Information Security Journal: A Global Perspective

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/uiss20

Privacy and biometrics for smart healthcare systems: attacks, and techniques

Alec Wells & Aminu Bello Usman

To cite this article: Alec Wells & Aminu Bello Usman (03 Oct 2023): Privacy and biometrics for smart healthcare systems: attacks, and techniques, Information Security Journal: A Global Perspective, DOI: 10.1080/19393555.2023.2260818

To link to this article: https://doi.org/10.1080/19393555.2023.2260818

INFORMATION SECURITY JOURNAL: A GLOBAL PERSPECTIVE
https://doi.org/10.1080/19393555.2023.2260818

Taylor & Francis
Taylor & Francis Group

Privacy and biometrics for smart healthcare systems: attacks, and techniques

Alec Wells and Aminu Bello Usman

Cyber Security Research Group, STH, York St John University, York, UK

ABSTRACT

Biometric technology has various applications in smart healthcare systems, including patient authentication, health monitoring, telemedicine, clinical decision support, and personalized care. In addition, medical records contain sensitive and personal information, making them vulnerable to unauthorized access and theft. Because biometric data is distinct and unchangeable, unlike passwords or PINs, using biometric technologies in smart healthcare systems creates privacy problems. This creates privacy concerns as this information is highly sensitive and can be used to identify an individual, making it a valuable target for malicious actors. Subsequently, the storage and use of biometric data in smart healthcare systems must be handled with care to ensure that individuals' privacy rights are protected. Privacy by design is a concept that emphasizes the importance of incorporating privacy considerations into the design and development of products, services, and systems. In this paper, we presented different forms of biometric factors and technologies and their applications in the smart healthcare system to enhance security and privacy in relation to principles of privacy by design. In addition, the study analyzed a variety of attacks and techniques that can be utilized to compromise biometric technology in a smart healthcare system and presented some open research questions.

KEYWORDS

Biometric systems; Internet of Things (IoT); privacy by design; smart healthcare system; voice biometric

1. Introduction

In recent years, the use of artificial intelligence (AI) and Internet of Things (IoT) in healthcare has exploded, with the aim of making it autonomous, intelligent, and easily accessible to users at the highest levels of operation. The integration of AI and IoT can guarantee efficient data collection, facilitate accurate data analysis, and enhance automation and management control. IoT provides a solid foundation for innovative SHS by using sensors to collect real-time data for analytics. When AI algorithms are applied to data, patients or doctors can perform real-time descriptive, diagnostic, or predictive analytics to make sense of the data or use for healthcare automation.

A smart healthcare system (SHS) is a technology-driven system that employs sophisticated technologies such as Artificial Intelligence, Internet of Things (IoT), Big Data Analytics, and other digital tools to increase the effectiveness, precision, and accessibility of healthcare services. Using real-time data management, predictive analytics, telemedicine, and other creative solutions, it seeks to improve patient outcomes, cut costs, and streamline healthcare operations. The combination of IoT devices and the increasingly networked nature of the healthcare environment enables healthcare professionals to provide more efficient and effective emergency and preventive medical services to their patients (Nidhya et al., 2022). Figure 1 illustrates the concept of IoT-enabled smart healthcare systems with all different components of sensor-based networking elements, and a networked platform comprising connectable devices that can acquire, transfer, and store data without human or computer intervention. SHS that use wearable sensors refer to the use of devices, such as fitness trackers, smartwatches, and other wearable technologies, to collect and transmit data about an individual's health and wellness. This data can then be analyzed to provide insights into an individual's health status, identify potential health issues, and track progress over time.

With numerous healthcare facilities seeking to enhance the digitization of data, particularly medical records, the vulnerability of outmoded

CONTACT Alec Wells alec.wells@yorksj.ac.uk Cyber Security Research Group, STH, York St John University, Lord Mayor's Walk, York YO31 7EX, UK

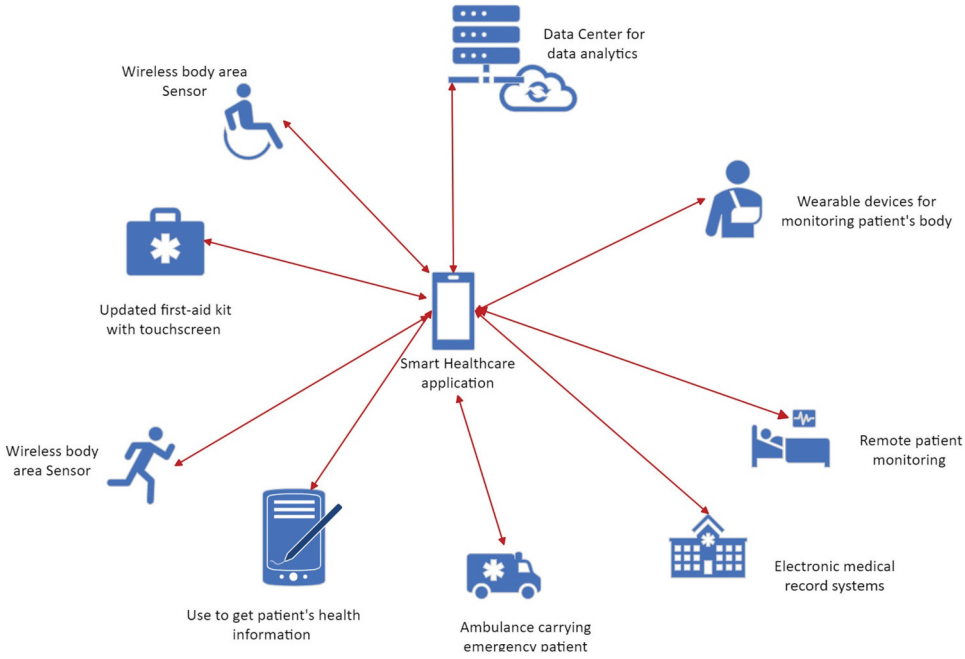

Figure 1. IoT-enabled smart healthcare – a figure containing all the ways smart healthcare applications can be used.

practises is an ethical, financial, and reputational concern. Inadvertently granting records or sensitive data access to the incorrect individuals might result in severe penalties under data privacy regulations or civil prosecution by aggrieved parties. In addition, the subsequent publicity might weaken patients' and physicians' confidence. The Remote Patient Monitoring (RPM) system for example, is among the most innovative SHS (Nait Hamoud et al., 2022) that collects and transmits health-related data from an individual to a healthcare professional, RPM enables continuous monitoring and treatment of the patient's health state. Subsequently, one of the main concerns with the SHS is the potential for unauthorized access to sensitive patient information, such as medical records, test results, and prescriptions (Gajmal & Udayakumar, 2022). This can lead to privacy breaches, identity theft, and other negative consequences. Another concern is the possibility of hacking into SHS and manipulating or corrupting patient data. This can lead to incorrect diagnoses and treatment, as well as loss of trust in the healthcare system.

Biometric factors are used to enhance the security and personalization of smart healthcare systems and to ensure that only authorized individuals have access to sensitive patient information such as medical records, test results, and prescriptions. Designing SHS applications to support users' privacy is important, for example a global survey showed that 88% of users were worried about who had access to their data and over 80% of users expected the government to regulate privacy and impose sanctions on companies that fail to use data responsibly (Spiekermann, 2012). It has also been observed about how privacy by design can be applied to different authentication systems.

The paper is structured as follows: Section 2 introduces the concept of biometrics for smart healthcare systems. In section 3 we introduce the principles of privacy by design and analyze the different biometrics relating to healthcare. Section 4 is an analysis of the various attacks on biometrics. In section 5 we present some open issues in the area. Finally, we present a conclusion in section 6 of the findings within this study that also discusses open issues and potential future research.

2. Biometrics for smart healthcare systems

The human body provides indispensable sources of distinctive features suitable to be used for the task of authentication systems, access control. The use of such distinctive features or a person's biometric

characteristics in healthcare systems is increasing. There are different IoT medical devices that are used for different applications including remote temperature monitoring for vaccines, medical-data transfer tools, air-quality sensors, drug-effectiveness tracking, vital signs data capture, sleep monitors, medication refill reminder technology, remote care biometrics scanners, and sleep and safety tools for babies. These devices use algorithms and techniques to extract the physical characteristics or biometric traits such as palmprints, hand geometry, ears, nose, and lips for authentication or access control. In the current state of the art, the analysis of the retinal vascular pattern with respect to individuals (pattern of blood vessels), appears to be one of the main sources of biometric features in methods like the vein matching, and the retinal scan (Rigas et al., 2016). Other forms of biometric-based traits that enfold behavioral distinctive characteristics, which are partially connected with the brain activity, include keystroke dynamics, voice recognition/speech analysis, and the eye movement driven biometrics.

There are two main types of biometric-based factors. The first is physical biometrics, which use physical features of the human body for users' authentication, this includes using characteristics such a person's fingerprint, iris, or face. Alternatively, there are behavioral biometrics, which utilize a pattern of behavior that is specific to the user, this could be a user's voice, the rhythm they type on a keyboard (Mateusz, 2020). However, there are also new types of biometrics being considered, for example the usage of hand gestures as a form of contactless authentication using convolution neural networks to authenticate users and while promising in regards accuracy, achieving an accuracy of 98.5%, has yet to be tested thoroughly against various forms of attacks or larger data sets (Dayal et al., 2021). Another form that is being tested is the usage of wearable sensors to measure human behavior which also applies convolution neural networks or long short-term memory deep learning which had an accuracy of 91.77% and 92.43% respectively, showing equally promising results (Mekruksavanich & Jitpattanakul, 2021). Recent developments also show that potentially even a user's social networking profiles, like how the user writes their profiles and replies, could contribute to a means of social biometric authentication (Tumpa & Gavrilova, 2020).

Privacy concerns related to biometric sensing systems include the collection, storage, and use of biometric data, as well as the potential for misuse of this data. In healthcare, biometric sensing systems can be used to improve patient care and streamline medical processes, but they also raise significant privacy concerns. Biometric data such as fingerprints, facial recognition, and iris scans can be used to identify patients and link them to their medical records.

2.1. Biometric sensing systems

There are two categories of biometric sensing system; unimodal and multimodal as presented in Figure 2 - a taxonomy of biometric systems.

2.1.1. Unimodal biometrics systems

Unimodal biometric sensing systems are biometric sensing systems that only use a single biometric trait for the individual's identification and verification. Examples of Unimodal Biometric systems includes Single-Source Single-Sample (SSSS), and Single-Source Multiple-Sample (SSMS). Unimodal biometrics, such as fingerprints and iris scans have been used in healthcare systems to improve patient identification and access to medical records (Hamidi, 2019). For example, using fingerprint recognition for patient identification can help to reduce the risk of medical errors and improve the efficiency of medical processes. In healthcare systems, the use of unimodal biometrics can help to ensure that patients are correctly identified and that their medical records are accessible only to authorized individuals. This can help to protect patient privacy and improve the quality of care. However, there are also some limitations and concerns with the use of unimodal biometrics in healthcare systems. One of the main concerns is the security of biometric data. If biometric data is stolen or misused, it can be difficult or impossible to change, making it a valuable target for hackers. Another concern is the ease of use and accessibility of the biometric technology. Some populations may have difficulty using certain types of biometrics, such as older adults or people with certain disabilities.

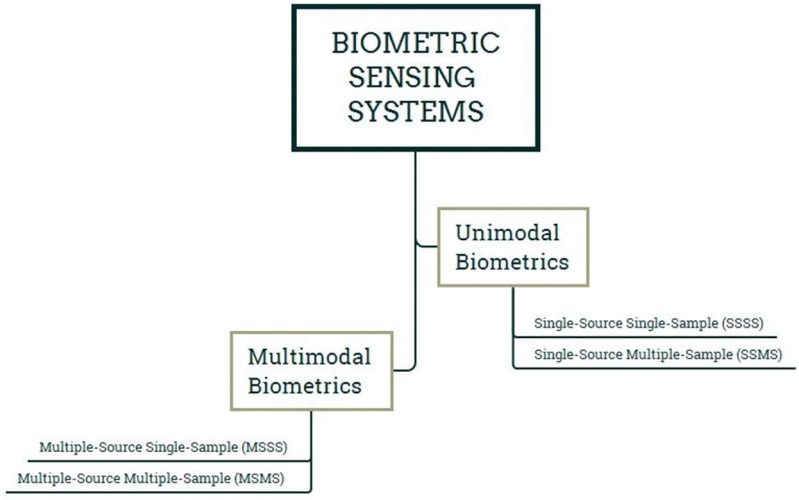

Figure 2. A taxonomy of biometric sensing systems - two different categories of biometric sensing system; unimodal and multimodal and examples of how they can be used.

