UNIVERSITY OF TARTU

FACULTY OF MATHEMATICS AND COMPUTER SCIENCE

Institute of Computer Science

Software Engineering

Shazia Javed

Service Integration for Biometric Authentication

Master Thesis (30 EAP)

Supervisors: Dr. Ulrich Norbisrath, PhD

Dr. Eero Vainikko, PhD

Author: _____ "___" May 2012
Supervisor: _____ "___" May 2012
Supervisor: _____ "___" May 2012

Approved for Defence

Professor: _____ "___" May 2012

TARTU 2012

Acknowledgements

All praises to Allah for the strengths and His blessings in completing this thesis.

It is difficult to overstate my gratitude to my supervisor, Dr. Ulrich Norbisrath. This thesis would not have been possible without his ever-present support and guidance. I believe by working with him I have increased myself in technical knowledge, and have become more practical and meticulous about details.

I am also thankful to my co-supervisor, Dr. Eero Vainikko, for his help and guidance.

I am extremely indebted to Dr. Marlon Gerardo Dumas Menjivar, my professor and program coordinator, for his constant encouragement, support, and guidance throughout my MSE.

I am grateful to the librarian, the lab attendants, and the secretaries in the Institute of Computer Science and International Student Service, for helping the department in running smoothly and for assisting me in many different ways. Ms. Laura Kalda, Ms. Heelika Strelkova, and Ms. Piret Pumm deserve special mention.

I also acknowledge the support provided through the European Regional Development Fund via Enterprise Estonia, project "Comparison and Evaluation of Fitness for Purpose of various Biometric Technologies". I want to thank Biometry.com for serving as the base for our case study, and its founder Werner Blessing for letting us use their patents.

I also wish to thank my many student colleagues for providing a stimulating and fun environment in which to learn and grow. I am especially grateful to Christopher Thomas Willmore, Volodymyr Floreskul, Karina Kisselite, Dmytro Fishman, Dmitri Danilov, and Naiad Hossain Khan. Karina Kisselite was particularly helpful with the translation of the abstract into Estonian language. Cüneyt Sina Koca, Inamullah Soomro, and Olgun Çakabey deserve a mention.

I gratefully acknowledge the integral role Muhammad Assad Safiullah, Mahjabeen Shahbaz, Mehr Tanvir, Tariq Hafeez Malik, Imran Hafeez Malik and Khurram Ahmed Bugvi have played in defining the person I am today. If it was not for their patience, sincerity, and faith in my capabilities, I would not have been able to pursue my ambition.

I also wish to thank my friends Katarzyna Zatylna, Anna Baranowska, Agata Pierścionek, Karen Ordones, Liisa Elts, and Karina Aslanyan, and my flat mates for all the emotional support, camaraderie, entertainment, and caring they provided.

Finally, and most importantly, I would like to express immense gratitude and deep appreciation to my parents and siblings on whose constant support, encouragement, love, and prayers I have relied throughout my time at the University of Tartu. I am extremely indebted to my parents for inspiring me to always work with conviction, honesty, and diligence. It is to my siblings, I dedicate my thesis.

Contents

List of Figures

List of Tables

Abbreviations and Acronyms

CBEFF	Common Biometric Exchange File Format
BioAPI	Biometric Application Programming Interface
API	Application Programming Interface
SPI	Service Provider Interface
HRS	Human Recognition Service
CDSA	Common Data Security Architecture
AbVIE	Activity based Verification, Identification, and Evaluation
MBAF	Multimodal Biometric Authentication Framework
XML	Extended Markup Language
CAS	Centralized Authentication Service
LASS	Local Authentication Subsystem
MBASSy	Modular Biometric Authentication Service System
BBM	BioBroker Model
SCD	Specification, Configuration, and Deployment
ATM	Automatic Teller Machine
SIBA-Rxxx	SIBA stands for Service Integration for Biometric Authentication, R stands for requirement, and xxx represents the three digit numeric requirement identifier
CEN/XFS	European Committee for Standardization / Extensions for Financial Services
JSON	JavaScript Object Notation
SLOC	Source Lines of Code
COCOMO	Constructive Cost Model

Thesis Outline

Background

The success of biometric authentication systems is evident from the increasing rate of adoption of unimodal biometric systems in civil and governmental applications. However, this does not imply that biometric systems offer a complete authentication solution. Unimodal biometric systems exhibit a multitude of limitations which can be overcome by using multimodal biometric authentication systems. Multimodal systems are considered more reliable, and capable of meeting stringent performance needs and addressing the problem of non-universality and spoof attacks effectively.

Problem Statement

Despite the relative advantages, implementation and usability of multimodal biometric systems remain a fundamental software engineering challenge. Multimodal systems are usually an amalgamation of unimodal biometric systems chosen in accordance with the needs dictated by the business process(es) and the respective environment under consideration. The heterogeneity, availability of source code, and the deployment needs for these systems incur significantly higher development and adaption costs.

Objective

Being software engineers, we naturally strive to simplify the engineering process and minimize the required amount of effort. Therefore this work focuses on making the existing biometric systems reusable. The objective is to define a service integration framework which automates seamless configuration, and deployment of heterogeneous biometric systems, and minimizes the development effort and related costs.

Contribution

In this effort we replace the need for development and integration of scenario-specific compatible systems by repetitive scenario-specific configuration and deployment of multimodal biometric systems. We also present tools for configuration and deployment, which respectively configure and deploy multimodal biometric systems comprising of heterogeneous open source and/or commercial biometric systems required for fulfillment of domain specific authentication needs. In comparison to the prevalent practices, our

approach reduces the effort required for developing and deploying reliable biometric authentication systems by 46.42%.

Document Organization

- Chapter 1 briefly explains the need for service integration for biometric authentication, related design and implementation issues, the existing solutions, and our approach.
- Chapter 2 gives a detailed account of the related work done so far in this field, and summarizes the shortcomings of the current research and the state-of-the-art solutions.
- Chapter 3 describes the proposed process, elicits the specification for the real-life authentication scenarios, and concludes with a brief description of the proposed model.
- Chapter 4 documents the tool support, presents experimental results achieved for both the conventional and the proposed implementation, and gives a brief analysis.

1. Introduction

This chapter provides an overview of the work presented in the succeeding chapters. Firstly, we explain the motivation for using the biometric authentication systems including the collaboration which inspired and supported our effort. Secondly, we discuss the design and implementation issues, and summarize the existing standards and solutions. Finally we conclude the chapter with brief introduction to our approach.

1.1. Motivation

Reliable identity management systems are vital to many daily-life applications where services are rendered only for the legitimately enrolled users. Some of the examples include gaining access to nuclear facilities, boarding commercial flights, performing online financial transactions, or sharing networked computing resources. This need is further enhanced with the widespread and decentralized provisioning of services where the intended security arrangements are undermined in event of loss, sharing, manipulation, or theft of knowledge-based or token-based information required for identification [1].

The International Business Machine Corporation (IBM) recognized the criticality of these systems and the weaknesses of the employed identification mechanism in the late 1960s during an analysis performed in the context of computer data security. The corporation determined that the computer users can be identified on the basis of something they know, memorize, or possess. However, it kept its focus strictly on voice recognition as possessed characteristic for human identification [2]. This marked the beginning of a new era introducing biometrics as the potential identification mechanism in identity management systems.

Later by the end of 1970s development of human recognition technologies were extended to the inclusion of hand geometry, face, fingerprints and automated handwriting as potential biometric traits. Since then the biometric research has witnessed tremendous growth resulting into the development of innovative sensors, novel feature extraction and matching algorithms, improved test methodologies, and cutting edge applications [2]. These advancements have established biometric systems as a reliable means of automated person identification in a variety of commercial, civilian, and forensic scenarios. For instance, in the recent past face scanners have been installed at Heathrow Airport to minimize the influx of illegal immigrants who fly inland for settlement after switching

their boarding pass with the local accomplices in the waiting lounge intended for both international and domestic passengers.

With time a number of small and medium sized companies have surfaced to acknowledge and employ the potential of biometrics for the secure functioning of socio-economic systems. Their proposed solution range from unimodal to multimodal solutions designed and developed with strict focus on selected modalities. One such startup company is BIOMETRY.com which has taken significant initiative in this arena by placing mobile biometric solutions at the heart of its strategy. The company offers a multimodal biometric system relying on face recognition and voice recognition. However, the initial patented offering is restrictive in design and implementation, and hence suffers. The limitations originate from the strict focus on face and voice as the selected set of biometrics, the lack of consideration for the scenario-specific needs, and dependency on the selected tools, devices and technology. In case a usage scenario necessitating a different combination of biometrics and implementation technology surfaces, the company needs to implement a new solution from the scratch. Furthermore, BIOMETRY.com is a solution provider for companies needing fused biometric processes for authentication. It needs to build pilot quickly and deploy them at large scale. The company does not develop biometric algorithms on its own but uses existing unimodal solutions, changing from one unimodal to another also demands a full re-development. The recurrent situation incurs substantial cost as well as time, later being the decisive and hence crucial factor in the competitive real world of today.

In order to explore potential possibilities capable of reducing the required time and related development cost, Biometry.com and the Distributed Computing research group of the University of Tartu have joined forces to perform exploratory research on the possible usage scenarios, elicitation of the authentication needs, identification of the relevant design and implementation issues, and the formulation of a generalized solution. For the purpose of this effort, the identified and considered usage scenarios pertain to the banking system referred to as BiometryBank (refer to Chapter 3). We consider that the BiometryBank requires multimodal biometric authentication systems for authorized online and ATM based transactions (refer to Section 3.2.1), background checks (refer to Section 3.2.3), and access to networked resources (refer to Section 3.2.2) and protected areas like bank vault (refer to Section 3.2.4).

Each of these usage scenarios require a different number and type of biometric authentication systems as the variation in environment, usage, and desired level of security necessitates the deployment of the scenario-specific multimodal biometric authentication system. For instance, the online financial transaction process requires a multimodal biometric authentication system comprising of face recognition and voice recognition module along with random challenge. The immediate availability of web camera and the microphone facilitates the end user, and random challenge deters spooking attack. On the other hand, the ATM based transaction can easily be made secure via authentication based on the provisioning of face and fingerprint data as today there are some ATM kiosks which come with both the inbuilt camera and the inbuilt fingerprint scanner.

