Biometrics in the cloud

What does cloud computing mean for biometric systems?

by Ravi Das

Until recently, businesses had to acquire their own information technology infrastructure, and house it within their own facilities. Although this set-up does have some advantages, it certainly has its disadvantages, the biggest being the cost of such an infrastructure. With the advent of cloud computing, however, all IT resources can now be housed with one hosting provider. Nowadays, even an organisation's security infrastructure including its biometric systems can be outsourced to a hosting provider, as Ravi Das explains.

Ravi Das *is a technical writer for BiometricNews.net, an independent publisher and leading source of news and information about the Biometrics Industry. Ravi holds a Master of Science Degree in Agribusiness Economics from Southern Illinois University and a Master of Business Administration (specialising in Management Information Systems) from Bowling Green State University.*

Not long ago, all types of businesses, no matter how small or how large, had to acquire their own information technology infrastructure, and house it within their own facilities. Not only is it costly to acquire the necessary hardware and software, but there are also costs involved with the required upgrades and the employment of staff necessary to monitor the IT infrastructure 24/7. With the advent of cloud computing, however, the need to purchase and house an entire IT infrastructure has diminished, and all IT resources can be housed with a hosting provider. The primary advantage of cloud computing is that the costs of having an IT infrastructure in the cloud are fixed and predictable. Nowadays, even an organisation's security infrastructure, including its biometric system(s), can be outsourced to a hosting provider.

Cloud computing and its characteristics

The term 'cloud computing' is defined by the National Institute of Standards and Technology as '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.'[1]

The most important characteristics of cloud computing are:

- On demand self-service: cloud services can be accessed automatically, anytime and anywhere in the world.
- Broad-based network access: all cloud-based services are available via any type of network connection, and can be accessed by any kind of device.
- Resource pooling: at the hosting provider, all IT and network resources are pooled together, which is what gives the cloud its economies of scale, resulting in fixed and predicable costs for a business.
- Rapid elasticity: the cloud resources can be released to the business within seconds, in proportion with the particular level of demand.

Cloud computing service models

There are three different types of cloud computing service models, which together are known as the SPI model[2]:

- Software as a Service (Saas)
  SaaS is a software distribution model in which software services and applications are hosted and run by a vendor or service provider and made available to customers over a network, typically the internet and graphical user interface.
- Platform as a Service (PaaS)
  PaaS is a paradigm for delivering operating systems and associated services over the internet without downloads or installation. This includes the programming languages, and other development tools.
- Infrastructure as a Service (IaaS)
  IaaS involves outsourcing the equipment used to support operations, including servers, storage, hardware and networking components to the hosting provider's cloud infrastructure (the 'virtual server').

Biometric infrastructure in the cloud

Biometrics in the Cloud means that the entire biometrics infrastructure of a business is placed in the hands of the hosting provider, and is available on demand, much like the IT infrastructure described above. This includes the servers which contain the biometric template database, the network connectivity to the business, and all of the processing which occurs in order to conduct the necessary verification and identification transactions. The necessary software applications will be housed here as well. The only thing

a business would have to do is to purchase the required biometrics hardware (such as a vein pattern recognition device), install it, and with a simple mouse click set up an account with the hosting provider to select the services they need.

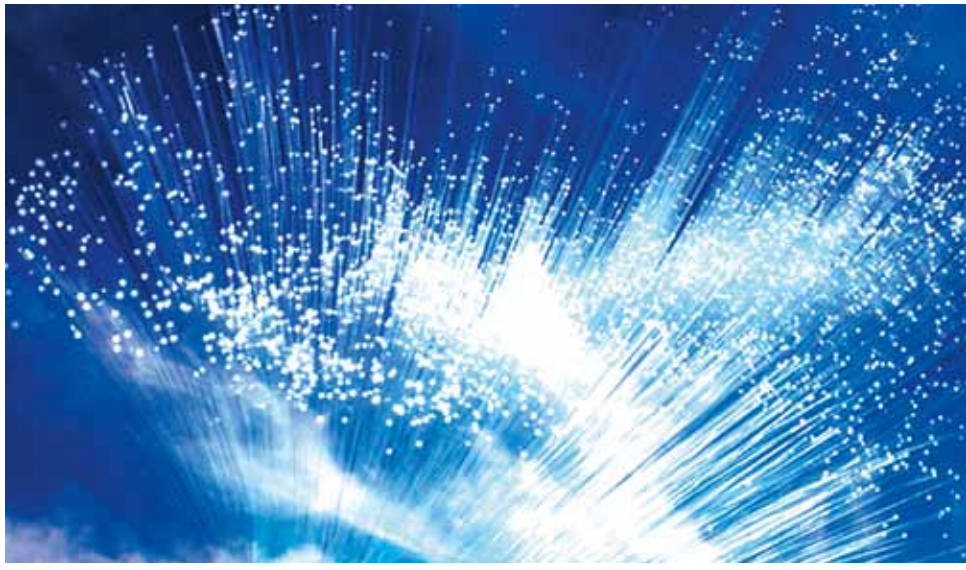
The types and kinds of applications are unlimited in scope. This hosted biometrics infrastructure will be designed to fit the wide gamut of large scale identification applications and biometric applications which exist today, such as Physical Access Entry, Time and Attendance and Single Sign On, but will also support any type or kind of biometric technology which is available today, including physical biometrics and behavioural biometrics.

Let us take a closer look at what the SPI model would mean for biometrics and cloud computing.

The IaaS component
As mentioned above, IaaS involves outsourcing for example servers, storage and networks.

