Volume 4, Issue 1, 2020

Eigenpub Review of Science and Technology
peer-reviewed journal dedicated to showcasing cutting-edge research and innovation in the fields of science and technology.
https://studies.eigenpub.com/index.php/erst

Spoofing Attacks and Mitigation Strategies in Biometrics-as-a-Service Systems

Anusha Bodepudi

Staff Engineer, Intuit, Plano, TX, USA,
Anusha_bodepudi@intuit.com

Manjunath Reddy

Customer Engineering Lead, Qualcomm , San diego, CA, USA,
reddymanjushari@gmail.com

ABSTRACT

Biometrics-as-a-Service (BaaS) systems have gained significant popularity as a secure method for authentication. However, like any other biometric authentication system, BaaS systems are susceptible to spoofing attacks. Spoofing attacks involve presenting fake biometric data to deceive the system into granting unauthorized access. In this research, we explore common spoofing techniques and the vulnerabilities they exploit in BaaS systems. The identified spoofing techniques include the use of fake biometric samples created with materials like silicone or gelatin for fingerprints and high-resolution photographs for facial recognition. Presentation attacks involve using imitations or replicas of biometric traits, such as high-quality photographs or 3D masks, to bypass facial recognition systems. Replay attacks, on the other hand, intercept and replay legitimate biometric data to gain unauthorized access. Furthermore, deepfake technology poses a significant threat by generating realistic synthetic media, which can be used to spoof facial recognition systems. To mitigate these spoofing attacks, several strategies are proposed. Incorporating liveness detection mechanisms in BaaS systems can verify that the biometric data presented is from a live person and not a spoofed sample. Additionally, multi-factor authentication can bolster security by combining biometrics with other authentication factors like passwords or tokens. Continuous monitoring using advanced machine learning algorithms helps detect suspicious activities or anomalies in the biometric data. Furthermore, the implementation of robust biometric algorithms designed to identify synthetic or manipulated traits is crucial in thwarting spoofing attempts. Finally, maintaining the security of BaaS systems requires regular updates and patches to address any known vulnerabilities or weaknesses in the system.

Keywords: *Biometrics-as-a-Service (BaaS) systems, Spoofing attacks, Fake biometric samples, Liveness detection, Robust biometric algorithms*

I. INTRODUCTION

The provision of security involves safeguarding sensitive data, services, or facilities by granting access only to authorized individuals. While passwords offer a level of protection, they often fall short as they can be easily guessed or cracked if they are too simple. Even with complex passwords, users may struggle to remember them and resort to storing them through less secure means [1]. Additionally, many individuals reuse the same password across multiple applications or platforms, which poses a significant risk. If a password is

compromised, it can grant unauthorized access to multiple resources, allowing fraudsters to exploit various systems [2].

A promising alternative to traditional passwords is biometric recognition. Biometrics utilize a person's unique behavioral and biological characteristics, including their face, fingerprint, iris, voice, hand geometry, and gait. These traits are highly discriminative, making it difficult for impostors to replicate them. Unlike passwords that can be lost or stolen, biometric data is inherently tied to an individual and less prone to unauthorized use. By leveraging biometrics for authentication purposes, organizations can enhance security while minimizing the risk associated with password-based systems.

In addition to the improved security offered by biometric recognition, this approach also brings added convenience for users. Unlike passwords that can be forgotten or require regular updates, biometric traits are inherently tied to an individual's identity and are unlikely to change over time. This eliminates the need for users to remember or manage complex passwords, reducing the likelihood of account lockouts or password reset requests. Biometrics provide a seamless and user-friendly authentication experience, improving efficiency and usability in various applications, such as accessing devices, unlocking doors, or logging into systems [3].

Despite their advantages, biometric systems are not immune to malicious attacks [2]. One notable vulnerability is the risk of spoofing attacks, also known as presentation attacks. These attacks involve individuals attempting to deceive biometric systems by impersonating someone else to gain unauthorized access to sensitive or protected resources. For instance, an attacker may trick a face recognition system by using a photograph, video, or even a three-dimensional mask that resembles the appearance of an authorized individual.

Spoofing attacks exploit the limitations of biometric systems, which rely on capturing and analyzing unique behavioral or physiological traits for identification purposes [4]. While biometric traits are highly discriminative, they can be replicated or manipulated by individuals with malicious intent. By presenting falsified biometric data that closely resembles the genuine data of an authorized user, attackers can deceive the system and gain access to restricted areas, sensitive information, or valuable resources [5].

To counter these spoofing attacks, robust anti-spoofing techniques are being developed and implemented [6]. These techniques aim to detect and differentiate between genuine biometric samples and forged or manipulated ones. Advanced algorithms and technologies, such as liveness detection, texture analysis, and multimodal fusion, are utilized to enhance the security of biometric systems [7].

