (Chen, 2015).

Federated IAM has evolved beyond enterprise use cases due to the evolution of the Internet and mobile devices. Unlike enterprises, in Internet-based applications and services, there may not be a direct and strong mapping of identities. A user visiting a website and opening an account may not have trustable information. The perimeter of federation is also not defined. To help these use cases, OAuth 2.0 was developed as an authorization system to allow users grant a third-party application limited access to resources owned by the user in a perimeter-less boundary of the Internet. Soon it was realized that the identity of the user (aka resource owner) performing the authorization was a crucial component missing in OAuth 2.0. Many use cases were using OAuth 2.0 as an authentication medium while the protocol did not have the capability for authentication. To deal with this limitation, the OpenID Connect (OIDC) protocol was developed to provide an identity layer on top of OAuth 2.0. There were still limitations in OAuth 2.0. For example, a user (aka resource owner) can only authorize a client application to access protected resources but cannot authorize another user. The User Managed Access (UMA) grant was drafted as an extension of OAuth 2.0 to enable party-to-party authorization and thus to allow one user to grant another user access to resources owned by the former (Machulak, 2017).

With the increased use of Internet based services, Fast Identity Online (FIDO) protocols were designed to use a password-less authentication approach and thus to improve user privacy and security (Ng, 2018). The protocols use public key cryptography where client authenticates by proving the possession of the private key. This has also enabled using authentication capabilities available on an end-user device, without the authentication data leaving the user's device. These days many online services leverage the FIDO protocol to take advantage of biometric authentication capabilities like fingerprint and face recognition on modern mobile devices.

The Kantara initiative introduced the concept of Identity Relationship Management and laid out the pillars for the shift from IAM to IRM. The business pillars driving the shift include: 1) consumer and things over employees, 2) adaptable over predictable, 3) top line revenue over operating expense, and 4) velocity over process, and the technical pillars driving the shift include 1) Internet-scale over enterprise-scale, 2) dynamic intelligence over static intelligence, 3) borderless over perimeter, and 4) modular over monolithic (Maerz, 2013). However, the initiative does not provide enough details on how this can be applied in real world.

2.2 IAM Framework for IoT

The identity management lifecycle for IoT devices include discovery, provisioning, management and de-provisioning. During the onboarding phase, an IoT device typically needs to be bound with one or more users, typically through user's smart phone or computer; an authentication scheme is applied, and roles and relationships are captured during this binding process; and finally, an authorization process is established to allow users, applications or other devices to access the device throughout its lifecycle.

The isolated IDM model, as discussed earlier, is the most common way of managing identities in current IoT world. Device manufacturers develop their own ways of identifying and managing identities of their devices. An IRM system can be more suitable for the IoT than the traditional IAM systems because IRM focuses on consumers and things over employees, Internet-scale over enterprise-scale and borderless over perimeter (Maler, et al., 2019). IRM can link people and things all together and can enable a dynamic context-based strategy.

There are many factors to be considered when designing an identity and access management model for the IoT. The following section discusses some major factors.

2.3 Authentication

To address the authentication of IoT devices, the CoAP protocol has been introduced to facilitate provisioning of resource constrained IoT devices and to support interoperability (Cirani & Picone, 2015). The CoAP is a web transfer protocol that is primarily designed for machine-to-machine (M2M) communication. It maps to HTTP and supports REST architecture for integration with existing web, however, unlike HTTP, it uses lightweight UDP over IP instead of TCP, because TCP is a connection-oriented protocol and has high congestion control features, both of which causes a lot of overhead. CoAP also allows multicast and discoverability.

There can be use cases where classic authentication mechanisms like username/password may not directly work for IoT devices. A context-based authentication can be a possible solution for that (Friese et al., 2014). This approach evaluates the context and environment of the authentication request. If a deviation is observed from the established pattern, other factors are checked for additional verification. For example, if a request comes from an internal network, a token may be sufficient, otherwise some other factors like LTE cell ID or geo-location can be checked additionally. Also, most IoT devices have some relationship with a person – owner, administrator, or group; the relationship may also be used for additional authentication proof.

2.4 Authorization

The OAuth protocol may solve the authorization problems for CoAP protocol; however, OAuth is CPU intensive for low power IoT devices. A stripped-down version of OAuth protocol has been proposed by Wu et al. (2017) to perform access control of resource constrained IoT devices. This research shows the protocol takes a little more memory usage than an OAuth based authorization protocol but smaller power consumption and more suitable for small scale IoT environment.

An owner-to-owner and owner-to-any authorization scheme on top of CoAP (Constrained application protocol) has been proposed by Cirani & Picone (2015) by tracking the relationship in the server side and using that during authorization process. The framework proposes an extended IoT-OAS (IoT OAuth-based Authorization Service) architecture, where users can log on using any authentication/authorization mechanisms accepted by IoT-OAS, for example, Open ID, OAuth2, Open ID Connect, to get an access token for interaction with IoT-OAS. Any users can request owners to grant access to an IoT device through the IoT-OAS server, The IoT-OAS server will then send a push notification to the owner. Once the owner approves, the access token will be updated with the new grants.

2.5 Identity of Devices

Identity can be used to uniquely identify a device within a given domain. Currently there is no standard way to globally identify an IoT device. For standard computer, a MAC address identifies the device locally in a network while an IP address locates the device for routing purposes for a specific period. However, neither of them can provide a global unique identifier.

A cryptographic identity will be an ideal candidate since it will not only uniquely identify devices, but also will enable devices to prove the possession of the assigned identity by cryptographical assertion. Public Key Infrastructure (PKI) based identity can offer such capabilities (Anantharaman et al., 2016). A device can sign a random challenge using its private key and other entities can verify that using the device’s public key (aka the certificate). The primary challenge for this approach is the availability of a global scale PKI infrastructure. All the necessary protocols and standards to build a global PKI exist - the global standardization bodies need to put them together and have an organization own and provide the service in a similar way DNS is managed (Martin, 2002).

Anantharaman et al. (2016) proposes macaroon credential as an alternative and improved solution over straight PKI based identity solutions. Macaroon provides a bearer token and public key certificate for authorization and delegation in web, mobile devices, and distributed cloud systems in a decentralized manner. Macaroon contains a public part, constructed from a random nonce and assertions called caveats, and a private part, constructed from the HMAC of a symmetric key on the public part. Bearer of a macaroon can delegate parts of their authority or a portion of it to other entity by deriving new macaroons with a partial set of caveats. An entity containing public part M1 and private part K1 can generate a new macaroon {M1, K2} – thus macaroons can be chained together. An entity which knows the secret key at the root of a macaroon chain can derive the private parts of all the macaroons along the chain (Birgisson et al., 2014). While macaroons add the capability of embedded authorization and delegation of authorization, it comes with the similar challenges observed in any PKI based solutions, for example, revocation, expiration, renewal, etc.

