Available Online at http://www.journalajst.com

ASIAN JOURNAL OF SCIENCE AND TECHNOLOGY

ISSN: 0976-3376

Asian Journal of Science and Technology
Vol. 14, Issue, 08, pp. 12636-12649, August, 2023

RESEARCH ARTICLE

ATTACKS AGAINST BIOMETRIC AUTHENTICATION IOT SYSTEM: A REVIEW, TAXONOMY AND OPEN CHALLENGES

***Joshua Teddy Ibibo**

School of Computing, Edinburgh Napier University 10 Colinton Rd, Edinburgh EH10 5DT, United Kingdom

ARTICLE INFO

Article History:
Received 17th May, 2023
Received in revised form
06th June, 2023
Accepted 24th July, 2023
Published online 30th August, 2023

Keywords:
Biometric authentication, Attacks, Biometrics, Attack detection, IoT.

ABSTRACT

Nigeria he interest in biometric technology is received much attention in the recent years. However, the security issue still persists the main challenge for the reliable functioning of biometric authentication systems (BAS). Much academic research has been reported on the vulnerabilities of biometric systems that breach the se-curity and user privacy in mobile devices. We present a high-level classication of taxonomy of attacks against BAS and discuss the severity of attacks on the BAS for mobile computing device. We present a multidimensional taxonomy of the biometric systems that includes Human factor, Software and hardware attacks, BAS threat models and countermeasures for mobile computing devices are also discussed. We point out the aws and limits of the current BAS for mobile computing devices throughout. We describe the research diculties and suggest directions for future research eorts in BAS using the present taxonomy. Our main contributions include: (1) a comprehensive taxonomy of the charac-teristics of biometrics authentication system approaches (2) systematic review of the landscape of existing biometrics authentication system approaches towards their categorization and classication, following the proposed taxonomy, for the aforementioned application domains (3) Classication of countermeasures and biometric system defences (4) Biometric authentication system failure (5) We examine the challenges of biometrics authentication system techniques and sug-gest future research paths.

Citation: ***Joshua Teddy Ibibo.*** **2023.** "Potentials of inter- coastal movement of goods in selected local government areas of akwa ibom state", *Asian Journal of Science and Technology*, 14, (08), 12636-12649.

INTRODUCTION

In today's world, there are an increasing number of situations in which our identication must be proven with certainty. People commonly identify with a password, a passport, or a social security number are frequently used. However, because such measures are continuously at risk of being lost, stolen, or falsied, the link between them and a person can be weak. Biometrics, which are a person's unique biological or behavioural traits, such as their face, ngerprint, iris, speech, and so on, is one of the most popular and promising solutions to this problem. Biometrics is both convenient and reliable because it is the only kind of authentication that conrms the user's actual presence. The usage of authentication technology to get access to Internet services and IoT devices has been around for a long time. They can be used to protect user devices, accounts, and content, especially if the user has several accounts on dierent apps. This type of user demands the usage of password management software, which is a time-consuming operation. Because of their particular properties, Biometric Authentication Systems (BASs) have been presented as a solution to these issues. Biometric traits that dier from one person to the next can be used to authenticate a person's identity instead of a standard password [1]. To secure user data, a cloud software vendor reported data stolen by hackers in early 2013 [2], forcing the company's 50 million users to reset their passwords and enter twice using dierent passwords for dual authentication. Because it is impossible to ensure the security of personal data using traditional encryption and decryption methods, digital identity verication based on unique physio-logical recognition technology has grown in popularity.

To conrm an individual's identication, traditional authentication approaches such as passwords, pin numbers, token numbers, and ID cards have been utilised. Passwords or pin numbers must be remembered by the user. As a result, an adversary can forged, steal, or compromise these techniques of identity manage-ment. Biometrics has an edge over traditional authentication schemes in that it determines an individual's identity based on physiological or behavioural char-acteristics. Fingerprints, facial features, iris, hand geometry, voice, signature, and other characteristics are examples of these traits. As a result, users do not need to memorise any passwords, pin numbers, or carry any tokens or ID cards to prove identity with biometrics. Biometric features have a lot of ad-vantages that make them valuable as authentication tokens, such as reliability, ease, universality, and so on. These traits have resulted in BAS well-known operation. There are still several diculties with biometric identication systems' secu-rity that need to be addressed in order to ensure its integrity and public accep-tance. Sensor, feature extractor, template database, matcher, and decision mod-ule are the ve main modules of a conventional BAS [3]. The US Federal Trade Commission reports that ID theft aects millions of innocent victims each year and is the most common consumer complaint (www.ftc.gov/opa/reporter/idtheft /index.shtml). Biometric systems have grown more economical and easy to install in a range of consumer gadgets as a result of rapid advancements in sensor and computer technologies, rendering them vulnerable to terrorists' and criminals' malevolent designs. Vulnerabilities in the biometric system must be detected and xed in a systematic manner in order to avoid any future security issues. A number of research [4, 5, 6, 7, 8] have looked into potential security aws in BAS and provided ways to prevent them. Attack trees [9] and other formal vulnerability research approaches have been used to

investigate how BAS security can be hacked. According to Javelin Strategy & Research, 12.7 million people were victims of identity theft in the United States alone in 2014, stealing 16 billion dollars [10], this gure is estimated without accounting for the nancial diculties and psychological trauma that victims of this fraud face. During enrollment, a biometric system captures a sample of a user's bio-metric attribute using an appropriate sensor [11], for example, a camera for the face. It then uses a software algorithm known as a feature extractor to extract important properties from the biometric sample, such as ngerprint minutiae. These extracted attributes are stored in a database as a template alongside other identiers such as a name or an identifying number. The user must give another biometric sample to the sensor in order to be authenticated. The query is made up of features derived from this sample, which the system then compares to the template of the claimed identity using a biometric matcher. The matcher produces a match score that indicates how similar the template and the query are. Only if the match score exceeds a predetermined threshold does the system accept the identication claim.

Contribution: The goal of this research is to oer a full analysis and taxonomy of the sorts of assaults against the entire BAS, which has been motivated by these issues. In this context, we address the early taxonomies' inherent limitations by proposing a new, comprehensive categorization that encompasses both old (pre-2021) and newer (post-2021) research areas, as well as potential future research areas in a comprehensive landscape of adversarial computing mobile devices. We use this taxonomy to survey and classify the various approaches available, with a focus on those given in the recent two years, and to determine which areas would benet greatly from additional research. In summary, the rest of the research paper is systematized as follows:

1. a comprehensive taxonomy of the characteristics of BAS approaches (Sec-tion 1)
2. systematic review of the landscape of existing BAS approaches towards their categorization and classication, following the proposed taxonomy, for the aforementioned application domains (Section 2)
3. Methodology, Aims Objectives (Section 3)
4. Classication of countermeasures and biometric system defences (Section 4)
5. Biometric authentication system failure (Section 5)
6. Then, in Section 6, we examine discussion and collusion.

Our primary goal in having conducted this investigation is to elucidate on this emerging attack approach so that it can be used as a baseline for the development of more robust countermeasures, and so that BAS can provide enhanced security and privacy capabilities that will help accelerate data-driven insights and knowledge acquirement.

Background: A biometric recognition system is an authentication method [12] that can identify an individual based on their biometric characteristics. A traditional biometric framework consists of four modules [13]:

Biometric sensor Device: The biometric sensor is an important component of a biometric recogni-tion device. The biometric sensor's behaviour is to capture the biometric picture. The role of the sensor is to scan the visible biometric image and store it in the biometric device. With the aid of a biometric sensor, the user may communicate with the biometric recognition device [7, 14].

Feature extraction Device: The biometric recognition system includes a feature extraction compo-nent. The feature extraction device's job is to extract the relevant and qualitative areas of a biometric image that can be used to identify a spe-cic person. Since biometric images have a number of issues, such as areas that are over-inked and areas that are under-inked. This problem is no longer an issue thanks to the biometric extraction device. The template was then saved in a database [15].

Biometric matcher Device: A biometric recognition system includes a biometric matcher device. The job of a biometric matcher is to match biometric features, compare them, and provide an output result in the form of a match score. The score indicates how close the two biometric images [14].

Decision- making Device: The prototype dataset is usually created during registration, when a user rst interacts with the system, and it is refreshed or modied over time to account for intra-class dierences [16]. The Deci-sion module is a Matcher module that determines if two biometric images are connected. Enrolment and verication or authentication are the two modes of operation for a standard biometric recognition scheme (see Fig-ures 1).

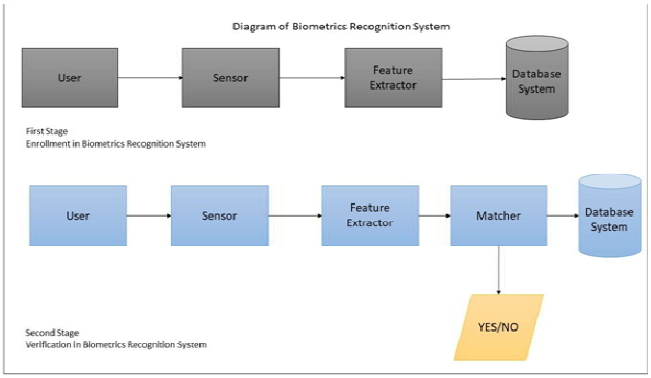

Figure 1. Biometric Recognition System

Competing Surveys: There have been few survey articles published in the last several years that deal with biometrics authentication. Table 1 shows how these survey articles are organised. Ratha et al. present a new remote authentication approach that combines the threat of a smartcard with the accuracy and simplicity of biometrics to verify a person's identication. This method eliminates the requirement for a big biometrics database [17]. Nalini et al. analyzed a pattern recognition-based threat model of a biomet-rics authentication system, this paper describes secure ngerprint authentica-tion. Several solutions are proposed to alleviate the threats using conventional encryption as well as novel techniques that exploit the richness of biometrics data [18]. [19] provides a brief overview of the various types of authentication and iden-tity management systems available. It tries to summarise a number of relevant works, including some of the most recent face and ngerprint recognition tech-niques. With a better understanding of electronic authentication techniques any organization can properly select and utilize the technologies which meet its needs. In modern days [20], the demand for stronger and more dependable user authentication procedures has exacerbated economic issues, as has the rapid improvements in networking, communication, and mobility. Biometrics is an example of an authentication mechanism that aids in the verication of system users. Biometric technologies are fast becoming the backbone of highly secure identication and personal verication systems. In [21], Velasquez et al. presented existing authentication mechanisms and procedures in order to determine which ones are most eective in various situ-ations. In [22], I. La Polla et al. presented a survey on computing mobile device authentication. They began by outlining various types of mobile malware and attempting to distinguish between attack solutions for cellphones and traditional PCs.They also discussed smartphone threats by examining the various method-ology that may be utilised to conduct an attack in a mobile environment and explaining how these approaches can be exploited for various goals. The au-thors propose solutions based on their investigation, which was completed in 2013, with an emphasis on intrusion detection systems and trusted platform technologies. In 2015, Yanushkevich et al. [23] published a Taxonomy and Modeling of Impersonation in e-Border Authentication. The focus of this paper is authenti-cation machines for border crossing applications (e-borders). A novel taxonomy of impersonation and seven impersonation strategies for border crossing control computing device applications are proposed.