Biometrics-as-a-Service (BaaS) refers to the cloud-based delivery model of biometric authentication and identification services [8]. It leverages the power of biometric technologies, such as fingerprint recognition, facial recognition, iris scanning, and voice recognition, to provide secure and reliable identity verification. BaaS allows organizations to incorporate biometric capabilities into their applications and systems without the need to develop and maintain complex infrastructure in-house. Instead, they can access biometric services through APIs (Application Programming Interfaces) provided by BaaS

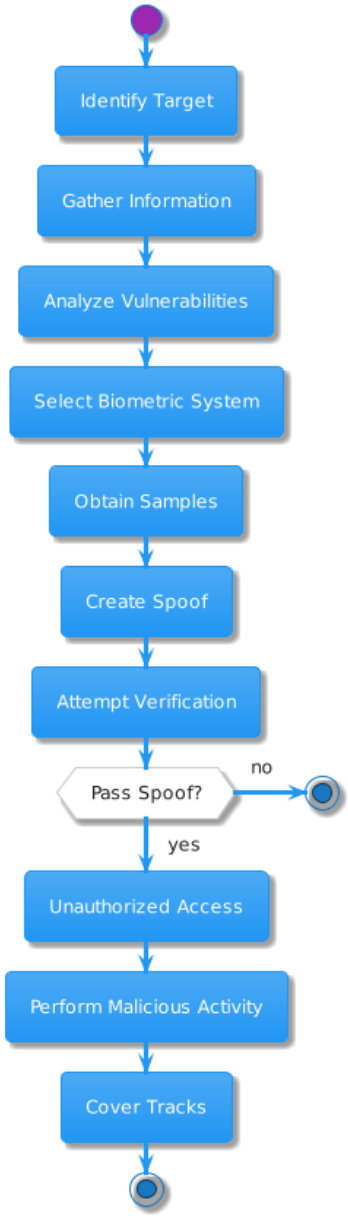
providers. This approach not only simplifies implementation but also ensures scalability, affordability, and compliance with industry standards and regulations [9].

The emergence of BaaS can be attributed to the increasing demand for stronger security measures and seamless user experiences in various industries [10], [11]. Traditional authentication methods like passwords and PINs are susceptible to breaches and often lead to user frustrations due to forgotten credentials. Biometric authentication offers a more reliable and convenient alternative, and BaaS makes this technology accessible to a broader range of businesses and developers. With the rise of cloud computing and advancements in biometric algorithms, BaaS has become feasible and cost-effective, attracting organizations seeking robust identity verification solutions [12], [13].

BaaS operates on a subscription-based model, where organizations can choose the biometric modalities they want to integrate into their applications. Upon subscribing to a BaaS provider's services, developers gain access to the provider's APIs, SDKs (Software Development Kits), and documentation. They can then integrate these tools into their applications, enabling users to enroll their biometric data (e.g., fingerprints, facial features) securely on the cloud platform. During authentication, the user's biometric data is captured, encrypted, and transmitted to the BaaS server for comparison with the pre-registered template. The server processes the biometric information and sends back a response indicating whether the user's biometrics match the enrolled data. The result is then used to grant or deny access to the application or service. BaaS providers handle the complexities of biometric data storage, processing, and updates, allowing organizations to focus on enhancing their applications and user experiences while ensuring robust and reliable identity verification [14], [15].

One significant concern in BaaS is the possibility of spoofing attacks. Spoofing attacks occur when malicious actors attempt to deceive the biometric system by presenting falsified or replicated biometric traits to gain unauthorized access [16]. One possible type of spoofing attack is fingerprint forgery, where an attacker fabricates a replica of a genuine fingerprint. This can be achieved through various methods, such as using molds or high-resolution photographs. By presenting the forged fingerprint to the biometric system, the attacker aims to fool the system into believing it is an authentic user, leading to potential unauthorized access [17]. Another form of spoofing attack is facial spoofing, where an attacker tries to deceive facial recognition systems by presenting photographs or videos of the genuine user's face. With the advancements in deepfake technology, attackers can create highly realistic synthetic media that mimics a real person's facial movements. This can pose a significant challenge for facial recognition systems, potentially compromising the security of BaaS applications. Voice spoofing is yet another concern in BaaS. Attackers can use voice samples of the genuine user to create synthetic speech or mimic the user's voice through text-to-speech techniques. By manipulating their voice to match the genuine user, they aim to bypass voice recognition systems and gain unauthorized access to sensitive information or resources [18].

Figure 1. A Biometric Spoofing attack on BaaS



SPOOFING VULNERABILITIES IN BAAS SYSTEMS

Fake Biometric Samples:

Fake biometric samples pose a significant threat to biometric authentication systems, particularly those implemented in Biometrics-as-a-Service (BaaS) platforms. Attackers have the ability to fabricate artificial samples of various biometric traits, including fingerprints, iris patterns, and facial features, with the intention of deceiving the system. To accomplish this, they may employ materials such as silicone or gelatin to replicate fingerprints, or exploit high-resolution photographs to simulate facial recognition.