Blockchain based identity for IoT has been another area. Zhu et al. (2017) proposes a Blockchain-based Identity Framework for IoT (BIFIT) to self-manage identities by end users. In this user-centric approach, all identities of owners are maintained in a blockchain while identities of things are associated with the owners via the signature signed by owners' private key. Subject identifier, public keys and signatures are used to construct the identity proof, which is sent to the blockchain peer-to-peer network and permanently added to the blockchain as a block.

2.6 Relationships in IoT

There are different entities involved in IAM ecosystem for IoT. While they may vary based on the functional category, environment and use cases, the major and common example of entities include device, gateway, user, identity provider and client. The device refers to the IoT device itself. The device may or may not be IP enabled – devices without direct Internet connectivity (typically primitive sensors) are connected to a gateway. The gateway refers to a service or a hub that has Internet connectivity. IoT devices that are not capable of directly connecting to the Internet can connect through the gateway. The user refers to an owner, an administrator or simply a user of the IoT devices. The Identity Provider refers to a service located in cloud providing identity and access management services to IoT devices and users associated with that. The client refers to an application that allows users to interact with IoT devices, gateways, or cloud service.

Based on the entities discussed above, an IAM framework for IoT devices need to consider many types of relationships, for example, relationships between devices and humans, relationships between homogeneous and heterogeneous devices, and relationships between devices and gateways/applications. Handling this diverse set of relationships poses different security challenges – how to identify, how to build and maintain relationship, how to control level of access, how to build the interface for interacting among these entities with each other, etc.

Today the boundaries between work and home have reduced. Users are bringing personal IoT and BYOD devices to work, accessing resources through them. With the increasing use cases for IoT devices, the current IAM frameworks will soon fail to meet the demand and will have difficulty in managing identities and access per user and per device. A relationship between users, between users and devices, and between devices will simplify the policy and identity management.

2.7 Identity Relationship Management in IoT

In many cases Identity Relationship Management (IRM) can be more suitable for IoT than traditional Identity and Access Management (IAM), since IRM has a focus on consumers and things over employees, Internet-scale over Enterprise-scale, and borderless over perimeter (Mordeno & Russell, 2017). IRM can link people, places and things and enable a dynamic context-based strategy that can be applied throughout the user, customer, or employee life cycle.

The Kantara initiative has defined some business and technical pillars for designing an effective IRM framework: consumer and things over employees, adaptable over predictable, top line revenue over operating expense, velocity over process, Internet scale over enterprise scale, dynamic intelligence over static intelligence, borderless over perimeter and modular over monolithic (Maerz, 2013). Traditional IAM frameworks only manage employees' access to authorized on-premises and cloud resources from preapproved computers. However, today's users are not limited in using computers only, they use smart phones, tablets, smart watches, fitness tracker, smart vehicles and many other things that are connected to Internet. Therefore, modern IAM systems need to focus on consumer and things over employees in order to be able to provision and manage variety of IoT devices quickly. The system needs to be adaptive to the context, with dynamic intelligence it should allow users to access resources from any devices from any locations. There is no corporate perimeter - users can be anywhere on the Internet, they can be employees, partners and customers, data can be located on-premise, in cloud, or in partners' premise. IAM systems should be fast to deploy and adapt, should not require a lot of processes and configurations to put into operation or to support federation.

Wilson et al. (2017) proposed IdM elements to be segmented into multiple identity layers, building an identity stack consisting of relationship, identities, attributes, authentication data, authentication metadata and deeper network layers, similar to the way OSI network stack organized. At the top of the stack is the relationships among users, devices, and service providers. Next comes identities of IoT devices, which are the base of relationships. Attributes can help in identification, can provide information about the capabilities of the devices, for example, to match services to users. Authentication data containing attributes and identities is exchanged between clients (users and devices) and servers (gateways or authentication providers). Authentication metadata contains quality data about the data, for example, data about the request, expiry date, source of attributes and authentication data, etc. Finally, the deeper network layers transport the identity stack.

2.8 Chapter Summary

This chapter presented a literature review of existing IAM methodologies, their evolution with the development of new technologies, IAM methods available for IoT domain, Identity Relationship Management, and application of IRM in IoT. The IAM frameworks for IoTs are still evolving - device manufacturers mostly develop their own ways of identifying and managing identities of their devices. IRM framework can be more suitable for IoT devices, because IRM has a focus on consumers and things over employees, Internet-scale over enterprise-scale, borderless over perimeter. It is more appropriate for end user or consumer use cases where the user is not a direct member of the enterprise.

CHAPTER 3

RESEARCH METHODOLOGY

The goal of this research is to build a borderless IRM framework for IoTs. We have adopted a design science research methodology in this research.

3.1 Design Science Research

A design science research (DSR) is an information technology research methodology that produces a theory, an artifact and impact analysis based on the result produced by the artifact (Baskerville et al., 2018). The methods used in this research is literature review, study relationship in IoT ecosystem, and evaluate the impact of applying Identity Relationship Management in IoT for access management by designing and developing a borderless IRM system. Thus, this research has followed the design science research methodology. This research has the all the DSR phases as shown in Figure 2 – identification of the problem, defining objective and scope of the research, system design, development of the proof of concept, collection of data, analysis, and validation.

