**Preparation and Implementation of a Biometric Authentication System**

Corbin Osman

American Public University System

ISSC325 – Biometrics

Dr. Harry Cooper

02/26/2023

**Abstract**

The security and protection of systems and information is important in the world that we live in today. Businesses, organizations and individuals alike face the threat of personal and confidential information being exposed to unauthorized parties, and the results of compromise can be disastrous for those affected. Whether an individual is protecting their own information, or an organization is securing their systems and servers, there are many options to ensure that confidential and sensitive information is secured, and its integrity protected.

This paper focuses on the protection of information and data through the use of biometric authentication systems. The primary target and audience will be businesses and organizations that use authentication and identification systems to secure access to physical locations and stored information and data. Biometric authentication and its use in security systems will be explained, and the planning and implementation of a biometric authentication system will be explored. Additional areas that will be included are strong practices in biometric authentication, potential vulnerabilities and considerations, and collected statistics for successful biometric authentication.

**Biometric Authentication and Biometric Systems**

In recent years there have been many advances in the field of identification. One recent advance and method for identifying an individual in security is through the use of biometrics. As shared by Navrup Tom in an article on biometric security, biometrics are “measurable human traits, characteristics, or behaviors that can be used to verify a person’s identity” (Tom, 2021). These traits or features are used to confirm that an individual identifying themself actually is who they say they are. Ensuring that all parties accessing secure locations are authorized to be doing so is critically important, especially for businesses that contain confidential information for employees and clients.

There are many methods of identification and authentication that can be utilized in both professional and personal environments, such as password-based and certificate-based authentication. Biometric authentication used in security is the practice of identifying an individual through biometrics features and authenticating them as one authorized to enter a location or access certain information. This can be used to secure a building or certain rooms and protect information and data held on servers and systems, which can prove useful in a business environment to ensure that those entering a location or accessing information are authorized to do so.

Biometrics authentication is performed by comparing the biometric features of an individual with biometric data that has been previously saved on the verifying system. An article on biometric authentication by Antonia Din offers insight into how this process is performed and how a biometric authentication system determines whether an individual is who they say they are. When an individual is identifying themselves, the biometric system will capture a feature or trait of the person, such as a fingerprint, an iris scan, or their voice. Once captured, the system will compare this feature to the biometric feature already saved in the system, such as a previously obtained fingerprint or iris scan. If the two features are nearly identical, the biometric system will determine that the individual identifying themselves is an authorized user, and they will then be authenticated to enter the location or access the information being secured by the system (Din, 2021).

With a better understanding of how a biometric system can be used to secure locations and information, as well as how such a system can analyze data to authenticate individuals, let us explore what to consider when planning and preparing to implement a biometric authentication system.

**Planning for the Implementation of a Biometric System**

When determining whether to implement and deploy a biometric system in an enterprise environment, there are many factors to consider and prepare for. A few points to consider are how the biometric system will fulfill and meet business security needs, what components should be chosen for the system, and how the system will comply with current existing business policies.

**How the Biometric System Will Fulfill Business Needs**

Most businesses and organizations that handle confidential and sensitive information have security policies and systems to help ensure information, employees and clients are safe and secure. When considering if a biometric system is the right choice of security for a place of business it is important to consider how such a system will meet the needs of securing a location or information.

An article on factors to consider when deploying a biometric system offers a few points to keep in mind and assess when preparing and deciding on implementation. The author, Billy Jones, shares these factors to consider improving business security. The first step that should be taken is to conduct an audit and analysis of the current business security infrastructure. This involves looking at current security systems and policies already implemented in the business and determining how a biometric system would work with pre-existing policies and systems (Jones, 2015).

Next it is important to consider what type of modality would be best for the new system. Biometrics offer a lot of different ways for one to identify themselves, and determining which form of authentication to use is important when implementing a biometric system. A few factors to consider when choosing the best biometric modality are shared by Mehedi Hassan, such as the accuracy of correctly authenticating individuals, accepting authorized persons, anti-spoofing protection, and the cost-effectiveness of the system being implemented (Hassan, 2016).

**Components to Choose for a Biometric System**

Continuing with the article by Billy Jones, another important factor to consider and explore is the large variety of components and options to choose from when implementing a new biometric system. Advancements in biometric technology are rapid and new types of hardware and software are being developed at a quick pace (Jones, 2015). Components and systems chosen should comply with business security policies, and if changes are needing to be made to fit the new system in with current security policies, these should be assessed and prepared for before deciding on which components to choose.

