UDC 004.056:004.75:061.1EU
Survey Paper

Technical, Legal, Economic and Social Aspects of Biometrics for Cloud Computing

Jernej Bule *jernej.bule@fri.uni-lj.si*
Faculty of Computer and Information Science
University of Ljubljana, Ljubljana, Slovenia

Peter Peer *peter.peer@fri.uni-lj.si*
Faculty of Computer and Information Science
University of Ljubljana, Ljubljana, Slovenia

Abstract

This article addresses technical, legal, economic and social aspects of biometrics for cloud computing, featuring application example, gains of such solution, current laws, directives and legislation for biometrics and cloud computing. It is primarily based on Slovenian example due to common general EU legislation in the field of cloud computing and biometrics. Authentication on the Internet is still mainly done using passwords, while biometrics is practically not used. It is commonly known that everything is moving to the cloud and biometrics is not an exception. Amount of biometric data is expected to grow significantly over the next few years and only cloud computing is possible to process such amounts of data. Due to these facts and increasing security needs, we propose and implement the use of biometry as a service in the cloud. A challenge regarding the use of biometric solutions in the cloud is the protection of the privacy of individuals and their personal data. In Slovenia privacy legislation is very strong, it permits usage of biometrics only for very specific reasons, but we predict that big players on the market will change this fact globally. One of the important reasons for that is also the fact that biometrics for cloud computing provides some strong benefits and economic incentives. Proper deployment can provide significant savings. Such solutions could improve people's quality of life in terms of social development, especially in sense of more convenient, safer and reliable identification over multiple government and non-government services.

Keywords: biometrics, cloud computing, cloud biometrics, legislation, privacy protection, economic gain, social impact, development

1. Introduction

Usability of biometric methods is reflected in the various fields, but the essence is the same everywhere: the concern for human safety and security of their data and assets. Biometric methods are already quite widely used for local authentication (for private use), while Internet authentication using biometrics is still relatively modest [12]. The main reasons for this state are open challenges pertaining mainly to the accessibility and scalability of existing biometric technology. More widespread use is also mainly limited by law.

However, biometric technology is slowly but noticeably entering our lives [23]. It is reasonable to look at the next generation biometric technology that will have to solve scalability and accessibility challenges that arise particularly from necessity to efficiently handle large numbers of users. The first solution that comes to mind with respect to the outlined challenges, is moving the technology to a cloud platform that ensures entry point for various applications and services [30].

When developing technology for the cloud, number of challenges and obstacles must be addressed. Choosing the most suitable platform, meeting the performance criteria, and developing the engine can be addressed from the technical aspect [30]. Cloud computing privacy concerns and mass use of biometrics in general can be viewed from privacy-legal

aspect. There are also economic and social aspects that needs to be considered, especially in terms of development.

The main purpose of this study is to present architecture of a biometric solution in the cloud, as we noticed that there are no widely known solutions for the architecture of biometric solutions in the cloud. Furthermore, we examine and present advantages and disadvantages that such a solution brings in multiple non-technical contexts, namely economic, legal, and social. In the existing literature very few articles are talking about architecture of biometric systems for the cloud [18], [24].

We describe development process of our solution for fingerprint verification in the cloud in chapter 2, present legal restrictions on the use of biometrics and data privacy protection in cloud computing in chapter 3, economic gain of such integration in chapter 4, social concerns and impact on society of such solution in chapter 5, and predict future development of biometric solutions in the cloud in chapter 6.

2. Technical Aspect

Biometric applications are closely linked to the science and mathematical statistics. Some of the technological considerations will revolve around what is the best biometric technology to be used. The most commonly used biometric methods are fingerprints, iris scanning, voice recognition, face recognition, hand measurements, palm prints, etc. [16].

Matching an individual's fingerprint seems to be the most adequate biometric technique to use, due to its long usage, maturity and reliability [3]. A proof of that are also already existing large fingerprint databases for criminals, military, and similar groups. This is the reason why we use fingerprints in our biometric solution in the cloud, although we could easily replace fingerprints with any other biometric method.

2.1. Biometrics - Overview

A biometric system is a real-time recognition system, which recognizes a person by measuring a particular physical or behavioural characteristic [16]. These characteristics are considered to be unique to each person and unlike knowledge or token-based security mechanisms cannot be forgotten, lost or stolen.

