IMAT2704   
Introduction to Research

**Assignment**

2000 Word Literature Review

Student: Georgios Karseras

P Number: 2424630

# How cloud-based biometrics increase security in smart devices and their potential implications regarding personal information and privacy for the users.

**Introduction**

As the Mobile Cloud Computing is rapidly growing, with more users connected than ever, there is a need for a stronger identification than possession and knowledge-based ones. That spot is being filled by the physiological and behavioural biometrics as they are believed to be unique to every person. Physiological biometrics includes the hand geometry, face, ear pattern, fingerprint, iris, palm vein and palm print, as for behavioural biometrics, voice, gait recognition, hand signatory and keystroke dynamics (Kiran, et al. 2018). Using biometrics makes it difficult for hackers to guess, convenient for users as it removes the necessity to remember a password or the probability of losing an access/identification card and most importantly it requires to be physically present for the authentication (Khatri, et al. 2017). Cloud-based Biometrics is the use of a centralized cloud server to store the templates, which are generated the first time a user enrols a biometric data to the Cloud and also to compare new data taken from the client-side devices to verify the user’s identity (Vorakulpipat, et al. 2018), thus offloading the computationally demanding task to the Cloud (Barra, Castiglione, et al. 2018). This is especially important in the case of Internet of Things (IoT) which are estimated to replace smart phones in the future, these are mostly small devices that serve a simple function and lack the computational power to perform authentication tasks (Vorakulpipat, et al. 2018). In most occasions, Cloud-Based biometrics provide faster processing, scalability, cost-effectiveness, quick integration and deployment, higher security and world-wide accessibility (Thakkar, n.d.), but a strong modification to the biometric information is required as to make them unusable in the case a hacker gets access to it (Patel, et al. 2015). With Cloud-Based Biometrics becoming more popular, a new market to offer Cloud Based Biometric services emerged, Biometrics as a Service or BaaS, being offered by Fujitsu (Fujitsu, 2017), BioID (BioID, n.d.) and many others (Thakkar, n.d.).

**General Biometrics**

Biometrics differ from the standard possession and knowledge-based identification in many ways. Besides the ability to uniquely identify a person and the ease of use as there is no need to remember a password, biometrics also differ from the older identification methods in negative ways. In the case of a compromise where your password gets leaked, you can easily change to a new one and never use the old, exposed, one. The same cannot be done in the case of Biometrics, as the uniqueness they provide also means the difficulty to modify them. When your data is breached, not only it becomes compromised forever and makes future authentications a problem, the user is then at a higher risk for identity theft (Ilga, 2008).   
Some questions were raised by Barra, Castiglione, et al., in regards to the security of biometrics which all companies should be weary of, firstly ”how do we ensure that the authentication mechanism in place cannot be compromised to wrongly identify an individual-for example, in national-security matters (such as terrorism) and serious and organized crime?” and secondly, how can we make sure that the collected biometric data are securely processed, stored and finally, when required, removed. Especially in the case of Cloud-Based Biometric systems, robust security is mandatory as the data continuously flows between the user and the server throughout the Web.   
Khatri et al. compared different physiological biometrics and found that iris scan as superior to the rest, due to these five reasons. Stability – the iris forms a unique pattern from the young age of 10 and does not have any changes throughout our lives, Unique – there is almost no chance that two people have the same iris code, Flexible – the sensors required to capture iris data are easy to incorporate to pre-existing security systems, Non-Invasive – as the sensors can operate from a distance while being fast and with incredible precision in comparison to alternative biometric gathering sensors, lastly, Reliable – as it is distinguishable, it cannot be lost or stolen.

