Chapter 17
Leveraging Cloud-Based Resources for Automated Biometric Identification

Wei Lu, John Hancock, Benjamin Osowiecki, Aram Taft, and Wei Li

1 Introduction to Cloud Computing

Cloud computing is one of the biggest subjects in the technology industry. In fact, it has become so widely known it has broken out of the tech world to become a household name. This should not come as much of a surprise, as cloud computing has become ubiquitous in many of our daily routines. However, if you ask someone what cloud computing actually is, there is a good chance they will not have a definitive answer. So what exactly is cloud computing?

The term cloud computing is often associated with the Internet giants of the mid-2000s, around the debut of Amazon's Elastic Compute Cloud, yet the term had come to be about 10 years earlier. The origin of the term, in the modern sense, has been traced back to a Compaq business plan dated 1996. Within is a prediction for the future, where "application software is no longer a feature of the hardware – but of the Internet" and would be known as "the cloud" [1]. Unfortunately, this still paints as very broad picture of what cloud computing actually is, simply defining it as software that runs remotely over the Internet, instead of on a local machine. Since this time the industry has exploded, but up until recently, there has been little guidance on what actually fits the definition of cloud computing. In the past few years, the industry has determined concrete guidelines as to what cloud computing is, going so far as to break it up into three distinct categories. Formally, cloud

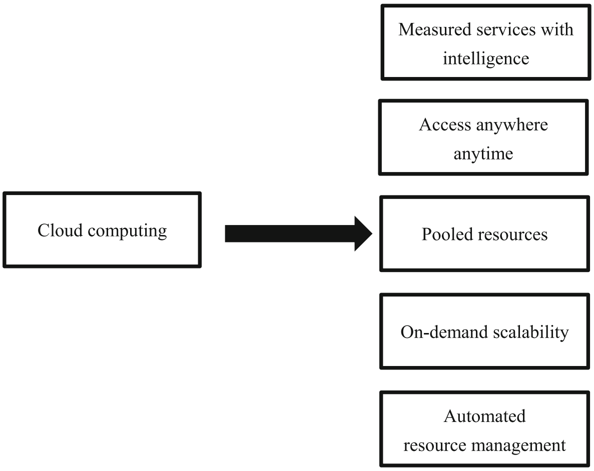
W. Lu (✉) · B. Osowiecki · A. Taft
Department of Computer Science, Keene State College, USNH, Keene, NH, USA
e-mail: wlu@keene.edu

J. Hancock
Fidelity, Durham, NC, USA

W. Li
New York Institute of Technology, Vancouver, BC, Canada
e-mail: wlu@keene.edu

M. S. Obaidat et al. (eds.), *Biometric-Based Physical and Cybersecurity Systems*,
https://doi.org/10.1007/978-3-319-98734-7_17

Fig. 17.1 Five characteristics of cloud computing



computing is defined as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or to service provider interaction" [2]. This is to say that a cloud computing service is one where a user can log in from almost anywhere and be given the service offered, requiring the backend components to be allocated and de-allocated as needed.

As illustrated in Fig. 17.1, there are also five characteristics that all cloud computing services have in common. The first is that they allow users to use their services and access required resources (such as server time or network storage) without having to interact with a human. Secondly, cloud computing services should be designed to allow devices of all different form factors to connect and utilize the service, whether it is a mobile phone, laptop, or desktop workstation. Third, resources should be pooled in such a manner that multiple users can be served simultaneously and do so in a way which is transparent to the user. The fourth characteristic builds off the third; a cloud computing system should have the ability to scale as demand increases and decreases. Lastly, the system should have the ability to automatically track, control, and optimize resource use.

Despite these rather detailed guidelines, the world of cloud computing is still extremely diverse. This is where the three categories of Software as a Service come into play. The models illustrated in Fig. 17.2 describe three distinct forms of cloud computing service, with each consecutive tier building on the one prior. At the lowest level is Infrastructure as a Service (IaaS) [18], a step up is Platform as a Service (PaaS) [19], and then at the highest level is Software as a Service (SaaS) [12].

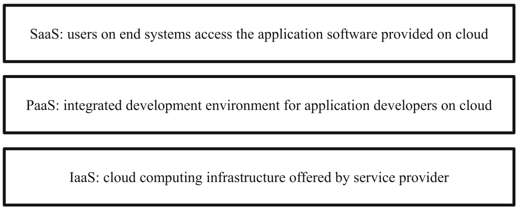

SaaS: users on end systems access the application software provided on cloud
PaaS: integrated development environment for application developers on cloud
IaaS: cloud computing infrastructure offered by service provider

Fig. 17.2 Three typical cloud computing models

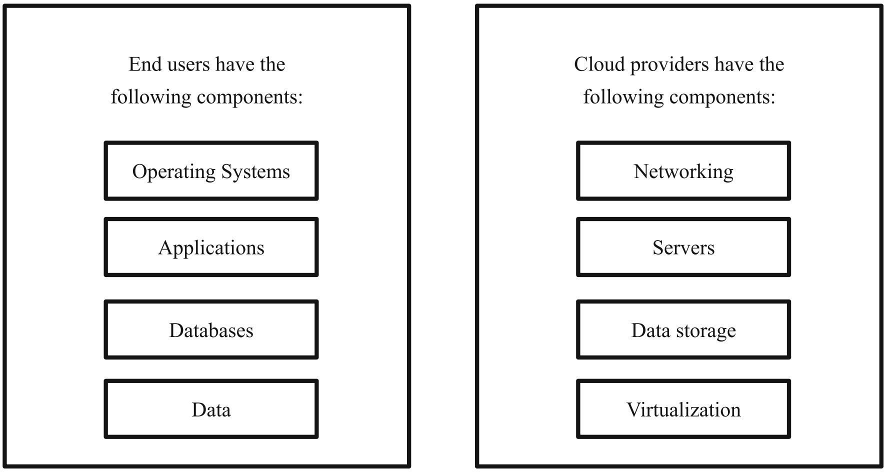

End users have the following components:
Operating Systems
Applications
Databases
Data
Cloud providers have the following components:
Networking
Servers
Data storage
Virtualization

