LICENTIATE THESIS

Digital Power of Attorney for authorization in industrial cyber-physical systems

Sreelakshmi Vattaparambil Sudarsan

Cyber Physical Systems

LULEÅ UNIVERSITY OF TECHNOLOGY

Digital Power of Attorney for authorization in industrial cyber-physical systems

Sreelakshmi Vattaparambil Sudarsan

Dept. of Computer Science and Electrical Engineering
Luleå University of Technology
Luleå, Sweden

Supervisors:

Olov Schelén, Ulf Bodin

To Abhi and my family...

Abstract

In the age of digitization, many Cyber-Physical Systems are semi-autonomous and have sufficient power and resources to perform tasks on behalf of users. This thesis defines an authorization technique to transfer the power of legitimate users to trusted CPS or IoT devices, allowing the device to sign or access resources on behalf of the user. The authorization technique is based on digital Power of Attorney, which is a self-contained document generated by the user (principal) and sent to the agent (trusted device). A Power of Attorney contains a timestamp, that makes it invalid after a period of time predefined by the principal. Here, the agent who receives the PoA does not require a separate account; instead, it uses the principal account with limited features. The thesis studies and analyzes other delegation-based and subgranting-based authorization techniques, such as the OAuth standard. There are certain similarities and differences between OAuth and PoA, that are analyzed based on metrics such as protocol flow, communication type, token format, and control expiration. Considering the benefits and challenges of both the OAuth and PoA, this thesis combines these two techniques and proposes a multilevel subgranting system. The conceptual architecture, protocol flow, design overview, PoA format, use case scenarios, and implementation details of the proposed system are presented. The system is implemented based on an industrial CPS usecase scenario. The results are qualitatively analyzed and also quantitatively evaluated based on metrics such as CPU and memory utilization. Future work includes security analysis, result evaluation, and comparison of findings with respect to OAuth and other delegation-based authorization standards, implementation of PoA based authorization technique from the scratch, and integration with frameworks such as Arrowhead.

Contents

Acknowledgments

My journey so far has been made possible by the encouragement and support of my teachers, family, and friends. Even though I can not mention everyone, I would like to express my gratitude to each and every one of them. This thesis is not the work of a single person; rather, it is the result of the efforts of many people who assisted me along the way.

I would like to thank my supervisors Olov Schelén and Ulf Bodin for your guidance and support. All of your feedbacks have always encouraged me and all I have achieved in the last two years is because of you. I would also like to thank Sabu M Thampi and Rajesh Koduri for introducing me to the field of research.

I would like to thank all my EISLAB friends, and I cannot think about a day without our long lunch. All the stupid things that we discuss are very stress releasing and interesting.

I did not feel far from home in Luleå as I had my Malayali gang hanging out often. All our weekend parties are a lot of fun and I don't remember most of them haha.

Thank you so much, Abhi for your support throughout this adventure. You've always been there for me and have always encouraged me. And I'm always motivated by your space research.

I am out of words to show gratitude to my parents and Sruthy who always stand by my side and encourage me. Without you, nothing would be possible.

Thank you all!!

Part I

Chapter 1

Introduction

1.1 Motivation and research questions

The world is becoming more digitized as technologies such as IoT and CPS connect things and improve people's lives. CPS devices, both automatic and semi-automatic, can be used to simplify a variety of tasks, particularly in an industrial environment. In an industrial scenario, a single user or contractor can be assigned to perform several tasks with different access privileges. For example, a user working on the collection of raw materials from the supplier will be also part of some other tasks within the supplier company.

What if the user's trusted automatic or semi-automatic device can act on behalf of the user with his/her same power?

This can increase the large utilization of intelligent devices in a CPS ecosystem and thereby increasing the overall productivity. The user can use his/her CPS devices with sufficient resources to perform tasks on the user's behalf. However, working on behalf of the user entails accessing protected resources, which necessitates additional security measures, because the protected resources are typically shared with the user and not the device. In the preceding example, the user instructs an autonomous truck to collect raw materials from a supplier on the behalf of the user. In this situation, we assume that the supplier trusts the user. As a result, to make the supplier trust and authorize the autonomous truck, the user requires a mechanism for transferring his/her access privileges to the truck.

Is there a pre-existing authorization technique that can be used to grant user power to a device, allowing the device to work on the user's behalf? What are the primary security concerns that must be addressed during this authorization process?

These questions motivated this research, which resulted in the development of the digital face of a traditional authorization mechanism known as *Power of Attorney (PoA)*. PoAs are legal documents that are used to delegate our privileges to someone we trust. By using the PoA, the secondary party legally acquires the same ownership and rights as the primary person [16].

