islington college
(इस्लिङ्टन कलेज)

CC5052NI Risk, Crisis & Security Management

50% Individual Coursework

on

{The Future of Biometrics: Beyond Fingerprints and Facial Recognition}

Semester 3

2024-25 Autumn

Student Name: Evani Raut

London Met ID: 23047473

College ID: np01nt4a230151@islingtoncollege.edu.np

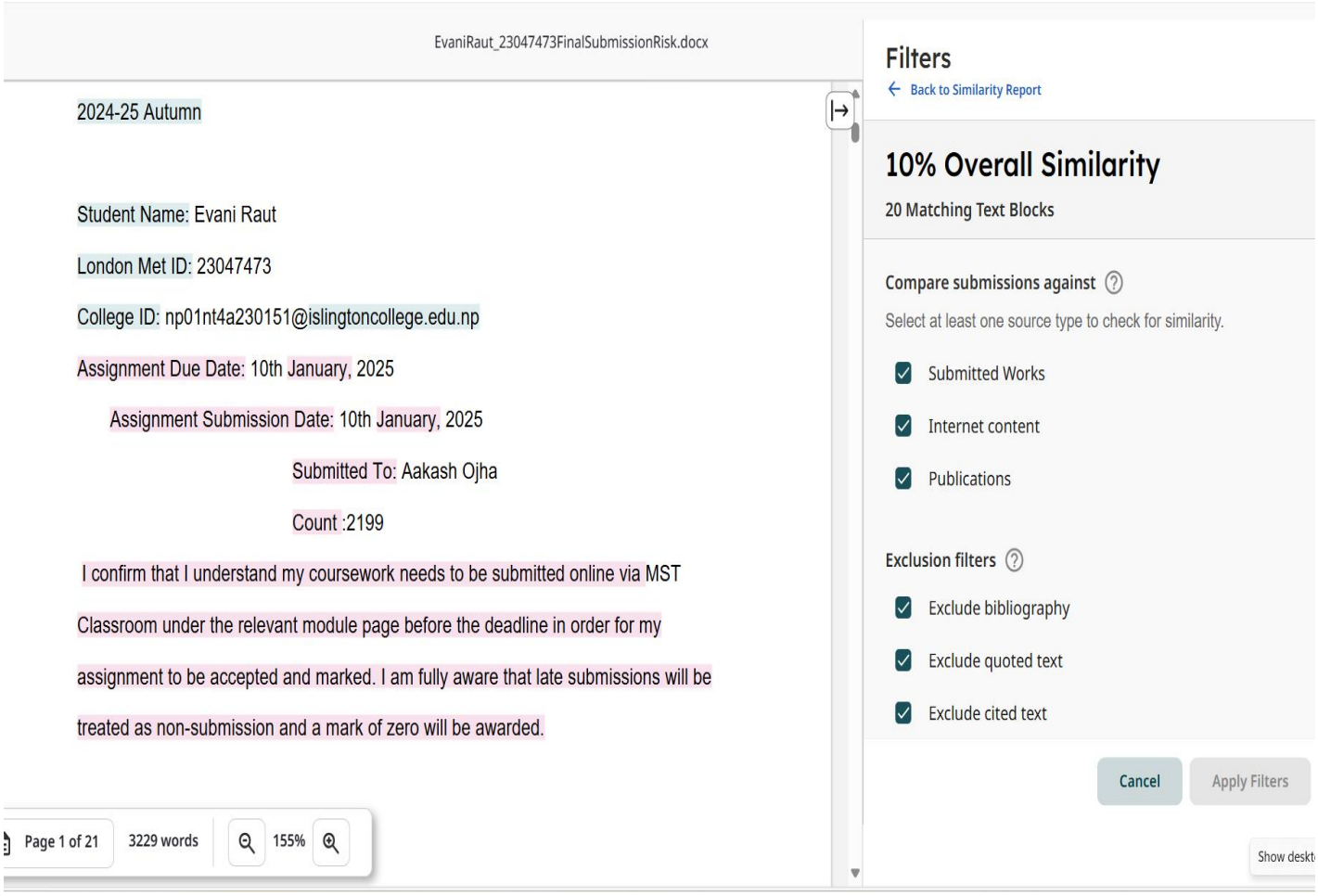
Assignment Due Date: 10th January, 2025

Assignment Submission Date: 10th January, 2025

Submitted To: Aakash Ojha

Count :2199

I confirm that I understand my coursework needs to be submitted online via MST Classroom under the relevant module page before the deadline in order for my assignment to be accepted and marked. I am fully aware that late submissions will be treated as non-submission and a mark of zero will be awarded.


