2013

A Conceptual Model For Federated Authentication in the Cloud

Abdulwahid Al Abdulwahid
Plymouth University, Abdulwahid.Alabdulwahid@plymouth.ac.uk

Nathan Clarke
Plymouth University, N.Clarke@plymouth.ac.uk

Steven Furnell
Plymouth University, S.Furnel@plymouth.ac.uk

Ingo Stengel
Plymouth University, Ingo.Stengel@plymouth.ac.uk

DOI: 10.4225/75/57b55feccd8df
Originally published in the Proceedings of the 11th Australian Information Security Management Conference, Edith Cowan University, Perth, Western Australia, 2nd-4th December, 2013

A CONCEPTUAL MODEL FOR FEDERATED AUTHENTICATION IN THE CLOUD

Abdulwahid Al Abdulwahid[1], Nathan Clarke[1,2], Steven Furnell[1,2] & Ingo Stengel[1,3]
[1]Centre for Security, Communications and Network Research, Plymouth University, Plymouth, UK
[2]Security Research Institute, Edith Cowan University, Perth, Australia
[3]Glyndwr University, Wales, UK
Abdulwahid.Alabdulwahid, N.Clarke, S.Furnel, Ingo.Stengel}@plymouth.ac.uk

Abstract
Authentication is a key security control for any computing system, whether that is a PC, server, laptop, tablet or mobile phone. However, authentication is traditionally poorly served, with existing implementations falling foul of a variety of weaknesses. Passwords are poorly selected, reused and shared (to name but a few). Research has suggested novel approaches to authentication such as transparent authentication and cooperative and distributed authentication. However, these technologies merely focus upon individual platforms rather than providing a universal and federated authentication approach that can be used across technologies and services. The advent of cloud computing, its universal connectivity, scalability and flexibility, offers a new opportunity of achieving usable and convenient authentication seamlessly in a technology and service independent fashion. The approach introduces a new dedicated authentication provider – the Managed Authentication Service Provider – that is able to provide state-of-the-art centralised verification of authenticity. However, relying upon such an environment also introduces a range of technology, privacy and trust-related issues that must be overcome.

Keywords
Authentication, Transparent Authentication, Federated Authentication, Cloud Computing

INTRODUCTION

There are 6.8 billion mobile subscribers currently in existence many of which are increasingly utilising smartphones and other devices with a wide range of capabilities. Smartphones are capable of making telephone calls, texting, surfing the Internet, checking emails, playing games, viewing documents, transferring money, shopping online and storing confidential information (to name but a few of the tasks available!). This leads individuals, corporations and governments to rely heavily and prevalently on computing systems (i.e. PCs, servers, laptops, tablets and mobile phones) for accessing, storing and processing personal, financial, medical and business information that are often considered sensitive and confidential.

Therefore, close attention has been drawn to the critical importance in securing them from any unauthorised access. To secure any system or information, it is crucial that it must fulfil the CIA triad principles: confidentiality, integrity and availability. In order to maintain the first two, it is paramount for a system to uniquely identify legitimate users by an effective user authentication technique, which, if achieved, enables authorisation and accountability. Thus, it is evident that authentication is a cornerstone of information systems security.

Whilst various methods of authentication exist, they are traditionally poorly served thereby falling foul of a variety of drawbacks (Clarke & Furnell, 2007). Knowledge-based authentication has been the common standard means for user authentication on computing systems, making up approximately 4 out of 5 of authentication events (CA Technologies, 2012). However, with recent strict password policies, users are required to remember multiple, complex, longer, recycled, unshared and changing passwords, which if met would augment security control while compromising users convenience. Token-based

authentication seems to solve some password shortcomings; however, they have higher cost and fundamentally authenticate the presence of the token rather than the individual. Usability also becomes an issue when the user is required to carry multiple tokens for accessing a variety of services. Due to these weaknesses, further attention has been placed upon the final form of authentication, biometrics. They arguably have high availability, strong defence against repudiation and good levels of usability as the burden from the user to recall passwords or carry tokens is removed. However, it is not impossible to forge single static biometrics, and the likely need for additional reader devices and their accuracy are questionable (Clarke, 2011; O'Gorman, 2003).