How can we bring this traditional paper-based legal authorization technique into the age of CPS and examine it from a digital standpoint?

This question inspires this research to integrate newer delegation and subgranting-based authorization techniques with traditional PoA-based authorization. This prompted this research to dive deeper into different authorization techniques in CPS, yielding the following research questions:

Q1 *How can an authorization model be created that can represent the relationships between different entities and transfer power to the user's trusted CPS device and make it work or sign on behalf of the user using PoA?*

This question leads this research to the development of a conceptual architecture for the PoA based authorization model. The primary stage of the fundamental conceptual model for PoA-based authorization has two main entities: the principal and the agent. The *principal* is the user who generates the PoA and then sends it to the agent, and the *agent* is the device that receives the PoA and acts on behalf of the user. In the second stage of this research, the *resource owner* or *resource server*, who owns and stores the resources that the agent requests on behalf of the principal are defined. The user is the principal in the previous example, and the autonomous truck is the agent, that can work on behalf of the user (principal) using the PoA and the supplier is the resource owner. The core component of this basic architecture is the PoA, which is a self-contained digital document with an expiration time predefined by the principal. For additional security, the public key certificate is used to identify the users in the signatory model, as well as a signatory registry for PoA management. Because of the self-contained nature, the PoA itself is used to transfer the powers, allowing the devices to access resources on behalf of the user. This raises the second research question as follows:

Q2 *What structure and cryptographic properties can the self-contained PoA have so that the principal can include all of the required information in the PoA for transferring power and for others to verify the PoA?*

The first part of this research question leads to the design of the PoA structure with different parameters that provide necessary information such as identity information of different entities, messages, timestamps, etc, based on a JSON web token (JWT) format. The second part of this research question, which requires verification of the PoA figure out different challenges associated with the PoA-based authorization. For everyone to use and

verify the PoA, requires different libraries or a downloadable image for different entities in the system. This part can be done by implementing the PoA-based authorization from the scratch or integrating it with an existing authorization standard, the second approach is more feasible from an industrial perspective. This identifies the third research question as follows:

Q3 *Which existing authorization technique can be integrated with the PoA-based authorization system? How can they be integrated so that the ease of deployment, usability, and security of the authorization system is improved?*

This question guides this research into evaluating existing authorization techniques, especially in IoT and CPS authorization scenarios, while considering the properties of PoA-based authorization. This leads to *delegation based authorization* systems, in which a user delegates another application or service (client) to access protected resources owned by the user on behalf of the user. Delegation-based authorization is reasonable to integrate with this research because it allows a third party to access data on the user's behalf. However, there are different access control models and other standards that use the delegation-based authorization technique, and this research chose the *OAuth* standard [10], which is the most common and flexible delegation-based authorization standard from IETF, particularly in IoT and CPS scenarios that can be integrated with the PoA based authorization system.

1.2 Research methodology

The research methodology used in this thesis falls under the category of Experimental computer science and engineering (ECSE) research. "ECSE is the fundamental underpinning of the computer hardware and software that drive the information age," [5]. The first part of this thesis is based on the literature study method. The literature study method is used to identify gaps in the state of the art; this method aids in narrowing down the main research area and focusing on a specific area in the field of study. This research begins with the development of the primary research question, which is considered the most fundamental. Newer sub-research questions are derived from the main research question, bringing the research closer to the actual problem or gap in the research area.

Following the gaps, this research proposes new solutions that can answer research questions. Each individual research question is examined and answered by developing a Proof of Concept (PoC), implementing the solution, and assessing the findings and results. In this thesis, paper A reviews the state of the art and identifies gaps in the research area, while papers B and C propose a solution, proof of concept, and implement and demonstrate the solution using real-world use case scenarios. The connection between different papers in this thesis are shown in Fig. 1.1.

The experiments in this study are performed in a lab setting, and the results are evaluated. Real-time experiments with actual hardware devices and humans are not part of lab-based research. In this study, we used the aforementioned methodologies to gain

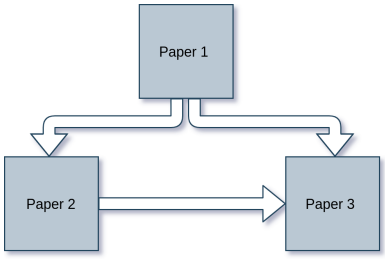

Figure 1.1: ***Connection between papers in this thesis***

a deep understanding of the field of study, identify potential gaps, and find solutions to existing problems.

