Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 05, May-2025

Are Biometrics Truly Better?

Arnav Jha
Independent Researcher, Student at the Georgia Institute of Technology

Abstract
Biometric authentication systems offer a convenient and increasingly affordable alternative to traditional passwords and PINs. This paper evaluates whether modern biometrics (specifically fingerprint and facial recognition) are truly better than conventional methods in terms of user convenience, accuracy, and cost-efficiency. We review the historical development of biometric technologies and analyze experimental data on their accuracy and implementation costs, comparing these to the security and practical effectiveness of passwords, PINs, and pattern locks on personal devices. Our findings indicate that fingerprint and facial recognition generally provide higher authentication accuracy than traditional credentials, and when factoring cost, they deliver equal or better "bang for the buck." However, biometric methods are not foolproof and typically rely on fallbacks to conventional methods. We conclude that while biometrics represent a superior option for most users—especially given the prevalence of weak passwords and PINs—a combination of biometric and traditional authentication provides the most robust security in practice.

Keywords: **biometrics, fingerprint recognition, facial recognition, passwords, PIN, authentication, cybersecurity, accuracy, cost-efficiency**

INTRODUCTION

Biometrics is a fast-expanding sector of digital security. Biometric technologies—automated systems for identifying people based on biological and behavioral traits—are becoming easier to use and cheaper every day [1][2]. This study examines how "good" these systems are at present by comparing the working processes, accuracy levels, and costs of the most common biometric systems (specifically fingerprint and face recognition) with those of conventional software-based security methods (passwords, PINs, and pattern locks). Data from a variety of sources and tests are utilized to evaluate authentication accuracy and implementation costs. We then construct an accuracy-per-cost index to estimate each system's cost efficiency—the proverbial "bang for the buck." Our scope is limited to personal consumer devices, recognizing that each manufacturer may implement these technologies differently and that actual performance can vary [3]. Moreover, because we draw on experimental data spanning several years, technological progress may cause some reported figures to shift over time [4]. The following sections provide an overview of biometric systems, describe two leading biometric modalities (fingerprint and facial recognition) in detail, review traditional knowledge-based authentication methods, and then present a comparative analysis of their relative effectiveness.

BIOMETRIC SYSTEMS

The term biometrics is derived from the Greek words bios (life) and metron (measure) [5]. The concept of using physical characteristics for identification is ancient: fingerprints were reportedly used on clay tablets in Babylon as early as 500 BC [6]. However, formal biometric identification systems emerged much later. In 1879, French criminologist Alphonse Bertillon introduced a system of body measurements (Bertillonage) to identify criminals, marking the first modern biometric identification method [7]. Throughout the 20th century, biometric technology advanced rapidly. By the 1960s, researchers like Woodrow ("Woody") Bledsoe were experimenting with semi-automated facial recognition under U.S. government contracts [8]. In 1969, fingerprint identification had gained such traction in law enforcement that the U.S. Federal Bureau of Investigation (FBI) began funding projects to automate the process [9]. The FBI commissioned the National Institute of Standards and Technology (NIST) to develop automated fingerprint matching, identifying challenges like scanning inked prints and matching minutiae [10]. By the 1980s, voice recognition joined the biometrics field when NIST established a Speech Group to advance speech recognition techniques [11]. Researchers proposed in 1985 that iris patterns are unique to each individual, leading to the first iris-recognition algorithm patent in 1994 [12]. A major breakthrough in 1991 was the development of real-time facial detection algorithms, which paved the way for modern face recognition technology [13].

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 05, May-2025

Biometric authentication has since evolved from a novel technology to a routine part of daily life. By the early 2000s, biometrics were not confined to government labs or corporate security—hundreds of biometric algorithms had been developed, and biometric tools appeared in consumer applications and even large public events [14]. A famous example was the "Facecam" system deployed to scan attendees at Super Bowl XXXV in 2001 [14]. In 2013, Apple's introduction of the Touch ID fingerprint scanner on the iPhone 5s brought biometric security firmly into the mainstream, signaling widespread public acceptance of using one's fingerprint to unlock personal devices [15]. By the late 2010s, facial recognition was also commonly available on smartphones, tablets, and laptops [16][15].

NEED FOR BIOMETRICS

Biometric authentication offers several advantages over traditional passwords or tokens. It provides high security and assurance by verifying who the user is based on a physical trait, rather than what the user knows or possesses [17]. This dual nature – something the user has (a body part or pattern) and is (a unique biometric identity) – makes it extremely difficult for an impostor to bypass. Unlike a password or PIN, a fingerprint or face cannot be simply shared, guessed, or left written on a sticky note. In fact, most users' passwords and PINs have likely been exposed in data breaches over the years [18]. Adding biometric authentication creates an additional roadblock for fraudsters, because even if a criminal knows someone's personal information or login credentials, they still cannot unlock an account without the person's live biometric on the spot [19]. For example, a hacker might obtain your pet's name and birthdate (common password ingredients), but they cannot replicate your fingerprint to unlock your phone without physically having your finger [19]. Furthermore, biometric input requires a live person. Today's systems include liveness detection safeguards – a robot or a high-quality photo would struggle to pass an iris or face scan under current technology [20].

Equally important is the user convenience of biometrics. The authentication process is typically extremely simple and swift for the end-user [21][22]. Placing a finger on a scanner or allowing a camera to scan your face takes only seconds, much faster than typing a complex password. There is nothing for the user to remember or carry, eliminating the common problem of forgotten passwords [22]. A biometric trait also cannot be lost or misplaced like an identification card. And while biometric data could in theory be stolen (if a database of biometric templates were compromised), one cannot easily change their fingerprints or face in the way a password can be reset—meaning such data is of limited use to attackers if proper anti-spoofing is in place. Modern biometric systems are nearly impossible to deceive with current technology. For instance, the probability that one person's fingerprint will exactly match another's is estimated at only about 1 in 64 billion [23][24]. In summary, these factors—along with the high accuracy rates discussed below—make biometric authentication an appealing and powerful security option for personal devices.

FINGERPRINT RECOGNITION

Fingerprint recognition is the most widely utilized biometric modality on consumer devices. By some industry estimates, fingerprint scanners account for roughly one-third of all biometric systems used in smartphones and similar personal devices [25][26]. The idea of using fingerprints for identification is not new: methods for using handprints to track workers in farms and factories were being explored in the late 1800s [27]. Truly effective automated fingerprint systems, however, only began to appear in the latter part of the 20th century with the advent of modern computing [28]. The field accelerated in the 1990s and fingerprints started to be integrated into everyday applications by the early 2000s [29]. One notable milestone came in 1969, when the FBI—overwhelmed by manual fingerprint filing—pushed to automate its identification process [9]. This led to decades of research, including the development of the first computerized fingerprint scanners and matching algorithms. A U.S. patent for automated hand identification was issued in 1985 [30], and biometric hand geometry scanners were even employed during the 1996 Olympics for participant identity verification [31]. By the late 2010s, fingerprint scanners had undergone exponential growth in adoption, becoming ubiquitous in personal electronics from smartphones to USB authentication devices [26].

