Technoarete Transactions on Intelligent Data Mining and Knowledge Discovery
Vol-2, Issue-2, May 2022
ISSN: 2583-195X

Importance of Data Biometric in the Organisational Culture

Geraldin B. Dela Cruz[1*], Rayner Alfred[2]

[1] Tarlac Agricultural University, Philippines
[2] Universiti Malaysia Sabah, Malaysia
*Corresponding Author Email: delacruz.geri@gmail.com

Abstract

Biometric data is a technology that users or workers use and saves a lot of time. This technology helps people to keep things, data, and information more safe. There are several types of biometric such as fingerprints scan, iris scan, palm scan, face scans and many more. Users no longer need to remember passwords or pin codes because of this technology. Users just have to scan their fingers or palm, face or eyes to unlock devices and this system is way more secure than any other systems. Though it is a high cost system, organisations can trust on this system because no one can easily hack this technology as every person has different characteristics. Passwords, pin codes, pattern locks can be easily hacked but hacking someone's fingerprints or iris scan is quite impossible. Still hackers can hack this technology sometimes. Mainly voice commands get hacked easily because anyone can record a user's voice without consent. In that case, users have to be more careful about personal things and should not share single information with anyone.

Keywords

Biometrics, Technology, System.

INTRODUCTION

Biometric data is a system used for the motive of validation and authentication of a person. This is an extremely secured system and has a low chance of duplicity. However, sometimes everyone has seen one can duplicate biometric data by using some of the same technologies quite easily. The best process for security would be both password based and biometric authentication. In possibly any multisensory approach various identification requirements are more secure than single identification applications. In the matter of learning technologies, it has proved to be more successful. Several identification systems accumulate images of face, iris scans, fingerprints or many other biometrics for biometric identification. Biometrics is simply the body estimation and measurements connected to human characteristics [1]. Biometric verification is used in computer science as a need of recognition or identification and approach control. This process is also applied to recognise one person in groups which are under observation.

Biometric modifiers are the particular, quantifiable characteristics applied to describe every person. Realistic identifiers are frequently classified as corporal characteristics which are connected to the appearance of the body. Genuine biometric use is quite application based. Determined biometrics will be way too better than many other security systems [2]. It is not possible for every single biometric to encounter every criterion. The process of a person using biometric for the first time is called "enrolment". During this period, biometric details of a person are stored and caught. In following uses, biometric details are compared and exposed with the details kept while enrolment. It is important to retrieve and store the system and it should be secured if the system is to be strong. The first sensor is the intersection between the system and the actual world. This system has to collect every possible data that is necessary. More often this is an image addition system, but this system can swap according to the characteristic aspiration [3]. The second block functions all the important pre-filtering. This has to remove all the antiquity from the sensor, to increase the input such as removing noises from the background, and use some regulation. The third block is used to extract the important features. It is a quite major step as it extracts the right features in an excellent way.

Through the enrolment process, the arrangement is clearly kept somewhere. In the matching phase, the acquired arrangement is passed to an intermediary who contrasts it with other living arrangements, approximating the space between them using any conclusion. The similar function will examine the arrangement with the input. It will be an output for an identified purpose such as access in a controlled area, however it is a worry that the usage of realistic data may cause a lot of mission creep. Parody attacks contain conforming fake unreal biometric systems, and these are some big warnings that can reduce the security [4]. In recent studies, it has shown that they can be avoided by considering every single biometric characteristic.

MATERIALS AND METHODS

Interpretivism research philosophy has been selected in this study. The reason behind choosing this philosophy is that it is built on the theory which expresses that the researcher executes a particular character in noticing the social world. As per this research belief, the research depends on the

ISSN: 2583-195X

investigator's interests. This philosophy includes investigators to explain matters of the study. In this study, cross-sectional research design has also been followed because it is a type of research design where one can gather information from several individuals in a moment. In this method one can notice changeable without affecting them. Inductive research approach is also followed in this study. The reason behind following this method is, this is a method of drawing closure by going from the particular to the extensive. This is actually differentiated with logical reasoning in which one can begin from basic information to particular conclusions. Secondary data has been collected in this study to develop and understand the value of biometric systems.

