International Journal of Advance Research in Science and Engineering
Volume No.07, Issue No.05, May 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

Investigation of Multibiometric on Samsung Galaxy S8

Thiyagu A/L S.Ravichandran[1], Maaniccaraja A/L N Tannirmalai[2]

Student[1&2], BSc (Hons) Cyber Security, Asia Pacific University, Kuala Lumpur, Malaysia

ABSTRACT

This research discusses the impact of multi-biometric technology on modern smartphones and its impact on performance, security and personal privacy. Privacy is necessary to human beings for who we are, and specific person to makes choices every day. An overview of multi-biometric and biometric are explained in this paper. Iris scanner offers a considerably more straightforward contrasting option to recollecting passwords and usernames. A client should simply enrol their iris on a database (not the retina – retinal filtering utilizes an alternate piece of the eye), which at that point coordinates the one of a kind example against its records consequently. Not exclusively does this give a speedier and more solid methods for validation, but on the other hand it's absolutely extraordinary to you – making life significantly more troublesome for a programmer. It's far simpler to figure somebody's watchword than imitate the extraordinary make-up of their eye. Lastly the studies are analysed and discussed which includes solutions and impacts.

Keywords: *Biometrics, Facial Recognition, Iris, Privacy, Performance, Security*

1. INTRODUCTION

Biometrics is automated methods of recognizing a person based on a physiological or behavioral characteristic. For example, type of features based on physiological are fingerprints, retina, face, iris or example of behavioral characteristic are gait and signature. As the level of security breach and transaction scam increases, the need for well secure identification and personal verification technologies is becoming apparent. Biometric identifiers or programs are being used in many applications. Each and every biometrics has its advantages and disadvantages and the selection typically depends on the applications. [1] The biometric verification process comprises of a few phases, measurement, signal processing, pattern matching, and decision making. Measurement includes detecting biometric attributes and is fundamental both for the making of the reference display and for every verification trial. For example, when voice check is used, this stage includes recording one's voice through an amplifier. At that point the computerized information is numerically demonstrated. At the point when the user needs to be authenticated, the device looks at the received information to the user model and makes a decision generally in light of a pre-figured limit. Biometric verification systems are not 100% exact. There are two sorts of errors in an average biometric system. A false reject (FR) error is the rejection of an approved individual attempting to get to the system. Errors is

the acceptance of an individual who isn't in actuality claims to be. These two sorts of errors are conversely corresponding and overall it can be controlled by a certainty limit. To expand the security of the system, the limit can be expanded, which decreases FA mistakes and increases FR blunders. [2].

