**Table of Contents**

1. Weaknesses in Unimodal Authentication Systems
   1. Thirteen (13) + solid points with justification for Uni modal weaknesses
2. Why Continuous authentication is necessary
   1. Enhanced security of CA mentioned in papers.
   2. Vulnerabilities in Traditional
   3. Six (6) solid points for CA strengths
3. Unimodal Vs Multimodal
   1. Four (4) points where Multimodal is better than Unimodal
   2. Existing work proves that Multimodal is outperforming Unimodal
   3. Four (4) Challenges and considerations in a multimodal system
4. Eyeblink pattern Justification for continuous authentication
   1. Advantages of eyeblink pattern – (7 points)
   2. Justification of eyeblink over other ocular traits (3 other traits)
   3. Eyeblink is a better option (4 common points)
   4. Eyeblink pattern vs other biometric traits (Physiological vs Behavioural & Complementary to Keystroke)
5. Keystroke Dynamics Justification for continuous authentication
   1. Benefits of Keystroke dynamics (9 points)
   2. How Keystroke Dynamics Complements Eye-Blink Patterns (5 points)
   3. Specific complementary aspects with eyeblink (3 points)
6. Eyeblink / Ocular authentication Architecture.
7. Keystroke dynamics authentication Architecture.

**01. Weaknesses in Unimodal Authentication Systems**

* Unimodal biometric systems, which rely on a single biometric trait for authentication, have several weaknesses, whether used in continuous or static authentication (Oloyede and Hancke, 2016)
  + “UNIMODAL BIOMETRIC SYSTEM A unimodal (or single) biometric system is a system that uses a single biometric trait [143], [144], or one source of information for verification or identification [145]. Unimodal systems have said to have improved steadily in accuracy and reliability; however, they often suffer from problems in the enrolment process because of non-universal biometric traits, spoofing and lack of accuracy due to noisy data as stated earlier. Furthermore, unimodal biometric systems achieve less desired performances in real world applications. Hence, a method to solve these issues is making use of a multimodal biometric authentication system [146]. The problems associated with unimodal biometric systems are discussed further.”
  + “The former (Unimodal) have several deficiencies that reduce the accuracy of the system, such as noisy data, inter-class similarity, intra-class variation, spoofing, and non-universality. However, multimodal biometric sensing and processing systems, which make use of the detection and processing of two or more behavioural or physiological traits, have proved to improve the success rate of identification and verification significantly"
    - **Noisy data**: Unimodal systems are susceptible to inaccuracies due to noisy data
    - **Poor recognition performance**: These systems can suffer from poor recognition performance
    - **Less accurate results**: Authentication results from unimodal systems are often less accurate
    - **Spoofing attacks**: Unimodal systems are vulnerable to spoofing attacks where an imposter can mimic an individual's biometric trait  
      *“LACK OF INDIVIDUALITY, SUSCEPTIBILITY TO CIRCUMVENTION”*
    - A single biometric factor can be a single point of failure (Ryu *et al.*, 2021)  
      *“ However, a unimodal system faces challenges such as noisy data, poor recognition performance, less accurate results, and spoofing attacks, as the authentication metric itself can be a single point of failure”*
    - **Lack of universality**: Not all individuals possess the biometric trait required by a specific unimodal system, leading to enrolment issues
    - **Inter-class similarity**: Traits used in unimodal systems can be similar among different individuals, such as in the case of identical twins, resulting in an increased false match rate
    - **Intra-class variation**: A user's own biometric data can change over time due to various factors, which can impact accuracy
    - **Circumvention**: It is possible to impersonate an individual's trait through spoofed traits, such as using a fake fingerprint
    - **Lower accuracy**: In general, unimodal systems have lower accuracy than multimodal systems (Baig and Eskeland, 2021)  
      “*Security concerns”*
    - **Single point of failure**: Because they rely on a single biometric trait, unimodal systems are vulnerable if that single point of data is compromised
    - **Limited resources**: Unimodal systems may have limited resources for uniquely identifying a person   
      “*Using a single biometric factor potentially lowers the authentication system’s accuracy rate due to poor data quality, the overlap between identities and limited resources to uniquely identify a person*” (Ryu *et al.*, 2021)
    - **Not suitable for all situations:** A unimodal system may not be suitable for all user situations (Baig and Eskeland, 2021)   
      *“Modality-Specific Issues. Regarding Research Question 4, this section discusses the limitations of each modality in different scenarios. In real-life scenarios, the employed authentication modality needs to be determined by the user situation, i.e., what the user is doing (or not doing) at the moment. To the best of our knowledge, none of the single approaches could be suitable for all user situations.”*For example, keystroke dynamics will not work if the user is not typing.(Baig, Eskeland and Yang, 2023)  
      *“Choosing a proper modality for continuous authentication is very crucial. Even using a single behavioural biometric modality faces certain limitations, for instance, utilizing only keystroke dynamics does not work when the user does not type. Such limitations can be overcome by combining different modalities of behavioural biometrics (for example, keystroke dynamics in combination with swipe-gestures, gait dynamics, GPS data, etc.); this term is referred to as multimodal authentication. In case, if an imposter gets access to a device, he has to use it by performing some actions; either he types, monitors screen by performing scrolling with mouse, or performs swipe gestures on the touch screen, etc. Such actions are utilized for continuous authentication and the imposter is detected.”*
    - **Modality-specific issues:** Each modality has specific issues, such as the need for user action with fingerprint recognition (Baig and Eskeland, 2021)  
      “Similarly, the voice recognition authentication mode does not fit well with the concept of continuous authentication, as this consequently does not work with quiet users but, in contrast, requires continuous speaking, which is not practical. Moreover, face and iris recognition modes could be utilized for continuous authentication, assuming that the user is holding the device in front of their face. ~~Nevertheless, continuous monitoring with a camera could also affect user acceptance~~.” – Could be inappropriate.
    - **Physiological biometrics** such as fingerprint, face and iris recognition are static and can be reproduced by an adversary (Baig and Eskeland, 2021)
    - **Physiological biometrics** require segmentation and preprocessing of data which can be computationally expensive and complex(Baig and Eskeland, 2021)
    - **Behavioural biometrics** may be susceptible to mimicry and generative adversarial attacks (Baig and Eskeland, 2021)  
      “**Attacks on Different Modes of Continuous Authentication**Behavioural biometric-based approaches also face distinct security vulnerabilities. Touch dynamics cannot withstand adversarial generative attacks; these attacks manipulate training models to produce erroneous outcomes, keystroke dynamics cannot resist mimicry attacks, designed imitation attacks on a gait-based authentication system by imitating user gait patterns by using a digital treadmill., presentation attacks in experiments that if an attacker captures a short template of ECG data by any means (malicious insider), these template data can be used to map attacker ECG data into the victim’s ECG data. They collected ECG templates of 52 users from Physikalisch-Technische Bundesanstalt (PTB) database for experiments. Their attacks achieved average success rates of 90% to 96%.”
    - **Context-aware modes** like location data can reveal personal information  
      “The potential problem with the modalities of continuous authentication is that they utilize user personal data. Adding more modalities may strengthen more security but also become more privacy invasive. These modalities dis-close the data about daily life activities, physical and logical locations, other personal and demographic information”
  + These limitations highlight the need for more robust authentication methods, such as multimodal biometric systems which combine multiple biometric traits (Ryu *et al.*, 2021), (Oloyede and Hancke, 2016).