RESULTS

Security benefits of Biometrics

The productive usage of biometrics can be a strong slice of a provision's access control system. As its basis, biometrics use every human characteristic to ensure their identification, and can develop security while reducing problems connected to stolen and lost pin codes or passwords. Few years ago, biometrics were functions that were only seen in detective movies, but, biometrics nowadays have become extremely common. It has become a basic feature on smartphones. Some frequently used biometric procedures include: eyeball scan, signature or voice, facial identification, fingerprint, hand shape and palm [5]. In the last decade, an unbelievable development has occurred in the field of biometrics that means these products are becoming more beneficial, fruitful and reliable. The high level recognition management which is provided by biometrics provides several advantages by controlled devices.

Correct identification

Conventional security systems use smart cards, passwords, pin codes. Biometrics provides high level prominence, by removing possible problems around stolen authorizations [6]. The usage of functions such as eyeball scans, fingerprints make sure genuine recognition which cannot be copied easily.

Time saving

Biometric technology can be fruitful for different workplaces. Biometric recognition technology is an excessively quick process and allows every individual to be rejected or recognised instantly [7]. This rapid movement of goods and staff can be beneficial to make sure the work flow is regulated.

High security

The biggest advantage that a biometric system provides is developed security for work. A worker member's physical details cannot be shared, stolen or guessed; that means an extra safe and secure work environment for every worker [8]. Furthermore, a biometric system is excessively adaptable and provides everyone an adjustable and expandable solution which can be used anywhere an individual may need a security counterpoint.

User Friendly

Once an organisation sets up its biometric system and gives proper training to all the workers and staff, it is a most easy and reliable process to maintain. This is also an extremely user-friendly explanation as once the process is done correctly there is no need of carrying extra access cards or remembering passwords or pin codes.

User Responsibility

Because of the accuracy of the biometric system, the person who is responsible for the facility's access control can directly link a person to a specific event or function. This survey sequence can prove to be exceptionally useful in the function of a security contravention.

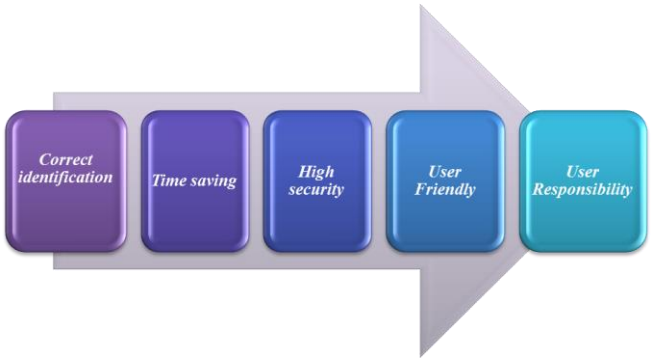

Figure 1: Security benefits of Biometrics

Everyone is using biometrics and that considers most of the customers nowadays think of biometrics to get the most sealed and stable method of ID verification. Every single technology has good sides as well as bad sides [9]. Bad side of any technology is the worst thing that can happen in the world. Every technology needs well trained, well cautious, sensible workers to maintain the system.

Some types of biometric and their barometer

Two different types of biometric are behavioural and physiological. These two types include different kinds of biometric identification criteria. At the time of unlocking a mobile phone with fingers or a face scanning system to work in some bank's application, or telling "Hey Alexa" to know about some information are several types of using biometric technology [10]. An individual's fingerprint is the most frequent biometric used in today's world. This type is considered a "physiological" biometric indicator. A specific person's face scanning or face identification is also a type of physiological biometric, but can also be separated to show different physiological biometric sensors such as nose length and shape, type of the hair, shape of the ear, eyes width and others [11]. Physiological biometric data is examined with things such as fingerprint readers and facial identification - features which are quite common on tablets, laptops and smartphones.