When only one type of biometric data is acquired, the sensor is more prone to noisy or incorrect data – especially when only a single-sample of biometric data is used. For example, a facial scanner may be influenced by lighting or facial expressions. This also means the data is more susceptible to spoof attacks (where an attacker is successfully verified by falsifying data), since only one type of biometric is being compared in the database. Depending on the data being measured, there could also be issues with unique circumstances such as faded fingerprints or inter-class similarities such as identical twins with facial recognition (Jain & Aggarwal, 2012).

2.1.2. Multimodal biometric systems

A multimodal biometric system uses multiple biometric characteristics, such as fingerprints, iris scans, and facial images, to identify and authenticate individuals. This approach can increase the accuracy and robustness of identification compared to using a single biometric characteristic. Examples include Multiple-Source Single-Sample (MSSS) and Multiple-Source Multiple-Sample (MSMS) (Bala et al., 2022). Multimodal biometric systems can combine both behavioral and physical characters together, like for example in a proposed authentication model which uses both the correct length of three fingers on the contact region as well as the behavioral factor of the shape of the three fingers on the tough screen or pad, to a high accuracy of 91.5% (J. Lee, Park, Kim, Lee, & Jo, 2021a).

In healthcare systems, a multimodal biometric system can be used to improve patient identification and access to medical records. For example, a system that uses both fingerprints and facial recognition can increase the accuracy of patient identification and reduce the risk of medical errors. It could also ensure that patient's medical records are accessible only to authorized individuals, protecting patient privacy (Arora & Bhatia, 2022). Another benefit of a multimodal biometric system is that it can accommodate people with different abilities and physical characteristics, making it more inclusive. For example, if a person is unable to use their fingerprint, facial recognition can still be used to identify them. However, implementing a multimodal biometric system can also be more expensive and complex than using a single biometric characteristic (Bala et al., 2022). Further, multi-sensor systems can combine information captured by multiple sensors to obtain the same biometric modality, such as in the study (Goswami et al., 2014) which uses the depth information along with RGB images to create a more accurate facial recognition. Some multialgorithm systems utilize multiple algorithms for processing an input sample. For example, in the study (Ross et al., 2003), a hybrid matching scheme is used that takes into account both minutiae and ridge flow information of fingerprints to construct a full

feature map. A similar system is adopted in the study (Kumar & Zhang, 2005), which uses several different palmprint representations to extract multiple different textures, lines and other features to construct a more detailed image of the users palmprint. Alternatively, multi-instance systems instead capture multiple instances of the same biometric trait. A typical example of such system include the use of adaptive Bloom filter-based transforms to mix binary iris biometric templates at feature level where iris-codes are obtained from both eyes of a single subject (Rathgeb & Busch, 2014). Another example is seen proposing a three-factor authentication for use in 6 G- aided intelligent healthcare combining smart cards, passwords and biometrics for patients and providers to establish secure communications (Le et al., 2022). Table 1 gives a comparison of unimodal and multimodal biometric systems in a healthcare system.

2.1.3. Cancellable multimodal biometrics systems

The term "cancelable multimodal biometrics" refers to a technique that lets users delete their biometric data if it has been stolen or otherwise compromised. One way this can be done, is by making a copy of the biometric data that can be used for identification but not for re-creating the original. Cancelable multimodal biometrics can be used to alleviate the security problems of biometric data in healthcare systems, allowing for better patient identification and access to medical records. If a person's biometric data is compromised in some way, they can delete it and replace it with a new, altered version that cannot be used to access the original. The usage of biometric templates, which are modified versions of the original biometric data used for identification, is an example of cancelable multimodal biometrics. Even if the original biometric data is stolen, these templates can be recreated thanks to cryptographic methods like randomization.

An alternate way of having cancelable multimodal biometrics is by using a biometric template algorithm with random projection and transformation-based feature extraction to have cancelable multimodal biometrics (J. Lee et al., 2021a). Another example is an approach that uses biometric templates and tokens together, which alternatively use toneless cancelable biometric schemes, such as multimodal extended feature vector, to eliminate the need for tokens (M. J. Lee, Teoh, Uhl, Liang, & Jin, 2021b). Another example of cancelable biometric systems is seen in the studies (Lee & Kim, 2010), and (Alam et al., 2018), which both protect the fingerprint template without requiring the alignment of fingerprints. This is done by injecting noise into the template to create a complex form that is difficult to attack by attacks such as record multiplicity. Similarly, a cancelable biometric system is proposed for healthcare systems using iris authentication by using symmetric key cryptography to encrypt healthcare data onto a smart card (Kausar, 2021).

Cancelable multimodal biometrics can be an effective method to enhance patient identification and gain access to medical records while addressing privacy and confidentiality issues. However, cancelable multimodal biometrics implementation in healthcare systems can be difficult and costly; trade-offs between security and usability must be considered, it must meet all healthcare and patient data privacy standards, and implementation needs to be done carefully and in accordance with existing laws (Carey & Zhan, 2020).

2.1.4. Multimodal biometric fusion

With the abundance of the existing biometric-based modalities and the heterogeneity of the associated features, the need for better security in healthcare systems will continue to evolve. One of the techniques that is being employed in this regard is the use of biometric fusion to combine the information coming from different modalities (e.g., fingerprints, face, iris etc.) Following, is a brief description of the different levels at which biometric fusion can occur (Singh et al., 2019):

Table 1. Comparison of unimodal and multimodal biometric in healthcare systems.

Feature	Unimodal Biometric	Multimodal Biometric
Biometrics	Uses only one type	Uses multiple types
Privacy	Higher risk	Lower risk
Security	Less secure	More secure
Implementation cost	Low	High
Flexibility	Limited flexibility	Greater flexibility
Usability	More convenient	Less convenient
Error Rate	Higher error rate	Lower error rate

- Sensor level fusion – where data is fused immediately after being acquired by the sensor, for example, combining face images of the frontal, left and right profiles.
- Feature level fusion – where data is fused by combining the features analyzed; for instance, combining textures and lines to construct a more complete palmprint.
- Matching score level fusion – fusion can be done at the stage of user authentication when a newly generated image of the user matched against a previous image of that user in the database or where fusion occurs where the match scores have been produced such as to create a mean score fusion or a max/min score of the fusion.
- Rank level fusion – fusion can be performed after comparing the input probe with the templates in the gallery/database with a ranked list of matching identities being produced.
- Decision level fusion – when the final decision is generated after a matcher module matches a fresh image in the database and generates a matching score. Alternatively, the fusion is done by comparing or combining the algorithms.

Compared to unimodal systems, multimodal biometric systems have many advantages for use in SHS, it is much harder to spoof multiple biometric sensors, it is a larklot more accurate at verifying the correct user, and it helps to reduce data distortion (Clark, 2020). Multimodal systems have demonstrated higher accuracy since they use multiple biometric modalities and combine independent evidence to make a more informed decision (Krawczyk & Jain, 2005). Studies such as (Dinerstein et al., 2007) proposed using multi-Support Vector Machines so that even when some biometric modalities were unavailable, classification could still occur. More recently, newer developments as seen in (Purohit & Ajmera, 2021) propose using multimodal biometric fusion with continuous user authentication by using a hybrid LCNN-Salp swarm optimization which "is a class of fake neural systems that builds up the standard feed-forward neural structure with coasts in affiliations." When authenticating online with biometrics, continuous authentication is important to allow for more secure authentication, as by constantly verifying the user, it is easier to identify potential fraud using recordings or images of biometric data. There are many examples of multimodal biometric fusion being applied, one example that has been proposed is to be used with travel cards (Cantarero et al., 2013), via an automated system to read and authenticate electronic travel documents by combining facial images and fingerprints to identify the user as well as performing background checks to make sure the user is eligible to travel. The techniques used in biometric fusion for intelligent biometric systems, such as multiple scoring systems, can also be applied using combinatorial fusion analysis in multiple domains. This can include biometric systems in cognitive neuroscience or visual cognitive systems (Hurley et al., 2020). Furthermore, another example of fusion of features can be seen in the approach of using segmented heartbeat data by extracting the Hilbert transform and power spectrum which are fused together, secondly the approach extracts deep feature signal using PCANet and MaxFusion algorithm to fuse and compress the two layers learning features before using a support vector machine to achieve a recognition success rate of 95% up to 99.77% (Liu et al., 2021).

2.2. Cloud-based healthcare system with biometrics

The use of cloud infrastructures to host Electronic Health Records (EHR) has enabled medical data sharing among various healthcare applications. As illustrated in Figure 3, patients' medical records in a cloud-based healthcare record system are kept on a remote server and may be accessed from anywhere with an internet connection, much like traditional electronic health record (EHR) (Nait Hamoud et al., 2022). Because of this, healthcare providers may now access and share patient data in real time between different hospitals, ultimately leading to better care for patients and more effective teamwork among healthcare professionals. The elimination of the need for expensive on-premises infrastructures and software and the increased accessibility to patients at a cheaper cost is made possible by the cloud architecture in the healthcare industry (Mageshkumar &

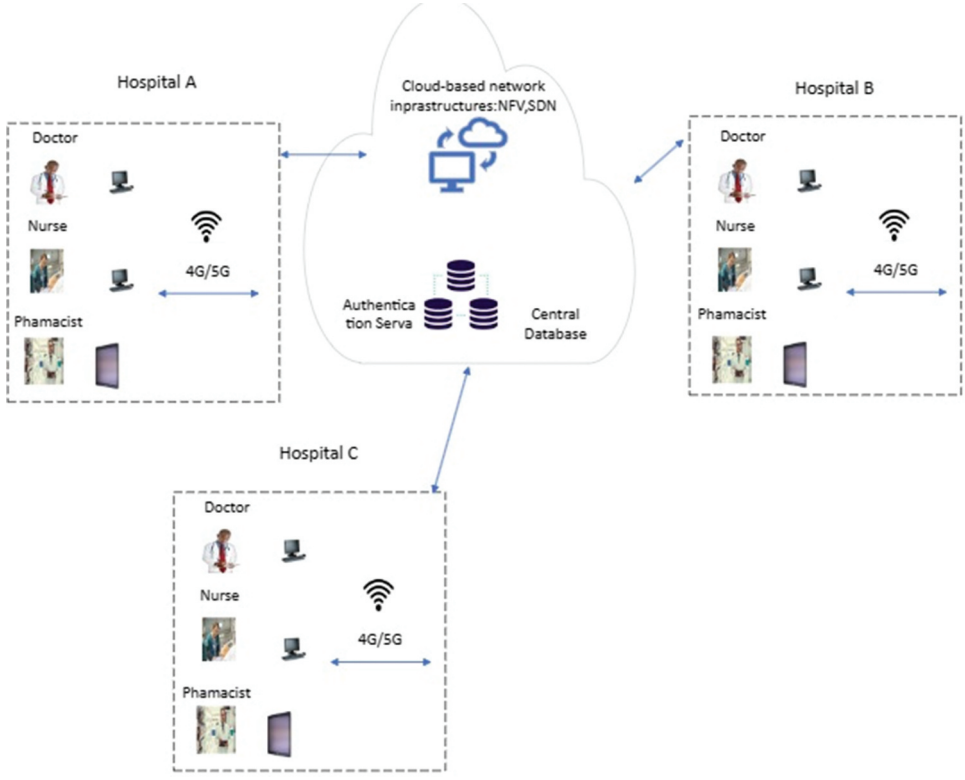

Figure 3. A cloud-based health records system – shows three hospitals connected to the same cloud network.

Lakshmanan, 2023). Cloud-based systems also have the advantage of being easily scalable to meet growing demands, and they receive regular updates to incorporate any new capabilities or security patches. When biometric system is combined with cloud technology, biometrics can provide an extra layer of security for accessing sensitive information stored in the cloud (Gajmal & Udayakumar, 2022). For example, a cloud-based healthcare system may use biometric authentication for accessing patient records, ensuring that only authorized individuals can access the information. This helps to prevent unauthorized access, protect sensitive patient information, and ensure privacy and compliance with regulations. By using biometrics in conjunction with cloud technology, organizations can enhance the security of their cloud-based systems while maintaining the convenience and accessibility of cloud computing (Castiglione et al., 2017). However, biometrics in the cloud can require large amounts of storage, computer power and processing capability. There are also concerns over cloud providers remaining compliant with national laws and standards, such as GDPR with data being destroyed after deletion as well as privacy concerns over where the data is stored and potential security breaches (Castiglione et al., 2017). Facial recognition has been proposed for use with cloud computing, in which cloud users can authenticate themselves by the system recognizing an image of their face compared to a facial template found within an encrypted database which is in an encrypted domain. Although the proposed system allows for secure login, it suffers from slow speed during matching of facial encryption and struggles to perform better recognition of individuals with a small database (Kumar et al., 2018).