**Cancellable Biometrics**

Patel et al. explains the need to have cancellable biometrics, which means the alteration of biometrics to the point where reverse-engineering to the original data is impossible without the original transformation code, while still be able to quickly reconstruct when needed for future identifications. As explained, the complete irreversible templates are not usable due to the captured biometrics almost never reproducing the same data, especially when passed through a permanent modification function like hash. Patel et al. dives down to various methods of achieving that, methods that are mandatory to have certain matcher and others that can function from pre-existing matchers, enrolment-free methods and ones that require good samples on the enrolment. These methods can then be broken in two groups, ones that function with the first enrolled biometric sample and others that function with the features taken from the biometric signals. Similar to cancellable biometrics but different is the use of cryptosystems, as explained by Patel et al., these are methods that “combine cryptographic keys with transformed versions of the original biometric templates to generate secure templates “. Besides the use of such methods to make the biometric data secure, there are also different ways of storing the data to help mitigate the entry points that hackers could leverage (Patel, et al. 2015).

**Storage of Biometric Data**

There are five main ways to store Biometric Data securely, a separate hardware embedded microchip unto the device which its sole purpose is the safe storage of Biometric data (Secure Enclave by Apple), a database server which stores the biometric information, a portable smart card or other storage device, on the primary device main memory which is the most frequent for smart phones and lastly, a combination of a server and local device storage (Ievo, 2018).   
Patel et al. suggested a combination for Cloud-Based Biometric storage, a part of the biometric data to be kept locally and the other part on a remote server, so that biometric information only takes readable form when needed, it also means that acquisition of only one part of the data has almost no value at all, which makes the data secure against hackers.   
Barra, Castiglione, et al. reviewed different proposed solutions to increase security in Cloud-Based Biometric, most of which had server-centric authentication, meaning the authentication process took place on the server while a user-centric solution was also given, PassBio, while this lost the computational advantage of the server, it gained the benefit in which the server never has the user’s biometric information (Zhou and Ren, 2018).

**Biometric Systems**

Multimodal Biometric Systems (MBSs) are the usage of more than 1 form of biometric information for authentication. According to Kiran et al. and the proposed framework from Khatri et al., it is much safer than the widely used Unimodal Biometric System (UBS) which is implemented in most devices. UBS, while being cheaper to implement and convenient, has several problems, as data obtained can be noisy due to sensors not being properly preserved or even malfunction, spoofing attacks, not being unique as some features are very similar on some people and in other cases, a person may not even be able to provide the compulsory biometric due to physical deterioration (Kiran, et al. 2018). Khatri et al. also proposed a MBSs framework with fingerprint and iris information to achieve higher security.

**Security in Biometrics**

As explained by Patel et al., biometric data cannot be kept a secret due to the nature of them being physically visible. That proves to be very dangerous as shown by Zhang, et al. in a Blackhat conference, as the reconstruction of fingerprint data can be achieved by obtaining any object touched even momentarily or from a high-resolution photograph. Jan Krissler, a hacker, managed to reconstruct the fingerprints of the German defence minister at the time, Ursula von der Leyen, using only photographs of her hands (Hern, 2014).  
At another Blackhat conference, that happened in 2019, Tencent employees Chen et al., showcased potential vulnerability in the security of the liveness detection of Face ID, the UBS of new Apple products. The vulnerability takes advantage of the sacrifice Apple did to security in favour of user experience. The Face ID works by the combination of a TrueDepth camera that constructs a depth map of the face and an infrared camera that takes a picture. With Secure Enclave, which is Apple’s embedded security chip, whose job is to protect the biometric data by transforming them, it makes the hacking of the device very difficult (Apple, 2020). As showcased though, not impossible, the vulnerability that Chen et al. discovered was with the usage of glasses, Face ID worked far less secure to accommodate for these user’s experience. Chen et al. said that “Face ID does not extract 3D information from the eye area”. Later is shown that with some glasses and a tape it could be used to manipulate the device and authenticate the user, even when used on the owner while sleeping which shouldn’t be possible if the liveness detection worked, thus having access to the phone and potentially stealing private information and money.

