International Research Journal of
SCIENCE, TECHNOLOGY, EDUCATION, AND MANAGEMENT
P-ISSN: 2799-063X | E-ISSN: 2799-0648
ISO 9001:2015 Certified
Volume 3, No. 2 | June 2023

Integration biometrics in web application: Security for web apps

Wulandari Kusuma Herdanu[1], Rabab Alayham Abbas Helmi[2], Mariana Syamsudin[3]
[1,2]*Management & Science University, Malaysia*
[3]*Pontianak State Polytechnic, Indonesia*
Corresponding email: wulandari.herda15@gmail.com

ABSTRACT

To evaluate the effectiveness of biometric security systems, an information theoretic framework is constructed. First, two performance metrics privacy, determined by the biometric measurements' normalized equivocation rate, and security, determined by the biometric measurements' key generation rate are specified. Then, it is decided that there is a fundamental tradeoff between these two measurements. First, we investigate the case where a potential attacker has no side knowledge. For this situation, the privacy-security region which defines the tradeoff mentioned above is derived. In perfect privacy biometric security systems, common knowledge among random variables plays a significant role. The case where the adversary possesses side knowledge is then considered. In this scenario, the privacy-security tradeoff has inner and outside bounds. Client-server and locally installable apps, which are getting older, have lost a considerable amount of market share to web applications. It is now possible because of some special benefits that web applications provide. They can function just as well as locally installed software and are accessible through web browsers without the need for installation or upkeep. Due to the lack of resources required by enterprises to administer them locally, web applications have gained popularity more swiftly. Now that new technologies, standards, and APIs have been developed, it is possible to employ more information security safeguards. The following sections of this article go into greater detail about web apps, web-based biometrics, and the integration of biometric authentication in web applications.

ARTICLE INFO

Received : May 25, 2023
Revised : June 18, 2023
Accepted : June 30, 2023

KEYWORDS

Biometrics, Security, Web apps

Suggested Citation (APA Style 7th Edition):

Herdanu. W.K., Helmi, R.A.A., & Syamsudin, M. (2023). Integration biometrics in web application: Security for web apps. *International Research Journal of Science, Technology, Education, and Management*, 3(2), 103-116. https://doi.org/10.5281/zenodo.8139747

INTRODUCTION

Despite being rapidly expanding industry today, biometric security is an old technology. Research on manually identifying fingerprints dates back to the 19th century, and iris recognition technology dates back to 1936. In the last few years, biometric technology has also expanded in the banking, retail, and mobile sectors. Unlike more conventional identification techniques like personal ID cards, magnetic cards, keys, or passwords, which can be easily compromised by theft, collusion, or loss, biometric technology is inherently connected to an individual person.

Client-server and locally installable apps, two ageing competitors, have lost a sizable portion of their market share to web applications. Due to the special benefits that web apps provide, it is now conceivable. They can perform just as well as locally installed applications without the installation and maintenance because they are accessible through web browsers. The lack of resources required by organizations to maintain web applications locally has also aided in their adoption.

Web apps have gained popularity and appeal among both business and consumer users due to a variety of additional variables. Because of advances in web development technology, wider access to the internet, faster bandwidth, competitive subscription costs, and the involvement of large corporations like Google, Amazon, Microsoft, etc., web apps have evolved into what they are today.

Because they can be accessed from anywhere via a URL, web apps need extra protection. In contrast to locally installed apps, which can also be secured with physical security access control, web applications lack this advantage. In the authentication phase, templates from the database were compared to the biometric data that had been acquired. Students' biometric data is recorded throughout class with either knowledge or ignorance. Since most face-based systems are contactless, pupils are unaware of the timing of the attendance check.

Integration of biometric fingerprints in web applications is essential for enhancing security in the field of web application development. Biometric fingerprints provide a robust and unique identifier for individuals, making them more secure and reliable than traditional password-based methods. They also reduce the risk of unauthorized access or impersonation by verifying the user's identity based on their unique biometric traits. Additionally, biometric fingerprints are inherently unique to each individual and difficult to replicate, making them highly resistant to identity theft and fraud. Finally, biometric fingerprint authentication offers a seamless and user-friendly experience.

The integration of biometric fingerprints in web applications is important and relevant to the field of web application security due to its ability to enhance authentication, mitigate vulnerabilities, resist identity theft, improve user experience, comply with regulations, and provide future-proof security measures. This can lead to higher user satisfaction and increased adoption of web applications, compliance with security standards and regulations, and future-proof security measures. Biometric fingerprint authentication provides a future-proof security measure by leveraging unique biological traits that are difficult to counterfeit. These aspects contribute to building a secure and trusted environment for users and businesses alike.

OBJECTIVES OF THE STUDY

This study's main goal is to undertake an in-depth analysis of Integration Biometrics In Web Application. In addition to identifying potential difficulties and potential avenues for future research, the review attempts to offer insights into the most recent state-of-the-art techniques and accomplishments in the fields. Specific objectives of the study include:

1. To investigate how biometrics system can be integrated into a website and the input will increase the security of a website;

2. To identify which biometrics that suitable to device nowadays;
3. To evaluate the purposes biometrics in terms of security and usability.

