DEFINE PROBLEM/PROBLEM UNDERSTANDING

SPECIFY THE BUSINESS PROBLEM

TEAM ID	NM2023TMID04400
PROJECT NAME	BIOMETRIC SECURITY SYSTEM FOR VOTING PLATFORM

Problems with biometric security systems:

Biometric systems can make two basic errors. A “false positive” occurs when the system incorrectly matches an input to a non-matching template, while in a “false negative”, the system fails to detect a match between an input and a matching template.

.

Businesses using biometrics for authentication:

By withholding biometric data such as fingerprints, facial features, iris patterns, or even voice recognition, companies can establish an advanced

and highly secure system that offers numerous benefits over conventional access control methods**.**

Biometric technology can be used to help businesses:

Trust-based services like dating apps are increasingly using biometrics as a competitive advantage; ensuring users match their profiles with other verified users gives them more confidence in who they are meeting and reduces fraud. In this way, businesses can use the technology to offer trust and safety.

The benefits of biometric devices:

- They are linked to a single individual (unlike a password, which can be used without authorisation),
- They are very convenient since there is no need to remember or carry anything,
- The security, they are highly fraud resistant.

The varieties of biometrics:

There are two broad varieties of biometrics. They work similarly in that a database of authenticated characteristics is stored on the system, and anyone seeking access has an attribute checked against that database.

1. **Physical biometrics:**

   These tend to be what most people think of as biometrics. Popular types include fingerprints, facial recognition, and iris or retina scans, as well as DNA, blood type, and heartbeat rate.

2. **Behavioural biometrics**

   This is more about the way an individual performs a process. So, it could be all about voice recognition, their gait, their signature, or their characteristic keystroke pattern. It could also include buying habits, IP addresses, or cookies. Say, for example, in hosted call centers, voice biometrics could be stored and then used to identify customers and bring up their details for the agent.

Advantages of biometrics:

So, there has to be a reason why the use of biometric access and authentication is becoming more widespread. There are, in fact, lots of reasons.

1. **Good security**

   The fundamental requirement of a property protection system is that it gives good security, and this is true of biometrics. Whereas passwords and PINs are eminently stealable by hackers, biometric information is unique to the person concerned and cannot be accessed and used illegitimately.

2. **User experience**

   This is such a benefit it almost makes you want to sing out loud with joy. The onus of having a different password for every device and every system you need to access makes life miserable for many. No wonder “123456” is the most popular password right now. It’s almost like some of us have pretty much given up.

3. **Non-transferable**

   Unless you’re in the habit of giving other people various of your body parts, it’s unlikely that someone else will have your

particular biometric characteristics. The characteristics we possess are ours and ours alone.

4. Imitation-proof

So, those characteristics are unique to an individual, which means, in turn, that it's all but impossible to synthesise them. Of course, the rapid development of technology means that you can never say never, but, at present, at least, a robot can't fake your DNA.

5. Time and attendance

A lot of biometric access systems include reasonably sophisticated time and attendance features, making it easy to track work patterns and entry activity, both in terms of the whole team and for specific individuals.

Disadvantages to using biometrics:

Well, there's no such thing as a perfect system. These are the most commonly cited problems with biometric methods.

Initial cost

The kit that an organisation needs to invest in can be extensive. It will include readers—biometric terminal hardware that contains the optical sensor device or other information gatherers.

Entire system failures

When biometric access control systems fail, no access can occur, and huge costs can result.