International Journal of Advance and Applied Research
www.ijaar.co.in
ISSN – 2347-7075 Impact Factor – 7.328
Peer Reviewed Bi-Monthly
Vol.10 No.4 March – April 2023

Enhancing the Security of E-Banking Systems Using Artificial Intelligence-Based Face Recognition, Voice Recognition, and Sign Recognition

Ast. Professor Sayema Shaikh[1], Mr. Rohit Naphade[2], Mr. Kunal Diwakar[3]
[1 2 3]Ashoka Centre of Business and Computer Studies Savitribai Phule University
***Corresponding Author* - Ast. Professor Sayema Shaikh**
Email- rohitnaphade026@gmail.com
DOI- 10.5281/zenodo.7791011

Abstract:
E-banking systems have become increasingly popular due to their convenience and accessibility, but they are also vulnerable to various security threats, such as identity theft and fraud. To enhance the security of e-banking systems, this research paper proposes an artificial intelligence-based approach that utilizes face recognition, voice recognition, and sign recognition. The proposed approach involves a multi-factor authentication process that requires users to provide their face, voice, and signature to access their e-banking account.

Keywords:
E-banking systems: This refers to the electronic banking systems that allow customers to access their banking services online through the internet.
Security: This refers to the measures taken to protect e-banking systems from unauthorized access and fraudulent activities.
Artificial intelligence: This refers to the use of machines and algorithms that mimic human intelligence to perform tasks such as pattern recognition, decision making, and natural language processing.
Face recognition: This refers to the use of artificial intelligence to identify and verify individuals by analyzing their facial features.
Voice recognition: This refers to the use of artificial intelligence to identify and verify individuals by analyzing their voice patterns.
Sign recognition: This refers to the use of artificial intelligence to identify and verify individuals by analyzing their handwritten signatures.

Introduction:

E-banking systems have become an integral part of modern banking and financial services, providing customers with convenient and accessible ways to manage their accounts, transfer funds, and conduct financial transactions. However, the widespread use of e-banking systems has also resulted in increased security risks, such as identity theft, fraud, and unauthorized access to user accounts. To address these security concerns, this research paper proposes an artificial intelligence-based approach that utilizes face recognition, voice recognition, and sign recognition for enhancing the security of e-banking systems. The proposed approach involves a multi-factor authentication process that requires users to provide their face, voice, and signature to access their e-banking account. The system then uses artificial intelligence algorithms to compare the provided information with the registered information to authenticate the user's identity. The face recognition component uses deep learning algorithms to extract facial features and match them with the registered facial features. The voice recognition component uses machine learning algorithms to analyze the user's voice and match it with the registered voice patterns. The sign recognition component uses computer vision algorithms to recognize the user's signature and match it with the registered signature. The use of artificial intelligence-based multi-factor authentication provides a robust and reliable security mechanism for e-banking systems. The proposed approach is expected to significantly reduce the risk of unauthorized access to e-banking accounts and prevent

identity theft and fraud. The next section of this research paper provides a detailed review of the literature on e-banking security and the use of artificial intelligence for enhancing the security of e-banking systems.

Objective:

The objective of using artificial intelligence-based face recognition, voice recognition, and sign recognition in e-banking systems is to enhance the security of these systems by providing reliable and accurate biometric authentication. This will make it more difficult for cybercriminals to gain unauthorized access to customer accounts, steal personal information, or conduct fraudulent activities. Additionally, the use of these technologies can improve the overall user experience for customers by providing a more convenient and efficient authentication process. Overall, the goal is to create a secure and trusted environment for customers to conduct their banking transactions online.

Research Methodology:

As this is a theoretical paper on the use of artificial intelligence-based face recognition, voice recognition, and sign recognition in enhancing the security of e-banking systems, the research methodology used is primarily a literature review. The review involved searching for relevant articles, journals, and conference proceedings related to the topic from various online databases, such as IEEE Xplore, ACM Digital Library, and Google Scholar. The search keywords used included "e-banking security," "biometric authentication," "face recognition," "voice recognition," "sign recognition," and "artificial intelligence. "The articles selected for the review were primarily based on their relevance to the topic and their quality as assessed by the authors. The articles were then analyzed to identify key findings, benefits, limitations, and challenges associated with the use of artificial intelligence-based face recognition, voice recognition, and sign recognition in enhancing the security of e-banking systems.