Passwords and PINs are authentication solutions with numerous limitations, Meng et al. [15] Kunda and Chishimba [24] undertook a detailed investigation into biometric-based approaches for mobile phone authentication. The authors included both physiological and behavioural approaches in their survey arti-cle, examined their practicality of deployment on touch-enabled mobile phones, and identied attack spots and their related countermeasures. Based on their ndings, they believe that a hybrid authentication mechanism that combines multimodal biometric authentication with standard PINs or passwords can im-prove the system's security and usability. Active authentication approaches, which constantly monitor the user's behaviour, are used to improve the security and privacy of mobile devices. Xi et al. [25] oered an idea based on transforming the locally matched fuzzy vault index to the central server for biometric authentication utilising the public key infrastructure to avoid the biometric template attack. In contrast to [26], [27], and [28], Chen et al. [29] developed a method for solving the asynchronous problem on mobile devices that simply uses hashing algorithms on ngerprint biometric remote authentication schemes. Khan et al. [30] updated Chen et aland .'s Truong et alschemes .'s with faster erroneous password detection in 2014, however they did not include location privacy. Biometrics provide the following benets: 1) they cannot be lost or forgot-ten, 2) they are exceedingly dicult to copy or share, 3) they are extremely dicult to counterfeit or distribute, and 4) they are tough to guess. In order to achieve non-repudiation, Li and Hwang [31] suggested a biometric-based remote user authentication scheme based on smart cards in 2010. The Li and Hwang technique [31] can withstand masquerade attacks, replay attacks, and parallel session attacks because no password and identity tables are stored in the sys-tem. The authors did not specify the scheme's application environment, but because the network architecture is not too sophisticated, it can be deployed to mobile computing devices. It's worth noting that Li and Hwang's plan has been decrypted multiple times. To our knowledge, this is the rst research in the eld of biometrics au-thentication to comprehensively cover the features of threat models, security analysis methodologies, spoong attacks, biometrics system defences and Tax-onomy of Biometric authentication attacks, that have recently been proposed by the research community.

Table 1. A Summary of Related Survey Papers

Reference	Threat Models	Countermeasures	Authentication Schemes	Biometrics
Ratha et al. (1996) [17]	V	S	V	V
Nalini et al. (2002) [18]	X	X	V	V
Mastal et al. (2002) [19]	V	X	V	V
Bala & Deepthi. (2008) [20]	X	V	V	V
Vel et. al. (2018) [21]	X	S	V	V
La Polla et al. (2012) [22]	V	X	V	V
Yanushkevich et al. (2015) [23]	X	X	V	V
Meng et al. (2014) [15]	X	X	V	X
Kunda et al. (2018) [24]	V	X	V	V
Xi et al. (2011) [25]	X	X	V	V
Park et al. (2010) [26]	V	X	V	X
Khan et al. (2008) [27]	V	X	V	V
Tasia et al. (2014) [28]	V	X	V	V
Chen et al. (2012) [29]	X	S	V	X
Khan et al. (2014) [30]	X	S	V	X
Li & Hwang (2010) [31]	X	X	V	V
Our work	V	V	V	V

Note: Indicates fully supported; X: indicates not supported; S: indicates partially supported.

Proposed taxonomy: We divided the taxonomy into four phase for the sake of this paper: Prove-nance, Attack Domain, Attack Specicity, and Attacks as shown in gure 2.

Provenance Phase: The inception of our taxonomy, is the identication of the provenance of the attacks against Fig Biometric Authentication Systems. This step is consid-ered fundamental for our proposed taxonomy it describes on a high level where the attacks come from, thus detailing at the same time the threat landscape. More specically, the provenance of the attacks against BAS is detailed in the following categories:

1. **Software:** Software-based solutions do not require unique sensors to deter-mine liveness; instead, they use the ordinary camera/microphone found on today's commodity smartphones. As a result, in mobile-based FR, software-based approaches are most typically utilised for liveness identi-cation. Some software-based solutions gather numerous photographs of the user at various distances from the mobile device, generate a "3D im-age" from these 2D maps, and match it to the registered prole, ensuring robustness against image/video attacks. The most prevalent software-based techniques, on the other hand, ask the user to do a certain action (such as a head movement, blinking, or uttering a pre-dened phrase) and then determine whether or not the challenge was appropriately answered by analysing the audio/video that results. A positive response to such a challenge is a clear sign of vitality [26].

Hardware: Hardware is the part of the BAS that identify the presence of life in the subject using specialised sensors. These sensor-based systems employ a range of techniques, including depth mapping and 3D sensing; sensors that measure and compare the reectance information of genuine and fake faces; thermal imaging sensors; and sensors that identify facial vein patterns. These kinds of solutions are far more common in customised high-end FR systems like those seen in airports and border security. How-ever, the sensors' high cost prevents them from being used for liveness detection in the bulk of consumer mobile devices. Due to sensing technol-ogy limitations or bad environmental conditions, a sensor may occasionally fail to acquire a user's biometric feature. A ngerprint sensor, for example, might not be able to capture a decent quality ngerprint of dry or moist ngertips. Failure-to-enroll (FTE) or failure-to-acquire (FTA) problems result [25].

Human Factor: The human factor we may say insider attack where all vulnerabilities could be encounter all because of improper administration of BAS because the system administrator has the privileges to register the biometric template and make the exceptions for the individual whose biometric sample cannot be obtained by the system due to some injury or disease [4].

Attack Domain Phase: As a way, the attack domain has genuine aws and the capacity to be used as a vector for attacks. An Attack Domain is one in which a bad actor either attempts to breach a biometrics

system or exploits its inherent haracteristics to launch a broader attack.

1. Privileged Access: Privileged access describes how someone mistakenly forget his/her credentials and an attacker mount a successful attack or instigate enrollment fraud or exception misuse on the sytem [5].

2. User Level: A user can intentionally or unintentionally harm a system. An administrator, for example, may install or congure the biometric system incorrectly, resulting in an ineective mechanism [6].

3. Non-Sensor Related Components: Non-sensor related components are those hardware parts of the sensor that suppose the sensor to perform its func-tions accurately such as Smart-card assisted hardware, such as System-on-Card, Match-on-Card, optical sensors, notebook Thinkpad T42 models and capacities sensors [7].

4. Sensors: Biometric sensors capture measurable biological traits (biometric signals) from humans, which can then be utilised with biometric recogni-tion algorithms to accomplish automated person identication [8].

5. Application Programming Interface (APIs): Application Programming In-terface (API) is a collection of connected programmable functions and processes that enable you to add a certain operation or feature to a soft-ware application. A Biometric API is a set of functions and procedures that help you integrate biometrics into your software [5]. Biometrics En-rollment and Biometrics Authentication are two biometrics features that you might want to incorporate into your software application with the use of a biometrics API.

6. Biometrics Templates: The core samples of a BAS identity acquired from the enrolled population for authentication are known as templates. When the templates are stolen from the database, the biometric identication of an individual is not a digital certicate that may be given by a third party. Individuals' iris codes, for example, are used to authenticate individuals using an iris-based recognition system. If the iris code templates are stolen, the users' sole option is to use the iris of another eye [20]. If a voice print is stolen by an adversary in a voice recognition system, it remains stolen for the rest of the user's life, and the user's identity can never be restored to a secure state. When a legitimate user's template is attacked by an adversary, several scenarios have been reported. An adversary can substitute a fake template for the genuine template, allowing the adversary to gain access to the system. An attacker can change or corrupt a valid template that results from a DoS to a legitimate user. As an example, a ngerprint template stolen from a bank's database may be used to search a criminal ngerprint database or cross-link to a person's health records [32].

Attack Specicity Phase: A specic area that seeks to allow an attack on the biometric system. An indiscriminate attack, on the other hand, causes widespread chaos on the system.

1. Attack against Machine Learning: Attackers can inuence the decision-making algorithms of such systems by targeting the data sets or compelling the model to provide the desired output, such as the mis-classication of anomalous occurrences. Poisoning and evasion attacks [33] let attackers to reduce overall performance, cause targeted mis-classication or bad behaviour, and introduce system vulnerabilities attacks [34].

2. Development Errors: The development process is halted if a development error occurs before the system is accepted for use and put into operation. Inecient imaging, incorrect data representation, or improper matching can cause it at any level of system design. The majority of development errors are caused by an inaccurate or erroneous assessment of the system's complexity. Inadequate design in terms of functionality or performance goals, defective or incomplete specications, insucient fault elimination capability, and incorrect development cost estimates are just a few exam-ples [25]. Interaction with the use environment causes BAS development faults. Software ageing, data corruption, and storage space fragmentation are examples of some development aws. Some errors are caused by human activities, such as failing to act when action is required or purposely conducting incorrect actions; these are human-caused errors.

3. Third-Party: This third party veries the identity of the user who has to be enrolled in the biometrics template [35].

4. Sensor Production Errors: These errors are primarily caused by sensor malfunctions at the production or manufacturing level, where security vulnerabilities occur and will aect the functionality of the sensor [15].

5. Sensor Design Errors: Infrastructure causes include system design defects that make the system susceptible to adversary attacks. The hardware components such as the sensor, the software implemented at the feature extraction module and matcher module along with the communication channel between various system components form the infrastructure of the biometric system [36].

6. Social Engineering: Computer hackers use social engineering to get users to divulge their passwords or other sensitive information. A single most eective strategy for assaulting a corporation with robust security mech-anisms is a denial-of-service attack. This type of malicious actor is con-stantly in the headlines, driving us to invest in new technology to prevent their attacks and strengthen our network defences [37].

7. Impersonation: Impersonation is a procedure in which an unauthenticated user claims an identity, which is then veried in BAS by matching a stored biometric signature to the user's previously presented biometric features [3].

8. Maintenance Errors: Maintenance Errors in BAS are when an authorised user in the system tries to update entries in the BAS database or software without realising it, causing serious system disruptions [37].

9. Malicious Insider Threats: Malicious threats have the goal of causing harm to the BAS, and the user is unaware of or does not intend to harm the system. Malicious threats are the outcome of poor decisions. Malicious threats can include Trojan horses, trap doors, logic bombs, viruses, and worms. Because interaction threats occur during a system's use phase, they are all operational aws such as incorrect system parameter settings that might impair the performance, storage, networking, security, and privacy [38].