The problem is further magnified as users are now in possession of an ever-growing number of advance digital devices; each one with its own associated security requirements. So, it is apparent that a more innovative, convenient and secure solution for user authentication is essential. Some attempts have emerged to counteract the aforementioned weaknesses of traditional authentication including deploying two/multi-factor authentication, such as the combination of password and token or two/multi-layer authentication. However, these techniques, on one hand merely augment security, but on the other hand degrade user friendliness. To enhance these solutions, research has proposed novel approaches to authentication, such as transparent authentication (Clarke et al., 2011), implicit authentication (Yazji et al., 2009), and cooperative and distributed authentication (Hocking et al., 2011). Nonetheless, these technologies merely focus upon individual platforms rather than providing a universal and federated authentication approach that can be used across different technologies and services. The advent of cloud computing, its universal connectivity, scalability and flexibility (Grobauer et al., 2011), offers a new opportunity of achieving usable and convenient authentication seamlessly in a technology and service independent fashion. However, relying upon such an environment also introduces a range of technology, privacy and trust-related issues that need to be considered in any proposed solution.

This paper builds upon existing research on transparent and distributed authentication, with a view of capitalising upon the benefits that cloud computing offers. The paper then presents the proposed federated authentication framework within the cloud. A detailed discussion and outline of the future work is subsequently presented.

LITERATURE REVIEW

Transparent Authentication

Point-of-entry authentication, which solely and initially establishes identification of the user at the beginning of the session but not throughout, has a number of flaws. The vulnerability increases when the identity of the user has been verified at login and the device is left on for long periods of time. For instance, 85% of mobile phone users who responded to Clarke & Furnell (2005) kept their mobiles on for more than 10 hours a day. This can lead to a high-risk environment in which an imposter targets the device following a legitimate login. If this occurs and the device is kept on and active, free and open misuse can be conducted for a substantial period of time. It was even pointed out in the original specifications for security in third generation (3G) networks that "It shall be possible for service providers to authenticate users at the start of, and during, service delivery" (3GPP, 2001) - the emphasis here on authenticating users during service delivery.

Therefore, it is imperative to increase the level of authentication beyond the standard point-of-entry technique. The potential aim is to use more advanced techniques that would enable periodic or continuous re-verification of the user without compromising the convenience. All authentication techniques are considered intrusive as they require the explicit interaction of the user. However, biometrics can also be deployed in a more usable fashion that allows the samples to be collected

spontaneously. They cannot easily be compromised, can be deployed in a non-intrusive manner and thus eliminate the potential threat posed by social engineering. Thus, the use of transparent authentication using biometrics would enhance both the requirement for a robust authentication mechanism and the user's need to eliminate any inconvenience during the authentication process. For this reason, Clarke & Furnell (2007) proposed transparent/non-intrusive continuous authentication using behavioural biometric techniques. This approach has the effect of moving away from a Boolean authentication result to a more meaningful and appropriate confidence measure. As illustrated in Figure 1, there is a disconnect in current authentication schemes that rather assume authenticity wherever an access control decision is made. However, through more closely aligning the authentication process with the access control decision, a more reliable and secure decision is made (as illustrated in Figure 2). Furthermore, the approach also takes into consideration that all authentication approaches are not equal and they have varying levels of authentication performance.