2.3. Biometrics with social networking

In a smart healthcare system, combining biometrics and social networking may offer a variety of benefits, such as enhancing patient involvement, facilitating telemedicine, and enabling remote patient monitoring. A patient's current health status and patterns of behavior can be monitored in real time thanks to the combination of biometric data and social media (Azam & Gavrilova, 2017). Biometric data, such as a patient's heart rate or

sleep patterns, can be tracked and shared with their doctor via a social media site. This knowledge can be used in the form of individualized treatment plans and preventative measures (Nowell et al., 2019). Using biometrics, such as facial recognition or fingerprint scanning, users might access their personal health information and engage with their healthcare professionals via social networking platforms. Alternatively, the paper (Paul et al., 2014) presents the idea of decision fusion using social network analysis with multimodal biometric systems, to help addresses problems with biometric data not being high enough quality to produce high recognition results, by constructing social networks based on similarity and correlation of features. However, the combination of biometrics and social networking in healthcare presents significant privacy and security problems. Biometric information is sensitive and can be used to identify persons; if compromised, it cannot be altered as easily as a password. Biometric data must be stored and sent securely, with suitable safeguards in place to prevent unwanted access and data breaches.

3. Privacy by design principles

Privacy by design is a framework for ensuring that privacy considerations are integrated into the design and development of products, services, and systems. It emphasizes the proactive inclusion of privacy features and protections into the architecture and operation of these systems, rather than addressing privacy issues as an afterthought. With the expectation that users' data will be kept safe and secure in SHS, especially given users' increased awareness and expectations of data protection due to GDPR, it is becoming increasingly important that healthcare system technology is built with privacy in mind from the start. One of the most common methodologies for system engineering is privacy by design. A framework that was released in 2009 and has subsequently been widely utilized, such as for the GDPR law (Cavoukian, 2009).

The seven key principles of privacy by design includes:

- **Proactive not Reactive; Preventative not Remedial**: It is important that applications that use privacy by design are proactive rather than reactive and try to anticipate and prevent potential breaches before they happen.
- **Privacy as the Default Setting**: Settings that keep data private should be automatically on, meaning the user needs to take no action to protect their data.
- **Privacy Embedded into Design**: Privacy features should not be bolted onto the application or architecture and should be an essential component of the system, without hurting the functionality.
- **Full Functionality – Positive-Sum not Zero-Sum**: No negative trade-offs should be taken, and it is desirable to have both privacy and security in a "win-win" scenario.
- **End-to-End Security – Full Lifecycle Protection**: Data should be protected throughout its entire usage from when it was conceptualized to its deletion.
- **Visibility and Transparency – Keep it Open**: The parts and operation of the application or architecture must remain visible and transparent to verified users and providers.
- **Respect for User Privacy – Keep it User-Centric**: The individuals' interests should be of the upmost importance, hence should have privacy defaults and remain user-friendly.

In the context of SHS, privacy by design can be used to ensure that personal health information is protected and kept confidential, while still allowing for data sharing and analysis to improve patient care. This can include implementing secure data storage and transmission, using privacy-enhancing technologies, and obtaining informed consent from patients to ensure that patient privacy is safeguarded throughout the system's life cycle. Some of the steps that healthcare providers are taking to achieve privacy by design in SHS are as follows:

- **Conducting a Privacy Impact Assessment (PIA)**: A PIA is a systematic process of evaluating the potential privacy impacts of a new technology system. By conducting a PIA, healthcare providers can identify potential privacy risks and take steps to mitigate them (Parks et al., 2022).
- **Implementing data minimization**: Data minimization is the practice of collecting, using, and retaining only the minimum

amount of personal data necessary to achieve the specific purpose of the system. By implementing data minimization, healthcare providers can reduce the amount of personal data that is collected and stored, which can help to reduce the risk of data breaches (Hornberger, 2021).

- **Enabling data access controls**: Data access controls are used to ensure that only authorized individuals have access to personal data. By enabling data access controls, healthcare providers can ensure that patient data is only accessible to authorized personnel, such as healthcare providers, medical researchers, or other authorized parties (Srikanth & Jaffrin, 2022).
- **Providing transparency and control to patients**: Giving patients control over their personal data can help to build trust in the system. By providing transparency about the data that is being collected, how it will be used, and who will have access to it, healthcare providers can empower patients to make informed decisions about their data (Gajmal & Udayakumar, 2022).
- **Using pseudonymous or anonymous data**: Using pseudonymous or anonymous data in SHS can help to protect patient privacy by making it more difficult to link the data back to a specific individual.

Some of the key privacy issues related to the use of biometric technology in healthcare systems include:

- **Data security**: Biometric data is sensitive information that if compromised, cannot be changed, or replaced like a password. This makes it a valuable target for hackers, and healthcare systems need to ensure that biometric data is stored and transmitted securely.
- **Data sharing and storage**: Biometric data is personal information, and healthcare providers need to be transparent about how it is collected, used, shared, and stored. Providers should also be mindful of the risks associated with sharing biometric data with third parties and should only do so with the patient's informed consent.
- **Privacy invasion**: Biometric technology can be used to track patients, monitor their behavior and activities, and target them with personalized advertising. This could be seen as an invasion of privacy and could lead to mistrust of the healthcare system.
- **Bias and discrimination**: Biometric technology is not always accurate, particularly for certain groups of people, such as those with disabilities, elderly, and certain racial or ethnic groups. This can lead to bias and discrimination and should be avoided.
- **Lack of legal protections**: There are currently few laws and regulations in place to govern the use of biometric technology in healthcare systems. This leaves patients with little legal recourse in the event of a data breach or other privacy violation.

3.1. Privacy and voice for SHS

Voice biometric is a form of inherence-based authentication factor in which user uses their own voice to authenticate themselves. To use voice biometrics, a user will give a sample of their speech via talking into a microphone, the speech will then be converted into a voiceprint that is stored in a database, which can referred back to and verified with in real time as the user speaks (Uniphone, 2018). While the technology for voice biometric authentication has been around for years now, only in recent years has it seen huge developments, primarily by companies such as Nuance, in regard to it being applied commercially and being considered a secure way for users to authenticate themselves, with voice recognition software already being used in healthcare to help with dictation. Voice biometrics can be considered an effective tool for authentication because each human has their own unique voice and speech patterns, where they have unique tones, rhythms, frequency, pitch and speech patterns in how they utter phrases (de Krom, 1994).

There are two main variations of VBA (voice biometric authentication), being text-dependent and text-independent examples, of which are Gaussian Mixture Models and Hidden Markov Models respectfully. Text-dependent systems

require the same specific phrase to by said by the user they used to set up the voice print, often called a passphrase. The more common, text-independent systems in contrast don't require the use of passphrases and instead the identification is often done without the user's knowledge (Microsoft, 2006). With the Gaussian Mixture Model approach, the system recognizes the keyword and utilizes a modeled statistical distribution of the speaker's characteristics and isolated speech from utterance, the model of the user is both calculated and stored in a database during the in-training phase (Janicki & Bial y, 2006). Though many other ways to authenticate voice by recognition exist, these include pitch tracking, vector quantization, dynamic time warping, fusion classifiers system and several others. In the case of Hidden Markov Models, after hearing the voice, the signal is converted into a digital signal, then each utterance is concerted to a Cepstrum domain. Afterwards the features parameters of the user are compared with the voice simple which in turn produces a likelihood ratio to discern is the user is an impostor or can be successfully authenticated (Shrawankar & Thakare, 2013).

Unlike other biometrics, no pictures or recordings are transferred during authentication as it is not done via specialist equipment, instead it can use things such as traditional telephones lines, smartphones or web applications. All these are already widespread and affordable solutions compared to other authentication means that require specialist equipment such as sensors or expensive cameras (Vittori, 2019). Authentication is also done in real-time further making the authentication much harder to attack from fraudsters, since there is no data stored on the system or can be swiftly deleted after authentication (Vittori, 2019), significantly reducing fraud with an Israeli bank having a 10-fold reduction in fraud (Beranek, 2013). In the event an attacker does gain access by utilizing a spoofed voice recording – providing that attempt is identified as being fraudulent, the organization can then use that recorded audio to create a 'voice print' which they can blacklist as a fraudster, preventing further breaches occurring using that same 'voice print' (Vittori, 2019). Passive VBA (where a specific passphrase is not needed) is a lot more secure against potential spoofing from playback recordings of the user by fraudsters, as they can verify with any speech the user makes. With advances in A.I systems; they can also identify callers under distress should they be in a situation forced to authenticate themselves but can be swapped back to active authentication should it be required (Vittori, 2019).

3.1.1. Privacy and smart homes for SHS

Voice recognition software has also seen wide popular usage in voice activated assistants found in smartphones and smart home speakers such as Amazon Alexa or Google Home. Smart homes consist of a range of products such as security cameras, thermostats, and door locks etc, all of which are interlinked with the central device and as such share the same privacy concerns as with multi-server environments. While not identical to the VBA utilized by banks etc. Voice activated assistants like Alexa, do utilize voice recognition software to recognize its users and fulfil their voice commands. Commands offered by smart speakers include playing music, purchasing products, acting as a calendar and much more. Similarly, voice recognition software is also seeing deployment in automobiles, allowing drivers to issue voice commands to their car without removing attention from the road. Voice assistants such as Alexa not only have many current features, but also have many developments over the course of the next few years. One such development is the speaker being able to perform person-to-person payments via voice commands (Crosman, 2018). Currently, the devices are able to distinguish between users, though soon speakers such as Alexa will have the ability to also perform verification on your identity to perform bank payments. Speakers such as Alexa also have many developments into smart healthcare as well, such as assisting the NHS. The Alexa speaker intends on using the NHS website information in order to answer a user's health queries, as well as many other applications such as managing health-improvement goals, blood-sugar readings and booking appointments (Fleming, 2019).

One of the largest concerns regarding smart speakers is that they are always listening. As such, a person or even a television/radio could unintentionally trigger the device and purchase something via voice commands accidentally.

This is especially a concern since natively, the Amazon Alexa supports only user identification and not authentication. So, although the user can train the speaker to recognize their voice, similar sounding voices may trigger the smart speaker. If users wish for better security, a 3rd-party API must be used for voice biometric authentication such as ArmorVox. Another concern of smart speakers is that they usually use a wake-up word from a predefined set of options. This presents many security risks as it is very easy for attackers to guess the wake-up word of the speaker (Edu et al., 2020). When a user is interacting with a smart speaker, the SSL traffic of the smart speaker correlates with when users are interacting with the speaker, which in turn could pose a privacy risk and that data be used for advertising (Apthorpe et al., 2017). Most importantly, any conversation that the speaker hears after the wake-up word is then recorded and consequently is uploaded to the Internet. This can cause huge risks to the user's privacy if private conversations containing sensitive information were leaked, that the smart speaker was not supposed to hear, but did due to an accidental wake-up (Edu et al., 2020).

Smart speakers can also be attacked maliciously, such as by injecting voice commands of the victim's voice via synthesized speech recordings such as in audio playback. Alternatively, an attacker may generate their own malicious commands and embed those commands into online videos or TV advertisements, which may sound like garbled noise to the human ear but are picked up by the smart speaker (Alanwar et al., 2017). Many smart home technologies are also lacking in authorization features with how they manage the level of access to data. For example, many smart homes don't offer proper role separation as to which users can access which services and almost all users share the same level of permissions. Similarly, smart home authorization for payment processes is also inadequate, mainly only offering a 4-digit PIN code to confirm purchases, which is often not enabled by default and suffers from weak lockout implementation, allowing two tries before lockout (Edu et al., 2020). Given unauthorized access could be used to control sensors and actuators, such as opening doors in the case of a robbery, it is of growing concern that smart homes have better security. Hence, there are several objectives to consider with smart home security (Shouran et al., 2019):

- **Confidentiality** – data will only be disclosed to authorized individuals.
- **Integrity** – over wireless networks it is important that the system confirms its identity to distinguish itself from malicious attackers.
- **Availability** – limit the actions from non-essential functions, to prevent the system from being overloaded and have data deteriorate.
- **Authenticity** – verify the identity of devices to prevent disguised malicious attackers from gaining access to the system.
- **Authorisation** – every entity and devices that uses the system has their access rights clearly defined as to what they can do.
- **Non-repudiation** – can verify the truthfulness of any claim of an entity.