EvaniRaut_23047473FinalSubmissionRisk.docx
2024-25 Autumn
Student Name: Evani Raut
London Met ID: 23047473
College ID: np01nt4a230151@islingtoncollege.edu.np
Assignment Due Date: 10th January, 2025
Assignment Submission Date: 10th January, 2025
Submitted To: Aakash Ojha
Count :2199
I confirm that I understand my coursework needs to be submitted online via MST Classroom under the relevant module page before the deadline in order for my assignment to be accepted and marked. I am fully aware that late submissions will be treated as non-submission and a mark of zero will be awarded.
Page 1 of 21
3229 words
155%
Filters
Back to Similarity Report
10% Overall Similarity
20 Matching Text Blocks
Compare submissions against
Select at least one source type to check for similarity.
Submitted Works
Internet content
Publications
Exclusion filters
Exclude bibliography
Exclude quoted text
Exclude cited text
Cancel
Apply Filters

Acknowledgment

I want to take a moment to sincerely thank everyone who supported me throughout the completion of this coursework, "The Future of Biometrics: Beyond Fingerprints and Facial Recognition."

First, I am deeply grateful to my subject teacher, Aakash Ojha, for his insightful guidance, feedback, and constant encouragement. His advice has been valuable in shaping the direction and quality of my coursework.

I am so thankful to Islington College and London Metropolitan University for providing access to the resources and a supportive learning environment that made this research possible.

A want to say a big thank you to my friends and my subject teacher for always being there for me and cheering me on during this journey. Their trust and encouragement gave me confidence to stay focused and overcome challenges along the way.

Lastly, I also want to acknowledge the incredible researchers and authors whose work I relied on for this coursework. Their insights and contributions to the field of biometrics have been an incredible source of knowledge and inspiration for my study.

Thank you all for being part of this journey with me. Your support has meant alot.

Abstract:

Biometric systems, like fingerprints and facial recognition, have become widely used in security and authentication processes as it allows quick and reliable identity verification with the help of fingerprints and facial recognition. As digital interactions grow, threats to identity security grow as well. Biometrics have become a great method of authentication due to their accuracy and convenience.

Yet, fingerprint and facial recognition technologies are facing limitations in terms of accuracy and susceptibility to spoofing. As cyberattacks and identity thefts become more complex, there is a growing need for biometric systems that offer more secure, reliable, and scalable solutions. increasing technologies like voice recognition and behavioral biometrics offer alternatives that can make security and user experience better. However, new and advanced technologies are being developed to make these systems more secure, accurate, and easier. This report explores the evolution of biometrics, focusing on newer methods like voice recognition, iris scanning, and behavior analysis. These technologies aim to improve how we verify identities, making systems more effective and user-friendly. At the same time, challenges such as privacy risks, ethical concerns, and technical limitations are becoming more important. This report examines these issues in detail, providing insights into how biometrics can adapt to the demands of the future.

Table of Contents

List of Figures

1. Introduction

1.1 Beyond Fingerprints and Facial Recognition

Figure 1:Beyond Fingerprints and Facial Recognition

Biometrics has the potential to transform the future how we secure and interact with technology, exploring possibilities beyond current methods. Future possibilities include:

1. Multimodal Biometric Systems: Combining biometric identifiers like fingerprints, facial recognition, and voice patterns boosts accuracy and security. Future systems may also integrate

physical and behavioral traits, using AI for real-time analysis to prevent spoofing (wikipedia, 2024).

2. Behavioral Biometrics: This approach analyzes behaviors like typing patterns, mouse movements, and browsing habits, enabling seamless, non-intrusive authentication. Real-time analysis could support always-active security, integrated with wearables and smart environments (Kelsey Kinzer, 2022).

3. Integration with Blockchain Technology: Blockchain-based biometric systems could create global, decentralized identity networks, allowing users to securely carry their identity across platforms and borders. This approach ensures safe storage and verification of biometric data, minimizing risks of identity theft and fraud (arxiv, 2023).

4. Advanced Liveness Detection: Next-gen liveness detection advances by using techniques like thermal imaging, micro-expression analysis, and neural activity monitoring to distinguish real biometric features from artificial replicas, such as masks or AI-generated deepfakes.

5. Privacy-Enhancing Innovations: Cancelable biometrics allow users to revoke and regenerate compromised templates. Future systems could use advanced cryptographic methods like homomorphic encryption to process biometric data securely without exposing personal information.

6. Biometric Applications in the Workplace: Biometric technology strengthens workplace security by enabling smarter access control for devices like PCs, USBs, and door locks. It adapts to employee behavior and integrates with IoT devices to automate access and personalize workflows. (Drew Robb, 2022).

7. Ethical and Legal Considerations: Global frameworks for biometric data protection could emerge, ensuring universal compliance and ethical use. AI-driven bias detection systems might also help address fairness concerns in biometric applications.