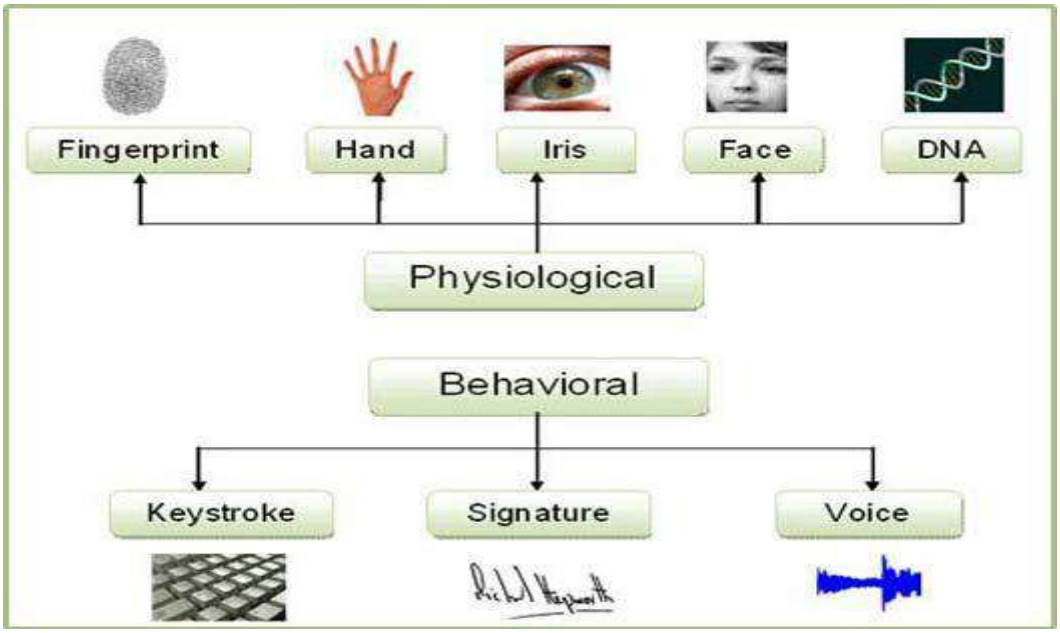

Figure 1: Types of Biometric

2. MULTI-BIOMETRIC

In a multi-biometric system more than one biometric quality are utilized for the identification purpose and expected to be more reliable due to the presence of multiple, independent pieces of evidence. Furthermore, multi-biometric system is an approach in biometric recognition technology that promises improved matching accuracy, reliability provides anti-spoofing measures by making it troublesome for an intruder to at the same time spoof the different biometric attributes of a genuine user. By requesting the user to display an irregular subset of biometric. In this manner, a test reaction compose of authentication can be made possible by the use of multimodal biometric systems. [1].

The use of multibiometric on smartphones is changing the smartphones security levels day by day. The technology has grown to become a more essential way to prove our individualities and it won't take too long time to biometrics plays a larger role to prove our identities for patient identification in healthcare, time and attendance (workforce management), and banking and finance. Examples of multibiometric playing a big role in smartphones are in the security of the phone, in the matters of payments and data access [3].

2.1 Security

There are huge number of people are practicing using smartphones for a purpose in their daily life. For example, for their daily activities, job, often storing highly sensitive information and etc. However, most of the people who are using smartphones are concerning about the security protection of using passwords. So, to overcome this problem a multi-factor security system using multibiometric recognition offers smartphones using higher security and connivance.

2.2 Payments

Biometrics payments are a Point of Sale (POS) technology which uses biometric authentication system to identify a person by their unique traits such as a fingerprint, facial recognition or iris recognition. However, the rising utilization of biometric identification for financial administration transactions has just started to spread quickly around the world. Moreover, big organizations and financial institutions out there has started to show their interest to implement biometric based payment solutions**.** This method has been encouraged by people because of its benefits which you don't need to carry cash, checks or credit cards, they offer stronger security, transactions can be processed faster, and banks don't charge any extra fees.

2.3 Data Access

Our smartphones are loaded with personal information and we create passwords to secure them. All the more particularly, we utilize passwords to access our smartphones. For example, Samsung galaxy s8 have some ability where they have a camera that can be utilized to verify individual identities through biometric innovations, for example, facial recognition or iris recognition.

3. BENEFITS OF MULTI-BIOMETRIC.

One of the advantage of multibiometric are the accuracy. The accuracy of a multibiometric system is estimated by the errors in image obtaining and matching of the biometric attributes. Moreover, multibiometric can reduce data distortion. For example, if a fingerprint scanner rejects the fingerprint image due to poor quality using another biometric modality such as facial rejection will lower the false rejection rates. Furthermore, multibiometric increase the security level. Multibiometric system extremely hard to be hacked when compare with single biometric system. If one of the biometric modality has been hacked, the individual still can access to the system using another biometric identifier [4].

4. CONTACTLESS BIOMETRIC TEMPLATES

There are many traits that can be obtained and utilized by a multibiometric innovation for identify a person which don't require physical contact with the gadgets being utilized. Below mentioned are some of the traits used.

4.1 Facial Recognition

Like hand geometry, facial recognition utilizes spatial geometry to recognize different features of the face. This innovation includes the utilization of camera to get the key features of a face and investigate it for recognizable identification and verification. In spite of the fact that this innovation was previously a prominent strategy in biometric identification proof, there are a few negative focuses which recommend powerless execution. The pictures taken for templates can be massively influenced by the encompassing components, for example, lighting while catching a picture, the posture and introduction of face, hair, any outward appearance, enlightenment and furthermore the way that the human face changes with time. Further, the creation and development of more unpredictable calculations can effectively disguise human faces.

4.2 Facial Thermography

Facial thermography process by which a person special physical and different quality are identified and recorded by an electronic gadget or system as a method for identify character. Facial thermography recognizes warm examples made by the branching of veins and discharged from the skin. These examples, called thermograms, are exceedingly particular. Created in the mid-1990s, thermography works much like facial recognition, with the exception of that an infrared camera is utilized to capture the pictures. Infrared systems work precisely even in diminish light or in darkness [5].