**Internet of Things with Cloud-Based Biometrics   
And  
Biometric as a Service (BaaS)**

Internet of things refers to small devices with specific purposes, this market is growing exponentially in recent years and is even estimated to replace smartphones in the future. These devices can be used in conjunction with IoT service platforms like Network Platform for Internet of Everything (NETPIE, n.d.) to connect them together, to the internet and generally make it easier to work with. With the usage of NETPIE it is also possible to connect IoT with Cloud-Based Biometrics, for example, a fingerprint reader captures the user’s data and sends it to NETPIE, which in turn connects with the server and gets the result back, after that it can notify other IoT devices connected to it to do various functions depending if the user is verified or not (Vorakulpipat et al. 2018).   
Biometrics as a Service is a relatively new market emerged with the large growth of biometrics, as many organizations cannot afford to design, implement and manage biometrics securely (Barra, Castiglione, et al. 2018), they turn to other organizations for these services. BaaS providers such as Fujitsu (Fujitsu, 2017) and BioID (BioID, n.d.) are more likely to have a strong security due to reputation, legal implications and just to gain a competitive edge (Barra, Choo, et al. 2018).

**Limitations of Research**

In the literature’s I have studied there were many proposed frameworks and solutions, but there wasn’t a clear one that had the best security, low cost, reliability and speed in terms of biometric data transformation. As Cloud-Based Biometrics is relatively new and the general usage of biometrics in devices is growing exponentially in recent years, there are a plethora of new researches being made with improved solutions. Patel et al. gave some limitations as well, firstly, the need to create a standard for testing and evaluation of proposed biometric systems and lastly, most cancellable biometric template schemes only got tested on medium or smaller size datasets, which does not reflect the millions from real case scenarios. There are also the new exploits being discovered daily, as seen through the Blackhat conventions and generally technical news sites, which means that at any given time a zero-day exploit could potentially put at risk the biometric information of millions if its target are databases or if its in the form of malware, the individual’s user’s data. As such, there is always a need to improve and make sure the biometric data is secure from attacks that do not even currently exist.

**Conclusion**

In conclusion, biometric data should be treated carefully due to their nature as being everlasting on a person. Firstly, these data should always be in an unreadable form in case of data breach, using cancellable biometrics, cryptosystem methods or a combination of both. Secondly, biometric data should be securely stored with either a dedicate chip on the device that exclusively handles the protection of biometric data such as Apples implementation, Secure Enclave, or the proposed by Patel et al., half of the transformed data on the device and half on a remote database. Thirdly, in accordance to both Kiran et al. and the framework that was given by Khatri et al., Multimodal Biometric System should also be implemented as it was calculated to increase security immensely in contrast to Unimodal Biometric System. Finally, we can see that with the combination of these methods, the biometric data is mostly secure and even the vulnerabilities discussed could be further mitigated in the future as new transformation methods are being discovered and technology advances, which means better sensors and higher computational power become widely available. In the case of smartphones, it could become safer if companies focus exclusively on security, even at the cost of the user’s experience.

# Bibliography

Barra, S., Choo, K.-K.R., et al. 2018. *Biometrics-as-a-Service: Cloud-Based Technology, Systems, and Applications*. IEEE Cloud Computing [Online] 5(4), pp. 33–37.  
Available at: https://ieeexplore-ieee-org.proxy.library.dmu.ac.uk/document/8436083  
[Accessed: 2nd May 2020].

Barra, S., Castiglione, A., et al. 2018. *Cloud-Based Biometrics (Biometrics as a Service) for Smart Cities, Nations, and Beyond*. IEEE Cloud Computing [Online] 5(5), pp. 92–100.  
Available at: https://ieeexplore-ieee-org.proxy.library.dmu.ac.uk/document/8497010  
[Accessed: 2nd May 2020].

Khatri, S.K., Monica and Vadi, V.R. 2017. *Biometrie based authentication and access control techniques to secure mobile cloud computing*.   
In: 2017 2nd International Conference on Telecommunication and Networks (TEL-NET) [Online] pp. 1–7.  
Available at: https://ieeexplore-ieee-org.proxy.library.dmu.ac.uk/document/8343558   
[Accessed: 3rd May 2020].