1.2 Limitations of Traditional Biometric Systems and Solution

Traditional biometric systems face significant challenges that limit their effectiveness in modern security. Privacy and security concerns are major issues, as biometric data is permanent and irreplaceable, making it a prime target for cybercriminals. These systems are also vulnerable to

spoofing and fraud, with high-quality replicas of fingerprints or facial images bypassing security measures. Environmental factors like poor lighting or angles can impact accuracy, while changes in appearance, such as aging, reduce reliability. Ethical and legal concerns that rise from the use of biometric data without consent, especially in cases like surveillance through facial recognition. Technological limitations, such as damaged fingerprints or altered appearances, further highlight the need for more secure and advanced alternatives. (Matt Burgess, 2024) (Omkar Hiremath, 2024)
.

My research into the future of biometrics focuses on overcoming the limitations of traditional systems by integrating advanced technologies to enhance accuracy, security, and privacy. Combining multiple identifiers like fingerprints, facial recognition, voice patterns, and behavioral traits like gait can create more robust systems that are harder to spoof. AI and machine learning will improve real-time analysis and adaptability, addressing challenges like environmental factors and changes in appearance. To protect privacy, I explore decentralized storage solutions that eliminate central databases, reducing the risk of breaches. Ethical concerns will be addressed through transparent systems requiring explicit consent and offering opt-out options, ensuring a fairer approach to biometric data usage.

1.3 Aim:
This research aims to explore the future potential of next-generation biometric technologies, addressing limitations in accuracy, security, and inclusivity while providing insights into their integration across various sectors.

1.4 Objectives:
1.To evaluate the strengths and weaknesses of existing biometric systems.
2. To examine the vulnerabilities of traditional biometric methods and propose solutions.
3.To explore the role of AI and machine learning in improving biometric system.
4.To investigate how advanced biometric technologies can be integrated into different sectors.
5.To give insight on real life case study.

2. Literature Review

2.1 Brief Overview of Biometrics

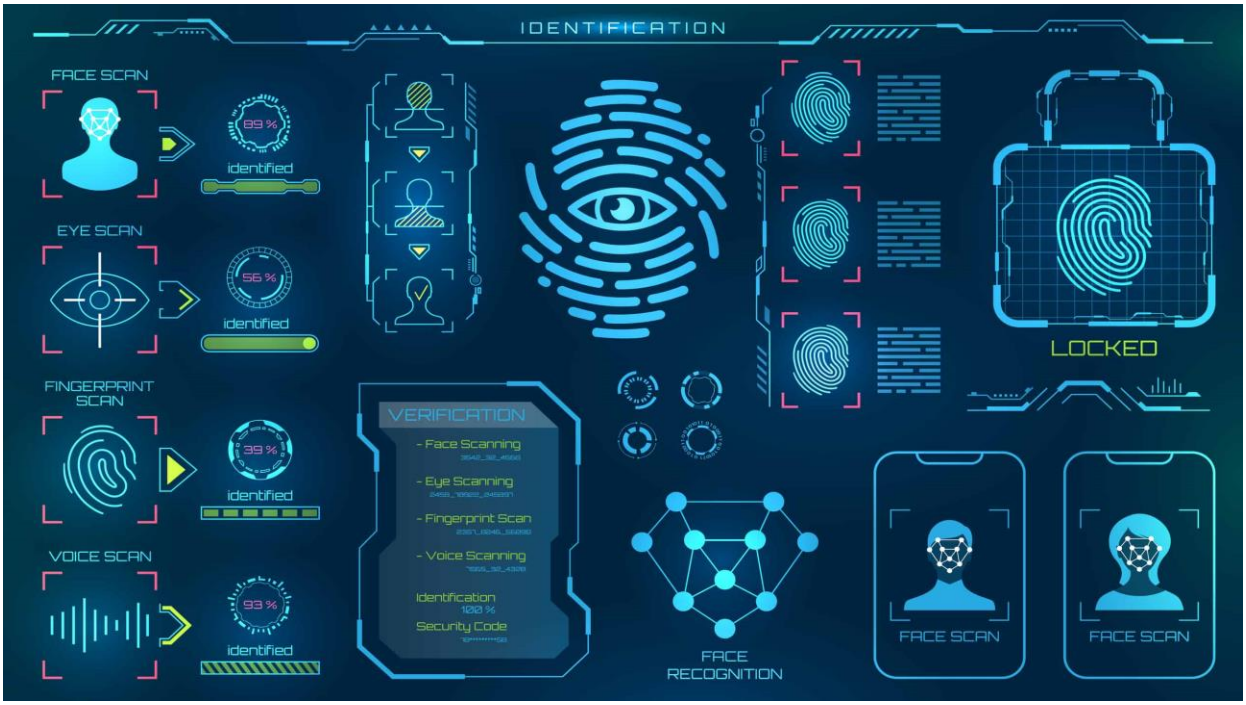


Figure 2:Biometrics

Biometrics measures and analyzes person's unique physiological and behavioral traits, like fingerprints, facial features, iris patterns, and typing or voice characteristics, for identity verification and security. Offering a more secure alternative to passwords, biometrics are widely used in government, healthcare, finance, and workplace security. However, challenges like privacy concerns, data security, and ethical issues remain. The future of biometrics promises greater integration with AI and blockchain, multimodal systems, wearable devices, and privacy-focused solutions for seamless and secure authentication (geeksforgeeks, 2024).