As such, many papers purpose solutions for adding more security and preserving the users privacy to smart homes. One example is adding a facial recognition camera to the smart speaker device, meaning to authenticate a user would first have to look at the smart speaker before using the wake work (Sudharsan et al., 2019). This method of facial recognition has been expanded on further by implementing a system architecture based on web service technology. The system utilizes a login manager which would hash the user's password, detect liveness of the facial scan, perform facial recognition, and notify the system. The approach also utilizes an admin manager to manage the user's access to the system, requiring an account to determine their permission as to which applications can only read sensor data, write a request to an actuator or perform both. The system also involves an optional voice recognition to concert the user's speech into typed type and a speech synthesis to read text aloud. A chatbot is used to act as a pre-processing step to convert input text into a phrase before performing entity recognition to correctly understand the users request and respond. Finally, the system uses the web service ThingsManager to pass instruction to the MQTT broker to monitor and control the smart home

application, which combine all the improved security of smart home devices (Al-Mutawa & Eassa, 2020).

3.2. Privacy in fingerprints for SHS

Fingerprints are a prominent biometric identifier used in SHS because they are simple to collect and give a high level of identification accuracy. Fingerprints have been used in Healthcare Information Management Systems such as CareMed to securely access patient health records (Azeta et al., 2017). However, the use of fingerprints in healthcare presents significant privacy problems because fingerprints are considered sensitive personal data.

Fingerprints are quite unique in how many minute details each one can have, there are six main classifications of fingerprint; arch, tented arch, right loop, left loop, whorl and twinloop (Jain et al., 1997). In order to discern if fingerprints match, 3 different types of fingerprint readers are used. The first way of reading fingerprints is optical scanners, optical scanners capture an optical image and utilize algorithms to detect unique patterns and discern if it is a matching fingerprint. Capacitive scanners, use arrays of tiny capacitors to collect highly detailed images of the ridges and valleys of a fingerprint. The third reader is ultrasonic scanners which capture the details of a fingerprint via an ultrasonic pulse transmitted against the finger to discern different ridges, pores etc. Optical scanners are the simplest form of scanning, being just an image and are the easiest to fool but are cheaper and can still work even when the user has wet fingers. Capacitive scanners are more secure and less easily fooled, but have trouble identifying the user with wet fingers. Whereas ultrasonic scanners are very secure and difficult to fool but have almost no trouble when the user's fingers are wet (Blog, 2019).

To safeguard patient privacy in intelligent healthcare systems that utilize fingerprints, obtaining patients' informed consent is essential before collecting and using their fingerprints – utilizing encryption and other security methods to prevent unauthorized access and breaches, storing fingerprints safely, and limiting the usage of fingerprints to authorized personnel and legitimate purposes, including patient identification and authentication. Reviewing and updating security measures frequently to ensure they are still effective.

3.3. Iris recognition for SHS

Iris recognition is another form of physical biometrics, which uses the user's eyes to verify their identity. Similar to fingerprint recognition, the structure of the iris is determined during embryonic development, thus, no two individuals, have the same iris patterns. Iris recognition involves taking a picture of the user's eyes and identifying a unique pattern of a user's iris to authenticate the user, such as by looking at the eye's blood vessels and pigmentation to create a unique profile for the user (Daugman, 2009). Iris recognition can be done by either using the visible imaging/visible light (VL) of the eye or by using what can be observed with near infrared imaging (NIR). Alternatively, a fusion of both types of images can be used. Primarily NIR technology is used, due to the dark pigmentation in human eyes being predominant which VL struggles to reveal visible texture, however, NIR technology eliminates most of the rich melamin information as the chromophore of the human iris is only visible under the VL (is near always the best) (Abdullah et al., 2015). Iris recognition was used during clinical trials to identify all health care provider participants enrolled in a vaccine trial, so that the correct patient received the vaccine at the right visit (Zola Matuvanga et al., 2021).

Like other biometric authentication methods, in the event of a security breach, it is important to protect the privacy of the user's template, given that each iris is unique and identifiable, hence, to protect a user's privacy the template must be protected. Studies such as (Barni et al., 2021) estimated that the privacy risk of a correct genuine identity comparison is 25.86% at a false matching rate (FMR) of 10 to 4, hence the study proposed a method based on generative adversarial networks to automatically generate novel images with a high visual realism to remove and replace all associated biometric information form the template. Alternatively, the study (Wickramaarachchi et al., 2019) proposes an effective biometric recognition system for iris templates using a XOR function, while simultaneously protecting the privacy of iris templates. Another

technique used to protect the privacy of the iris biometric modality is to fuse the data with another biometric modality, like for example with the face modality at the feature-level to produce a discriminating embedding that can be used for recognition (Ledala, 2021).

The use of iris recognition in healthcare raises important privacy concerns, as iris patterns are considered sensitive personal information. There are several privacy concerns that may arise from the use of iris recognition in SHS. For example, Iris patterns are sensitive personal information, and if they are not stored and transmitted securely, they can be compromised by unauthorized access or breaches (Anne et al., 2020). Also, while using iris recognition in healthcare system, patients must be informed about how long their iris patterns will be kept and how they will be disposed of after they are no longer needed, and they must be fully informed about the collection, use, and storage of their iris patterns, and they must give their explicit consent before their iris patterns are collected and used.

3.4. Gait recognition for SHS

Gait recognition is a biometric technology that uses an individual's unique walking style to identify them. It can be utilized in intelligent healthcare systems for patient identification, authentication, and physical therapy progress tracking (Bala et al., 2022). Like other biometrics systems there are learning processes for Gait biometrics that could expose sensitive personal information about the user, especially since gait biometrics can reveal a lot of personally information about the user with their sensors. Studies including (Delgado-Santos et al., 2021) propose novel solutions such as GaitPrivacyON to provide accurate authentication results while still preserving the privacy of the user but use two modules. One which utilizes a combination of a Convolutional Neural Network and Recurrent Neural Network and the other which is a convolutional Autoencoder to transform the raw attributes of the biometric data. Similarly, the work proposed by (Malek-Podjaski & Deligianni, 2021) also uses a novel deep neural network (DNN) architecture so that they can disentangle human emotions and biometrics as needed and hence preserve the user's privacy without affecting the performance of the recognition after training a multi-encoder auto encoder DNN. Alternatively, another proposed solution to preserve the user's privacy is to utilize a biometric cryptosystems (BCS) approach, for securing wireless communications for wearable and implantable health care devices which use gait signal energy variations and an artificial neural network framework; via extracting similar features from BSN sensors to generate binary keys on demand (Sun & Lo, 2018).

3.5. Retina scans for SHS

Retina scans, also known as retinal scans, are a type of biometric technology that identifies individuals using the distinct patterns of blood vessels in the retina, located at the back of the eye. It can be used for patient identification, authentication, and access to private health information in intelligent smart healthcare system.

In terms of security and attack resistance, retina scans are by far the most secure biometric-based authentication system. Since the retina is located from within the structure of the eye itself, it is not prone to the harshness of the external environment like hand geometry recognition or fingerprint recognition. However, the measurement of retina scan accuracy can be affected by illness such as cataracts, and astigmatism. Another disadvantage of retina scan is the scanning procedure is perceived by some as invasive and a violation of the users' privacy since diseases like AIDS and malaria can be detected from the user's retina scan image (Tognetto et al., 2019).

However, the use of retina scans in healthcare raises important privacy concerns, as retina patterns are considered sensitive personal information, arguably more so than other biometric given how invasive they can be on the user's health.

3.6. Facial recognition for SHS

Facial recognition authentication is one of the most widely evolving means of biometric authentication systems which involves the use of algorithms to analysis facial landmarks (nodal points) such as the nose, cheekbones, general shape, and position of the eyes to verify a person from a digital image or

a video frame. Facial recognition technology uses an algorithm to match the unique features of a person's face to a stored image to identify and authenticate them. This technology is used in SHS to identify patients, authenticate access to personal health information, ID staff, detect certain diseases, or track patient movements in a hospital (Praveen & Dakala, 2020). By utilizing a face recognition application, any photo or digital image can be converted to a mathematical code that describes an individual's face.

3.7. Hand/Palmprint patterns for SHS

Palmprint recognition consists of a five-step process involving a scanner, prepossessing, feature extraction, matcher, and database illustrated. Palmprints consist of a few main features that are extracted – flexion creases (principal lines), secondary creases (wrinkles), and ridges with the three major flexion curses being genetically dependent, whereas secondary creases are not so, giving everyone unique palmprint patterns (Kong et al., 2009). As such, palmprint recognition was used to distribute medication in two psychiatric hospitals in Japan, in which each patient-specific drug box was accessed by palm vein authentication (Sawa et al., 2022).

Four main different types of sensors are used to capture palmprint scans, CCD-based palmprint scanners, digital cameras, digital scanners, and video cameras. CCD-based palmprint scanners require suitable conditions of light, lens and camera but can capture every high-quality images. Digital and video cameras can capture images without palmprint contact, but this can cause recognition problems or low-quality scans. Digital scanners meanwhile capture high quality images but require a long scanning time making them more impractical for real-time applications.

3.8. Other behavioral biometrics for SHS

Other forms of behavioral biometrics include signature recognition and keystroke recognition. Signature recognition involves using a person's signature as a way to identify them, this can be done in two different ways, static and dynamic. Static signature recognition is done by users writing their signature on a piece of paper which is then digitized by an optical scanner and compared with the signature template for accuracy. Alternatively, dynamic signature recognition is more sophisticated and requires a digital tablet for the user to write their signature digitally. Other factors can also be observed to identify the user, such as the pressure of pen, the position of the pen, and the angle of the pen in respect to the tablet (Faundez-Zanuy, 2005). Signature recognition does have some privacy concerns such as with the policy-controlled signature scheme used to access the policy to control signature verification permission. Public access to this policy could have sensitive information of the users leak, although privacy preserving schemes have been proposed such as with linear secret sharing schemes using bilinear groups to hide the attribute value to not expose private data (Zheng et al., 2021). Alternatively, other studies have proposed privacy- preserving frameworks based on fog devices for use with cloud-based signature matching to protect private data during the detection process (Wang et al., 2018). Signature recognition can be used in smart healthcare to confirm bookings or to sign every medical/surgery consent form (Huh, 2020).

Keystroke recognition observes how users type on keyboards to identify them using AI and neural networks. Many factors can be observed about the user, such as the time it takes them find a key, how long it takes them to hold down each key press and the speed at which they are typing, all of which contribute to the user's pattern for typing (Monrose & Rubin, 2000). Keystroke dynamics can also be utilized with smart phones, as seen in the study (Liu et al., 2015), which proposed a keystroke dynamic authentication system to smart phones using the pressure, time, size and novel angel of the keypress. Likewise, keystroke dynamics have been used in smart healthcare to protect medical records which are processed and stored in systems with keyboard-based interfaces (Wesolowski et al., 2016).

4. Security attacks of biometric systems

While biometrics have many advantages over other user authentication methods, it is also susceptible to various types of threats. Some of the

threats to a biometric system are aimed directly at the user's biometric template itself, by effecting the integrity of the biometric template including: "(i) accidental template corruption due to a system malfunction such as a hardware failure, (ii) deliberate alteration of an enrolled template by an attacker, and (iii) substitution of a valid template with a bogus template for the purpose of deterring system functionality" (Jain et al., 2005). Likewise, another concern for biometrics is an issue with alignment, generally there is a difference in results between the position users use for enrollment and then recognition, hence biometric systems need good recognition algorithms.

One of the main issues with biometrics, unlike other forms of authentication, is they are not always private. For instance, while a password might only be known by the user, a user's face is constantly on display (unless covered) to any person or camera (Karimovich & Turakulovich, 2016). This is especially true due to the digital age we live in, where people share their lives online through social media, always having their faces on display. Factors such as fingerprints are not immune to this either, and while less on display than perhaps facial features, fingerprints leave marks on surfaces they touch. More importantly is when a biometric is compromised, which in the short term is a very bad thing, however, has great repercussions in the long-term as unlike knowledge or ownership-based factors, biometrics are almost impossible to be changed and once hacked could be hacked for life.

4.1. Attacks definitions

There are many different security attacks on biometric systems as presented in Figure 5 and in Table 2. We provide brief descriptions of those attacks below.