Similarly, it is important that businesses implementing a new biometric system determine how the cost could affect business needs. The prices for biometric components and systems can greatly vary in cost and ensuring that the return on investment for implementation of the system does not put the business in a difficult situation financially is also important. Depending on the size of the location being secured, multiple systems may be needed which should also be considered when determining costs for biometric systems.

**Implementing a Biometric System into Business Security Policy**

Businesses have security policies and procedures to ensure that information, employees, and clients are protected and secure. When implementing a new system or policy into a place of business, the addition should be assessed and performed in accordance with currently existing policies and procedures. This is to help ensure that vulnerabilities or breaches do not occur and that the security of business property and affiliates is not compromised. As offered by Joseph Mathenge in an article on security policy, three points to consider when implementing security policy are the value the policy brings to the organization, the trust needed of employees and customers, and an obligation to comply with established policies and procedures (Mathenge, 2021).

At times the implementation of a newer system or policy can require changes to be made in previously existing security policies and procedures. Whether changes are required, or new systems and policies comply with the previously established security measures, it is necessary for employees and clients to know what is expected and required of them to comply with business security requirements. Proper training and instruction should be given so that all understand how the new systems and policies will be used to identify and authenticate them for access.

**Integration and Deployment of a Biometric Authentication System**

Once the planning for a new biometric authentication system is complete and preparations are finished, the integration and deployment of the new system can be performed. Similar to the previous steps of careful planning and factors to consider, it is important to have an outline and plan to follow to ensure that all systems and policies implemented are done correctly and as authorized by the business.

**Process of Implementing a Biometric System**

As shared by Ravi Das in an article on project management when deploying biometrics, a clear picture should be in mind as to what the biometric system should look like and what its function and role will be in the place of business (Das, 2016). Having this idea of what is expected and knowing what steps to follow in order to achieve it is crucial for all business parties involved. Obstacles and set-backs can be avoided more easily when a plan for all to follow is presented and utilized by those involved with the implementation and maintenance processes.

The success of the deployment of the new biometric system greatly depends upon the work and planning performed beforehand. For example, the physical location where the biometric system will be located should be chosen in advance and prepared to make implementation simple. Similarly, other peripherals the system will require such as power and connection to the local network or internet must be prepared in order to connect with the system in the location it is being deployed (Das, 2016).

**Testing the Functionality of a Newly Integrated Biometric System**

Before a new biometric authentication system or policy is fully implemented and used it is important that testing of the system is performed to ensure that it functions as intended. This process and phase can be as extensive as the business would like, though no matter how much time is taken the testing should be thoroughly performed to ensure that the biometric system and functions are successful in identifying and authenticating users. When confidential information and secure locations are protected by a new system, businesses do not want unauthorized individuals accessing the data or areas because their system did not work as intended.

As with any security system, there are risks that should be considered during implementation and testing. One important factor to ensure is that the system is as accurate as possible in identifying and authenticating individuals. Blocking authorized individuals and allowing unauthorized individuals access can lead to problems for business and system security (Hiremath, 2022). Employee and client privacy can also be at risk if unauthorized users gain access to the stored biometric information, which could prove as a liability for the business. System failure is also a possibility, and when it does occur proper testing and analysis should be performed to identify the cause of failure and find a solution to repair it (Hiremath, 2022).

If testing and troubleshooting are not performed prior to full business use the drawbacks and consequences could lead to greater issues. While there may not be apparent issues or problems with the system or its functions, improper testing could lead to security vulnerabilities going unnoticed. These could lead to the exploitation of the current system, whether intentional or accidental, which would grant individuals access to locations or information when they may not legitimately be authorized to do so. If these vulnerabilities are caught during testing and troubleshooting, businesses can avoid unnecessary issues beforehand and better ensure the functionality of the new system and policies.

**Maintaining a Biometric Authentication System in Proper Condition**

Due to the amount of biometric information that will be stored for use with the biometric system, it is important that such pertinent information is kept secure from unauthorized access. This data, along with copies of it, should be maintained and secured through additional levels of security to ensure its integrity. Whether it is stored on a server or system in another location or kept on the biometric system itself, measures should be taken to ensure that access to this information is possible only by those authenticated to view it. This information, such as captured fingerprints, iris scans, or voice recordings, should be updated on a regularly scheduled basis to ensure that older copies cannot be used and that current captures are up to date to ensure that authentication success and denial rates are as accurate as possible.