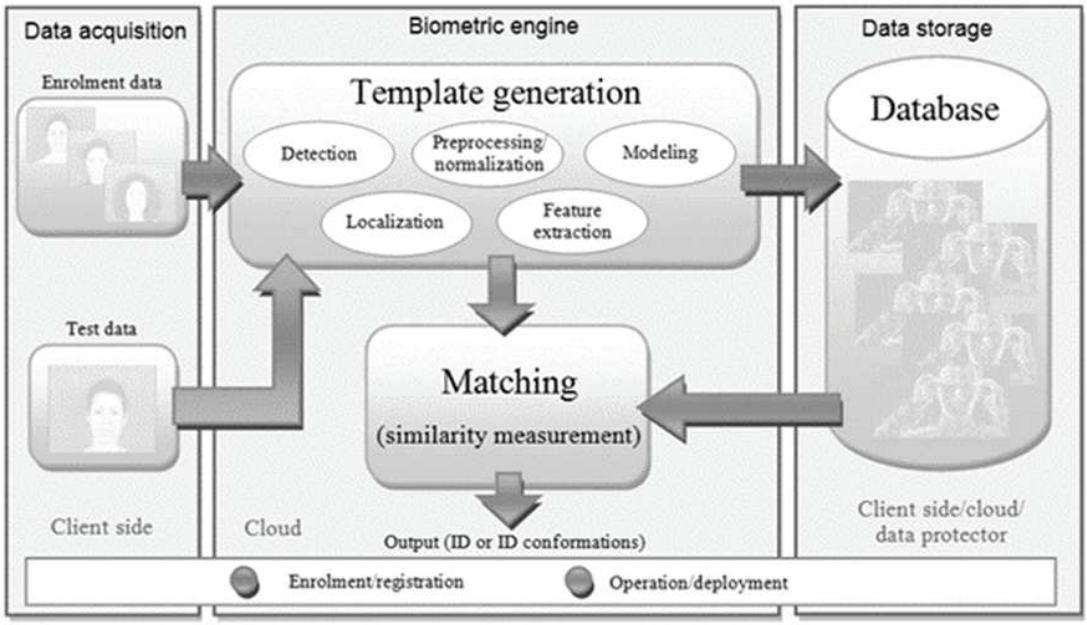

Figure 1 - Block diagram of a typical biometric recognition system [26].

Biometric recognition system can operate in two modes: verification (authentication) and identification. Verification accepts or rejects the identity claim of a person, while identification determines, which of the registered persons a given biometric data corresponds to [17].

A typical biometric system usually contains same basic components (Figure 1), regardless of whether it is made for cloud or some other platform. These components are [30]:

- Sensor that captures still image of user that is trying to enroll into the system or to use the system for verification/identification purposes.
- A template generation component, where input picture is processed. Component extracts features (e.g. minutiae's in case of fingerprint image extraction) and create a template from it.
- A database, where biometric templates are stored. Database can be hosted locally or in the cloud.
- A matching component that compares biometric sample derived from the sensor with those stored in the database. The user is successfully recognised when it comes to pattern matching.

2.2. Cloud Computing - Overview

Cloud computing is no longer on the horizon - it has become the next logical step for the IT industry [5] because it is the most cost-effective technology for hosting Internet-scale applications [2]. Despite the fact that expression cloud computing is new, people use cloud-based services for quite some time now, such as Gmail, Dropbox, Google Drive, Apple iCloud, YouTube and others. As seen in practice, their success is unquestionable. Cloud computing is attractive to business owners as it eliminates the requirement for users to plan ahead for provisioning and allows enterprises to start from basic resources and increase them only when there is a rise in a service demand [32]. Therefore, cloud service has some distinct characteristics that differentiate it from traditional hosting. It is sold on demand, typically by the minute or the hour, it is elastic – user can have as much or as little of service as they want at any given time, and the service is fully managed by the provider (the consumer needs nothing except a personal computer and Internet access) [12].

There are many common definitions of cloud computing, but the most widely used is given by National Institute of Standards and Technology (NIST) [21]: "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.". According to NIST definition the cloud model is composed of four deployment models [21]:

- *Private cloud*: The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.
- *Community cloud*: The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.
- *Public cloud*: The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.
- *Hybrid cloud*: The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

Cloud computing employs a service-driven business model [21]. That means models are based on a type of the service. Service models can be performed in three different ways, which are usually built one on top of another and can be used independently of each other [34]. These three models are Infrastructure as a Service, Platform as a Service and Software as a Service (Figure 2).

Virtualization represents a fundamental building block of infrastructure as a service (IaaS). IaaS is based either on offering individual virtual source (eg. disk) or virtualized server infrastructure, which may fully replace the usual physical server. A typical commercial example of virtual source is the Amazon Simple Storage Service (S3), which represents a single addressable disk space with virtual infinite capacity.

The next step is the platform as a service (PaaS) which takes the IaaS as its basis. Platform hides the infrastructure (physical or virtual hardware) to its users and offers them specific functionality that enables the development of applications. Cloud providers deliver a computing platform typically including operating system, programming language execution environment, database, and a web server. Application developers can develop and run their software solutions without the cost and complexity of buying and managing the underlying hardware and software layers. Google App Engine represents a commercial example of PaaS, which allows developers dynamic and scalable platform for driving applications written in the programming language Python and Java.