Modern fingerprint recognition systems fall into three primary categories based on their sensing technology: optical, capacitive, and ultrasonic scanners [32][33]. Each type uses a different method to capture the unique pattern of ridges and valleys on a person's fingertip, as described below.

OPTICAL FINGERPRINT SENSORS

Optical scanners are the oldest and once the most prevalent fingerprint sensors. As the name implies, an optical fingerprint scanner functions by taking a detailed image of the finger's surface using light [34]. The scanner typically consists of a light source (often an LED), a prism or focusing lens, and an image sensor (a light-sensitive microchip similar to a camera sensor) [34]. When a finger is placed on the scanner, a bright light flashes over the fingerprint. The sensor captures the reflected light to produce a high-contrast digital image of the fingerprint's

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 05, May-2025

pattern [34]. The ridges (raised lines) of the fingerprint appear dark in the image, while the valleys (recessed areas) appear lighter. The scanning software then analyzes the image, converting the pattern of ridges and valleys into a binary code of 1s and 0s that constitutes the user's unique fingerprint template [34]. Essentially, the optical sensor translates the visual pattern into a numerical representation used for matching. Figure 1 illustrates how the light source reads the fingerprint and where that information is transmitted in a typical optical scanner [35].

Optical fingerprint technology is reliable and inexpensive, but it has a few drawbacks. The most notable (though still highly unlikely in practice) is that a digital image can theoretically be replicated or spoofed. In other words, a high-quality photograph of a fingerprint could be used to fool a simple optical scanner, assuming the system lacks advanced liveness detection [36]. Smudges or debris on the scanner surface can also interfere with image quality. For these reasons, optical sensors in newer devices are often coupled with anti-spoofing measures or have been supplanted by other sensor types. Nonetheless, optical scanners remain in use (particularly in some under-display fingerprint readers for smartphones) due to their lower cost and straightforward design.

CAPACITIVE FINGERPRINT SENSORS

Capacitive fingerprint scanners are now one of the most common types found on smartphones and laptops [37]. Instead of capturing an optical image, capacitive sensors leverage the electrical properties of the human skin. They operate on principles similar to a touchscreen: using an array of tiny capacitors and measuring changes in electric charge caused by the ridges of a fingerprint. When you place your finger on a capacitive sensor, each ridge that touches a conductive plate in the sensor alters the charge stored in the corresponding tiny capacitor, whereas air gaps in the valleys leave the charge unchanged [38]. The scanner contains dozens or hundreds of these capacitors arranged in a grid, each acting like a pixel that records the presence or absence of a ridge at that location. An integrated circuit (including an operational amplifier and analog-to-digital converter) monitors the charge changes across the array and converts these analog signals into a digital fingerprint image [38]. The result is a detailed map of the fingerprint pattern, derived from electrical signals rather than light.

Capacitive fingerprint sensors produce highly accurate data and are much harder to fool than optical scanners. Because they sense the three-dimensional shape of the skin's surface via electrical contact, simply overlaying a 2D printed image of a fingerprint will not produce the correct charge pattern [39]. Materials that are not electrically similar to human skin (such as paper or a photograph) won't generate the same response as a real finger. This makes capacitive systems far more resistant to spoofing attempts; an imposter would need a life-like prosthetic or dummy finger with similar conductive properties to have any chance of success. The trade-off is that capacitive sensors can be more expensive and complex to manufacture than optical ones [39]. Nonetheless, their superior security and the falling cost of electronics have made them the de facto standard in smartphones for many years. Figure 2 shows the mechanism of a typical capacitive fingerprint scanner, including how the ridges and valleys affect the stored charges [38][40].

ULTRASONIC FINGERPRINT SENSORS

Ultrasonic fingerprint scanners represent the latest advancement in fingerprint sensing and are generally considered the most sophisticated and secure type. These sensors use high-frequency sound waves to map the fingerprint's details in three dimensions [41][42]. An ultrasonic scanner contains a tiny ultrasonic transmitter and a receiver beneath the sensing surface. When a finger is placed on the sensor, the transmitter emits an ultrasonic pulse (sound waves typically in the MHz range, well above human hearing) toward the finger's surface [43]. As the ultrasonic pulse encounters the fingerprint's ridges and valleys – essentially an "uneven surface" – it gets partially reflected back to the receiver. The ridges, which directly contact the sensor, reflect the sound strongly, while the valleys, which are slightly farther away and often air-separated, tend to absorb or dissipate the sound [44]. By measuring the time it takes for the echoes to return and their intensity at various points, the system constructs a detailed 3D map of the fingerprint. This map includes depth information that 2D optical or capacitive images lack [45][46]. To authenticate, the scanner compares this 3D fingerprint data to the stored 3D reference data captured during enrollment.

Ultrasonic fingerprint technology is significantly harder to deceive than either optical or capacitive methods [47][48]. Because it effectively creates a three-dimensional representation of the fingerprint's surface and sub-surface features, a simple printed image or even a basic mold of a finger is unlikely to fool the system. Only an identical twin (in the case of fingerprints this is essentially impossible) or an extremely well-crafted prosthetic finger with the exact 3D characteristics of the victim's fingerprint could consistently trick an ultrasonic sensor [48]. This makes ultrasonic scanners the most robust against spoofing among the three technologies. Another advantage is that ultrasonic sensors can operate through other materials; they are often placed under smartphone displays or behind glass without issue, because the sound waves can penetrate these solid layers. This allows for convenient in-screen fingerprint readers on modern phones, maintaining a sleek design without a dedicated sensor pad.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 05, May-2025

The primary drawback of ultrasonic scanners is that the mechanical scanning process can be slightly slower than the nearly instantaneous optical or capacitive reads [42]. Early generations of ultrasonic readers had a noticeable lag (a fraction of a second) compared to other types. However, ongoing improvements – such as Qualcomm's 3D Sonic Sensor second-generation technology – have significantly increased speed and accuracy, making the difference negligible in practice [49]. Ultrasonic modules are also typically more expensive to produce, contributing to their inclusion mainly in higher-end devices. As of the early 2020s, only a number of premium Android smartphones (and no Apple devices, which use capacitive Touch ID or optical Face ID instead) feature ultrasonic fingerprint readers [50][51]. Despite these considerations, the enhanced security of ultrasonic scanners (which can even detect blood flow or fingerprint liveness in some implementations) is highly valued, especially for sensitive applications like mobile payments [52][53].

ACCURACY OF FINGERPRINT RECOGNITION

Fingerprint recognition is widely regarded as a highly accurate authentication method. A comprehensive 2004 study by NIST evaluated 34 commercially available fingerprint-matching systems on a dataset of 48,105 fingers (from 25,309 individuals), totaling 393,370 fingerprint images [54]. The results showed that the top-performing algorithms were extremely accurate: the best systems correctly matched single fingerprints 98.6% of the time, and when using two fingerprints from the same person, accuracy rose to 99.6% [55]. Using four fingerprints (e.g., four-finger slap impressions) yielded 99.9% accuracy [55]. These performance figures were achieved at a very low false-positive rate of 0.01% (i.e., only 1 in 10,000 non-matching attempts was incorrectly accepted) [56]. In practical terms, for personal devices which typically authenticate with one finger, we can reasonably assume around 98–99% accuracy in matching, under ideal conditions, for modern high-quality fingerprint scanners [55]. Real-world accuracy may be slightly lower if the finger is placed at an angle, dirty, or if the sensor is small, but modern smartphones still report unlock success rates well above 95% in normal use.