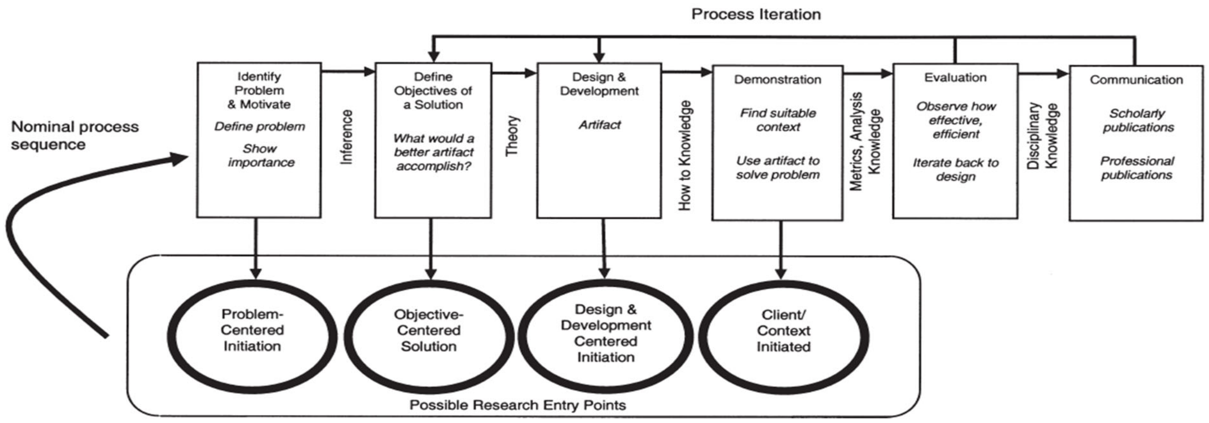

Process Iteration
Nominal process sequence
Identify Problem & Motivate
Define problem
Show importance
Inference
Define Objectives of a Solution
What would a better artifact accomplish?
Theory
Design & Development
Artifact
How to Knowledge
Demonstration
Find suitable context
Use artifact to solve problem
Metrics, Analysis Knowledge
Evaluation
Observe how effective, efficient
Iterate back to design
Disciplinary Knowledge
Communication
Scholarly publications
Professional publications
Problem-Centered Initiation
Objective-Centered Solution
Design & Development Centered Initiation
Client/ Context Initiated
Possible Research Entry Points

Figure 2. Design Science Research Methodology (Peffers et al., 2007)

3.2 Identify Problem & Motivate

Traditional IAM technologies are limited in managing access control for known set of users and resources within a pre-defined boundary of an organization and its partners. However, due to having a dynamic user base and the portable nature of IoTs, an IAM system for IoTs needs to have capabilities to deal with unknown set of users and devices in a dynamic way. Chapters 1 and 2 have identified these problems and thoroughly surveyed different available IAM frameworks for a solution in the IoT space.

3.3 Defining Objective of a Solution

Identity Relationship Management framework can provide intelligence about users, devices and their relationships with each other, and facilitate in relationship-based access control, which can help in solving problems with boundary and unknown userbase of traditional IAM systems. Chapter 1, section 1.1, titled as “Research Objective & Research Questions”, has defined the objectives for building an IRM based solution to manage access to resources in IoT space.

3.4 Design & Development

Chapters 4, 5 and 6 have demonstrated a high-level design of this proposed system with a careful evaluation of all the criteria. In this process, all the entities involved in the IoT ecosystem and the relationship among them have been identified first. Second, a thorough assessment has been performed to find the entities and relationships that are relevant and required in relationship-based access control using the IRM framework. Third, the relationships have been analyzed to identify their characteristics to be used for access control. Fourth, an access control framework for IoTs has been designed using IRM; the primary focus of this design phase was to eliminate the limitations of traditional IAM frameworks. Thus, borderless and modular characteristics have been the key considerations when designing and developing the relationship-based framework. Fifth, to keep the solution modular and borderless, the global-scale IRM system has been designed such a way that any IAM service can plug in with the IRM service to get intelligence about relationships between a requestor and an IoT device and take access control decisions using that knowledge. The UMA 2.0 grant, with slight modification in the authorization process, has been used for the connecting IRM service to the IAM services. IAM services has the authority and independence for taking the ultimate access control decision, to maximize security.

3.5 Demonstration

A proof of concept (POC) has been developed in Java for demonstrating the relationship-based access control methodology using the IRM framework. A small scale IRM service and a demo IAM service have been developed to illustrate the relationship registration, relationships calculation and access control decision making processes. Chapter 5 and 6 provide the detail of the artifact and demonstrate how IRM can provide a relationship-based access control in a perimeter-less manner.

3.6 Evaluation

The evaluation of the IRM framework for IoT has been performed in three ways: building a Proof of Concept (POC), performing use case studies and comparing IRM with traditional IAM technologies.

3.6.1 Proof of Concept (POC)

The goal of building the IRM POC is to build a platform where we can validate the design decisions of the proposed IRM framework, verify that relationship-based access control can be designed in real world, and finally prove that IRM can help with the challenges observed in traditional IAM technologies.

3.6.2 Use Case Studies

In order to evaluate the effectiveness of IRM framework in solving access control challenges observed in IoT space, an example use case of a smart wearable medical IoT device has been executed and studied through the POC platform. In this case study, the owner (of the device) carries the device all the time; the owner visits a hospital while travelling away from home; the hospital is able to access the owner’s contact and insurance info from that device and the doctors in the hospital are able to access the health history, vitals and current medication list from that device without any lengthy manual onboarding or validation processes. The goal of these use case studies is to show that IRM can help with instantaneous access to IoT devices to users that the IoT device does not have any knowledge about and who are not from a pre-defined organizational boundary. The dynamic intelligence and borderless capabilities in IRM are the key to the instantaneous access grant and thus the enablement of these capabilities is critical for the success of this research. The use case studies also establish the importance certification authorities in the IRM framework and discuss some challenges in policy evaluation.

3.6.3 Comparison with Traditional IAM Technologies

The comparisons of the IRM framework with traditional IAM technologies have been performed to show that these IAM technologies cannot solve the access control challenges in IoT space in a practical and feasible way as IRM service, and that is due to the absence of borderless and dynamic intelligence capabilities in these technologies.

3.7 Communication

We have published a paper and presented the paper in the 39th IEEE International Conference on Consumer Electronics (ICCE) on Jan 10-12, 2021. The title of the paper is “An Overview of Identity Relationship Management in the Internet of Things” (Nur & Wang, 2021).

3.8 Chapter Summary

In this chapter we have discussed what is design science research, how we have followed this methodology in our research. A design science research methodology produces a theory, an artifact and impact analysis based on the result produced by the artifact. The methods used in our research is literature review, study relationship in IoT ecosystem, and evaluate the impact of applying Identity Relationship Management in IoT for access management by designing and developing a borderless IRM system. Thus, this research has followed the design science research methodology. We have followed all the phases of the design science research in our work - identification of the problem, defining objective and scope of the research, system design, development of the proof of concept, collection of data, analysis and validation.