Software as a service (SaaS) represents the last step of abstraction. It is designed for end users. Software as a Service means providing the entire infrastructure, including software and settings for its operation. In the SaaS model, cloud providers install and operate application software in the cloud and cloud users access the software from cloud clients. The cloud users do not manage the cloud infrastructure and platform on which the application is running.

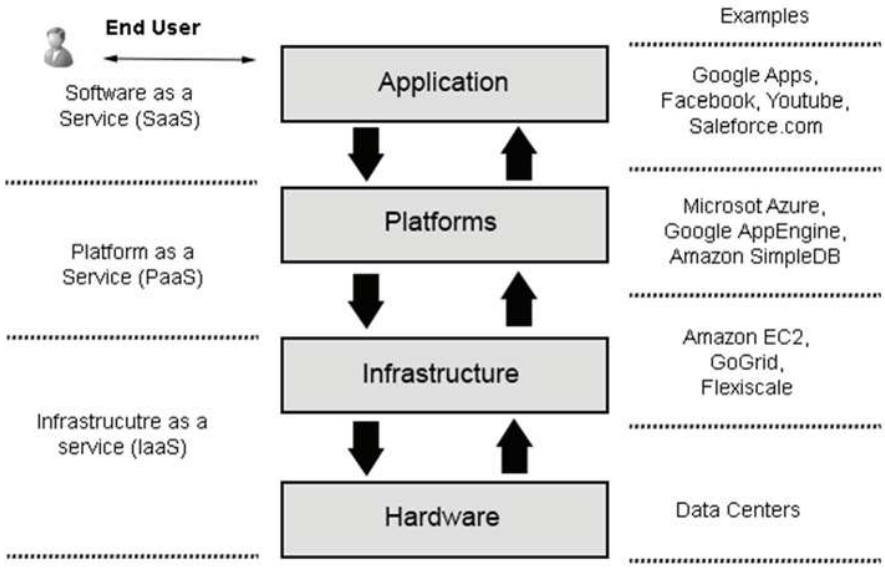

Figure 2 - Cloud Computing Architecture.

Biometrics for cloud computing is deployed in PaaS layer, and provided as a service in SaaS layer.

2.3. Biometrics in the Cloud

When we talk about biometrics in the cloud, first of all, we think about biometric engine, which is located in the cloud and not on some sort of local processing unit, as it is the case with the traditional biometric systems. This feature makes cloud based biometric technology broadly

accessible and provides the necessary means for integration in other security or consumer applications. We can use same biometric templates in multiple applications connected to cloud biometric service, which is not the case in traditional solutions, which operates on the local basis. Second of all, storing biometric data in the cloud makes the system highly scalable and allows quick and reliable adaptation of the technology to increasing user base [18]. Scalability is very important feature that is missing in traditional systems.

The technological capability of biometrics in the cloud is also determined by other existing technological dependencies – e.g. biometrics for secure access is limited since the hardware is a limiting factor; not every computer has a fingerprint reader integrated, which means user must purchase it additionally.

A review of some solutions [6] in the field of biometrics in the cloud showed some common points between them. All solutions operate on the principle of the client-server model. Client is the user's computer, which is responsible for capturing biometric data and sending it to the cloud service (server), where processing is executed. For the safety of network traffic between the client and server, security protocols and mechanisms are used.

In the continuation of the chapter we focus on our own biometric verification system in the cloud, where we use fingerprints – the most widely used biometric [6]. It is necessary to point out that the system concept is independent of the biometric modality and can be replaced with other modalities, such as voice recognition, face recognition, gait etc. A scheme of the system is given in Figure 3, and detailed description is provided below.