The deployment of these two multimodal biometric authentication systems require that systems be developed from scratch, or at least the integration code be written each time a system is selected for formation of multimodal system. The process takes up substantial time and incurs costs which can be avoided if the already existing unimodal systems can be reused rather than redeveloped. We envision that this can be achieved through divide-and-conquer strategy. That is, if the required multimodal system is divided into small components which are developed once but integrated on need basis, the related time and costs can be saved.

Generally, we need to consider a multitude of factors while designing a multimodal biometric authentication system. These include

1. the biometric traits of choice and their count,
2. the integration level for combining the data acquired from multiple biometric traits,
3. the integration methodology, and
4. the tradeoff between cost and performance [3].

The usage scenario largely determines the selection and cardinality of biometric traits. The selection of multiple traits introduces overhead like additional computational demands and cost. This requires consideration of certain decisive factors like correlation between the selected traits. The uncorrelated biometric information is preferred as it improves the performance substantially. Further, the performance needs can be addressed by introducing indexing mechanism in case of the widely deployed multimodal systems [4].

One example of usage scenario could be the option to perform financial transactions via smart phone or ATM once the user is successfully authenticated. For authentication over smart phone, face recognition and voice recognition systems can be deployed as the chosen biometric traits are convenient to use. Whereas for authentication at an ATM, it might be easier to deploy fingerprint recognition system and face recognition system.

Once a decision has been made on these factors for intended multimodal biometric system, the fundamental software engineering challenge comes into play. The implementation of a multimodal biometric system requires either or both of the following:

1. Acquisition of commercial or open source unimodal biometric system(s)
2. Development of constituent biometric modalities from scratch.

Irrespective of implementation strategy, significant amount of development and adaption effort, which in turn incurs substantial direct and indirect costs, is required. Opting for commercial systems yield acquisition cost, whereas the differences in implementation technology and deployed equipment may necessitate integration via wrapper classes which makes up for the development cost.

1.2. Existing Solutions

A number of standards have been introduced to resolve the software engineering challenge of having a balance between flexibility and abstraction through provisioning of common software interface. We present a brief summary here, and discuss these standards in detail in Chapter 2.

Common Biometric Exchange File Format (CBEFF) provides data structures for easy integration of heterogeneous hardware and software. However, it does not introduce compatibility between the components on its own and requires the developers to address the shortcomings [9]. BioApi offers interoperability through two of its APIs but it suffers from pointer indirections and ill memory management [10]. Human Recognition Services (HRS) provides biometric services which can only be used in conjunction with other security modules offered by Common Data Security Architecture [8]. There also exist additional standards, for instance X9.84-2000 [8] and ANSI B10.8/AAMVA [8], which are either industry-specific or biometric-specific.

There are also some frameworks designed to facilitate the development of multimodal authentication systems. The Activity based Verification, Identification and Evaluation Framework (AbVIE) is a Java based black box approach with limited usage owing to its focus on behavioral biometrics only [11]. Multimodal Biometric Authentication Framework (MBAF) is a flexible distributed approach for integrating existing applications [12]. However, it is BioAPI incompliant, and inflexible for integration of native code and parallel uses of modalities. Multiplatform Java Native Interface wrapper for BioAPI framework resolves the incompatibility between platform-specific wrappers, and provides an instantaneous and flexible solution for developing multiplatform web-oriented unimodal and multimodal biometric applications [13].

Last but not the least, there exist some worth mentioning authentication solutions. Local Authentication Subsystem (LASS), for instance, provides infrastructure for authentication independent of application and mechanism [17]. However, it does not support activation of multiple modules. MBASSy [17], on the other hand, allows activation of multiple modules but is intended for Andriod based systems. The WhoIsIt biometric server converts encrypted biometric information to password [18], but is difficult to integrate because of technological, platform and vendor dependence. Universal Biometric System (Universal BioSys) overcomes the weaknesses of BioAPI and introduces two novel ideas: many-to-many device-to-host mapping and device hierarchy [19]. But it is limited in application and does not support automatic deployment.

1.3. Proposed Approach

Although these standards, frameworks, and solutions do not minimize associated development and integration costs, they provide us with ample ground to proceed with. We propose an approach: Specification, Configuration and Deployment (SCD) process, which is contrary to the prevalent development processes. The prevalent processes are carried out in full from requirements engineering to deployment and maintenance. The possibility of reusability is therefore very low in these processes. Our approach enables reusability of a-priori developed unimodal biometric authentication systems, and therefore reduces the required time and development effort significantly. Our SCD process starts off with the specification of authentication needs for a usage scenario under consideration. For instance, in case of multimodal authentication system deployment for online transaction security, BiometryBank specifies that it needs a multimodal system comprising of face and

voice recognition modules. The voice recognition module should be accompanied by random challenge to minimize the spooking attacks. The deployed multimodal biometric system should be independent of already existing system as the bank intends to deploy another internet banking system in a year's time. Furthermore, the deployed system should be independent of underlying technology, platform, and devices as these differ from end-user to end-user. Input to all biometric modules is mandatory for the end user. This specification is then used to generate configuration graph which provides all the information including technical details required for the deployment.

We provide a Configuration Tool (see Chapter 4) which assists the customer in specifying the desired multimodal biometric system. During specification the tool proposes the unimodal biometric systems already existing in the repository. One-time development effort has been undertaken to ensure that the available unimodal systems can be integrated as and when the needs arises, without any need for gluing code. By the end of specification phase, the Configuration Tool generates a configuration graph which is used by the Deployment Tool for deploying the configured multimodal systems.

Our presented Deployment Tool (see Chapter 4) deploys and integrates the configured multimodal systems into the existing system. The deployment begins with the spawning of virtual machines which host the deployed selected unimodal biometric authentication systems and random challenge modules. It also installs and initializes the devices, and sets up the network to ensure integration and system availability for authentication when needed. Once all components are set up, the deployed multimodal system(s) is/are launched and tested for smooth functioning of the entire system.

The deployment of our multimodal authentication system for logical access needs of BiometryBank starts with spawning a Xubuntu based virtual instance. The launched instance hosts the deployed Java based face recognition, Python based voice recognition and C++ based random challenge for voice recognition system. The network is configured to make the hosted multimodal solution accessible by BiometryBank's clients, and in the end deployed unimodal systems are launched and tested.

1.4. Summary

The recent rapid developments in networking, communication and mobility have heightened concerns for security which in turn have created a necessity for reliable

authentication mechanisms. Biometrics is gaining acceptance as a legitimate and reliable method owing to its inherent properties. Authentication systems relying on biometrics are being deployed in commercial and civilian applications. Unimodal biometric systems offer authentication on the basis of single biometric trait. Despite the wide deployment these systems exhibit a multitude of limitations; noise in sensed data, intra-class variations, distinctiveness, non-universality, spoof attacks, and unacceptable error rates. Some of these weaknesses can be overcome by multimodal biometric authentication systems. However, the deployment of scenario-specific multimodal systems remains a software engineering challenge owing to the associated substantial development and adaption costs. A number of standards, frameworks, and solutions have been introduced to resolve the software engineering challenge of having a balance between flexibility and abstraction through provisioning of common software interface. Although the proposed solutions do not minimize the associated development and integration costs, they provide us with ample ground to proceed with. We propose an approach which replaces the repeated scenario-specific development by one-time development effort and repeated configuration and deployment process. Our approach: Specification, Configuration, and Deployment (SCD) process starts off with specification of required biometric authentication system. This specification is used by the Configuration Tool for configuring the specified biometric modules. The Configuration Tool generates a configuration graph which is used by our developed Deployment Tool for setting up and initializing the configured modules for the required multimodal systems.

2. Related Work

This chapter elicits the unaddressed integration problem through discussion on related research efforts and existing solutions. There are several approaches dealing with better interoperability and abstraction like biometric standards, authentication frameworks and solutions that are related and worth mentioning here.

2.1. Biometric Standards

The biometrics industry consists of more than 150 hardware and software vendors, each one of them with their own proprietary algorithms, data structures, and interfaces [7]. In order to address this issue, many standards emerged. They all define a common software interface. Furthermore, they allow template sharing, and comparison and evaluation of different biometric technologies. Whereas most of these standards are technology independent, standards specific to the underlying biometric technology (like fingerprints and facial identification data) have also been developed [8]. Further, some of these standards are being continuously revised to accommodate integration of multiple unimodal biometric systems.

The Common Biometric Exchange File Format (CBEFF) is a standard that provides a set of data elements capable of supporting biometric technologies independent of underlying hardware and software. CBEFF enables data interchange between heterogeneous entities, promotes interoperability, offers forward compatibility for future improvements, and simplifies the software and hardware integration process. It should be noted here that CBEFF only facilitates the identification and co-existence of different biometric technologies in a system. It does not introduce compatibility. Also, CBEFF does not provide content definition for the data structures it defines. This limitation requires the application to have knowledge on used patron and data encoding scheme [9]. For instance, consider the application of CBEFF in the fingerprint module deployed for the ATM based transactions (detailed in section 3.2.2). In this usage scenario, the knowledge on object structure for fingerprint data storage would not suffice. The selected fingerprint recognition module would need to know if the fingerprint data was stored by the BiometryManufacturer's fingerprint scanner in little endian or big endian format.

The Biometric Application Programming Interface (BioAPI) is an open-systems standard developed by a consortium of more than 60 vendors and government agencies. The

standard promotes interoperability by providing an interface between a wide variety of biometric technology modules and applications. The interface ensures easy substitution of biometric technologies, and easy integration of multiple biometrics. Further, it allows utilization of the same biometric technology across multiple applications. This platform, technology, and vendor independence is achieved through provisioning of two separate APIs; An Application Program Interface (API) for the application developers and a Service Provider Interface (SPI) for the device manufacturer [22]. The availability of standard basic and primitive functions, and biometric data format; an instantiation of CBEFF, enables rapid application development which in turn assists in cutting down costs through competition [5]. However, the complex (union) data structures, pointers with level three indirection on average, and gruesome memory management requires more than average development skills and incurs substantial effort [22]. Furthermore, we consider this standard as an exaggerated software engineering effort as it does not simplify the problem while introducing structure and relative ease. This structure versus simplicity dilemma especially serves as a bottleneck for many small companies with good ideas but limited finances.

Human Recognition Services (HRS) is an extension of Open Group's Common Data Security Architecture (CDSA) which is a set of layered security services and cryptographic framework [8]. CDSA provides infrastructure for creating interoperable security enabled applications for client-server environments. The HRS module offers biometric authentication services which are used in conjunction with other security modules (digital certificates, cryptographic, and data libraries) offered by CDSA. The biometric component of HRS is compatible with the BioAPI and CBEFF specification. The HRS standard does not serve our purpose as it confines itself to client-server architecture where as we focus on component based approach. However, this standard can be of use in our future efforts addressing certificate and licensing related aspects.