2.2 Biometrics Working Mechanism

It involves several key stages (Mara Calvello, 2019):

1. **Data Collection (Enrollment)**: During enrollment, the system collects data to create a mathematical reference template, protecting user privacy by not storing raw data.

2. **Feature Extraction**: The system extracts unique features from the biometric sample, such as facial landmarks in facial recognition or pitch and tone in voice recognition.

3. **Template Storage**: Extracted features are condensed into a biometric template stored in the database for future comparisons.

4. **Comparison (Verification or Identification)**: The system compares new samples with stored templates for:

Verification: Matching a specific individual.

Identification: Finding a match in a database.

5. **Decision and Access**: Access is granted if a match is found, otherwise denied. Accuracy is measured by minimizing false acceptance (FAR) and false rejection (FRR) rates.

2.3 Types/Components of Biometrics

1.Physiological Biometrics

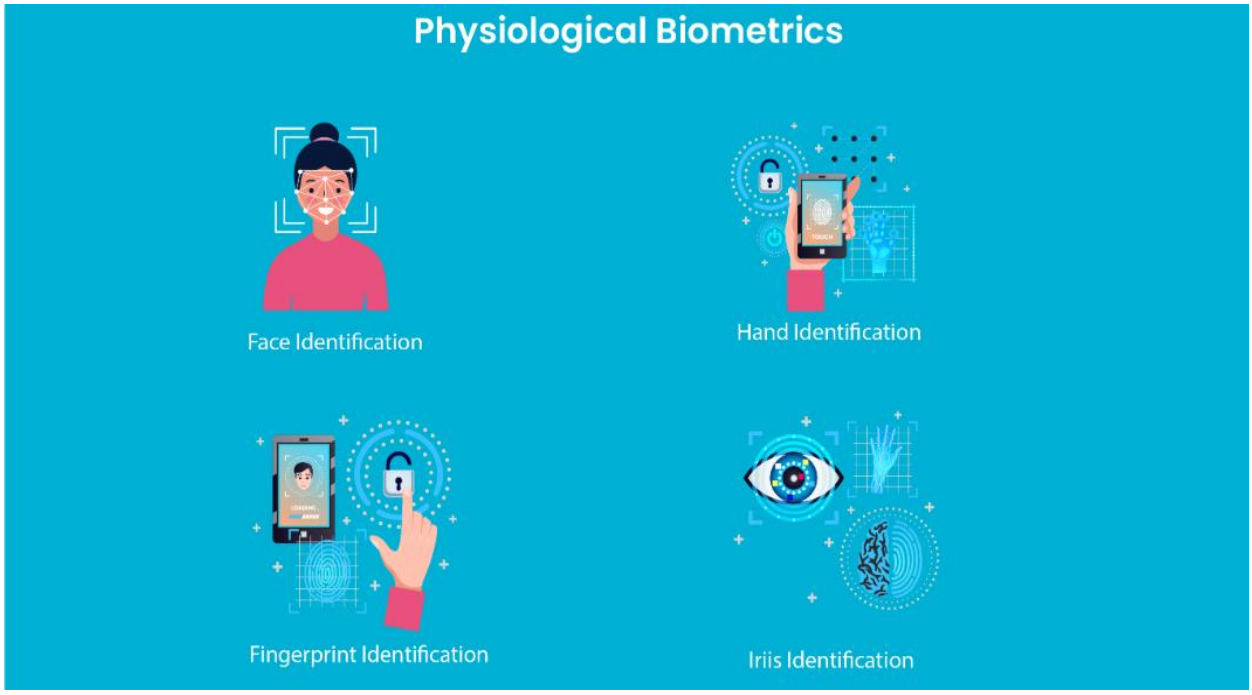


Figure 3:Physiological Biometrics

These biometrics focus on the physical attributes of an individual:

Fingerprint Recognition: Identifying individuals by analyzing the recognizable patterns of ridges and valleys on their fingertips.

Facial Recognition: Recognizing people by assessing the unique structure and features of their face.

Iris Recognition: Identifying individuals by analyzing the detailed patterns in the colored part of the eye.

Retina Scanning: Maps the unique pattern of blood vessels in the thin tissue at the back of the eye.

Hand Geometry: Analyzing the size and shape of a hand for identification purposes.

DNA Analysis: Identifying individuals based on their unique genetic code found in their cells.

Ear Shape Recognition: Recognizing individuals by the distinctive shape and features of their ears.