This study follows the research ethics by avoiding harm to others and being honest and trustworthy with the data. The ACM code of ethics and professional conduct [1] defines different ethical issues in computer science research and provides guidelines to address them. Accordingly, this thesis has shown respect for other people's intellectual works by including adequate references. The efforts to help others have been made by making all the publications, results and experimental data of this research publicly available [8].

1.3 Thesis outline

This compilation thesis consists of two parts: Part 1 comprises several chapters, beginning with an introduction that defines the motivation, research questions, and research methodology. It also provides the research background discussing CPS, IoT, and different authorization techniques in CPS and IoT. The contribution and summary of the appended papers are also provided in a separate chapter. Finally it presents the conclusions and future work of this thesis.

Part II contains two published papers and one submitted journal manuscript that have been reformatted to comply with the thesis format. There is a table of contents for the detailed outline.

Chapter 2

Research Background

This chapter provides an overview of the research domain of this research, where a literature review is conducted to determine the state of the art and the different existing gaps. The focus is primarily on cyber-physical systems, the Internet of Things, and the security concerns and requirements in these areas, especially authorization techniques.

2.1 Cyber Physical-Systems and Internet of Things

2.1.1 Cyber Physical-System

Cyber-Physical Systems (CPS) integrate Internet Technologies (IT) with electronic or mechanical devices that can control and monitor the physical world over data exchanges [17]. An important property of CPS is the interaction between cyber components (eg: processing units, computing devices) and physical components (eg. sensors and actuators) of CPS [11]. The CPS uses computer-based algorithms for the automated and controlled functioning of hardware and software components in the network.

In contrast to the Internet of Things, which primarily pertains to the interconnection of things via the Internet and the exchange of data between them, a CPS is typically more domain-specific, with the interaction between more advanced, often semi-autonomous, physical, and cyber environments achieved through the integration of algorithmic computations. A common aspect is that both the IoT and CPS pose high security and privacy concerns [2].

CPS comprises mainly three components. 1) communication, 2) control, and 3) computation are all integrated with the physical world. Since 2006, there has been an interesting evolution of embedded systems from information management systems (the 1960s) to CPS. CPS has more physical components than embedded systems. CPS, unlike embedded systems, focuses on the link between computational and physical elements rather than the computing element itself. The link is established for data exchange between the physical and computing elements through the CPS communication component.

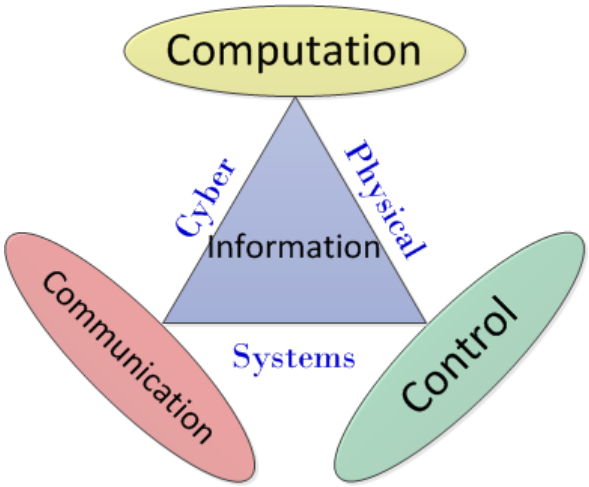

Figure 2.1: Three main components of CPS [19]

The general workflow of CPS includes three different steps: monitoring, networking, computing, and actuation. The monitoring step monitors the physical environment of the system, which includes different sensors and actuators. In the networking step, aggregation and diffusion of a large amount of real-time data from different types of sensors are carried out. The aggregated data is used by the analyzers to process further. The data collected from the physical environment is analyzed and checked in the computing step to see if the physical process meets certain pre-defined criteria. If the system fails to meet the criteria, the system will suggest corrective actions. In the actuation step [18], the actions determined in the computing step are carried out. The complex concept of CPS is defined using a concept map [15], which defines CPS as networked/distributed control systems that are intelligent, adaptive and predictive systems that possibly interact with humans in real time. The CPS can be used in different application domains such as consumer and industry, smart energy systems, healthcare, military, robotics, and transportation. The primary requirements of CPS are improved design tools, design methodology, and cybersecurity. Cybersecurity is mainly concerned with resilience, privacy, intrusion detection, and malicious attacks. The increased interaction between the cyber system and the physical system of the CPS can lead to an increase in the number of security vulnerabilities in the cyber system. This thesis targets the cybersecurity requirements of the CPS [15].