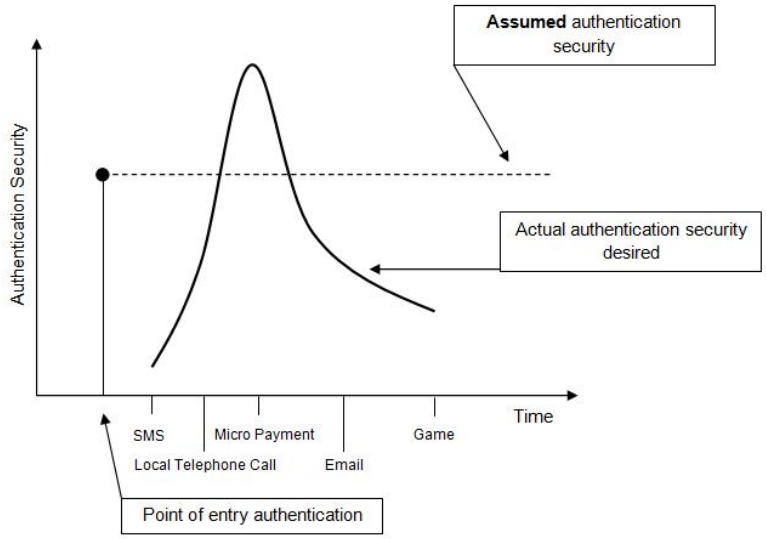

Figure 1: A Model of Traditional Authentication Security

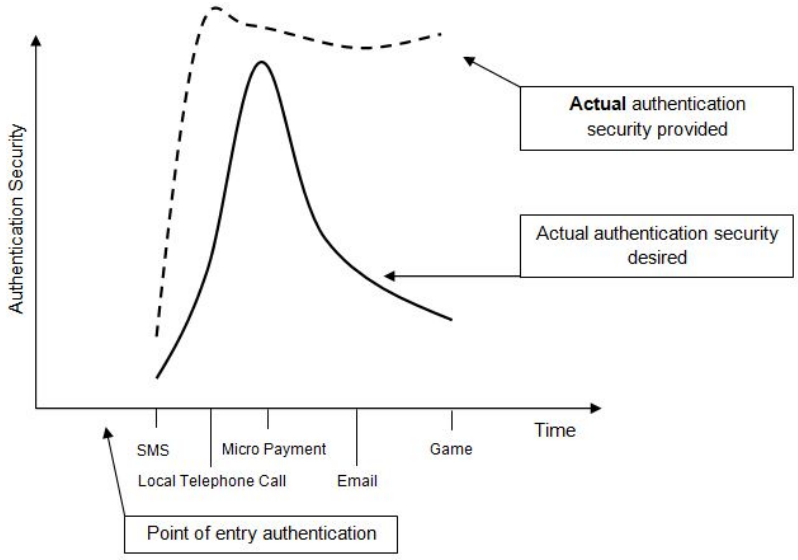

Figure 2: A Model of Continuous Authentication Confidence

Transparent Authentication Systems (TAS) has been developed by numerous prior researchers involving the authors and others. One implementation of TAS, the Non-Intrusive and Continuous Authentication (NICA) (Clarke et al, 2009) is a mobile-based solution that utilised a combination of several chosen available biometric techniques, which accomplished a performance of below 0.01% Equal Error Rate (EER). It is capable of choosing individual biometric techniques to verify a mobile user based upon the configuration of his/her device. For instance, if a mobile device is not equipped with an inbuilt camera, the TAS will only choose keystroke analysis and voice verification to verify the user. TAS does also consider the assumption that different services and data require different security provisions. Through understanding the risk associated with particular user actions and services, the protection level required can vary from almost none for checking the time, medium for texting, to significantly high for online banking. The level of confidence is continuously fluctuating based upon the biometric samples captured which is subsequently reflected on the privileges to access services and applications, enabling the device to shut down functionality if insufficient confidence exists. Whilst TAS can be appreciated as a remarkable solution to effectively remove the reliance upon the human aspects to ensure a robust and usable authentication, its applicability and universality have to be considered as it is confined to a single device. With every device requiring biometric setup and enrolment, user configuration and management, risk assessment and continual refinement.

Authentication Aura

The number of individuals having several digital devices to carry and/or use concurrently has increased. For example, it is a common place for people to have mobile phone (in many cases more than one), tablet, laptop, PC, and game console. It is likely that similar authentication techniques are applied across distinct devices possessed by the same individual. The repeated intrusive authentication process for each device is likely to be annoying and time consuming. To counteract this burden, communicating the identity confidence between devices would be useful. In the one hand, collective identity knowledge controlled by the array of secured devices operated by an individual at any given time offers an opportunity to enhance security and usability. Accordingly, this has led to the proposal of deploying and sharing the credentials of the individual's devices authentication confidence in a distributed and cooperative fashion, enabling a near field adaptive security envelope to be established and maintained around the individual- the user's Authentication Aura (Hocking et al., 2011). Authentication Aura enables the individual and distinct devices to communicate their own authentication status and confidence, and hence to establish an accumulative level of confidence.

Distinct devices are likely to employ different methods of authentication as shown conceptually in Figure 3. For instance, a laptop has an inbuilt fingerprint scanner, a smart phone has a PIN number, voice recognition and an inbuilt front camera, and a PDA has handwriting recognition. If a user has initially logged-in to a device by any authentication technique, the established combined confidence can be utilised to provide specific access to other trusted devices within a close proximity via a near field communication (NFC) channel. Consequently, the potential case is to acquire consolidating multi-biometric samples, which in turn mitigates some of the limitations of uni-modal biometrics by enhancing recognition accuracy, security, and usability (Ross et al, 2006). Confidence adaptation and degradation is applied over the time of missing or error acquired credentials and based on the un/known locales. Locking the system and asking for re-authentication would be necessary to re-determine the users credentials when an inappropriate level of confidence has been reached.