It should be noted that false negatives (the system failing to recognize a legitimate enrolled fingerprint) can occur occasionally – requiring the user to adjust their finger position or try again. However, false positives (an unauthorized person being recognized as the owner) are exceedingly rare with a properly configured system [55]. Performance can also vary by algorithm; for instance, systems by certain vendors (NEC, Cogent, Sagem in the NIST study) performed better than others [55]. Overall, fingerprint biometrics have proven to be highly reliable for personal authentication, which explains their ubiquity in security applications ranging from phone unlocking to border control. Even aging or worn fingerprints can usually be enrolled and matched successfully with today's sensitive scanners, though individuals with certain conditions (e.g., very dry skin or scars) might need multiple fingers enrolled for consistency.

COST OF FINGERPRINT RECOGNITION

Implementing fingerprint recognition in consumer devices entails both hardware and software components, but the cost per device has become relatively modest. Standalone fingerprint sensor modules for personal devices can range roughly from $30 up to $130, based on their sophistication and economies of scale (with simpler optical sensors at the lower end and advanced ultrasonic modules at the higher end) [57]. In smartphones and laptops, however, the fingerprint sensor is just one part of the overall device. Most mid-range devices that include a "reasonably usable" fingerprint scanner are priced in the range of about $70–$110 of manufacturing cost for that component and its integration, according to online listings and tear-down analyses [58]. For the purposes of comparison, we use an average hardware cost of $90 for a fingerprint authentication feature in a device.

Software implementation costs (the algorithm and firmware for fingerprint processing) are relatively minor on a per-device basis. While developing a reliable fingerprint matching algorithm and secure enclave might involve significant up-front R&D expense, those costs are amortized over millions of devices. In other words, the incremental cost of including fingerprint authentication in a device is mainly the sensor itself, as the software comes bundled in the device's OS or firmware. Therefore, one can reasonably treat the per-device cost of fingerprint security as approximately $90 in hardware (with software costs negligible per unit once developed) [59]. This cost estimate will be used later when we compare cost-effectiveness across different security methods.

FACIAL RECOGNITION

Facial recognition is the second most used type of biometric technology in personal devices, after fingerprinting. First conceived in the 1960s, face recognition technology has a long research history. One of the earliest known efforts was by Woodrow W. Bledsoe, who in the mid-60s developed a semi-automated system to identify faces in photographs by locating features like the eyes, nose, and mouth and measuring their distances—work done under a U.S. government contract [60]. These pioneering methods relied on manually plotted facial feature coordinates and were limited by the lack of computing power; in fact, face recognition remained a largely manual

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 05, May-2025

or semi-automated process until the 1990s. It wasn't until researchers applied linear algebra techniques (such as principal component analysis) and statistical error analysis in the 1990s that fully automated face recognition began to achieve usable accuracy [61]. For example, the well-known "eigenfaces" algorithm (Turk & Pentland, 1991) demonstrated that the residual error when representing an image with a set of basis faces could be used to recognize individuals, dramatically improving automation.

Recognizing the potential of face recognition, the U.S. Defense Advanced Research Projects Agency (DARPA) and the Department of Defense funded the Face Recognition Technology (FERET) program from 1993 to 1997. The FERET program supported the development and evaluation of face recognition algorithms, creating a standardized database of facial images for researchers [62]. This helped transition face recognition from an academic prototype to a commercial product. Subsequently, the first Face Recognition Vendor Test (FRVT 2000) was conducted in 2000 to benchmark the performance of different algorithms on a large scale [62]. By 2001, facial recognition had its first high-profile public trial during Super Bowl XXXV in Tampa, where surveillance cameras attempted to match attendees' faces against a database of known criminals [63]. Although that particular deployment had limited success and raised privacy concerns, it signaled that facial recognition had moved out of the lab. By the late 2010s, facial recognition became common in consumer devices; for instance, Apple introduced Face ID (a sophisticated 3D facial recognition system) on the iPhone X in 2017, and many Android manufacturers offer face unlock features for phones and laptops [63].

MECHANISM AND WORKING OF FACE RECOGNITION

Face recognition is the process of identifying or verifying a person by analyzing the characteristics of their face. In a typical face recognition system, an image or video frame of a person's face is captured and then compared to a database of stored face data (such as face templates for authorized users) to find a match [64]. Several factors can influence the performance of face recognition, including the person's pose (orientation of the face), facial expression, lighting conditions, occlusion (whether part of the face is covered, e.g. by glasses or masks), and image quality [64]. Over the years, face recognition algorithms have evolved from relying on simple geometric relationships (distances between key facial features) to using sophisticated machine learning models that analyze the face holistically or via learned features.

There are broadly two classes of face recognition algorithms: feature-based (analytic) and holistic. Early systems including Bledsoe's were feature-based – they measured distinctive features like the width of the nose, the distance between the eyes, the angle of the jawline, height of cheekbones, etc., to create a unique numerical code for the face [65]. This code (sometimes called a faceprint) would then be compared against reference codes in the database to determine the closest match [66]. Modern approaches often use holistic methods such as deep learning: the entire face image is processed by a neural network that outputs a high-dimensional feature vector uniquely representing the face. Either way, the face image undergoes several standard processing steps: face detection (to locate the face in the scene), feature extraction (to measure or compute salient features from the face), and finally face matching/recognition (to compare these features to the known entries) [67].

Most smartphones today implement one of two types of device-based face authentication: a basic 2D facial recognition using a single camera, or a more advanced 3D facial recognition using specialized sensors. The following sections describe each in turn.

TWO-DIMENSIONAL FACIAL RECOGNITION

In 2D facial recognition (such as the "Face Unlock" found on many phones and laptops without dedicated depth sensors), the system relies on one or more cameras to capture a flat image of the user's face, often with infrared illumination to improve performance in low light [68]. A typical 2D face unlock setup on a device consists of the front-facing camera and perhaps an infrared emitter or filter, but notably does not include a dot projector for depth mapping (which is the key differentiator from 3D systems) [68]. During enrollment, the user's face is captured in a controlled pose and lighting, and important features of that 2D image are stored as the reference template [69]. On each unlock attempt, the camera takes a new image of the face and the software compares the facial features (or the overall face vector) to the saved template. If the new image is sufficiently similar to the stored one, access is granted [70].