4.3 Iris Scan

As the uniqueness of iris is well known, the iris filter has turned into the most broadly embraced and most precise biometric template for verification. Aside from papillary reaction to light, the iris isn't impacted by any natural and surrounding factors, it is likewise one of the constant organs of one's body. Since, iris designs are framed in total irregularity and have stable random surface, no two iris designs coordinate each-other, and they are different from left eye to right eye. For scanning purposes, a simple charged-coupled gadget (CCD) computerized camera is utilized which utilizes close infrared light and unique lights to catch a high complexity particularly clear photo of an iris. The iris transforms into dark black color, because of which the camera can recognize and separate iris from pupil. Once the camera is centred around the iris, at that point finds and captures pictures of the focal point of the pupil, the edge of the pupil, the edge of iris and the eyelids and eyelashes which are changed over into computerized information as to be utilized as a template. These templates provide 200 reference points to compare and verify.

4.4 Voice recognition

Voice recognition systems perform the task of authenticating an individual's claimed identity by using certain characteristics extracted from his or her voice. An example of voice authentication is in telephone banking systems where the system operates with the user's knowledge and also requires co-operation from the users. It is also possible to implement these identification systems covertly without the user's knowledge [6]. For example, it can be used to identify the speakers in a discussion or alert automated systems of speaker changes. This technology can be evaluated on various techniques such as false acceptance rate and false rejection rate. For sensor subject distance of 20 cm, false acceptance rate is 2% and false rejection rate is 10%.

5. BIOMETRIC SCANNERS TECHNOLOGY ON PRIVACY

Like all personal data collection, biometric technologies can also pose problems related to privacy protection. First, many biometric technologies can detect diseases. Venous recognition, in fact, detects vascular diseases, while some types of fingerprint recognition may show chromosomal diseases.Behavioural measurements can present the same problem: gait recognition, or fingerprint and signature recognition can show signs of neurological disease, in addition to identifying the person. Gait analysis has concerned attention because of the faults of other biometric security techniques. Iris scans and face recognition require reasonably high-quality images, for example. They also generally require a cooperative subject, as do fingerprints. By contrast, a person's gait can be recognised from low-quality CCTV footage. In one leading method, known as the gait energy image, computer vision techniques use video images of a person to create a blurred outline that is characteristic of their gait. A human operator links this gait "signature" to a person's identity, allowing the system to automatically spot that person when they are next caught on film [7] .The iris- recognition highlight in Samsung's new Galaxy S8 plus smartphone has been crushed by German programmers, not as much as a month after it hit retires the world over. Concerns about privacy can be divided into three groups:

- Identification beyond the objective: the very purpose of recognizing a person is distorted and their medical condition is revealed.
- Unwanted objective: recognize a person who did not want to be identified.
- Hidden identification: a person is identified without his knowledge

A video posted by the Chaos Computer Club, a long-running programmer aggregate framed in Berlin in 1981, demonstrates the security highlight being tricked by a spurious eye into feeling that it is being opened by an honest to goodness proprietor [8]. The fake eye, which is made utilizing only a printer and a contact focal point to coordinate the ebb and flow of the eye is best made utilizing photos of the iris taken with an advanced camera in night mode.

6. PERFORMANCE SECURITY

The Samsung Galaxy S8 plus is an awesome phone with bounty to love, however it's not great. In the wake of being accessible for almost a year we're beginning to see a considerable measure of grievances about Galaxy S8 performance issues. Furthermore, tragically more keep on surfacing as clients sit tight for the move up to Android 8.0 Oreo.The greatest Galaxy S8 issue for most is the unique mark scanner area. It's set in a ghastly spot. Raise mounted scanners are wherever on Android, however never in favour of the camera. Far and away more terrible, the Galaxy S8 and S8+ are longer than most, nearly putting it distant.Unfortunately, there's no genuine method to settle this, proprietors basically need to get used to the new area. Muscle memory will make them look for a home catch that isn't there. Our best answer for genuine unique finger impression issues is set it up again for a more exact perusing.

Apps launch faster and battery life is longer: Galaxy S8 and S8+ are speedier and better-performing phones thanks to the innovation of the 10nm processor that runs on 20% less power. It's as efficient as you are. Downloads, charging, and switching from app to app are all accomplished at incredibly fast speeds. Thanks to the most advanced 10nm processor: It's the world's first and it's on the Galaxy S8 and S8+. And because the Galaxy S8 and S8+ are meant to take spills, splashes, and dunks, you can keep going even in the rain—or in the shower.