Attack Phase: This is part of the taxonomy where dierent attacks are lunched on the attacks against Biometric Authentication System.This stage is critical for our proposed taxonomy since it identies where the attacks aect the BAS on a high level, outlining the threat landscape at the same time. More specically, the attack phase of BAS attacks is broken down into the following areas.

1. Insider Attack: An insider attack on the biometric system can be aided by the system administrator or another authorised individual. The ad-ministrator informs the attacker about the system's weaknesses or the legitimate user assists in the execution of such assaults. In a collision situation, the attacker is a valid user with full access privileges, such as the system administrator. He gains unauthorised access to and changes system parameters, such as the predened threshold. An approved user's access rights can be changed by the attacker [38]. As an enrolled user, the system administrator assisted the attacker in accessing the system. The specied threshold is reset to a lower number by the system administrator, allowing the adversary to take advantage of the false match mistake and gain authorization. The BAS should have many system administrators,

each with distinct levels of access, so that an insider attack, such as collu-sion and exception abuse, cannot be carried out by a single authority. To avoid the likelihood of enrollment fraud, an organisation can delegate en-rollment duty to several divisions. Every employee whose document-based verication is undertaken by another department can be issued a smart-card cum identity card by one department [39]. This card can be used by a third department to save his biometrics on the card itself (during the enrolment procedure).

2. ***Negligence:*** While the attacker is observing him, a legitimate user may forget to log out of the biometric programme. The adversary takes advan-tage of such a lapse of judgement. He can carry out more transactions or even access sensitive information about the user if he continues the session as an authorised user [40].

3. Presentation Attack (PA): An impostor uses an artifacts of some type to impersonate an individual who has been registered in the system, which isknown as a presentation attack also known as spoong attack [41, 42, 43, 44, 45]. Based on the user intent, there are few classes can be dened as PA; Fingerprint presentation attack, face presentation attacks and video reply attacks [46], 3D mask attacks [47] and photo attacks [48, 46]. For example, by taking a high-resolution picture of their face, ngertip, or iris, or recording their voice, and then utilising that to generate a copy picture (2D or 3D), which can subsequently be used as a mask or overlay by an impostor. Diamonds are Forever, released in 1971, featured James Bond deceiving a (rudimentary) ngerprint scanner with latex overlays, as well as using a voice impersonation device: notions that were allegedly beyond the CIA's own thinking at the time [49]. To interfere with the capture device's intended behaviour, the attacker can simply present it with a presentation attack instrument (PAI), such as a gummy nger or a ngerprint overlay. The primary purpose may be to imitate someone else (active impostor) or to escape detection (i.e., identity concealer). These assaults are referred to as presentation attacks in ISO/IEC 30107 [5] (PAs) [50, 51]. The biometric capture device is most likely the most vulnerable: the at-tacker does not need to know anything about the inner workings of the biometric system to attack the sensor. He can provide the capture de-vice with a Presentation Attack Instrument (PAI), such as a 3D mask, a printed nger vein picture, or a ngerprint overlay, to mislead the bio-metric system. These are referred to as Presentation Attacks (PA).

4. Phishing: Phishing is today's most popular sort of social engineering as-sault. But, exactly, what is it? Most phishing schemes aim to do three things: get personal information such as names, addresses, and Social Security numbers, and Use truncated or deceptive links that lead to sus-picious websites with phishing landing pages. Use threats, anxiety, and a sense of urgency to get the user to reply swiftly [52].

5. Swamping attack: Attempts to nd matches for inaccurate data by ex-ploiting a aw in the algorithm. For instance, in a ngerprint system, an attacker would try to submit a print with a lot of minutiae in the hopes that the threshold number N of them matches the stored template. The algorithm's aw is that it allows such a representation to be used [53].

6. Overloading Attack: Overloading attack is an attempt to defeat or cir-cumvent a system by damaging the input device or overwhelming it in the attempt to generate errors. This is also sometimes called a buer overow attack for other security mechanisms [54]. An example of this type of attack for a biometric system would be the rapid ashing of bright lights against optical ngerprint sensors or facial recognition capture devices can disrupt their proper functioning. Silicon sensors can be easily damaged by short circuiting them or dousing them with water. Although many biomet-ric systems rely on sensitive equipment that can be quickly overwhelmed, users may have possibilities to cause device or system failure. Basic func-tions must not fail if a system is overburdened. When biometric devices can no longer perform their intended function, fallback procedures must be devised and implemented. A person who causes a biometric system to fail may be aware that as a result, an unguarded door may be exploited as a temporary alternative means of admission. Security systems must accommodate for the potential functional failure of biometric systems and devices by implementing suitable backup mechanisms.

7. Hill-climbing: The communication interfaces between separate modules can be sabotaged or intruded upon by an attacker. He could, for example, position an interfering source close to the communication channel (e.g., a jammer to obstruct a wireless interface). An attacker may intercept and/or manipulate data being conveyed if the channel is not physically or cryptographically secured. An e-passport application that uses biometric authentication, for example, described the security and privacy diculties caused by insecure communication channels. Hill-climbing attacks are also possible due to insecure communication connections [55].

8. Intrinsic Failure: Intrinsic failure is caused by a aw in the BAS sen-sor, feature extraction, or matching technology. The biometric matcher module makes the wrong decision due to intrinsic failure. The biomet-ric verication system makes two types of errors while using the decision matcher module: A false accept rate (FAR) or false match error rate (FMER) species the proportion of cases (or the probability with which) the system accepts an invader (non-enrolled) user. It is the ratio of non-enrolled users' attempts to the matching score when the system accepts some of them as authorised users. The false non-match error rate (FRR) is the percentage of cases (or the probability with which) the system re-jects a valid user. When the system rejects some of the enrolled users as unauthorised users, it is the ratio of the number of tries made by enrolled users to the matching score [56, 39]. When no explicit eort is made by a third party, intrinsic failures can occur. This is known as a zero eort attack. When the likelihood of erroneous accept and reject is large, it can provide an issue. As a result, the goal is to develop sensors that can reduce inherent failure while also being dependable, practical, and secure.

9. Material deciency: A material deciency in sensor production error over BAS, causing errors at the production or manufacturing level, where secu-rity risks develop and inuence the functionality of manufactured devices [57].

10. Denial of Service: Denial-of-service refers to a situation in which a genuine user is denied access to a service to which he is entitled. An attacker can disable the infrastructure (for example, by physically damaging a nger-print sensor), preventing users from accessing the system and a server that processes access requests can be bombarded with a large number of bogus requests, thereby overloading its computational resources and preventing valid requests from being processed [58].For a BAS, an online authentica-tion server that processes access requests (by retrieving templates from a database and matching them against transferred biometric data) can be assaulted with so many fake access requests that the server's processing resources can no longer accept real requests. In most cases, these attacks are recognised within a short period. However, in some circumstances, the goal is to draw attention to the attack to cause confusion and panic, causing alternative or exception handling methods to be activated [59]. DOS attacks have gained a lot of attention in the media in recent years, and they should be regarded a very real threat to biometric authentica-tion systems as well. Trac analysis and trac monitoring are prominent strategies for thwarting DOS attacks.

11. Enrollment Integrity Attack: This attacks only have an impact on tem-plates that have been saved in the system. The majority of the enrollment processes take place in a secure environment with additional security mea-sures in place for identication. When high levels of security are necessary, a third party, such as government workers or any other party trusted by the system issuer and user, is frequently involved [60]. The enrolment procedure could be hacked, allowing for the acceptance of false enrolment data.

Table 2. Comparative analysis of Presentation attacks on BAS

Reference	Threat Models	Counter measures	Authentication Schemes	Bimetrics	Experimental Results
Yanushkevich et al.(2015)[23]	X	V	X	V	V
Meng et al. (2014) [15]	V	S	V	V	V
Kunda et al. (2018) [24]	V	V	V	V	V
Xi et al. (2011) [25]	V	X	S	V	X
Park et al. (2010) [26]	X	V	V	V	X
Khan et al. (2008) [27]	X	V	V	V	X
Storisteanu et al. (2016) [95]	V	X	V	V	X
Akhtar et al. (2018) [96]	X	X	S	V	V
Hadid et al. (2015) [98]	V	V	V	V	V
Singh et al. (2012) [99]	V	V	X	V	V
Mastali & Agbinya (2010) [1]	V	V	X	V	V
Liu Yi (2021) [2]	V	V	X	V	V
Uludag & Jai (2004) [3]	X	X	V	V	V
Jain et al. (2006) [4]	V	X	S	V	X

Table 3. Comparative analysis of Overloading Attack on BAS

Reference	Threat Models	Counter measures	Authentication Schemes	Bimetrics	Experimental Results
Pitropakis et al (2019) [32]	V	V	X	V	V
Barreno et al. (2006) [33]	X	X	V	V	X
Dalvi et al. (2004) [34]	V	X	V	V	X
Banerjee et al (2018) [35]	X	V	V	V	X
Biggio et al (2012) [36]	X	X	V	V	S
Chen eta al (2018) [37]	V	X	V	V	X
Maltoni et al (2003) [38]	X	X	V	V	X
Banerjee et al.(2018) [35]	S	V	X	V	V
Li et al.(2004) [50]	V	V	X	V	V
Parthasaradhi et.al.(2005)[83]	X	X	S	V	X
Moon et al. (2005) [84]	V	X	V	X	X
Chang et al. (2011) [85]	X	X	S	X	V
Li et al. (2004) [87]	V	V	V	X	V
Toth B (2005) [88]	V	V	X	X	V
Unar et al. (2014) [89]	V	V	X	V	V
Jain et al. (2004) [90]	V	V	X	V	V
Council et al. (2010) [91]	X	X	V	V	V
Prabhakar et al. (2003) [92]	V	X	S	V	X
Panigrahy et al. (2009) [93]	X	V	V	V	X
Qipeng et al. (2003) [94]	X	X	S	V	X

If an item is enrolled in the system, for example, an attacker may be able to utilise the same artefact to be recognised in the future. A user's template must be present in a data storage subsystem before he or she may utilise a biometric system for authentication or identication. Enrollment is the process of initialising a biometric system with such a template, and it is the source of a second error rate that might restrict biometric sys-tems' utility. As a result, the integrity of the enrollment process must be guaranteed [54].

12. Trojan Horse: Trojan-horse attacks modify the executable programme in a module such that it always outputs the values the attacker wants. A Trojan horse is a malicious programme that the attacker can operate remotely via commands. The Trojan can delete, copy, or modify data from the targeted system component once it has been triggered. In such a case, the Trojan will generate a preprogrammed feature set that will be fed into the template protection strategies module as input [61].