Virtual servers
The virtual servers are the main point of contact for a business. It will have total control over its Biometrics in the Cloud infrastructure. At this level, the business will have a control panel from which it will be able to provide services and have total administrative control over its cloud-based biometrics application. The underlying premise here is that the business can essentially do whatever it needs or wants without further intervention. The key component of the virtual server is the Biometrics Operating System, which will support both open source and closed source platforms, such as Linux and Windows, respectively.

Storage
All biometric templates will be stored at this level, as well as the associated databases which will process the various transactions of these templates, such as verification and identification. The hosting provider will supply full developmental freedom in the way and manner in which the databases will be designed. This means that a business will have a choice as to which technology platform its databases will be built upon. In these databases, the biometric templates to be stored will include every employee's enrolment template and the verification templates.



Networks
A Biometrics in the Cloud infrastructure will have network connectivity to the biometric devices at the physical location of the business, and vice versa. In order for the hosting provider and the biometric devices to recognise each other, however, each cloud-based biometrics application will have its own unique Internet Protocol (IP) address so that the business and its cloud-based infrastructure can be uniquely identified in the vast expanse of the internet.

The SaaS component
The second major component of the Biometrics in the Cloud infrastructure, the SaaS component, will have two different options:

1. Software which is already created and can be purchased on demand by the business.
2. A software platform in which customised development will take place.

With respect to the first option, it is envisioned that the biometrics vendors will create and develop software applications for all biometric technologies available today (which will then be deployed to the hosting provider), both in terms of physical biometrics and behavioural biometrics. With regards to the customised software platform, this will give the business the opportunity to create and develop its own biometrics software applications to support its cloud-based infrastructure.

The PaaS Component
The third major component of the Biometrics in the Cloud, 'PaaS', is not a unique structure such as SaaS or IaaS, but a vehicle for software development. The main difference is the magnitude upon which these biometrics software applications can be built. For example, where the SaaS will support on demand software applications and customised software development which deal primarily with 1:1 verification scenarios, the PaaS will support much larger biometrics applications, such as 1:n scenarios.

Advantages and disadvantages of Biometrics in the Cloud

The advantages of Biometrics in the Cloud include:

- A biometrics infrastructure can be set up within literally minutes, all at the click of a mouse.
- It is on demand: biometrics services and other components can be added on or cancelled instantaneously.
- It is affordable, especially for the small to medium-sized businesses. Because of the cloud-based infrastructure, any costs will be at a fixed and predictable monthly

price; this is unlike traditional biometric systems where the costs can greatly escalate over a short period of time.
- It is highly scalable, meaning that a biometrics application can be cut back or expanded in just a matter of seconds. In traditional biometric deployments, the databases have to be literally redesigned and rebuilt in order to cope with increased demand, thus making it virtually cost prohibitive to do so. Because of resource pooling, the biometrics database(s) can be scaled to fit any array of biometrics applications within just a matter of minutes for a wide array of applications, ranging from the simplest 1:1 to the most complex 1:n verification scenarios.
- Redundancy is very easy and cost effective, given the pooled resource nature of the Biometrics in the Cloud infrastructure, whereas in traditional biometric deployments, redundancy very often means extra servers to store the biometric templates and other processes, resulting in a much greater expense.

- An enterprise grade level biometrics system is available to all. Traditionally, highly sophisticated biometric systems with the best performance were only available to those businesses that could afford it. With Biometrics in the Cloud, an enterprise grade biometrics system can be made available to all, and not just a select few.

The disadvantages include:
- Changes in biometric business processes. At the present time, each and every biometrics vendor has their own production processes and research and development strategies. However, when Biometrics in the Cloud does indeed become a reality, the entire biometrics industry as we know it will have to shift their strategies entirely to an on demand, services-based environment.
- Cloud resources need to be scalable to demand: it is very important that resources are not devoted entirely and exclusively to cloud-based biometrics just yet. There should not be any idle cloud-based resources waiting to be consumed, but they should be used up proportionally to the demand. Furthermore, the biometric algorithms need elasticity as well in order to fit the scalability requirements of the cloud.
- Legalities and privacy rights could become serious issues: biometrics has always been prone to claims civil liberties violations, loss of personal freedom, etc. This fear will only be heightened as biometrics moves into the cloud, because the biometric templates will be literally held at the hands of the hosting provider. Also, concerns can be expressed about the clear, legal separation between the biometric templates and other information/data which are stored at the hosting provider, even though technically they will be stored on different servers.

General acceptance

How easily will the concept of Biometrics in the Cloud be accepted? Interestingly enough, it is the geographic location as to where Biometrics in the Cloud will be implemented which will play a big role in terms of acceptance. For instance, in the United States, the acceptance rate of biometrics is extremely slow, which impedes the growth rate of Biometrics in the Cloud just that much further. However, in the developing nations (especially in Africa) the acceptance rate of biometrics is much higher, thus making it a catalyst for the adoption of Biometrics in the Cloud.

Conclusion

This article has examined what a Biometrics in the Cloud infrastructure will look like. Looking at the advantages, cloud computing for biometrics is clearly a positive solution for all those involved, once it proves itself and takes root over time. The only thing a business will have to do is procure the biometric hardware they need; the rest of the processes is the responsibility of the hosting provider, and is available on demand. Another major advantage of Biometrics in the Cloud is that it offers an affordable enterprise grade level biometrics system to all kinds and types of businesses.

But despite all this, the biggest impediment to Biometrics in the Cloud is time: it will take a long time to get these concepts fully accepted and implemented. However, it is highly anticipated that Biometrics in the Cloud will become fully accepted and very quickly implemented on a large scale.

References:
1 http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.
2 http://searchcloudcomputing.techtarget.com/definition/SPI-model.