CHAPTER 4

RELATIONSHIP IN IRM FOR IOT

Relationship is in the core of the IRM system. A relationship refers to the affiliation between two entities in IRM. This chapter identifies the characteristics of relationship in IoT and outlines the relationship design for IRM.

4.1 Entities in IRM

There are many entities involved in the IoT lifecycle and ecosystem. To identify the characteristics of relationships, the very first step is to identify the entities in an IRM system. Figure 3 shows the entities identified in an IoT ecosystem. These entities are described briefly in the following paragraphs.

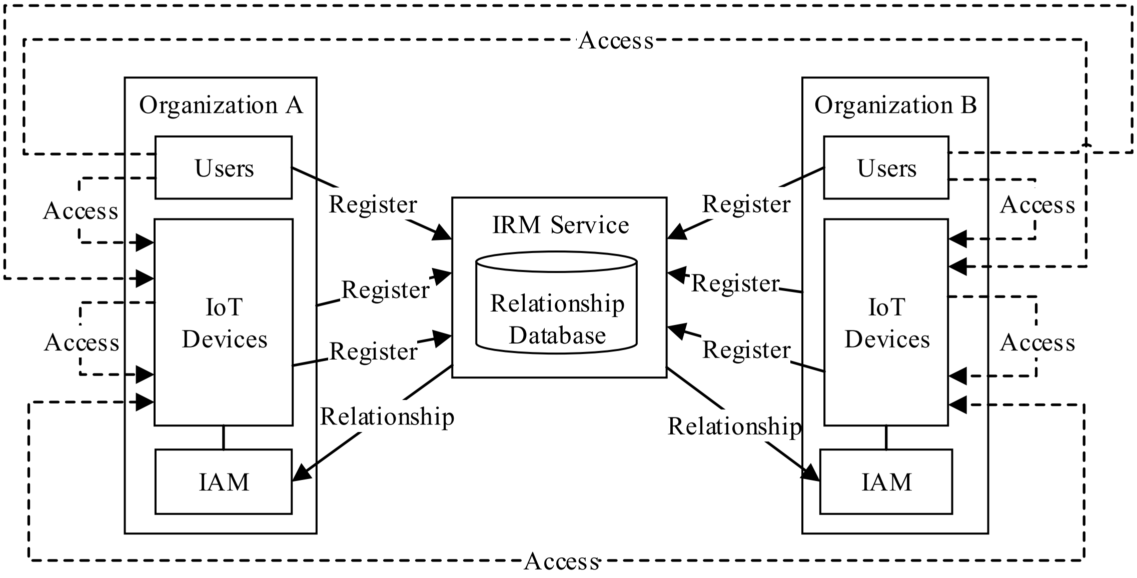


Figure 3. Entities in IRM Ecosystem for IoT

4.1.1 Organizations

An organization entity (E_O) is an entity that groups together a set of users, devices, applications and services for a common logical purpose. It is very important not to confuse the concept of an organization in IoT ecosystem with a corporation. An organization in the IoT ecosystem can be any collective unit, for example, a home, a company, a city, a hospital, a mall, a toll gate, etc., where an explicit or embedded IAM system is available to control access to resources via policies.

4.1.2 Users

A user entity (E_U) is an individual who directly interacts with the IRM service and is a consumer of some functionalities offered by an IoT device, for example, an owner of an IoT device, family members, employees, doctors, citizens of a city, etc.

4.1.3 IoT Devices

An IoT device (E_D) refers to a device owned by a user or an organization. It has Internet connectivity and can be used to carry out certain functionalities. An IoT device can be directly connected to the Internet, therefore it will be self-contained from hardware and software capability wise to connect to the Internet. Sometimes a collection of devices, for example, sensors of a security system, can be connected to the Internet via an IoT hub. In this case, the hub will have the hardware and software capability to connect to the Internet. The IoT hub is considered as an IoT entity for this research since this is the device that has internet connectivity and representative of the sensors in the collection.

4.1.4 IAM Services

An IAM service (E_{IAM}) is a software module that controls access to resources. This can be an IAM service in a large organization that controls access to thousands of resources or can be a mini IAM module built and embedded in to a single IoT device for controlling access to the capabilities provided by the device. The IAM service has a policy engine that contains the policies for access control and can make access control decisions based on relationship. The service can be registered with the IRM service to take relationship information as an input to make an access control decision based on the defined policies.

4.1.5 IRM Service

The IRM service (E_{IRM}) is the distributed software component that captures and stores relationships among entities, manages the relationship lifecycle of the entities and relationships inside it, and finally provides the relationship information between two entities to authorized IAM services for relationship-based access control.

4.1.6 Applications and Services

An application or service (E_{AS}) is a software program designed to perform certain functions for authorized users. Applications and services are connected to IAM services for controlling users, devices or other applications and services accessing to them based on relationships.

In summary, the entity set can be expressed as below:

$$E = \{E_U, E_O, E_D, E_{IRM}, E_{IAM}, E_{AS}\} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

4.2 Relationships in IRM

These entities in IRM system are related to each other in many ways, e.g., relationships through social bonding, employment, ownership, service provider, service consumer, etc.

$R_{XY} = f\ (E_X, E_Y)$, where R_{XY} is the relationship between entity E_X and E_Y

In theory, it is possible to have some relationships between any of the two entities in the entity set E. However, not all these relationships are applicable or important to be captured for identity relationship management. The only relationships important to IRM are the relationships that can be used in making a relationship-based policy decision for controlling access.

4.2.1 Relationships Cannot Be Used in IRM

The following relationships cannot be used in any relationship-based policy decision and thus these do not require to be captured in IRM service:

- The IAM service gets relationship information between two entities from the IRM service.

- Applications and services in an organization use IAM service to control users and other applications accessing to the capabilities they provide. They are functionality-wise similar to IoT devices.
- IoT devices can be connected to an IAM service or a small-scale IAM module built into the devices for controlling who can access to what functionalities they provide.

Some relationships are not direct and need to be calculated dynamically from other relationships. Thus, even though these can be used for policy decision making in relationship-based access management, these are not necessary to be captured in IRM service:

- The relationship between two IoT devices can be calculated if we capture the relationship between users and organizations, between users and devices and between organizations and devices, for example, if two devices have the same owner, we know these devices have a relationship. Capturing this relationship would be duplication, would require unnecessary effort.

4.2.2 Relationships Can Be Used in IRM

The following relationships can help in making a relationship-based access control decision:

- Relationship between two users (E_{U1} and E_{U2}), e.g., a patient wearing a device and the physician that has prescribed and is administering the device.