13. Poisoning attacks: Client templates are updated in real time by adaptive biometric systems to accommodate for natural changes (e.g., ageing of biometric templates). It was recently demonstrated that an attacker could use this update to compromise the clients' templates: by presenting the sensor with a proper sequence of fake biometric traits, the attacker could eventually impersonate the targeted clients without any fake traits, and even force the system to deny access to them. However, this attack has only been shown for face verication with one template per client, using worst-case assumptions about the attacker's system knowledge [62, 63].

14. Evasion Attack: Biometrics is now widely used for individual authentica-tion and identication. Biometric systems themselves must become more safe and dependable in order to provide secure authentication in a variety of applications. Biometric authentication frameworks must be designed to withstand multiple types of attacks in order to maximise security. There is a cunning adversary component in security sensitive applications that tries to fool the detection mechanism. In a well-motivated attack sce-nario, an attacker may attempt to dodge a well-established system at test time by carefully modifying attack samples, which is known as an Evasion Attack [64, 65].

Attacks against Biometric Authentication System: The various attacks on BAS that is highly vulnerable to adversarial at-tacks includes the quality scanner (1), feature extractor, template database, and matcher. Examples of these attacks include the replay of raw biometric print or the injection of false data into a system's processing chain, as depicted by attack types (2) and (3), respectively [66] (see Figure 4). Hill-climbing is one method for creating the synthesised templates. This technique works itera-tively, improving the synthesised features until they match the stored template incorrectly [60, 27]. While these attacks are being carried out on the system, a legitimate user will not notice any exceptions or warnings from the system, and it will continue to grant them access [28]. Attacks on the matcher to override the match scores to change an impostor's score to a higher passing score are examples of type attacks (6). The attacks of type (7) aim to add, modify, or delete user information from the template database; we will discuss these attacks separately. The type (8) of attacks inter-cepts the transmission channel to control theow of template information and override it with tempered information.

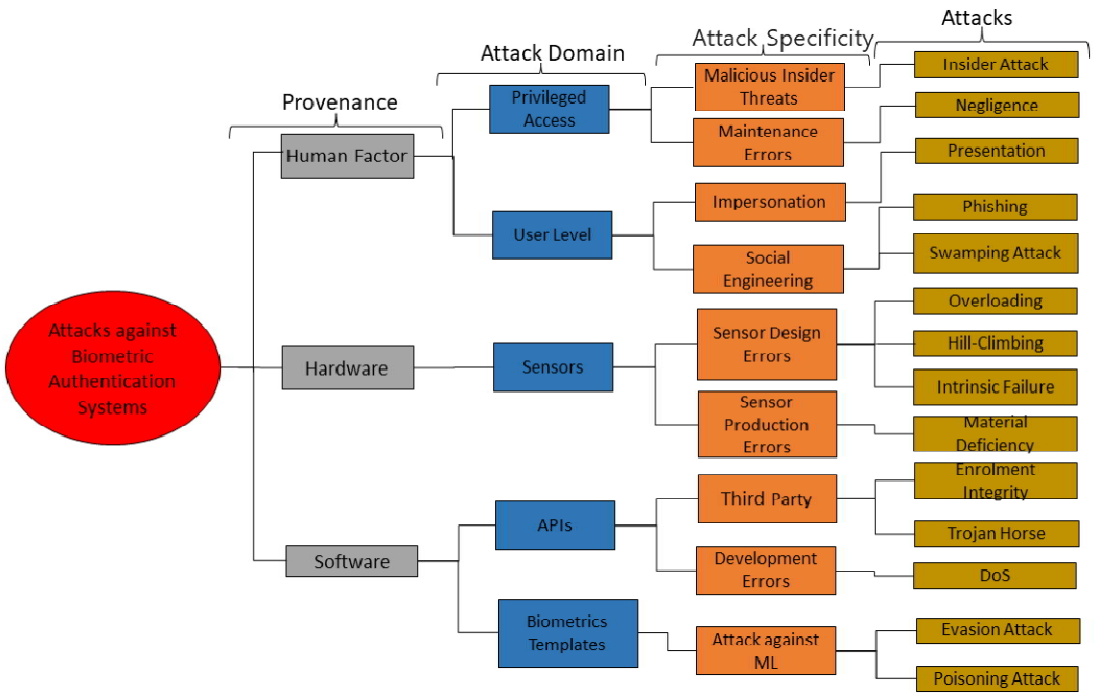

Figure 2. Taxonomy of attacks against Biometric Authentication System

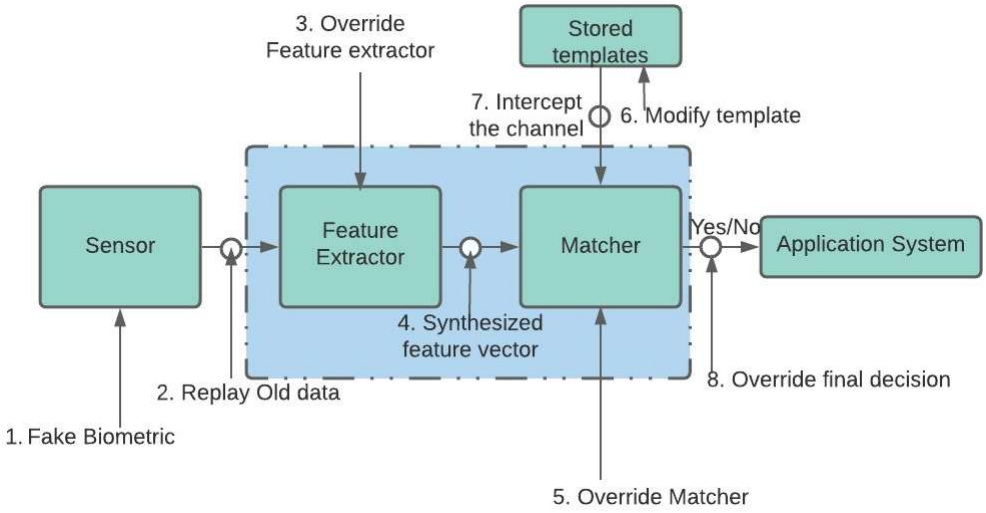

Figure 3. Attacks on Biometric Authentication System

Finally, attacks of type (9) seek to over-ride the matching decision, which can result in acceptance of an impostor but rejection of a genuine user. The interfaces of various components are attacked with the goal of concealing a component's intermediate code and intercepting information on its way to the next component. For example, the code gener-ated by a feature extractor can be intercepted by malicious programmes such as Trojan horses or logic bombs, resulting in the production of a new (forged) set of features as desired by an adversary. Similarly, a matcher can be attacked by trap doors or viruses, allowing it to bypass the matching process, or it can always produce the highest matching scores, allowing it to avoid the device. In this section, we also go over the various adversarial attacks that can be used against systems that use BAS. We've organised the articles by application domain so that you can see how adversarial BAS has progressed in each of these elds [65]. The percentage of articles addressing adversarial attacks on BAS for various application domains is seen in Figure 5. With the name \Others"(See Tables 2) we refer to articles that do not fall in any of the popular, within the eld of adversarial attacks on BAS, application domains (i.e., Overloading Attack see Tables 3, Presentation Attack see Tables 4, Intrinsic Failure see Tables 5) while \Insider attack" (See Tables 6) refers to papers that have investigated more than one application domain in order to assess their contributions. Statistics show that the \Presentation Attack" category covers the highest percentage of papers demonstrating the tendency of most authors to evaluate their work using dierent applications domains and understand the eect of the domain to the performance evaluation results. We observe that Insider attack is the second most investigated domain, which largely is due to the existence and the ease of use of well-known datasets such as the MNIST database of handwritten digits [67], ImageNet database [68].

METHODOLOGY, AIMS & OBJECTIVES

The proposed research aims are to research and identify the security issues of BAS, as can be seen in Figure 2 and to develop an advanced security framework model for BAS implementation. Furthermore, to develop countermeasures for the detection and prevention of these attacks in gure 2. The research will focus on the collection, analysis and review of literature related to IoT BAS. Honeypot and IDS technology will be used and deployed to monitor the techniques used by attackers on the captured biometric samples.

Table 4. Comparative analysis of "Others" papers on BAS

Reference	Threat Models	Counter measures	Authentication Schemes	Bimetrics	Experimental Results
Tasia et al. (2014) [28]	V	V	X	V	V
Chen et al. (2012) [29]	X	X	V	X	V
Khan et al. (2014) [30]	V	X	S	X	X
Li & Hwang (2010) [31]	X	V	V	X	V
Hadid et al.(2015) [59]	X	X	S	X	V
Tronci et al.(2011) [62]	V	X	V	X	V
Maltoni et al (2003) [38]	X	X	S	X	V
Yampolskiy et al (2008) [46]	V	V	V	X	V
Banerjee et al.(2018) [35]	V	V	X	V	V
Li et al.(2004) [50]	V	V	X	V	V
Jain et al. (2005) [8]	V	V	X	V	V
Jia et al. (2020) [6]	X	X	V	X	V
Clarke & Furne (2007) [70]	V	X	S	X	X
Hankerson et al. (2006) [71]	X	V	V	X	X
Matsumoto et al. (2002) [73]	X	X	S	X	X
Schucker et al. (2002) [44]	V	X	V	X	X
Kollreider et al. (2005) [74]	X	X	S	X	V
Matsumoto et al. (2004) [75]	V	V	V	X	V
Singh & Singh et.al.(2011)[77]	V	V	X	X	V
Kiss et al. (2001) [78]	V	V	X	V	V
Baldisserra et al. (2006) [79]	V	V	X	V	V
Reddy et al. (2008) [80]	X	X	V	X	V
Lapsley et al. (2008) [81]	V	X	S	X	X
Coli et al. (2007) [82]	X	V	V	X	X

Table 5. Comparative analysis of Intrinsic Failure on BAS

Reference	Threat Models	Counter measures	Authentication Schemes	Bimetrics	Experimental Results
Tasia et al. (2014) [28]	X	V	X	V	X
Chen et al. (2012) [29]	V	V	X	V	X
Khan et al. (2014) [30]	X	X	V	V	V
Li & Hwang (2010) [31]	X	X	X	V	V
Hadid et al.(2015) [59]	X	X	V	V	X
Tronci et al.(2011) [62]	X	X	X	V	V
C. Roberts et al. (2007) [5]	X	V	V	V	X
Jia et al. (2020) [6]	X	X	S	V	X
Buhan & Hart (2005) [7]	V	X	V	X	X
Jain et al. (2005) [8]	X	X	S	X	V
Cukic & Bartlow [9]	V	V	V	X	V
Sen & S. Borle (2015) [10]	V	V	X	V	V

Table 6. Comparative analysis of Insider attack on BAS

Reference	Threat Models	Counter measures	Authentication Schemes	Biometrics	Experimental Results
Tasia et al. (2014) [28]	V	V	X	V	V
Chen et al. (2012) [29]	X	X	S	X	V
Khan et al. (2014) [30]	V	V	V	X	V
Li & Hwang (2010) [31]	V	V	X	V	V
Hadid et al.(2015) [59]	V	V	X	V	V
Tronci et al.(2011) [62]	V	V	X	V	V
Maltoni et al (2003) [38]	X	X	S	X	V
Banerjee et al.(2018) [35]	V	V	X	V	V
Li et al.(2004) [50]	V	V	X	V	V
Frank et al. (2012) [11]	V	V	X	V	V
Chen et al. (2012) [12]	X	X	S	X	V
Uludag & Jain (2004) [13]	V	V	V	X	V
Meng et al. (2014) [14]	V	V	X	V	V
Jain et al. (2003) [16]	V	V	X	V	V

The result gathered through dif-ferent approaches, as stated above among many, will create more understanding about securing information and investigation of biometric information systems in a logical way which may aid in creating a hypothesis for further testing to either agree or disagree with any existing theory. The theory will be used to recommend the nal course of action.