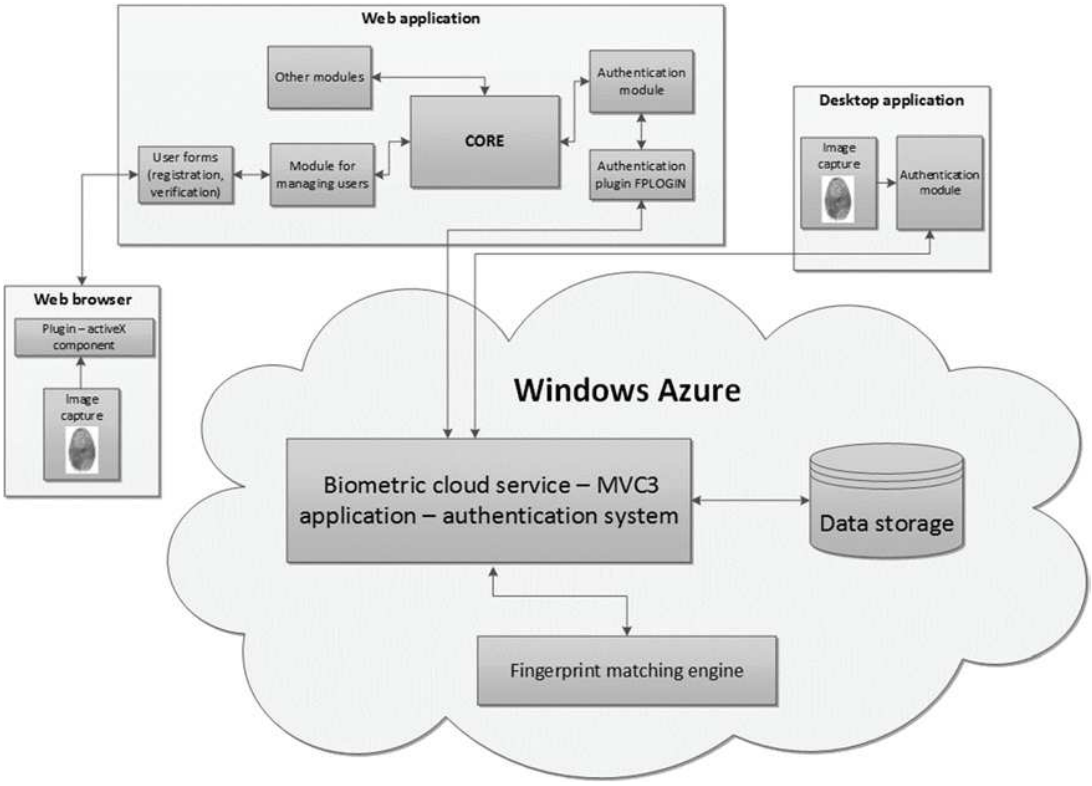

Figure 3 - Scheme of our fingerprint verification system in the cloud [26].

Verification process using fingerprint biometric solution in the cloud is done using a following scenario: First, a fingerprint is captured via fingerprint scanner. Scanner libraries that allows you to capture the image must be integrated into the web or desktop application. Image is captured via ActiveX plugin that activates the scanner. Application (web, cloud, mobile, desktop) communicates with Application Programming Interface (API), which is hosted in the cloud, in our case in Microsoft's cloud platform Windows Azure, and runs as a service. Encrypted fingerprint image is sent to the API, which integrates fingerprint matching engine.

Communication is protected with SSL certificate, which provides additional level of security. Access to cloud service is also protected with 40-digit password. Image is processed in the fingerprint matching engine and results are sent back to the application via API. Biometric database stores only features of the fingerprint, called minutaes – and not the image of fingerprint. All values stored in the database are additionally encrypted. The reconstruction of the original fingerprint image is impossible [26].

Web application that use this biometric solution as a service usually integrate different modules. Authentication module is for sure one of them and it is the part of the application that communicates with cloud service. An integration of our solution in web or desktop application with such an approach is pretty straightforward. Furthermore, proposed solution can be easily applied to different biometric modalities, also in the context of multimodal person authentication.

Biometry in the cloud offers multiple advantages [7]. An infrastructure which runs a biometric engine can be set very quickly with the cloud's virtualization technology. User or organization does not need own infrastructure, data centers and staff for maintenance and expansion. In addition to saving investments in the fixed resources there are also lower operating costs. The main advantage is certainly the elasticity: when the biometric application requires more resources (increased number of concurrent requests) the system can provide it.

One of the biggest features cloud services offer is the ability to create biometric applications with worldwide access. Large enterprises can create one application in the cloud that can be accessed by thousands of users from different locations around the world. Small scale businesses also benefit because they can create small solutions that fit the needs of their company, without having to heavily invest in hardware or software development. Cloud services reduce development costs, infrastructure costs, and the need for IT maintenance and support, while at the same time improving reliability and scalability [1].

On the other hand, storing biometric data in the cloud may raise privacy concerns and may not be in accordance with national legislation. Therefore, the possibility of using a locally hosted database needs to be considered when designing a cloud-based biometric system. Such a setting may limit the scalability of the technology to a certain extent, but is reasonable as it makes technology more easily adjustable to the existing legislation.

3. Privacy-Legal Aspect

3.1. Biometric Legislation

When it comes to legal, privacy and data protection concerns when using biometric data with cloud computing, there are usually no universal solutions, as they differ from country to country. We address privacy from the perspective of Slovenia, because Slovenia is in the EU, and all EU countries have common general legislation [8] – directive on the protection of individuals with regard to the processing of personal data and the free movement of such data.

Slovenian Information Commissioner has composed several guidelines/recommendations both for the cloud as well as biometric technology. The recommendations relating to biometric technology, biometric data protection and template storage fall in the domain of Protection of Personal Data Law [28] called ZVOP-1, while the guidelines for cloud computing are given in [27].

The law in Slovenia allows use of biometrics in the following cases [27]:

- For the *public sector*: when required by law (e.g. citizens travel documents), and exceptionally if it is strictly necessary for the safety of persons or property, for protection of classified information if the purpose cannot be achieved by less restrictive assets. Biometrics can be applied in the case of compliance to mandatory international agreements or identification of individuals when crossing national borders.
- For the *private sector*, only if it is necessary for:
  - safety of persons or property,
  - protection of classified information,

- protection of business secret,
- carrying out an activity.