One common technique employed by attackers involves creating artificial fingerprints using silicone or gelatin. By meticulously crafting a mold of a legitimate fingerprint and filling it with these materials, they can produce a fake fingerprint that closely resembles the real one. This can then be used to bypass fingerprint recognition systems, granting unauthorized access to secure areas or sensitive data. Additionally, attackers can utilize techniques like fingerprint lifting to obtain genuine prints and subsequently reproduce them in a fabricated form [19].

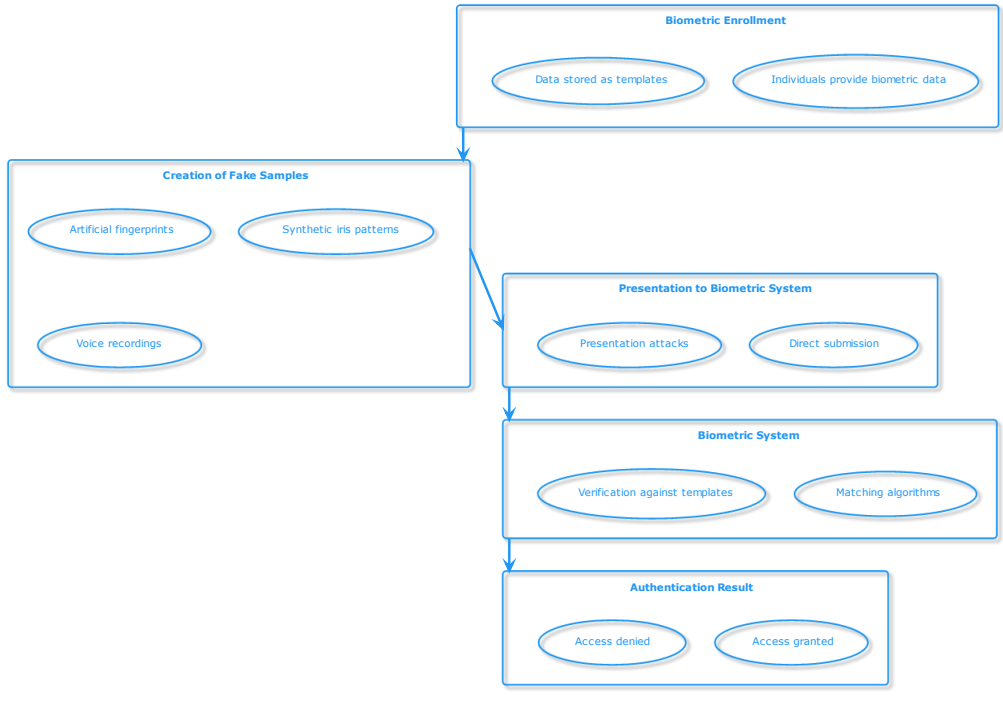
Another method employed to deceive biometric systems is the use of high-resolution photographs for facial recognition. Attackers can capture or obtain a clear image of an authorized user's face and print it with high precision on a flat surface or create a lifelike 3D mask [20]. These fake samples can then be presented to the facial recognition system, tricking it into believing that the attacker is the legitimate user. Such attacks have been successful in bypassing facial recognition-based security measures, potentially leading to unauthorized access or identity theft [21].

Furthermore, the advancements in digital manipulation techniques pose a significant threat to biometric systems. With the availability of sophisticated image editing software, attackers can alter or enhance photographs to create more realistic fake biometric samples. They can adjust the lighting, texture, and other attributes of the images to make them indistinguishable from genuine biometric data. This makes it even more challenging for biometric systems to differentiate between real and fabricated samples, increasing the risk of successful attacks.

Presentation Attacks:

Presentation attacks refer to the utilization of imitations or replicas of a user's biometric traits with the intention to deceive the BaaS system. An attacker might employ various techniques, such as presenting a meticulously captured high-quality photograph or a lifelike 3D mask that closely resembles the authentic user's face. By doing so, they aim to exploit vulnerabilities in facial recognition systems and successfully bypass the security measures in place [22].

Figure 2. Fake Biometric Samples works in Biometrics-as-a-Service



The essence of presentation attacks lies in the deceptive nature of the fabricated samples. Attackers may go to great lengths to ensure that the imitation closely resembles the genuine biometric trait. For instance, they may acquire a high-resolution photograph of the user's face, meticulously capturing the facial features and details. This photograph can then be precisely printed or projected onto a flat surface, giving the illusion of a real face when presented to the facial recognition system [23].

In some cases, attackers take their presentation attacks to the next level by creating 3D masks that exhibit an uncanny resemblance to the user's face. These masks are carefully crafted using advanced techniques, such as 3D printing or sculpting, to capture the intricate details of the target's facial structure. When presented to the facial recognition system, the 3D mask can deceive the system into believing that the attacker is the genuine user, effectively granting unauthorized access [24].

Replay Attacks:

Replay attacks refer to a type of cyber attack where an unauthorized individual intercepts and replays previously recorded data to deceive a system into granting access or performing unintended actions. In the context of biometrics, replay attacks involve capturing the biometric data of a legitimate user during the authentication process and replaying it later to trick the system into believing that the attacker is the authorized user. This form of attack exploits the inherent vulnerability of systems that solely rely on biometric authentication without additional security measures [25].