By accomplishing these objectives, this review aims to provide researchers and practitioners with a comprehensive understanding of the current state of Web-Based Biometrics Integration and serve as a foundation for further advancements in this rapidly evolving field.

MATERIALS AND METHODS

The goal of this project is to build a web-based computer centre that connects all system addresses to the programme server and employs biometric fingerprints for authentication and verification. Platform and cross-platform authenticators are the two main types. On many devices, cross-platform authenticators can be utilised. Platform authenticators are connected to a particular gadget, like a phone. Most biometric authenticators geared towards consumers are built within an operating system like iOS, Android, or Windows(Alay & Al-Baity, 2020). They are therefore platform authenticators because they are connected to a specific device.

Whether an authenticator tests for user presence or user verification is another crucial factor. User presence just shows that someone made an "authorization gesture" with the authenticator, which may have been as simple as clicking a button(Richardson et al., 2022). If you're employing an authenticator as a part of a multi-factor authentication procedure, such a presence test is helpful. On the other side, user verification provides confirmations that the user who authenticated is in fact who we believe they are. This can be done by asking them for something they know or, in the case of biometrics, by using a characteristic of the user, like the size of their face(Ali et al., 2018). The majority of the time, you'll be looking for user verification, which is what the typical biometric authenticators offer.

The integration of biometric fingerprints in web applications is essential for enhancing security in the field of web application development. Biometric fingerprints provide a robust and unique identifier for individuals, making them more secure and reliable than traditional password-based methods. They also reduce the risk of unauthorized access or impersonation by verifying the user's identity based on their unique biometric traits. Additionally, biometric fingerprint authentication offers a seamless and user-friendly experience. This allows users to access web applications and authenticate themselves quickly and conveniently with a simple touch of their finger, streamlining the authentication process and enhancing the overall user experience(Yadav et al., 2020). It also helps organizations comply with security standards and regulations and demonstrate their commitment to data security and user privacy. Finally, it provides a future-proof security measure by leveraging unique biological traits that are difficult to counterfeit(Ayo et al., 2021).

In order to build this project, we will employ a quantitative method approach, namely a survey, in which the same, structured questions are asked of a large number of respondents. The replies are then gathered, processed, and analysed. The likert scale with the following levels will be used to collect data while utilising this survey method: Very satisfied, Satisfied, Neutral, Not satisfied, and Very Dissatisfied.

After getting the problems and research objectives, data collection is carried out to get an overview of the system with the features that are really needed and related to the phenomena that occur. In this case the author chose a survey with a target of 30 respondents who have close access to the author such as family and friends where respondents will receive questionnaires that must be filled out.

RESEARCH METHOD

The choice of research method should align with the research objectives and questions related to the integration of biometric fingerprints in web applications for security purposes. Surveys can be a valuable research method,

but it is important to consider their suitability in this context. Data Collection Needs: Surveys are well-suited for collecting quantitative data, such as demographic information, user preferences, or self-reported experiences.

Ethical Considerations: Consider the ethical implications of collecting sensitive information, such as biometric data, through a survey. Additional research methods may be worth considering, such as user testing and usability studies to evaluate the effectiveness and user experience of biometric authentication in web applications. By considering the research objectives, questions, data needs, and ethical considerations, you can select the most appropriate research methods, which may include surveys along with other methods, to address the integration of biometric fingerprints in web applications for security.

DEVELOPMENT METHODOLOGY

In development, this system will be using a Software Development Life Cycle called Agile. Agile is a suitable method for this development which does not require many teams in this case individually and requires a relatively short time for each change in each process. In this method there are several steps to be carried out as shown in the statement below.

Agile integration of biometric fingerprints in web applications aligns well with the project's requirements, particularly in terms of flexibility and shorter development cycles. Here is the explanation:

- Flexibility: Agile methodologies, such as Scrum or Kanban, emphasize adaptability and flexibility in the development process.
- Integrating biometric fingerprints in web applications using an agile approach allows for iterative development and enables the project team to respond to changing requirements or emerging challenges.
- This flexibility ensures that the integration of biometric fingerprints can be seamlessly incorporated into the development process without disrupting the overall project timeline.
- Incremental Development: Agile methodologies promote incremental development, where features and functionalities are delivered in smaller increments or iterations.
- This approach allows for early integration of biometric fingerprint authentication into the web application, enabling the project team to gather feedback and validate its effectiveness at an early stage.
- It also allows for rapid iterations and improvements based on user feedback or changing security requirements.
- Continuous Integration and Testing: Agile methodologies encourage continuous integration and testing practices, ensuring that the integrated biometric fingerprint authentication is thoroughly tested throughout the development process.
- Regular testing and integration of biometric fingerprints help ensure a seamless and secure authentication experience for users.
- Collaboration and Communication: Agile methodologies emphasize close collaboration and effective communication within the project team and stakeholders.
- Shorter development cycles facilitate rapid deployment of security features and allow the project team to adapt to evolving security requirements efficiently.
- User-Centric Approach: Agile methodologies prioritize a user-centric approach by involving users and stakeholders in the development process.
- Regular feedback from users and usability testing can help refine the integration and address any usability or privacy concerns associated with biometric authentication.