2.Behavioral Biometrics

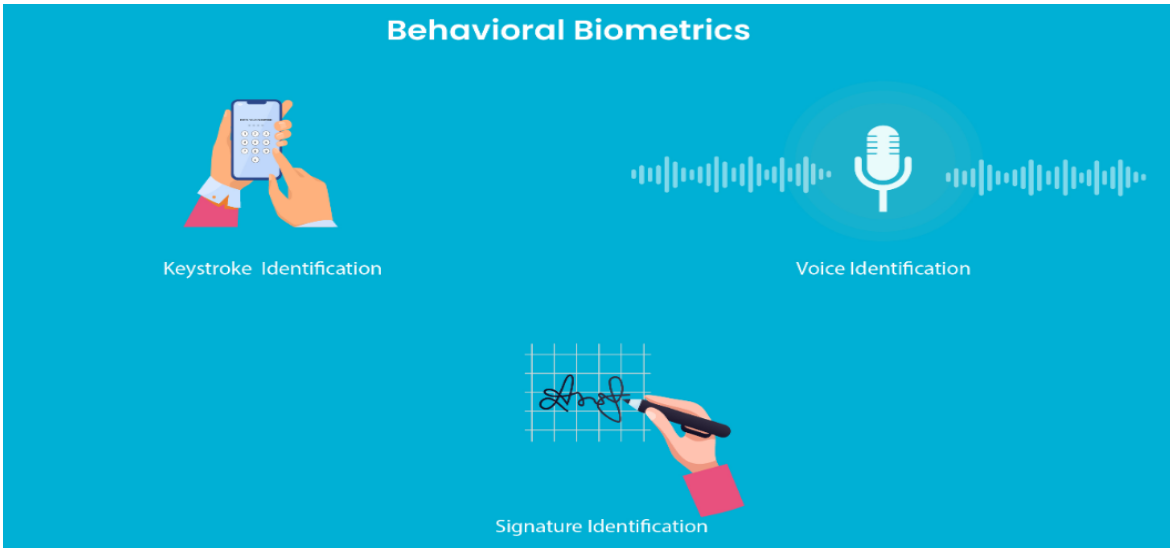


Figure 4:Behavioral Biometrics

These biometrics analyze patterns in human activity:

Signature Dynamics: Analyzing the way a person signs their name, including speed, pressure, and rhythm.

Keystroke Dynamics: Monitoring typing patterns, such as speed and rhythm.

Gait Analysis: Observing the unique way of person's walks.

Voice Recognition: Identifying the person based on vocal characteristics and speech patterns (recfaces, 2024).

2.4 Future of Biometrics

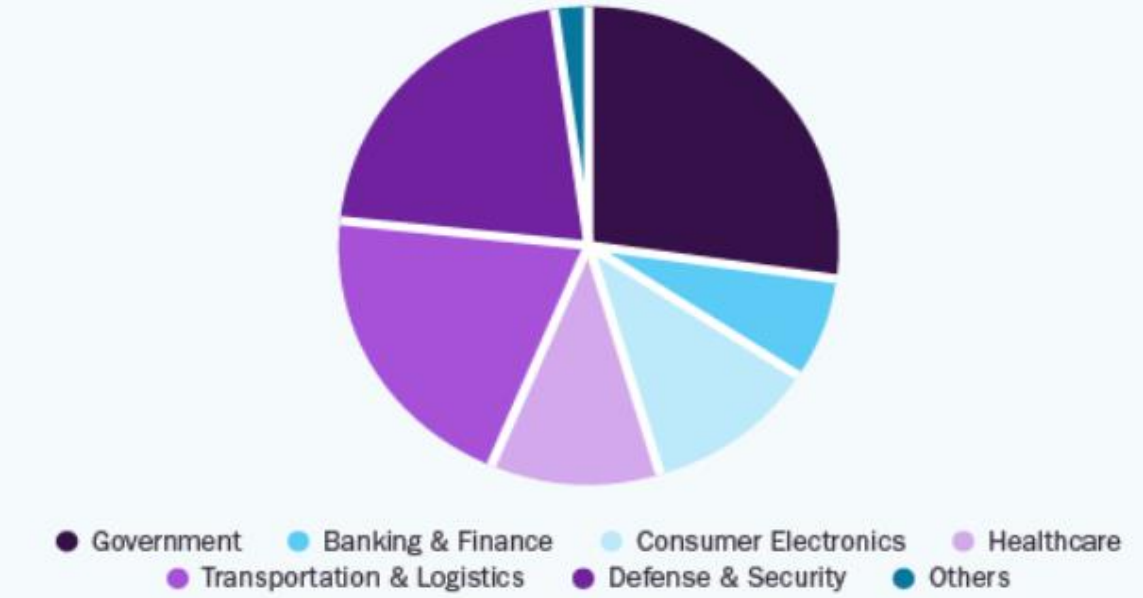


Figure 5:Future of Biometrics

The global biometrics market is expanding quickly, influenced by rising security needs, technological advancements, and widespread adoption across sectors. Worth roughly USD 45.1 billion in 2024, it is expected to grow at a CAGR of 14.4%, reaching USD 173.1 billion by 2033. (imarcgroup, 2024).