- **Spoofing Attacks** – Attacking a biometric system by either stealing, copying or replicating a synthetic biometric trait in order to gain access to a system (Biggio et al., 2012a). Spoofing attacks also occur when an attacker falsifies biometric data, biometric traits, or reconstructs the original biometric image from the biometric hashcode to impersonate the user and bypass biometric authentication technologies.
- **Brute Force Attack** – Attacking a biometric system by submitting a large number of attempts attempting to spoof the system, usually because the system has not enough reliable information to discern between similar samples (Mihailescu, 2007). These forms of attacks are common against different forms of biometric factors including: Fingerprint, Iris, Face, Plam and Signature as presented in Table 2.
- **Blended Substitution Attack** – An attacker changes the contents in the fuzzy vault that is stored in the database by either preventing the user from authentication, combining the users and attackers templates together to spoof the system, or inject their data during a user's enrollment (Karimovich & Turakulovich, 2016) (Centre, 2019) (Sarala et al., 2016).
- **Attack via Record Multiplicity** – The attacker knows the secret access to the record database and collects multiple enrollment templates to combine the data and at the minimum link records to access the user's biometric template (Karimovich & Turakulovich, 2016) (Scheirer & Boult, 2007).
- **Masquerade Attack** – A type of spoofing attack, where an attacker attempts to spoof the channel between the sensor and feature extractor module by using false data that is commonly available such as digital facial images or digitized laten fingerprints (Karimovich & Turakulovich, 2016) (Roberts, 2007).
- **Attacks on Error Correcting Code** – An attack against the fuzzy commitment and fuzzy extract which abuses the sensors correction algorithm by inputting biometric data close to the user's which is corrected by the system to falsely authenticate the attacker (Karimovich & Turakulovich, 2016) (Stoianov et al., 2009).
- **Chaff Elimination** – The attackers remove chaff points from the user's biometric template to make the biometric sensor easier to be spoofed by similar biometric prints (Karimovich & Turakulovich, 2016).

Table 2. Attacks on biometrics factors.

Biometric Factors	Fingerprint	Iris	Retina	Face	Voice	Palm	Signature	Keystroke
Brute Force	✓ (Mihailescu, 2007)	✓ (Zhao et al., 2015)		✓ (Galbally et al., 2010)		✓ (Kong etal., 2006)	✓ (Galbally et al., 2009)	
Spoofing	✓ (Biggio et al., 2012b)	✓ (Gupta et al., 2014)	✓ (Rodrigues et al., 2009)	✓ (Farmanbar & Toygar, 2017)	✓ (Wu et al., 2012)	✓ (Farmanbar & Toygar, 2017b)		✓ (Monaco et al., 2015)
Chaff Elimination	✓ (Clancy et al., 2003)					✓ (Brindha & Natarajan, 2012		
Masquerade	✓ (Hill, 2001)	✓ (Gupta & Sehgal, 2016)	✓ (Hill, 2001)	✓ (Feng et al., 2014)	✓ (Hill, 2001)	✓ (Hill, 2001)	✓ (Hill, 2001)	✓ (Hill, 2001)
Hill-Climbing	✓ (Martinez-Diaz et al., 2006)	✓ (Rathgeb & Uhl, 2010)		✓ (Galbally et al., 2010)			✓ (Gomez-Barrero et al., 2011)	
Man-in-the-Middle		✓ (Kohli et al., 2017)						
Presentation	✓ (Marcel et al., 2019)	✓ (Pinto et al., 2018)		✓ (Tolosana et al., 2019)	✓ (Pinto et al., 2018)		✓ (Sanchez-Reillo et al., 2017)	
Replay	✓ (Smith et al., 2015)	✓ (Shelton et al., 2014)		✓ (Smith et al., 2015)	✓ (Patil & Kamble, 2018)	✓ (Kong, 2007)	✓ (Zhang et al., 2015)	✓ (Hazan et al., 2019)
Cross Matching	✓ (Kelkboom et al., 2010)	✓ (Gupta & Sehgal, 2016)						
Record Multiplicity	✓ (Li & Hu, 2014)	✓ (Punithavathi et al., 2017)	✓ (Meenakshi & Padmavathi, 2010)	✓ (Merkle & Tams, 2013)	✓ (Chee, 2018)		✓ (Maiorana et al., 2010)	
Blended Substitution	✓ (Scheirer & Boult, 2007)	✓ (Dang et al., 2016)		✓ (Dang et al., 2016)				
False Acceptance	✓ (Karabina & Robinson, 2016)	✓ (Karabina & Robinson, 2016)	✓ (Karabina & Robinson, 2016)	✓ (Karabina & Robinson, 2016)		✓ (Karabina & Robinson, 2016)		
Keylogger								✓ (Olzak, 2008)

- **False Acceptance Attack** – A form of bypass attack where the system accepts the user even though it is not the user by overriding the processing and decision data due to biometrics being extremely similar (Karimovich & Turakulovich, 2016) (Roberts, 2007).
- **Hill-Climbing attacks** - A form of brute force attack that requires the attacker to gradually develop and submit repeated fake synthetic biometric data while improving the result, which could eventually allow the attacker to compromise the biometric system or achieve a false acceptance.
- **Man-in-the-Middle attacks** - A man-in-the-middle attack is an attack where an attacker may seek to alter or intercept the data output from the sensor in transit between the biometric feature extractor, biometric template generator, or matcher of the application device. An attacker could utilize intercepted data to obtain the biometric characteristics for further attacks.
- **Presentation attacks** - A presentation attack is another form of impersonation or spoofing attack mostly using Presentation Attack Instruments (PAIs) such as a camera, mask, or fake silicone fingerprints, etc. Using PAIs, an attacker can attempt to impersonate a user's biometric identity to bypass the biometric system in various ways. As shown in Table 2, presentation attack is a real challenge to most biometric modalities, including face, fingerprint, voice, and signature.
- **Replay attacks** - A replay attack is a form of meet-in-the-middle (man-in-the-middle) attack in which an attacker intercepts biometric data and re-transmits it. This attack doesn't require an attacker to have specific expertise to either decrypt or further process data after intercepting it. This makes it a common form of attack on biometric systems as illustrated in Table 2.

Figure 4 presents point of attacks to biometric systems. The figure shows eight possible points of attacks hackers can attempt to attack biometrics systems (Uludag & Jain, 2004). At point 1, a presentation attack is used, where an imposter attempts to spoof a user's biometrics with a fake image. For instance, in a facial recognition system an attacker may try to spoof the system with a photograph of the user's face, alternatively in a fingerprint system they may use a mold of the user's fingerprint. At points 2, 3, 4 & 5, hackers may try a sensor output interception, which involves them intercepting or perhaps modifying the data from the sensor with either a previously captured sample and then substituting the biometric with a different individual's biometrics at the points of feature extraction or obtaining an artificially high matching score at the fifth point. Alternatively, attackers may even target the IT system the sensor is tied to. Perhaps stealing biometric data to use at point 1, or adding/modifying existing templates in the database, by attacking point 6 or altering the transmission at point 7. Or alternatively the attacker might just override the matcher result at point 8 (Centre, 2019; Uludag & Jain, 2004).

4.2. Comparison of biometric factors

In the context of biometric system, security can be defined as the strength of the biometric system in terms of covered risk and its efficiency to resist potential attacks – its sophistication (Jain et al., 2005). We compared the presented authentication factors in Figure 5 and in terms of security and accuracy the comparison is presented in Table 3.

4.3. Accuracy

In terms of accuracy, there are two key performance metrics of evaluating biometric system, namely False Acceptance Rate (FAR) and False Rejection Rate (FRR). FAR is the probability that the system incorrectly authorizes a non-authorized person, due to incorrectly matching the biometric input with a template. FRR is the probability that the system incorrectly rejects access to an authorized person, due to failing to match the biometric input with a template (Arulkumar & Vivekanandan, 2018).

- **High accuracy**: fingerprint, iris, retinal.
- **Medium accuracy**: facial, hand geometry, handwritten signature, gait and voice.
- **Low accuracy**: keystroke dynamics.

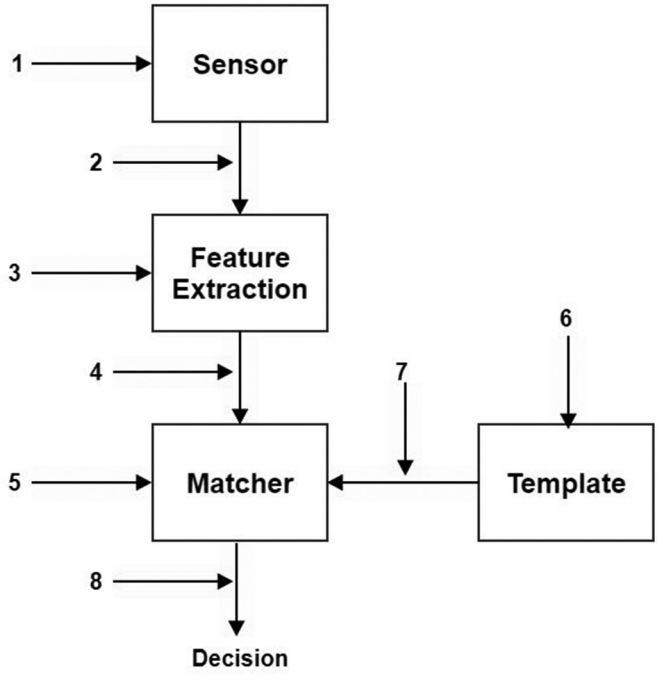

Figure 4. Point of attacks on biometric fusion - diagram showcasing the various points in which a biometric system can be attacked at.

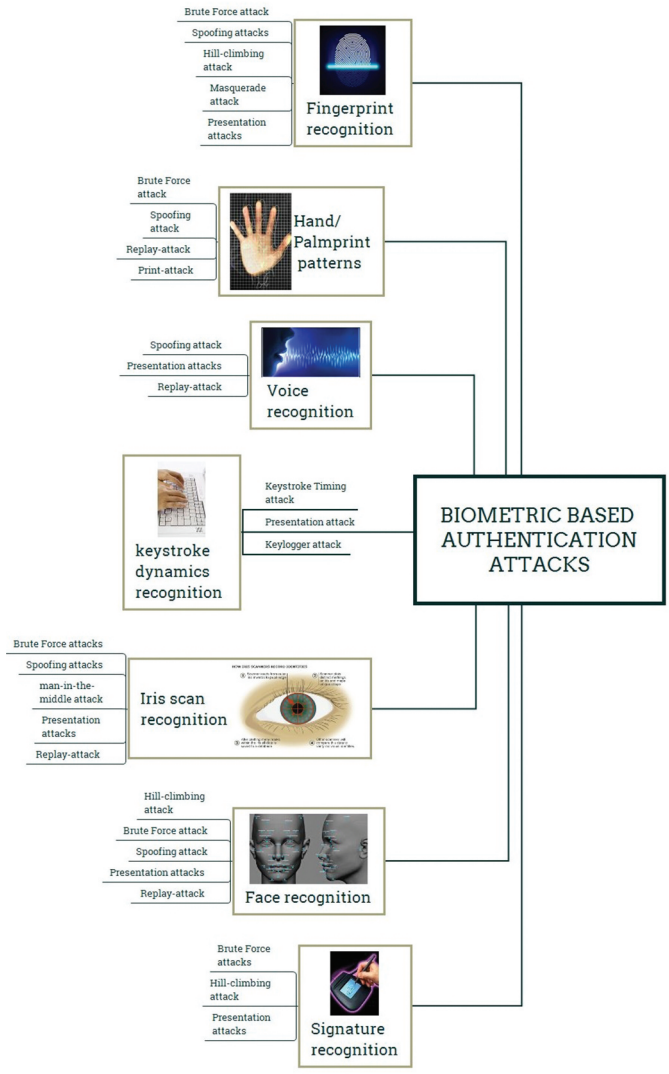

Figure 5. A taxonomy of attacks on biometric authentication factors - an illustration of various types of biometric authentication and the type of attacks they can be attacked by.

Table 3. Comparison of biometric factors.

Biometric Factors	Security	Accuracy
Fingerprint	Medium	High
Iris	High	High
Retina	High	High
Face	Medium	Medium
Voice	Medium	Medium
Palm	High	Medium
Signature	Medium	Medium
Keystroke	Low	Low
Gait	Medium	Medium

There are two generic approaches for securing biometric templates: biometric feature transformation and biometric cryptosystems. Biometric feature transformation involves "applying a non-invertible or one-way transformation function to the original template to create a secure template" in which during authentication the same query is applied to verify if the two match (Jain & Nandakumar, 2012). Biometric cryptosystems however "only store a fraction of the original template, known as the secure sketch. Which is just enough data to recover the template if another biometric sample closely matched the enrolled sample" (Jain & Nandakumar, 2012). One of the main countermeasures to biometric fraud, is to develop precise sensors that cannot easily be spoofed by copies imitating a user's features (Finextra, 2017). Likewise, it is also important that users use multi-factor authentication to prevent just a single breach causing lots of problems either combining inherence factors with

other types of factors or more forms of biometric authentication, for instance the use of a fingerprint scanner and other forms of biometrics such as facial or iris.