2.1.2 Internet of Things

Kevin Ashton coined the term "Internet of Things" (IoT) in 1999 for the supply chain management. However, people are now using IoT for a variety of applications such as healthcare, utilities, transportation, smart homes, smart cities, and so on [9]. The number

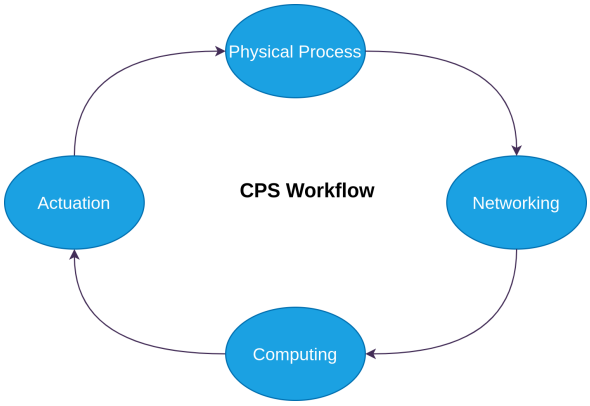

Figure 2.2: CPS workflow [18]

of connected things in the world has now reached billions or trillions. IoT technology connects things and smart objects that can sense and monitor their surroundings, as well as process and transmit the collected sensor data. The industrial IoT (IIoT) is a subset of IoT that is used to connect all industrial assets through automated M2M and industrial communications.

IoT consists of three components: 1) hardware, 2) middleware, and 3) presentation. Sensors, actuators, and embedded communication hardware are all part of the hardware. The middleware primarily provides the computational tools and storage required for data analytics. The presentation includes tools for visualization and interpretation that can be used on a variety of platforms and applications. Radio Frequency Identification (RFID), Wireless Sensor Networks (WSN), addressing schemes, data storage, and analytics, visualization are important technologies that make up these IoT components.

IoT architecture

There are different IoT architectures with a different number of layers. According to many works such as [22], [13], and [3] the most basic IoT architecture has three main layers: a perception layer or device layer, a network layer, and an application layer. The functions and features of each layer are defined based on the devices present within it. The perception layer mainly consists of physical devices such as RFIDs, sensors, and actuators. The main functions of this layer are data acquisition, data processing from physical devices, and transmitting data to the higher layers. These valuable sensor data are then transmitted to the network layer [14] [20]. This layer also performs IoT node collaboration in local and short-range networks.

The network layer is the middle layer of the IoT architecture, which primarily contains network devices. The main function of this layer is to route data between heterogeneous networks and devices using different network devices (switch, hub, router, etc.), communication technologies (Bluetooth, WiFi, etc.), and different protocols such as CoAP and

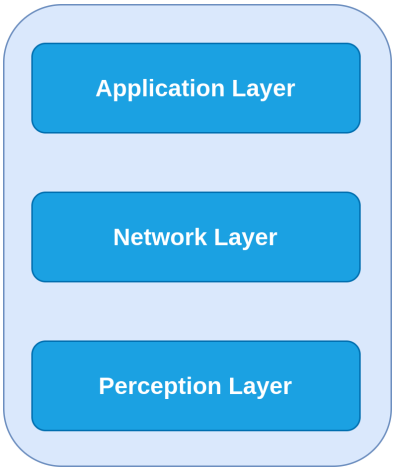

Figure 2.3: ***IoT three-layer architecture***

MQTT [12].

The application layer is the high-level IoT layer, that defines different IoT applications and provides the end-user with the processed data from different IoT devices [3]. Fig. 2.3 shows the IoT security architecture with three different layers.

Some works demonstrate a five-layer IoT architecture that introduces two more layers, referred to as the midware layer and business layer, for service management and management of the entire IoT architecture using business models [12].

There are different security procedures in the IoT network, such as network entry and secure connection to a distant peer. The network entry procedure specifies how IoT devices are authenticated for remote servers. In the secured connection to a distant peer procedure, the connection between an IoT device and an unconstrained node is defined using two secure channels via a gateway [4]. There are different challenges in IoT security such as object identification, authentication, authorization, privacy, lightweight cryptosystems, and security protocols, software vulnerability and backdoor analysis, malware in IoT, and security issues from android [21].

2.2 Authorization techniques in CPS and IoT

There are different security requirements such as identity management, authentication, authorization, confidentiality, and integrity, which are interconnected to provide different aspects of security in the research domain of CPS and IoT [7]. In this thesis, the focus is on authorization techniques, that are used to provide access to protected resources based on the access privileges. Authorization is closely related to access control, where authorization is part of the policy definition phase of access control, and the access policy enforcement is based on the authorization process in the policy definition phase.