If the implementation of biometrics in private sector is not required by law, a person who wishes to apply it, must obtain a decision from the Information Commissioner. Applying biometrics without approval from Commissioner is considered as a law violation, which is punishable with a fine. After approval is obtained, biometrics can only be used on employees if they have been informed about it in advance.

3.2. Data Protection and Cloud Computing

Cloud computing promises access to computing resources from any location in an economical, flexible and scalable manner, and it is not surprising that more and more organizations that process personal data are interested in cloud computing [1]. This raises doubts about the compliance with the protection of personal data and privacy legislation.

3.2.1. Data Controllers

According to the provisions of ZVOP-1, the user or contracting entity, which collects personal data, is usually considered as the data controller authority. For instance a company is the controller of its clients and employees, a library is the controller of its borrower's data, etc. Data controllers determine purposes and means for the processing of personal data. This applies to both, public and private sector. Controllers can collect and process personal data only when this is legally permitted. They must respond to complaints regarding breaches of data protection rules and collaborate with national data protection supervisory authorities.

3.2.2. Data Processors

Providers of cloud computing services are treated as data processor authorities, doing some or all of the processing in the data centre under that provider's supervision. ZVOP-1 states that contractor (processor authority) should carry out tasks related to the processing of personal data in the scope of users authorizations and personal information, but data may not be processed for any other purpose.

3.3. Transferring Data Outside the EU

Special difficulties in providing the expected level of protection of personal data raises the related question of exporting personal data to third countries that do not provide the same level of protection for personal data as legislation in country where biometric service is provided.

We talk about data transfer to third countries, when controller authority (which is located in EU – in our case in Slovenia) wants to export personal data to countries outside the EU, or when access to data is enabled to organizations, individuals from third countries. Before data exporting, controller authority must obtain an approval from the Information Commissioner. When deciding about data export, commissioner is bound to the decision of the European Commission, which has already found, that some countries provide an adequate level of protection for personal data. Some of those countries are: Andorra, Argentina, Australia, Canada, Switzerland, Faroe Islands, Guernsey, Israel, and USA (only in specific parts – partially adequate protection). Among the countries in which it is found that protection of personal data is only partially adequate we must highlight USA. Adequate protection is provided by organizations that committed Safe Harbor statement [31]. Safe Harbor statement allows controller authority to transmit their data to processor authority located in the USA, if processor is committed to respect the principles of this contract. Currently there are few laws in the USA that directly address the use of biometric systems or the storage of biometric templates [4]. USA prefers a so-called "sectoral" approach to data protection legislation, which

relies on a combination of legislation, regulation, and self-regulation, rather than governmental regulation alone.

3.4. Privacy Concerns

Most biometric characteristics (face images, voice, iris images, fingerprints, gait, etc.) are exposed on a daily basis. The technology is available to covertly capture these biometric characteristics with different degrees of difficulty. It is necessary to be aware that this fact could lead to identity theft, also when placing biometric data on the Internet. Moreover, raw biometrics cannot be revoked, cancelled, or reissued if compromised, since they are user's intrinsic characteristics and they exist in limited number.

Different biometric applications can have a different impact on privacy. Privacy risks increase when biometric data are stored for an unlimited amount of time. In fact, if the system deployment is indefinite in time, threats such as function creep may become more pressing. If the database is violated, biometric traits related to several users can be compromised. The use of biometrics can have secondary purposes when both governmental institutions and private companies are involved. In different societies one or the other can be perceived more threatening to the privacy. Also the role of the individual (employee, citizen or customer) in the biometric system impacts on the privacy assessment [3].

Concerns about the privacy and use of biometrics for identification purposes surely exists. But the fact is that use of biometrics in a combination with standard identification methods (PINs, usernames, passwords) is much more effective and secure than using just standard methods.

4. Economic Aspect

There are various ways to describe the economic factors affecting biometric development, adoption and use. Biometric technologies are strong recognition techniques and as such they influence the level of trust in economic transactions. In other words, they can help reduce fraud and thus help materialize the efficiency, development and equity gains of the information society. Their widespread deployment in the public sector can make recognition over the network easier, more secure and may bring down costs per secure transaction [14], [12] , [19], [9].