6.1 Performance of Samsung Galaxy S8 Plus

Figure 2: detailed of GPU and CPU

International Journal of Advance Research in Science and Engineering
Volume No.07, Issue No.05, May 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

6.2 Security of Samsung Galaxy S8 Plus

Figure 3: detailed of security

Knox protects application and data by strictly defining what each process is allowed to do and what data it can access. This allow Knox to separate, encrypt, and protect enterprise data within a managed contain. Periodic Kernel Measurement &amp, Real-time Kernel Protection work to constantly inspect the core software of the OS, the kernel. These checks ensure that requests to bypass device security are blocked and sensitive data is protected.The Knox platform leverages a processor architecture in which highly sensitive computations are isolated from the rest of the device's operations, protecting enterprise data. To prevent security measures from being bypassed or compromised, Knox uses Boot-time Protections backed by Hardware Root of Trust to verify integrity of the device during the boot process.

Figure 4: detailed of security layer

Some of the most sensitive activities like paying with your credit or debit card and accessing bank accounts is fast, easy, and secure on your Galaxy S8 or S8+ with its selection of authentication options, including biometric verification. Scan your irises or fingerprint to make purchases with Samsung Pay in-store, check your bank accounts via Samsung Pass, and log into your favourite sites right away with the Web sign-in feature. Keep private files and apps separately in the Secure Folder to keep them accessible only to you

7. IRIS VS FINGERPRINT RECOGNITION

Fingerprint recognition is a dominant security highlight in the more up to date age of smartphones and is an outstanding biometric innovation. Since Microsoft presenting iris recognition highlight in its smartphones, there were correlations between these two biometric characteristics. We will talk about both these biometric advances, their abilities and security highlights.

Iris and fingerprint recognition acknowledgment both have higher precision, unwavering quality and straightforwardness when contrasted with other biometric attributes. These properties make iris and unique finger impression recognition perform better and an especially encouraging security arrangement in the present society. The procedure begins by catching the pictures of iris and unique mark which are then pre-prepared to evacuate any clamour impacts [4]. The recognizing highlights are then removed and coordinated to discover comparability between both the capabilities. The coordinating scores that are created from the individual recognizers are given to the choice module which chooses if a man is certified or an impostor.

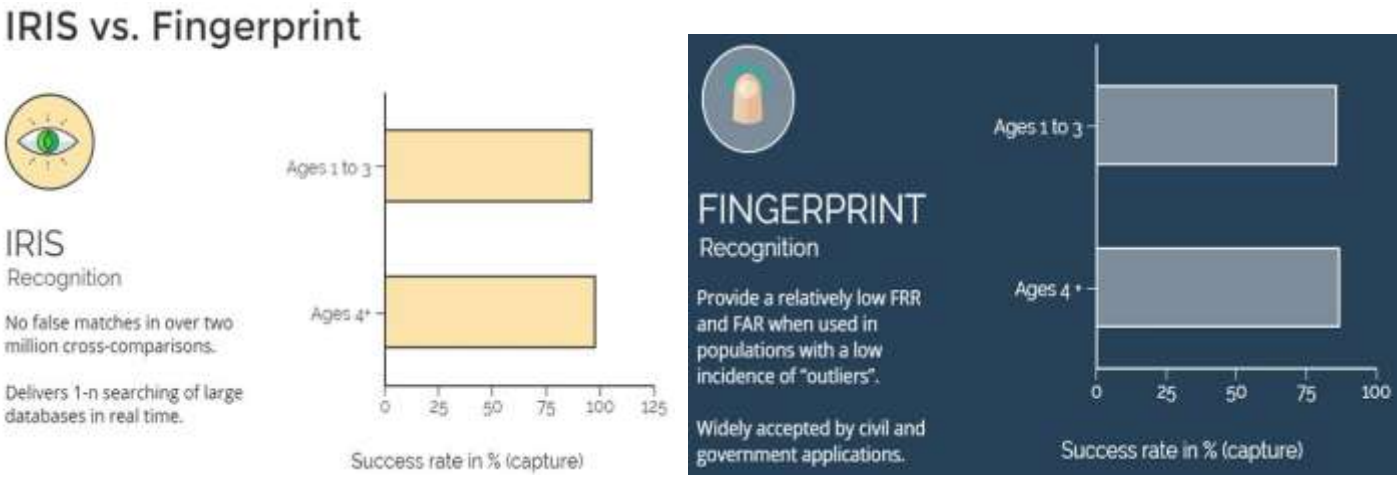

Figure 6: IRIS vs. Fingerprint

8. FUTURE OF IRIS SCANNER

The adaptability of iris recognition fits practically any application where character confirmation is required to upgrade security, guarantee benefit, wipe out misrepresentation or augment accommodation.