Fig. 17.3 Infrastructure as a Service

1.1 Infrastructure as a Service

As illustrated in Fig. 17.3, IaaS is the most "bare bones" of the three cloud computing models. In this model, the service provider provides only the computing infrastructure, including virtualization, servers, storage hardware, and networking capabilities. Often IaaS providers use this virtualization to hide the hardware from the customer, as it is irrelevant to them. The virtualization is accomplished through the use of a hypervisor, otherwise known as a virtual machine monitor. These systems allow for vast numbers of virtual machines, known as guest machines, to be hosted. These virtual machines are then provided to the customer for use with their software of choice. As such it is up to the user to supply the data, applications, databases, and operating system. Examples of such systems include Google Compute Engine [3] and Amazon EC2 [4]. IaaS systems are designed for those who have built (or are building) their application for either a specific or a custom platform and need complete control of what can be run, but do not want to have to acquire and maintain computing hardware.

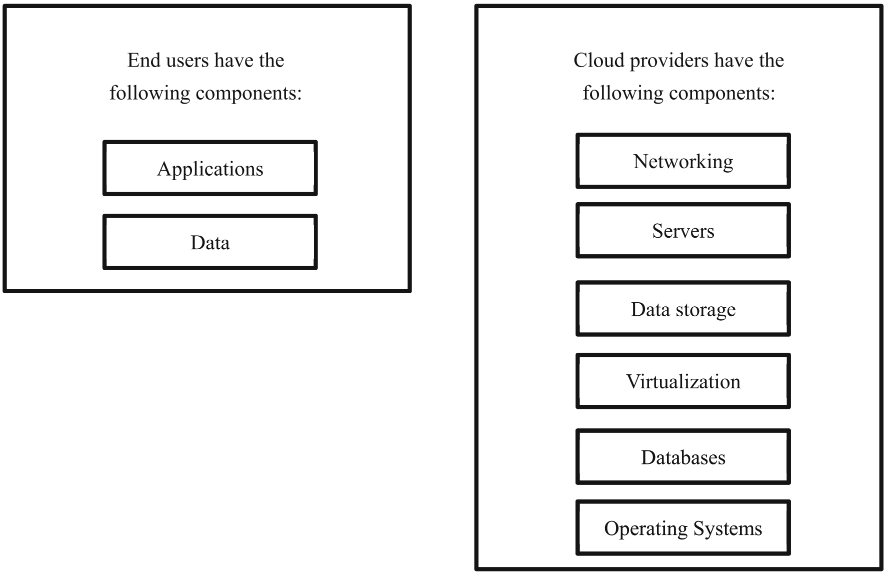

End users have the following components:
Applications
Data
Cloud providers have the following components:
Networking
Servers
Data storage
Virtualization
Databases
Operating Systems

Fig. 17.4 Platform as a Service

1.2 Platform as a Service

PaaS is the second model that is illustrated in Fig. 17.4. In this model the service provider is responsible for everything related to hardware and for systems which will be required by a customer's applications (such as databases and the operating system). In other terms, Platform as a Service providers supply application developers with development environments on which they can develop and host their applications. Often times the service provider will create APIs, toolkits, and distribution systems for their respective platforms. Together, these allow application developers to develop apps without having to acquire, manage, and maintain the hardware, operating system, databases, or web server. Examples of PaaS services include Microsoft Azure [5] and Google App Engine [6].

1.3 Software as a Service

SaaS is the cloud computing model most consumers consider "the cloud." It is at this level that services such as Google Drive, Facebook, or Amazon Marketplace exist. As illustrated in Fig. 17.5 in this model, the users are often nontechnical people, as they are using already built application software. They do not have to deal with any hardware and OS or have to program the applications; they simply provide their data into the application. These platforms are otherwise referred to as "on-demand