There are several types of replay attacks that can be employed to compromise biometric authentication systems. One common method is known as a "passive replay attack." In this scenario, the attacker captures the biometric data, such as fingerprints or facial features, during a legitimate user's authentication attempt without the user's knowledge. The captured data is then later replayed to the system, tricking it into granting unauthorized access [26].

Another type of replay attack is the "active replay attack." This attack involves the attacker actively participating in the authentication process, usually by presenting the captured biometric data directly to the biometric sensor. By doing so, the attacker bypasses any security mechanisms that may be in place, fooling the system into believing that the attacker is the genuine user. Replay attacks pose a significant threat to biometric authentication systems, as they exploit the limitations of relying solely on biometric data for user verification [27].

Deepfakes:

Deepfake technology has emerged as a significant concern in the digital age, as it leverages the power of artificial intelligence to create convincing synthetic media that can deceive and manipulate viewers. With deepfakes, it is possible to generate highly realistic videos or audio that can be used to impersonate individuals, leading to potential misuse and harm. By manipulating facial expressions, speech patterns, and other visual and auditory cues, deepfakes can convincingly mimic someone else, making it difficult to discern between genuine and synthetic content.

In the context of biometrics, deepfakes pose a particular threat to facial recognition systems. These systems are designed to identify and authenticate individuals based on their unique facial features. However, deepfakes can be used to create fabricated videos of a targeted user's face, thereby fooling the facial recognition algorithms and enabling unauthorized access to sensitive information or secure facilities [28]. By crafting deepfakes that closely resemble the appearance of the targeted user, adversaries can bypass biometric security measures and exploit vulnerabilities in authentication systems.

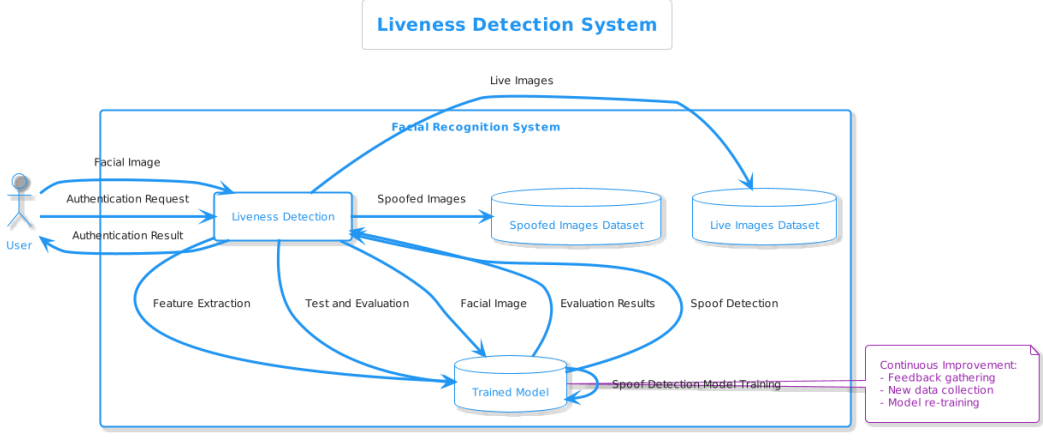
The implications of deepfake technology extend beyond mere impersonation and security breaches. They have the potential to undermine public trust and compromise the integrity of digital media. Deepfakes can be used to spread misinformation, manipulate public opinion, and even fabricate evidence, leading to severe social and political consequences. The widespread dissemination of deepfakes can erode trust in media sources, disrupt democratic processes, and create confusion and uncertainty in various domains [29].

MITIGATION STRATEGIES

Liveness detection

A liveness detection system serves the crucial purpose of differentiating between live and non-live (spoofed) biometric samples, such as facial images or fingerprints, thereby strengthening the security and reliability of biometric authentication systems [30]. To develop such a system specifically for facial recognition, several key steps are involved.

Figure 3. Liveness detection system



Firstly, the system begins with data collection, where a diverse dataset of both live and spoofed facial images is gathered. This dataset encompasses various spoofing techniques, including printed photos, replay attacks, 3D masks, and digital screen presentations. Next, the system moves to feature extraction, extracting meaningful characteristics from the collected facial images. Multiple techniques can be employed for this purpose, such as Local Binary Patterns (LBP), Scale-Invariant Feature Transform (SIFT), or Convolutional Neural Networks (CNNs), to extract distinguishing features from the images [31], [32].

After feature extraction, the system proceeds with spoof detection model training. The collected dataset is utilized to train a machine learning model or a deep neural network classifier. This model's primary objective is to accurately differentiate between live and spoofed images based on the extracted features. Algorithms like Support Vector Machines (SVM), Random Forests, or deep learning architectures like Convolutional Neural Networks (CNNs) are commonly employed for this task [18], [25].