There are different types of authorization techniques, most of the applications use access control models such as Mandatory Access Control (MAC), Discretionary Access Control (DAC), and Role-Based Access Control (RBAC) to control the access to protected resources. Another important type of authorization technique is Delegation-based authorization, where users provides or delegates their privileges to other entities or client services [22]. A common example for delegation-based authorization is Open Authorization (OAuth) protocol, which is a web-based authorization standard based on the representational state transfer (REST) protocol. It is primarily used to authorize third-party services. In OAuth, third-party services (clients) access the user's (resource owner's) protected resources on the user's behalf. Access tokens are used to provide authorization via the OAuth authorization server. Client services use the access tokens generated by the OAuth authorization server to access protected resources from the resource server on behalf of the user (resource owner).

Chapter 3

Contributions

The goal of this thesis is to develop a secure authorization technique that allows users to subgrant power to devices so that the devices can perform tasks on behalf of the users. The authorization model proposed in this thesis is based on the concept of digital Power of Attorney (PoA). PoA based authorization technique can be used to allow non-constrained CPS devices to access protected resources and perform tasks on behalf of the user for a predefined time period. Consider the same scenario described in the introduction section, in which the user uses his/her autonomous truck to collect raw materials from the supplier on behalf of the user. Here, the user can generate a PoA for his/her trusted autonomous truck to collect raw materials from the supplier on behalf of the user. Here, the user is referred to as the principal, the autonomous truck is referred to as the agent, and the supplier is the resource owner.

The PoA is a self-contained document that allows the agent (autonomous truck) to access protected resources on behalf of the principal (user) for a specified period. PoA-based authorization technique is classified as subgranting-based authorization technique, in which the person subgrants his/her power to the device for a predefined time period. The thesis describes the conceptual architecture of the PoA-based authorization system, PoA structure, and other security techniques and database management systems that can be used in conjunction with the PoA authorization system, such as CA, digital signature, and signatory registry.

PoA has different advantages on its own, such as it doesn't require a separate account for the device to work or sign on behalf of the user (principal), the decentralized nature of the authorization system, and the self-contained nature of PoA. However, there are several challenges with the PoA-based authorization system. The primary challenge is to enable PoA execution in any system that participates in the authorization process, which can be provided by an open-source library or a reliable downloadable image. Another approach is to combine PoA-based authorization with a system, that includes a trusted authorization server capable of handling some parts of the PoA.

There are several similarities and differences between OAuth and PoA-based authorization. Both of these techniques enable third-party applications or services (clients)

to access resources on the user's or principal's behalf. While OAuth controls delegation via authorization servers, the PoAs enable decentralized authorization because of the self-contained nature of PoAs. OAuth mentions some features that are outside the scope of the specification and are intentionally left open for future research and improvement of the OAuth standard.

Taking the characteristics and the challenges of the PoA-based authorization technique into account, this thesis integrates PoA based authorization technique with existing delegation based authorization techniques in particular OAuth.

The integrated authorization model contains entities such as principal, agent/client, authorization server, resource owner, and resource server. The principal generates the PoA and sends it to the agent (client device) so that the agent can sign on behalf of the principal; in this case, the agent does not require a separate account for communication. The agent/client receives the PoA and sends a request along with the PoA to the authorization server. The authorization server registers the client and sends back a client ID. To obtain the authorization grant, the client ID and PoA are sent to the resource owner. When the client receives the authorization grant from the resource owner, it can send a request for the access token to the authorization server. The authorization server generates and sends the access token to the client, which the client uses to obtain requested resources from the resource owner. PoA is a key component of the proposed authorization technique, which is of self-contained JWT format. The PoA contains the following parameters: principal public key, principal name, resource owner ID, agent public key, agent name, signing algorithm, transferable, iat (Issued at), eat (Expires at), and metadata.

We found that the integrated PoA and OAuth model provides multiple levels of delegation in OAuth, separation of the resource owner from the contractor, the addition of centralized authorization server to the PoA system, and PoA execution in any system using OAuth security.

3.1 Paper A

Title: A Model for Signatories in Cyber-Physical Systems
Authors: Sreelakshmi Vattaparambil Sudarsan, Olov Schelén, and Ulf Bodin
Status: Published in 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), 2020

Summary: This manuscript proposes a conceptual architecture for the PoA based authorization model. The paper also defines other security concepts that can be used in conjunction with the PoA-based authorization technique, such as Certificate Authority (CA) and signatory registry for PoA management.

Personal Contribution: The paper's draft was written by me, and the findings and observations were discussed with Olov Schelén and Ulf Bodin.
Relevance: This paper address research question one (Q1).