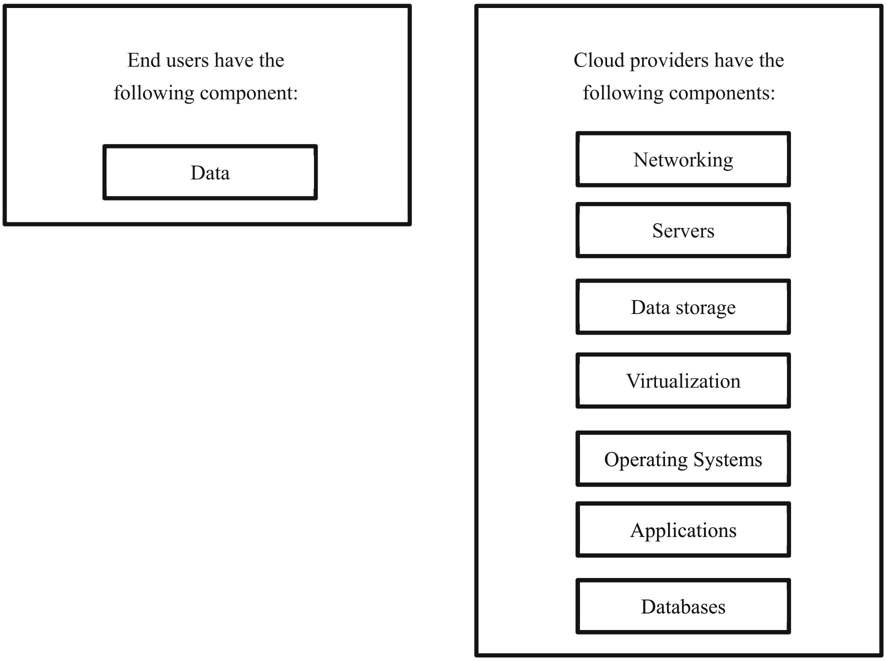

End users have the following component:
Data
Cloud providers have the following components:
Networking
Servers
Data storage
Virtualization
Operating Systems
Applications
Databases

Fig. 17.5 Software as a Service

software" as they can be accessed on an as needed basis, from almost any device. This also alleviates the need for the user to install application software locally, as it is hosted on the provider's servers. To keep up with large demand this can cause, these services use load balancers to distribute work over sets of virtual machines; however, this process is invisible to the user. Often times these systems are priced on either a reoccurring subscription plan or on a pay as needed (often seen on cloud storage services).

2 Introduction to Biometrics for Authentication

Biometrics is defined as the "automated recognition of individuals based on their biological and behavioral characteristics" by the International Standardization Organization [7]. Biometrics is made to have an authentication which is not so easily spoofed by social engineering or hacking into a terminal. The complexity of the human body makes it rare for people to have the exact same fingerprint or vein pattern when trying to gain access to something with such biometric security protocols. Scanning these characteristics makes it available as a service to prove one's identity and gain access to things such as bank account, credit cards, and online profiles, to name a few. When you scan your fingerprint, iris, or palm, the reading from the scanner will be compared to what was originally stored when the account was set up, similar to passwords systems. Once checked it will get a result from the checking algorithm and either allow or deny access to what is trying to be accessed. The improved security comes with the human body characteristics that are similar in structure but unique to a majority of the population on earth as well as how many points of scanning the system does for authentication. Having multiple points will help with authentication given you have not a single point of failure where that one trait being scanned was altered or removed from you. An example can be if you were to cut your finger on the bottom and if the system scans one specific ridge in your print, that would be the point of failure. If the system was grabbing multiple points on your fingerprint, it could get a close enough match to still uniquely identify you and not someone else. In the following we will discuss some of the more popular options for biometrics including such as facial scanning, iris scanning, vein recognition, and fingerprint scanning.

2.1 Fingerprint Scanning

Fingerprint is a popular form of biometrics and is widely implementable in many security systems. There is a one in 64 billion chance that your fingerprint will match up exactly with someone else [8]. One of the problems of times now is coming up with ways to have a unique hash or password encryption. MD5 hashing algorithm is a great example and has been having hash collision for a while now, and you can even type it into google, and it will give you what was hashed back out. With so many possibilities in a fingerprint, it serves as a great authentication for a system or application.

Fingerprints have an assortment of friction ridges that form in the development process of human beings. As illustrated in Fig. 17.6, there are some of the various fingerprint styles, including such as arch, whorl, double loops, and simple loop. There are glands underneath the skin of your fingers are what make the distinct ridges visible on surfaces you touch such as glass or the fingerprint readers. By looking at the amount of ridges, direction, and pattern of the fingerprint, people were able to be identified uniquely from one another. This was used as early means of crime investigating where matching a set of print to an ink card someone had made

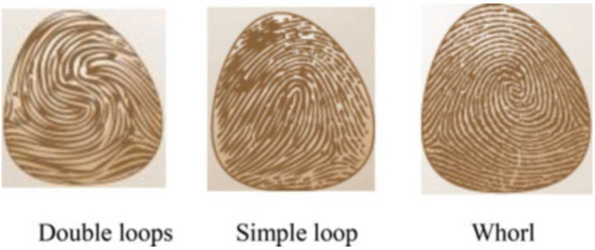


Fig. 17.6 Typical fingerprint styles

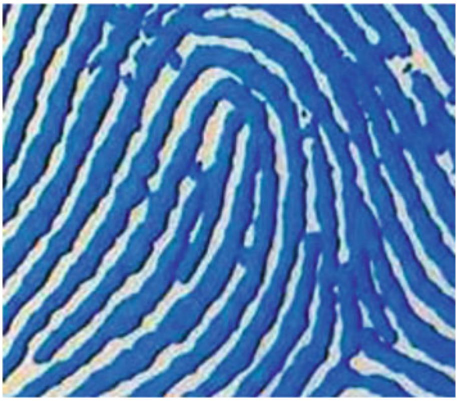


Fig. 17.7 An example of a scanned fingerprint

could tell if someone had left their fingerprints at a location. Now in the digital age, we have evolved to have algorithms to analyze the pattern and characteristics of the fingerprint and come up with a result of it is a match to the record they have on file.