Subsequently, the system goes through test and evaluation phases. The dataset is divided into training and testing sets, and the trained model's performance is evaluated using the testing set. Metrics such as accuracy, precision, recall, and F1 score are used to gauge the efficacy of the liveness detection system.

The trained liveness detection model is then integrated into the facial recognition system. Whenever a user attempts facial recognition, their image is passed through the liveness

detection system first. If the system detects any indication of a spoof attempt, it promptly rejects the authentication request [33].

For continuous improvement, the system's performance is continually monitored in real-world scenarios. Feedback and data on new spoofing techniques are gathered to enhance the system's accuracy and robustness. Regularly re-training the model with new data helps the system stay adaptive and effective against evolving spoofing attacks, ensuring the security of the biometric authentication process.

Multi-Factor Authentication (MFA)

Multi-Factor Authentication (MFA) is a security mechanism designed to protect sensitive information and systems by requiring multiple factors or elements for user authentication. It enhances the security of traditional username-password combinations by incorporating additional layers of verification. While biometrics, such as fingerprint or facial recognition, are one factor commonly used in MFA, it is crucial not to solely rely on them for authentication. By including other factors like passwords, tokens, or one-time codes, MFA adds an extra layer of security, making it more challenging for attackers to bypass the system.

The process of Multi-Factor Authentication typically works by prompting users to provide multiple forms of identification before granting access to a system or data. These factors can fall into three categories: knowledge factors (something the user knows), possession factors (something the user has), and inherence factors (something the user is). For example, a typical MFA process may require users to enter a password (knowledge factor), use a physical token or smart card (possession factor), and provide a fingerprint scan (inherence factor). By combining these multiple factors, MFA ensures that even if one factor is compromised, the overall security remains intact [34].

The inclusion of additional factors in MFA strengthens security in several ways. Firstly, it mitigates the risk of password-related vulnerabilities such as weak or reused passwords. Even if an attacker manages to obtain a user's password, they would still need the other authentication factors to gain access. Secondly, it protects against unauthorized access in case a device or token is stolen. The possession factor ensures that the person attempting to authenticate is in physical possession of a specific item, reducing the risk of unauthorized access. Lastly, incorporating diverse factors makes it significantly more challenging for attackers to impersonate users. It requires them to possess not only the user's knowledge but also their physical attributes or personal possessions.

MFA can be implemented using various methods depending on the system or application. Common approaches include one-time codes sent via SMS or email, biometric authentication (fingerprint, face, voice), physical tokens or smart cards, or software-based authenticator apps. Organizations can choose the combination of factors that best suits their security requirements and user experience. However, it is important to strike a balance between security and usability to avoid inconveniencing users with overly complex or cumbersome authentication processes [35].

Continuous Monitoring:

Continuous Monitoring is a crucial component of Biometric-as-a-Service (BaaS) systems, aimed at ensuring the ongoing security and integrity of biometric data. It involves the

implementation of advanced machine learning algorithms that continuously analyze patterns and detect any suspicious activities or anomalies in the biometric data. By employing continuous monitoring, BaaS systems can effectively identify potential spoofing attempts and mitigate security risks.

The process of continuous monitoring in BaaS systems works by collecting and analyzing real-time data from various biometric sensors or sources. This data can include fingerprint scans, facial images, voice samples, or other biometric modalities. The collected data is then processed and compared against established patterns and behavioral models. Advanced machine learning algorithms play a vital role in this analysis, as they can learn from historical data and detect deviations from normal patterns, indicating potential threats or fraudulent activities. By continuously monitoring the biometric data and analyzing it for anomalies, the system can identify potential spoofing attacks and trigger appropriate security measures. For example, if a facial recognition system detects unusual movement patterns or inconsistencies in facial features during an authentication attempt, it can raise an alert or prompt additional verification steps. Continuous monitoring also enables the system to adapt and evolve based on new patterns or emerging threats. Machine learning algorithms can continuously learn from the data they process, allowing them to improve their accuracy and effectiveness over time. This adaptive capability is crucial in keeping up with evolving attack techniques and maintaining a high level of security [36].

Moreover, continuous monitoring helps in compliance with data protection regulations and standards. By actively monitoring biometric data, organizations can demonstrate their commitment to safeguarding sensitive information and promptly respond to any security incidents or breaches. This proactive approach enhances transparency and accountability, which are essential elements of a robust security framework.

Robust Biometric Algorithms:

Robust Biometric Algorithms are specifically designed to withstand and detect spoofing attacks, where individuals attempt to deceive the system using synthetic or manipulated biometric traits. Researchers continuously strive to develop and enhance such algorithms to improve the overall robustness and accuracy of biometric recognition.

The primary objective of robust biometric algorithms is to differentiate between genuine biometric traits and spoofed or manipulated ones. They achieve this by analyzing various characteristics and patterns within the biometric data. For example, in fingerprint recognition, algorithms may examine ridge structures, minutiae points, or the overall consistency of the fingerprint image. Similarly, in facial recognition, algorithms may focus on specific facial landmarks, texture patterns, or depth information. By analyzing these unique features, robust biometric algorithms aim to identify any inconsistencies or irregularities that may indicate a spoofing attempt.

