

Biometric Security in Organization

¹Bibi Jahara Varekar, ²Dr.Abhijit Banubakode

¹Student, Dept. of Computer Science MET College Mumbai, Maharashtra, India

²Principal, Dept. of Computer Science MET College Mumbai, Maharashtra, India

Abstract: *Biometric Security recognizes and validates as per biological or behavioral characteristics. As this innovation is made sure about and advantageous, the turn of events and utilization is expanding quickly. For instance, five years back, individuals didn't consider the employments of a unique mark in their mobile phones, yet today this is a basic element of a cell phone to secure client information. The same extent of Biometrics Technology is growing hurriedly and making life progressively agreeable, increasingly direct, more brilliant just as ensured.*

1. INTRODUCTION

The exponential development of the web alongside the expansion in internet business applications use calls for stricter security controls (i.e. using biometric security devices). The need to protect customer and financial data from unauthorized access make logical secure Biometrics provide security benefits for everyone in the organization – end users, IT vendors, security system personnel, etc. Biometric technology is one area that organizations cannot afford to ignore. Biometrics has been effectively executed in numerous basic applications and has been utilized to get to control for over 10 years. Although passwords have been traditionally used to authorize access to computer systems and networks, they cannot be considered a reliable security measure because of their vulnerability to being stolen or lost.

Biometrics satisfies the conditions of authentication, non-repudiation, confidentiality, and integrity. Out of all the currently existing security methodologies, biometrics can provide very strong access control and security solution for organizations.

The usage of the unique mark based biometric security gadgets in an association can fundamentally build the security of electronic gadgets, for example, PCs, organization PCs, and so on. Furthermore, the organization can protect its sensitive data better by implementing fingerprint biometrics as compared to passwords. Often laptops nowadays come with built-in fingerprint recognition features that helps users to increase the security of their data. Therefore, organizations looking to enhance the security of their premises, networks, systems, and data can do so conveniently and reliably with the help of biometric devices. Notwithstanding wellbeing and security, biometric security gadgets permit associations to effortlessly follow worker time.

1.1 Fingerprint

Biometric Fingerprint Reader is making representative distinguishing proof increasingly solid and easy to understand. Companies who want to keep their offices safe from unauthorized personnel as well as maintain accurate records of employee hours.

Security is a big issue these days, especially in large companies where all employees or temporary workers are not well known by the entire staff. Employers need a reliable way to provide the safest environment possible. This includes finding ways to be sure that only authorized personnel are in the office building or on the job site.

1.2 Iris Recognition

Iris-based arrangements have for some time been perceived as the most exact of biometric advancements. However, for years they were used largely to authenticate identity, often with an access control card, at doors in high-value government and enterprise locations. But that as it may, iris acknowledgment has significantly more to offer than just passage control. Here's a gander at some creative ways diverse market fragments use iris acknowledgment frameworks. Business— Iris systems are used for time-and-attendance, eliminating timecards, simplifying the back-office process and ending an expensive fraud known as buddy punching, a practice in which one employee clocks in or out for a friend.

Enterprise – Large public and private organizations count on iris recognition as an end-to-end solution, identifying employees at the front door and then again to confirm authorization to access computer networks.

1.3 Retina Recognition

Retinal Biometrics is a refined method for recognizing individuals by the example of veins on the retina (the deepest layer of the back piece of the eye). It requires the utilization of an uncommon scanner about the size of a shoebox that can delineate an exceptional example of veins on the retina. The example is mind-boggling to such an extent that even indistinguishable twins don't have a similar vein arrangement. The individuals who favor its utilization guarantee retinography has a blunder pace of just one out of many.

A retinal scanner uses infrared light for mapping. As an individual investigates the eyepiece, an undetectable light emission vitality infrared light follows a roundabout way on the retina at the rear of the eye. The blood-filled vessels assimilate a greater amount of the infrared light than the encompassing tissue. Along these lines, there is a variety in the force of the reflection. The scanner quantifies this reflection at 320 focuses along the shaftway. It at that point allocates a force grade somewhere in the range of zero and 4,095. The subsequent numbers are compacted into an 80-byte PC code. This code would then be able to be contrasted and designs that have just been gone into the PC's database. Retina checks are as of now being used in the Pentagon and government and corporate associations where individuals should be distinguished before they can enter a zone.