By adopting an agile approach to the integration of biometric fingerprints in web applications, development teams can maintain flexibility, deliver incrementally, ensure continuous testing, facilitate collaboration, adhere to shorter development cycles, and prioritize user needs. This approach aligns with the

project's requirements and helps to build a secure and user-friendly web application with integrated biometric authentication.

When evaluating privacy and security in the context of integrating biometrics, such as fingerprint authentication, into web applications, several metrics can be considered. Here are some common metrics and methodologies used:

a. False Acceptance Rate (FAR) : a metric that tracks the frequency with which access is inadvertently granted to unauthorised people.
b. Better security is indicated by a lower FAR.
c. False Rejection Rate (FRR): FRR tracks the frequency with which legitimate users are wrongfully refused access.
d. Equal Error Rate (EER): This statistic shows where the FAR and FRR are equal.
e. It is employed to evaluate the overall effectiveness of various biometric systems.
f. Lower EER values represent overall superior performance.
g. Receiver Operating Characteristic (ROC) Curve: The ROC curve shows how the FAR and FRR relate at different decision thresholds.
h. It offers a visual depiction of the system's functionality and enables comparison of various operating points.

To derive the privacy-security region and the inner and outer bounds, a systematic methodology is required.

Here's a general approach:

a. System Analysis: Analyse the web application and its security requirements.
b. Identify the potential privacy and security risks associated with integrating biometrics.
c. Threat Modelling: Identify potential threats to the system's privacy and security.
d. Performance Evaluation: Evaluate the performance of the integrated biometric system using the defined metrics (e.g., FAR, FRR, EER).
e. Privacy Evaluation: Assess the system's privacy aspects, considering factors like data collection, storage, and usage.
f. Evaluate compliance with privacy regulations (e.g., GDPR) and ensure that user consent and data protection measures are implemented.
g. Iterative Optimization: Based on the evaluation results, refine the system and security measures iteratively to achieve the desired privacy-security balance.
h. This may involve adjusting system parameters, fine-tuning algorithms, or enhancing data protection mechanisms.

Construction of the Information Theoretic Framework:

In the context of integrating biometrics, such as fingerprint authentication, into web applications, constructing an information theoretic framework involves quantifying the information content, privacy, and security aspects of the system. In order to facilitate the investigation of the privacy-security trade-off, this framework tries to offer a formal description of the interactions between these components.

Analysis of the Privacy-Security Trade-off:

The tension that exists between preserving user privacy and implementing effective security measures is referred to as the privacy-security trade-off. Analysing this trade-off involves examining the impact of different security measures on user privacy and vice versa. It requires evaluating the potential risks and benefits associated with integrating biometrics into web applications.

Advantages of Web Applications:

Web applications offer several advantages for integrating biometric authentication:

1. Accessibility: Web applications can be accessed from various devices with an internet connection, enabling widespread usage and user convenience.
2. Scalability: Web applications can handle many users concurrently, making them suitable for scenarios with high user volumes.
3. Cross-Platform Compatibility: Web applications can run on different operating systems and platforms, providing flexibility for users.
4. Easy Updates and Maintenance: Web applications can be easily updated and maintained, ensuring that security patches and improvements can be implemented seamlessly.

Incorporation of Integration Biometrics Fingerprint in Web Application: Security for Web Apps:

Incorporating integration biometrics, specifically fingerprint authentication, into web applications enhances security and user experience. Some key benefits include:

1. Strong Authentication: Fingerprint authentication provides a high level of security, as fingerprints are unique to individuals and difficult to forge.
2. User Convenience: Fingerprint authentication offers a convenient and user-friendly way to access web applications, eliminating the need to remember and enter complex passwords.
3. Multi-Factor Authentication: Fingerprint authentication can be combined with other authentication factors, such as passwords or tokens, to create a multi-factor authentication approach, further strengthening security.
4. Rapid Authentication: Fingerprint recognition is fast and efficient, allowing users to authenticate quickly and seamlessly.
5. Enhanced Security: Incorporating biometric authentication adds an additional layer of security to web applications, reducing the risk of unauthorized access and identity theft.

By considering these advantages and understanding the privacy-security trade-off, web application developers can design and implement integration biometrics, such as fingerprint authentication, in a manner that balances security, usability, and privacy concerns effectively.