To develop robust algorithms, researchers employ advanced techniques from machine learning, computer vision, and pattern recognition. These algorithms are trained using large datasets that include both genuine biometric samples and various types of spoofing attacks. Through this training process, the algorithms learn to distinguish between authentic and manipulated biometric traits, enabling them to accurately detect and mitigate spoofing attempts in real-time [37].

Continuous research and development efforts are essential to stay ahead of evolving spoofing techniques. As attackers become more sophisticated in their methods, robust biometric algorithms need to adapt and identify new types of synthetic or manipulated biometric traits. By closely monitoring emerging attack vectors and analyzing real-world data, researchers can refine the algorithms and improve their ability to detect even the most sophisticated spoofing attempts.

The adoption of robust biometric algorithms is crucial in sectors where security is paramount, such as border control, financial institutions, or critical infrastructure. By implementing these algorithms, organizations can significantly enhance the reliability and trustworthiness of their biometric recognition systems. It reduces the risk of unauthorized access, identity theft, and other fraudulent activities, providing a higher level of security for both individuals and institutions.

Regular Updates and Patches:

Regular updates and patches are crucial for maintaining the security and integrity of Biometric-as-a-Service (BaaS) systems. These updates ensure that the system remains protected against known vulnerabilities or weaknesses that could be exploited by attackers. By keeping BaaS systems up to date with the latest security patches, organizations can minimize the risk of unauthorized access and protect the confidentiality, integrity, and availability of biometric data.

The landscape of cybersecurity is constantly evolving, and new threats and vulnerabilities emerge regularly. Software vendors and developers actively monitor these developments and release updates and patches to address any identified security issues. These updates may include bug fixes, security enhancements, or patches for known vulnerabilities. By applying these updates to BaaS systems, organizations can ensure that any previously identified weaknesses are mitigated, reducing the risk of potential attacks [38].

One critical aspect of regular updates is the timely application of security patches. Promptly installing patches helps to close security gaps and prevent potential exploits that can lead to unauthorized access or data breaches. Delaying the application of patches increases the window of opportunity for attackers to exploit known vulnerabilities in the system. Therefore, organizations should establish a regular schedule for patch management and ensure that updates are applied as soon as they become available [39].

Regular updates not only address known vulnerabilities but also help to enhance the overall performance and functionality of the BaaS system. Software updates often include new features, improved user experience, and performance optimizations. By keeping the system up to date, organizations can benefit from the latest advancements in technology and ensure that their BaaS system operates efficiently and effectively. Additionally, compliance with industry regulations and standards often mandates the regular application of updates and patches [40]. These regulations aim to safeguard sensitive information and protect individuals' privacy rights. By adhering to these requirements and regularly updating the BaaS system, organizations demonstrate their commitment to maintaining a secure and reliable infrastructure.

CONCLUSION

Biometrics-as-a-Service (BaaS) systems have gained significant traction as a reliable and secure method for authentication in various industries and applications. These systems utilize unique physiological or behavioral characteristics of individuals, such as fingerprints, facial features, or iris patterns, to establish identity and grant access to authorized users. BaaS systems offer advantages like convenience, accuracy, and resistance to lost or stolen credentials, making them increasingly popular in areas like mobile devices, banking, healthcare, and law enforcement. However, despite their effectiveness, BaaS systems are not impervious to attacks. One major concern is the susceptibility of these systems to spoofing attacks, which involve presenting counterfeit or manipulated biometric data to deceive the system and gain unauthorized access. It is crucial to address these vulnerabilities and develop robust countermeasures to ensure the integrity and security of BaaS systems in the face of evolving spoofing techniques.

This study has highlighted the vulnerabilities and risks associated with spoofing attacks in Biometrics-as-a-Service (BaaS) systems. Spoofing attacks, which involve presenting fake biometric data to deceive the system, pose a significant threat to the security of BaaS systems. The identified spoofing techniques, including the use of fake biometric samples and presentation attacks, exploit vulnerabilities in fingerprint and facial recognition systems. Replay attacks and the emergence of deepfake technology further exacerbate the challenges faced by BaaS systems.

To mitigate these spoofing attacks, several strategies have been proposed. One such strategy is the incorporation of liveness detection mechanisms in BaaS systems. Liveness detection can verify that the presented biometric data is from a live person and not a spoofed sample, thus enhancing the security of the system. Additionally, the adoption of multi-factor authentication, combining biometrics with other authentication factors like passwords or tokens, can significantly bolster security and prevent unauthorized access.

Continuous monitoring using advanced machine learning algorithms is another crucial strategy to detect suspicious activities or anomalies in the biometric data. By constantly analyzing the biometric data, any unusual patterns or discrepancies can be identified promptly, enabling timely responses to potential spoofing attempts. Furthermore, the implementation of robust biometric algorithms designed to identify synthetic or manipulated traits is imperative in thwarting spoofing attacks. These algorithms can detect and reject fake biometric samples generated using materials like silicone or gelatin, as well as identify deepfake-generated facial images.