Manufacturers often improve 2D face unlock reliability by using infrared (IR) light. In low-light or dark conditions, an IR illuminator will project invisible light onto the user's face, and an IR-sensitive camera can then "see" the face clearly even without visible light [71]. This allows face recognition to work at night or in dim environments. The IR approach also helps in regular conditions by ignoring the colors and focusing on the structure of the face, which can improve consistency across different lighting. However, because 2D systems only analyze the face as a flat image, they are inherently less secure than 3D systems. A 2D face unlock may be fooled by a photograph or video of the authorized person, since a photo can look identical to the real face from the camera's perspective [48]. Some advanced 2D systems attempt to detect liveliness by requiring a blink or a head movement, but these measures are not foolproof. Additionally, there is a risk of false acceptance if someone looks

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 05, May-2025

very similar to the owner (e.g. a sibling) – though this is still uncommon, as even identical twins can sometimes fool 2D systems whereas 3D might discern them.

The accuracy of 2D facial recognition can vary widely depending on the algorithm and conditions. Many research studies have evaluated different 2D face recognition methods over the years. Table 1 provides a sampling of accuracy results reported in various studies from 1993–2005 for 2D face recognition algorithms (as compiled by Abate et al., 2007). Reported accuracies in those studies range from as low as ~65–70% in difficult conditions up to ~100% in favorable scenarios [72][73]. For example, methods by Turk & Pentland (1991, not listed in the excerpt) and Belhumeur et al. (1997) achieved over 99% on certain datasets [73], whereas others dealing with more variation (Adini et al., 1997; Martinez, 2002) saw around 70–81% [72][74]. Modern deep learning-based 2D face recognition (post-2012) can reach very high accuracy (over 97-99% on standardized benchmarks) under good conditions, but in uncontrolled settings with occlusion or lighting issues, performance drops. Overall, a reasonable median accuracy for 2D face recognition algorithms is around 95% as reported in surveys [72][75]. It must be emphasized that this is under the assumption that the user's face is presented more or less as during enrollment (frontal view, no heavy occlusions). Extreme changes in lighting or appearance (hats, sunglasses) can degrade accuracy significantly.

THREE-DIMENSIONAL FACIAL RECOGNITION

Three-dimensional facial recognition uses depth sensing to overcome the weaknesses of 2D methods. A 3D face unlock system uses a combination of a traditional camera and depth sensors (often an infrared dot projector and an IR camera) to create a detailed 3D depth map of the user's face [76]. A prominent example is Apple's Face ID, which projects around 30,000 infrared dots in a known pattern onto the face and uses an IR camera to read the distortion of this dot matrix to infer depth at each point [77]. The result is a high-resolution 3D model of the face's contours (essentially a cloud of points or a mesh) that serves as the stored reference [78]. The more points of data captured, the more precise and secure the system tends to be [79]. When the user attempts to unlock the device, the system projects the infrared dot matrix again and captures the new depth map, then compares it to the stored reference map. If the 3D patterns match within an acceptable tolerance, the device unlocks [80].

Three-dimensional recognition greatly increases security because it is much more difficult to falsify the required input. A regular 2D photograph will not contain the correct depth information to match the stored 3D profile. Likewise, an unrelated person who merely resembles the user will not match the precise 3D shape of the user's face. The only known methods to consistently fool a well-implemented 3D face recognition system are to either use an identical twin of the enrolled user or to create an extremely accurate 3D prosthetic mask of the user's face [81]. Both scenarios are either uncontrollable (twins) or highly impractical for an attacker. Therefore, 3D face unlock is considered the most secure form of facial authentication, to the point that it is recommended for high-security applications like online payment authorization [52][53]. In fact, many banking and payment apps will only trust device face authentication if it's a 3D system (e.g., Face ID) and not a basic 2D camera-based system.

The trade-offs for 3D face recognition are hardware cost and, sometimes, speed. Devices with 3D face sensors (dot projectors, IR cameras, flood illuminators) typically cost more, and thus this feature is found mostly in higher-end phones and tablets [82]. The specialized hardware also consumes space in the device (hence the "notch" on phones like the iPhone). As for speed, earlier 3D systems had a minor delay as they projected the dots and read the pattern, but current generation ones are very fast. If anything, 3D face systems can be faster for users in daily use because they work in the dark and at various angles more reliably than 2D systems, reducing the need for multiple attempts.

Accuracy of 3D face recognition is generally excellent. Various studies in the early 2000s (when 3D face recognition was nascent) reported recognition rates often above 95% or 98% for 3D models [83]. For instance, algorithms by Chua et al. (2000), Gordon (1991), and others achieved 98–100% on their test sets [83]. Even accounting for more challenging conditions, a 2018 survey found the median accuracy across numerous 3D face recognition experiments to be about 96.6% [83][84], slightly higher than for 2D methods. In practice, a well-made 3D system like Face ID has a very low false reject rate (it almost always recognizes its owner correctly) and an extremely low false accept rate – Apple claimed Face ID's probability of a random person unlocking your phone was on the order of 1 in 1,000,000 (except in the case of a twin). These figures underscore that, accuracy-wise, 3D face recognition rivals fingerprint technology for personal device authentication.

COST OF FACIAL RECOGNITION

The cost of implementing facial recognition on a device can be higher than that for fingerprints due to the additional sensors involved. A complete hardware suite for face recognition can range from relatively inexpensive cameras to specialized IR + dot projector setups costing up to several hundred dollars. For example, a basic webcam-style face unlock (2D) might only add on the order of $80 or so in components, whereas the advanced Face ID module in an iPhone (which includes an IR camera, dot projector, and flood illuminator) has been estimated to cost in the $300–$400 range in early iterations [85]. Standalone commercial facial recognition

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 05, May-2025

systems (e.g., for door access) can cost even more, up to $1000 or beyond for high-end units with multiple cameras and processors [85].

However, much like fingerprint tech, the software development cost can be spread across many devices. A company might invest tens of thousands of dollars (the figure of $30,000 is sometimes cited) to develop robust face recognition software [86], but that software then runs on millions of phones, making the per-device software cost negligible. The primary per-unit cost is the hardware.

In consumer electronics, most devices that include a high-quality facial scanning system (especially 3D) are on the higher end of the price spectrum – typically devices retailing for $500 and up. But if we attribute an isolated value to the biometric component, industry analysis suggests such devices have about $100–$170 worth of face recognition-related hardware built in (again, lower end for a basic camera setup, higher for 3D) [86]. Taking the midpoint, we use $130 as an approximate cost for including facial recognition capability per device. This reflects something like an infrared camera + dot projector module in a smartphone. It's worth noting that as technology progresses, these costs tend to decrease; for instance, a newer phone might integrate these sensors more cheaply than the first generations did. But for our comparative purposes, $130 per device is a reasonable average for facial recognition hardware.

Lastly, the power and processing overhead of face recognition (especially 3D) is non-trivial; the device needs a secure enclave or processor to perform the face matching encryption and to store face data securely. This is implicitly counted in the device's cost. As with fingerprints, the security software is part of the platform's operating system and doesn't add a direct cost per device beyond initial development.