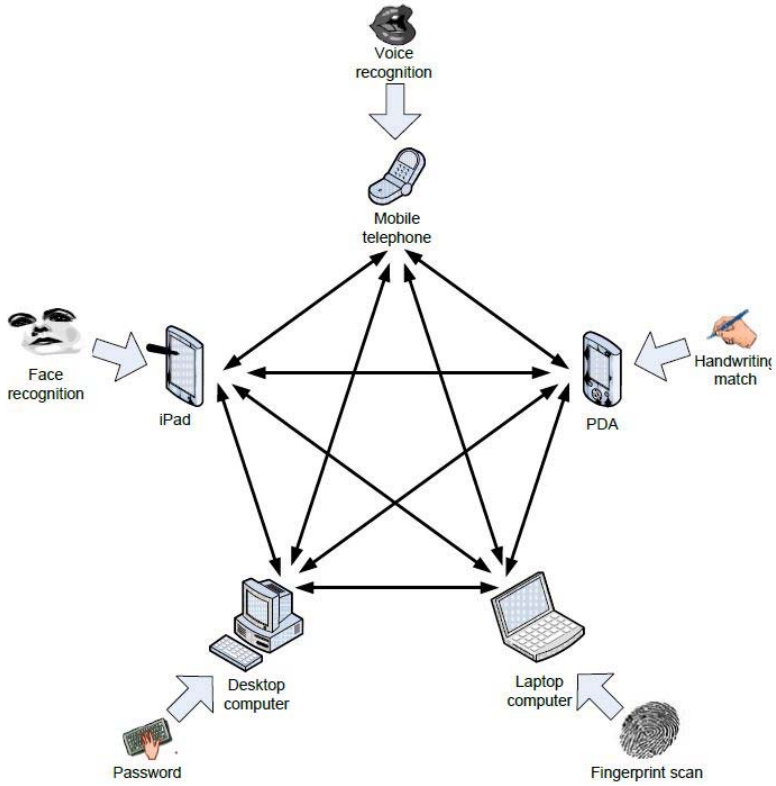

Figure 3: The Potential intra-device relationship and authentication techniques (Hocking et al., 2011)

The approach further improves the level of security being afforded whilst reducing the burden of user inconvenience. However, the approach to authentication is still disparate, with individual authentication approaches being supported on a number of technologies. Furthermore, the effective performance being achieved is highly correlated to the biometric software – a cheap facial recognition will experience a significantly different level of recognition accuracy to an expensive military-grade system. It is therefore not appropriate to merely have devices that supports biometric capture but also recognition capabilities with a good level of performance. Establishing trust in such an environment is complicated further. It also requires each device to support the Aura-framework and thus be capable of supporting a level of biometric processing, configuration and management.

FEDERATED AUTHENTICATION IN THE CLOUD

With the aforementioned evolution of authentication mechanisms and of digital device functionality, the necessity for transparent, universal and federated authentication approach that can be used across technologies and services is becoming more apparent. Federated authentication is similar to federated identity in that it extends the concept of authentication beyond an organisation or domain like single-sign-on does for federated identity. However, federated authentication is focused solely on the provision of authentication and not access control (as federated identity is). The concept of federated authentication is to centralise the task of authenticating an individual to a trusted third-party. Through providing a device and service independent authentication approach, the centralised authority benefits from specialisation, enabling it to provide the most appropriate authentication technologies and essentially removes duplication as the user no longer needs to enrol on each device, configure each device and authenticate to each device. Instead, the user has a single authentication profile within the Managed Authentication Service Provider (MASP), where they are able to manage and monitor their profile. Any MASP-enabled device or service will merely send a request to the MASP and be informed of its current real-time identity confidence. In this manner, individual devices themselves are relieved of a

significant amount of data processing and storage, including a large volume of duplicated activities that would be occurring with TAS and Aura enabled systems.

Extending the concept of the authentication aura, this approach permits devices and services that are not biometrically enabled to benefit from stronger authentication approaches. For example, current password-based web services, such as Google email, would now be able to transparently verify your identity – requiring the user to merely access the web page and the background services will check whether the identity confidence is sufficient to provide immediate access. Obviously in cases where the confidence is not sufficient, the user would be asked to verify their identity. The system allows for both device and service-level authentication. For device-level authentication, the user is required to initially install a service that will provide the interconnection between the local authentication mechanisms/services and the MASP. Once configured at start-up, this becomes a completely transparent process from the user perspective – with all future logins only required if sufficient confidence does not exist. For example, had the user in the morning, logged into his mobile phone using a strong biometric approach they would, within an appropriate timeframe and proximity as defined by the Authentication Aura (Hocking et al., 2011), may be automatically logged into his computer or any other device he owns.
The approach can also be utilised on devices the user does not own – providing a web-service level of integration. Upon initially connecting to the MASP identity through a web-based biometrically-enabled login, a user will be able to access any of his web-based services transparently without having to repeatedly enter his credentials. This can be achieved in one of two approaches:

1. (Preferred) The MASP connects directly to a federated identity system (e.g. OpenID) to provide seamless inter-domain single-sign on.
2. (Optional) The MASP provides a web service credential database (i.e. password store) and releases the appropriate credentials to the web service if sufficient confidence exists.