1.The future of biometrics in healthcare: It is set to grow with technologies like facial recognition, which enhances patient identity authentication, speeds up check-in processes, and

even aids in diagnostics by analyzing emotional responses. The healthcare biometrics market was priced at USD 9.45 billion in 2023 and is calculated to grow at a compound annual growth rate of 23.8% from 2024 to 2030 (grandviewresearch, 2024).

2.The future of biometrics in B**anking and Financial Services:** It is crucial in banking due to KYC and anti-money laundering regulations. They use facial recognition for identity verification, replacing card swipes at ATMs, and selfies for document verification, improving security and convenience. The biometrics market in the banking and financial services sector is predicted to reach USD 51.15 billion in 2024 and grow at a CAGR of 15.30% to reach USD 104.22 billion by 2029 (mordorintelligence, 2024).

3. The future of biometrics in Government and Border Control: The biometric market is projected to rise from USD 42.9 billion in 2022 to USD 82.9 billion by 2027, at a CAGR of 14.1%. Government agencies are increasingly deploying biometric solutions for identity verification in passports, national IDs, and border security, aiming to improve safety and streamline processes (marketsandmarkets, 2024).

4. The future of biometrics in Consumer Electronics: The global biometric technology market is expected to increase at a CAGR of 20.4% from 2023 to 2030, reaching USD 150.58 billion by 2030. This rise is driven by the integration of biometric features like fingerprint and facial recognition in smartphones and personal devices, offering enhanced security and user convenience (grandviewresearch, 2024).

5. The future of biometrics in Behavioral Biometrics: The behavioral biometrics market is projected to advance from USD 1.53 billion in 2023 to USD 13.00 billion by 2033, with a CAGR of 23.8% through 2033. This sector focuses on analyzing patterns in human activity, such as keystroke dynamics and mouse movements, to enhance security measures across various applications (futuremarketinsights, 2024).

6. The future of biometrics in Hospitality and Travel: The market for biometric digital identity in travel is expected to expand at a compound annual growth rate (CAGR) of 92%, generating over $72 billion globally by 2028 (indicio, 2024).

3. Methodology or Analysis

3.1 Case Study: The Biostar 2 Breach

Figure 6:The Biostar 2 Breach

The BioStar 2 data breach in August 2019 exposed over 27.8 million records, affecting around 1 million users globally. The 23GB database contained sensitive biometric data, usernames, and passwords, used by 5,700 companies. The breach created significant security risks and potential financial damages, including regulatory fines of up to €20 million under GDPR. Attackers exploited an exposed database with no firewall or proper security, where unencrypted biometric data was stored. Weak access controls and lack of monitoring allowed unauthorized access, enabling attackers to steal sensitive data without detection (Josh Taylor, 2019) (trendmicro, 2019).