3.2 Paper B

Title: Survey on delegated and self-contained authorization techniques in CPS and IoT
Authors: Sreelakshmi Vattaparambil Sudarsan, Olov Schelén, and Ulf Bodin
Status: Published in the journal IEEE Access, 2021

Summary: This paper provides an overview of authorization techniques in Cyber-Physical Systems (CPS) and the Internet of Things (IoT). The survey is done in three different dimensions: access control models, subgranting models, and authorization governance. The paper focuses on authorization subgranting techniques such as delegation-based authorization and self-contained PoA-based authorization. Comparisons are also provided based on parameters such as communication type, authorization method, expiration control, and use of techniques such as public-key certificates, encryption techniques, and tokens. The paper discusses the differences and similarities of server-based and PoA based authorization techniques. Authorization standards and authorization governance such as centralized and decentralized authorization approaches are also included in the paper.

Personal Contribution: I conducted a literature review on the topic, wrote a draft of the paper, and discussed the findings and observations with Olov Schelén and Ulf Bodin.
Relevance: This paper address research question three (Q3).

3.3 Paper C

Title: Multi-level Sub-granting by Power of Attorney and OAuth
Authors: Sreelakshmi Vattaparambil Sudarsan, Olov Schelén, and Ulf Bodin
Status: Submitted to the journal of MDPI Sensors, 2021

Summary: This manuscript demonstrates the proof of concept for a PoA-based authorization technique. The paper defines the differences and similarities between PoA and OAuth, as well as the limitations of both authorization techniques. To address the challenges of both authentication techniques, the paper proposes an integration of OAuth and PoA. This paper presents the architecture, structure of the PoA, and implementation details of the proposed model, as well as a use case scenario.

Personal Contribution: I worked on the methodology part, as well as the implementation of the proof of concept, and wrote the first draft of the paper. The findings and observations were discussed with Olov Schelén and Ulf Bodin.
Relevance: This paper address research question two and three (Q2 and Q3).

Chapter 4

Conclusions

The research questions posed at the beginning of the thesis are revisited and answered in this chapter based on the research findings and results. The various questions that emerged after this research have been added to this chapter as future work.

Q1 *How can an authorization model be created that can represent the relationships between different entities and transfer power to the user's trusted CPS device and make it work or sign on behalf of the user using PoA?*

A PoA based authorization technique is proposed in this thesis, that allows CPS and IoT devices (agents) to sign on behalf of the user (principal). The different entities involved in this model are the principal, agent, and resource owner or resource server. The communication between the different entities is done through the use of digital PoAs, which are self-contained documents, that allow the principal to provide his/her powers to the agent in a decentralized way (without using a centralized authorization server), allowing the agent to sign on behalf of the principal. PoA contains all of the sufficient information required for the power transfer and authorization. The expiration time defined by the principal makes the agent device only use the PoA until the expiration time, otherwise, it will be considered as invalid PoA, which removes all the stale PoAs.

Paper A presents the basic idea and conceptual architecture of the PoA based authorization technique. Paper A also discusses the integration of security concepts such as the Certificate Authority (CA), which issues public key certificates for the corresponding public keys of the users. A signatory registry is also proposed in paper A, which is a SQL database used to identify the relationships between different entities in the authorization system and to manage the PoAs.

Q2 *What structure and cryptographic properties can the self-contained PoA have so that the principal can include all of the required information in the PoA for transferring power and for others to verify the PoA?*

The self-contained nature of PoAs is an important feature that allows them to be

used for authorization purposes on their own. PoA is designed as a JWT token, which is the standard format for most authorization tokens, including OAuth access tokens. Two parameters are used to identify the principal who generates the PoA: the principal public key and the principal name. Similarly, the agent identification information, such as agent public key and agent name are also included in the PoA. The identification of the resource owner is also included in the PoA as the resource owner ID parameter. Cryptographic techniques such as digital signatures are used to protect the PoA, where the principal signs the PoA with his/her private key. The parameter signing algorithm is used to indicate the type of digital signature (for eg: SHA225) that will be used for the signing. PoA may or may not be transferred by including it in another PoA, i.e., it is signed in several delegation steps. The parameter transferable indicates the number of PoA transfers; by default it is set to 0, indicating that the PoA is not transferable. The expiration time of the PoA is defined by the parameters iat (Issued at), eat (Expires at). Application-specific information with other sub-parameters are added to the PoA using the metadata parameter.

Paper C provides detailed information regarding the structure and format of self-contained PoA. The design and implementation architecture and specific algorithms for digital signature and encryption, the verification of PoAs are explained in detail in paper C.