Implementing web-based biometric authentication systems, including integration biometrics like fingerprint authentication, comes with practical implications and challenges. Here are some key considerations:

a. User Acceptance: The success of biometric authentication systems depends heavily on user acceptability. Some users may have concerns about privacy and the security of their biometric data.
b. Usability and User Experience: Biometric authentication systems should be designed with usability in mind.
c. Biometric Data Storage and Protection: Storing and protecting biometric data is crucial to maintain the security and privacy of users.
d. Regulatory and Legal Compliance: Integrating biometric authentication into online applications necessitates adherence to all necessary laws and standards, including those governing data protection (such as the GDPR).
e. Ensuring compliance with privacy and security requirements, obtaining necessary consents, and handling sensitive biometric data in a lawful and ethical manner are essential considerations.
f. Interoperability: Biometric authentication systems used in web applications should be interoperable with different devices, browsers, and platforms.

Addressing these practical implications and challenges requires a comprehensive approach, involving collaboration between experts in biometrics, web development, security, and privacy. Thorough risk assessments, usability testing, and continuous evaluation of the system's performance and user feedback are crucial to ensure the successful implementation of integration biometrics, like fingerprint authentication, in web applications.

Real-world case studies about tradeoff between privacy and security

1. Case Study: Mobile Banking App

Scenario: A mobile banking app wants to enhance its security by implementing fingerprint authentication for users to access their accounts.
Tradeoff: The tradeoff here lies between the improved security provided by fingerprint authentication and the potential privacy concerns associated with collecting and storing users' biometric data.
Decision-Making Process: The app developer assesses the risks and benefits, considering factors such as the sensitivity of the data involved, regulatory requirements, and user preferences. They may implement strong security measures to protect the biometric data, communicate the security measures clearly to users, and provide an opt-out option for those who have privacy concerns. User feedback and market research help inform the decision-making process.
Insights: In this case, the convenience and enhanced security offered by fingerprint authentication outweigh the potential privacy concerns for most users. By implementing robust security measures and respecting user choices, the app strikes a balance between privacy and security.

2. Case Study: Airport Security System

Scenario: An airport security system wants to expedite the security screening process by implementing biometric fingerprint authentication for frequent travelers.
Tradeoff: The trade-off here is between increasing security by precisely identifying passengers and potential issues with the collecting, storage, and sharing of biometric data in a delicate context.
Decision-Making Process: The airport authority conducts a thorough privacy impact assessment, taking into account legal obligations, user expectations, and the sensitivity of the data. They implement strict data protection measures, such as encryption and access controls, and ensure compliance with relevant privacy regulations. Additionally, they provide clear communication about the purpose and handling of biometric data to gain user trust.
Insights: The airport security system recognizes the importance of maintaining a high level of security while addressing privacy concerns. By implementing appropriate safeguards and maintaining transparency, the system balances privacy and security considerations to improve the efficiency of the security screening process.

3. Case Study: Employee Time and Attendance System

Scenario: A company wants to implement a web-based biometric fingerprint authentication system for employees to clock in and out of work.
Tradeoff: The tradeoff here lies between accurate time and attendance tracking, which improves efficiency, and employee concerns about privacy and potential misuse of biometric data.
Decision-Making Process: The company engages in open dialogue with employees, addressing their privacy concerns and ensuring that their consent is obtained for using biometric data. Strong security measures are put in place to protect the biometric templates, and regular training is provided to employees on the system's security features and their rights related to data protection.
Insights: In this case, the company acknowledges the importance of addressing employee privacy concerns and involving them in the decision-making process. By implementing robust security measures and respecting

employee rights, the system strikes a balance between privacy and security, leading to accurate time and attendance tracking while maintaining trust among employees.

These case studies highlight that the decision-making process for implementing integration biometrics in web applications involves carefully weighing privacy and security considerations, evaluating risks and benefits, and implementing appropriate safeguards. Transparency, user engagement, and compliance with privacy regulations are essential to achieving the desired balance between privacy and security.

Emerging technologies like machine learning and blockchain have the potential to significantly enhance the privacy and security of integration biometrics, specifically fingerprint authentication, in web applications. Here's how these technologies can make an impact:

Machine Learning

Machine learning techniques can improve the accuracy and robustness of integration biometric systems while addressing privacy concerns. Here's how:

a) Anti-Spoofing: Machine learning algorithms can be trained to detect and differentiate between real fingerprints and spoofing attempts, such as artificial fingerprints or photos. By incorporating anti-spoofing measures based on machine learning, the system becomes more resilient to attacks, enhancing security.
b) Feature Extraction and Matching: Machine learning algorithms can extract pertinent elements from fingerprint data and carry out effective matching, enhancing the biometric system's overall functionality and precision. This improves security and usability by lowering the frequencies of erroneous acceptance and rejection.
c) Privacy-Preserving Techniques: Machine learning models can be trained using privacy-preserving techniques such as federated learning or differential privacy. These methods allow the training of models without the need for centralizing or sharing sensitive biometric data, thus mitigating privacy risks.