Vorakulpipat, C., Takahashi, T., et al. 2018. *Usable and Secure Cloud-based Biometric Authentication Solution for IoT Devices*.   
In: 2018 IEEE Symposium on Computers and Communications (ISCC) [Online] pp. 00274–00277.  
Available at: https://ieeexplore-ieee-org.proxy.library.dmu.ac.uk/document/8538712   
[Accessed: 2nd May 2020].

Kiran, M.A., et al. 2018. *Biometric Authentication: A Holistic Review*.   
In: 2018 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) [Online] pp. 428–433.  
Available at: https://ieeexplore-ieee-org.proxy.library.dmu.ac.uk/document/8653751   
[Accessed: 3rd May 2020].

Patel, V.M., Ratha, N.K. and Chellappa, R. 2015. *Cancelable Biometrics: A review*. IEEE Signal Processing Magazine [Online] 32(5), pp. 54–65.  
Available at: https://ieeexplore-ieee-org.proxy.library.dmu.ac.uk/document/7192838  
[Accessed: 5th May 2020].

Zhou, K. and Ren, J. 2018. *PassBio: Privacy-Preserving User-Centric Biometric Authentication*. IEEE Transactions on Information Forensics and Security, 13(12), pp. 3050–3063. [Online].  
Available at: https://ieeexplore-ieee-org.proxy.library.dmu.ac.uk/document/8361432  
[Accessed: 6th May 2020].

Zhang, Y., et al. 2015. *Fingerprints on Mobile Devices: Abusing and Leaking* [Online].  
Available at: https://www.blackhat.com/docs/us-15/materials/us-15-Zhang-Fingerprints-On-Mobile-Devices-Abusing-And-Leaking-wp.pdf  
[Accessed: 4th May 2020].

Chen, Y. et al. 2019. *Biometric Authentication Under Threat: Liveness Detection Hacking* [Online].  
Available at: https://i.blackhat.com/USA-19/Wednesday/us-19-Chen-Biometric-Authentication-Under-Threat-Liveness-Detection-Hacking-wp.pdf  
[Accessed: 4th May 2020].

Ievo Ltd (2018). *How Biometric Data is Stored* [Online].   
Available at: https://ievoreader.com/how-biometric-data-is-stored/   
[Accessed: 2nd May 2020].

NETPIE (n.d.). *Network Platform for Internet of Everything* [Online].  
Available at: https://netpie.io/   
[Accessed: 6th May 2020].

Fujitsu (2017). *Fact Sheet Biometrics-as-a-Service™ (BIOaaS™) Solution* [Online].  
Available at: https://www.fujitsu.com/us/Images/Biometrics-as-a-Service\_factsheet.pdf  
[Accessed: 3rd May 2020].

Thakkar, D. (n.d.). *Biometrics as a Service: Taking Biometrics to the Cloud*. [Online].   
Available at: https://www.bayometric.com/biometrics-service-taking-biometrics-cloud/   
[Accessed: 6th May 2020].

BioID (n.d.). *The BioID Web Service. Biometric authentication in the cloud*. [Online].   
Available at: https://www.bioid.com/bioid-web-service/   
[Accessed: 6th May 2020].

Ilga (2008). *Biometric Information Privacy Act.* Illinois General Assembly [Online].  
Available at: www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57  
[Accessed: 6th May 2020].

Hern A. (2014). *Hacker fakes German minister's fingerprints using photos of her hands* [Online].  
Available at https://www.theguardian.com/technology/2014/dec/30/hacker-fakes-german-ministers-fingerprints-using-photos-of-her-hands  
[Accessed: 6th May 2020].

Apple (2020). *About Face ID advanced technology* [Online].  
Available at https://support.apple.com/en-us/HT208108  
[Accessed: 6th May 2020].