Scanning a fingerprint can be done by using an optical scanner which involves a charged coupled device which is in term a light sensor, the same as found in digital cameras. The array of diodes underneath make up the many sensors for reporting how much light is hitting that sensor in the array. The device will emit its own light source when you start the scanning process and place your finger on the designated area, it will start recording the light that is be reflected back by the ridges of your fingerprint and then the software will invert the image to have the ridges of your finger as the darker portions instead of the areas between ridges; Fig. 17.7 shows what the inverted image looks like for the software to scan and compare to a stored set of data.

Lastly the software will check to see if there are sufficient characteristics between the print on record and the print you just scanned in. That way when you scan your print if the scanner does not pick up on every ridge or pattern, it will still grant you access because it still is proving to be a match to your print that it has stored. Another device to pick up fingerprint imaging is the capacitance scanner which uses electrical currents to have your salty skin complete the circuit and generate a map of the fingerprint. This device is made up of an array of cells; each cell is made up of two conductor plates for the positive and negatives within a capacitor circuit. These capacitors are very tiny so that they can be in between ridges of the fingerprint and get an accurate representation of the layout of the fingerprint. To get the signal out to the computing unit, the signal from the capacitors is so small that integrated into the device is an amplifier to step up the voltage and have the computing device an easily distinguishable reading, and signal is needed to travel the distance of the wiring connecting the sensor to the computing device, and we do not want the signal to degrade between the capacitor and the computing device. Before scanning begins all the capacitors need to be reset and drop any charge they may have then, when the fingerprint is applied that will start the charging of the capacitors again for imaging. Advantages of the capacitor scanning include having to use a real-time fingerprint

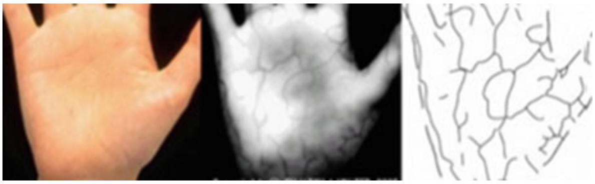


Fig. 17.8 An example of a scanned vein

reading which means without an actual finger you cannot so easily fool the scanner into thinking it is the right fingerprint on the sensor. An optical sensor takes an image, so having a very detailed fingerprint can trick the sensor into thinking you are someone else because it has no idea on the difference between image and a real finger.

2.2 Vein Recognition

Vein recognition is similar to fingerprint scanning, but instead of ridges formed in development, it is scanning the veins within your palm for distinct patterns. Veins offer another form of security with the matter of it is located beneath the skin where without surgery it is not an easy task to alter for the scanning device. Veins can be seen near the surface, but there are many veins underneath that you cannot see which also helps for creating the secure authentication and makes it harder for people to counterfeit a vein pattern. Veins also act as a viable use for authentication because they change shape and geometry very little as a person ages. The vein scanners work by using near-infrared light waves and projecting them onto your palm. Your red blood cells naturally absorb the light waves and appear darker because of the light being absorbed instead of reflected back; Fig. 17.8 gives an image of what the scanner is seeing when sending and receiving the wave lengths back. The scanner will then start mapping the darker lines to create a map of where the veins in your hand are located. After the geometry of your veins are scanned, they can be compared to the record stored and start checking points to which match and create an outcome within certainty that you are the person trying to authenticate with a specific user level of permission and access.

2.3 Iris Scanning

Iris scanning is another form of biometrics with complexity within its generation creating personal and unique characteristics for authentication making it another great resource of the biometrics industry. The iris can be seen in Fig. 17.9 for clarification on where the iris portion of the eye is located [9]. The iris is comprised of melanin pigments that form during development of the body and is still today not

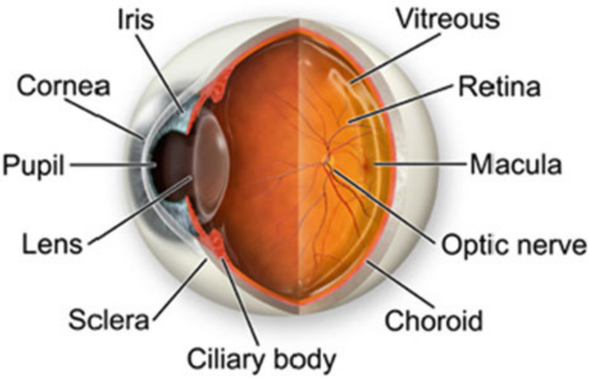


Fig. 17.9 Iris location in a normal eye anatomy

an exact science of how a specific color is produced, but we do understand how the colors come to be. Within the iris, eumelanin (appears as a brown/black pigments) and pheomelanin (appears as red or yellow pigments) combine in different strengths to create everyone's eye color. Other factors that play into the complexity of the iris are the fibers and blood vessels within the iris stroma. These randomly generated formations during the development process of the aforementioned factors make interesting geometric patterns within the iris and then through software and mathematics algorithms are created to scan your iris and create a data set for comparison.

Iris scanning makes for a more secure system because the iris can be scanned for 200 or more points for identification of an iris data set, whereas a fingerprint scan is normally 60–70 points for authenticating. The software for iris scanning is more complex in where the different regions of the eye as depicted in Fig. 17.9 shows that algorithms have to identify and map edges of the pupils, iris, sclera, and the eyelid itself. These regions are to focus in on the iris and see the patterns for authentication and ignore the regions you scanned but do not want to use for data analyzing. The iris also makes for a more reliable tool in biometrics as it is more of an internal organ with protection from the elements by the transparent but sensitive layer called the cornea. The protection of the iris means it is not going to break down or be worn down like fingerprints can be with manual labor and extensive use of the fingertips or hands.