Objectives

1. Literature review of attacks against biometric authentication systems.
2. Literature review of proposed defensive mechanisms for attacks against biometric authentication systems
3. Evaluation of existing defensive methodologies against popular attacks against biometric authentication systems
4. Study the performance of spoong attacks against biometric authentica-tion systems
5. Related popular biometric authentication system attacks with IoT threat landscape
6. Propose eective defensive mechanisms to fortify biometric authentication systems against known attack vectors.

Table 7. Comparative analysis of "Others" papers on BAS

Reference	Provenance	Attack Domain	Attack Specicity	Attack
Harrison (1958) [38]	S	S	S	V
Eriksson and Wretling(1997) [40]	S	S	S	V
Baracaldo et al (2018) [46]	S	S	V	S
Huang et al. (2011) [47]	S	S	V	S
Biggio et al (2013) [48]	S	S	V	S
Banerje et. al. (2018) [50]	S	S	S	V
ISO/IEC 2382-37:2012 (2016)[56]	S	S	S	V
NCSC (2019) [57]	S	S	S	V
Hadid et al. (2015) [58]	S	S	S	V
Schucker et al. (2002)[42]	S	S	S	V
Biggio et. al. (2012) [49]	S	S	V	S
Banerje et al (2018) [50]	S	S	V	S
Pitropaki et al. (2019) [51)	S	S	V	S
Xi et. al. (2011) [25]	S	S	V	S
Faruk et al (2014) [52]	S	S	V	S
Kolberg et al. (2020) [59]	S	S	S	V
Kaspersky (2020) [60]	S	S	S	V
ISO/IEC 30107 (2020) [61]	S	S	S	V
Bond Fingerprint Technology (1971)[62]	S	S	S	V
Tolosana et al. (2019) [63]	S	S	S	V
Wasnik et al. (2016) [64]	S	S	S	V
Kollreider et al. (2005) [65]	S	S	S	V
Li et al. (2004) [66]	S	S	S	V
Alaswad et al. (2014) [67]S	S	S	S	V
Martinez-Diaz et al. (2006) [68]	S	S	S	V
Ahmad et al. (2018) [69]	S	S	S	V
Joshi et al. (2018) [39]	S	S	S	V
Anjos et al. (2014) [70]	S	S	S	V
Khan et al. (2012) [71]	S	S	S	V
Yahaya et al. (2009) [72]	S	S	S	V
Kiss et al. (2001) [73]	S	S	S	V
Qin et al. (2016) [74]	S	V	S	S
Robert. C (2007) [5]	S	V	S	S
Jia et al. (2020) [6]	S	V	S	S

Aims

1. Study literature around biometric authentication system attacks
2. Test existing attacks against modern biometric authentication systems
3. Study IoT threat landscape and identify any connections with biometric authentication system attacks
4. Study defensive methodologies that improve the resilience of biometric authentication systems and investigate possible improvements.

Research Questions

1. How biometric authentications systems are used to provide security for modern ICT systems.
2. How IoT devices' security overlaps with BAS.
3. How can attacks based on the presentation of fake biometric authentica-tion be mitigated.
4. How captured biometric samples are used as an attack vector and what is there lifetime.
5. What are the gaps in the present biometric security strategies and how can we develop robust techniques that can increase the resilience of BAS.

Research Signicance: The signicance of the research proposed would be the security of captured biometric samples, and maintain database integrity of the organization, or gov-ernmental agency so it can trust and minimize economical and industrial losses and also whereby security principles of availability, integrity, condentiality and non repudiation is guaranteed.

Countermeasures and Biometric System Defences

Countermeasures: To protect users of a variety of computing mobile devices against insider and outsider assaults, a safe and ecient authentication mechanism is required.

When a user accesses the devices, the authentication method uses both cryp-tosystems and non-cryptosystem countermeasures to conduct user authentica-tion. We'll talk about the countermeasures utilised by authentication techniques for smart mobile devices in this part.

Cryptographic functions, personal identity, classication algorithms, and channel characteristics are among the countermeasures utilised by authenti-cation schemes for computing mobile devices, as shown in Figure 5. The coun-termeasures employed in authentication techniques are shown in Figure 6.

1. ***Cryptographic functions:*** Most authentication techniques for computing mobile devices use cryptographic functions to meet security goals, and these functions can be grouped into three categories: asymmetric encryp-tion, symmetric encryption, and hash functions. Table II shows that bi-linear pairings and elliptic curve cryptosystems are the most commonly utilised cryptographic functions (ECC). Although the elliptic curve cryp-tosystem is used in the authentication schemes [8, 6, 46, 69], it still has some drawbacks, such as the necessity for a key authentication centre to keep track of the certicates for users' public keys.

2. ***Personal Identity:*** Personal identication can be divided into two types: (e.g, Personal Identication Number (PIN), International Mobile Equip-ment Identity (IMEI), and Password). Clarke and Furnell's approach [70] uses inter-keystroke latency to classify users based on entering phone num-bers and PINs, with users authenticated based on three interaction sce-narios: 1) 11-digit phone numbers; 2) 4-digit PINs; and 3) text messages Clarke and Furnell's architecture collects the following forms of input data: 1) telephone numbers, 2) telephone area code (5-digit), 3) text message, and 4) 4-digit PIN code, similar to the approach [70]. The numbers-based countermeasures, according to Wiedenbeck et al. [71], should be simple to remember, random, and dicult to guess; they should be updated fre-quently, and dierent

for each user's account; and they should not be written down or saved in plain text. As a result, countermeasures focused on numbers are vulnerable to attacks like shoulder surng.

3. Biometrics-based countermeasures: Are there any physiological (e.g., face, eyes, ngerprints, palm, or ECG) or behavioural (e.g., signature, voice, gait, or keystroke) patterns in the human body? Biometrics-based coun- termeasures are more common than numbers-based countermeasures to-day since PIN codes obstruct convenience and ease of access. Capacitive ngerprint scanners have begun to be integrated into the enclosure of several modern computing mobile devices (e.g., iPhone 5S and up, and Samsung Galaxy S5 and up).

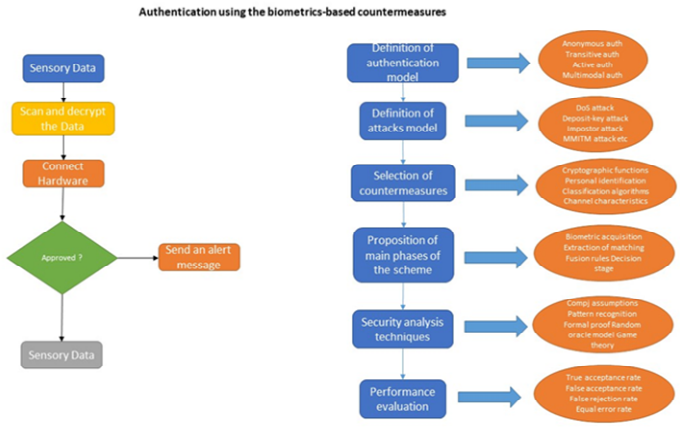

Figure 5. Flowcharts process of authentication using the biometrics-based countermeasures

Biometric System Defences: Individual biometrics are distinct, but they are not hidden. Biometric data is irreversible, and regaining one's identity can be dicult. As a result, the chal-lenge is to create a secure and reliable authentication system using system com-ponents that are neither secret nor revocable. A typical biometric system begins by storing the data. Features extracted from an enrolled biometric identity as templates in the system database, and then matching the template features with features extracted from biometric data given during successive authentication eorts. If a biometric security system ensures that biometric features are re-trieved from a person to be validated and then compared to template features in a database, it will work correctly. In an ideal world, no electronic authentica-tion (eID) system is totally secure, and no one security method is adequate to protect the system completely. However, by taking sensible and practical steps, the risk of security risks can be eciently reduced to an acceptable level. There are a variety of proven defensive strategies in use that eectively prevent or decrease the danger of biometric system security threats and vulnerabilities. A generic biometric system's security approaches that are eective against system threats can be divided into two categories:

Vitality detection

Biometric template protection: Each category, on the other hand, has its own set of security procedures. Other useful countermeasures that can lessen the faults and failures of a biometric system include the design of prominent feature detectors and robust match-ers. Furthermore, practical techniques such as the use of various biometrics, solid governance procedures, and physical security can help to reduce biometric system security vulnerabilities.

Vitality Detection: A biometric system's vitality detection could be used as a defence against spoong attempts. It guarantees that the biometric sample supplied is genuine and not a forgery. Furthermore, it ensures that the supplied biometric corre-sponds to a real person who was previously enrolled in the system, rather than just any real person with or without a phoney biometric. The goal of vitality detection is to take a biometric sample from a real, live person who is present at the moment of enrollment.Successful vitality detection approaches improve the dependability of a biometric system by preventing artefact from being en-rolled and ensuring that no non-live sample is accepted. Although biometric technologies employ a person's physiological information to authenticate him or her, they don't detect their vitality. It has been demonstrated, however, that biometric systems may be spoong with fake samples, such as a prosthetic n-ger made of gelatine, silicon, latex, or Play-Doh[72], Face and iris recognition systems [73] can be fooled by static and high-resolution photographs of the face and irises [44], [74], [75] and iris recognition system [76].