As illustrated in Figure 4, the framework incorporates functionality on the device to capture and pre-process (if necessary) authentication credentials, typically biometric-based information. This is a continuous process depending upon the device, its capturing capabilities and usage – the latter aspect being key to achieving transparent authentication. Beyond capture however, all remaining processing and responsibilities are undertaken by the MASP, removing any unnecessary processing and storage burden on the device. When utilising devices that the user does now own, this also serves to minimise any privacy implications and the local storage of biometric-based information.

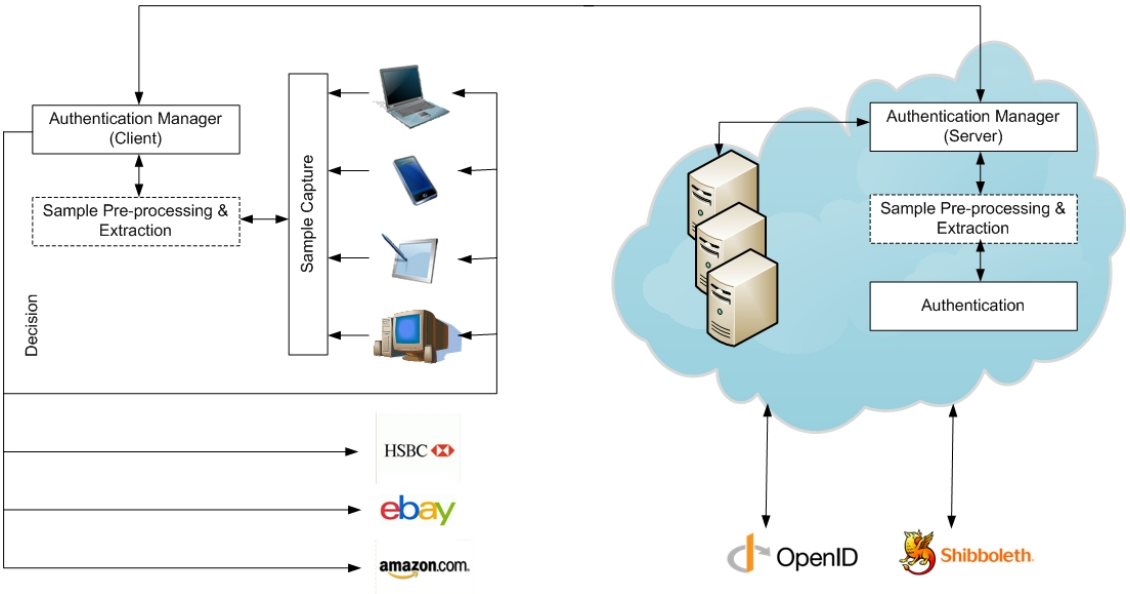

Figure 4: A Framework for Federated Authentication in the Cloud

An advantage of a centralised cloud solution is the ability to unify all authentication information, providing an in-depth understanding of what the user is doing (in terms of devices and services) and thereby providing additional identity intelligence of the user. For example, it will be possible to determine if two authentication requests are simultaneously made from different locations from devices that belong to the owner or otherwise – thus highlighting potential misuse. The centralised approach also enables the use of multibiometrics and multi-factor authentication – providing a robust framework of authentication models that are stronger than any uni-modal or single factor authentication approach. For example, depending upon the available authentication approaches (which themselves will be dependent upon the devices and technology a user utilises), a variety of multi-instance, multi-algorithmic, multi-modal approaches exist that seek to optimise the authentication decision. As illustrated in Figure 5, a multi-algorithmic approach would enable a MASP to utilise a range of biometric classification algorithms (each crafted to focus of differing aspects of the problem) and combine the result through fusion. Typically, cost, processing and vendor-specific solutions have prevented this for happening to date and continue to do so. As a centralised authentication service, the MASP, through ISO standards (i.e. ISO 19794, 19785, 19784) will be in a position to incorporate any and all approaches – something individual devices would never be able to achieve due to prohibitive costs and processing requirements (ISO, 2006a, 2006b, 2011).