Blockchain

Blockchain technology, with its decentralized and immutable nature, can address privacy and security concerns related to the storage and sharing of biometric data. Here's how blockchain can contribute:

a) Data Integrity and Security: By storing biometric data on a blockchain, it becomes highly secure and tamper-proof. Data is distributed across several nodes because to the blockchain's decentralised design, making it harder for hackers to change or compromise the data.
b) User Control and Consent: Blockchain-based systems can empower users to have control over their biometric data. Users can grant and revoke access to their data using cryptographic keys and smart contracts, ensuring their privacy preferences are respected.
c) Auditability and Transparency: Blockchain provides an auditable and transparent record of data access and transactions. This enables traceability and accountability, ensuring that data usage is transparent and adheres to privacy regulations.
d) Interoperability and Trust: Blockchain can facilitate secure and trusted interoperability between different entities involved in the biometric authentication process, such as web applications, authentication providers, and identity verification services. It enables seamless and secure exchange of data while maintaining privacy.

It's important to note that the adoption of these emerging technologies in integration biometrics should be done with careful consideration of their limitations, implementation challenges, and potential ethical

implications. Thorough risk assessments, industry standards, and regulatory compliance should guide the integration process to ensure the privacy and security enhancements are effectively implemented.

Legal and ethical considerations are crucial

When integrating biometrics, notably fingerprint authentication, in web applications, legal and ethical considerations are crucial. Here are some key considerations:

- Data Privacy Regulations: Integration biometrics involve the collection, storage, and processing of sensitive biometric data.
- It is essential to comply with data privacy regulations, such as the General Data Protection Regulation (GDPR) in the European Union, which outline specific requirements for the handling of personal data, including biometric information.
- User Consent: Respecting user consent is crucial when implementing integration biometrics.
- Biases and Discrimination: Integration biometrics systems, including fingerprint authentication, must be designed and implemented in a way that avoids biases and discrimination.
- Transparency and Accountability: Organizations implementing integration biometrics should prioritize transparency and accountability.
- Organizations should conduct ethical reviews to assess the potential risks and benefits of using biometric data.
- By addressing these legal and ethical aspects, organizations can promote user trust, protect privacy rights, and mitigate potential risks and harms associated with integration biometrics in web applications.
- Compliance with data privacy regulations and ethical guidelines helps ensure that biometric data usage is transparent, fair, and respectful of individual rights and dignity.

Biometric technology, particularly fingerprint authentication, has made significant advancements and found widespread applications in various industries, including banking, retail, and the mobile sector. Here are some specific advancements and applications that showcase the current state of biometric technology:

Banking Industry:

Biometric technology has revolutionized the banking sector by providing secure and convenient authentication methods. Some advancements and applications include:

a. Fingerprint-based ATM and Branch Authentication: Banks have implemented fingerprint authentication on ATMs and in branches, enabling customers to access their accounts securely without the need for PINs or passwords.
b. Mobile Banking: Biometric authentication, such as fingerprint recognition, has been integrated into mobile banking applications. Users can conveniently and securely access their accounts, authorize transactions, and perform various banking activities using their fingerprints.
c. Secure Payment Authorization: Biometrics, including fingerprints, are used for secure payment authorization in mobile wallets and payment apps. Users can authenticate transactions using their fingerprints, adding an extra layer of security.

Retail Industry:

Biometric technology has found applications in the retail sector, enhancing security and improving customer experiences. Some advancements and applications include:

a. Point of Sale (POS) Systems: Retailers have integrated biometric fingerprint authentication into POS systems. This helps prevent unauthorized access, enables secure cashier logins, and facilitates streamlined transactions.
b. Loyalty Programs: Biometric identification, such as fingerprint scanning, can be used for enrollment and verification in customer loyalty programs. This enables personalized and secure rewards and promotions for customers.
c. Loss Prevention: Biometric systems, such as fingerprint recognition, can be used for employee access control and authorization in areas with restricted inventory or high-value items, reducing the risk of theft or unauthorized access.

Mobile Industry:

The mobile industry has been at the forefront of adopting biometric technology, with fingerprint authentication becoming a standard feature in many smartphones. Advancements and applications include:

a. Unlocking Devices: Fingerprint sensors integrated into smartphones allow users to unlock their devices securely and conveniently using their fingerprints, replacing traditional PINs or patterns.
b. App Authentication: Biometric authentication is used to secure individual apps, ensuring that only authorized users can access sensitive data within specific applications.
c. Mobile Payments: Biometric authentication, such as fingerprint recognition, is widely used to authenticate mobile payments through mobile wallets or payment apps, providing a secure and convenient payment experience.

These advancements and applications highlight how biometric fingerprint technology has become an integral part of web applications in the banking, retail, and mobile industries. The technology offers improved security, convenience, and personalized experiences for users, transforming the way authentication and authorization are conducted in various sectors.