Additionally there are some industry-specific and biometric-specific standards. For instance, X9.84-2000 is a CBEFF compatible standard meant for biometrics management and security in the financial services industry [8]. Similarly, ANSI B10.8/AAMVA [8] is a BioAPI and CBEFF compatible data format for fingerprint minutiae, and ANSI/NIST-ITL-1-2000 [8] is a data interchange format defined for the fingerprint, facial, scar mark, and tattoo (SMT) information. Yet another standard, entitled "Information Technology - Identification cards - Integrated circuit(s) cards with contacts - Part 11: Personal

verification through biometric methods", specifies inter-industry commands and data objects useful for personal verification with biometric methods based in integrated circuit cards like smart cards [8]. These standards are continuously revised to meet the practical needs of authentication scenarios, but the efforts remain segregated as the standards are application specific.

In our approach we consider accommodating as many standards as is possible, but our prime focus remains on the general integration of commercial and open source solutions irrespective of their compliance to any of the above mentioned standards. As the future efforts elicit more usage scenarios yielding more information for the stabilization of our approach, we believe that we'll accommodate the more widely accepted standards like BioAPI, CBEFF and HRS.

2.2. Biometric Authentication Frameworks

The Activity based Verification, Identification and Evaluation Framework (AbVIE) is a Java based framework and runtime environment designed to assist developers and analysts of behavioral biometric authentication systems in developing, evaluating, and comparing their biometric solutions. The framework regards the authentication approach as a black box, and allows the user to prepare a property configuration file for a new authentication approach. Following this, the user has to extend and implement the defined approach using the appropriate interface(s): the identification and/or the verification interface. The framework takes responsibility for event data transmission and allows the developer to focus on the actual algorithm implementation [11]. Despite the advantage of the black box approach, the required development effort and focus on behavioral biometrics restricts the usage of the AbVIE framework. It is a research effort, and its usage is limited to related research efforts.

The Multimodal Biometric Authentication Framework (MBAF) is a flexible distributed approach for integrating existing biometric software modules. The Java based framework offers network transparency, end-to-end encryption, biometric data management services and a set of base classes for biometric authentication applications. However, the implementation for MBAF is BioAPI incompliant, and has no registered owner for the biometric data format thwarting massive adoption owing to potential incompatibility between systems and devices. Further, the framework is inflexible for integration of native code and parallel use of modalities [12].

The Multiplatform Java Native Interface wrapper for BioAPI framework addresses the BioAPI's compatibility issues between different Java wrappers available for windows and Linux/Ubuntu. The modified interfaces support distributed behavior via access to low-level primitives. Further the framework uses web services technology as middleware for improving interoperability, and facilitates development of multiplatform web-oriented biometric applications. This research effort provides an instantaneous and flexible solution for developing multiplatform web-oriented unimodal and multimodal biometric applications [13].

Yet another open source approach introduces a BioAPI based Java framework for biometric web authentication. It offers maximized portability, maximized interoperability, and maximized code reusability and maintainability. It also allows the use of free open source software, and provides multilingual support for all deployment platforms. The acquisition process and biometric authentication or verification mode is specified in an XML document. The intermediate data and outcomes are persisted in database which can be accessed for web based user authentication through centralized authentication service (CAS). The portability of this client-server model based application to mobile devices yet remains to be seen [14, 15, 16].

2.3. Biometric Authentication Solutions

Recent research and development efforts strive to address biometric authentication needs for enterprises and individuals. A few worth mentioning authentication solutions are described here.

The Local Authentication Subsystem (LASS), designed for Windows Mobile, provides an infrastructure that allows user authentication independent of application and authentication mechanism. It supports deployment of alternative authentication algorithms at Dynamic Link Library (DLL). However, it does not support the activation of multiple biometric authentication modules [17].

The Modular Biometric Authentication Service System (MBASSy) is meant for Android operating system. It provides an infrastructure that allows the implementation and usage of alternative authentication procedures. Further, in comparison to LASS, MBASSy allows its users to activate multiple authentication modules at the same time [17]. However, it strives to promote authentication on mobile devices and hence is limited in usage.

The WhoIsIt biometric server is an internet based application server designed for centralized encrypted biometric-to-password conversions for user initiated e-commerce transactions. The server needs to be aware of underlying technologies and restricts users to vendors in a commercial agreement. This essentially translates to platform, technology, and vendor dependence which hinders integration to a significant extend [18].

Universal Biometric System (Universal BioSys) is a proof of concept third party biometric authentication system based on BioAPI. It offers an easy-to-use development environment void of the weaknesses offered by BioAPI. Further, it introduces two novel ideas; many-to-many mapping and device hierarchy. Many-to-many mapping reduces the total cost of ownership by mapping m biometric devices to n hosts. The Device Hierarchy introduced by many-to-many mapping enforces tighter security by necessitating authentication at all possible organizational levels. However, Universal BioSys is limited in its applications as it only caters for some basic security and network practices. Furthermore, Unversial BioSys is a client-server architecture, which does not support automatic deployments [19].

The aforementioned research efforts require or assist in the development of partial or complete multimodal biometric authentication systems through provisioning of wrapper classes or architectural details. In most of the approaches focus remains restricted to usage industry, selected (subset of) biometrics, or platform for implementation. Although these approaches do not provide seamless scenario-specific automatic integration of heterogeneous unimodal biometric systems, they form a good potential base for our component based approach elicited in the succeeding chapters.

2.4. Summary

A number of standards have been introduced to provide common software interface. Common Biometric Exchange File Format (CBEFF) provides data structures for easy integration of heterogeneous hardware and software. However, it does not introduce compatibility on its own and requires developers to address the shortcomings. BioApi offers interoperability through two of its APIs but it suffers from pointer indirections and ill memory management. Human Recognition Services (HRS) provides biometric services which can only be used in conjunction with other security modules offered by Common Data Security Architecture. There exist additional standards which are either industry-specific or biometric-specific. Furthermore, there are some frameworks designed to facilitate the development of multimodal authentication systems. Activity based

Verification, Identification and Evaluation Framework (AbVIE) is a Java based black box approach with limited usage owing to its focus on behavioral biometrics only. Multimodal Biometric Authentication Framework (MBAF) is a flexible distributed approach for integrating existing applications. However, it is BioAPI incompliant, and inflexible for integration of native code and parallel uses of modalities. Multiplatform Java Native Interface wrapper for BioAPI framework resolves the incompatibility between platform-specific wrappers, and provides an instantaneous and flexible solution for developing multiplatform web-oriented unimodal and multimodal biometric applications. There also exist some notable authentication solutions. Local Authentication Subsystem (LASS), for instance, provides infrastructure for authentication independent of application and mechanism. However, it does not support activation of multiple modules. MBASSy, on the other hand, allows activation of multiple modules but is intended for Andriod based systems. The WhoIsIt biometric server converts encrypted biometric information to password, but is difficult to integrate because of technological, platform and vendor dependence. Universal Biometric System (Universal BioSys) overcomes the weaknesses of BioAPI and introduces two novel ideas: many-to-many device-to-host mapping and device hierarchy. But it is limited in application and does not support automatic deployment. These approaches don’t solve the actual problem but form sufficient basis for and give direction to our approach.

3. Proposed Process and Model

This chapter describes the proposed Specification, Configuration and Deployment (SCD) process. Further, it elicits multiple usage scenarios and derives specification for relevant biometric authentication systems. The chapter concludes with description of our proposed model: BioBroker Model (BBM) generalized on the basis of elicited specification.

3.1. Proposed Process

The prevalent way of developing multimodal biometric systems encompasses still a completely new development process for each change or new business process. The process starts with the requirements engineering phase and culminates with the deployment and ongoing maintenance.

The prevalent approach introduces some pre-requisites for the customer (for instance, a bank or R&D developing a new authentication system for their employees or their clients). First the customer is expected to know beforehand which combination of biometric systems they require for their business processes. Following this, the desired unimodal systems are either implemented from scratch or acquired for integration. In either case significant development effort is required. Further, the process is ongoing due to maintenance and changes thereafter, and requires additional effort.

Our approach addresses these shortcomings by reducing repetitive parts of the development effort. We replace the service oriented development with an a-priori development of reusable systems, and introduce a repetitive configuration process. Furthermore, we avoid the challenging task of manual configuration by automating this process. Functionality composition and automatic resolution of subservices automates the configuration process which we refer to as specification, configuration, and deployment (SCD) process as is explained in [20]. In comparison to the reference solution here, our approach retains agility and simplicity.

The SCD process strives to automate the provisioning of multimodal biometric systems by establishing an iterative chain of procedural activities: specification, configuration, and deployment. The manual activities include the specification of business processes for elicitation of usage scenario(s) and the identification of related authentication needs, selection of required systems, and installation of necessary hardware. This is contrary to

current research for biometric systems on configuration management as the research mainly deals with software deployments and manual configurations [21, 22]. Whereas in the SCD process, automation of configuration and deployment activities and support for functionality composition places an explicit focus on semantic support rather than on versioning aspects.

During the specification phase, the customer specifies the business process and related authentication need(s), desired biometric systems, point(s) of integration, and required biometric devices for installation. Specification of existing biometric devices and systems is also required during the specification or modification phase. For instance, in the banking scenario briefly introduced in Chapter 1 (and detailed in the next section), the customer specifies their need for multimodal biometric authentication system for physical level access (e.g. vault), and selects face and hand geometry recognition systems for deployment. Following this, the customer describes the surveillance camera system and fingerprint scanner of their choice as the final step during the specification.

The selected multimodal or unimodal biometric systems are automatically configured for the specified biometric devices. If required sub-systems are missing in the specification, they are added to satisfy the functional requirements of the selected systems. The impact of this configuration might be the obligation on the customer to purchase the specified biometric devices, if they are not already in place. The reason is that the selected BioAPI incompliant unimodal or multimodal biometric systems may fail in communicating with the deployed devices. Following this procedure, the configuration object graph (an example excerpt is depicted in figure 6) includes all the information required for the deployment.

The deployment phase pertains to automatic deployment, initialization and launching of the biometric systems specified and configured during the first two phases: specification and configuration. During this phase virtual machines are remotely spawned and configured on remote networks nodes. Following this, the selected authentication systems are deployed and initiated in accordance with the configuration. The SCD process finishes with the execution of tests designed for cross-validation of deployment.