Biometric solution in the cloud, which we presented in this article, has an additional economic impact, unlike standard biometric solutions, because with the introduction of such cloud-based service we save more [12]. Evidence to that is also the announcement of the Slovenian government to establish a national computing cloud with which it aims to cut costs by 45 million Euros [29]. By moving services to the cloud there is no longer need to maintain multiple systems within companies or public institutions. There is also a new way of charging for services – pay-as-you-go. Furthermore, economic gains of cloud solutions result mainly from the following areas [11]:

- *Cost of power*: Power Usage tends to be significantly lower in large facilities than in smaller one. That means big companies profit more than small one (regarding power usage).
- *Infrastructure labour costs*: Labour costs are significantly lower at any scale by automating many repetitive management's tasks. Larger facilities are able to lower them further than smaller ones.
- *Security and reliability*: Large cloud providers are often better able to bring deep expertise to bear on this problem than a typical corporate IT department, thus, actually making cloud systems more secure and reliable. Integration of biometrics introduces additional level of trust and increases security.
- *Buying power*: Operators of large data centres can get discount on hardware purchases over small buyers.

Some advantages of the cloud also include productivity gain, development of innovative services (e.g. biometrics in the cloud), efficient supply chain management, and development of a skilled workforce. The increased use of cloud computing will allow countries all over the world to become more competitive, boost job creation, and better deliver government services [9].

In addition, the growth in cloud computing will drive more investment in broadband networks. As the cloud becomes fundamental to the world of information and communications technology, it will deliver major benefits for both low and high income countries. There are both short and medium-term efficiencies with very large payoffs, as well as the possibility of medium and long-term expansion of local innovation capacity [19]. All this facts talks in favour of economic development in multiple fields.

5. Social Aspect

As with any technology, the developmental impact of biometric identification on society depends largely on the political, technological, and legal context in which it is used. Some cases suggest large returns on biometric identification in economic and social programs, with potential gains in efficiency, governance, and inclusion [10]. One key conclusion is that identification services should become a standard element of development planning, including the delivery of social services. Rather than funding one-off applications, it is better to strengthen on-going identity management systems with multiple possible uses [14]. Biometric services in the cloud provide exactly that possibility, since such system can be easily integrated into existing identity management systems [25].

There are certainly some particular social concerns related to biometrics, as there are with any particular tool or technology. From a social perspective, resistance to change to an unfamiliar technology could manifest itself in various ways. Systems of such complexity and infrastructural coherence must be deployed with a great caution. From this perspective it is vital that additional research is carried out with the aim of examining the acceptability of such technologies at respective national levels and documenting clear contextual factors that are associated with cultural and broader social aspects that might be crucial for the acceptability of such systems, a fundamental element for their success. Biometric systems in the cloud assume and require an intimate relationship between people and technologies that collect and record the biological and behavioral characteristics of their bodies. The key social challenge surrounding biometrics is the seemingly irrevocable link between biometric traits and a persistent information record about a person. Unlike most other forms of recognition, biometric techniques are firmly tied to our physical bodies. Cost of failure in such systems is very high. If you lose a credit card, you can cancel it and get a new one. If a biometric trait is stolen, you've lost it for life. Any biometric system must be built to the highest levels of data security, including transmission that prevents interception, storage that prevents theft, and system-wide architecture to prevent both intrusion and compromise by corrupt or deceitful agents within the organization. The tight link between personal records and biometrics can have both positive and negative consequences for individuals and for society at large. Convenience, improved security, and fraud reduction are some of the benefits often associated with the use of biometrics. These benefits may flow to particular individuals, corporations, and societies, but are sometimes realized only at the expense of others. Who benefits at whose expense and the relative balance between benefits and costs can influence the success of such biometric deployments [22].

Negative effects of identification using biometric methods should also be taken into account. Yet many common fears relate to identification more generally and are not specific to biometric technology. The most common fears are the risk of exclusion, threats to privacy and cost-efficiency [10]. A small percentage of the population cannot present suitable features to participate in certain biometric system. For example, when using fingerprint-based biometric system, it should be noted that some people have fingers that simply do not print well. Those who may have difficultly are infants, the elderly, and manual labourers, who are often already marginalized within society. Even if people with bad prints represent 1% of the population, this

would mean massive inconvenience and suspicion for that minority. Because of that, it should always be possible to use an alternative. Taking multiple biometrics (multi-modality) can minimize this risk and almost guarantee identity. Still, there must be an alternative, such as the use of usernames and passwords in combination with secure certificates.

Second fact is that there will also be those who decline to participate on the basis of religious values, cultural norms, or even an aversion to the process. Religious beliefs about the body and personal characteristics or interpersonal contact (for example, taking photographs, touching or exposing parts of the body) may make a biometric system an unacceptable intrusion. Mandatory or strongly encouraged use of such a system may undermine religious authority and create de facto discrimination against certain groups whose members are not allowed to travel freely, take certain jobs, or obtain certain services without those violating their religious beliefs. Another category of people who may choose not to participate is concerned about misuse or compromise of the system or its data — and its implications for privacy and personal liberty. Although a decision to participate or not may be an individual one, biometric systems can inadvertently affect groups whose shared characteristics make them less inclined to use the systems, assuming that participation is voluntary. Where use is mandatory even more consideration of these challenges may be needed [25]. By far the most significant negative aspect of biometric systems is their potential to locate and track people physically. While many surveillance systems seek to locate and track, biometric systems present the greatest danger precisely because they promise extremely high accuracy. Whether a specific biometric system actually poses a risk of such tracking depends on how it is designed.