1.4 Face Recognition

Face location/acknowledgment has been a developing field throughout the previous scarcely any years.

With advancements in computer vision, companies have been able to leverage powerful algorithms to help solve a variety of problems. However, there have been debates about the balance between benefit to society vs the cost of people's privacy.

Here are a few ways that organizations are using face detection.

1.4.1 Tracking and Monitoring

One of the most controversial areas right now concerning organizations using face detection technology is law enforcement.

This is a complicated issue because while this will induce valid privacy concerns from the public, this can also help save lives and prevent potential crimes or find criminals after a committed crime.

The way that law enforcement agencies can use these algorithms is to typically purchase services from a different company.

Amazon is one popular option that offers its **Recognition** API service to help law enforcement agencies in identifying faces from uploaded video, social media, and other sources.

1.4.2 Security

Another well-known way that organizations are utilizing face identification/acknowledgment is by including individuals' appearances as a layer of security for getting to gadgets.

Using Apple as an example, they have completely replaced the industry standard of using a fingerprint scanner to unlock a smartphone. In 2017, Apple announced their new Face ID technology that would replace their fingerprint "*Touch ID*" method of unlocking the iPhone. All subsequent iPhones have used Face ID as the only option to quickly unlock the phone. This suggests how confident Apple is in its face recognition technology that they made it the sole way (aside from manually inputting a PIN code) to access the phone.

Microsoft has also made use of face recognition as part of its "*Windows Hello*" biometric-based system. This system allows users to unlock their Windows 10 device by either a fingerprint, iris scan, or face recognition.

1.5 Computer access

In PC security, biometrics alludes to verification methods that depend on quantifiable physical attributes that can be consequently checked.

1.6 Serve Rooms Entry

biometric filtering or something to that effect, (for example, voice acknowledgment or unique mark examines) is getting progressively normal, making it undeniably increasingly hard for somebody to take or duplicate access certifications. A few offices go above and beyond by controlling room get to remotely, requiring even approved workforce to be confirmed again by safety faculty.

2. RESULTS AND DISCUSSION

We have created a survey form and collected data from different employees of organizations. We have asked the employee which biometric security device he/she has used from the following identifiers list:

1. fingerprint
2. Retina Recognition
3. Iris Recognition

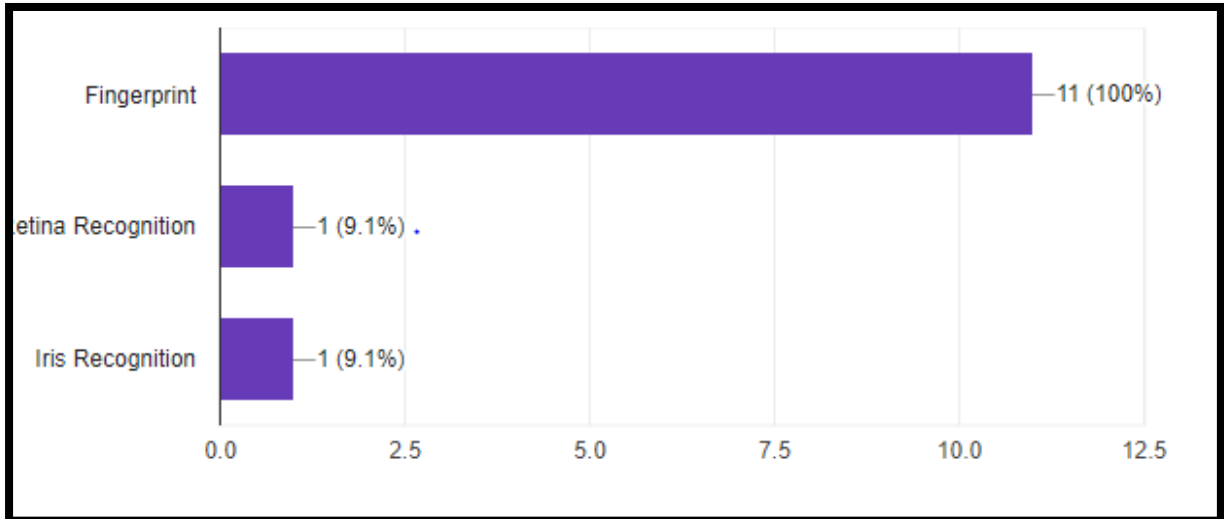


Fig.1 Biometric security device used by an employee

We have also asked the employee which of the above identifier /biometric device the organization he/she works uses.