Q3 *Which existing authorization technique can be integrated with the PoA-based authorization system? How can they be integrated so that the ease of deployment, usability, and security of the authorization system is improved?*

There are different authorization techniques used in the domain area of CPS and IoT. Paper B provides a survey on different authorization techniques in this domain. One of the important and widely used authorization techniques is the delegation-based OAuth authorization technique. The PoA based authorization technique is a delegation or subgranting-based authorization technique with several similarities and differences with the OAuth authorization standard. There are several challenges associated with both of these authorization techniques. In the OAuth standard, certain out-of-the-scope specifications are deliberately left open for future research and OAuth extension. The OAuth protocol could not separate the contractor (principal) from the resource owner entity and only supports one step of delegation as well as the use of a centralized authorization server for the authorization of different parties involved.

The PoA is completely decentralized and does not require a separate centralized authorization server due to the self-contained nature of PoAs. PoA based authorization system can separate the resource owner from the contractor (principal) entity on an arbitrary number of levels, providing a new perspective for the authorization technique. However, the infrastructure required for each party and device to independently process PoAs is not yet in place. As a result, it is reasonable to integrate OAuth and PoA based authorization techniques so that some critical aspects of PoA execution can be handled by the OAuth authorization server and the benefits of both approaches can be obtained.

Paper C studies, analyzes, and compares the similarities, differences and, limitations of both of these authorization techniques and proposes an integration of OAuth and PoA based authorization systems. Different security and usability features of the proposed model is discussed in paper C. The architecture, design overview, protocol flow of the proposed model along implementation details using a specific CPS industrial use case is also defined in paper C.

Chapter 5

Discussion and Future Work

This thesis examines the literature, identifies gaps in the state-of-the-art, and proposes a conceptual architecture and proof of concept for a newer authorization technique based on the concept of PoAs. The proposed authorization technique, which makes use of digital PoAs and the OAuth standard, allows CPS and IoT devices to sign on the user's behalf. The integrated model addresses several limitations of both PoA and OAuth. The findings indicate that the proposed model can provide a new perspective on OAuth authorization using multiple levels of delegation and introducing a principal entity that is distinct from the resource owner entity. Because PoAs are self-contained for decentralized operation, the authorization server in this model does not need to communicate with the principal (user/contractor) during the client authorization process.

This thesis's future work will include large-scale implementation, data analysis, and so on. The following points provide specifics about this thesis's future work.

1) *Implementation of PoA based authorization technique from the scratch.*

Due to the challenges, a PoA-based authorization technique is integrated with the OAuth standard to address the existing issues. PoA-based authorization techniques will be developed and implemented from the scratch in future work. This includes different open-source libraries (container images) or a reliable downloadable image (similar to what is provided for PGP). The different libs will be the principal lib, which will be used by the principal to create PoAs, the agent lib, which will be used to carry and transfer the PoAs, the resource server or authorization lib for decentralized PoA execution, or by a third-party. This eliminates the need for centralized servers such as the OAuth authorization server and completely decentralizes the proposed authorization model and PoA execution.

2) *Use of PoA based authorization technique in the Arrowhead framework.*

Future work integrates PoA with the Arrowhead framework, which includes everything required for anyone to design, implement, and deploy an automation system of systems. It is based on the concept of local clouds combined with the system of systems. The mandatory core systems of the Arrowhead framework are the service registry system, authorization system, and orchestration system. The authorization system performs access control and assists the service provider in providing access to different consumers [6]. PoA based authorization system can for example be used for complementary authorization for on-boarding new devices

3) *Security analysis and the quantitative evaluation of the findings.*

A security evaluation of the PoA-based authorization framework will be performed in the future, which will be accomplished by testing the proposed system against different malicious attacks to identify existing vulnerabilities and their security fixes. This evaluation method contributes to the overall security of the system.

Paper C provides the implementation details of the proposed authorization system. Further works are required to obtain quantitative results based on the security tests. The obtained results had to be analyzed and compared to the OAuth standard. More specific implementations integrated with the Arrowhead framework, as well as results evaluation, are planned for the future.

References

Bibliography

[1] Ronald E Anderson. Acm code of ethics and professional conduct. *Communications of the ACM*, 35(5):94–99, 1992.

[2] Rabeea Basir, Saad Qaisar, Mudassar Ali, Monther Aldwairi, Muhammad Ikram Ashraf, Aamir Mahmood, and Mikael Gidlund. Fog computing enabling industrial internet of things: State-of-the-art and research challenges. *Sensors*, 19(21):4807, 2019.