Currently hardware for scanning iris are not as prevalent as fingerprint scanners but require a bit more specific hardware even though they contain the same sensor for collecting data on your iris. The scanners have been coming to market for a while now, but with more options becoming available and the pricing going down, there are more affordable options coming to market. Iris scanners can use the same technology as optical fingerprint scanners with the CCD sending out and scanning near-infrared light waves as well as visible light waves to produce a high-contrast image of your eye. The NIR (near-infrared) waves are good at getting the structure of the eye for comparison and make a more accurate picture because of the light wave being recorded. The ambient light is not affecting the imaging software and/or hardware.

2.4 Facial Scanning

Facial scanning is similar in number of points to fingerprint scanning with a bit higher 80 points of recognition to check between stored records and a current image scan. Facial scans can be done in either 2D or 3D depending on the machine and software suite running. 2D images are checked between images for similar patterns and geometrics with the image stored in the database. Facial images can be scanned for landmarks that make faces distinguishable from one another. Some of the notable landmarks that are scanned included distances between eyes, width of the nose, the shape of the jaw line, depth of the eye sockets, and shape of the cheekbones. The main drawback of 2D images is that the face needs to be 35 degrees toward the camera for calculating the similarities and differences between them. 3D imaging of facial features proves to be more accurate with more freedom of images whether its graphing is from a 2D image or from video to get a true 3D image. 3D imaging also allows for up to 90 degrees of rotation from the camera to be able to calculate facial features. The 3D imaging targets areas of the face including the chin, nose, rigid bone, and tissue areas as well as the curvature of the eye sockets. The 3D software allows for taking a 3D capture and calculates the distances on the face to create an accurate 2D image that can be turned to face the camera directly. Once generated, it can be compared with an older 2D image within an older database of facial scans.

Figure 17.10 shows the steps how a video feed can be converted from an image to a comparable image to search a database of faces. Another resource being developed for better recognition was to zoom in on the skin of the facial scan and verify the texture of the skin. The process named Surface Texture Analysis is breaking the skin into patches for scanning the texture, lines, and pores to even distinguish twins. It has been mentioned that combining the facial scanning with the texture analysis increases the match accuracy by 20% to 25%.

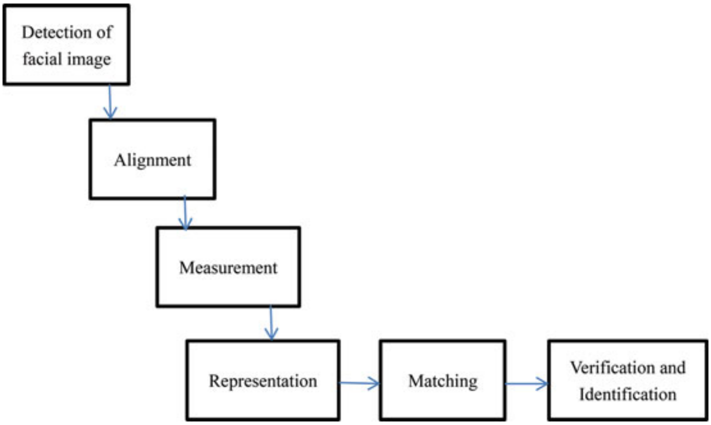


Fig. 17.10 Typical steps for facial recognition

3 Biometrics as a Service

Breaking down the term “Biometrics as a Service,” biometrics – as defined by the International Standardization Organization – is the “automated recognition of individuals based on their biological and behavioral characteristics” [7]. Service is defined as “a facility supplying maintenance, repair and demand to the consumer” [10]. BaaS is a means of secure authentication using biometrics as layer of security. Biometrics since the 1990s has been slowly coming into the forefront as the leading method of securing data. In [11], Risch and Devlin stated that “individual DNA profiles are extremely uncommon, if not unique.” It is much better in many ways regarding the fact that each human has unique biometric makeup. Also, forgetting your “password” is now a lot more difficult since people cannot forget to bring their hands, fingers, or eyes with them since they are attached to your person.

BaaS is considered a variant of Software as a Service. SaaS is defined as a software distribution model in which a third-party provider hosts applications and makes them available to customers over the Internet. All SaaS variants have these three things in common: they are licensed on a subscription basis, they are hosted by the service provider, and they are inseparable from cloud computing. Biometric authentication has been widely adopted by financial service industries, medical centers, law enforcement, and governments across the world.

As stated above, biometric services are inseparable from cloud computing technology. Typically, capabilities of cloud computing include (1) elasticity and agility, i.e., the ability to shift and deploy resources across disparate infrastructures; (2) network-centricity, i.e., the availability on any network and device; (3) on-demand domain, i.e., being able to be accessed anytime, anywhere in the world; and (4) data supremacy, i.e., data over the cloud ensures data supremacy [13]. Mobile strategies are being adopted by businesses, enterprises, and service providers around the world. Most companies today have a policy regarding the term bring your own device (BYOD). By incorporating mobile devices in everyday business affairs, it tremendously facilitates smooth cooperation with all parties involved. BYOD brings numerous benefits to businesses including job efficiency and flexibility, accelerated chain and business operations, and cost-saving regarding IT departments. Employees and employers are constantly using software to access sensitive personal information along with transactions related to payments. The cost that comes with efficiency from mobile devices is security.