TRADITIONAL FORMS OF SECURITY

Before biometrics became feasible for everyday use, the primary methods of securing devices and accounts were knowledge-based (passwords, passphrases, PINs) or pattern-based (unlock patterns). These methods are essentially secrets that the user knows or codes the user remembers, in contrast to biometrics which are tied to the user's physical being. Traditional credentials have existed for millennia in one form or another. In fact, the concept of a password (a secret word or phrase to prove identity) is ancient – Roman soldiers used daily changing "watchwords" to distinguish friend from foe in military camps [87][88]. This practice underscores that even in antiquity, controlling access through shared secret knowledge was understood to be crucial for security. Fast-forward to the 20th century: the modern computer password was introduced by Fernando Corbató at MIT in 1960, when he implemented password protection for individual user files on the CTSS time-sharing system [87]. Corbató is often dubbed the "godfather of the computer password" for this contribution [89]. As multiple users shared a single mainframe computer, Corbató's idea was to assign each user a secret password so that each person could access only their own files during their allotted time [90]. This was the birth of digital password security.

Throughout the 1970s and 80s, as computing went mainstream, researchers worked to improve password security. A major development came from Bell Labs cryptographer Robert Morris Sr., who in the early 1970s devised the concept of hashing passwords [91]. Hashing is the process of transforming a password into a numerical code (a hash) such that the original password does not need to be stored – only the hash is stored for verification [92]. Morris implemented one of the first password hashing schemes for Unix systems (using a modified DES encryption) so that even if an attacker obtained the password file, they would not see actual passwords, only the hashed values [91]. This innovation dramatically improved the security of stored passwords and remains a cornerstone of password storage today (modern systems hash and salt passwords). By the 1990s, with the explosion of internet services, passwords had become the ubiquitous key to our digital lives. Even as new ideas like graphical passwords or two-factor authentication emerged, the traditional alphanumeric password persisted due to its simplicity and familiarity.

Today, virtually every personal computing device uses some form of password, PIN, or pattern as a fallback or primary lock. Smartphones, for example, require users to set a PIN, passcode, or pattern, which serves both as a direct unlock method and as a backup if a biometric fails. Below, we overview the most common traditional authentication methods: passwords, PINs, and pattern locks, along with their security properties.

PASSWORDS

A password is a secret string of characters (letters, numbers, and symbols) that a user memorizes and provides to gain access to a system. In an authentication context, passwords are considered a form of shared secret: the system stores (a hashed version of) the password, and the user's knowledge of the correct sequence serves as proof of identity [93]. Passwords remain the most widely used method of account authentication on everything from email and banking websites to local computer logins [94]. A strong password is typically one that is long and complex enough to resist guessing or brute-force attacks – often incorporating a mix of upper- and lower-case letters, digits, and special symbols. Despite the rise of biometrics and other methods, the username-password combination is still prevalent largely because it is simple to implement and works across all digital platforms.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 05, May-2025

It is worth noting that passwords, in the context of computing, were arguably the first form of digital encryption accessible to everyday users – not encryption of data, but of access. In the early days, protecting files with a password was a novel way to encrypt access permissions [95]. However, passwords have significant drawbacks: users often choose weak passwords, reuse the same password on multiple services, or fall for phishing attacks that reveal their password. The human element often undermines the theoretical security of passwords. Nonetheless, when used properly (i.e., strong, unique passwords kept secret), they provide a baseline level of security that has stood the test of time. They rely solely on software: a password check involves comparing an input string to a stored hash in a database. This means no additional hardware cost is needed, but it also means that if the software or database is compromised, the passwords can be stolen en masse (which has happened in countless breaches).

PINS

A PIN (Personal Identification Number) is essentially a numeric password, usually shorter in length (commonly 4 to 6 digits). At first glance, a PIN appears to be just a specific type of password (and indeed both are something a user must remember). However, PINs often serve slightly different purposes and contexts. Notably, PINs are typically associated with devices or local authentication. For example, you unlock your smartphone or decrypt your SIM card with a PIN, or you authenticate at an ATM using a PIN. In contrast, passwords are more often used for remote authentication to websites or accounts. One key distinction is local vs. remote authentication: PINs are usually verified locally on the device, whereas passwords are often transmitted to a server for verification [96]. This has security implications; for instance, a 4-digit PIN on a phone is not sent over networks and can be rate-limited (the phone can enforce a wipe after too many failures), whereas an online password might be subjected to large-scale guessing if the server isn't properly secured.

Because PINs are generally numeric and shorter, their theoretical entropy (randomness) is lower than a full password – a 4-digit PIN has 10,000 possibilities. However, devices compensate with strict retry limits (e.g., you usually only get a few tries before a phone delays input or locks out) so that guessing all 10,000 combinations is infeasible in practice. Moreover, PINs are device-dependent: you typically use a different PIN for each device (e.g., phone PIN, ATM PIN), which limits the damage of one being compromised. In contrast, a user might (inadvisedly) reuse the same password on multiple websites, causing one breach to affect many accounts. In everyday use, PINs offer a good balance of memorability and basic security for device unlock. Many people find a 4-6 digit PIN easier to remember and faster to input than a complex alphanumeric password on a small touchscreen.

In some cases, services have adopted PIN-like codes for account sign-in (for example, certain banking apps or customer service verifications will use a numeric PIN). But by and large, PINs are predominantly used for local authentication – you "unlock" something in your possession. This distinction means PINs and passwords often complement rather than directly compete with each other in terms of usage scenarios.

PATTERN LOCKS

A pattern lock is a graphical authentication method, popularized by Android smartphones, where the user draws a specific connecting pattern on a grid of dots (typically 3x3) to unlock the device. The pattern is essentially a shape created by tracing through the dots without lifting your finger, subject to certain rules (for example, you must use at least 4 dots, and you cannot use a dot twice unless a special setting allows overlaps) [97]. Pattern locks became a favored alternative to PINs for many users, as some find patterns easier to remember than arbitrary numbers. In fact, studies have shown that around 40% of Android users prefer and use pattern locks instead of PINs or text passwords on their device lock screen [98][99]. The appeal is often that a pattern can be a more intuitive memory cue (like a shape or letter), and input can be quicker – just a single continuous swipe.

However, pattern locks have notable security weaknesses. Human-chosen patterns tend to be predictable. Much like weak passwords ("123456", "password") are common, many people choose simple patterns (for instance, an L-shape or a letter shape). Moreover, patterns are highly vulnerable to shoulder surfing and smudge attacks. If someone watches you draw the pattern, even from a distance, they have a high chance of remembering it due to the visual nature. A 2017 joint study by U.S. and Chinese researchers quantified how easy patterns are to steal by observation: when participants watched someone draw an unlock pattern just once, they could reproduce it from memory 64% of the time; after multiple observations, this success rate jumped to 80% [100][101]. In comparison, observing a PIN being entered (with multiple digits) yielded a much lower success rate (the same study found only ~10% success for a 6-digit PIN after one viewing) [102]. This indicates that patterns, being graphical and perhaps more distinct to the eye, are significantly less secure against shoulder surfing. Another security issue is that the finger's path often leaves oily smudge trails on the screen. These smudges can sometimes be visible and reveal the pattern, especially if the phone's screen is observed at an angle under light.