On the other hand, "behavioural" biometric indicator is

ISSN: 2583-195X

about an individual's voice - particular patterns which are connected to a person's steps. A corporal fingerprint scan can be lifted off of a device and can be calculated to create a portrait. However there are some intersections to physical features, behavioural biometric indicators are growingly being used in online and digital apps to determine and follow an individual build on a set of structures made by how they behave.

The main and most important parts which are mostly scanned in Physiological (body shape) biometric systems are - fingerprints that define creases on fingers. Every human being has different kinds of finger creases. In the finger print scanner, a device actually scans finger creases. Palm print that defines the lines seen on everyone's palm and palm width [12]. Some specific lines on the palm look almost the same on everyone's hand but every person has different palm lines. In this process the device also scans those lines. Measurements of face that describe the distance between eyes, colour of hair, size of head, nose and the ear geometry. All these things vary from one to another.

Scanner scans those specific things on the human body. Hand graphics define the distance between one fingers to another finger. Every person has a different structure and shape of fingers. Even the distance between fingers varies from one to another. The length of the fingers is also being scanned in a device [13]. Blood explains an individual's blood group or blood type. There are different kinds of blood groups or blood types, and the scanner scans them. DNA illustrates a hereditary pattern. Veins define patterns of veins in hands and eyes. Every person has different vein patterns in their hands and eyes, devices scan the veins of everyone. Device scans Electrocardiogram and heart beats on a human body.

On the other hand, in behavioural biometric indicators, patterns are identified in human behaviour. Human gestures are being scanned in this process. Web navigation includes swiping and scrolling. This process adds speech and voice conjugation [14]. In behavioural biometric indicators, IP address and geo-location, usage of device, history of browser and cookies, habits of purchasing are also included. As mentioned earlier, every technology has both advantages and disadvantages. Disadvantages in any matter are the worst thing. Some disadvantages of biometrics are - cost problems, data contravention, traces and data [15]. Notable funding is extremely needed in biometrics for security purposes. To make the system stronger and more powerful and useful, a heavy investment is needed in this process. There is no doubt that an advanced and maintained security system would need a remarkable cost and investment to implement.

Nowadays every single thing that is done online can be hacked. This is obvious that biometric databases can also be hacked and if it is getting hacked, that will be extremely dangerous. Both governments and private businesses gathering personal information are under continuous warning directly from hackers. Biometric data is unique; companies have to treat delicate biometric systems with growing caution and security [16]. Some systems that are quite expensive and strong are always difficult to hack. In the matter of pin codes of password, one can change it but no one can change a person's behavioural and physiological biometrics. This is a confidential matter or process of every company or organisation. Biometric systems such as facial identification devices can control privacy for buyers. Machine learning and techniques are quite advanced to reduce biometric analytical prejudice. Sometimes users face problems like false rejection and wrong acceptance. This is quite disturbing and dangerous for every user.

Importance of biometric in organisations

Every organisation or company or business and government always wants to update every work and technical process. Biometrics is more or less being used in every organisation. In recent times, biometrics are helping companies in cooperating remote, hybrid and pliable working arrangements for their workers without being exposed to growing security dangers. Biometric technology only provides control to sanctioned users. , this is why it is tough to sneak and trick, and never allows adaptable attacks. It decreases the danger of being hacked and violation through sneaked credentials, lost systems or deficiently secured networks.

The rebel of biometrics has been reserved by a regulation and awareness of privacy. Worker details are way more major than they used to be[17]. Concentrated storage of delicate biometric data is a big concern. Managers, though, can rotate to compounds that use on-system biometric data storage. This removes the managerial burden of making, protecting and maintaining a middle database. Another matter that cools down biometrics is security. After all, data contravention is increasing. Hackers would face hard problems by using the data fetched from a biometric sensor.