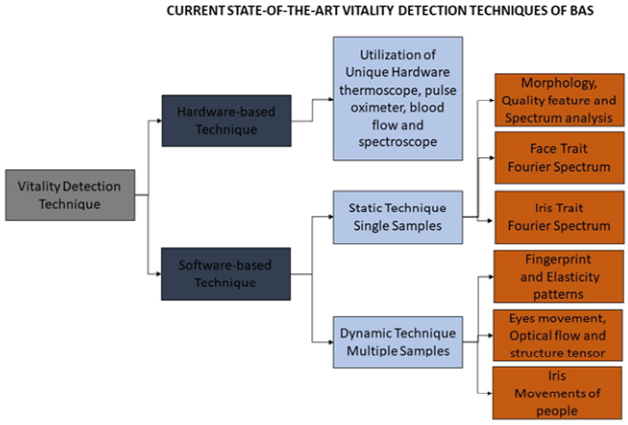

Figure 6. Current state-of-the-art vitality detection techniques of BAS

Various methods have been proposed in the studies to ensure the vitality indicators from biometric samples. As illustrated in Figure 5, presented a clas-sication of current state-of-the-art vitality detection approaches of commonly used biometrics [77] (e.g., ngerprint, face, and iris). Existing approaches can be split into two groups: hardware and software base techniques.

1. **Hardware-based Techniques** During the acquisition stage, hardware-based approaches detect vital signs from the available biometric sample. These methods rely on additional gear to extract live signs from biometric data. Temperature [78], smell [79], pulse oximetry [80], blood ow [81], and spectral information are some of the approaches used to measure vital signs from a ngertip put on a sensor [82]. The cost of the system rises when a specialised device is integrated at the sensor, and the added circuitry may be intrusive to consumers.
2. **Software-based techniques** During the processing step, software-based ap-proaches detect vitality indications in biometric samples. The goal of these strategies is to extract any one unique characteristic of live signs from a single sample (static techniques) or numerous samples (dynamic techniques) that diers from articial replication. The vitality signs of a biometric sample can be detected in a ngerprint recognition system by analysing a single image of ngerprint using skin perspiration [83], mor-phology characteristics [84], spectrum analysis [85], and quality related features [86]. skin distortion analysis, or several pictures of a ngerprint. The Fourier spectrums [87] can also be used to identify a live sample of face or iris from its fake image. By dynamically analysing the movement of the eyes and spatial 2D motions on the face an image sequence of the face is employed to detect the live indicators. Using pupillary motions and illumination, the iris image sequence can detect live signs.

Achievement reviewed of vitality detection techniques: Regardless of the fact that a range of vitality detection techniques exist, determining vitality from biometric samples is a practical challenge [88]. The matching dierence in distribution between live and fake samples is smaller than the matching dierence in distribution between real and imposter samples, according to an independent measure of vitality detection. As a result, spoong the system in the absence of a vitality detection technique results in a false match without the attacker doing

any eort. Furthermore, the eectiveness of vitality detection approaches may be assessed by calculating the proportion of transactions with a fake sample that are erroneously matched (FMRNL) and the fraction of interactions with a live sample that are incorrectly non-matched (IMRNL) (FNMRL). For this aim, an equal error rate (ERR) between FNMRNL and FMRL can also be used. Table 7 shows the achievement of vitality detection techniques linked with the various biometrics indicated. It is, however, more dicult to draw any conclusions about the ecacy of one vitality detecting technique against each other.

Issues and Challenges: Border control, forensics, criminal identication, access control, computer logins, e-commerce, welfare disbursements, missing children identication, id-cards, passports, user authentication on mobile devices, and time and atten-dance monitoring systems all use biometric technology [89]. Because biometric systems are widely accepted as a viable way of user identication and authorisa-tion, it has become necessary to solve a variety of diculties in order to improve system performance and strengthen system security. In [90], Jain et al. classi-ed the fundamental hurdles in biometrics into four categories: accuracy, scale, security, and privacy. The accuracy of a biometric system is heavily inuenced by false-match and false-non match errors in making the proper conclusion. The scale barrier raises the question of the impact of the number of enrolled users on making the correct decision. The security of the biometric system against potential assaults, as well as the privacy of user data, are of the greatest priority. The paper [91] discusses the future of biometric systems, as well as potential research opportunities. The authors addressed opportunities in modality-related research, information security research, testing and evaluation research, systems level statistical engineering research, scale research, and social science. [92, 93] discusses the privacy diculties associated with biometric systems. The privacy concerns are primarily about user data (i.e. biometrics). Privacy concerns occur when biometric data is used for secondary purposes, such as function creep, data matching, aggregation, surveillance, and proling [94]. To address the privacy issue of an individual's biometrics, [95] introduces a ngerprint authentication method for the privacy protection of the ngerprint template maintained in a database. In this situation, an individual's identity is concealed in a thinning ngerprint template, which is kept in an online database and retrieved during the authentication step. Because of privacy concerns, some people are sceptical of the biometric technology. As a result, the research community is faced with the challenge of developing a biometric system that ensures not only the security but also the privacy of user data. According to the World Bank, more than 1.5 billion individuals worldwide do not have ocial status [96]. A biometric system could be a potential answer to the global challenge of making government resources and services more available to the public. In [97], Akhtar et al. conducted a comprehensive study on biometric systems and attempted to solve some key biometric questions. The writers divided the questions into groups such as the current state of biometrics, current concerns and challenges in biometrics, hot subjects in biometrics, biometric security, and biometric future.

Biometric Authentication System Failure: BAS failures are viewed as errors from the correct implementation of system functions. Service failures, development failures, and security failures are all examples of system failures [36, 98]. When the given service diers from the expected service, it is called a service failure. Development failures are the result of development aws. The development process is ended if a development failure occurs before the system is accepted for use and put into operation. Due to ineective imaging, poor data representation, or improper matching, it can occur at any level of system architecture.The majority of development failures are caused by an inaccurate or misleading estimation of the system's complexity. It includes things like poor design in terms of functionality or performance goals, incorrect or incomplete specications, insucient fault elimination capability, and inaccurate development cost projections. For example, the government of India's Unique Identication Authority of India (UIDAI) programme, which intends to distribute biometric-based unique identication (UID) numbers to all citizens, is now facing diculties.The success of the UID programme is in doubt because the magnitude (technical, social, and nancial) of such a massive undertaking has not been fully assessed. The UID authority has consistently misjudged the project's diculty [99]. As a result, it should come as no surprise if a large-scale project like UIDAI falls short of its goals. If this occurs, the most serious aspect of the project failure would be the loss of money, which will exceed 30 billions, which is more than the cost of the AAS system, which was shut down due to total development failure (US Department of Transportation, 1998). When a BAS is breached, it will result in one of two outcomes [100]: (I) denial of service (Dos) (ii) intrusion.

1. A DoS attack occurs when a lawful user is denied access to a service to which he is entitled. An adversary can disable the infrastructure (for ex-ample, by physically damaging a ngerprint sensor), preventing users from gaining access to the device. Denial-of-service is often caused by intrin-sic errors such as false reject, failure-to- capture, and failure-to-acquire. Administrative abuse, such as tampering with models or the biometric system's operating parameters (e.g., matching threshold), may result in service denial.
2. Intrusion occurs when an impostor gains unauthorised access to a device, resulting in data loss (e.g., unauthorised access to personal data) and se-curity risks (e.g., terrorists crossing borders). Intrusion may be caused by any of the four factors that cause biometric device vulnerability: in-trinsic malfunction, administrative misuse, nonsecure infrastructure, and biometric overtness.

DISCUSSION & CONCLUSION

Biometric systems are commonly used for secure identity management, how-ever they are prone to a variety of security risks. Biometric security systems are vulnerable to intentional or inadvertent security aws, which can result in unauthorised inltration, denial of service, or theft of enrolled individuals' sen-sitive information. Attacks on saved biometric templates are a prominent worry among the described vulnerabilities that are related to the development and use phase of a biometric system. Furthermore, because there is a tight link between an individual's template and his or her identity, biometric templates are im-mutable. We feel that current template protection solutions are insuciently developed to handle large-scale security applications. The choice of a template protection technique, on the other hand, is determined by the application sce-nario and its requirements. The apparent nature of the important information and the system's re-stricted vitality detection techniques are the main sources of a biometric sys-tem's vulnerabilities. An opponent can easily generate a spoof biometric from a real user's biometric sample, or even steal a stored template to get unauthorised access. Many state-of-the-art vitality detection algorithms exist for various bio-metrics, but it has been suggested that collecting multiple biometric identities from people at the same time during enrolment could be a useful option for iden-tifying vitality indicators from biometric data. Bioelectrical signals, such as the ECG or electroencephalogram (EEG), are gaining popularity as novel biometrics for identifying individuals. According to the ndings, cardiac rhythm impulses and brain electrical activity recorded in the ECG and EEG, respectively, have distinct properties that can be used as biometrics [101]. The inherent trait of vitality that imply life signs, which is a strong protection against spoof assaults, is a favourable aspect for using the ECG or EEG as a biometric.

Dierent approaches to safeguard the stored template have been developed to eectively prevent against vulnerabilities. Furthermore, the design of a tem-plate protection mechanism is totally dependent on how biometric features are represented. For minutia-based ngerprint features, a non-invertible transform is a good choice, while a biometric cryptosystem is a good choice for a xed-length binary

representation of iris code. If the biometric samples contain a lot of intraclass variation, neither non-invertible transforms nor biometric cryp-tosystem procedures will work. Considering the benets of several template protection measures, the biomet-ric industry has made no persistent eorts to implement such security solutions. It's possible that this is due to a lack of standards for developing and maintain-ing modied templates, a computationally expensive matching process, and an increase in authentication error while utilising modied templates. More secure procedures, on the other hand, we believe, will weaken security threats and give assurance about the system's integrity. As the usage of biometric-based authentication grows in popularity, the most critical concern that must be addressed throughout the design of a biometric authentication system is undoubtedly security. A variety of threats can com-promise biometric systems. Human factor, hardware, and software attacks have been characterised as dangers to a biometric system. A high-level classication of biometric systems vulnerabilities is oered, with a multidimensional threat environment for a BAS and its impacts depicted using a BAS diagram. We propose a taxonomy of biometric system security threats, as well as po-tential defences techniques. BAS attacks are classied in a comprehensive and methodical way. Human factor, hardware, and software threats are all discussed as BAS threat vectors. We oer a BAS with a multidimensional threat envi-ronment and a BAS diagram to show the consequences. Various solutions for the necessity of dependable vitality testing and biometric data condentiality have been oered in the literature as a countermeasure to biometric system weaknesses. We go forward to reviewed previous cyber-attacks and ENISA case studies on organisations all across the world. According to our ndings, BAS requires additive research in order to improve the current system's performance and accuracy while also addressing its aws. In addition, the implementation of multi-level BAS is seen as a future study topic that will necessitate additional studies and research.