  $R_{UU} = f\ (E_{U1}, E_{U2})$ ………………………………………………………… (2)

- Relationship between two organizations (E_{O1} and E_{O2}), e.g., a hospital and a nursing home:

  $R_{OO} = f\ (E_{O1}, E_{O2})$ ………………………………………………………… (3)

- Relationship between two devices (E_{D1} and E_{D2}), e.g., two devices working as a group, both with Internet connectivity, and only one is associated with an owner:

  $R_{DD} = f\ (E_{D1}, E_{D2})$ ………………………………………………………… (4)

- Relationship between an organization (E_O) and a user (E_U), e.g., a company and its employees or customers.

  $R_{OU} = f\ (E_O, E_U)$ …………………………………………………………… (5)

- Relationship between a user (E_U) and a device (E_D), e.g., a patient and his smart vital monitor.

$R_{UD} = f\ (E_U, E_D)$ .... (6)

- Relationship between an organization (E_O) and a device (E_D), e.g., a company and a computer owned by the company.

$R_{OD} = f\ (E_O, E_D)$ .... (7)

To summarize, the relationships among the following three entities are important from identity relationship management perspective and hence need to be captured in the IRM service: (a) users, (b) organizations and (c) IoT devices. The relationship set in IRM can be expressed as below:

$R = \{R_{UU}, R_{OO}, R_{DD}, R_{OU}, R_{UD}, R_{OD}\}$ .... (8)

The entity set for IRM in equation (1) can be revised only to have the entities relevant to IRM:

$E = \{E_U, E_O, E_D\}$ .... (9)

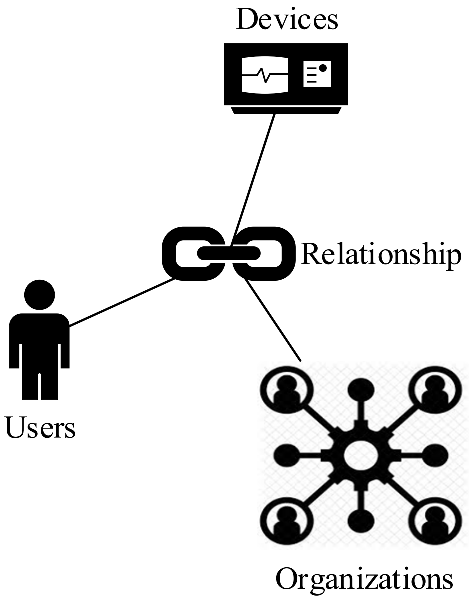


Figure 4. Relationships among Entities in IRM

4.3 Design Considerations for Relationship in IRM

There are some important characteristics of relationship from IRM and IoT perspective that need to be considered when designing relationship for IRM service. The following paragraphs discusses those briefly.

4.3.1 Adaptability

There are many kinds of relationships available via social bonding and organizational membership, for example, family, spouse, children, friend, neighbor, citizen, employee, contractor, coworker, mentor, doctor, patient, student, teacher and so on. There can be subcategories and variations among them, for example, employees can be manager, individual contributor, etc. The relationship largely depends on the need of an organization and its access control policy needs. Therefore, the IRM service needs to be flexible enough to adopt any kind of possible relationships demanded by use cases in an organization.

4.3.2 Transient Relationship

Some relationships are transient, for example, a guest accessing an IoT device at home or an interviewee trying to use a smart elevator or a smart vending machine. These relationships are temporary, based on the situational context, and can change over time.

4.3.3 Degree of Relationship and Relationship Graph

Some relationships are direct, for example, the wife of a person accessing an IoT device owned by that person has a direct relationship with the person. Some relationships are indirect, for example, the brother of that wife trying to access the IoT device has an indirect relationship with the person. The distance in relationships can be expressed as degree of relationship, for example, the person has first-degree relationship with the device, his wife has a second-degree relationship with the device, his wife's brother has a third-degree relationship with the device and so on. Figure 5 illustrates the degree of relationship through a relationship graph where each node or vertex represents an entity, e.g., a user, an organization or a device, and each edge represents a relationship between the entities or vertices it connects. E_D in the graph is the IoT device that is being accessed to, E_{O-D} is the owner of the device and E_R is the requestor that is trying to access the device. Each entity has been marked with the distance (aka degree of relationship) from the device that is being accessed.