3.2. Specification for Real-Life Biometric Authentication Scenarios

Banking sector is one of the potential industries frequently considered for its potential for deployment of biometric authentication systems for both logical level access: transaction security, network security, and background checks, and physical level access: access control. Therefore, we derive and generalize specification in the following sections through elicitation of authentication needs of a bank.

We are building pilots for a bank due to anonymity here called "BiometryBank". Our customer bank requires multimodal authentication systems for a multitude of authentication scenarios. There is a need for authentication during physical access to vault and safety deposit boxes, and logical access for online financial transactions, transactions at ATM, network security and background checks.

These usage scenarios are illustrated as follows:

3.2.1. Transaction Security

BiometryBank allows its customers to perform transactions via two channels: Automatic Teller Machine (ATM) and internet banking system. For physical withdrawals, the bank has deployed touchscreen and traditional BiometryManufacturer ATMs at multiple locations across the country. For virtual transactions, BiometryBank provides an internet banking interface which allows its customers to perform online financial transactions on provisioning of randomly generated token.

Considering the risks involved in such arrangements, BiometryBank wants to introduce robust and reliable preventive measures (for instance, user identification mechanism, and encrypted communication) appropriate to the usage scenario. As one of the key features, the bank requires the introduced measures to be immune to possible loss and theft, as well as insusceptible to the potential spoofing attacks.

Requirement SIBA-R001: Two distinct multimodal biometric authentication systems are required at the logical access level.

Requirement SIBA-R002: The multimodal system for ATM based transactions should be capable of processing both the touch input and the button clicks.

Requirement SIBA-R003: The multimodal system for ATM based transactions should be capable of interacting with the biometric devices deployed as built-in part of ATMs manufactured by BiometryManufacturer.

BiometryBank plans to introduce a new internet banking system in a year's time. Therefore, it requires that the selected authentication system for internet banking should be independent of the existing system. However, the introduced solution should communicate, directly or indirectly, the validity of the authenticated user to the banking system so that the financial transaction is considered authorized.

Requirement SIBA-R004: The multimodal system for logical access should integrate with the existing system in a decoupled fashion.

BiometryBank illustrates its envisioned transaction flow for the internet banking system as follows: let us assume that we (the bank) have a customer Peter who wishes to transfer 100 Euros from his account to his friend Olivia's account. For this, Peter browses the internet banking interface where he needs to specify his full name, account number and password for login. Peter types in his full name, account number and password. The internet banking interface validates the provided credentials and displays the interface for financial transaction. On this interface, Peter needs to provide Olivia's account number, 100 Euros as the amount to be transferred and a security token auto-generated by the already in place Token Generator application.

Peter accesses another interface (Token Generator application) using any type of installed browser, operating system, and computing device (personal computer, mobile).

Requirement SIBA-R005: The multimodal system for internet banking should be independent of underlying technology and platform.

On browsing, the Token Generator asks Peter to input his account number, position himself in front of the web or in-built mobile camera for input for facial recognition, and read given random string as input for voice recognition. This input is required for generating a random security token. Peter types in his account number, positions himself in front of the camera, clicks the 'Record' button, and reads the given random string loudly.

Requirement SIBA-R006: The multimodal systems should be independent of devices in place.

Requirement SIBA-R007: The multimodal system for internet banking should consist of modules for face recognition and voice recognition.

Requirement SIBA-R008: The selected voice recognition module for internet banking should be accompanied by module for posing random challenge.

Once done with the input of biometric traits, Peter clicks the 'Authenticate' button. On click, the Token Generator processes the input and determines if the user is really the one with the provided account number. Here, it turns out that Peter is the one with the provided account number; therefore Token Generator displays a success message and gives a random security token X which Peter can now use for intended financial transaction.

Requirement SIBA-R009: Biometric input to both biometrics is mandatory.

Peter returns to the interface meant for transactions, and types in Olivia's account number, 100 Euros as the amount to be transferred, and security token X. He clicks the 'Transfer' button to complete the process. The system updates financial figures for both Peter and Olivia, and displays the success message.

Furthermore, BiometryBank explains its desired transaction flow at its own ATMs as follows: there is a customer named Peter who needs to withdraw 50 Euros. He locates an ATM deployed by his own bank. He approaches the physical interface and inserts his ATM card. ATM processes the card to determine if it belongs to the same bank. Peter's debit card is from the same bank so ATM instantly prompts Peter to type in his PIN. Peter types in his PIN. ATM verifies if the typed in PIN is correct. Since PIN is correct, ATM asks Peter to position himself in front of the installed camera for face recognition, and place his finger over the installed scanner for fingerprint recognition. Peter positions himself in front of the camera and places his finger. The scanners read in and process the biometric input for authenticating the user.

Requirement SIBA-R010: The multimodal system for ATMs should consist of modules for face recognition and fingerprint recognition.

Requirement SIBA-R011: The multimodal system for ATMs should be independent of underlying technology and platform.

Upon provisioning of required biometric data, the multimodal system processes it and communicates the outcomes to the CEN/XFS compliant application deployed at the ATM. The ATM application also takes over the control and displays the main menu listing available operations to select from. Peter clicks the withdrawal options, selects 50 Euros as the amount to be withdrawn, collects money and card, and makes ATM available for other customers.

Requirement SIBA-R012: The multimodal system for ATMs should integrate with CEN/XFS compliant ATM application.

Figure 1 lists the object graph derived from the requirements (SIBA-R001 to SIBA-R012) identified for the deployment of desired biometric authentication systems:

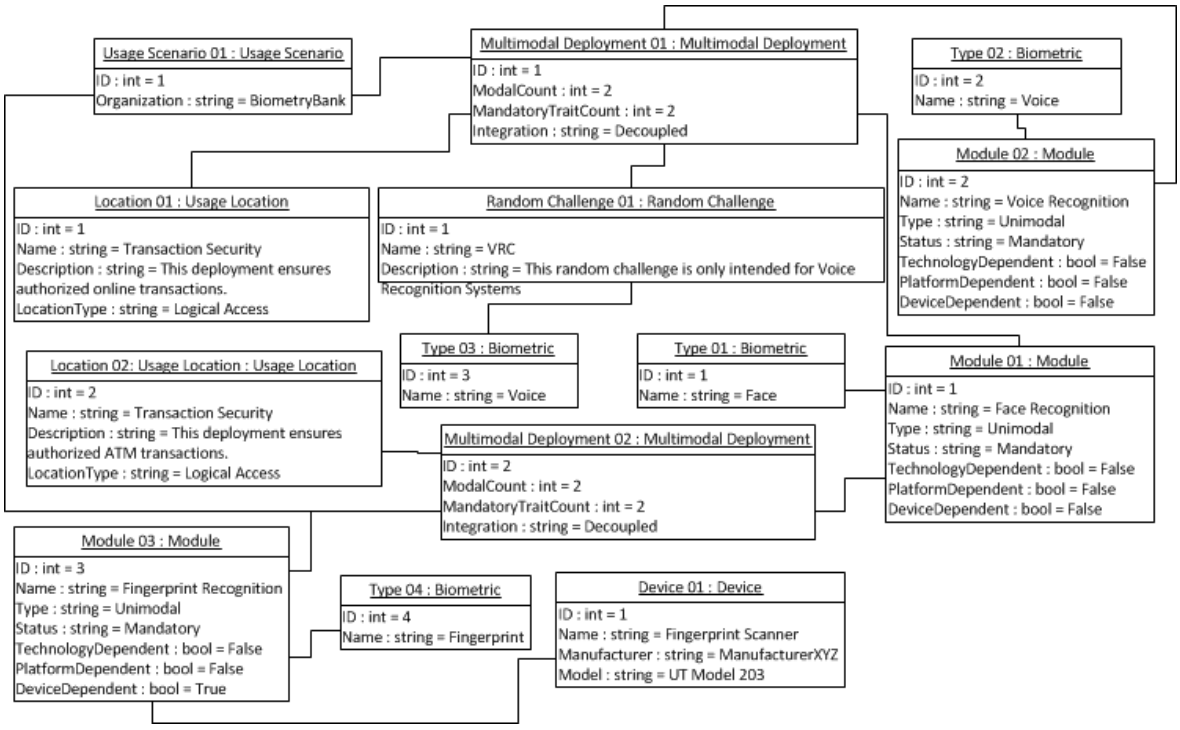

Figure 1. Object graph for multimodal system for transaction security.

3.2.2. Network Security

BiometryBank has all the financial records for its customer from all of its branches in the electronic format. Where the immediate access to these records speeds up the processes, it also poses security threats. The confidentiality and criticality of customer records require authorized access to minimize the occurrences of potential fraud scenarios. BiometryBank understands the need for preventive measures. Therefore, the bank wants to introduce

biometric authentication system for user authentication whenever the networked resources are accessed.

BiometryBank explains its requirements as follows: let's assume that there is a bank employee named Derek who has been appointed as the in-charge officer for an in-process loan application. During application processing, Derek learns from his customer (applicant) that he has an account with another branch which can add weight to his loan application. Although the assertion sounds genuine, Derek needs to validate the claim. For this, he needs to access the customer records from another branch. Derek logs into his system using the fingerprint recognition available as in-built feature in his system.

Once logged in, Derek wants to access the central database for retrieving records, and printer deployed at his floor for printing the account summary as an attachment to the loan application. On access, the system prompts for specification of credentials. Derek types in his username and password. Following this, the system displays three biometric traits: face recognition, voice recognition, and fingerprint recognition, with an option to specify input to any two of the biometrics of his choice.

Requirement SIBA-R013: The multimodal system for authorized access to networked resources should consist of modules for face recognition, voice recognition, and fingerprint recognition.

Requirement SIBA-R014: The user should be allowed to specify biometric input to any of the three biometric modalities deployed for authorized access to networked resources.

Derek chooses to provide biometric input to the facial recognition system and the fingerprint recognition system. Therefore, he selects the biometrics of his choice from the list, and clicks the 'Continue' button. The system gets the input biometric data from the installed devices on user initiated authentication request (i.e. following to the click on 'Authenticate' button). The multimodal system then processes the biometric input, and communicates Derek's legitimacy as a user to the accessed resources.

It should be noted here that BiometryBank has already installed BiometryManufacturer webcams at all of its branches. Considering that it's a fairly recent and large investment, the bank requires that the selected module for face recognition should work with the webcams manufactured by BiometryManufacturer. BiometryManufacturer's webcams are

not BioAPI complaint, but they meet the requirements of any standard face recognition system.