Quality assurance is important in a business environment, and a biometric authentication system should also be designed to maintain a high level of security quality (M2SYS, 2016). Systems should be updated regularly to ensure that they are running the most up-to-date software and patches that fix potential bugs or vulnerabilities in the system. Regular testing can prove to be useful as well to ensure biometric devices and authentication work as intended.

**Strong Practices in Utilizing a Biometric Authentication System**

Once the biometric system has been fully integrated and policies are in place governing its use, it is critical that businesses maintain the system in working condition and employ good habits and practices to ensure its success in the business. As other biometric authentication methods may be implemented in business too, such as mobile device biometrics, it is critical that policies governing their use also be established to ensure that business information and assets remain secure.

It can be common for sensitive and confidential information to be viewed or sent using a personal device, which can prove harmful for a business as this information may reach the hands of unauthorized individuals. Policies should be in place governing the use of personal devices in the workplace to ensure that they are not used to collect or share sensitive information (Kinzer, 2022). Furthermore, implementing multi-factor authentication in the business can improve the level of security. This can be performed in many ways, such as requiring two forms of biometrics (fingerprint and iris, fingerprint and voice, etc.), or a combination of biometric-based and password-based. Due to users being familiar with biometric authentication as many mobile and personal devices employ fingerprint scanners or facial recognition software, biometrics can prove to be of comfort to some in granting access to premises or information (Kinzer, 2022).

Following the implementation of a biometric authentication system, some may still be wary or untrusting of biometrics and authentication. It can be beneficial in this scenario to help users see the benefits of using such a system and raise awareness on how their information and environment is secured through the system (Vakulov, 2022). As biometrics become more common and utilized in corporate environments, so too will the target be greater on biometric information. Hackers may attempt to access and capture biometric data, which means businesses should ensure that the information is stored in secure locations with trusted hardware and software that can only be accessed by those who need to do so (Vakulov, 2022).

**Conclusion**

When planning to implement and deploy a biometric authentication system in a corporate environment there are many factors to consider and prepare for. Proper planning and integration are critical to ensure that implementation is done correctly and that the level of security is strengthened and not lowered. Important factors to consider are components to choose from, which modalities to utilize, acceptance and rejection levels, additional methods that can be used for multi-factor authentication, and how training will be performed to raise understanding and awareness in the business.

Businesses and organizations handle a large amount of sensitive and confidential information, whether it be business property or the information of employees and clients. Ensuring the security and integrity of this information should be a top priority for corporate entities, and the implementation of a biometric authentication system can provide a strong level of physical security to protect important information and property.

References

Das, R. (2016, November 22). A Project Management Guide to Deploying Biometrics: The Basics. *Resources.infosecinstitute.com*. https://resources.infosecinstitute.com/topic/a-project-management-guide-to-deploying-biometrics-part-1/

Din, A. (2021, July 15). What is Biometric Authentication? A Complete Overview. *Heimdalsecurity.org*. https://heimdalsecurity.com/blog/biometric-authentication/

Hassan, M. (2016, October 22). 5 Factors to Consider in Choosing the Best Biometric Modality. *M2sys.com*. https://www.m2sys.com/blog/biometric-resources/5-factors-consider-choosing-best-biometric-modality/

Hiremath, O. (2022. August 8). Risks and Benefits of Biometrics in Security. *Softwaresecured.com*. https://www.softwaresecured.com/risks-and-benefits-of-biometrics-in-security/

Jones, B. (2015, March 31). 5 Things to Consider Before Deploying a Biometric System for Your Business. *M2sys.com*. https://www.m2sys.com/blog/workforce-management/5-things-to-consider-before-deploying-a-biometric-system-for-your-business/

Kinzer, K. (2022, May 17). How to Keep Biometric Information Secure. *Jumpcloud.com*. https://jumpcloud.com/blog/how-to-keep-biometric-information-secure

Mathenge, J. (2021, February 26). IT Security Policy: Key Components and Best Practices for Every Business. *Bmc.com*. https://www.bmc.com/blogs/it-security-policy/

M2SYS. (2016, January 3). Why Biometric Data Testing is Important for QA. *M2sys.com*. https://www.m2sys.com/blog/guest-blog-posts/why-biometric-data-testing-is-important-for-qa/

Tom, N. (2021, May 24). What Are Biometrics? The Pros/Cons of Biometric Security. *Auth0.com*. https://auth0.com/blog/what-are-biometrics-the-proscons-of-biometric-security/

Vakulov, A. (2022, June 17). Biometric Authentication: Best Practices. *Dzone.com*. https://dzone.com/articles/biometric-authentication-best-practices