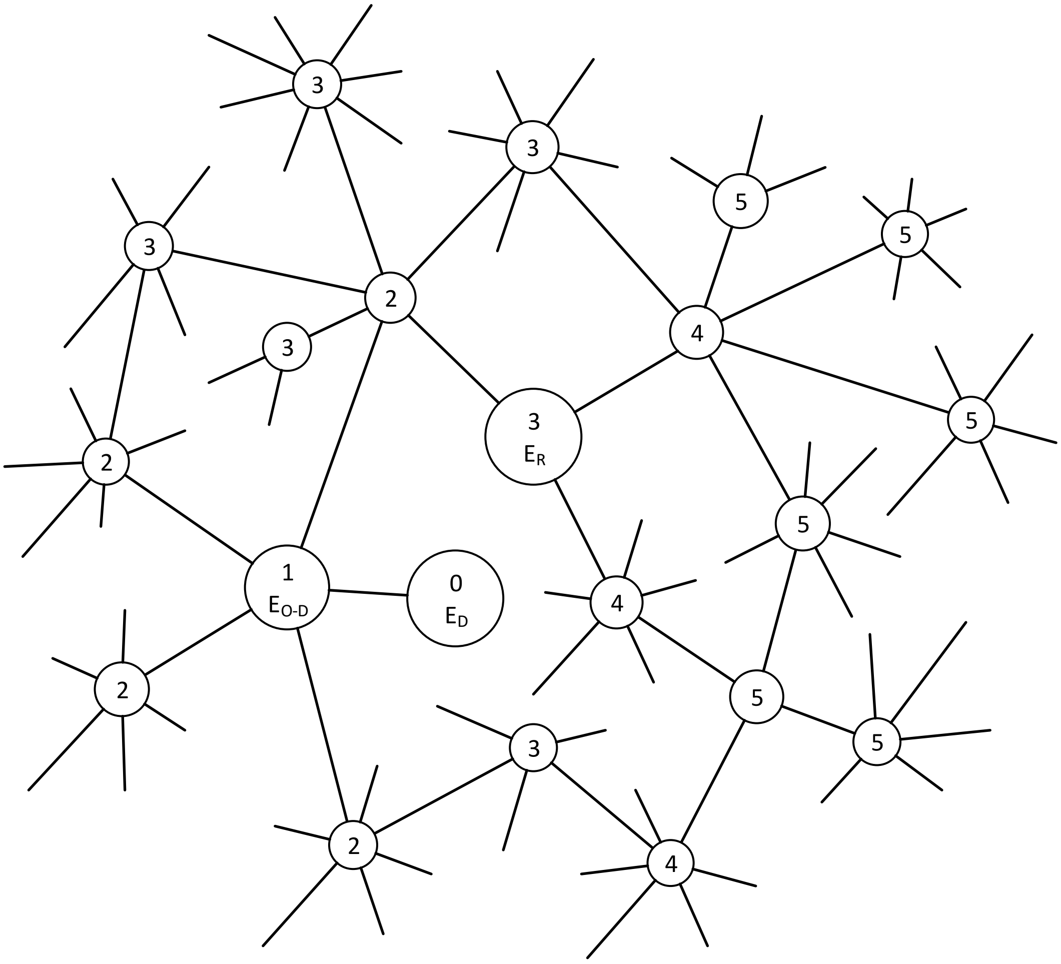


Figure 5. Relationship Graph and Degree of Relationship

We can rewrite equations (2) to (7) with a new parameter, degree of relationship (D_R), which can be used in specifying the degree of relationship acceptable when a relationship-based access control decision is being made:

$R_{UU} = f\ (E_{U1}, E_{U2}, D_R)$ ………………………………………………………… (10)

$R_{OO} = f\ (E_{O1}, E_{O2}, D_R)$ ………………………………………………………… (11)

$R_{DD} = f\ (E_{D1}, E_{D2}, D_R)$ ………………………………………………………… (12)

$R_{OU} = f\ (E_O, E_U, D_R)$ …………………………………………………………… (13)

$R_{UD} = f\ (E_U, E_D, D_R)$ …………………………………………………………… (14)

$R_{OD} = f\ (E_O, E_D, D_R)$ …………………………………………………………… (15)

4.3.4 Legal Recognition

Some relationships are legally recognized and certified by social and organizational authorities, for example, family relationships are certified via marriage certificate or birth certificate, employment are certified by the employer, etc. On the other side, some relationships are not structured that way, for example, friend. These relationships are equally important for IoT use cases.

4.3.5 Level of Trust

The level of trust is tied with the legal recognition of the relationship and integrity of relationship captured in IRM service, for example, marriage or employee relationships have higher level of trust due to the legal aspect of these relationships compared to a friend or guest relationship. However, a marriage relationship in IRM, unless it is validated, may not have the level of trust needed for strong policy decision.

4.3.6 Certification Authority

To address the legal recognition and level of trust issues, there has to be an attestation and verification process for integrity and trustworthiness of the relationships. This triggers the need of another entity in IRM framework – the certification authorities. Certification authorities are bodies that attest entities and the relationship claimed by two entities. For example, a certification authority can attest an organization, and the organization can attest the employer-employee relationship with an employee. Figure 6 illustrates the concept of certificate attestation process. It is up to the IAM service and its policy on how to weigh certified vs uncertified relationships for policy decision. Digitalization of identities and automation of identity and document verification process can facilitate in this certification process for IRM. A PKI model can be used to implement the attestation and validation in the certification process, exactly the way digital certificate framework works. However, this is out of scope of this particular research.

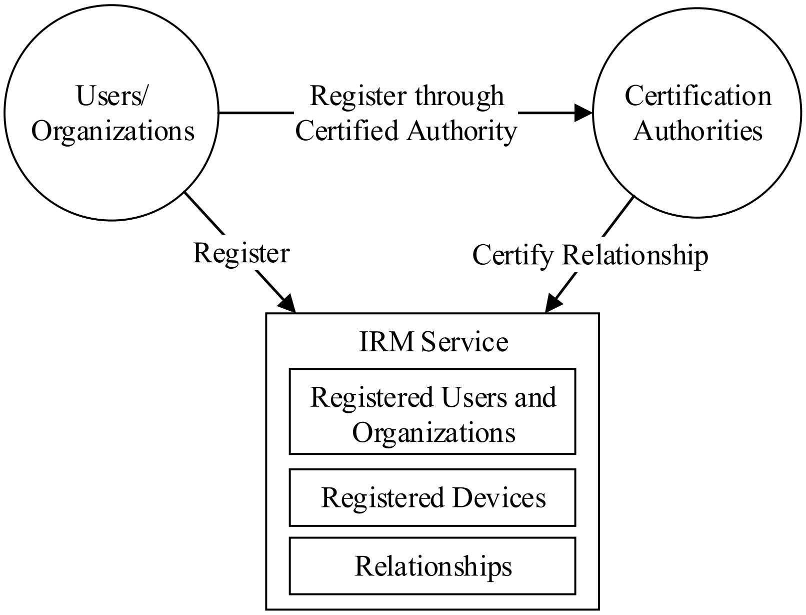


Figure 6. Relationship Registration and Certification

4.4 Relationship Design for IRM

Based on the discussion about entities, relationships and relationship design characteristics from the earlier sections, Figure 7 captures a simplified model of relationship data that need to be captured in the IRM. Users, organizations, and devices tables track the registrations of the corresponding entities with the IRM system. Relationships table tracks relationships among users, organizations, and devices along with attestation. Certification Authorities table contains information about the authority that verifies relationship and the certificates used by the certificate authorities for attestation. Chapter 5 will provide more details about why the attributes captured in different tables are required and how they contribute in relationship-based access control.