[3] Mardiana binti Mohamad Noor and Wan Haslina Hassan. Current research on internet of things (iot) security: A survey. *Computer Networks*, 148:283–294, 2019.

[4] Riccardo Bonetto, Nicola Bui, Vishwas Lakkundi, Alexis Olivereau, Alexandru Serbanati, and Michele Rossi. Secure communication for smart iot objects: Protocol stacks, use cases and practical examples. In *2012 IEEE international symposium on a world of wireless, mobile and multimedia networks (WoWMoM)*, pages 1–7. IEEE, 2012.

[5] National Research Council et al. *Academic careers for experimental computer scientists and engineers*. National Academies Press, 1994.

[6] Jerker Delsing. *Iot automation: Arrowhead framework*. Crc Press, 2017.

[7] Mohammed El-hajj, Maroun Chamoun, Ahmad Fadlallah, and Ahmed Serhrouchni. Taxonomy of authentication techniques in internet of things (iot). In *2017 IEEE 15th Student Conference on Research and Development (SCOReD)*, pages 67–71. IEEE, 2017.

[8] Don Gotterbarn, Keith Miller, and Simon Rogerson. Software engineering code of ethics. *Communications of the ACM*, 40(11):110–118, 1997.

[9] Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, and Marimuthu Palaniswami. Internet of things (iot): A vision, architectural elements, and future directions. *Future generation computer systems*, 29(7):1645–1660, 2013.

[10] Dick Hardt et al. The oauth 2.0 authorization framework. Technical report, RFC 6749, October, 2012.

[11] Abdulmalik Humayed, Jingqiang Lin, Fengjun Li, and Bo Luo. Cyber-physical systems security a survey. *IEEE Internet of Things Journal*, 4(6):1802–1831, 2017.

[12] Madhusanka Liyanage, An Braeken, Pardeep Kumar, and Mika Ylianttila. *IoT security: Advances in authentication*. John Wiley & Sons, 2020.

[13] Rwan Mahmoud, Tasneem Yousuf, Fadi Aloul, and Imran Zualkernan. Internet of things (iot) security: Current status, challenges and prospective measures. In *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, pages 336–341, 2015.

[14] Nangialay Nangial and SeyedAkbar Mostafavi. Internet of things: Architecture, security issues and solutions.

[15] Alyona Skorobogatjko, Andrejs Romanovs, Nadezhda Kunicina, et al. State of the art in the healthcare cyber-physical systems. *Information Technology and Management Science*, 17(1):126–131, 2014.

[16] Sreelakshmi Vattaparambil Sudarsan, Olov Schelén, and Ulf Bodin. A model for signatories in cyber-physical systems. In *2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, volume 1, pages 15–21. IEEE, 2020.

[17] Sreelakshmi Vattaparambil Sudarsan, Olov Schelén, and Ulf Bodin. Survey on delegated and self-contained authorization techniques in cps and iot. *IEEE Access*, 2021.

[18] Eric Ke Wang, Yunming Ye, Xiaofei Xu, S. M. Yiu, L. C. K. Hui, and K. P. Chow. Security issues and challenges for cyber physical system. In *2010 IEEE/ACM Int'l Conference on Green Computing and Communications Int'l Conference on Cyber, Physical and Social Computing*, pages 733–738, 2010.

[19] N Wu and X Li. Rfid applications in cyberphysical system, deploying rfid-challenges, solutions, and open issues, c. *DOI*, 10(17464):291–302, 2011.

[20] Tasneem Yousuf, Rwan Mahmoud, Fadi Aloul, and Imran Zualkernan. Internet of things (iot) security: Current status, challenges and countermeasures. *International Journal for Information Security Research (IJISR)*, 5(4):608–616, 2015.

[21] Zhi-Kai Zhang, Michael Cheng Yi Cho, Chia-Wei Wang, Chia-Wei Hsu, Chong-Kuan Chen, and Shiuhpyng Shieh. Iot security: Ongoing challenges and research opportunities. In *2014 IEEE 7th International Conference on Service-Oriented Computing and Applications*, pages 230–234, 2014.

[22] Kai Zhao and Lina Ge. A survey on the internet of things security. In *2013 Ninth international conference on computational intelligence and security*, pages 663–667. IEEE, 2013.

Department of Computer Science, Electrical and Space Engineering
Division of Embedded Intelligent Systems LAB

ISSN 1402-1757
ISBN 978-91-7790-940-8 (print)
ISBN 978-91-7790-941-5 (pdf)

Luleå University of Technology 2021

Print: Lenanders Grafiska, 141453

LULEÅ
UNIVERSITY
OF TECHNOLOGY