The societal impact of biometric systems in the cloud will vary significantly depending on their type and purpose. The potential impacts on particular social groups and thus their receptions by these groups may also vary dramatically due to differences in how the group interprets the cultural beliefs, values, and specific behaviors. System performance may be degraded if social factors are not adequately taken into consideration. These factors are of two types: those that motivate and those that facilitate participant engagement with the system. As a rule, people's willingness to participate in a system and their commitment to it depends on their understanding of its benefits. For example, a biometric system that allows convenient access to a worksite might be perceived as beneficial to individuals by relieving them of the necessity to carry an identification card. On the other hand, a biometric system that tracks daytime movement of employees might be perceived as primarily beneficial to the employer and as undermining the employee's personal freedom. Participation may also be motivated by the possibility of negative consequences for nonparticipation – for instance restrictions on access to locations or services (perhaps entry to the United States), requirements to use a much more lengthy process for a routine activity (for example to open a bank account), and even the threat of legal action (for example the requirement to enroll in a biometric system in order to maintain legal alien status). Nonparticipation may also subject individuals to social pressure and/or prevent them from joining some collective activities.

At a basic level, biometrics with cloud computing can strengthen core identity systems like civil registries and national identification cards. Beyond these foundational applications, especially when combined with other advances in information and communications technology, it can also be leveraged for more functional purposes (voting, transfers or enabling financial access, health care systems, health insurance systems etc.) that facilitate access to rights and services, and strengthen public accountability. Relative to alternatives, biometric identification in the cloud can increase inclusion, privacy and efficiency, and may save greatly in the long run due to more automation and reduced fraud.

It can be concluded that the implementation of biometric solution in the cloud could improve people's quality of life in terms of more secure authentication over multiple government and non-government services and applications, but there are also multiple social concerns that needs to be considered.

6. Prediction

Many services are moving to the cloud [5] (this is also the direction of the Slovenian government) and forecasts say biometrics will not be an exception. Prediction for the future definitely shows that biometric technology will gradually replace passwords [13]. The problem with passwords is that we use too many of them, their rules are complex and they differ for different websites. Very important event confirming that was Intel Developer Forum 2012, held in San Francisco, where director of security research at Intel Labs announced that they plan to improve security and usability in authentication with the use of biometrics [15]. As he said, biometrics will be used as a cloud-based service to solve the scalability and accessibility challenges. Such an approach will also enable access from smartphones and tables, which will have scanning sensors integrated. Evidence to that is also the fact that Apple bought fingerprint-sensor maker AuthenTec for $350 million last year [20]. Apple has integrated a fingerprint reader into the new iPhone 5s, which provides additional security for the smartphone users [33].

Despite the fact that the legislation in the field of biometrics and storing data in the cloud is quite strict (see chapter 3), we predict that big players on the market, such as Intel and Apple, will change that fact in favour of more easy and convenient use of biometrics in general and its integration with cloud computing.

7. Conclusion

Cloud based biometric services have an enormous potential market value and as such attracts the interest of research and development groups from all around the world. In this article we presented how to move existing biometric technology to the cloud and examined the facts relating to the personal data protection and legislation. We also addressed economic view of the proposed solution, which was corroborated by the fact that Slovenian government wants to move its information technology to the cloud, primarily due to cost reduction and unification. By moving services to the cloud, there is no longer need to maintain a number of systems within individual or public institutions and this can save a lot of money. The social impact of such solutions will vary significantly depending on their type and purpose. Convenience, improved security, fraud reduction and reliability are some of the benefits that biometrics brings, and can certainly help in economic and social development.

There are many reasons to believe that biometrics will change the life of people in the near future, mostly because its use will be much more convenient than other techniques in use today. The potential for practical use of biometrics seems enormous. But before biometric services can be applied massively, legislation regarding storing personal data in the cloud and use of biometrics must be adjusted. We believe that big players on the market will change that fact, as discussed in chapter 6.

References

[1] Armbrust M.; Fox A.; Griffith R.; Joseph A.; Katz R., Konwinski A.; Lee G.; Patterson D.; Rabkin A.; Stoica I.; Zaharia M. A view of cloud computing, In *Communications of the ACM* , pages 50-58, 53(4), 2010.

[2] Boutaba R.; Cheng L.; Zhang Q. On Cloud computational models and the heterogeneity challenge. *Journal of Internet Services and Applications*, pages 77-86, 3(1), 2012.

[3] Biometric European Stakeholders Network, Biometrics in eID systems *(Deliverable D4.1)*, 2010.

[4] BiometricsDirect Web site. http://www.biometricsdirect.com/Biometrics/biometricslaws.htm, downloaded: February 20th 2014.