Due to these vulnerabilities, the effective security of pattern locks is quite low. In terms of brute-force space, there are 389,112 possible patterns on a standard 3x3 grid meeting the minimum 4-dot rule [103]. But because of user choices and observational attacks, the real-world security is much weaker. One analysis concluded that an attacker

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 05, May-2025

who sees a pattern entered has roughly a 70–80% chance to get it, meaning only ~20-30% of patterns remain secure after such exposure [100]. Indeed, combining the shoulder-surfing stats above: if 64% can replicate after one viewing and 80% after more, one could say the pattern system only provided ~20-36% security in those scenarios. In other words, from the perspective of resisting an informed attacker, a pattern might only be ~30% as effective as hoped (hence the author's calculation of "net accuracy = 28%" for pattern locks, meaning roughly 72% of attempts to breach by observation succeed) [104].
It is recommended by security experts not to rely on pattern locks if stronger options are available [105][106]. Many Android phone manufacturers have themselves started nudging users towards PIN or biometric unlock by making pattern unlock a bit less prominent in setup. Nonetheless, the pattern lock's popularity with a segment of users means it will likely remain an option, albeit an insecure one.

SECURITY OF TRADITIONAL METHODS (ACCURACY AND VULNERABILITIES)

To evaluate the security effectiveness of traditional authentication methods, we consider how often they successfully keep attackers out (analogous to "accuracy" in biometric terms). Unlike biometrics, which have measurable false acceptance rates, traditional methods' "accuracy" is inversely related to how easily they are compromised by guessing, observation, or other attacks.

- Pattern Locks: As discussed, pattern locks are highly susceptible to being observed and copied. In controlled studies, attackers who saw a pattern entered could later unlock the device 64% of the time after a single observation, and up to 80% of the time after repeated observations [104][101]. This means the pattern system only prevented access in about 20-36% of those cases. Put differently, if an attacker has a chance to glance at someone unlocking their phone in public, there is a high probability the attacker can reproduce the pattern. If we define "security accuracy" as the chance that an unauthorized person cannot gain access, pattern locks might offer as low as ~28–36% effectiveness (the complement of the 64–80% success rates) in such scenarios. Even without direct observation, common patterns can be guessed by trying a few of the simplest shapes (e.g., the "N" or "Z" shape patterns many choose). Thus, pattern locks rate poorly in security – they rely on secrecy, which is easily compromised, and have no complexity requirements by default (users often choose the simplest allowed pattern). In our comparative analysis later, we will assign pattern locks a low effective security score (on the order of 25–30% "accuracy" in keeping attackers out, under realistic conditions).
- PINs: A PIN, if treated as a random 4-digit code, has a 1 in 10,000 chance of being guessed by a single random attempt (0.01% chance). However, targeted attacks benefit from the fact that humans often choose certain PINs more frequently (e.g., 1234, 1111, 1212 are famously overused). Aside from guessing, one major attack avenue is device sensor or side-channel leakage. For example, researchers developed a proof-of-concept called PINlogger.js that used a smartphone's motion and orientation sensors accessible via a malicious webpage to infer PINs as a user entered them. Shockingly, this method was able to guess a 4-digit PIN correctly on the first try 74% of the time, and with up to 94% accuracy by the third attempt by using machine learning on the sensor data [107][108]. These figures assume the PIN is from a set of 50 common PINs and the attacker can analyze the device's movement when you type – it's a very powerful attack scenario, though not one that average attackers can easily execute. Under normal conditions, a PIN's security comes from the system limiting the number of attempts. Most phones will introduce delays or even wipe themselves after a certain number of incorrect PIN entries (e.g., iPhones disable after 5-10 wrong tries). So brute forcing a 4-digit PIN on a locked phone is not practical without special tools, despite the low theoretical space. Therefore, for a casual attacker, the chance of breaking a PIN is low unless they see you entering it or you use a common one. But as the PINlogger study shows, side channels can greatly reduce PIN security. The researchers effectively demonstrated that within 3 guesses, the PIN could be compromised 94% of the time via sensor analysis [108]. From a defender's perspective, one could interpret this as meaning only ~6% of PINs remained secure after such an attack (hence the author's calculated "effective accuracy" of ~15.3% for PINs by averaging across multiple attempts, though the exact method of that calculation is a bit unclear) [109]. Realistically, if an attacker has sophisticated tools, a PIN's protection might be quite weak. We will consider PIN systems to have an effective security success rate on the order of 15% in adversarial scenarios (meaning an 85% chance an attacker with advanced methods can crack it within a few tries), as per the cited experiment [109]. In more everyday terms, if an attacker just randomly guesses, they have only 0.01% per try for 4-digit, but we assume a smarter attacker leveraging likely PINs or shoulder surfing could do much better.
- Passwords: Password security varies enormously with password strength and user behavior. Unfortunately, many users choose weak passwords or reuse them. According to several surveys and breach analyses, a substantial portion of passwords are compromised each year. For instance, a recent study commissioned by Forbes Advisor found that 46% of Americans reported having a password stolen in the past year [110]. Other industry statistics indicate roughly 30-40% of users experience a password compromise annually, through various means [111][110]. From another angle, Verizon's annual Data Breach Investigations Report

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 05, May-2025

consistently finds that a large percentage of breaches involve stolen or weak credentials (often over 80% of hacking-related breaches) [112]. For our analysis, we use a figure of about 31% compromise rate per year for passwords, meaning approximately 1 in 3 user passwords gets exposed or cracked in a given year (either via breaches, phishing, or cracking) [113]. Thus, only roughly 69% of passwords remain uncompromised annually on average [113]. This aligns with the idea that the "accuracy" (security) of passwords in protecting accounts is around 69% in the face of real-world threats. Additionally, password strength heavily depends on length: a simple theoretical calculation shows that a 5-character password can be brute-forced in seconds, whereas a 9-character password could take years or more under exhaustive search [114]. For example, a password of 5 lowercase letters (26^5 combinations) could be broken in on the order of 10 seconds with modern hardware, while a password of 9 mixed-case letters and numbers (62^9 combinations) might take many decades at the same rate [115]. In one rough estimation, increasing password length by just one character multiplies the crack time by about 94x (assuming 94 printable characters). Indeed, one source indicates: 5 characters ~10 seconds, 6 chars ~1000 seconds (~16 minutes), 7 chars ~1 day, 8 chars ~115 days, 9 chars ~31 years, 10 chars ~3000 years to brute force at a certain speed [115]. These figures are for offline attacks without lockouts and assuming a certain computational speed, but they illustrate how dramatically the "work factor" grows with length. Unfortunately, many people still use passwords under 8 characters or common words, which are far less secure than these theoretical maximums. To summarize, while a strong, unique password can be very secure, the average password offers only moderate security in practice, given user habits and attack vectors.