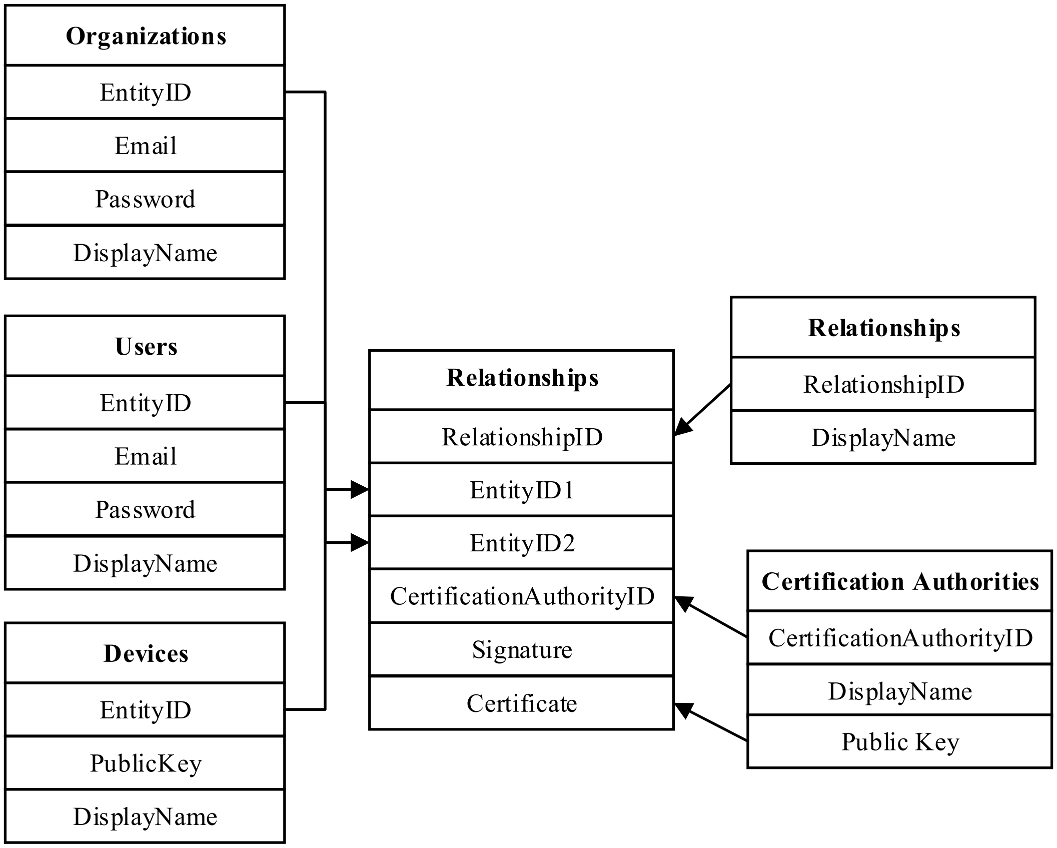


Figure 7. Relationship Model in IRM

4.5 Chapter Summary

In this chapter, we have identified the entities we need to capture relationships for, what relationships need to be captured and how, in order to use relationships in access control of IoT devices through IRM framework. We have identified three types of entities that are relevant for IRM in IoT ecosystem: (a) users, (b) organizations, (c) IoT devices. We also have discussed the characteristics of relationship in IoT space that are important design considerations for IRM: adaptability, transient relationship, degree of relationship, legal recognition, level of trust and certification authorities.

CHAPTER 5

ACCESS MANAGEMENT FOR IOT USING RELATIONSHIP

Relationship can be used in access control of IoT devices using IRM – from both authentication and authorization perspective. This chapter provides a detail design of how access control of IoT devices can be implemented using an Identity Relationship Management system. The research has made the following assumptions and therefore these are beyond the scope of this research: IoT devices have the following capabilities:

- ✓ Devices can generate their own public-private key pairs.
- ✓ Devices can protect their private keys.
- ✓ The connections to and from the device are always secured.

5.1 Relationship in Authorization

In IRM system, relationship is the factor that drives access control of resources. In a Role Based Access Control (RBAC) model, accesses are granted using roles. If the policy indicates that an employee needs manager's approval to get access to a system, the manager is the role controlling the access. In an Attribute Based Access Control (ABAC) model, accesses are granted using attributes. If a policy indicates only employees whose "office=Building 40" can access that building, the attribute "office" is controlling the access to that given building. Similarly, in a Relationship Based Access Control model (RelBAC), accesses are granted based on relationships. If the policy indicates if employees of a company can access to a device, it is the "employer-employee" relationship that is governing the access to the device.

Figure 8 illustrates a borderless IRM-based IAM concept. Jim is married to Pam and Oliver is their child. Jim owns an IoT device. Due to policy 2 (owner-to-user relationship), Pam and Oliver also get owner level access to that device. Jim takes his device to work. Due to policy 2 (owner-to-device relationship), he can access the corporate resource 1 through his personal IoT device just like corporate IoT device 3. Traditional IAM systems cannot manage users and devices outside of the organizational scope (in this case, Jim's home is outside of corporate scope) due to the lack of intelligence about relationships, and thus, they would not be able to grant access to resources in such dynamic approach.