[5] Bojanova I.; Zhang J.; Voas J. Cloud Computing, *IEEE IT Professional Magazine*, pages 12-14, 2013.

[6] Bule J.; Peer P., Fingerprint Verification as a Service in KC CLASS, *Proceedings of the 1st International Conference on CLoud Assisted ServiceS,* Ljubljana: Univerza v Ljubljani, Fakulteta za gradbeništvo in geodezijo, Komisija za informatiko, knjižničarstvo in založništvo, pages 76-82, 2012.

[7] Das R., Biometrics in the cloud - What does cloud computing mean for biometric systems?, *Keesing Journal of Documents & Identity*, pages 21-25, 2013.

[8] European Parliament and Council , *EU Data Protection Directive 95/46/EC*, Luxembourg, 1995.

[9] Gantz J.; Toncheva A.; Minton S., *Cloud Computing's Role in Job Creation*, Framingham, 2012.

[10] Gelb A.; Clark J., *Identification for Development: The Biometrics Revolution (Working paper 315)*, Washington, 2013.

[11] Harms R.; Yamartino M., *The Economics of the cloud*, 2010.

[12] Höllwarth T., Ed., *Pot v oblak [Path to the cloud]*. Ljubljana: Pasadena, 2012.

[13] Honan M., Kill the Password: Why a String of Characters Can't Protect Us Anymore., *Wired Magazine*, 2012.

[14] Institute for Prospective Technological Studies, Biometrics at the Frontiers: Accessing the Impact on Society *(Technical report EUR 21585 EN)*, 2005.

[15] Iyengar S., Replace passwords with biometrics, *Intel Developer Forum*, San Francisco, 2012.

[16] Jain A.; Flynn P; Ross A., Eds., *Handbook of Biometrics*.: Springer, 2008.

[17] Jain A.; Ross A.; Prabhakar S., An introduction to biometric recognition, *IEEE Transactions on Circuits and Systems for Video Technology*, pages 4–20, 2004.

[18] Kohlwey E.; Sussman A.; Trost J.; Maurer A., Leveraging the Cloud for Big Data Biometrics: Meeting the performance requirements of the Next Generation Biometric Systems, *Proceeding of the IEEE World Congress on Services*, pages 597-601, 2011.

[19] Kshetri N, Cloud Computing in Developing Economies, *Computer*, 43(10), pages 47-55, 2010.

[20] Mawad M.; Ewing A., Apple IPhone Rumor Boosts Biometrics Companies, *Businessweek*, 2013.

[21] Mell P; Grance T., *The NIST Definition of Cloud Computing (NIST Special Publication 800-145)*, Gaithersburg, 2011.

[22] Mordini E.; Petrini C., Ethical and social implications of biometric identification technology, *Annali dell'Istituto Superiore di Sanità*, 43(1), pages 5-11, 2007.

[23] Mordini E; Tzovaras D., Eds., Biometric Recognition: An Overview, in *Second Generation Biometrics: The Ethical, Legal and Social Context*. pages 49-79, Springer, 2012.

[24] Panchumarthy R.; Subramanian R.; Sarkar S.; Biometric Evaluation on the Cloud: A Case Study with HumanID Gait Challenge, in *Utility and Cloud Computing (UCC), 2012 IEEE Fifth International Conference*, pages 219-222, 2012.

[25] Pato J.; Millett L., *Biometric Recognition: Challenges and Opportunities*. Washington: The National Academies Press, 2010.

[26] Peer P.; Bule J., Žganec-Gros J.; Štruc V., Building Cloud-based Biometric Services, *Informatica*, 37(2), pages 115-122, 2013.

[27] Slovenian Information Commisioner, *Protection of personal data & cloud computing*, Ljubljana, 2012.

[28] Slovenian Government, *Protection of Personal Data Law*, Ljubljana, 2007.

[29] Slovenian Ministry of Justice and Public Admin.. *Effective national IT strategy in Slovenia*, 2012.

[30] Štruc V.; Žganec-Gros J., Developing Face Recognition Technology for the KC Class Biometrics service, *Proceedings of the 1st International Conference on CLoud Assisted ServiceS*, pages 68-75, 2012.

[31] USA Department of Commerce. USA-EU Safe Harbor list. https://safeharbor.export.gov/list.aspx, downloaded: February 20th 2014.

[32] Vidmar T., *Računalništvo v oblaku – 1.del: Teorija distribuiranih sistemov [Cloud computing – 1.part: Theory of distributed systems]*. Ljubljana: Pasadena, 2011.

[33] Yadron D., Apple's Latest iPhone Puts Focus Back on Fingerprint Security, *The Wall Street Journal*, 2013.

[34] Zhang Q.; Cheng L.; Boutaba R., Cloud computing: state-of-the-art and research challenges, *Journal of Internet Services and Application*, 1(1), pages 7-18, 2010.