Finally, the security of BaaS systems heavily relies on regular updates and patches to address any known vulnerabilities or weaknesses in the system. As new spoofing techniques and attack vectors emerge, it is essential to keep the BaaS systems up to date with the latest security measures and countermeasures. This proactive approach ensures that the systems remain resilient against evolving spoofing threats and reduces the likelihood of successful attacks.

REFERENCES

[1] D. Bhattacharyya and R. Ranjan, "Biometric authentication: A review," *Journal of u- and e ...*, 2009.

[2] M. Boatwright and X. Luo, "What do we know about biometrics authentication?," in *Proceedings of the 4th annual conference on Information security curriculum development*, Kennesaw Georgia, 2007.

[3] Q. Xiao, "Security issues in biometric authentication," in *Proceedings from the Sixth Annual IEEE SMC Information Assurance Workshop*, 2005, pp. 8–13.

[4] Z. Akhtar, S. Kale, and N. Alfarid, "Spoof attacks on multimodal biometric systems," *International Conference on Information*, 2011.

[5] C. Roberts, "Biometric attack vectors and defences," *Comput. Secur.*, vol. 26, no. 1, pp. 14–25, Feb. 2007.

[6] A. Hadid, "Face biometrics under spoofing attacks: Vulnerabilities, countermeasures, open issues, and research directions," in *2014 IEEE Conference on Computer Vision and Pattern Recognition Workshops*, Columbus, OH, USA, 2014, pp. 113–118.

[7] A. Anjos, J. Komulainen, S. Marcel, A. Hadid, and M. Pietikäinen, "Face Anti-spoofing: Visual Approach," in *Handbook of Biometric Anti-Spoofing: Trusted Biometrics under Spoofing Attacks*, S. Marcel, M. S. Nixon, and S. Z. Li, Eds. London: Springer London, 2014, pp. 65–82.

[8] J. Rose, "Biometrics as a service: the next giant leap?," *Biometric Technology Today*, 2016.

[9] V. A. Bharadi, H. A. Mestry, and A. Watve, "Biometric Authentication as a Service (BaaS): a NOSQL Database and CUDA based Implementation," in *2019 5th International Conference On Computing, Communication, Control And Automation (ICCUBEA)*, 2019, pp. 1–5.

[10] A. Castiglione, K.-K. R. Choo, M. Nappi, and F. Narducci, "Biometrics in the Cloud: Challenges and Research Opportunities," *IEEE Cloud Computing*, vol. 4, no. 4, pp. 12–17, Jul. 2017.

[11] S. Barra, A. Castiglione, M. De Marsico, M. Nappi, and K.-K. R. Choo, "Cloud-Based Biometrics (Biometrics as a Service) for Smart Cities, Nations, and Beyond," *IEEE Cloud Computing*, vol. 5, no. 5, pp. 92–100, Sep. 2018.

[12] S. Barra, K.-K. R. Choo, M. Nappi, A. Castiglione, F. Narducci, and R. Ranjan, "Biometrics-as-a-Service: Cloud-Based Technology, Systems, and Applications," *IEEE Cloud Computing*, vol. 5, no. 4, pp. 33–37, Jul. 2018.

[13] T. M. Alsultan, A. A. Salam, K. A. Alissa, and N. A. Saqib, "A Comparative Study of Biometric Authentication in Cloud Computing," in *2019 International Symposium on Networks, Computers and Communications (ISNCC)*, 2019, pp. 1–6.

[14] A. Kanak, "Biometric ontology for semantic biometric-as-a-service (BaaS) applications: a border security use case," *IET Biometrics*, 2018.

[15] V. Talreja, T. Ferrett, M. C. Valenti, and A. Ross, "Biometrics-as-a-service: A framework to promote innovative biometric recognition in the cloud," in *2018 IEEE International Conference on Consumer Electronics (ICCE)*, 2018, pp. 1–6.

[16] A. Taneja, A. Tayal, A. Malhorta, A. Sankaran, M. Vatsa, and R. Singh, "Fingerphoto spoofing in mobile devices: A preliminary study," in *2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, 2016, pp. 1–7.

[17] T. A. Siddiqui *et al.*, "Face anti-spoofing with multifeature videolet aggregation," in *2016 23rd International Conference on Pattern Recognition (ICPR)*, 2016, pp. 1035–1040.