Requirement SIBA-R015: The multimodal system for authorized access to networked resources should integrate with existing network services in a decoupled fashion.

Requirement SIBA-R016: The selected face recognition module should be compatible with BiometryManufacturer's webcams.

In case of network security, BiometryBank does not require random challenge with any of the requested biometric authentication systems.

Figure 2 lists the object graph derived from the requirements (SIBA-R013 to SIBA-R016) identified for the deployment of desired biometric authentication systems:

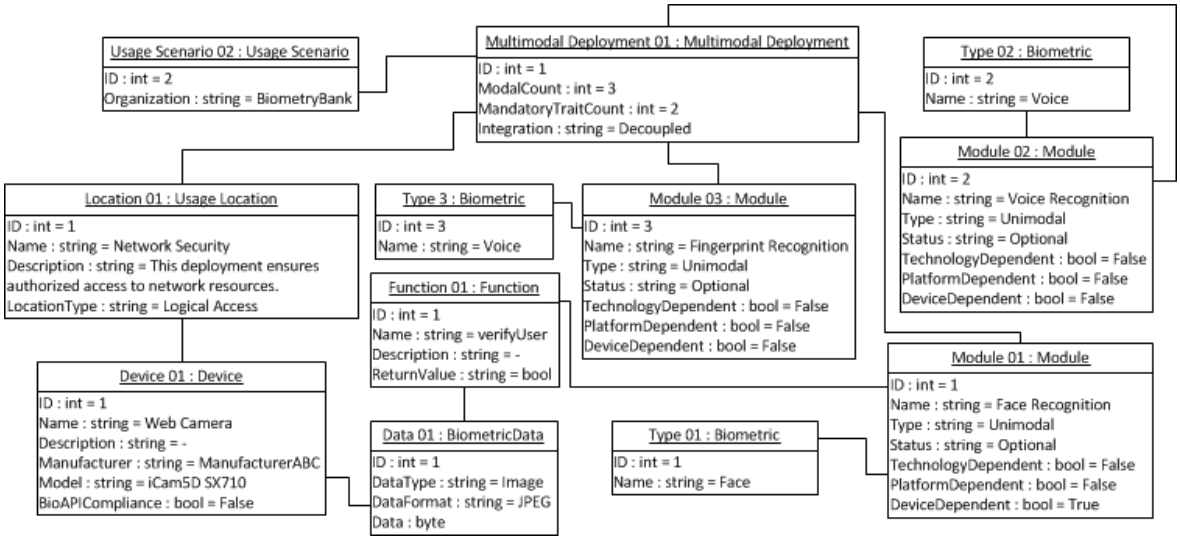

Figure 2. Object graph for multimodal system for network security.

3.2.3. Background Checks

Prior to that a resource is hired, resource's profile (criminal activities and credit) as well as background (academic and employment history) needs to be checked. The data acquisition and the manual checks span a duration of four to six weeks on average. While the checks are in process, the institution invests resources in training the candidate and introducing work procedures. In case the checks yield negative results, the investment made by the institutions is wasted. To minimize the costs at the institutions' end, the process needs to be revised in such a way that the time taken for the same is minimized. One way of improving the process is by providing the biometric information online. The provided

biometrics is used for authenticating the person being hired, validity of provided profile, and eligibility of the same person.

BiometryBank acknowledges the need and potential of biometric authentication systems for background checks. Therefore, it requires a multimodal biometric authentication system comprising of face, voice, and fingerprint recognition modules. Once the required system is deployed for usage, the resource under consideration is asked to provide the required biometrics. The recorded biometrics are the used for two purposes. Initially the data is forwarded to the government agencies for screening. Later the same data can be used for internal authentication needs like authentication for logging into system, accessing networked resources.

Requirement SIBA-R017: The multimodal system for employment screening comprises of face recognition, voice recognition and fingerprint recognition modules.

Requirement SIBA-R018: The provided biometrics serves as the training data for similar authentication systems across the organization.

Figure 3 illustrates the object graph derived from the above mentioned requirements (SIBA-R017 and SIBA-R018):

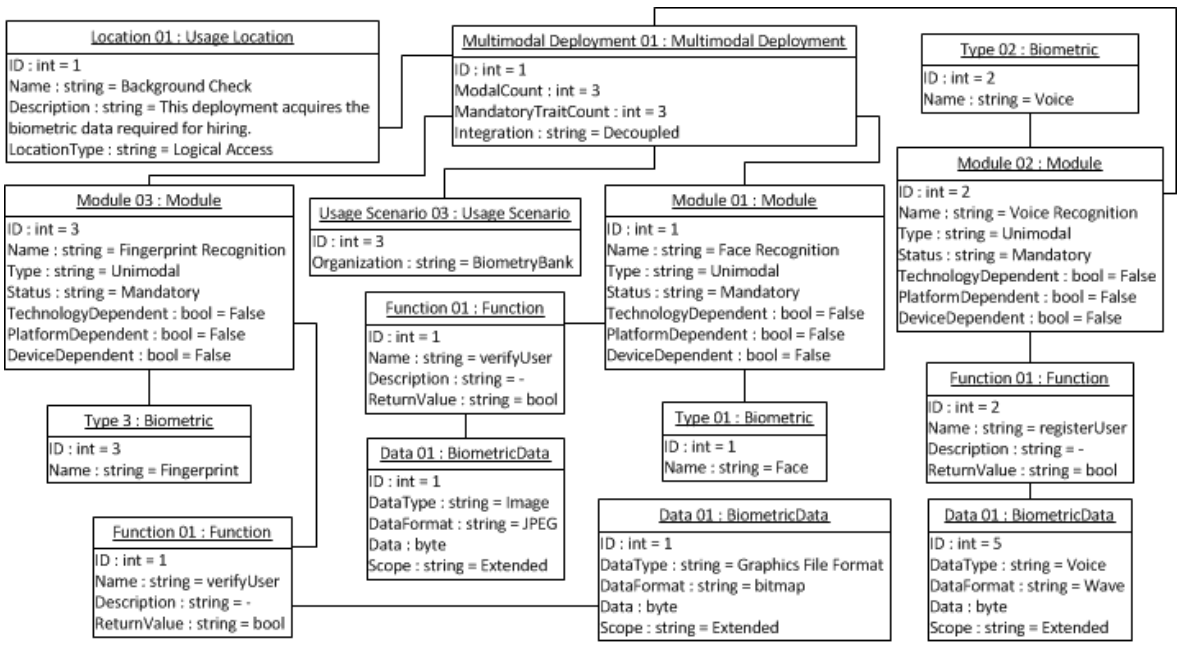

Figure 3. Object graph for multimodal system for background check.

3.2.4. Access Control

Last but not the least BiometryBank requires the deployment of biometric authentication system at physical access level, such as safety deposit boxes, as well. The BiometryBank specifies its need for biometric authentication system as follows: A bank client need to access his safety deposit box. After filling in the request to access, he is accompanied by the bank manager who is authorized to provide physical access to the vault with all the safety deposit boxes.

At the vault door, the bank manager is asked for authentication. The bank manager positions himself in front of the camera for providing input to the deployed face recognition system. He also places his hand for hand geometry recognition system. The system reads and processes the input on "Authenticate" button click. Once positively authenticated, the bank manager is granted access to the vault.

Requirement SIBA-R019: The multimodal system for physical access to bank vault comprises of face recognition, and hand geometry recognition modules.

Requirement SIBA-R020: The biometric input is compulsory for all biometric systems deployed for physical access.

Figure 4 lists the object graph for this usage scenario which is similar to the ones listed previously in figure 1, 2 and 3:

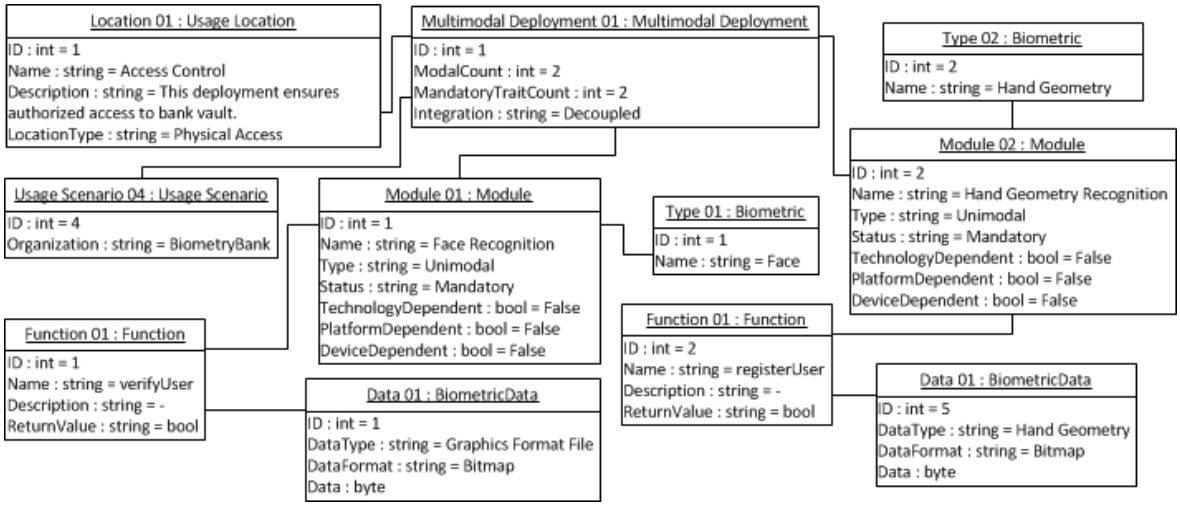

Figure 4. Object graph for multimodal system for access control.

3.3. Proposed Model

Based on these usage scenarios and the preliminary object graphs, we design our model: BioBroker Model (BBM) presented in figure 5. Our SCD process is strongly linked to our model. In general, the BBM is a meta model for describing authentication scenarios, information relevant to the process, biometric systems, and the corresponding runtime environment. The visualization of one particular instance of BBM represents the previously mentioned configuration object graph. An example is visible in figure 6.