The discussion on the growing popularity of web applications and their benefits compared to client-server and locally installable apps is relevant for Integration Biometrics Fingerprint in Web Application: Security For Web Apps. The explanations below:

a. Accessibility and User Convenience:
Web applications offer greater accessibility and convenience with biometric authentication, eliminating the need for installable apps.
b. Cross-Platform Compatibility:
Biometrics enable cross-platform compatibility, allowing users to access and authenticate themselves.
c. Lower Development and Maintenance Costs:
Web applications with integration biometrics can be more cost-effective than client-server or locally installable apps.
d. Seamless Updates and Version Control:
Web applications with integration biometrics benefit from seamless updates and version control, reducing the need for manual updates.
e. Enhanced Security and Data Privacy:
Biometrics can be securely transmitted and stored on the server side, reducing risk of unauthorized access and data breaches.

While client-server and locally installable apps may still be relevant in certain contexts, the growing popularity of web applications with integration biometrics showcases the benefits they offer in terms of accessibility, cross-platform compatibility, cost-effectiveness, seamless updates, and enhanced security. These

advantages make web applications a compelling choice for implementing integration biometrics, such as fingerprint authentication, in the context of web-based security applications.

The integration of biometric fingerprints in web applications for security purposes brings both benefits and potential risks that need to be addressed. Here are some potential risks and vulnerabilities associated with the integration of biometric fingerprints in web applications:

1. Securing Biometric Data during Transmission:
   Encryption protocols such as TLS can be used to ensure secure transmission of biometric data, protecting confidentiality and integrity.
2. Spoofing and Impersonation Attacks:
   Anti-spoofing measures must be implemented to detect and prevent spoofing and impersonation attacks, such as liveness detection techniques.
3. Privacy Concerns:
   Biometric fingerprints should be handled and stored in compliance with data protection laws and regulations, and privacy policies should be communicated to users.
4. Potential Database Breaches:
   Implementing security measures such as access controls, encryption, and regular audits can help mitigate the risk of database breaches and protect stored biometric data.
5. User Acceptance and Perception:
   Transparent communication and informed user consent are essential for establishing trust and ensuring user acceptance of biometric authentication.

Addressing these risks and vulnerabilities requires a holistic approach that combines strong security measures, privacy safeguards, user education, and compliance with relevant regulations. By implementing robust security protocols, anti-spoofing techniques, privacy-preserving practices, and transparent communication, the integration of biometric fingerprints in web applications can be made more secure and trustworthy for users.

The integration of biometric fingerprints in web applications for security purposes brings both benefits and potential risks that need to be addressed. Here are some potential risks and vulnerabilities associated with the integration of biometric fingerprints in web applications:

a. Securing Biometric Data during Transmission:
   Encryption protocols such as TLS can be used to ensure secure transmission of biometric data, protecting confidentiality and integrity.
b. Spoofing and Impersonation Attacks:
   Anti-spoofing measures must be implemented to detect and prevent spoofing and impersonation attacks, such as liveness detection techniques.
c. Privacy Concerns:
   Biometric fingerprints should be handled and stored in compliance with data protection laws and regulations, and privacy policies should be communicated to users.
d. Potential Database Breaches:
   Implementing security measures such as access controls, encryption, and regular audits can help mitigate the risk of database breaches and protect stored biometric data.
e. User Acceptance and Perception:
   Transparent communication and informed user consent are essential for establishing trust and ensuring user acceptance of biometric authentication.

Addressing these risks and vulnerabilities requires a holistic approach that combines strong security measures, privacy safeguards, user education, and compliance with relevant regulations. By implementing

robust security protocols, anti-spoofing techniques, privacy-preserving practices, and transparent communication, the integration of biometric fingerprints in web applications can be made more secure and trustworthy for users.

RESULTS AND DISCUSSION

The Web Authentication API enables web applications to give users access to an authenticator through a user agent (often a hardware token that can be accessible by USB, BLE, or NFC or a platform-integrated module). can be used to create (eTLD+k) public key credentials for applications. This opens up a number of application scenarios, including: An example of low-friction 2FA that is phishing-resistant is when it is combined with passwords. biometric-based re-authentication without a password. Low-friction, phishing-resistant two-factor authentication without passwords provided by (Praseetha et al., 2018).