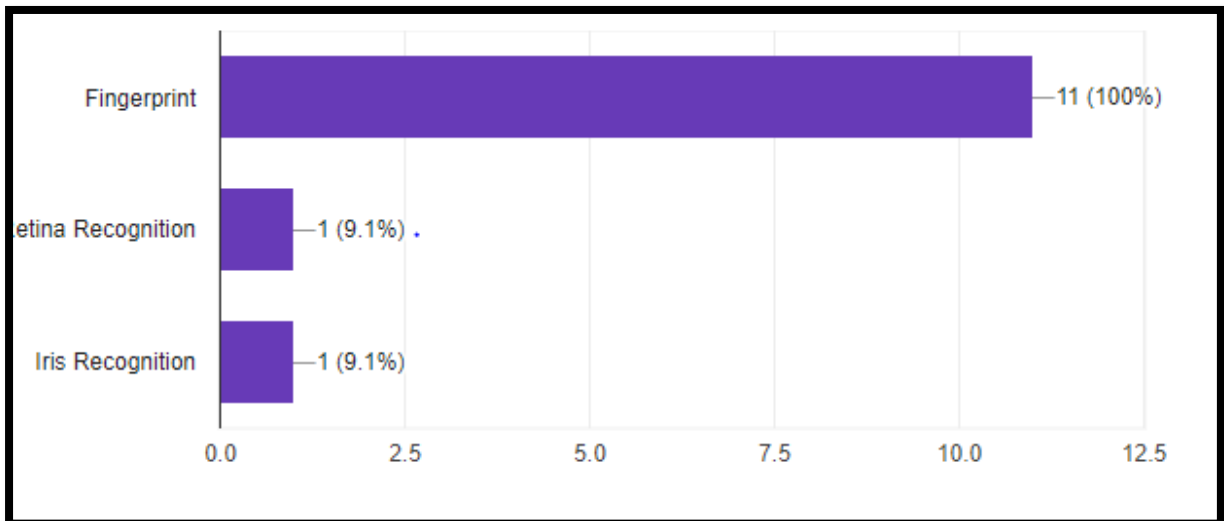


Fig.2 Biometric security device used by Organization

From figure 1 and 2 we can see all the employee who has filled the survey form as well as an organization where that employee work uses the fingerprint and there are 9.1 % uses Retina Recognition,

Similarly, Iris Recognition is used by 9.1%.