There are two categories of biometric identifiers: behavioral and physiological attributes. Behavioral biometrics assess unique and measureable human traits, including patterns in attributes including voice, a person’s gait (manner of walking), and typing rhythms. Physiological biometrics identifies a person’s identity by using their fingerprints, facial recognition, palm veins, and retina and iris recognition. Biometric scanners use algorithms to take the data and inputs from the user to match said data points, which give authentication access for users.

This is where software and hardware from companies like ImageWare Systems and IriTech come into play. Solutions to cloud-based biometric authentication include topics ranging anywhere from mobile security and credentialing to healthcare and government that are being tackled by many different companies at many different angles. Leaders in the industry of BaaS currently are ImageWare Systems, Inc. who recently partnered with Fujitsu, BioID, IriTech, FingerCheck, and MorphoTrust. The topics covered in the portion will be directly referencing these five companies and their technologies.

3.1 ImageWare Systems, Inc.

ImageWare Systems has their hands in a variety of different markets. They offer an abundance of services regarding topics of access control to healthcare. On November 15, 2016 ImageWare Systems announced their Enterprise Suite for GoVerifyID. The product was created to provide full support for a Microsoft Ecosystem using end-to-end biometric authentication. GoVerifyID is a secure, flexible, and scalable biometric user authentication service. The way this software works is by having the servers pinging ImageWare Systems servers when an event – like a retail transaction – occurs. The user is asked for biometric verification which is then verified with anonymous templates on the server which will approve or deny the access or transaction.

GoVerifyID offers a demo of their product upon request via email. You are given a temporary account to test the product out. The way the software works is when you attempt to log in to a site that uses GoVerifyID, their server will push a request to your mobile device. This request opens the GoVerifyID application which then prompts you for a combination of your fingerprint, a voice passphrase, and facial recognition. Once you have successfully passed all the verification steps, the application sends a confirmation back to the website that enables you to log in.

3.2 BioID

BioID specializes in facial and voice recognition. BioID is designed to protect user information. Just like the other software services covered in this chapter, anonymity is a prevalent feature when verifying face and voices. The software uses a template that has no information about the user that is not necessary. Some biometric services usually do storage on a local, so nothing leaves the user’s device. BioID – just like ImageWare Systems – uses secure data centers they are in control of due to the vulnerability of keeping data on a client’s device.

BioID offers a trial version of their product which offers two ways to demonstrate their algorithms. The google play store has an application which offers a limited demo which features their facial recognition technology, which is displayed in Fig. 17.11. Their website does too but also offers voice recognition. You will have to sign up for an account as illustrated in Fig. 17.12. Then you must enroll your face so they can then recognize you for future authorization attempts.

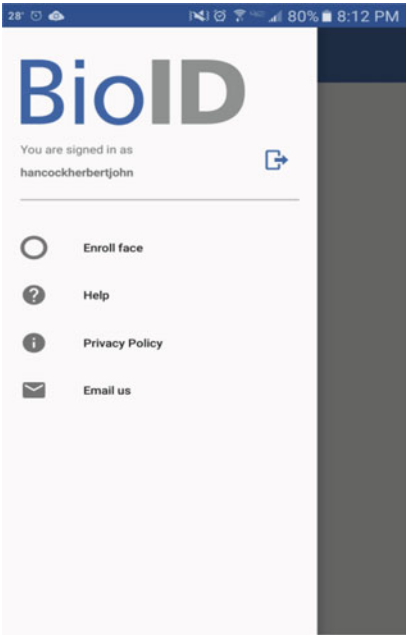
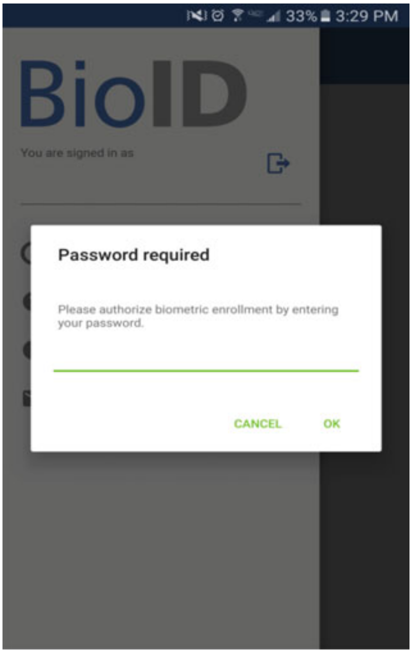


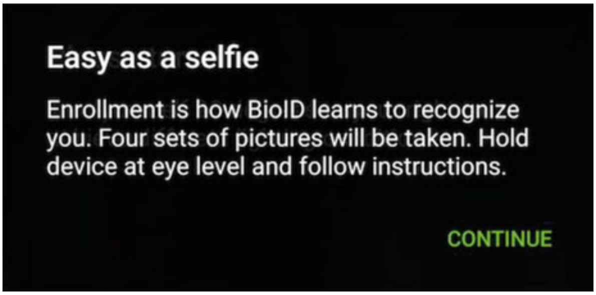
Fig. 17.11 Sign in GUI of BioID application



Password required

Please authorize biometric enrollment by entering your password.

Fig. 17.12 User verification of BioID application



Easy as a selfie

Enrollment is how BioID learns to recognize you. Four sets of pictures will be taken. Hold device at eye level and follow instructions.