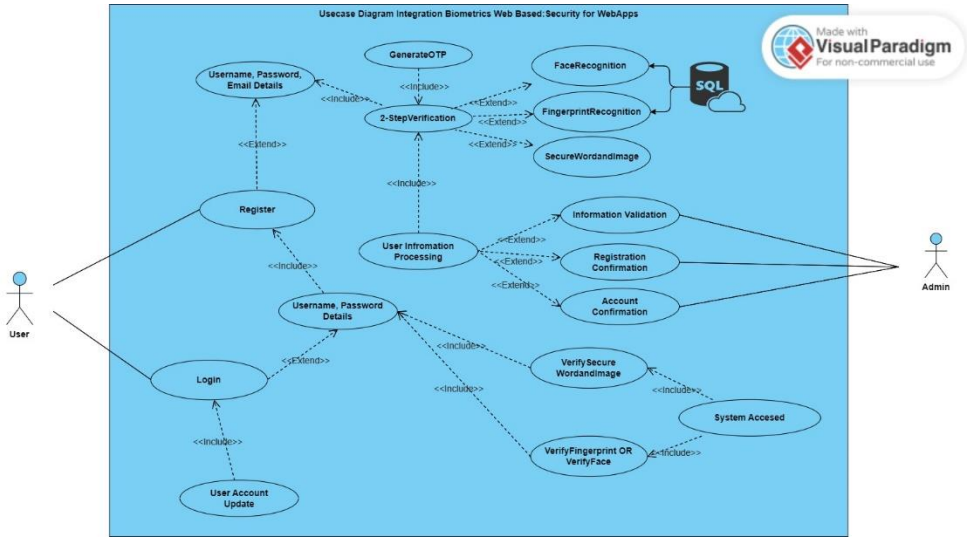

Figure 1.0 Use Case Design

Through a web browser, users can utilise biometrics to identify themselves to websites by using their behavioural traits. In applications for access control, device login, cell phones, attendance tracking, and other things, biometrics have essentially taken the place of passwords and his PIN. To make the authentication procedure more streamlined and safer, Hover uses biometrics in his web application (Kabir et al., 2021).

Without needing to be downloaded or installed on your device, the web application functions as standalone software that can be viewed from your browser. Therefore, only the browser may be used for biometric authentication. Through an application programme interface (API), a web browser connects to a web application server and a local biometric device. Email and SNS accounts can both employ biometric authentication (Vibin Mammen et al., 2020).

Web-based biometric authentication is a technique that involves programming biometric authentication over the Internet. With web-based biometrics, users log into Internet resources using a browser after being authenticated by a biometric identifier. This method of authentication can be utilised with a variety of secure online resources, including web apps, email accounts, and many more (Toli & Preneel, 2018).

Web applications must have the right hardware and software support in order to use biometrics. Users can easily install the SDK on their system and link their biometric device. The integration of biometrics into a website can be done in a variety of ways (Rahman et al., 2018).

Manufacturers of biometrics can offer APIs to developers so they can connect to their technology. Such APIs have the drawback of only working with specific hardware. Fast Identity Online (FIDO) and the World Wide Web Consortium (W3C) have developed Web-Authn and a new standard called Biometric identification in Web apps to satisfy the growing demand for a single standard for biometric identification in web apps. Major corporations including Google, Microsoft, Mozilla, PayPal, and Qualcomm endorse this standard. Through browsing, consumers are able to employ biometrics on her websites and applications refer to (Baig & Eskeland, 2021).

This is where biometrics can potentially enable seamless authentication for any web application. Biometrics allow employees to mark their presence at their desk or remotely on their computer. Their presence is only marked when the employee logs into the work application. Ultimately, the advent of multi-biometric identities on the Internet will allow users to lose their password and her PIN(Sujana & Reddy, 2021) .

To authenticate your users, you can construct and use origin-based public key credentials using the Web Authentication API, often known as Web-Authn. The API allows the usage of platform authenticators that enable user authentication using a fingerprint or screen lock, as well as roaming U2F or FIDO2 authenticators (also known as security keys), BLE, NFC, and USB (Lv et al., 2021).

When a website must demonstrate that it is communicating with the right user A list of the user's registered credentials is provided to the browser by the relying party, which also generates a query. Additionally, you can specify the location of the credentials (Ademola et al., 2019).

An external authenticator via USB, BLE, etc., or a built-in local authenticator. The browser requests that the challenge be signed by the authenticator. After obtaining the user's permission, the authenticator returns a signed assertion to her web app if it contains any of the supplied credentials. The web application sends the signed assertion to the server for the relying party to validate. The server verifies the results, and the authentication flow is deemed successful(Yang et al., 2021).

Web Authentication API, often known as Web-Authn, is a reliable technology that provides password-less or low-friction two-factor authentication in web applications. In order to integrate biometric fingerprints and increase security, the Web Authentication API can be used in applications and use cases such fingerprint-based two-factor authentication, password-less authentication, and multi-factor authentication with biometrics(Ali et al., 2020).

The Web Authentication API provides strong protection against phishing attacks, as it relies on public-key cryptography and ensures that authentication credentials are securely transmitted, and that the authenticity of the web application is verified. Cross-Platform Compatibility: The Web Authentication API is supported by major web browsers and operating systems, making it a widely compatible solution. Integrating biometric fingerprints into a web application involves several steps and techniques, such as using Biometric APIs, Web-Authn, Server-Side Integration, and Template Extraction and Storage. The integration process involves using the biometric API or libraries to capture the user's fingerprint, verifying it against the stored template, and granting access.

Security considerations include implementing secure communication protocols, encrypting, and securely storing the biometric templates, and implementing robust access controls. Developers should refer to the documentation and resources provided by the biometric device manufacturer or relevant industry standards to implement the integration effectively and securely.

CONCLUSION AND RECOMMENDATION

A tool for authentication is biometrics, which are a person's distinctive bodily traits. It is not perfect, though, just like every other type of verification. Examples include the use of a fake hand to bypass vein authentication and false fingerprint software. This article contends that rather than being utilised as a stand-alone authentication technique, biometrics should be a part of a multi-factor authentication scheme to boost security.