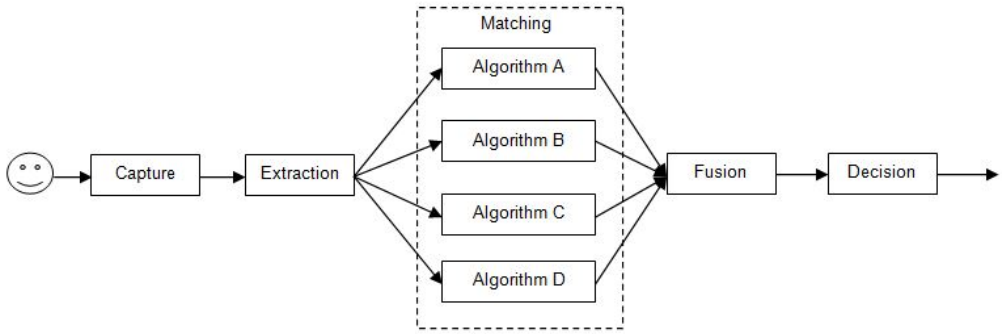

Figure 5: Multi-Algorithmic

Figure 6 illustrates a relatively simple multibiometric model that incorporations varying degrees of multi-

algorithmic processing and fusion at differing levels of the biometric process. These models would be unique to the user, varying depending upon which samples are present. This approach to the optimisation of authentication confidence will provide a very strong indicator as to the authenticity of the user. For example, as illustrated in Table 1, the use of multimodal systems can result in a significant improvement in the classification performance (Jain et al., 2005).

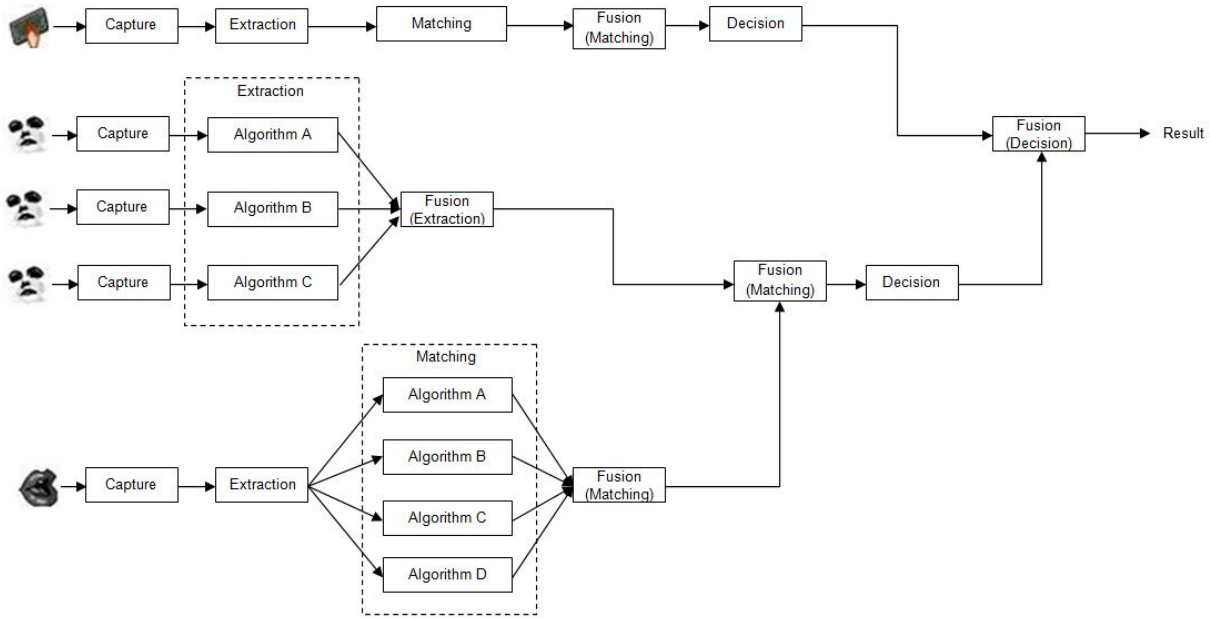

Figure 6: A Model for Multibiometrics within Federated Authentication

Classifier	**FRR at a FAR=0.1%**
Finger	16.4
Face	32.3
Hand	53.2
Multimodal (Minmax Norm)	2.2
Multimodal (Tanh Norm)	1.5