Fig. 17.13 Pictures taken in BioID application

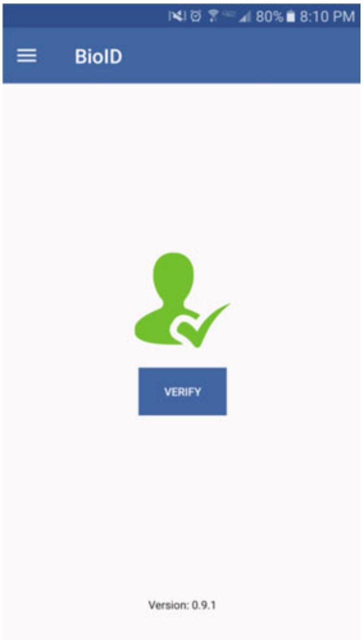


Fig. 17.14 Verify prompt in BioID application

After submitting your password, you are then asked to position your face in the center at a reasonable distance away from the camera. It will ask you to then position yourself 90 degrees to get better lighting as illustrated in Fig. 17.13.

Once you have successfully enrolled your face, you can then start the trial verification by selecting verify prompt depicted below in Fig. 17.14.

This is the same procedure you will go through if you wanted to do this trial on a web browser via your computer or laptop. Once BioID has fully captured your bio template, you can then test out the accuracy by having a friend or colleague try to get their face to substitute for yours. You will most likely find that even if someone gets your password to initiate the bio-authorization, they will fail the facial recognition portion. Figure 17.15 shows the interface after completing the setup of BioID.

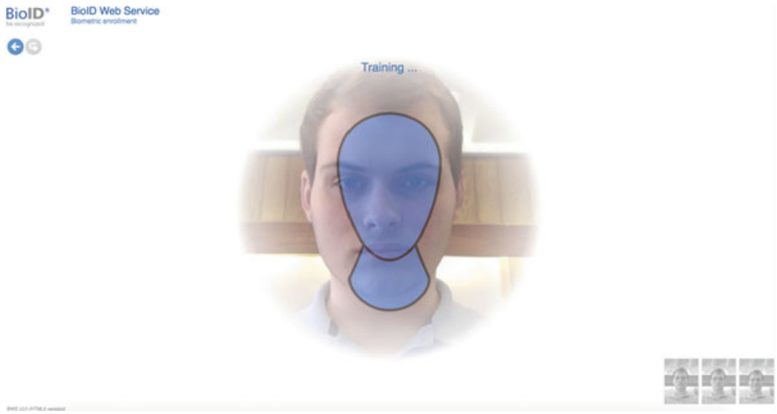


Fig. 17.15 Interface after completing the setup of BioID

3.3 IriTech

As you may perceive from IriTech's name, they specialize in iris scanning. The thing about IriTech is that their initial products were not only software but hardware. Obviously with scanning anything, you need a device to capture the data. Before smartphones were up-and-coming, there was not a mobile friendly way of securing your data via iris scanning. IriTech sells hardware and software as a package for a unique all-in-one solution to your biometric iris scanning needs. Now, they offer a cloud bases solution which can be used by just downloading an app on your smartphone. This software coupled with cloud-based servers is very secure and easily integrated into existing applications and services that support standard web service architecture.

Iritech's Iritracker was created as a time and attendance system which can help employers eliminate manual input, time theft, and identity card theft/exchanging. Their key features can be summarized as followed: The user interface is easy-to-use. Attendance data is generated from different locations. It has flexibility and manageability that offers administration create, replace, update, and delete functionality. The system's time reports are highly accurate and reliable. It supports multiple languages, capable of working in biometrically intolerable workplaces, and has automated message delivery with a bulletin board function.

Iritech – as discussed above – also offers a mobile option. The mobile application offers no option to test the functionality due to needing specific hardware from Iritech or having a mobile device that is supported by the application. The mobile application works by making a template of your iris using their underlying algorithm to use as a reference for authentication. More details on Iritech and its mobile application can see [14, 15].

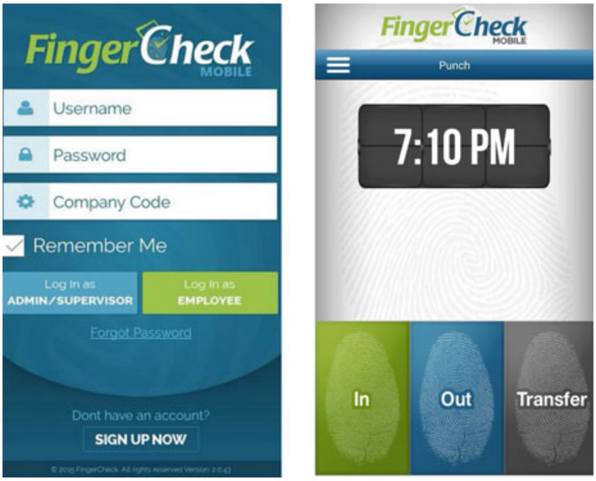


Fig. 17.16 An example of FingerCheck application

3.4 FingerCheck

FingerCheck has dedicated its software to combine time tracking and payroll into one solution. FingerCheck's software is reliable that uses fingerprint scanning via your phones scanner to keep track of worker's hours on the clock. They offer two ways to utilize their service. Download an application on a smartphone or tablet with fingerprint scanning capabilities coupled with a monthly paid service or hardware you can purchase that comes with the software and a fingerprint scanner. This software also uses cloud-based servers – specifically Amazon's redundant servers – to keep your data safe and secure. FingerCheck offers hardware and software solutions involving an all-in-one system and a mobile application. Covering the application, a login screen is the first thing you see as illustrated in Fig. 17.16 [16]. There are two options: one is for administrators and the other for employees. You will then be greeted by a selection to punch in and out or a transfer.