Biometric technology is often used in smart locks known as biometric access cards that can clarify physical entrance control for pliable working, and also working time becomes more nimble. Biometrics also works with time management, attendance systems and time so properly that it makes human resource decision makers and security personnel's job easier [18]. One of the most major advantages of this process is it helps organisations or companies or any users become password less and this process literally saves time for every person. Workers can finally get rid of remembering passwords for everything they do. Not only have the workers of the organisation, the mobile device users are also getting rid of remembering passwords and saving timed as much as they can.

Biometric ID systems provide assurance and extremely high security. It helps users to confirm everyone's identity. Users face hugely fast and convenient experiences. Biometric systems are being used by more or less every organisation. It is obvious that organisations want to save time and have enough security at any cost. The worldwide biometric identification and authentication is about to expand to 100 billion US dollars by 2027 [19]. During the predicted period

ISSN: 2583-195X

of 2019 to 2027, the market is estimated to increase at a combined annual growth rate of 14.6 percent. This data provides an idea about the acceptance of biometrics technology in current days.

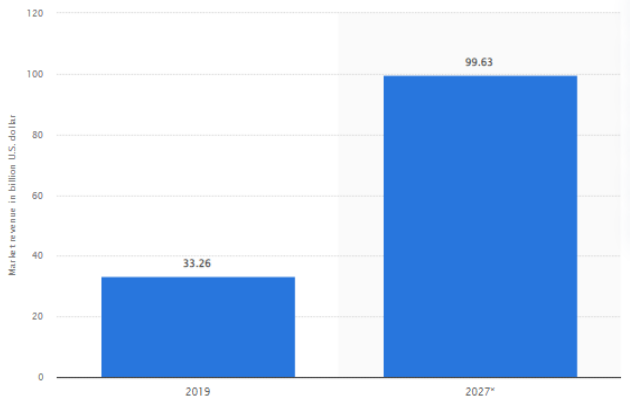

Figure 2: Biometric authentication and recognition market revenue across the world in 2019 and 2027

This process is non-transferable because every person has a unique set of biometrics. Biometric has now become a regular practice for several workspaces. Mainly, these organisations quote the health pros of many several technologies. Systems like building access, recording of time, security monitoring of temperature and many other things help decrease the number of workers coming into contact with each other and make sure that every worker is fit and fine for the job. Several organisations have acquired a usual example of a biometrics system - thermal imaging [20]. Organisations can fast verify a worker's body temperature if it is above the required limit while they pass through the gate. This removes the need of an actual person who manually checks the employee's body temperature which saves money and time at the same time. This might seem an expensive system but actually it is a onetime investment thing. Workers no longer need to think about themselves about being in the wrong hands. This system does not allow users to access any files that are related to companies or any business functions and buildings without authenticating them. Biometric recognition involves regulating the ID of a worker. The motto is to catch a product of biometric data from workers. It might be a record of a worker's voice or a scan of their fingerprints or it can be a face scan. One of the major benefits of the devices that have biometric security systems is it helps to grow the protection [21]. It is quite tough to steal anyone's fingerprint or face image or voice command. Biometrics are not only a single verification thing, it can include multiple verification in case of increasing security level. Biometric is a high level security maintained technology which authenticates and recognises every person based on the body characteristics. Biometric might be the most used system in the future as this system gives different levels of security. Biometric characters are most compatible and unique across the whole world.

Some problems of biometric system

Biometric systems are excessively used in every verification place but this system is not achievable for users who have extremely uncertain signatures. Also, there are some people whose signatures are quite simple and forged very often. It decreases the performance of this system. Besides, there are twin siblings whose facial identification system might be confusing for the system. This system seems to be the most secured method but it is not more secure than passwords [22]. A password or pin code is essentially a personal staff because only the user has the right to know that. In Spite of the fact, the hackers can obtain it by force attacks, but in general, normal users cannot use or access it. Alternatively, biometrics is fundamentally public. People disclose their ears, eyes, and nose every time. It is impossible for anyone to hide their face. Rather than that, there are so many high technological gadgets; anyone can record a user's voice command without their concession. Also a hacker can easily crack every database to steal and leak a user's biometric IDs.