[18] M. Sajjad *et al.*, "CNN-based anti-spoofing two-tier multi-factor authentication system," *Pattern Recognit. Lett.*, vol. 126, pp. 123–131, Sep. 2019.
[19] J. Galbally, S. Marcel, and J. Fierrez, "Biometric Antispoofing Methods: A Survey in Face Recognition," *IEEE Access*, vol. 2, pp. 1530–1552, 2014.
[20] S. Marcel, M. S. Nixon, J. Fierrez, and N. Evans, *Handbook of biometric anti-spoofing: Presentation attack detection*, 2nd ed. Cham, Switzerland: Springer International Publishing, 2019.
[21] J. Galbally and M. Gomez-Barrero, "A review of iris anti-spoofing," in *2016 4th International Conference on Biometrics and Forensics (IWBF)*, 2016, pp. 1–6.
[22] P. Wild, P. Radu, L. Chen, and J. Ferryman, "Robust multimodal face and fingerprint fusion in the presence of spoofing attacks," *Pattern Recognit.*, vol. 50, pp. 17–25, Feb. 2016.
[23] A. da S. Pinto, H. Pedrini, W. Schwartz, and A. Rocha, "Video-Based Face Spoofing Detection through Visual Rhythm Analysis," in *2012 25th SIBGRAPI Conference on Graphics, Patterns and Images*, 2012, pp. 221–228.
[24] L. Li, P. L. Correia, and A. Hadid, "Face recognition under spoofing attacks: countermeasures and research directions," *IET Biom.*, vol. 7, no. 1, pp. 3–14, Jan. 2018.
[25] D. Gragnaniello, C. Sansone, G. Poggi, and L. Verdoliva, "Biometric Spoofing Detection by a Domain-Aware Convolutional Neural Network," in *2016 12th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS)*, 2016, pp. 193–198.
[26] Z. Akhtar, C. Micheloni, and G. L. Foresti, "Biometric Liveness Detection: Challenges and Research Opportunities," *IEEE Secur. Priv.*, vol. 13, no. 5, pp. 63–72, Sep. 2015.
[27] I. Chingovska, A. Anjos, and S. Marcel, "Anti-spoofing in action: joint operation with a verification system," *Proc. IEEE*, 2013.
[28] I. Chingovska, A. R. dos Anjos, and S. Marcel, "Biometrics Evaluation Under Spoofing Attacks," *IEEE Trans. Inf. Forensics Secur.*, vol. 9, no. 12, pp. 2264–2276, Dec. 2014.
[29] W. R. Schwartz, A. Rocha, and H. Pedrini, "Face spoofing detection through partial least squares and low-level descriptors," in *2011 International Joint Conference on Biometrics (IJCB)*, 2011, pp. 1–8.
[30] K. M. Sudar, P. Deepalakshmi, K. Ponmozhi, and P. Nagaraj, "Analysis of Security Threats and Countermeasures for various Biometric Techniques," in *2019 IEEE International Conference on Clean Energy and Energy Efficient Electronics Circuit for Sustainable Development (INCCES)*, 2019, pp. 1–6.
[31] A. Pinto, H. Pedrini, W. R. Schwartz, and A. Rocha, "Face Spoofing Detection Through Visual Codebooks of Spectral Temporal Cubes," *IEEE Trans. Image Process.*, vol. 24, no. 12, pp. 4726–4740, Dec. 2015.
[32] I. Chingovska, A. Anjos, and S. Marcel, "On the effectiveness of local binary patterns in face anti-spoofing," in *2012 BIOSIG - Proceedings of the International Conference of Biometrics Special Interest Group (BIOSIG)*, 2012, pp. 1–7.
[33] N. Kohli, D. Yadav, M. Vatsa, R. Singh, and A. Noore, "Detecting medley of iris spoofing attacks using DESIST," in *2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, 2016, pp. 1–6.
[34] Y. Atoum, Y. Liu, A. Jourabloo, and X. Liu, "Face anti-spoofing using patch and depth-based CNNs," in *2017 IEEE International Joint Conference on Biometrics (IJCB)*, 2017, pp. 319–328.

[35] A. Gumaei, R. Sammouda, A. M. S. Al-Salman, and A. Alsanad, "Anti-spoofing cloud-based multi-spectral biometric identification system for enterprise security and privacy-preservation," *J. Parallel Distrib. Comput.*, vol. 124, pp. 27–40, Feb. 2019.
[36] S. Kumar, S. Singh, and J. Kumar, "A comparative study on face spoofing attacks," in *2017 International Conference on Computing, Communication and Automation (ICCCA)*, 2017, pp. 1104–1108.
[37] C. Nagpal and S. R. Dubey, "A Performance Evaluation of Convolutional Neural Networks for Face Anti Spoofing," in *2019 International Joint Conference on Neural Networks (IJCNN)*, 2019, pp. 1–8.
[38] Z. Akhtar, G. Fumera, G. L. Marcialis, and F. Roli, "Evaluation of serial and parallel multibiometric systems under spoofing attacks," in *2012 IEEE Fifth International Conference on Biometrics: Theory, Applications and Systems (BTAS)*, 2012, pp. 283–288.
[39] T. de Freitas Pereira, A. Anjos, J. M. De Martino, and S. Marcel, "LBP − TOP Based Countermeasure against Face Spoofing Attacks," in *Computer Vision - ACCV 2012 Workshops*, 2013, pp. 121–132.
[40] D. Menotti *et al.*, "Deep Representations for Iris, Face, and Fingerprint Spoofing Detection," *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 4, pp. 864–879, Apr. 2015.