REFERENCES

[1] N. Mastali, J. I. Agbinya, Authentication of subjects and devices using biometrics and identity management systems for persuasive mobile com-puting: A survey paper, in: 2010 Fifth International Conference on Broad-band and Biomedical Communications, IEEE, 2010, pp. 1{6.

[2] F. T. T. D. Liu Yi, news magazines, Available: http://news. networkmagazine.com.tw/magazine/2013/10/09/55018, 14 November, 2021 (2021).

[3] U. Uludag, A. K. Jain, Attacks on biometric systems: a case study in ngerprints, in: Security, steganography, and watermarking of multimedia contents VI, Vol. 5306, International Society for Optics and Photonics, 2004, pp. 622{633.

[4] A. K. Jain, A. Ross, S. Pankanti, Biometrics: a tool for information secu-rity, IEEE transactions on information forensics and security 1 (2) (2006) 125{143.

[5] C. Roberts, Biometric attack vectors and defences, Computers & Security 26 (1) (2007) 14{25.

[6] S. Jia, G. Guo, Z. Xu, A survey on 3d mask presentation attack detection and countermeasures, Pattern Recognition 98 (2020) 107032.

[7] I. Buhan, P. H. Hartel, The state of the art in abuse of biometrics, Citeseer, 2005.

[8] A. K. Jain, A. Ross, U. Uludag, Biometric template security: Challenges and solutions, in: 2005 13th European signal processing conference, IEEE, 2005, pp. 1{4.

[9] B. Cukic, N. Bartlow, Biometric system threats and countermeasures: a risk based approach, in: Proceedings of the Biometric Consortium Con-ference (BCC'05), 2005.

[10] R. Sen, S. Borle, Estimating the contextual risk of data breach: An empir-ical approach, Journal of Management Information Systems 32 (2) (2015) 314{341.

[11] M. Frank, R. Biedert, E. Ma, I. Martinovic, D. Song, Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication, IEEE transactions on information forensics and security 8 (1) (2012) 136{148.

[12] C.-L. Chen, C.-C. Lee, C.-Y. Hsu, Mobile device integration of a nger-print biometric remote authentication scheme, International Journal of Communication Systems 25 (5) (2012) 585{597.

[13] U. Uludag, A. K. Jain, Attacks on biometric systems: a case study in ngerprints, in: Security, steganography, and watermarking of multimedia contents VI, Vol. 5306, International Society for Optics and Photonics, 2004, pp. 622{633.

[14] W. Meng, D. S. Wong, S. Furnell, J. Zhou, Surveying the development of biometric user authentication on mobile phones, IEEE Communications Surveys & Tutorials 17 (3) (2014) 1268{1293.

[15] W. Meng, D. S. Wong, S. Furnell, J. Zhou, Surveying the development of biometric user authentication on mobile phones, IEEE Communications Surveys & Tutorials 17 (3) (2014) 1268{1293.

[16] A. Jain, U. Uludag, A. Ross, Biometric template selection: a case study in ngerprints, in: International Conference on Audio-and Video-Based Biometric Person Authentication, Springer, 2003, pp. 335{342.

[17] N. K. Ratha, R. Bolle, Smartcard based authentication, in: Biometrics, Springer, 1996, pp. 369{384.

[18] N. K. Ratha, J. H. Connell, R. M. Bolle, Secure ngerprint authentication, in: Biometric Solutions, Springer, 2002, pp. 263{288.

[19] N. Mastali, J. I. Agbinya, Authentication of subjects and devices using biometrics and identity management systems for persuasive mobile com-puting: A survey paper, in: 2010 Fifth International Conference on Broad-band and Biomedical Communications, IEEE, 2010, pp. 1{6.

[20] D. Bala, Biometrics and information security, in: Proceedings of the 5th annual conference on Information security curriculum development, 2008, pp. 64{66.

[21] I. Velasquez, A. Caro, A. Rodrguez, Authentication schemes and meth-ods: A systematic literature review, Information and Software Technology 94 (2018) 30{37.

[22] M. La Polla, F. Martinelli, D. Sgandurra, A survey on security for mobile devices, IEEE communications surveys & tutorials 15 (1) (2012) 446{471.

[23] S. Yanushkevich, S. Eastwood, S. Samoil, V. P. Shmerko, T. Manderson, M. Drahansky, Taxonomy and modeling of impersonation in e-border au-thentication, in: 2015 Sixth International Conference on Emerging Secu-rity Technologies (EST), IEEE, 2015, pp. 38{43.

[24] D. Kunda, M. Chishimba, A survey of android mobile phone authentica-tion schemes, Mobile Networks and Applications (2018) 1{9.

[25] K. Xi, T. Ahmad, F. Han, J. Hu, A ngerprint based bio-cryptographic security protocol designed for client/server authentication in mobile com-puting environment, Security and communication networks 4 (5) (2011) 487{499.

[26] H.-A. Park, J. W. Hong, J. H. Park, J. Zhan, D. H. Lee, Combined authentication-based multilevel access control in mobile application for daily life service, IEEE Transactions on Mobile Computing 9 (6) (2010) 824{837.

[27] C.-J. Tasia, T.-Y. Chang, P.-C. Cheng, J.-H. Lin, Two novel biometric features in keystroke dynamics authentication systems for touch screen devices, Security and Communication Networks 7 (4) (2014) 750{758.

[28] M. K. Khan, J. Zhang, X. Wang, Chaotic hash-based ngerprint biometric remote user authentication scheme on mobile devices, Chaos, Solitons & Fractals 35 (3) (2008) 519{524.

[29] C.-L. Chen, C.-C. Lee, C.-Y. Hsu, Mobile device integration of a nger-print biometric remote authentication scheme, International Journal of Communication Systems 25 (5) (2012) 585{597.

[30] M. K. Khan, S. Kumari, M. K. Gupta, More ecient key-hash based ngerprint remote authentication scheme using mobile device, Computing 96 (9) (2014) 793{816.

[31] C.-T. Li, M.-S. Hwang, An ecient biometrics-based remote user authenti-cation scheme using smart cards, Journal of Network and

Computer Appli-cations 33 (1) (2010) 1{5. doi: https://doi.org/10.1016/j.jnca.2009.08.001. URL https://www.sciencedirect.com/science/article/pii/S1084804509001192

[32] D. Maltoni, D. Maio, A. K. Jain, S. Prabhakar, Fingerprint matching, Handbook of Fingerprint Recognition (2003) 131{171.

[33] N. Baracaldo, B. Chen, H. Ludwig, A. Safavi, R. Zhang, Detecting poi-soning attacks on machine learning in iot environments, in: 2018 IEEE international congress on internet of things (ICIOT), IEEE, 2018, pp. 57{ 64.

[34] L. Huang, A. Joseph, B. Nelson, B. Rubinstein, J. Tygar, Proceedings of the 4th acm workshop on security and articial intelligence (2011).

[35] P. Faruki, A. Bharmal, V. Laxmi, V. Ganmoor, M. S. Gaur, M. Conti, M. Rajarajan, Android security: a survey of issues, malware penetration, and defenses, IEEE communications surveys & tutorials 17 (2) (2014) 998{1022.

[36] A. Avizienis, J.-C. Laprie, B. Randell, C. Landwehr, Basic concepts and taxonomy of dependable and secure computing, IEEE transactions on dependable and secure computing 1 (1) (2004) 11{33.

[37] ECSC 2020 ANALYSIS REPORT Maturity assessment of and lessons learned from the European Cyber Security Challenge, author=ENISA, https://op.europa.eu/en/publication-detail/-/publication/8a7fd763-a63a-11eb-9585-01aa75 09th May 2021 (2021).

[38] S. Rajamanickam, N. Ramasubramanian, S. Vollala, Insider attack pre-vention using multifactor authentication protocols-a survey, in: Applied Information Processing Systems, Springer, 2022, pp. 331{339.

[39] A. Eriksson, P. Wretling, How exible is the human voice?-a case study of mimicry, in: Fifth European Conference on Speech Communication and Technology, 1997.

[40] S. T. Parthasaradhi, R. Derakhshani, L. A. Hornak, S. A. Schuckers, Time-series detection of perspiration as a liveness test in ngerprint de-vices, IEEE Transactions on Systems, Man, and Cybernetics, Part C (Ap-plications and Reviews) 35 (3) (2005) 335{343.

[41] ISO/IEC 2382-37:2012, Information technolog Vo-cabulary | Part 37: Biometrics, author=ISO/IEC, http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html, 19th December 2021 (2016).

[42] Biometric recognition and authentication systems, author=NCSC, https://www.ncsc.gov.uk/collection/biometrics/how-biometrics-are-attackedsection2;19th D

[43] A. Hadid, N. Evans, S. Marcel, J. Fierrez, Biometrics systems under spoof-ing attack: an evaluation methodology and lessons learned, IEEE Signal Processing Magazine 32 (5) (2015) 20{30.

[44] S. A. Schuckers, Spoong and anti-spoong measures, Information Secu-rity technical report 7 (4) (2002) 56{62.

[45] J. Kolberg, M. Gomez-Barrero, S. Venkatesh, R. Ramachandra, C. Busch, Presentation attack detection for nger recognition, in: Handbook of Vas-cular Biometrics, Springer, Cham, 2020, pp. 435{463.

[46] Kaspersky Security Bulletin 2020 Statistics, author=Kaspersky Lab, https://go.kaspersky.com/rs/802-IJN-240/images/KSB statistics2020en:pdf;11thMay2021(2020)

[47] S. Jia, G. Guo, Z. Xu, A survey on 3d mask presentation attack detection and countermeasures, Pattern Recognition 98 (2020) 107032. doi:https://doi.org/10.1016/j.patcog.2019.107032. URL https://www.sciencedirect.com/science/article/pii/S0031320319303358

[48] Presentation Attack Detection- ISO/IEC 30107, https://christoph-busch.de/files/Busch-PAD-200915.pdf, 20th December 2021 (2020).

[49] Bond Fingerprint Technology, author=IntlSpyMuseum, https://www.youtube.com/watch?v=yP5ku2IJgAY,26th December 2021 (1971).

[50] R. Tolosana, M. Gomez-Barrero, C. Busch, J. Ortega-Garcia, Biometric presentation attack detection: Beyond the visible spectrum, IEEE Trans-actions on Information Forensics and Security 15 (2019) 1261{1275.

[51] P. Wasnik, K. B. Raja, R. Raghavendra, C. Busch, Presentation attack detection in face biometric systems using raw sensor data from smartphones, in: 2016 12th International Conference on Signal-Image Technology Internet-Based Systems (SITIS), 2016, pp. 104{111. doi:10.1109/SITIS.2016.25.