Table 1: Multimodal Performance using Finger, Face and Hand Modalities

The centralised approach also overcomes another hurdle in the creation of effective biometric classifiers – the availability of impostor data. Many modern classifiers utilise approaches that allow them to train the classifier to behave according to the valid or authorised user (e.g. neural networks); however, in practical live systems, the lack of availability inhibits the performance that can be achieved. Often this data needs to be simulated or created rather than being real user data. Moreover, many classifiers utilise full sample data, rather than derived statistics (such as a mean and standard deviation), making the creation of simulated data very challenging. Within a centralised system, anonymised impostor data will be available to all users for both initial enrolment and template refinement; ensuring classifiers are optimised.

MASP requirements will be largely dependent upon the number of users subscribed to the service, the number of active users and thus the volume of authentication decisions it needs to make at any point in time. With such variability in the level of service demand, a flexible and highly scalable processing and storage system is essential. Whilst distributed computing paradigms would be a solution, cloud

computing provides an ideal solution to this requirement – with Platform-as-a-Service (PaaS) providing an effective model for developing the necessary architecture for a highly scalable and adaptive solution.

DISCUSSION

Federated authentication provides a universal approach to identity verification that can be utilised by any network-enabled device or service. Whilst the introduction of such a system has the foundations for solving the authentication problem – both in terms of effective security and usability – it also introduces a range of further issues that need to be resolved in order for the system to operate effectively.

First and foremost is the need for users and organisations to trust a third-party provider with their authentication services. Fundamentally, to date, this is not a typical expectation and there might become concern over doing so. However, users already trust service providers with authentication credentials, albeit not all in one place. Furthermore, federated identity has become widely popular and this is based on the use of a single authentication credential. Federated authentication will offer a range of authentication technologies for inclusion within federated identity – extending the concept of federated identity but more thoroughly confirming the identity prior to the access control decision that is made. It arguably therefore should not be a complete leap in faith of organisations, but merely a logical extension of the services that are already being provided. It does however change the paradigm under which authentication will be performed – rather than a zero-cost solution as is (incorrectly) perceived to be cost of many secret-knowledge solutions, a federated authentication provider will need to charge at some level for the service it provides (perhaps on a per-authentication, per-user, monthly or organisational-basis). However, given the nature and scale of the authentication and security problem, the concept of paying to ensure appropriate authentication security should be more than viable.

With the technology itself, there are a number of areas that need to be further investigated. Considerations such as the time taken to process and authenticate a sample – in particular the lag introduced through the network and the potential bottleneck at the MASP. The latter can be addressed through the cloud and successful capacity planning. However, adding all the additional time lags introduced in a networked solution over a device-centric model might reduce levels of acceptability – so care must be taken to ensure this does not have a serious impact. It is not envisaged to be a major problem, as the concept of network-based authentication already exists for devices in network domains, and we all already login to remote services with the authentication process occurring on the remote server. Furthermore, the process of transparently authenticating individuals means, the capture and authentication of those samples will be undertaken continuously throughout the use of a service or device, not at point-of-entry. Therefore the user should not be left waiting.

Further issues surround the use of biometric information. From an end-user perspective, privacy is a key factor to consider. The storage, use and communication of biometric samples must be achieved in a manner that minimises the threat to interception and misuse of the information. The MASP architecture must be appropriately designed to provide separation and segregation of duties to ensure the opportunity of access the sensitive data is only possible to specific entities. Operationally, consideration needs to be given to effectively managing enrolment and template renewal. In TAS systems, they often rely upon many biometric approaches that are behavioural in nature and thus have features that are not time-invariant (as would be ideal). It is therefore necessary to update and renew the template in a timely fashion to ensure it is a true reflection of the users current set of features. Knowing when to do this and the implications it will have upon the processing infrastructure (as template creation is a far more processing and memory intensive task than authentication) is essential to the smooth and seamless running of the MASP. Bearing in mind, cost is also an important factor – it would not necessarily be suitable to merely utilise more systems but rather better manage existing resources.

CONCLUSION AND FUTURE WORK

Verifying the authenticity of a user to use a digital device or service has become crucial. Individuals, businesses and governments undertake an ever-growing range of activities online and via mobile devices and unfortunately these activities, services and information are the targets of cybercrimes. Authentication is at the vanguard of ensuring only the authorised user is given access; however, it has historically suffered from a range of issues related to the security and usability of the approaches. In order to provide them with adequate protection, innovative robust authentication mechanisms have to be utilised in a universal level, so they operate in a transparent, continuous and user-friendly fashion.