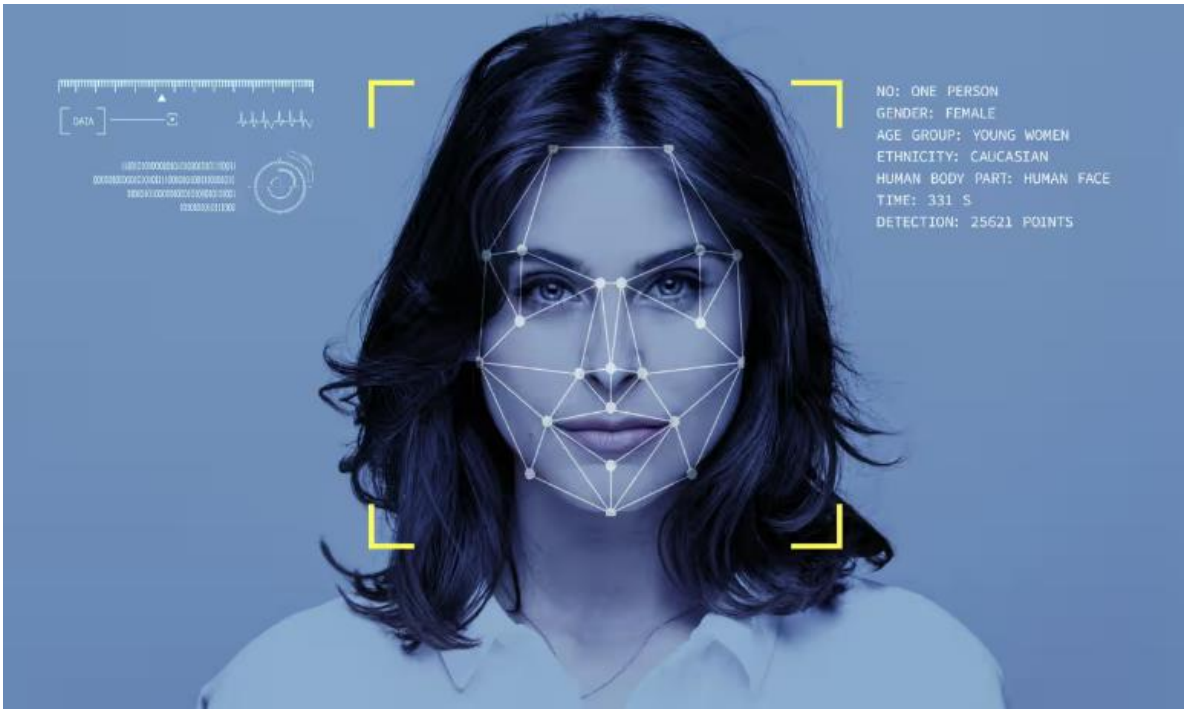


Figure 7:Causes of the Breach

3.2 Causes of the Breach

Unencrypted Biometric Data:

Biometric templates (fingerprints and facial recognition data) were stored in plaintext, making them vulnerable to theft and misuse. This is a fundamental failure in securing sensitive, immutable data.

Exposed Database:

The database containing biometric and personal information was left publicly accessible without adequate protection, such as a firewall or proper network security configurations.

Weak or Missing Authentication:

The system lacked robust access controls or multi-factor authentication (MFA), allowing unauthorized users to access the database.

Poor Data Isolation:

Biometric data was not stored in a secure, isolated environment, increasing the risk of exposure when the system was breached.

Inadequate Monitoring and Auditing:

There was no effective monitoring to detect unusual access or unauthorized activity, allowing the breach to occur and persist without immediate detection.

No Use of Secure Biometric Standards:

The system did not follow best practices for securing biometric data, such as hashing biometric templates with irreversible algorithms or using secure enclaves for storage (bbc, 2019).

3.3 Reflection/How Futuristic Biometrics system could have prevented this attack?

1. Decentralized Biometric Data Storage

Instead of storing biometric data centrally, a futuristic system could use decentralized storage, such as blockchain or edge computing, to store biometric templates securely on user devices. (e.g., an exposed database).

2. Biometric Data Encryption with Quantum-Safe Algorithms

Using quantum-safe encryption helps keep biometric data secure, even in the face of potential threats from future quantum computers. Advanced cryptographic methods, such as lattice-based encryption, can safeguard biometric templates from these emerging risks**.**

3. Template Protection with Cancelable Biometrics

Using cancelable biometrics, where biometric data is transformed into a revocable and non-invertible template, ensures that stolen templates cannot be used or reconstructed. New templates can be issued if compromised.

4. Federated Learning for Model Training

Biometric recognition systems could use federated learning, where models are trained locally on user devices and only anonymized updates are shared. This reduces the need to store raw biometric data centrally.

5. Homomorphic Encryption

Biometric systems could implement homomorphic encryption, which allows computations on encrypted data without decryption. This will ensure biometric data is never exposed during authentication or processing.

6. Advanced Behavioral Biometrics

Incorporating behavioral biometrics for example typing patterns, gait analysis alongside physical biometrics adds an extra layer of security. Behavioral data is dynamic and harder to replicate, making it less useful if stolen.

7. Secure Hardware Integration

Storing biometric data in secure hardware modules like Trusted Platform Modules or Secure Enclaves on devices ensures data remains isolated and tamper-proof.

8. Continuous Biometric Authentication

Future systems could employ continuous authentication that constantly verifies user identity based on multiple biometric signals, reducing the risk of misuse even if data is compromised.

9. Privacy-Preserving Biometrics with Differential Privacy

Embedding differential privacy in biometric systems ensures that individual data remains anonymous and secure, even when used for training or analysis.

10. AI-Powered Threat Detection

Advanced AI algorithms could monitor biometric systems for unusual activity, such as repeated failed attempts or unauthorized database access, enabling real-time breach prevention (jumpcloud, 2022) (hyperverge, 2024).

4. Conclusion:

Biometric technology is rapidly evolving, with the potential to transform identity security and our interaction with technology. While traditional systems like fingerprint and facial recognition have been groundbreaking, they face challenges such as spoofing, centralized data breaches, and privacy concerns. These limitations emphasize the need for more secure and adaptable solutions.

The future of biometrics lies in systems that combine multiple biometric traits, such as voice and behavior, enhanced by AI, decentralized data storage, and next-gen encryption. These advancements can address current vulnerabilities and protect user privacy. Lessons from breaches like BioStar 2 highlight the need for robust security measures, including decentralized storage and quantum-safe encryption. By adopting these innovations, biometrics can create systems that are secure, adaptive, and trustworthy, leading to a safer and more convenient future across various sectors.