Literature Review:

E-banking systems have become increasingly popular due to their convenience and accessibility. However, this has also led to an increase in cyber-attacks and threats to customer privacy and security. To address these challenges, artificial intelligence-based technologies such as face recognition, voice recognition, and sign recognition are being used to enhance the security of e-banking systems.

Case study use cases:

Here are some potential use cases for enhancing the security of e-banking systems using artificial intelligence-based face recognition, voice recognition, and sign recognition:

- **Face recognition for login authentication**: E-banking systems can use artificial intelligence-based face recognition to authenticate customers during the login process. This would prevent unauthorized access to customer accounts, as it would require the customer's face to be recognized before granting access to their account. It uses computer algorithms to identify and verify the identity of the user by analyzing their facial features. Artificial intelligence-based face recognition systems are more accurate and reliable than traditional face recognition techniques. These systems use deep learning algorithms to extract facial features, which can detect and recognize even minor changes in the user's face, making them more secure.
- **Voice recognition for account verification**: E-banking systems can use artificial intelligence-based voice recognition to verify customers during transactions. It analyzes the user's voice to identify and verify their identity. The user's voice is analyzed based on factors such as tone, pitch, and cadence. Artificial intelligence-based voice recognition systems use machine learning algorithms to learn and recognize the user's voice patterns, making them more secure than traditional voice recognition techniques. For example, if a customer wants to transfer a large sum of money, the system can ask the customer to speak a passphrase to verify their identity before completing the transaction.
- **Sign recognition for document verification**: E-banking systems can use artificial intelligence-based sign recognition to verify documents such as loan applications or account opening forms. The system can compare the signature on the document with the customer's known signature on file to ensure that the document is genuine. It analyzes the user's signature to identify and verify their identity. The user's

signature is analyzed based on factors such as pressure, speed, and stroke patterns. Artificial intelligence-based sign recognition systems use machine learning algorithms to learn and recognize the user's signature patterns, making them more secure than traditional sign recognition techniques.

- Let's consider a scenario where a customer wants to perform a transaction through an e-banking system. The customer logs in to their account and selects the transaction they want to perform. The system prompts the user to provide their biometric information for authentication. The user can choose to provide their facial, voice, or signature information for authentication. If the user chooses facial recognition, the system uses its artificial intelligence-based face recognition algorithm to analyze the user's facial features and authenticate their identity. The system compares the facial features with the ones stored in the database during the enrollment process. If the facial features match, the system grants access to the user to perform the transaction. If the facial features do not match, the system denies access to the user. If the user chooses voice recognition, the system uses its artificial intelligence-based voice recognition algorithm to analyze the user's voice patterns and authenticate their identity. The system compares the voice patterns with the ones stored in the database during the enrollment process. If the voice patterns match, the system grants access to the user to perform the transaction. If the voice patterns do not match, the system denies access to the user. If the user chooses sign recognition, the system uses its artificial intelligence-based sign recognition algorithm to analyze the user's signature patterns and authenticate their identity. The system compares the signature patterns with the ones stored in the database during the enrollment process. If the signature patterns match, the system grants access to the user to perform the transaction. If the signature patterns do not match, the system denies access to the user.

Conclusion:

In conclusion, the use of artificial intelligence-based face recognition, voice recognition, and sign recognition has the potential to significantly enhance the security of e-banking systems. By combining these technologies with other security measures such as encryption and multi-factor authentication, e-banking systems can create a highly secure environment for customers to conduct their banking transactions online. The use of these technologies also provides a more convenient and efficient user experience by eliminating the need for customers to remember multiple passwords or security questions. As the use of e-banking systems continues to grow, it is essential for banks and financial institutions to adopt these technologies to stay ahead of the evolving threats posed by cybercriminals.

References:

- https://ijarcce.com/wp-content/uploads/2022/05/IJARCCE.2022.114161.pdf
- Face and Speech Recognition Based Smart Home | IEEE Conference Publication | IEEE Xplore