5. Open issues

There are several open research issues in this area, including data protection and privacy, data storage and management, compliance with privacy laws and regulations, and public trust and perception. Addressing these research issues is crucial for the successful adoption of smart healthcare systems that use biometric data, as they play a crucial role in ensuring the protection of patient privacy and the security of biometric data. By developing effective and secure methods for using biometric data in healthcare, researchers and practitioners can help to improve the quality and accessibility of healthcare services for patients worldwide. Below is the summary of the open issues in this topic, some of these open issues includes:

- Anonymous biometric data: One challenge is to provide a way for biometric data to be used for patient care and treatment without compromising the privacy of individuals. This includes techniques for anonymizing biometric data, such as biometric data hashing, and for providing secure and private biometric authentication.
- Public trust and perception: Building public trust and addressing negative perceptions about the use of biometric data in healthcare is important for the successful adoption of smart healthcare systems. Research is needed to understand public perception of biometric data and to develop strategies to increase public trust in these systems.
- Further work is required to explore Compliance with privacy laws and regulations. Smart healthcare systems must comply with privacy laws and regulations, such as the General Data Protection Regulation (GDPR) to ensure the protection of biometric data.
- There is abundant room for further progress in exploring the Cross-cultural and demographic diversity of biometric factors in smart healthcare systems. Biometric systems must be able to accurately recognize individuals from diverse backgrounds and demographic groups, including elderly people, people with disabilities, and individuals with unique physical features.
- Interoperability: Biometric systems must be able to interoperate with existing healthcare systems, including electronic health records (EHRs) and wearable devices, to provide seamless and integrated healthcare services. Further studies, which will enhance the interoperability between biometric systems and the legacy SHS, will need to be undertaken while taking into account privacy by design principles.
- It is of the utmost to keep biometric templates held in databases, as secure as possible, given that it is one of the main ways biometrics can successfully be attacked. There is also a concern around biometrics that once a person's biometrics are compromised – they are compromised for life, given that they cannot easily be changed like a password or PIN number (Bowman, 2019) hence, a better solution needs to be devised for compromised biometrics.
- Because of the potential for biometrics to be spoofed, biometric sensors must be able to accurately identify liveness in images. Voice biometrics, for instance, can be tricked through imitation, technologically generated synthetic mimicry, or a previously recorded voice sample (Farmanbar & Toygar, 2017).
- Real-time and remote biometric authentication: With the increasing trend of telemedicine and remote healthcare, real-time and remote biometric authentication is becoming increasingly important. Ensuring the reliability and security of remote biometric authentication is a significant challenge. This is an important issue for future research.
- There are also concerns about the quality and availability of biometric sensors. High precision sensors for biometrics can be expensive and not available all environment, not to mention that biometric data can often be 'noisy' due to the environment. This is also still a potential concern for biometrics such as voice, which use existing infrastructure, due

to areas with bad reception or slow internet, causing the users voice sound distorted and unclear, so algorithms need to be sophisticated enough to work around problems such as background noise or crosstalk (Beranek, 2013).

Research questions that could be asked include:

- How can smart healthcare systems effectively balance privacy and security concerns with the benefits of data sharing and collaboration between healthcare providers, patients, and family members?
- What are the ethical and legal considerations surrounding the use of personal health information in smart healthcare systems and how can they be addressed in the development of privacy-protective technologies?
- How can privacy by design principles be effectively integrated into the development of smart healthcare systems to ensure the protection of personal health information? And what role do patients play in determining the privacy and security of their personal health information in smart healthcare systems, and how can their preferences be incorporated into the design of these systems?

More study on this subject is required to facilitate the development and implementation of privacy protection policies and procedures, including data security measures, data sharing, data storage, and data usage policies around biometrics and smart healthcare systems.

6. Conclusion

The paper underlines the growing use of biometric technology in healthcare to improve patient experience, improve patient identification and access to medical records, and deliver more accurate and timely medical monitoring. Biometric technology such as fingerprint recognition, facial recognition, and iris scanning enable quick, safe, and convenient patient authentication and data access. Further, biometrics are considered as being the future of authentication as they are seen as being more secure than other authentication methods, such as knowledge-based factors, in part due to requiring more sophisticated systems to attack or spoof. The paper highlighted potential aspects of biometric technologies in terms of ease, accuracy, and security. However, there are issues with data security and privacy. While biometrics hold enormous promise for the future of healthcare, healthcare organizations must address privacy and security issues in order to secure widespread adoption and develop confidence among patients and healthcare providers. The paper, on the other hand, explored privacy and data security issues, such as data breaches and the danger of biometric information being abused and different forms of biometric attack techniques and countermeasures, including spoofing attacks, presentation attacks, man-in-the-middle attacks, etc. To summarize, biometrics hold enormous promise for the future of healthcare, but healthcare organizations must implement strong privacy and security safeguards to protect patient information and develop trust in the technology.

Disclosure statement

No potential conflict of interest was reported by the author(s).

References

Abdullah, M. A., Chambers, J. A., Woo, W. L., and Dlay, S. S. (2015). Iris biometrie: Is the near-infrared spectrum always the best? In *2015 3rd IAPR Asian Conference on Pattern Recognition (ACPR)*, 3-6 November 2015, Kuala Lumpur, Malaysia (pp. 816–819). IEEE.

Alam, B., Jin, Z., Yap, W.-S., & Goi, B.-M. (2018). An alignment-free cancelable fingerprint template for bio-cryptosystems. *Journal of Network and Computer Applications*, *115*, 20–32. https://doi.org/10.1016/j.jnca.2018.04.013

Alanwar, A., Balaji, B., Tian, Y., Yang, S., and Srivastava, M. (2017). Echosafe: Sonar-based verifiable interaction with intelligent digital agents. In *Proceedings of the 1st ACM Workshop on the Internet of Safe Things*, November 5, 2017, Delft, The Netherlands (pp. 38–43).

Al-Mutawa, R. F., & Eassa, F. A. (2020). A smart home system based on internet of things. International Journal of Advanced Computer Science and Applications, *11*(2), 252–259. *arXiv preprint arXiv:2009.05328*. https://doi.org/10.14569/IJACSA.2020.0110234

Anne, N., Dunbar, M. D., Abuna, F., Simpson, P., Macharia, P., Betz, B., Cherutich, P., Bukusi, D., &

Carey, F. (2020). Feasibility and acceptability of an iris biometric system for unique patient identification in routine HIV services in kenya. *International Journal of Medical Informatics*, *133*, 104006. https://doi.org/10.1016/j.ijmedinf.2019.104006

Apthorpe, N., Reisman, D., & Feamster, N. (2017). A smart home is no castle: Privacy vulnerabilities of encrypted iot traffic. *ArXiv*, abs/1705.068005. *arXiv preprint arXiv:1705.06805*.

Arora, S., & Bhatia, M. (2022). Challenges and opportunities in biometric security: A survey. *Information Security Journal: A Global Perspective*, *31*(1), 28–48. https://doi.org/10.1080/19393555.2021.1873464

Arulkumar, V., & Vivekanandan, P. (2018). An intelligent technique for uniquely recognising face and finger image using learning vector quantisation (lvq)-based template key generation. *International Journal of Biomedical Engineering and Technology*, *26*(3–4), 237–249. https://doi.org/10.1504/IJBET.2018.089951

Azam, S., & Gavrilova, M. L. (2017). Biometric pattern recognition from social media aesthetics. *International Journal of Cognitive Informatics and Natural Intelligence (IJCINI)*, *11*(3), 1–16. https://doi.org/10.4018/IJCINI.2017070101

Azeta, A. A., Iboroma, D.-O. A., Azeta, V. I., Igbekele, E. O., Fatinikun, D. O., and Ekpunobi, E. (2017). Implementing a medical record system with biometrics authentication in e-health. In *2017 IEEE AFRICON* 18-20 September Cape Town, South Africa (pp. 979–983).

Bala, N., Gupta, R., & Kumar, A. (2022). Multimodal biometric system based on fusion techniques: A review. *Information Security Journal: A Global Perspective*, *31*(3), 289–337. https://doi.org/10.1080/19393555.2021.1974130

Barni, M., Labati, R. D., Genovese, A., Piuri, V., & Scotti, F. (2021). Iris deidentification with high visual realism for privacy protection on websites and social networks. *IEEE Access*, *9*, 131995–132010. https://doi.org/10.1109/ACCESS.2021.3114588

Beranek, B. (2013). Voice biometrics: Success stories, success factors and what's next. *Biometric Technology Today*, *2013*(7), 9–11. https://doi.org/10.1016/S0969-4765(13)70128-0

Biggio, B., Akhtar, Z., Fumera, G., Marcialis, G. L., & Roli, F. (2012a). Security evaluation of biometric authentication systems under real spoofing attacks. *IET Biometrics*, *1*(1), 11–24. https://doi.org/10.1049/iet-bmt.2011.0012

Blog, G. P. (2019). 3 different types of fingerprint scanner and how they work – General Post Blog. Retrieved January 06, 2020, from https://genolomu.wordpress.com/2019/03/08/3-different-types-of-fingerprint-scanner-and-how-they-work/

Bowman, B. (2019). Biometric hacking. Retrieved January 06, 2020, from https://securityboulevard.com/2019/04/biometric-hacking/

Brindha, V. E., & Natarajan, A. (2012). Multi-modal biometric template security: Fingerprint and palmprint based fuzzy vault. *Journal of Biometrics and Biostatistics*, *3*(3), 100–150. https://doi.org/10.4172/2155-6180.1000150

Cantarero, D. C., Herrero, D. A. P., and M´endez, F. M. (2013). A multi-modal biometric fusion implementation for ABC systems. In *2013 European Intelligence and Security Informatics Conference*, August 12-14, Uppsala, Sweden (pp. 277–280). IEEE.

Carey, A. N. and Zhan, J. (2020). A cancelable multi-modal biometric based encryption scheme for medical images. In *2020 IEEE International Conference on Big Data (Big Data)*, December 10-13, Virtual (pp. 3711–3720). IEEE.

Castiglione, A., Choo, K.-K. R., Nappi, M., & Narducci, F. (2017). Biometrics in the cloud: Challenges and research opportunities. *IEEE Cloud Computing*, *4*(4), 12–17. https://doi.org/10.1109/MCC.2017.3791012

Cavoukian, A. (2009). Privacy by design. Retrieved January 01, 2020, from https://privacysecurityacademy.com/wp-content/uploads/2020/08/PbD-Principles-and-Mapping.pdf

Centre, N. C. S. (2019). Biometric recognition and authentication systems. Retrieved January 01, 2020, from https://www.ncsc.gov.uk/collection/biometrics/how-biometrics-are-attacked

Chee, K. Y. (2018). *Design and Analysis of Voice Template Protection Schemes Based on Winner-takes-all Hashing* [PhD thesis]. UTAR.

Clancy, T. C., Kiyavash, N., and Lin, D. J. (2003). Secure smartcardbased fingerprint authentication. In *Proceedings of the 2003 ACM SIGMM workshop on Biometrics methods and applications* Berkeley, California (pp. 45–52).

Clark, M. (2020). Unimodal biometrics vs. multimodal biometrics. *Bayometric*. Retrieved January 01, 2020, from https://www.bayometric.com/unimodal-vs-multimodal/

Crosman, P. (2018). Is amazon's Alexa ready for person-to-person payments? Retrieved January 01, 2020, from https://www.americanbanker.com/news/is-amazons-alexa-ready-for-p2p-payments

Dang, T. K., Truong, Q. C., Le, T. T. B., & Truong, H. (2016). Cancellable fuzzy vault with periodic transformation for biometric template protection. *IET Biometrics*, *5*(3), 229–235. https://doi.org/10.1049/iet-bmt.2015.0029

Daugman, J. (2009). How iris recognition works. In *The essential guide to image processing* (pp. 715–739). Elsevier.

Dayal, A., Paluru, N., Cenkeramaddi, L. R., Yalavarthy, P. K., & Yalavarthy, P. K. (2021). Design and implementation of deep learning based contactless authentication system using hand gestures. *Electronics*, *10*(2), 182. https://doi.org/10.3390/electronics10020182

de Krom, G. (1994). Consistency and reliability of voice quality ratings for different types of speech fragments. *Journal of Speech, Language, & Hearing Research*, *37*(5), 985–1000. https://doi.org/10.1044/jshr.3705.985

Delgado-Santos, P., Tolosana, R., Guest, R., Vera, R., Deravi, F., & Morales, A. (2021). Gaitprivacyon: Privacy-preserving mobile gait biometrics using unsupervised learning. *Pattern Recognition Letters 161*, 30–37. *arXiv preprint arXiv:2110.03967*. https://doi.org/10.1016/j.patrec.2022.07.015

Dinerstein, S., Dinerstein, J., and Ventura, D. (2007). Robust multi-modal biometric fusion via multiple svms. In *2007 IEEE International Conference on Systems, Man and Cybernetics*, October 7-10, Montreal, Quebec, Canada(pp. 1530–1535). IEEE.