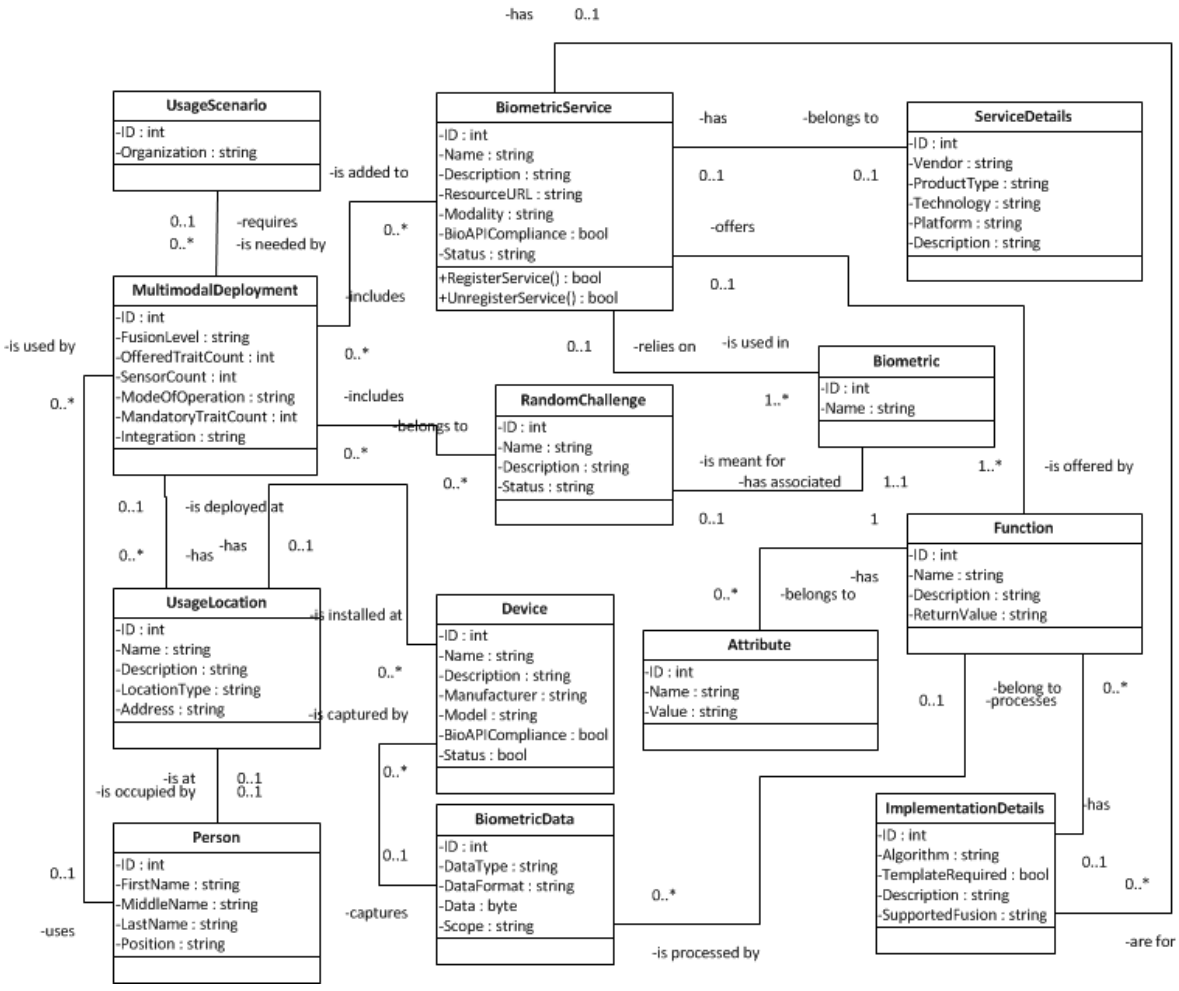

Figure 5. Core of BiometryBroker Model.

Instances of `MultimodalDeployment`, `Function`, and `BiometricService` are essential for the configuration phase. The configuration phase requires details on the deployment needs. The instances of the `MultimodalDeployment` class describe the technical requirements for the desired multimodal systems. The `FusionLevel` specifies if the acquired biometric data will be fused at data or feature, match score, or decision level [25]. `TraitCount` specifies the number of unimodal systems required for this

multimodal system, and SensorCount indicates the number of data samples per constituent system acquired for authentication. Further, the ModeOfOperation field indicates if the authentication system will operate in serial, parallel, or hierarchical mode [25].

The unimodal biometric systems required for the formation of the desired multimodal biometric system are captured by the instances of the BiometricService class. This class describes the modality of selected systems, compliance with BioAPI, and resource URI which is used for deployment. Each of the selected systems offers enrollment, verification, and/or authentication functions which are represented by the instantiation of the Function class. The instances of this class give the information on function name and return type only. Information on function arguments are represented by the Attribute class. Additional details like implementation technology, implemented algorithm, need for data template from user, and supported fusion level is captured by the instances of the ImplementationDetails class and ServiceDetails class.

The UsageScenario, UsageLocation, and Device classes are used to describe the deployment and integration environment. UsageLocation class instances describe both physical and virtual deployment locations. The instances of Device class hold information on BioAPI compliance of devices, manufacturer, and model. It should be noted here that our approach is not restricted to BioAPI compliant biometric systems. The values for stated attributes only ensure that the selected biometric implementations and devices are compatible.

In figure 6, we present a part of object model for multimodal deployment required for our logical access banking scenario. The basic requirement is represented by the MultimodalDeployment class which states that the intended deployment consists of two authentication traits with one sensor per trait. The integration of subsystems is decision level and mode of operation parallel. The instances of BiometricService and Biometric represent the customer selected unimodal systems and related biometrics. Here the customer has specified face and voice recognition systems as their preference. The technical details of selected systems are exemplified by the instances of the ServiceDetails and ImplementationDetails class. These instances indicate the

implemented algorithm and supported fusion for the selected unimodal systems. The supported fusion and fusion level from `MultimodalDeployment` instance match.

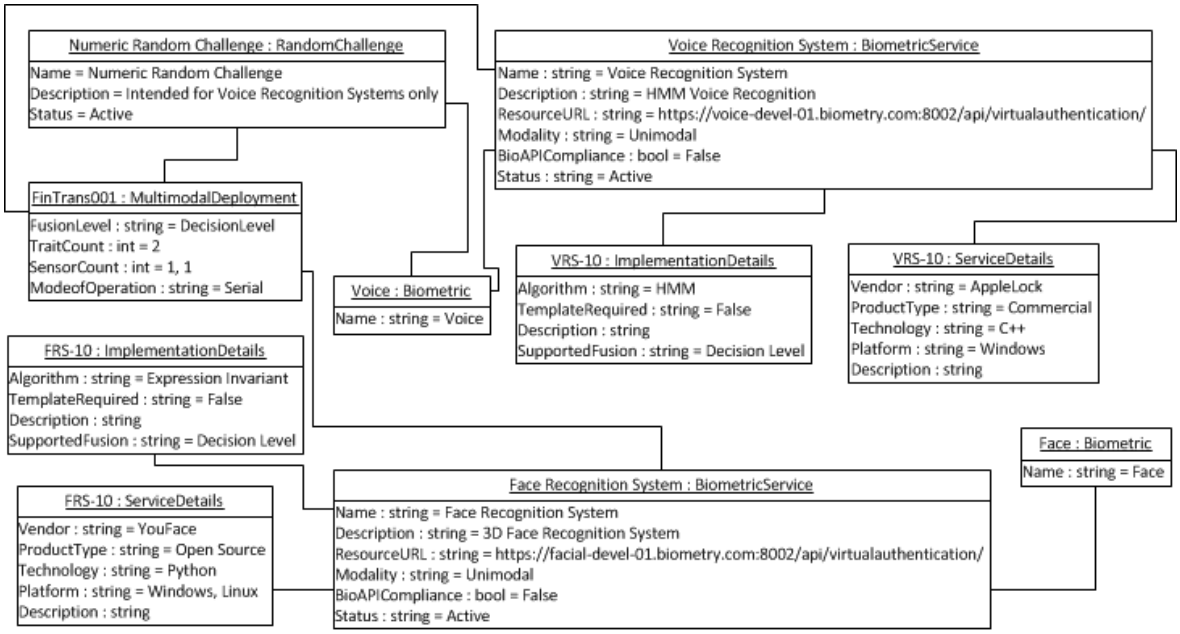

Figure 6. Excerpt from object model for multimodal deployment.

Our customer also wants random challenge with voice recognition system in order to ensure a high level of security. This requirement is represented by an instance of the `RandomChallenge` class which is associated with an instance of the `Biometric` class to classify the biometric nature of the selected random challenge.

3.4. Summary

We show that our approach: Specification, Configuration and Deployment (SCD) process, is contrary to the prevalent development processes which are carried out in full from requirements engineering to deployment and maintenance. The possibility of reusability is therefore very low in these processes. Our approach enables reusability of a-priori developed unimodal biometric authentication systems, and therefore reduces the development effort significantly. Our SCD process starts off with the specification of authentication needs. The specification is then used to generate configuration graph which provides all the information including technical details required for the deployment. For illustration purposes we provide the details on authentication needs of BiometryBank in detail. We describe the usage scenarios both for physical and logical access level. These include the biometric authentication needs for securing online and ATM based transactions, networked resources, background checks, and physical access to the bank

vault. The specification lists the combination of unimodal biometric systems required for each of the identified usage scenario. Further, it elicits the required modality count, module dependency on platform, technology, and devices, and intended level of integration among other defining attributes. On the basis of these details, we derive the requirements which serve as the basis for our model: BioBroker Model (BBM). The BBM lists the classes and associations in between them which once instantiated represents the configuration for intended deployment. Some of the classes crucial to the intended deployment include `MultimodalDeployment` for holding the general details on multimodal biometric deployment, `RandomChallenge` for details on type of random challenge generator to be included in the deployment, `BiometricService` for specification of selected modality, URL for access and information on BioAPI compliance, `ImplementationDetails` for specifying the implemented algorithm and level of fusion supported by the selected modules, `ServiceDetails` for details on technology, platform and devices supported by the selected modules as well as information on commercial or open-source nature of the product, `UsageScenario` for customer's information, and `UsageLocation` for details on access level and deployment address for integration purposes.

4. Implemented Solution

This chapter continues with the description of our SCD process (introduced in the preceding chapter), and provides details on the configuration and the deployment phase. First, we introduce the tools developed for generating the configuration, and deploying the configured multimodal system(s). Next, we present the experimental results. Finally, we concluded this chapter with the analysis of our proposed solution and achieved results.