COST OF TRADITIONAL SECURITY METHODS

One benefit of traditional authentication (passwords, PINs, patterns) is that they incur essentially no additional hardware cost. They are implemented purely in software on the existing device interface. There is also usually no licensing cost for using a PIN or password system – it's built into the operating system's security framework. Thus, from a manufacturer's perspective, adding a password or PIN option to a phone doesn't raise the device cost (beyond minimal development of the user interface).

However, one could argue there are indirect costs associated with supporting and securing these methods. For instance, software updates are required to patch security vulnerabilities that might allow PIN bypass or password database leaks. Smartphone vendors typically provide security patches for their system software for 4-5 years. The cost of providing ongoing software support (which includes authentication system maintenance among many other things) could be considered part of the cost of the security feature. If one estimates that a phone receives, say, five years of security updates and that the manufacturer's cost for that support is, perhaps, $15-20 per year per device sold (a very rough approximation), that would be on the order of $70–$100 over the device's lifespan dedicated to security maintenance [116]. Not all of that is for the lock method, of course – it includes all security aspects – but it's a way to assign a notional cost value to the software security infrastructure. Using the midpoint, we can take $85 as the average "cost" of providing ongoing software security for a device over its life [117]. This figure will serve as the comparable cost in our analysis for password/PIN security, acknowledging that it's not a direct hardware cost but rather an allocated portion of device/software cost. In effect, this means we assume supporting secure software (encryption, patches, etc.) costs roughly the same order as a fingerprint sensor.

In reality, consumers pay for security as part of the device price and ongoing service, but since we are constructing a cost-benefit index, assigning $85 to the traditional methods allows a parallel comparison with biometrics hardware costs.

COMPARATIVE ANALYSIS: BIOMETRICS VS. TRADITIONAL SECURITY

To quantitatively compare biometric and traditional authentication, we consider both accuracy (or security effectiveness) and cost for each method. Table 2 below summarizes the approximate median accuracy rates and the representative costs we outlined above for each system, and then computes an Accuracy/Cost index for each (where higher values indicate more "security per dollar"):

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 05, May-2025

Authentication Method	Accuracy (Success Rate)	Cost (per device)	Accuracy/Cost Index
Fingerprint	~98.6% (single finger)	$90	1.096
Facial Recognition*	~95.8% (2D/3D avg.)	$130	0.737
Password	~69% (not compromised)	$85	0.812
Pattern Lock	~28% (secure rate)	$85	0.329
PIN	~15.3% (secure rate)	$85	0.180

*Note: For facial recognition, 2D methods have ~95% accuracy and 3D methods ~96.66% in tests; we use the mean ~95.8% for overall effectiveness [118].

This Accuracy/Cost index provides a rough measure of efficiency – how much security payoff one gets for the investment in that technology. Even when considering both accuracy and cost, biometrics appear to outperform traditional forms of security overall. Fingerprint scanning, with an index of ~1.096, offers the best value in this simplified model. It delivers high accuracy (nearly 99% reliable) at a moderate cost around $90, resulting in a security-per-cost about 3.3 times greater than pattern locks, 6.1 times greater than PINs, and about 1.35 times greater than passwords. Facial recognition scores lower, about 0.737, primarily because of its higher cost; nonetheless, it still comes out about 4.1 times better than PINs and 2.24 times better than pattern locks in this metric. The one area where facial recognition lags is compared to passwords – its index is roughly 0.91 times that of passwords, meaning on pure cost-effectiveness, a well-implemented password system could slightly edge out current facial recognition [119].

This particular result (face recognition being ~0.91 times as effective as passwords) suggests two things. First, if users actually chose and used passwords properly, a strong password can be very cost-effective security – essentially free aside from user effort – and might protect nearly as well as today's face unlock, at least for a single device scenario [120]. Second, it indicates that facial recognition technology still has room for improvement in terms of either increasing accuracy or reducing cost. High-end 3D face systems are expensive; if that cost comes down, the index would improve. On the accuracy front, face recognition also faces challenges (lighting, face coverings, etc.) that can reduce real-world reliability, and ongoing improvements (perhaps integrating additional sensors or better algorithms) will be needed to surpass the resilience of a truly strong password.

Importantly, the comparison above assumes an average user context – many users, however, do not follow best practices for passwords, which greatly diminishes the real security of password-based systems. In practice, people often use short, guessable passwords or reuse them, which is partly why we see such high compromise rates annually. Biometrics, by contrast, don't rely on user behavior for their strength (you can't choose a "weak fingerprint"). For this reason, even though our cost-efficiency model gives passwords a decent score, in real-world use biometrics tend to provide more consistent and user-friendly security.

Even factoring in cost, the biometric methods outperform the knowledge-based methods in most respects. Fingerprint scanners deliver the highest security at moderate cost, and facial recognition – while slightly less cost-efficient than an ideal password – still outperforms the typical security of PINs and patterns by a wide margin. Pattern locks and PINs, as shown, have very low security indices (0.329 and 0.180 respectively), confirming that they offer comparatively poor protection for the (minimal) cost. Essentially, pattern and PIN are "cheap" in hardware but also "cheap" in the security they provide, which aligns with known vulnerabilities.

To summarize: fingerprints offer the best overall value in securing personal devices, followed by facial recognition. Passwords can be theoretically competitive, but human factors reduce their practical security. Patterns and PINs lag far behind in effective protection.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 05, May-2025

INFERENCES AND CONCLUSIONS

The analysis presented in this study provides strong evidence that, on average, biometric authentication systems are more accurate and cost-efficient than passwords, PINs, or pattern locks for securing personal devices. In fact, by the measures used, biometrics can be nearly twice as good in combined effectiveness. From our findings, we draw several key inferences and conclusions:

1. Biometrics integrate hardware and software for security, whereas passwords/PINs rely solely on software – making the latter easier to bypass or attack remotely. A biometric system requires possession of a physical trait plus the matching algorithm. In contrast, traditional methods are purely data that can be stolen or cracked without physical presence. This means biometric systems inherently add a layer of security by tying authentication to something tangible and non-transferable [121][19]. It also means attackers need to overcome both a hardware sensor and algorithm protections, rather than just database or user weaknesses.
2. There are scenarios where devices need to be unlocked or bypassed (e.g., law enforcement, emergencies), and these are generally more feasible with software-based methods. For example, if a phone is seized in an investigation or a user is incapacitated, a numeric PIN might be discoverable or reset through forensic tools or recovery modes, whereas a biometric lock could be harder to bypass without the person's biometric input (or a sophisticated spoof). This is a double-edged sword: from a user security perspective, it's good (harder for thieves to break in), but from an accessibility/legal perspective it can be challenging. As a result, virtually all biometric implementations still include a fallback to a PIN/password for such contingencies [122]. Devices typically require a PIN after a reboot or after a certain time, precisely to ensure there's a backup method.
3. Despite their advantages, biometrics are not perfect or infallible. They still need improvements in precision and affordability. Facial recognition, in particular, while convenient, can underperform in certain conditions (e.g., identical twins, faces obscured by masks) [123]. There have been documented cases of high-end 3D face systems being spoofed with extremely well-made masks, though it is very difficult. Likewise, fingerprint sensors can sometimes be tricked by high-quality fingerprint molds or suffer failures if the finger is too dry or injured. So the technology is still developing and is not 100% foolproof. False rejections (legitimate user not recognized) and even rare false accepts continue to be areas for refinement. Cost-wise, biometric sensors add expense, which is why low-end devices sometimes omit them. Over time, we expect these costs to come down as the tech matures.
4. The primary goal of personal device security (for most users) is to prevent casual or opportunistic access and protect privacy, not to withstand nation-state adversaries. Under this threat model, the security provided by standard phone locks (whether PIN or biometrics) is generally sufficient for the average person [124]. Not everyone is at risk of a sophisticated hacker; most phone thieves, for instance, will move on if they can't easily guess the PIN. For this level of need, all these methods "serve the purpose" adequately, though biometrics do so with more convenience and fewer user errors. The average user isn't targeted by advanced side-channel attacks or face-unlock spoofs – they just need to keep nosy acquaintances or pickpockets out, which all these methods can do if used properly.
5. Biometric systems still rely on backups – and thus, in practice, are used in conjunction with traditional methods rather than completely replacing them. Every smartphone that offers fingerprint or face unlock also requires a PIN/password as an alternative (for enrollment, fallback, or if the biometric fails) [125]. This means the overall security of the device is as strong as both factors: biometrics add security and convenience, but you still need a strong password/PIN as a failsafe. It's telling that manufacturers have not allowed users to only have a biometric with no fallback; it's partly for user safety (if the sensor breaks or you're wearing gloves, etc.) and partly for continued trust in a proven method. Therefore, the best practice today is actually to use biometrics and a traditional method together. For example, unlock with fingerprint most of the time, but have a strong password that's occasionally required (e.g., on restart). This two-layer approach covers the gaps of each method.

In conclusion, while not declaring biometrics to be a silver bullet, our study indicates that in current times, biometrics are a considerably superior option for user authentication on personal devices. They combine high accuracy and ease-of-use, which encourages users to actually lock their devices (something that, before fingerprint sensors, many people didn't bother to do due to inconvenience). The results show that a well-implemented fingerprint scanner offers both excellent security and a seamless user experience that passwords or patterns alone cannot match [121][22]. Even so, it's important to note that no security measure is perfect; biometric systems can and do have vulnerabilities, and ongoing improvements are needed (for instance, enhancing facial recognition to handle more cases and resist spoofing as effectively as fingerprints do) [126][125].

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 05, May-2025

Looking ahead, we anticipate that continued advancements in technology will further bolster biometric performance and reduce costs. This may include better liveness detection (to ensure only a real person's traits are accepted), higher resolution sensors, and the integration of multiple biometrics (e.g., combining face and voice or face and fingerprint) for even greater confidence. In parallel, user education and security practices must continue to address the human element – because as secure as biometrics are, users will still be vulnerable if they reuse a weak cloud account password or fall for phishing that bypasses device locks entirely.

For now, the pragmatic advice is to use both biometric and traditional authentication in tandem. Biometrics can handle the day-to-day unlocking with speed and convenience, while a strong password/PIN stands by as a necessary backup. This layered approach ensures that if one factor fails or is compromised, the other still protects the device. Given the findings of this research, such a combination currently offers the best mix of security and usability for protecting personal devices and data.

REFERENCES

Abate, A. F., Nappi, M., Riccio, D., & Sabatino, G. (2007). 2D and 3D Face Recognition: A Survey. Pattern Recognition Letters, 28(14), 1885–1906. DOI: 10.1016/j.patrec.2007.05.018.

[1][2][3][4][5][16][21][23][25][26][27][28][29][30][31][32][33][41][42][43][44][45][46][47][48][52][53][56][57][58][59][60][61][62][63][64][65][66][67][68][69][70][71][72][73][74][75][76][77][78][79][80][81][82][83][84][85][86][93][94][96][97][98][100][104][107][109][113][114][116][117][118][119][120][121][122][123][124][125][126] (PDF) Are Biometrics Truly Better. https://www.academia.edu/85826836/Are_Biometrics_Truly_Better?uc-sb-sw=64908533

[6][7][9][11][12][13][14][15] A Brief History of Biometrics. https://bioconnect.com/blog/2021/12/08/a-brief-history-of-biometrics

[8] Biometrics | History, Types, & Facts | Britannica. https://www.britannica.com/science/biometrics

[10] History of Biometrics | Biometric Update. https://www.biometricupdate.com/201802/history-of-biometrics-2

[17][18][19][20][22][127] What are the Advantages of Biometrics? https://www.enterprisesecuritymag.com/news/what-are-the-advantages-of-biometrics-nid-1841-cid-92.html

[24][129] What are fingerprints? | HowStuffWorks. https://science.howstuffworks.com/fingerprinting1.htm

[34][35][36][37][38][39][40] How Do Fingerprint Scanners Work? Optical vs Capacitive | Arrow.com. https://www.arrow.com/en/research-and-events/articles/how-fingerprint-sensors-work

[49][50][51][128] Understanding Capacitive, Optical and Ultrasonic fingerprint sensors. https://indianexpress.com/article/technology/tech-news-technology/tech-indepth-understanding-capacitive-optical-and-ultrasonic-fingerprint-sensors-7878767/

[54][55] Study: Computerized Fingerprint Systems Extremely Accurate | InformationWeek. https://www.informationweek.com/it-leadership/study-computerized-fingerprint-systems-extremely-accurate

[87][89][90][91][92][95] A short history of the computer password. https://www.welivesecurity.com/2017/05/04/short-history-computer-password/

[88] A Comprehensive Look at the History of Passwords | Hankering for History. https://hankeringforhistory.com/a-comprehensive-look-at-the-history-of-passwords/

[99] Researchers find devices using Pattern Lock can be reliably unlocked in five tries — or less - Electronic Products. https://www.electronicproducts.com/researchers-find-devices-using-pattern-lock-can-be-reliably-unlocked-in-five-tries-or-less/

[101][102][103][106] Android unlock patterns are too easy to guess, stop using them – Sophos News. https://news.sophos.com/en-us/2017/09/28/android-unlock-patterns-are-too-easy-to-guess-stop-using-them/

[105] Why you should never use pattern passwords on your phone | WIRED. https://www.wired.com/story/phone-lock-screen-password/

[108] Sensor data can be used to guess your PIN, unlock your phone – Sophos News. https://news.sophos.com/en-us/2018/01/03/sensor-data-can-be-used-to-guess-your-pin-unlock-your-phone/

[110] In a study commissioned by Forbes Advisor, an alarming 46% of ... https://www.linkedin.com/posts/forbes-advisor_americas-password-habits-46-report-having-activity-7162883077306839040-G5R8

[111] 50+ Password Statistics: The State of Password Security in 2024. https://explodingtopics.com/blog/password-stats

[112] 139 password statistics to help you stay safe. https://us.norton.com/blog/privacy/password-statistics

[115] The PaSsWoRd Trap - Zip ReportsZip Reports. https://zipreports.net/the-password-trap/