Edu, J. S., Such, J. M., & Suarez-Tangil, G. (2020). Smart home personal assistants: A security and privacy review. *ACM Computing Surveys (CSUR)*, *53*(6), 1–36. https://doi.org/10.1145/3412383

Farmanbar, M., & Toygar, O. (2017). Spoof detection on face and palmprint biometrics.¨ *signal. Image and Video Processing*, *11*(7), 1253–1260. https://doi.org/10.1007/s11760-017-1082-y

Faundez-Zanuy, M. (2005). Signature recognition state-of-the -art. *IEEE Aerospace and Electronic Systems Magazine*, *20* (7), 28–32. https://doi.org/10.1109/MAES.2005.1499249

Feng, Y. C., Lim, M.-H., & Yuen, P. C. (2014). Masquerade attack on transform-based binary-template protection based on perceptron learning. *Pattern Recognition*, *47*(9), 3019–3033. https://doi.org/10.1016/j.patcog.2014.03.003

Finextra. (2017). Precise biometrics debuts spoof tech to identify fake and dead fingers. Retrieved January 01, 2020, from https://www.finextra.com/pressarticle/69825/precise-biometrics-debuts-spoof-tech-to-identify-fake-and-dead-fingers

Fleming, N. (2019). Does amazon have answers for the future of the nhs? Retrieved January 01, 2020, from https://www.theguardian.com/technology/2019/aug/24/alexa-nhs-future-amazon-artificial-intelligence-healthcare

Gajmal, Y. M., & Udayakumar, R. (2022). Privacy and utility-assisted data protection strategy for secure data sharing and retrieval in cloud system. *Information Security Journal: A Global Perspective*, *31*(4), 451–465. https://doi.org/10.1080/19393555.2021.1933270

Galbally, J., Fierrez, J., Martinez-Diaz, M., and Ortega-Garcia, J. (2009). Evaluation of brute-force attack to dynamic signature verification using synthetic samples. In *2009 10th International Conference on Document Analysis and Recognition*, July 29, Barcelona, Spain (pp. 131–135). IEEE.

Galbally, J., McCool, C., Fierrez, J., Marcel, S., & Ortega-Garcia, J. (2010). On the vulnerability of face verification systems to hill-climbing attacks. *Pattern Recognition*, *43*(3), 1027–1038. https://doi.org/10.1016/j.patcog.2009.08.022

Gomez-Barrero, M., Galbally, J., Fierrez, J., & Ortega-Garcia, J. (2011). Hill-climbing attack based on the uphill simplex algorithm and its application to signature verification. In *European Workshop on Biometrics and identity management* (pp. 83–94). Springer. https://doi.org/10.1007/978-3-642-19530-3_8

Goswami, G., Vatsa, M., & Singh, R. (2014). RGB-D face recognition with texture and attribute features. *IEEE Transactions on Information Forensics and Security*, *9*(10), 1629–1640. https://doi.org/10.1109/TIFS.2014.2343913

Gupta, P., Behera, S., Vatsa, M., and Singh, R. (2014). On iris spoofing using print attack. In *2014 22nd International Conference on Pattern Recognition*, August 24-28, Stockholm, Sweden (pp. 1681–1686). IEEE.

Gupta, R., & Sehgal, P. (2016). A survey of attacks on iris biometric systems. *International Journal of Biometrics*, *8*(2), 145–178. https://doi.org/10.1504/IJBM.2016.077833

Hamidi, H. (2019). An approach to develop the smart health using internet of things and authentication based on biometric technology. *Future Generation Computer Systems*, *91*, 434–449. https://doi.org/10.1016/j.future.2018.09.024

Hazan, I., Margalit, O., & Rokach, L. (2019). Securing keystroke dynamics from replay attacks. *Applied Soft Computing*, *85*, 105798. https://doi.org/10.1016/j.asoc.2019.105798

Hill, C. J. (2001). *Risk of masquerade arising from the storage of biometrics* [*Bachelor of Science thesis*]. The Department of Computer Science, Australian National University.

Hornberger, R. C. (2021). Creating a sense of digital privacy in the private sector. *Information Security Journal: A Global Perspective*, *30*(1), 30–56. https://doi.org/10.1080/19393555.2020.1797948

Huh, J.-H. (2020). Surgery agreement signature authentication system for mobile health care. *Electronics*, *9*(6), 890. https://doi.org/10.3390/electronics9060890

Hurley, L., Kristal, B. S., Sirimulla, S., Schweikert, C., & Hsu, D. F. (2020). Multi-layer combinatorial fusion using cognitive diversity. *IEEE Access*, *9*, 3919–3935. https://doi.org/10.1109/ACCESS.2020.3047057

Jain, A., & Aggarwal, S. (2012). Multimodal biometric system: A survey. *International Journal of Applied Science and Advance Technology*, *1*(1), 58–63.

Jain, A. K., Hong, L., Pankanti, S., & Bolle, R. (1997). An identity-authentication system using fingerprints. *Proceedings of the IEEE*, *85*(9), 1365–1388. https://doi.org/10.1109/5.628674

Jain, A. K., & Nandakumar, K. (2012). Biometric authentication: System security and user privacy. *Computer*, *45*(11), 87–92. https://doi.org/10.1109/MC.2012.364

Jain, A. K., Ross, A., and Uludag, U. (2005). Biometric template security: Challenges and solutions. In *2005 13th European signal processing conference*, September 4-8, Antalya, Turkey (pp. 1–4). IEEE.

Janicki, A. and Bial y, S. (2006). Improving gmm based speaker recognition using trained voice activity detection. In *5th Conference on signals and electronic systems*, *Lodz*, *Poland*.

Karabina, K. and Robinson, A. (2016). Revisiting the false acceptance rate attack on biometric visual cryptographic schemes. In *International Conference on Information Theoretic Security* 29 November - 2 December Hong Kong, China (pp. 114–125). Springer.

Karimovich, G. S. and Turakulovich, K. Z. (2016). Biometric cryptosystems: Open issues and challenges. In *2016 International Conference on Information Science and Communications Technologies (ICISCT)*, November 2-4, Tashkent, Uzbekistan (pp. 1–3). IEEE.

Kausar, F. (2021). Iris based cancelable biometric cryptosystem for secure healthcare smart card. *Egyptian Informatics Journal*, *22*(4), 447–453. https://doi.org/10.1016/j.eij.2021.01.004

Kelkboom, E. J., Breebaart, J., Kevenaar, T. A., Buhan, I., & Veldhuis, R. N. (2010). Preventing the decodability attack based cross-matching in a fuzzy commitment scheme. *IEEE Transactions on Information Forensics and Security*, *6*(1), 107–121. https://doi.org/10.1109/TIFS.2010.2091637

Kohli, N., Yadav, D., Vatsa, M., Singh, R., and Noore, A. (2017). Synthetic iris presentation attack using idcgan. In *2017 IEEE International Joint Conference on Biometrics (IJCB)* October 1 - 4 Denver, Colorado, USA (pp. 674–680). IEEE.

Kong, A. (2007). Palmprint identification based on generalization of iriscode (University of Waterloo). Retrieved January 01, 2020, from https://uwspace.uwaterloo.ca/bitstream/handle/10012/2708/PhD_thesis_Adams_Final.pdf?sequence=1

Kong, A., Zhang, D., & Kamel, M. (2009). A survey of palmprint recognition. *Pattern Recognition*, *42*(7), 1408–1418. https://doi.org/10.1016/j.patcog.2009.01.018

Kong, A. W.-K., Zhang, D., & Kamel, M. (2006). Analysis of brute-force break-ins of a palmprint authentication system. *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, *36*(5), 1201–1205. https://doi.org/10.1109/TSMCB.2006.876168

Krawczyk, S. and Jain, A. K. (2005). Securing electronic medical records using biometric authentication. In *International Conference on Audio-and Video-Based Biometric Person Authentication*, July 20-22, Rye Brook, NY, USA (pp. 1110–1119). Springer.

Kumar, S., Singh, S. K., Singh, A. K., Tiwari, S., & Singh, R. S. (2018). Privacy preserving security using biometrics in cloud computing. *Multimedia Tools and Applications*, *77* (9), 11017–11039. https://doi.org/10.1007/s11042-017-4966-5

Kumar, A., & Zhang, D. (2005). Personal authentication using multiple palmprint representation. *Pattern Recognition*, *38* (10), 1695–1704. https://doi.org/10.1016/j.patcog.2005.03.012

Ledala, A. J. (2021). *Combining Face and Iris for Privacy Preservation*. [PhD thesis]. Michigan State University.

Lee, C., & Kim, J. (2010). Cancelable fingerprint templates using minutiae-based bitstrings. *Journal of Network and Computer Applications*, *33*(3), 236–246. https://doi.org/10.1016/j.jnca.2009.12.011

Lee, J., Park, S., Kim, Y.-G., Lee, E.-K., & Jo, J. (2021a). Advanced authentication method by geometric data analysis based on user behavior and biometrics for iot device with touchscreen. *Electronics*, *10*(21), 2583. https://doi.org/10.3390/electronics10212583

Lee, M. J., Teoh, A. B. J., Uhl, A., Liang, S.-N., & Jin, Z. (2021b). A tokenless cancellable scheme for multimodal biometric systems. *Computers & Security*, *108*, 102350. https://doi.org/10.1016/j.cose.2021.102350

Le, T.-V., Lu, C.-F., Hsu, C.-L., Do, T. K., Chou, Y.-F., & Wei, W.-C. (2022). A novel three-factor authentication protocol for multiple service providers in 6g-aided intelligent healthcare systems. *IEEE Access*, *10*, 28975–28990. https://doi.org/10.1109/ACCESS.2022.3158756

Li, C., & Hu, J. (2014). Attacks via record multiplicity on cancelable biometrics templates. *Concurrency & Computation: Practice & Experience*, *26*(8), 1593–1605. https://doi.org/10.1002/cpe.3042

Liu, X., Si, Y., & Yang, W. (2021). A novel two-level fusion feature for mixed ECG identity recognition. *Electronics*, *10* (17), 2052. https://doi.org/10.3390/electronics10172052

Liu, C.-L., Tsai, C.-J., Chang, T.-Y., Tsai, W.-J., & Zhong, P.-K. (2015). Implementing multiple biometric features for a recall-based graphical keystroke dynamics authentication system on a smart phone. *Journal of Network and Computer Applications*, *53*, 128–139. https://doi.org/10.1016/j.jnca.2015.03.006

Mageshkumar, N., & Lakshmanan, L. (2023). Intelligent data deduplication with deep transfer learning enabled classification model for cloud-based healthcare system. *Expert Systems with Applications*, *215*, 119257. https://doi.org/10.1016/j.eswa.2022.119257

Maiorana, E., Campisi, P., Fierrez, J., Ortega-Garcia, J., & Neri, A. (2010). Cancelable templates for sequence-based biometrics with application to on-line signature recognition. *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, *40*(3), 525–538. https://doi.org/10.1109/TSMCA.2010.2041653

Malek-Podjaski, M., & Deligianni, F. (2021). Towards Explainable, Preserving privacy in human-motion affect recognition *Symposium Series on Computational Intelligence (SSCI)* (pp. 01–09). *arXiv preprint arXiv:2105.03958*.

Marcel, S., Nixon, M. S., Fierrez, J., and Evans, N., Marcel, S., Nixon, M. S., Fierrez, J., Evans, N. (2019). *Handbook of biometric antispoofing: Presentation attack detection*. Springer. https://doi.org/10.1007/978-3-319-92627-8

Martinez-Diaz, M., Fierrez-Aguilar, J., Alonso-Fernandez, F., Ortega-Garc´ıa, J., and Siguenza, J. A. (2006). Hill-climbing and brute-force attacks on biometric systems: A case study in match-on-card fingerprint verification. In *Proceedings 40th Annual 2006 International Carnahan Conference on Security Technology*, October 16-19, Lexington, Kentucky (pp. 151–159). IEEE.

Mateusz, C. (2020). Physical biometrics vs behavioral biometrics. Retrieved January 01 2020, from https://www.buguroo.com/en/blog/physical-biometrics-vs-behavioral-biometrics

Meenakshi, V., & Padmavathi, G. (2010). Security analysis of password hardened multimodal biometric fuzzy vault with combined feature points extracted from fingerprint, iris and retina for high security applications. *Procedia Computer Science*, *2*, 195–206. https://doi.org/10.1016/j.procs.2010.11.025

Mekruksavanich, S., & Jitpattanakul, A. (2021). Biometric user identification based on human activity recognition using wearable sensors: An experiment using deep learning models. *Electronics*, *10*(3), 308. https://doi.org/10.3390/electronics10030308

Merkle, J., & Tams, B. (2013). Security of the improved fuzzy vault scheme in the presence of record multiplicity (full version). *arXiv preprint arXiv:1312.5225*.