Sturdiness of biometric system environment

The high performances demanded by the manufacturers of biometrics were difficult to realise in real operating environments. Nearly every operating test is managed in controlled lab environments where every single thing was tested in a genuine environmental place, and that is not possible in a real place of work or at any workspace because of the voice identification system which worked good with a silent background will affect the exactness of the verification system of voice due to the background noise. The same happens with the face identification system which is based on normal cameras is extremely affected by the issue of light.

DISCUSSION

In today's world technologies are getting updated every day and this fact has a good side and a bad side equally. Biometric system is an extremely updated technology which is a life saviour kind of thing for more or less every organisation and the government as well. Workers are saving much more time during work. The biometric system is being really helpful for mobile device users. Mobile devices are getting unlocked real quickly. Users are giving fingerprints or facing the front camera to unlock the device which saves their time. These systems are actually using an individual's personal characteristics to verify or recognise a person. These characteristics are prepared by a biometric system that can do a great job on comparing face features, fingerprints, blood types, body temperature to recognise a user. In spite of the fact that, biometrics are extremely safe and secure and highly recommended technology, this technology also can get hacked. This system is quite problematic for the users who have inconsistent signatures [23]. In case any person wants to hack the voice identification system, they can easily copy the voice command without the user's consent. Though it is a highly maintained and secured system, users have to

ISSN: 2583-195X

remember that it is a system and any system will have issues. But this technology is getting updated every day and of course in the future the cost of this product will decrease. The security system of this technology will increase with time. Even the workers of biometric technology have started to work on the face scanner, fingerprints and every other scanning issue the users are facing. Technicians are also increasing the security system of voice command scan as that is getting hacked more often. The camera issue is also getting recovered by the technicians. Every organisation is trying to install a biometric identification system but cannot get one because of the fund. Once the cost of the system will start to decrease, every organisation including the small businesses will be able to use this system.

CONCLUSION

Users of every technology will also have to be concerned and responsible with the technologies. It is true that technologies get hacked more often but that happens not only for the issues of the technology, sometimes it happens for the users also. Some cases are giving access to someone on mobile phones or smart devices. Users often give access to other people and give them permission to enter their fingerprints as the biometric system has the option of giving multiple fingerprints. This is quite valuable and good technology for information security in case the system is being used properly. Nevertheless, like any other systems for verifying, authenticating and recognising a user this has disadvantages of its own. Not a single technology is flawless; this is why biometric systems should be used in concurrence with one other system. The most valuable and important motto of a biometric device is accuracy.

The contravention of privacy as an outcome of possible data exude and data revelation, ID robbery, misuse of personal information and many other dangers remain the main social and moral concerns in case of using biometric systems. Biometrics holds personal recognisable living structures of the human body to exclusively identify the users. Fingerprint scan and other ways of identification have often been used in law administration and forensics for decades. Some biometric scanner systems might gather and keep personal details of the users, which can probably harm the user's privacy. The protection technique of biometric systems is especially important because theft fingerprint scans may put workers at danger, providing hackers control of information like worker's health or crime records. Each and every technology works with risk, biometric identification systems are still hugely reviewed as one of the most secure, genuine and accurate technologies by the experts of verifying user's identification because of its accuracy.