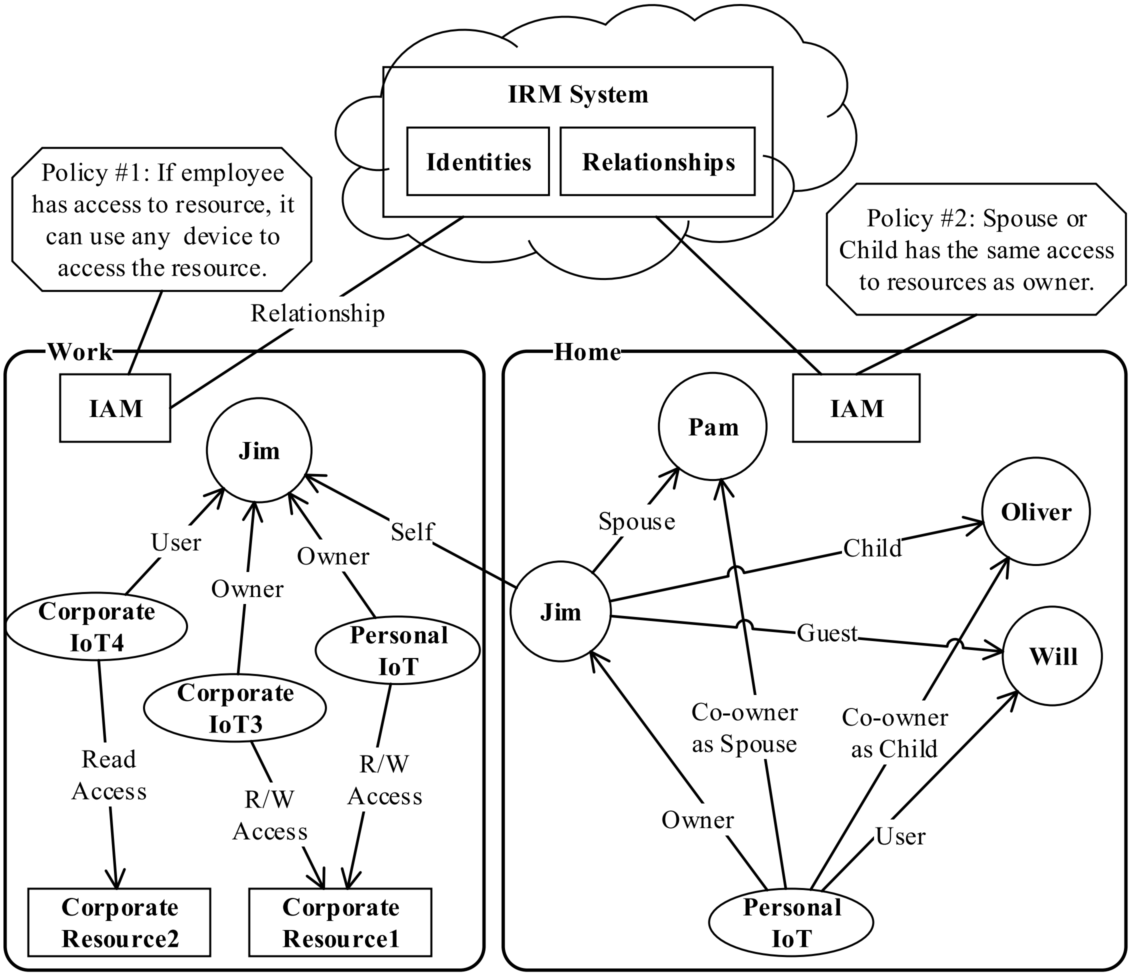


Figure 8. Access Control using Relationships with IRM

There can be different types of relationships between users which will impact the level of accesses to an IoT device. For example, a homeowner, the spouse, the child, and guests will have different level of permissions on a device. The policies in IRM system can also address the scope of permissions to allow limiting access to resources based on the relationship. For example, one permission can grant users read access to a device while another can grant write access to the resource. During the authorization process, different entities will be assigned different scopes based on the policy definitions.

5.2 Relationship in Authentication

Authentication is the very first step in any identity and access management system. There are three primary authentication factors: something you know (e.g., username and password), something you have (e.g., a physical token or a smartcard), and something you are (e.g., fingerprint or face recognition). In addition, Context-Based Authentication (CBA), also known as Risk-Based Authentication or Adaptive Authentication (Steinegger, et al., 2016), has become very popular these days as a secondary authentication factor. The CBA method builds behavior profile for each user based on two factors: somewhere you are and something you do. In this process, the location where the user is logging in from, the hardware and software used by the user to log in, the time of the day the user logs in, the kind of activities the user performs, etc. are captured to build the behavioral profile of the user. Later the CBA method uses this profile to determine if there is a deviation from the norm, and therefore if there is any risk associated with the transaction. IP address, geo-location, MAC address, OS or browser information, time zone and timestamp of the transaction are some example CBA factors.

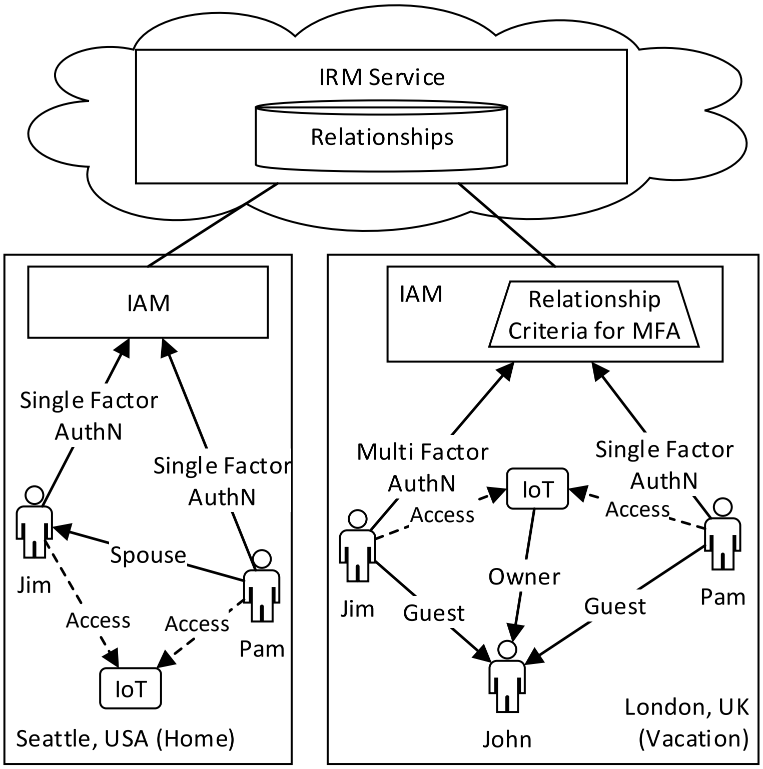


Figure 9. Authentication using Relationships with IRM

While relationship does not have the properties of a primary authentication factor, it can be utilized in Context-Based Authentication. Relationship can help in gaining real-time intelligence about a user. Figure 9 illustrates a use of relationship in CBA. Jim and Pam, a married couple and Seattle resident, go to London for vacation and stay at a friend's place. While on vacation, Jim attempts to access an IoT device. With the help of the IRM system, the home IAM module determines that Jim is a friend visiting the owner and grants access to the IoT device, however, it also triggers a multi-factor authentication (MFA) as defined by a policy. Shortly after Jim, Pam also attempts to access the IoT device and the home IAM identifies her as the owner's friend's wife and thus eligible to access the IoT device. Since Jim has logged in shortly before Pam from the same location, Pam's attempt to access the device is considered as low risk and she is not asked for second factor authentication. Traditional IAM systems cannot track relationship and thus, in the example above, will not allow to authentication and second factor authentication for Pam. However, authentication is not in the scope of this research – the focus is authorization perspective of access control.

5.3 Design Considerations for Relationship Based Access Control in IRM

IRM service has some technical and business pillars (Maerz, 2013) that are very important for the success of IRM. The following paragraphs discuss those pillars.

5.3.1 Borderless

The IRM service for IoT cannot be bound by perimeter of a single or a federation of organizations, rather it needs to be able to track relationship beyond the boundaries of the organizations. IRM can offer intelligence about relationships of external devices, users and organizations with internal devices, users, and organizations, and the IAM system can use this intelligence to make the access control decision based on the relationship criteria defined in the policies.