Microsoft (2006) Speaker verification: Text-dependent vs text-independent. Retrieved January 01, 2020, from https://www.microsoft.com/en-us/research/project/speaker-verification-text-dependent-vs-text-independent/

Mihailescu, P. (2007). The fuzzy vault for fingerprints is vulnerable to brute force attack. *arXiv preprint arXiv:0708.2974*.

Monaco, J. V., Ali, M. L., and Tappert, C. C. (2015). Spoofing key-press latencies with a generative keystroke dynamics model. In *2015 IEEE 7th international conference on biometrics theory, applications and systems (BTAS)*, September 25-28, Ljubljana, Slovenia (pp. 1–8). IEEE.

Monrose, F., & Rubin, A. D. (2000). Keystroke dynamics as a biometric for authentication. *Future Generation Computer Systems*, *16*(4), 351–359. https://doi.org/10.1016/S0167-739X(99)00059-X

Nait Hamoud, O., Kenaza, T., Challal, Y., Ben-Abdelatif, L., & Ouaked, M. (2022). Implementing a secure remote patient monitoring system. *Information Security Journal: A Global Perspective*, *32*(1), 21–38. https://doi.org/10.1080/19393555.2022.2047839

Nidhya, R., Kumar, M., Maheswar, R., & Pavithra, D. (2022). Security and privacy issues in smart healthcare system using internet of things. *IoT-Enabled Smart Healthcare Systems, Services and Applications*, 63–85.

Nowell, W. B., Curtis, J. R., Nolot, S. K., Curtis, D., Venkatachalam, S., Owensby, J. K., Poon, J. L., Calvin, A. B., Kannowski, C. L., & Faries, D. E. (2019). Digital tracking of rheumatoid arthritis longitudinally (digital) using biosensor and patient-reported outcome data: Protocol for a real-world study. *JMIR Research Protocols*, *8*(9), e14665. https://doi.org/10.2196/14665

Olzak, T. (2008). Keystroke logging (keylogging). *Adventures in Security, April*, *8*, 1–6.

Parks, R. F., Wigand, R. T., & Benjamin Lowry, P. (2022). Balancing information privacy and operational utility in healthcare: Proposing a privacy impact assessment (pia) framework. *European Journal of Information Systems*, 1–18. https://doi.org/10.1080/0960085X.2022.2103044

Patil, H. A. and Kamble, M. R. (2018). A survey on replay attack detection for automatic speaker verification (ASV) system. In *2018 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC)*, November 12-15, Honolulu, Hawaii, USA (pp. 1047–1053). IEEE.

Paul, P. P., Gavrilova, M. L., & Alhajj, R. (2014). Decision fusion for multimodal biometrics using social network analysis. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *44*(11), 1522–1533. https://doi.org/10.1109/TSMC.2014.2331920

Pinto, A., Pedrini, H., Krumdick, M., Becker, B., Czajka, A., Bowyer, K. W., & Rocha, A. (2018). Counteracting presentation attacks in face, fingerprint, and iris recognition. *Deep Learning in Biometrics*, *245*.

Praveen, G. and Dakala, J. (2020). Face recognition: Challenges and issues in smart city/environments. In *2020 International Conference on COMmunication Systems & NETworkS (COMSNETS)*, January 7-11, Bengaluru, India (pp. 791–793). IEEE.

Punithavathi, P., Geetha, S., and Sasikala, S. (2017). Generation of cancelable iris template using bi-level transformation. In *Proceedings of the 6th International Conference on Bioinformatics and Biomedical Science*, June 22 - 24, Singapore (pp. 94–100).

Purohit, H., & Ajmera, P. K. (2021). Multi-modal biometric fusion based continuous user authentication for e-proctoring using hybrid lcnn-salp swarm optimization. *Cluster Computing*, *25*(2), 827–846. https://doi.org/10.1007/s10586-021-03450-w

Rathgeb, C., & Busch, C. (2014). Cancelable multi-biometrics: Mixing iris-codes based on adaptive bloom filters. *Computers & Security*, *42*, 1–12. https://doi.org/10.1016/j.cose.2013.12.005

Rathgeb, C. and Uhl, A. (2010). Attacking iris recognition: An efficient hill-climbing technique. In *2010 20th International Conference on Pattern Recognition*, August 23-26, Istanbul, Turkey (pp. 1217–1220). IEEE.

Rigas, I., Abdulin, E., & Komogortsev, O. (2016). Towards a multi-source fusion approach for eye movement-driven recognition. *Information Fusion*, *32*, 13–25. https://doi.org/10.1016/j.inffus.2015.08.003

Roberts, C. (2007). Biometric attack vectors and defences. *Computers & Security*, *26*(1), 14–25. https://doi.org/10.1016/j.cose.2006.12.008

Rodrigues, R. N., Ling, L. L., & Govindaraju, V. (2009). Robustness of multimodal biometric fusion methods against spoof attacks. *Journal of Visual Languages & Computing*, *20*(3), 169–179. https://doi.org/10.1016/j.jvlc.2009.01.010

Ross, A., Jain, A., & Reisman, J. (2003). A hybrid fingerprint matcher. *Pattern Recognition*, *36*(7), 1661–1673. https://doi.org/10.1016/S0031-3203(02)00349-7

Sanchez-Reillo, R., Quiros-Sandoval, H. C., Goicoechea-Telleria, I., & PonceHernandez, W. (2017). Improving presentation attack detection in dynamic handwritten signature biometrics. *IEEE Access*, *5*, 20463–20469. https://doi.org/10.1109/ACCESS.2017.2755771

Sarala, S. M., Karki, M. V., and Yadav, D. S. (2016). Blended substitution attack independent; fuzzy vault for fingerprint template security. In *2016 International Conference on Circuits, Controls, Communications and Computing (I4C)*, October 4-6, Bangalore, India (pp. 1–6). IEEE.

Sawa, M., Inoue, T., & Manabe, S. (2022). Biometric palm vein authentication of psychiatric patients for reducing in-hospital medication errors: A pre–post observational study. *British Medical Journal Open*, *12*(4), e055107. https://doi.org/10.1136/bmjopen-2021-055107

Scheirer, W. J. and Boult, T. E. (2007). Cracking fuzzy vaults and biometric encryption. In *2007 Biometrics Symposium*, September 11-13, Baltimore, Maryland (pp. 1–6). IEEE.

Shelton, J., Roy, K., O'Connor, B., & Dozier, G. V. (2014). Mitigating iris-based replay attacks. *International Journal of Machine Learning and Computing*, *4*(3), 204. https://doi.org/10.7763/IJMLC.2014.V4.413

Shouran, Z., Ashari, A., & Priyambodo, T. (2019). Internet of things (iot) of smart home: Privacy and security. *International Journal of Computer Applications*, *182*(39), 3–8. https://doi.org/10.5120/ijca2019918450

Shrawankar, U., & Thakare, V. M. (2013). Techniques for feature extraction in speech recognition system: A comparative study International Journal Of Computer Applications In Engineering, Technology and Sciences (IJCAETS) pp 412–418 . *arXiv preprint arXiv:1305.1145*.

Singh, M., Singh, R., & Ross, A. (2019). A comprehensive overview of biometric fusion. *Information Fusion*, *52*, 187–205. https://doi.org/10.1016/j.inffus.2018.12.003

Smith, D. F., Wiliem, A., & Lovell, B. C. (2015). Face recognition on consumer devices: Reflections on replay attacks. *IEEE Transactions on Information Forensics and Security*, *10*(4), 736–745. https://doi.org/10.1109/TIFS.2015.2398819

Spiekermann, S. (2012). The challenges of privacy by design. *Communications of the ACM*, *55*(7), 38–40. https://doi.org/10.1145/2209249.2209263

Srikanth, G. U., & Jaffrin, L. C. (2022). Security issues in cloud and mobile cloud: A comprehensive survey. *Information Security Journal: A Global Perspective*, *31*(6), 686–710. https://doi.org/10.1080/19393555.2022.2035470

Stoianov, A., Kevenaar, T., and der Veen, M. V. (2009). Security issues of biometric encryption. In *2009 IEEE Toronto International Conference Science and Technology for Humanity (TIC-STH)*, September 26-27, Toronto, Ontario, Canada (pp. 34–39). IEEE.

Sudharsan, B., Corcoran, P., & Ali, M. I. (2019). Smart speaker design and implementation with biometric authentication and advanced voice interaction capability. *AICS*, 305–316.

Sun, Y., & Lo, B. (2018). An artificial neural network framework for gait-based biometrics. *IEEE Journal of Biomedical and Health Informatics*, *23*(3), 987–998. https://doi.org/10.1109/JBHI.2018.2860780

Tognetto, D., Pastore, M. R., De Giacinto, C., Merli, R., Franzon, M., D'Aloisio, R., Belfanti, L., Giglio, R., & Cirigliano, G. (2019). Swept-source optical coherence tomography biometer as screening strategy for macular disease in patients scheduled for cataract surgery. *Scientific Reports*, *9*(1), 9912. https://doi.org/10.1038/s41598-019-46243-3

Tolosana, R., Gomez-Barrero, M., Busch, C., & Ortega-Garcia, J. (2019). Biometric presentation attack detection: Beyond the visible spectrum. *IEEE Transactions on Information Forensics and Security*, *15*, 1261–1275. https://doi.org/10.1109/TIFS.2019.2934867

Tumpa, S. N., & Gavrilova, M. L. (2020). Score and rank level fusion algorithms for social behavioral biometrics. *IEEE Access*, *8*, 157663–157675. https://doi.org/10.1109/ACCESS.2020.3018958

Uludag, U., & Jain, A. K. (2004). Attacks on biometric systems: A case study in fingerprints. In *Security, steganography, and watermarking of multimedia contents* (Vol. VIVol. 5306, pp. 622–633). International Society for Optics and Photonics.

Uniphone. (2018). Voice Biometrics. *uniphore*. Retrieved January 01, 2020, from https://www.uniphore.com/glossary/voice-biometrics/#

Vittori, P. (2019). Ultimate password: Is voice the best biometric to beat hackers? *Biometric Technology Today*, *2019*(9), 8–10. https://doi.org/10.1016/S0969-4765(19)30127-4

Wang, Y., Meng, W., Li, W., Li, J., Liu, W.-X., & Xiang, Y. (2018). A fog-based privacy-preserving approach for distributed signature-based intrusion detection. *Journal of Parallel and Distributed Computing*, *122*, 26–35. https://doi.org/10.1016/j.jpdc.2018.07.013

Wesolowski, T. E., Porwik, P., & Doroz, R. (2016). Electronic health record security based on ensemble classification of keystroke dynamics. *Applied Artificial Intelligence*, *30*(6), 521–540. https://doi.org/10.1080/08839514.2016.1193715

Wickramaarachchi, W. U., Alhaj, Y. A., and Gunesekera, A. (2019). Effective privacy preserving iris recognition. In *2019 IEEE 4th International Conference on Image, Vision and Computing (ICIVC)*, July 5-7, Xiamen, China (pp. 421–426). IEEE.

Wu, Z., Kinnunen, T., Chng, E. S., Li, H., and Ambikairajah, E. (2012). A study on spoofing attack in state-of-the-art speaker verification: The telephone speech case. In *Proceedings of The 2012 Asia Pacific Signal and Information Processing Association Annual Summit and Conference*, December 3-6, Hollywood, California, USA (pp. 1–5). IEEE.

Zhang, Y., Zhang, Y., Li, Y., & Wang, C. (2015). Strong designated verifier signature scheme resisting replay attack. *Information Technology and Control*, *44*(2), 165–171. https://doi.org/10.5755/j01.itc.44.2.7625

Zhao, D., Luo, W., Liu, R., & Yue, L. (2015). Negative iris recognition. *IEEE Transactions on Dependable and Secure Computing*, *15*(1), 112–125. https://doi.org/10.1109/TDSC.2015.2507133

Zheng, X., Zheng, F., Liu, X., Wang, D., Wang, J., & Meng, B. (2021). A secure and policy-controlled signature scheme with strong expressiveness and privacy-preserving policy. *IEEE Access*, *9*, 14945–14957. https://doi.org/10.1109/ACCESS.2021.3052463

Zola Matuvanga, T., Johnson, G., Larivi`ere, Y., Esanga Longomo, E., Matangila, J., Maketa, V., Lapika, B., Mitashi, P., McKenna, P., De Bie, J., Van Geertruyden, J.-P., Van Damme, P., & Muhindo Mavoko, H. (2021). Use of iris scanning for biometric recognition of healthy adults participating in an Ebola vaccine trial in the democratic republic of the Congo: Mixed methods study. *Journal of Medical Internet Research*, *23*(8), e28573. https://doi.org/10.2196/28573