The below graph represents the use of biometric security to secure the data

- a) Yes
- b) No
- c) Maybe

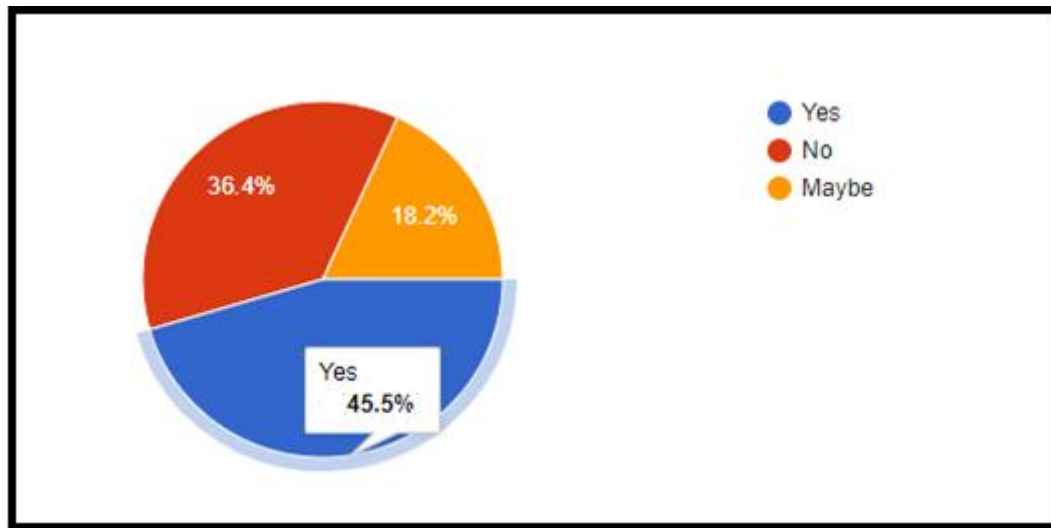


Fig.3 Biometric security to secure data

From the above graph, we can see that there are 45.5% of employee's organization who have filled this survey form uses the biometric security to secure the data and 36.4% of organization does not used biometric security to secure data, and left 18.2% employee don't know about it.

From the following graph, we can see there a large number of organizations that use biometric security for entry in the organization. Here 81.8% of employee's organization used biometric security device for entry and 18.2% employee's organization does not use biometric device for entry.

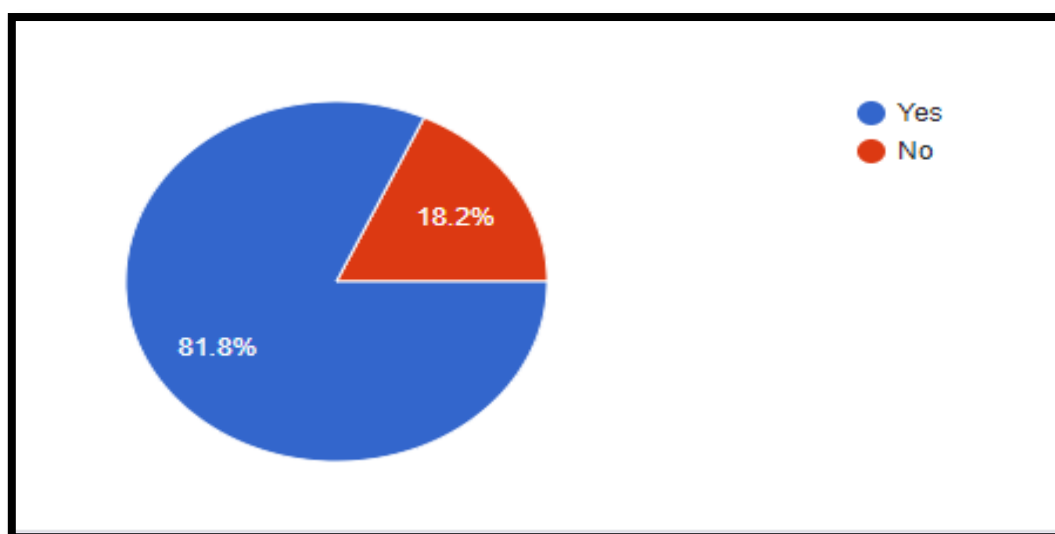


Fig.4 Biometric security device used for entry in organization.

In the survey, we have also asked employees to whether they find biometric security is an easy way of authentication