Integrating biometric fingerprints into a web application involves using Biometric APIs, WebAuthn, Server-Side Integration, and Template Extraction and Storage. Integrating biometric fingerprints into web applications requires security considerations such as secure communication protocols, encryption, and access controls to ensure privacy and security of biometric data.

REFERENCES

Ademola, A., Somefun, T. E., Agbetuyi, A. F., & Olufayo, A. (2019). Web based fingerprint roll call attendance management system. *International Journal of Electrical and Computer Engineering*, 9(5), 4364–4371. https://doi.org/10.11591/ijece.v9i5.pp4364-4371

Alay, N. & Al-Baity, H. H. (2020). *Deep Learning Approach for Multimodal Biometric*. 1–17.

Ali, G., Dida, M.A., & Sam, A.E. (2020). Two-factor authentication scheme for mobile money: A review of threat models and countermeasures. *Future Internet*, 12(10), 1–27. https://doi.org/10.3390/fi12100160

Ali, G., Dida, M.A., Sam, A.E., Ademola, A., Somefun, T.E., Agbetuyi, A. F., Olufayo, A., Praseetha, V. M., Dattagupta, A., Suma, R., Vadivel, S., Study, A. I., Martin, T., Zhang, J., Nick, W., Sabol, C., Esterline, A., Lv, X., Ding, L., … Alam, D. (2018). Multi-Factor Authentication Fingerprinting Device Using Biometrics. *Algorithms*, *9*(1), 678–683. https://doi.org/10.1504/IJBM.2021.112214

Ayo, C.K., Mac-Eze, C.M., Adebiyi, A.A., Oni, A., Okesola, J.O., & Odun-Ayo, I. (2021). Developing a Multi-factor Authentication-based Cardless Electronic Payment System. *IOP Conference Series: Earth and Environmental Science*, *665*(1). https://doi.org/10.1088/1755-1315/665/1/012009

Baig, A. F., & Eskeland, S. (2021). Security, privacy, and usability in continuous authentication: A survey. *Sensors*, *21*(17), 1–26. https://doi.org/10.3390/s21175967

Kabir, M., Roy, S., Ahmed, M., & Alam, D. (2021). Smart Attendance and Leave Management System Using Fingerprint Recognition for Students and Employees in Academic Institute. *Global Journal of Computer Science and Technology*, 10(September), 268–276.

Lv, X., Ding, L., & Zhang, G. (2021). Research on fingerprint feature recognition of access control based on deep learning. *International Journal of Biometrics*, *13*(1), 80–95. https://doi.org/10.1504/IJBM.2021.112214

Praseetha, V.M., Dattagupta, A., Suma, R., & Vadivel, S. (2018). Novel Web Service Based Fingerprint Identification Using Steganography and Xml Mining. *IOP Conference Series: Materials Science and Engineering*, *396*(1), 0–11. https://doi.org/10.1088/1757-899X/396/1/012026

Rahman, S., Rahman, M., & Rahman, M. (2018). *Edelweiss Applied Science and Technology using Fingerprint Recognition*. *2*(1), 90–94.

Richardson, T., Shelton, J., Eady, Y., Kyei, K., & Esterline, A. (2022). WebID + biometrics with permuted disposable features. *Proceedings of the 2022 ACMSE Conference - ACMSE 2022: The Annual ACM Southeast Conference*, 99–105. https://doi.org/10.1145/3476883.3524050

Sujana, S., & Reddy, V. S. K. (2021). Comparison of levels and fusion approaches for multimodal biometrics. *Indonesian Journal of Electrical Engineering and Computer Science*, *23*(2). https://doi.org/10.11591/ijeecs.v23.i2.pp791-801

Toli, C. A., & Preneel, B. (2018). Privacy-preserving biometric authentication model for E-finance applications. *ICISSP 2018 - Proceedings of the 4th International Conference on Information Systems Security and Privacy*, *2018-Janua*(Icissp), 353–360. https://doi.org/10.5220/0006611303530360

Vibin Mammen, V., Thokaiandal, S., Sindhuja, C. S., Mekala, V., Manimegalai, M., & Prabhuram, N. (2020). A comprehensive study on academic and industry authentication and attendance systems. *International Journal of Scientific and Technology Research*, *9*(3), 5426–5432.

Yadav, B. P., Prasad, C. S. S., Padmaja, C., Korra, S. N., & Sudarshan, E. (2020). A Coherent and Privacy-Protecting Biometric Authentication Strategy in Cloud Computing. *IOP Conference Series: Materials Science and Engineering*, *981*(2). https://doi.org/10.1088/1757-899X/981/2/022043

Yang, W., Wang, S., Sahri, N.M., Karie, N.M., Ahmed, M., & Valli, C. (2021). Biometrics for internet-of-things security: A review. Sensors, 21(18). https://doi.org/10.3390/s21186163