Appendices

Breadth and Depth of Content Reviewed

Challenges in Traditional Systems

Research shows that significant limitations in traditional biometric systems, such as their susceptibility to spoofing and demographic biases. For instance, facial recognition systems have shown to be less accurate for individuals with darker skin tones, which reflects the systemic issues in algorithm design and training datasets. These challenges focuses on the need for more inclusive and reliable biometric technologies.

Innovations in Emerging Technologies

The development of advanced modalities, including multimodal systems that combine fingerprint, iris, and voice recognition, enhances both security and dependability. Behavioral biometrics, which analyze unique patterns such as typing speed or gait, are emerging as promising solutions for continuous and dynamic authentication. These technologies offer more robust, context-aware alternatives to traditional systems.

Ethics and Privacy

Ethical considerations around biometric data have become a major focus, with an emphasis on frameworks like the GDPR that govern data protection. New methods such as encrypted data storage and federated learning are being explored to ensure privacy while allowing biometrics to be used in secure, ethical ways. These solutions are critical in maintaining public trust and ensuring that biometric systems adhere to privacy standards.

Applications in Real-World Scenarios

Advanced biometrics are already being implemented in various sectors, including banking, healthcare, and IoT devices. In banking, biometric authentication enables secure, password-free transactions. In healthcare, biometrics ensure accurate patient identification, which enhances both security and efficiency. Additionally, in IoT environments, biometrics provide seamless authentication, improving user experience and safety. These diverse applications illustrate the versatility and scalability of biometric technologies across industries.

Bibliography

(2019, Aug 14). Retrieved from bbc: https://www.bbc.com/news/technology-49343774

(2019, Aug 15). Retrieved from trendmicro: https://www.trendmicro.com/vinfo/us/security/news/online-privacy/over-27-8m-records-exposed-in-biostar-2-data-breach?utm_source=chatgpt.com

(2022, April 13). Retrieved from jumpcloud: https://jumpcloud.com/blog/future-of-biometrics#:~:text=The%20Future%20of%20Biometrics%3A%20What%E2%80%99s%20Next%3F%201%20Responding,...%204%20Continuous%20Authentication%20and%20Zero%20Trust%20

(2023, Dec 1). Retrieved from arxiv: https://arxiv.org/abs/2302.10883?utm_source=chatgpt.com

(2024, Nov 5). Retrieved from wikipedia: https://en.wikipedia.org/wiki/Biometrics?utm_source=chatgpt.com

(2024, Mar 20). Retrieved from geeksforgeeks: https://www.geeksforgeeks.org/what-is-biometrics/

(2024, Jan 14). Retrieved from recfaces: https://recfaces.com/articles/types-of-biometrics

(2024, Dec 26). Retrieved from imarcgroup: https://www.imarcgroup.com/biometrics-market?utm_source=chatgpt.com

(2024, Dec 26). Retrieved from grandviewresearch: https://www.grandviewresearch.com/industry-analysis/biometrics-in-healthcare-market

(2024). Retrieved from mordorintelligence: https://www.mordorintelligence.com/industry-reports/biometrics-market?utm_source=chatgpt.com

(2024). Retrieved from marketsandmarkets: https://www.marketsandmarkets.com/Market-Reports/next-generation-biometric-technologies-market-697.html?utm_source=chatgpt.com

(2024). Retrieved from grandviewresearch: https://www.grandviewresearch.com/industry-analysis/biometrics-industry

(2024). Retrieved from futuremarketinsights: https://www.futuremarketinsights.com/reports/behavioral-biometrics-market?utm_source=chatgpt.com

(2024). Retrieved from indicio: https://indicio.tech/new-industry-report-highlights-indicios-masterful-innovation-in-biometric-digital-identity-for-travel-and-hospitality-sectors/?utm_source=chatgpt.com

(2024, Dec 27). Retrieved from hyperverge: https://hyperverge.co/blog/future-of-biometrics/

Drew Robb. (2022, Jan 22). Retrieved from shrm: https://www.shrm.org/topics-tools/news/technology/future-biometrics-workplace?utm_source=chatgpt.com

Josh Taylor. (2019, Aug 14). Retrieved from theguardian: https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms?utm_source=chatgpt.com

Kelsey Kinzer. (2022, April 13). Retrieved from jumpcloud: https://jumpcloud.com/blog/future-of-biometrics?utm_source=chatgpt.com

Mara Calvello. (2019, October 30). Retrieved from learn.g2: https://learn.g2.com/biometrics

Matt Burgess. (2024, May 23). Retrieved from wired: https://www.wired.com/story/police-face-recognition-biometrics-leak-india/?utm_source=chatgpt.com

Omkar Hiremath. (2024, Dec 26). Retrieved from softwaresecured: https://www.softwaresecured.com/post/risks-and-benefits-of-biometrics-in-security?utm_source=chatgpt.com