The proposal builds upon existing research on transparent and distributed authentication, with a view of capitalising upon the benefits that cloud computing provide. An authentication system built upon this would provide a more secure, user-friendly, universal and technology independent environment. As this proposed framework evolves, further research will be undertaken to consider human-aspects of security, including the privacy of highly sensitive biometric data and the operational factors that must be incorporated within the architecture to ensure a usable but highly secure system.

REFERENCES

3GPP. (2001). Universal Mobile Telecommunications System (UMTS); 3G security; Security threats and requirements. In *3GPP TS 21.133 version 4.1.0 Release 4*. ETSI 3rd Generation Partnership Project (3GPP).

CA Technologies. (2012). Advanced authentication methods: software vs . hardware. Retrieved from http://www.ca.com/~/media/Files/whitepapers/AMM_ebooklayout.pdf

Clarke, N. (2011). *Transparent user authentication: biometrics, RFID and behavioural profiling*. Springer London. Retrieved from http://www.springer.com/computer/swe/book/978-0-85729-804-1

Clarke, N. L., & Furnell, S. M. (2005). Authentication of users on mobile telephones – A survey of attitudes and practices. *Computers & Security*, *24*(7), 519–527. doi:10.1016/j.cose.2005.08.003

Clarke, N. L., & Furnell, S. M. (2007). Advanced user authentication for mobile devices. *Computers & Security*, *26*(2), 109–119. doi:10.1016/j.cose.2006.08.008

Clarke, N., Karatzouni, S., & Furnell, S. (2009). Flexible and Transparent User Authentication for Mobile Devices. In Gritzalis D And Lopez J (Ed.), *the 24th IFIP TC 11 International Information Security Conference* (Vol. 297, pp. 1–12). Pafos, Cyprus: Springer. Retrieved from http://link.springer.com/chapter/10.1007/978-3-642-01244-0_1

Clarke, NL, Karatzouni, S., & Furnell, S. (2011). Towards a Flexible, Multi-Level Security Framework for Mobile Devices. In *The 10th Security Conference*. Las Vegas, USA. Retrieved from http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Towards+a+Flexible,+Multi-Level+Security+Framework+for+Mobile+Devices#1

Grobauer, B., Walloschek, T., & Stocker, E. (2011). Understanding Cloud Computing Vulnerabilities. *IEEE Security & Privacy Magazine*, *9*(2), 50–57. doi:10.1109/MSP.2010.115

Hocking, C. G., Furnell, S. M., Clarke, N. L., & Reynolds, P. L. (2011). Authentication Aura - A distributed approach to user authentication. *Journal of Information Assurance and Security*, *6*(2), 149–156.

ISO. (2006a). ISO/IEC 19785-1:2006 - Information technology - Common Biometric Exchange Formats Framework - Part 1: Data element specification. Retrieved October 14, 2013, from http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=41047

ISO. (2006b). ISO/IEC 19784-1:2006 - Information technology - Biometric application programming interface - Part 1: BioAPI specification. Retrieved October 14, 2013, from http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=33922

ISO. (2011). ISO/IEC 19794-1:2011 - Information technology - Biometric data interchange formats - Part 1: Framework. Retrieved October 14, 2013, from http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=50862

Jain, A., Nandakumar, K., & Ross, A. (2005). Score normalization in multimodal biometric systems. *Pattern Recognition*, *38*(12), 2270–2285. doi:10.1016/j.patcog.2005.01.012

O'Gorman, L. (2003). Comparing Passwords, Tokens, and Biometrics for User Authentication. *Proceedings of the IEEE*, *91*(12), 2021–2040. doi:10.1109/JPROC.2003.819611

Ross, A., Nandakumar, K., & Jain, A. (2006). *Handbook of multibiometrics* (1st ed., Vol. 6, p. 202). New York, New York, USA: Springer. Retrieved from http://books.google.com/books?hl=en&lr=&id=JpUdlJnuE2MC&oi=fnd&pg=PR7&dq=Handbook+of+Multibiometrics&ots=k9Xpj2JG-U&sig=GnpcJo5652E5htmjIOYRk7cFKaQ

Yazji, S., Chen, X., Dick, R. P., & Scheuermann, P. (2009). Implicit User Re-Authentication for Mobile Devices. In *Ubiquitous Intelligence and Computing* (pp. 1–15). Springer-Verlag New York Inc. doi:10.1007/978-3-642-02830-4_25