3.5 MorphoTrust

MorphoTrust specializes in identity protection and storage. Having physical identification can become cumbersome, so MorphoTrust has created a service that uses biometrics to safely store and authenticate identification cards like licenses for vehicles and aircraft, badges and IDs for law enforcement to hospital staff, and insurance cards. The main theme from these five companies is that they all use cloud services, license on a subscription basis, and are hosted by the provider and not the client. There are 42 states in the USA that use MorphoTrust's service. As illustrated in Fig. 17.17, MorphoTrust's way of processing identity includes three steps, i.e., enroll, verify, and issue [17].

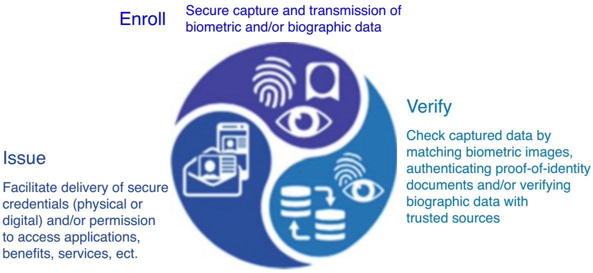

Enroll
Secure capture and transmission of biometric and/or biographic data
Verify
Check captured data by matching biometric images, authenticating proof-of-identity documents and/or verifying biographic data with trusted sources
Issue
Facilitate delivery of secure credentials (physical or digital) and/or permission to access applications, benefits, services, ect.

Fig. 17.17 The MorphoTrust identity lifecycle

4 Conclusions

Biometrics technologies have already been widely adopted by government sectors such as law enforcement and border control. With growth of mobile computing everywhere, we can expect to see the growing demand for applying BaaS for identity authentication and online transactions in the field of high-risk industries such as health insurances, banks, and financial institutions because of the highly secure capability provided by the biometric identification and verification in managing risk and recruiting and retaining customers. It is our belief that leveraging cloud-based resources for automated biometric identification will be expanded across markets led by convergence trends, thus affecting biometrics technology providers, networking infrastructures, security and cloud storage industries, banking, healthcare, and retail as well as device manufacturers including smartphone makers, to name a few.

References

1. A. Regalado, Who coined ‘cloud computing’? MIT Technology Review 1–10 (2011)
2. P. Mell, T. France, The NIST definition of cloud computing. In *NIST Special Publication* 800-145, Sept. 2011
3. D. Harris, What google compute engine means for cloud computing. GigaOM-Tech News, Analysis and Trends (2012)
4. E. Walker, Benchmarking Amazon EC2 for high-performance scientific computing. The Magazine of USENIX and SAGE **33**(5), 18–23 (2008)
5. D. Agarwal, S. Prasad, AzureBench: benchmarking the storage services of the azure cloud platform. In *Proceedings of the* 2012 *IEEE 26th International Parallel and Distributed Processing Symposium Workshops and PhD Forum* (IPDPSW ‘12). IEEE Computer Society, Washington, DC, pp. 1048–1057
6. R. Prodan, M. Sperk, S. Ostermann, Evaluating high-performance computing on Google app engine. Software, IEEE **29**(2), 52–58 (2012)
7. ISO/IEC 17788:2014 1st Information technology – Cloud computing – Overview and vocabulary JTC1/SC38
8. P. Pakutharivu, M.V. Srinath. A comprehensive survey on fingerprint recognition systems. Indian J. Sci. Technol. **8**(35) 1–7 (2015)

9. Z. Zhu, Q. Ji, Novel eye gaze tracking techniques under natural head movement. IEEE Trans. Biomed. Eng. **54**(12), 2246–2260 (2007)
10. Service https://www.merriam-webster.com/dictionary/service. Retrieved in Mar. 7 2017
11. N. Risch, B. Devlin, On the probability of matching DNA fingerprints. Science (New Series) **255**(5045), 717–720 (1992)
12. F. Liu, W.P. Guo, Z.Q. Zhao, W. Chou. SaaS integration for software cloud. In *Proceedings of 2010 I.E. 3rd International Conference on Cloud Computing*, 2010, pp. 402–409
13. Frost and Sullivan. Cloud-based Identity and Authentication: Biometrics-as-a-Service. Fujitsu. http://www.fujitsu.com/us/Images/Fujitsu-FrostSullivan_Cloud_WP_Biometrics-as-a-Service.pdf. Retrieved in Mar. 1 2017
14. Cloud-Based Iris Recognition Solution, http://www.iritech.com/products/solutions/cloud-based-iris-recognition-solution-0. Retrieved in Mar. 23 2017
15. IriShield Demo, https://play.google.com/store/apps/details?id=com.iritech.iddk.demo. Retrieved in Mar. 23 2017
16. FingerCheck, https://fingercheck.com/latest-updates-to-the-fingercheck-mobile-app/. Retrieved in Mar. 23 2017
17. MorphoTrust, http://www.morphotrust.com/Portals/0/MorphoTrust_Intro_Brief.pdf. Retrieved in Mar. 23 2017
18. A. Iosup, R. Prodan, D. Epema, Iaas cloud benchmarking: approaches, challenges, and experience, in *Cloud Computing for Data-Intensive Applications*, (Springer, New York, 2014), pp. 83–104
19. B. Butler, PaaS primer: what is platform as a service and why does it matter?. Network World, February 11, 1–5 2013