4.1. Tool Support for Configuration and Deployment

We provide a set of tools for automatic integration and deployment of biometric authentication systems. The set consists of Configuration and Deployment Tool. Source code for these tools is available on request from the contact information listed on the biometry.ulno.net.

4.1.1. Configuration Tool


```
{
  "MultimodalDeployment": {
    "ID": "10",
    "FusionLevel": "DecisionLevel",
    "TraitCount": "2",
    "SensorCount": [
      "1",
      "1"
    ],
    "ModeOfOperation": "Serial"
  },
  "BiometricService": [
    {
      "ID": "1",
      "Name": "Facial Recognition System",
      "Description": "Java based application to authenticate user on the basis of 3D face data",
      "ResourceURL": "http: //facial-devel-01.biometry.com:8002/api/virtualauthentication/",
      "Modality": "Unimodal",
      "BioAPICompliance": "False",
      "Status": "Active"
    },
    {
      "ID": "2",
      "Name": "Voice Recognition System",
      "Description": "Python based application to authenticate user on voice input.",
      "ResourceURL": "http: //voice-devel-01.biometry.com:8002/api/virtualauthentication/",
      "Modality": "Unimodal",
      "BioAPICompliance": "False",
      "Status": "Active"
    }
  ],
  "RandomChallenge": {
    "ID": "7",
    "Name": "Numeric Random Challenge",
    "Description": "Intended for Voice Recognition Systems Only.",
    "Status": "Active"
  }
}
```


Figure 7. Extract of a JSON-based scenario specific configuration.

The configuration tool allows the customer to describe their authentication needs (the specification phase). Upon specification, the configuration tool generates a configuration

file in JSON format which is then used by the Deployment Tool for automatic integration and deployment of selected systems.

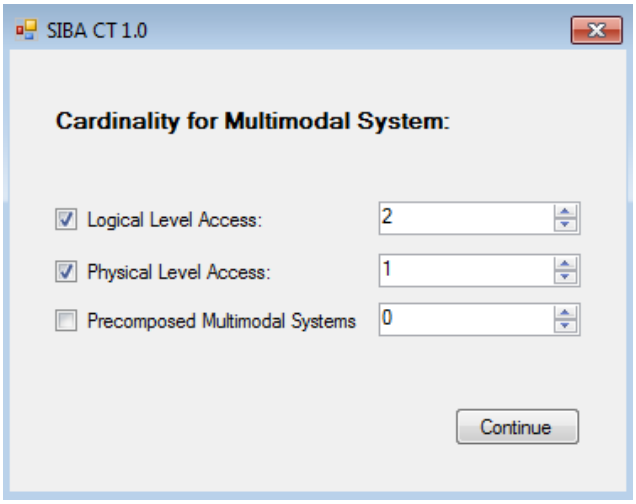

Figure 8. Specifying cardinality for intended multimodal deployment.

During configuration, the customer first specifies the number of physical and logical level access solutions required by their authentication scenario (figure 8). The Configuration Tool helps the customer in specifying each of the desired solutions. For each of the required solutions, the tool suggests appropriate unimodal systems for selection. The customer selects the unimodal systems for integration, and indicates if there has to be an option for choosing a subset of offered biometric authentication systems during authentication (figure 9).

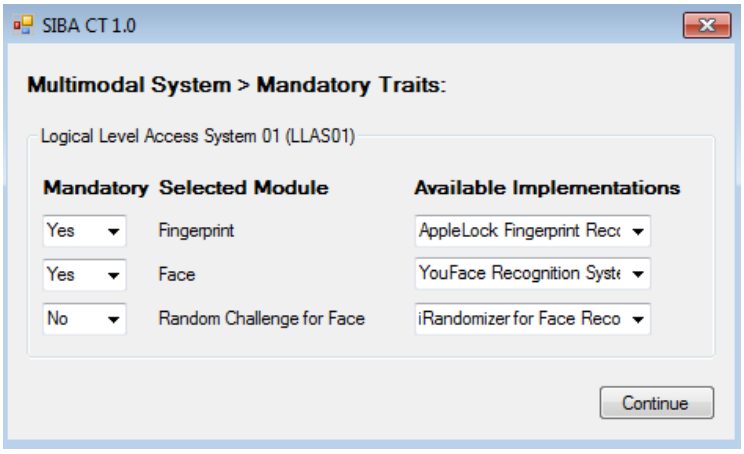

Figure 9. Module selection for multimodal system integration.

Once the requisite software details have been recorded, the customer selects biometric trait readers and sensors appropriate to the selected authentication systems. This step finalizes the multimodal biometric system configuration, requiring the user to install the selected

devices for system usage. The Configuration Tool generates a JSON based configuration file (see figure 7) to end the process.

4.1.2. Deployment Tool

The Deployment Tool receives the generated systems configuration as input and processes it to identify the systems to be deployed and corresponding locations. In accordance with the recorded configuration, the Deployment Tool deploys and integrates the configured multimodal systems into the existing system. The deployment begins with the spawning of virtual machines which host the selected unimodal biometric authentication systems and random challenge modules. These virtual hosts are remotely spawned and configured on target network nodes (figure 10).

```
#!/bin/bash
# Build tunnels to and login to external biometry server hoted at strato
ssh -C biometry-devel.ulno.net -p 4242 -l biometry \
    -L "10223:localhost:10222" \
    -L "5911:localhost:5910"
```

Figure 10. Building tunnel to and login to Biometry server.

Next the selected authentication systems and random challenge modules are deployed. The network is set up to ensure integration and system availability for authentication when needed. The biometric devices are installed and initialized. Once all components are set up, the deployed multimodal system(s) is/are launched, and the deployment process finishes with the execution of tests designed for cross-validation of deployment.

```
#!/bin/bash
# Start the biometry virtual machine

# make sure we get started from the right path
my_path=$(realpath $(dirname "$0"))

cd "$my_path/../vms"
./run.sh &
sleep 2
xvncviewer localhost:10
```

Figure 11. Starting the Biometry virtual machine.

The deployment of our multimodal authentication system for logical access needs of BiometryBank starts with spawning a xubuntu based virtual instance (associated code is listed in figure 11). The launched instance hosts the deployed Java based face recognition, Python based voice recognition and C++ based random challenge for voice recognition

system. The network is configured to make the hosted multimodal solution accessible by BiometryBank's clients, and in the end deployed unimodal systems are launched.

4.2. Experimental Results

In order to perform a comparison between the classic and prevalent on the one hand and our automated approach on the other hand, we have developed a Python and Java based multimodal biometric systems integrating facial and voice recognition systems in a traditional manner.

This multimodal system also incorporates the C/C++ based random challenge for voice recognition system. The system is deployed for logical level access; more precisely, for generating token required for online financial transaction. Additionally, there exist shell scripts for setting up and launching this multimodal system. The Count Lines of Code (CLOC) software [23] yields a total of 118949 SLOC for this development effort. The detailed breakdown of numbers is listed in Table 1.

Table 1. SLOC estimate for traditional development effort.

Language	File	Blank	Comment	Code
Python	335	13907	22269	49414
Java	549	9583	18387	45865
C++	151	3031	4789	15538
C Header	252	2283	5801	7083
Shell	46	322	259	855
C	3	119	102	194
Total	1336	29245	51607	118949

On the contrary, the automated approach does not necessitate any development effort apart from the one-time definition and adoption of constituent biometric systems to fit our SCD process. We take already developed open source and commercial software, and configure them for deployment. The configuration step does not require any coding as it is a set of automatically issued configuration and deployment commands. Only a one-time effort is required for developing Java based Configuration and Deployment tools. CLOC [23] gives a total of 67592 SLOC for both of the tools as is listed in Table 2.

We use COCOMO II model [24] to estimate the cost, effort and schedule required for the two implementations. For estimation, we specified the development flexibility and the team cohesion as high. The personnel related cost drivers are specified as high, and platform related cost drivers as nominal. We consider required software reliability,

database size, and product complexity as high, developed for usability as low, and documentation match to lifecycle needs as nominal. We specified software labor rates as €1200. The estimates are listed in Table 3.

Table 2. SLOC for configuration and deployment tools (one-time effort).

Tools and Adaption	File	Blank	Comment	Code
Configuration	537	9220	17752	43860
Deployment	150	2565	291	18394
Fingerprint	7	418	512	1239
Speaker	6	286	414	1664
Random Challenge	9	410	385	1034
Face Recognition	7	215	390	1401
Total	716	13114	19744	67592

The figures from Table 1, 2, and 3 indicate that our approach reduces development effort and cost by 46.42% at the expense of a few schedule months. It should be noted here that this tradeoff comes with an additional advantage of replacing recurrent efforts required for scenario specific system development by one time effort for both tools development and trait adoption.

Table 3. COCOMO II based cost estimation.

	Effort (Person Months)	Cost (Euros)	Schedule (Months)
Multimodal System	359.1	538693	25.6
Configuration and Deployment Tool	178.6	267945	20.3
One-Time Adaption	13.8	20680	8.7

4.3. Analysis of Proposed Solution and Achieved Results

Service Integration for Biometric Authentication is a proof-of-concept effort. The proposed approach comprises of the SCD process (as discussed in the preceding chapter) and the BioBroker Model. It is a derivation from the identified authentication needs for banking sector. Although biometric authentication needs are more or less the same across usage domains, the integration of biometric authentication systems into existing processes vary from industry to industry. Therefore our approach needs to be enhanced for standardization across various usage domains. The developed tools for configuration and deployment need to be improved for usability as the existing interfaces and application flow suffices the deployment needs but lacks intuitiveness and ease of use. The deployment tool, in specific, is scripts based and focuses on Ubuntu as the intended operating system for deployment purposes. It needs to be improved for adaptability to various deployment technologies and environments. Additionally, the integrated deployment of multimodal biometric systems

and implementation of underlying unimodal systems requires explicit attention to issues like usability [27], interpretability, implementation cost and need for reduction in matching levels [26].

Our experimental results show reduction in development efforts and associated costs by 46.42%. This advantage is gained at the expense of few schedule months. The compromise, however, pertains to the initial one-time development effort required for making a unimodal biometric system configurable and deployable on the go. The results are also restrictive in some ways. They only take the multimodal system comprising of face, fingerprint, and voice recognition systems deployed along with a voice related random challenge module into consideration. In order to generalize the required efforts, test multimodal systems comprising of biometrics other than the ones listed above need to be integrated. The analysis of these systems will yield grounded numbers pertaining to achieved reductions in efforts and related improvements.