[52] K. Kollreider, H. Fronthaler, J. Bigun, Evaluating liveness by face images and the structure tensor, in: Fourth IEEE Workshop on Automatic Iden-tication Advanced Technologies (AutoID'05), IEEE, 2005, pp. 75{80.

[53] J. Li, Y. Wang, T. Tan, A. K. Jain, Live face detection based on the analysis of fourier spectra, in: Biometric technology for human identica-tion, Vol. 5404, International Society for Optics and Photonics, 2004, pp. 296{303.

[54] A. O. Alaswad, A. H. Montaser, F. E. Mohamad, Vulnerabilities of biomet-ric authentication \threats and countermeasures", International Journal of Information & Computation Technology 4 (10) (2014) 947{58.

[55] M. Martinez-Diaz, J. Fierrez-Aguilar, F. Alonso-Fernandez, J. Ortega-Garca, J. Siguenza, Hill-climbing and brute-force attacks on biometric systems: A case study in match-on-card ngerprint verication, in: Pro-ceedings 40th Annual 2006 International Carnahan Conference on Security Technology, IEEE, 2006, pp. 151{159.

[56] M. Joshi, B. Mazumdar, S. Dey, Security vulnerabilities against ngerprint biometric system, arXiv preprint arXiv:1805.07116 (2018).

[57] S. Ahmad, A. Badwelan, A. M. Ghaleb, A. Qamhan, M. Sharaf, M. Alate, A. Moohialdin, Analyzing critical failures in a production process: Is in-dustrial iot the solution?, Wireless Communications and Mobile Comput-ing 2018 (2018).

[58] A. Anjos, M. M. Chakka, S. Marcel, Motion-based counter-measures to photo attacks in face recognition, IET biometrics 3 (3) (2014) 147{158.

[59] W. Z. Khan, Y. Xiang, M. Y. Aalsalem, Q. Arshad, Mobile phone sensing systems: A survey, IEEE Communications Surveys & Tutorials 15 (1) (2012) 402{427.

[60] Y. H. Yahaya, M. R. M. Isa, M. I. Aziz, Fingerprint biometrics au-thentication on smart card, in: 2009 Second International Conference on Computer and Electrical Engineering, Vol. 2, 2009, pp. 671{673. doi:10.1109/ICCEE.2009.155.

[61] Y. Qin, Q. Z. Sheng, N. J. Falkner, S. Dustdar, H. Wang, A. V. Vasilakos, When things matter: A survey on data-centric internet of things, Journal of Network and Computer Applications 64 (2016) 137{153.

[62] B. Biggio, L. Didaci, G. Fumera, F. Roli, Poisoning attacks to compromise face templates, in: 2013 International Conference on Biometrics (ICB), IEEE, 2013, pp. 1{7.

[63] B. Biggio, B. Nelson, P. Laskov, Poisoning attacks against support vector machines, arXiv preprint arXiv:1206.6389 (2012).

[64] N. Banerjee, T. Giannetsos, E. Panaousis, C. C. Took, Unsupervised learn-ing for trustworthy iot, in: 2018 IEEE international conference on fuzzy systems (FUZZ-IEEE), IEEE, 2018, pp. 1{8.

[65] N. Pitropakis, E. Panaousis, T. Giannetsos, E. Anastasiadis, G. Loukas, A taxonomy and survey of attacks against machine learning, Computer Science Review 34 (2019) 100199.

[66] K. Xi, T. Ahmad, F. Han, J. Hu, A ngerprint based bio-cryptographic security protocol designed for client/server authentication in mobile com-puting environment, Security and communication networks 4 (5) (2011) 487{499.

[67] Y. LeCun, The mnist database of handwritten digits, http://yann.lecun. com/exdb/mnist/ (1998).

[68] J. Deng, W. Dong, R. Socher, L.-J. Li, K. Li, L. Fei-Fei, Imagenet: A large-scale hierarchical image database, in: 2009 IEEE conference on computer vision and pattern recognition, Ieee, 2009, pp. 248{255.

[69] K. Nandakumar, A. K. Jain, Multibiometric template security using fuzzy vault, in: 2008 IEEE Second International Conference on Biometrics: The-ory, Applications and Systems, IEEE, 2008, pp. 1{6.

[70] N. L. Clarke, S. Furnell, Advanced user authentication for mobile devices, computers & security 26 (2) (2007) 109{119.
[71] D. Hankerson, A. J. Menezes, S. Vanstone, Guide to elliptic curve cryp-tography, Springer Science & Business Media, 2006.
[72] T. Van der Putte, J. Keuning, Biometrical ngerprint recognition: don't get your ngers burned, in: Smart Card Research and Advanced Appli-cations, Springer, 2000, pp. 289{303.
[73] T. Matsumoto, H. Matsumoto, K. Yamada, S. Hoshino, Impact of arti-cial" gummy" ngers on ngerprint systems, in: Optical Security and Counterfeit Deterrence Techniques IV, Vol. 4677, International Society for Optics and Photonics, 2002, pp. 275{289.
[74] K. Kollreider, H. Fronthaler, J. Bigun, Evaluating liveness by face images and the structure tensor, in: Fourth IEEE Workshop on Automatic Iden-tication Advanced Technologies (AutoID'05), IEEE, 2005, pp. 75{80.
[75] T. Matsumoto, Articial irises: importance of vulnerability analysis, in: Proc. Asian Biometrics Workshop (AWB), Vol. 45, 2004.
[76] T. Matsumoto, Assessing the security of advanced biometric systems: n-ger, vein and iris, in: Proc. of the 10th International Biometrics Confer-ence, 2007.
[77] Y. N. Singh, S. K. Singh, Vitality detection from biometrics: state-of-the-art, in: 2011 World Congress on Information and Communication Technologies, IEEE, 2011, pp. 106{111.
[78] I. Kiss, et al., Detector for recognizing the living character of a nger in a ngerprint recognizing apparatus, uS Patent 6,175,641 (Jan. 16 2001).
[79] D. Baldisserra, A. Franco, D. Maio, D. Maltoni, Fake ngerprint detection by odor analysis, in: International Conference on Biometrics, Springer, 2006, pp. 265{272.
[80] P. V. Reddy, A. Kumar, S. Rahman, T. S. Mundra, A new antispoong approach for biometric devices, IEEE transactions on biomedical circuits and systems 2 (4) (2008) 328{337.
[81] P. D. Lapsley, J. A. Lee, D. F. Pare Jr, N. Homan, Anti-fraud biometric scanner that accurately detects blood ow, uS Patent 5,737,439 (Apr. 7 1998).
[82] P. Coli, G. L. Marcialis, F. Roli, Power spectrum-based ngerprint vitality detection, in: 2007 IEEE Workshop on Automatic Identication Advanced Technologies, IEEE, 2007, pp. 169{173.
[83] S. T. Parthasaradhi, R. Derakhshani, L. A. Hornak, S. A. Schuckers, Time-series detection of perspiration as a liveness test in ngerprint de-vices, IEEE Transactions on Systems, Man, and Cybernetics, Part C (Ap-plications and Reviews) 35 (3) (2005) 335{343.
[84] Y. S. Moon, J. Chen, K. Chan, K. So, K. Woo, Wavelet based ngerprint liveness detection, Electronics Letters 41 (20) (2005) 1112{1113.
[85] S. Chang, J. Secker, Q. Xiao, B. Reid, A. Bergeron, W. Almuhtadi, Arti-cial nger detection by spectrum analysis, *International Journal of Bio-metrics* 3 (4) (2011) 376{389.
[86] S. T. Parthasaradhi, R. Derakhshani, L. A. Hornak, S. A. Schuckers, Time-series detection of perspiration as a liveness test in ngerprint de-vices, IEEE Transactions on Systems, Man, and Cybernetics, Part C (Ap-plications and Reviews) 35 (3) (2005) 335{343.
[87] J. Li, Y. Wang, T. Tan, A. K. Jain, Live face detection based on the analysis of fourier spectra, in: Biometric technology for human identica-tion, Vol. 5404, International Society for Optics and Photonics, 2004, pp. 296{303.
[88] B. Toth, Biometric liveness detection, Information Security Bulletin 10 (8) (2005) 291{297.
[89] J. Unar, W. C. Seng, A. Abbasi, A review of biometric technology along with trends and prospects, Pattern recognition 47 (8) (2014) 2673{2688.
[90] A. K. Jain, S. Pankanti, S. Prabhakar, L. Hong, A. Ross, Biometrics: a grand challenge, in: Proceedings of the 17th International Conference on Pattern Recognition, 2004. ICPR 2004., Vol. 2, IEEE, 2004, pp. 935{942.
[91] N. R. Council, W. B. Committee, et al., Biometric recognition: Challenges and opportunities (2010).
[92] S. P. Prabhakar, S. Pankanti, S., & jain, ak, 2003. biometric recognition: security & privacy concerns, IEEE Security & Privacy Magazine 1 (2) 33{42.
[93] S. Rajamanickam, N. Ramasubramanian, S. Vollala, Insider attack pre-vention using multifactor authentication protocols-a survey, in: Applied Information Processing Systems, Springer, 2022, pp. 331{339.
[94] S. K. Panigrahy, D. Jena, S. B. Korra, S. K. Jena, On the privacy protec-tion of biometric traits: palmprint, face, and signature, in: International Conference on Contemporary Computing, Springer, 2009, pp. 182{193.
[95] L. Qipeng, Y. Xiaoling, F. Quanke, Fault diagnosis using wavelet neural networks, Neural processing letters 18 (2) (2003) 115{123.
[96] D. M. Storisteanu, T. L. Norman, A. Grigore, A. B. Labrique, Can biomet-rics beat the developing world's challenges?, Biometric Technology Today 2016 (11) (2016) 5{9.
[97] Z. Akhtar, A. Hadid, M. S. Nixon, M. Tistarelli, J.-L. Dugelay, S. Marcel, Biometrics: In search of identity and security (q & a), IEEE MultiMedia 25 (3) (2018) 22{35.
[98] A. K. Jain, A. Ross, S. Pankanti, Biometrics: a tool for information secu-rity, IEEE transactions on information forensics and security 1 (2) (2006) 125{143.
[99] Y. N. Singh, S. K. Singh, Vitality detection from biometrics: state-of-the-art, in: 2011 World Congress on Information and Communication Technologies, IEEE, 2011, pp. 106{111.
[100] A. Hadid, N. Evans, S. Marcel, J. Fierrez, Biometrics systems under spoof-ing attack: an evaluation methodology and lessons learned, IEEE Signal Processing Magazine 32 (5) (2015) 20{30.
[101] Y. N. Singh, S. K. Singh, A. K. Ray, Bioelectrical signals as emerging bio-metrics: Issues and challenges, International Scholarly Research Notices 2012 (2012).

****