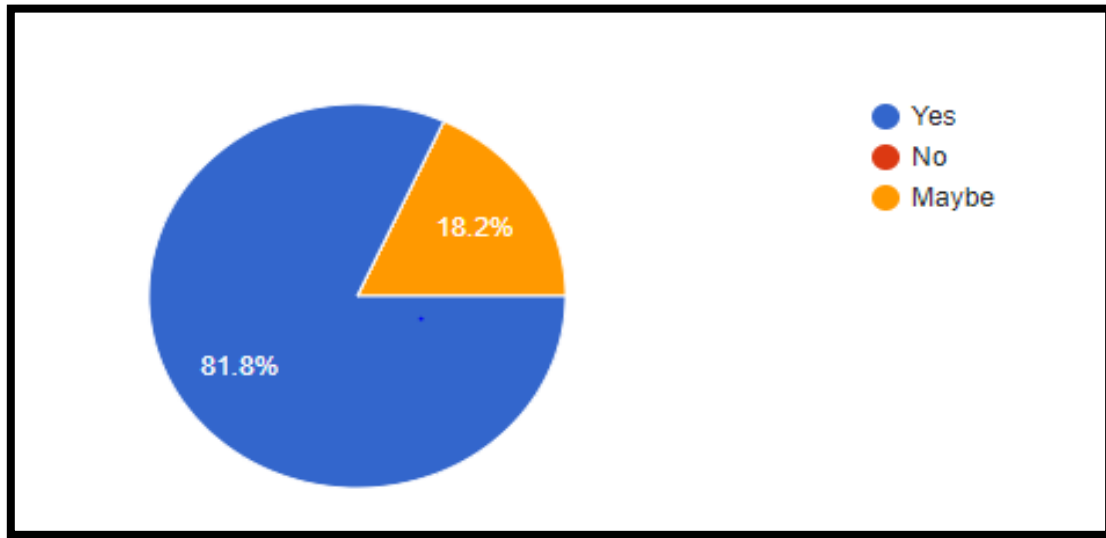


Fig.5 Biometric security device easy way of authentication

Many of the employees 81.8% of all the employees how have filled this survey form find biometric security as an easy way of authentication. Where on the other hand 18.2% employee think that biometric security is not an easy ay of authentication.

We have marked survey on a scale of 1 to 10 based on according to them, how secure is biometric authentication.

Here, 1 represent very less secure and 10 represent highly secure

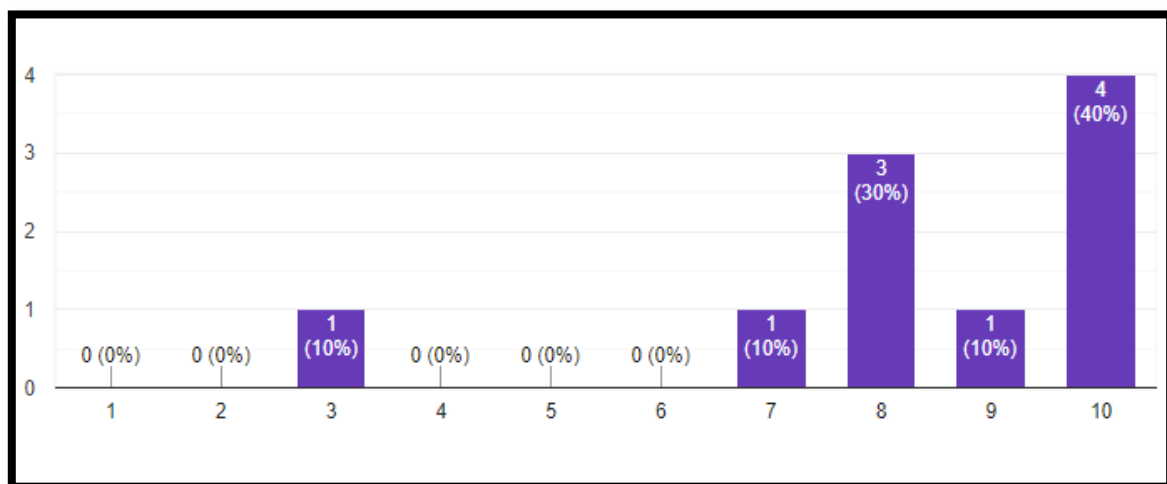


Fig.6 How secure is Biometric authentication

From above graph we can analyse that most of the employee think that biometric authentication is highly secure ay of authentication.

3. FUTURE ENHANCEMENT

In this research, we have discussed about biometric security in organization. As Biometric innovation is improving, and availability is growing over the globe, all through creating countries just as set up business sectors, In the future, we're going to see new chances and concerns proliferate. Be that as it may, regardless, the development of biometrics doesn't appear to back off at any point soon.

4. CONCLUSION

Biometric security provides more authentication, privacy or data discretion, authorization or access control, data veracity, and non-repudiation.

REFERENCES

- [1]. *Biometrics: Concepts and Applications* by Dr. G. R. Sinha
- [2]. *Information Systems Security and Privacy* by Christophe Bidan and Olivier Camp
- [3]. *Information System Security* by R Sekar Anand Arun K Pujari