4.4. Summary

In order to illustrate the configuration and deployment phase of our SCD process we introduce two tools: Configuration Tool and Deployment Tool. The source code for these tools is available on request from the contact listed on the biometry.ulno.net website. Our Configuration Tool allows the specification of biometric authentication needs, and generates a JSON based configuration file. This configuration file is used as an input to the Deployment Tool for the initialization and launching of the configured biometric systems on the remotely spawned and configured networks nodes. We estimate the impact of our process through comparison of traditional development test case and multimodal system integrated for BiometryBank using our approach. The COCOMO II based cost estimates indicate a reduction of 46.42% in development efforts. We find these results satisfactory and have been able to get them published. Our approach needs to be improved to usability and adaptability to various tools and technologies. Furthermore, additional usage domains need to be considered for generalization and maturity of proposed solution. These test cases will revise and yield more practical numbers regarding reduction in development efforts and related costs.

Conclusion and Future Work

Automatic configuration and deployment of multimodal biometric authentication systems is important for a wide adoption of biometric systems. In this effort we present an approach for specifying requirements for scenario-specific multimodal biometric system(s) comprising various types of unimodal systems, and performing automatic configuration and deployment. We have developed a configuration tool and a deployment tool to support all steps of our SCD process: specification, configuration, and deployment. The configuration tool assists the customer in configuring multimodal system(s) for physical and logical access needs, and generates a JSON based file detailing user requirements. The deployment tool integrates and deploys the multimodal system(s) described in the JSON file.

In the classical development process, significant effort is required for elicitation and analysis of requirements, manual specification and formalization, and programming basic biometric functionality and integrating code. Multiple specialists are engaged for every new usage scenario and deployment environment. Our approach focuses on a-priori development of unimodal biometric systems, thereby eliminating the need for specialists and repeated development process. The remaining tasks required for multimodal deployment can easily be carried out by most of the intermediate customers (like banks or their R&D department deploying a new authentication system) using such configuration and deployment tools.

As this is mostly an academic work so far, there remains a need for improving user interface in our tools and inclusion of more unimodal biometric system on the biometric service provider's side. The availability of multiple modules will allow the customers to choose the constituent systems of their preference. Further research on additional usage scenarios will assist in generalizing our approach, and introducing enhancements in constituent systems for standardization, improved usability, and adaption. For instance, in future we intend to cater authentication needs for the vendor specific ticketing systems intended to facilitate cashless online transactions. Furthermore, our current solution concentrates on Ubuntu based instances instantiated using Virtual Box. In our future efforts, we will also concentrate on the usage of better virtual machine and network integration support for different virtualization technologies, and need for licensing and certificate support to ensure secure network and resource initialization and access.

Biomeetriliste autentimisteenuste integreerimine

Magistritöö (30 EAP)

Autor: Shazia Javed

Juhendajad: Dr. Ulrich Norbisrath, Dr. Eero Vainikko

Resümee

Unimodaalsete biomeetriliste süsteemide kasvav kasutuselevõtt era- ja riigiasutustes näitab biomeetriliste autentimissüsteemide edu. See aga ei tähenda, et biomeetrilised süsteemid pakuvad terviklikku autentimislahendust. Unimodaalsetes biomeetrilistes süsteemides ilmneb hulk piiranguid, mida on võimalik ületada kasutades multimodaalseid biomeetrilisi autentimissüsteeme. Multimodaalseid süsteeme peetakse töökindlamaks ja võimeliseks rahuldama rangeid jõudlusvajadusi. Lisaks võimaldavad multimodaalsed süsteemid arvestada mitteuniversaalsuse probleemiga ja tõhusalt tõrjuda võltsimisrünnakuid.

Vaatamata suhtelistele eelistele on multimodaalsete biomeetriliste süsteemide realisatsioon ja kasutusmugavus jäänud fundamentaalseks väljakutseks tarkvaraarenduses. Multimodaalsed süsteemid on enamasti sulam unimodaalsetest süsteemidest, mis on valitud vastavalt äriprotsessi ja vaadeldava keskkonna nõuetele. Nende süsteemide mitmekesisus, lähtekoodi kättesaadavus ja juurutamisvajadused muudavad nende arenduse ja kasutuselevõtu oluliselt kulukamaks.

Tarkvaraarendajatena üritame me lihtsustada arendusprotsessi ja minimeerides selleks vajamineva jõupingutuse suurust. Seetõttu keskendub see töö olemasolevate biomeetriliste süsteemide taaskasutatavaks muutmisele. Eesmärgiks on kirjeldada teenuste integratsiooni raamistik, mis automatiseerib heterogeensete biomeetriliste süsteemide sujuvat seadistamist ja paigaldust ning vähendab arenduse töömahtu ja sellega seotud kulutusi. Selle eesmärgi saavutamiseks kõrvaldame me vajaduse korduva stsenaariumipõhise ühilduvate süsteemide arenduse ja integratsiooni järgi. Biomeetriliste süsteemide arendus muudetakse ühekordseks tööks. Me esitleme ka vahendeid heterogeensetest avatud lähetekoodiga ja kommerts biomeetrilistest süsteemidest koosnevate multimodaalsete biomeetriliste süsteemide seadistamiseks ja paigaldamiseks lähtuvalt valdkonnaspetsiifilistest autentimisvajadustest. Võrreldes levinud praktikatega vähendab meie lähenemine stsenaariumi-spetsiifilise biomeetrilise autentimissüsteemi arendusele ja paigaldusele kuluvat töö hulka 46,42%.

References

[1] A. A. Ross, K. Nandakumar, and A. K. Jain. “Biometrics: When Identity Matters” in *Handbook of Multibiometrics*. New York: Springer, 2006, pp. 23.

[2] A. K. Jain, A. A. Ross, K. Nandakumar, "Foreword” in *Introduction to Biometrics: A Textbook*, Springer Publishers, 2011, pp. 6.

[3] A. Ross and A. K. Jain, “Multimodal biometrics: an overview.” In: Proceedings of 12th European Signal Processing Conference, pp. 1221-1224, 2004.

[4] E. Bigun, J. Bigun, B. Duc, and S. Fischer, “Expert conciliation for multimodal person authentication systems using Bayesian Statistics,” in First International Conference on AVBPA, (Crans-Montana, Switzerland), pp. 291–300, March 1997.

[5] S. Liu and M. Silverman. A practical guide to biometric security technology. In: IT Professional, 3(1): 27–32, 2001.

[6] S. Venkatraman and I. Delpachitra. Biometrics in banking security: A case study. Information Management & Computer Security, 16(4): 415-430, 2008.

[7] S. Liu and M. Silverman. A practical guide to biometric security technology. In: IT Professional, 3(1): 27–32, 2001.

[8] F. L. Podio. Biometrics - Technologies for highly secure personal authentication. NIST ITL Bulletin, 2001.

[9] F. Podio, J. Dunn, L. Reinert, C. Tilton, Dr. L. O'Gorman, M. P. Collier, M. Jerde, and Dr. B. Wirtz. Common Biometric Exchange File Format (CBEFF). NISTIR 6529, 2000.

[10] BioAPI Consortium. BioAPI specification v1.1 and BioAPI reference implementation. 2001.

[11] A. Messerman, T. Mustafic, S. A. Camtepe, and S. Albayrak. A generic framework and runtime environment for development and evaluation of behavioral biometrics solutions. In: Proceedings of 10th International Conference on Intelligent Systems Design and Applications, 2010.

[12] J. Richiardi, A. Drygajlo, A. Palacios-Venin, R. Ludvig, O. Genton, and L. Houmgny. A distributed multimodal biometric authentication framework. In: Proceedings of 3rd COST 275 Workshop: Biometrics on the Internet, 2005.

[13] E. Gonzalez-Agulla, E. Otero-Muras, C. Garcia-Mateo, and J. L. Alba-Castro. A multiplatform Java Wrapper for the BioAPI framework. Computer Standards and Interfaces, 31(1): 186–191, 2007.

[14] E. Otero-Muras, E. González-Agulla, J. L. Alba-Castro, C. GarcíaMateo, and O. W. Márquez-Flórez. An open framework for distributed biometric authentication in a web environment. In: Annals of Telecommunication. Special issue on Multimodal Biometrics, 62(1-2):1702–1717, 2007.

[15] E. Otero-Muras, E.González-Agulla, J. L. Alba-Castro, and C. García-Mateo. Biometrics for web authentication: an open source Java-based approach, 2007.

[16] E. González-Agulla, E. Otero-Muras, J. L. Alba-Castro, and C. García-Mateo. An open source Java framework for biometric web authentication based on BioAPI. Knowledge-based Intelligent Information and Engineering Systems (Lecture Notes in Computer Science), pp. 809-815, 2007.

[17] H. Witte and C. Nickel. Modular biometric authentication service system (MBASSy). In: Proceedings of the Special Interest Group on Biometrics and Electronic Signatures, 2010.

[18] The WhoIsIt biometric server for E-commerce, Available: http://www.qvbiometrics.com/E_Metrics_server.htm

[19] H. M. N. D. Bandara, S. M. R. P. De Silva, and P. W. H. D. Weerasinghe. The universal biometric system. In: Proceedings of 6th International Information Technology Conference, 2004.

[20] U. Norbisrath and C. Mosler. Functionality configuration for eHome systems. In: Proceedings of the 2006 conference of the Centre for Advanced Studies on Collaborative research, IBM Press, 2006.

[21] A. van der Hoek. Integrating configuration management and software deployment. In: Proceedings of the Working Conference on Complex and Dynamic Systems Architecture, 2001.

[22] B. Westfechtel and R. Conradi. Version models for software configuration management. ACM Computing Surveys, 30(2), 1998.

[23] Northrop Grumman Corporation. CLOC – Count Lines of Code. Internet: http://cloc.sourceforge.net/, Apr. 9, 2012.

[24] R. Madachy. COCOMO II – Constructive Cost Model. Internet: http://sunset.usc.edu/csse/research/COCOMOII/cocomo_main.html, [Apr. 19, 2012].

[25] A. K. Jain, A. Ross, and S. Prabhakar. An introduction to biometric recognition. IEEE Transactions on Circuits and Systems for Video Technology, 14(1): 4-20, 2004.

[26] A. Mishra. Multimodal biometrics it is: Need for future systems. International Journal of Computer Applications, 3(4): 28-33, 2010.

[27] Y. Isobe, Y. Seto, and M. Kataoka. Development of personal authentication system using fingerprint with digital signature technologies. In: Proceedings of the 34th Hawaii International Conference on System Sciences, 2001.