8.1 Tomorrow

Endeavor and government both recognize the merging of physical and data security conditions, yet there are new security challenges not too far off – without a moment to spare stock control, advanced inventory network administration, and even a wonder called "coopetition"- in which organizations that contend in a few regions, collaborate in others.Dealing with this merging of physical and data security prerequisites now drives security framework engineering plan and execution and is an inexorably enter factor in biometric innovation choice. Overseeing merging will just turn into a more intricate errand in light of the fact that as the IT and interchanges turns out to be progressively remote, the requirement for vigorous character administration will turn out to be more intense.

9. LIMITATIONS AND RECOMMENDATIONS

In this paper, it discussed the impact and limitation of multibiometric technologies. There are several limitations on the research in this paper. Firstly, it is about the cost. Multibiometric are very expensive. Due to multi type of biometric were built in, the device is expensive as well as the installation will be expensive. Secondly, high enrollment time. Due to more than biometric were used it takes some time for the enrollment process. Besides that, it also increases the system development and complexity.

As a recommendation for the future study of this topic, we can say that there is both positive and negative of biometric although biometric security is becoming more advanced and common with the latest technologies. However, facial scanners can be fake using a special pair of glasses and fingerprint readers can be tricked using Play-Doh. We can say that it can lead to a comparatively safer security solution if biometrics is attended by MFA (multi-factor authentication). Moreover, the researcher that study for this topic needs to discuss more on the privacy issues by collecting the information and evaluate it to improve the biometric technologies in the future. Therefore, it can also help to minimize the impact of the privacy in the biometric technologies in the future.

10. CONCLUSION

Identity authentication can allow access to high security facilities, perform exchanges and let individual cross borders, so exact user authentication has become very vital in today's connected and fast-moving world. Since biometrics is being used for physical as well computerized identity authentication, it has become important to improve reliability of present biometric systems. Biometrics began its journey with biometric systems, in which it

used single source of biometric information. As biometrics advanced toward personal identification for access to high security facilities as well as mainstream identification method, it ended up matching performance and reliability of these systems are trustworthy. This level of reliance on biometric identification and authentication made researchers look for new ways, which led to multi-biometrics [4]. Multi-biometrics can be enhanced by incorporating diverse systems and merging biometric information at different combination levels.

11. ACKNOWLEDGMENT

Author would like to thank Mr Umapathy Eaganathan, Faculty in Computing, Asia Pacific University, Malaysia for his constant support and encouragement to publish and attend this international conference in India.

REFERENCES

[1] MohmadKashif Qureshi "Liveness Detection of Biometric Traits" on International Journal of Information Technology and Knowledge Management, January-June 2011, Volume 4, No.1, pp.293-295

[2] Erden, Mustafa. "Advantages and Disadvantages of Biometric Authentication". SESTEK Blog, SESTEK.N.p., 2017, Web.16 Mar.2017.

[3] Hassan Sbeyti "Mobile User Authentication Based on User Behavioral Pattern (MOUBE)". International Journal of Computer Science and Security (IJCSS), Volume-10, Issue-4, 2016, pp:120-139.

[4] Danny Thakkar "Importance of Biometric Fingerprint Technology: Does Your Organization Really Need it? This Will Help You Decide!". Online Access (www.bayometric.com)

[5] Hannah Dear, Kate Wittkowski "Facial Thermography". Online Access (www.prezi.com)

[6] Tarun Agarwal. 2018. *Biometric Sensors – Types and Its Working*. [ONLINE] Available at: https://www.elprocus.com/different-types-biometric-sensors/. [Accessed 8 March 2018].

[7] Belen Rios-Sanchez, Miguel Viana-Matesanz, Carmen Sanchez-Avila, Maria Jose Melcon De Giles, "A Configurable Multibiometric System for Authentication at Different Security Levels Using Mobile Devices". 2016 IEEE 35th Symposium on Reliable Distributed Systems Workshops (SRDSW) (2016), Budapest, Hungray, Sept.26,2016, ISBN: 978-1-5090-5260-8, pp: 19-24

[8] Public Safety : Products & Solutions | NEC. 2018. *Public Safety : Products & Solutions | NEC*. [ONLINE] Available at: http://www.nec.com/en/global/solutions/safety/Technology/Multi-Biometrics/index.html?. [Accessed 08 March 2018].