REFERENCES

[1] Zou, Zhengbo, and Semiha Ergan. "Evaluating the effectiveness of biometric sensors and their signal features for classifying human experience in virtual environments." *Advanced Engineering Informatics* 49 (2021): 101358.
[2] Radzi, Syafeeza Ahmad, et al. "IoT based facial recognition door access control home security system using raspberry pi." *International Journal of Power Electronics and Drive Systems* 11.1 (2020): 417.
[3] Zhou, JianQiao, et al. "2020 Chinese guidelines for ultrasound malignancy risk stratification of thyroid nodules: the C-TIRADS." *Endocrine* 70.2 (2020): 256-279.
[4] Parody attacks contain conforming fake unreal biometric systems, and these are some big warnings that can reduce the security
[5] Sharif, Muhammad, et al. "An overview of biometrics methods." *Handbook of Multimedia Information Security: Techniques and Applications* (2019): 15-35.
[6] Yadav, Chandra Shekhar, et al. "Malware Analysis in IoT & Android Systems with Defensive Mechanism." *Electronics* 11.15 (2022): 2354.
[7] Kloppenburg, Sanneke, and Irma Van der Ploeg. "Securing identities: Biometric technologies and the enactment of human bodily differences." *Science as Culture* 29.1 (2020): 57-76.
[8] Schwartz, Stephanie P., et al. "Work-life balance behaviours cluster in work settings and relate to burnout and safety culture: a cross-sectional survey analysis." *BMJ Quality & Safety* 28.2 (2019): 142-150.
[9] Jakovljevic, Miro, et al. "COVID-19 pandemia and public and global mental health from the perspective of global health security." *Psychiatria Danubina* 32.1 (2020): 6-14.
[10] Neville, Stephen J. "Eavesmining: A critical audit of the Amazon Echo and Alexa conditions of use." *Surveillance and Society* 18.3 (2020): 343-56.
[11] Amali, S. Miruna Joe, and G. Rajeswari. "Evolution of Deep Learning for Biometric Identification and Recognition." *Handbook of Research on Computer Vision and Image Processing in the Deep Learning Era*. IGI Global, 2023. 147-160.
[12] Boone, Leggie L. "Fingerprints." *Manual of Crime Scene Investigation*. CRC Press, 2023. 181-192.
[13] Rudy, Hayeem L., et al. "Three-dimensional facial scanning at the fingertips of patients and surgeons: accuracy and precision testing of iPhone X three-dimensional scanner." *Plastic and reconstructive surgery* 146.6 (2020): 1407-1417.
[14] Cheong, YeonJoon, K. Alex Shorter, and Bogdan-Ioan Popa. "Self-focusing in the ocean using out-of-band phase conjugation." *Applied Acoustics* 174 (2021): 107800.
[15] Zhang, Xichen, et al. "Data breach: analysis, countermeasures and challenges." *International Journal of Information and Computer Security* 19.3-4 (2022): 402-442.
[16] Holland, Peter, and Tse Leng Tham. "Workplace biometrics: Protecting employee privacy one fingerprint at a time." *Economic and Industrial Democracy* 43.2 (2022): 501-515.
[17] Charalampous, Maria, et al. "Systematically reviewing remote e-workers' well-being at work: A multidimensional approach." *European Journal of Work and Organizational Psychology* 28.1 (2019): 51-73.
[18] Trivedi, Sandeep, and Nikhil Patel. "Virtual Employee Monitoring: A Review on Tools, Opportunities, Challenges, and Decision Factors." *Empirical Quests for Management Essences* 1.1 (2021): 86-99.
[19] Sava, Justina Alexandra**.** **"**Biometric authentication and identification market revenue worldwide in 2019 and 2027". *statista*. Nov 8, 2022,

ISSN: 2583-195X

https://www.statista.com/statistics/1012215/worldwide-biometric-authentication-and-identification-market-value/

[20] George, Anjith, et al. "Biometric face presentation attack detection with multi-channel convolutional neural network." *IEEE Transactions on Information Forensics and Security* 15 (2019): 42-55.

[21] Hamidi, Hodjat. "An approach to develop the smart health using Internet of Things and authentication based on biometric technology." *Future generation computer systems* 91 (2019): 434-449.

[22] Reese, Ken, et al. "A Usability Study of Five {Two-Factor} Authentication Methods." *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. 2019.

[23] Rodrigues, Rita, Rita Coelho, and João Manuel RS Tavares. "Healthcare signage design: a review on recommendations for effective signing systems." *HERD: Health Environments Research & Design Journal* 12.3 (2019): 45-65.