**02. Why continuous authentication is necessary**

* Continuous authentication is necessary to **enhance security** and mitigate the limitations of traditional, static authentication methods   
  (Bansal and Ouda, 2024)  
  *“Furthermore, traditional authentication methods such as knowledge-based authentication (KBA) or two-factor authentication (2FA) have been proven to be ineffective against social engineering attacks, where attackers manipulate users into revealing sensitive information [5]. This emphasizes the need for a more advanced and secure authentication system that can resist such attacks. To mitigate these risks, it is crucial for businesses to have a system that is reliable and trusted for identifying and authenticating users, to protect sensitive assets and financial data. To further strengthen security, it is important for the system to continuously authenticate users in addition to static authentication methods ”*(Ryu *et al.*, 2021) *“Existing user authentication schemes suffer from challenges in detecting impersonation attacks which leave systems vulnerable and susceptible to misuse. A range of research proposals have suggested continuous multimodal biometric authentication (CMBA) systems as a reliable solution”****“The majority of the studies in the literature reviewed apply supervised learning approaches as a classification technique, and score level fusion is predominantly used as a fusion model.”***(Abuhamad *et al.*, 2021)  
  *“Continuous authentication is a user authentication mechanism coined to enhance the security and privacy of the personal information stored in the smartphone. In contrast to entry-point authentication, continuous authentication extends the authentication process throughout the active session or till locks the smartphone’s touch-screen. Therefore, this survey believes that continuous authentication is an additional choice to improve the security and privacy of the confidential information stored in the smartphone.”*

(Adegbenle *et al.*, 2024)

“The current state of traditional authentication methods has made it difficult to ward off the increasing sophistication

of cyber-attacks on mobile apps [1]. Aside, from the challenges of preventing online identity theft, cyber fraud,

malicious attacks, and phishing in Short Message Service (SMS), and man-in-the-middle attacks, traditional

authentication systems are now groping with sterner social engineering attacks”  
  
**Traditional methods**, such as passwords or one-time biometric checks, only verify a user's identity at the beginning of a session, leaving systems vulnerable to **security breaches**  
(Rayani and Changder, 2023)  
*“to conquer existing issues with entry-point authentication, the smartphone user must authenticate implicitly without their consent.   
Continuous authentication is also known as the “implicit, transparent, or progressive authentication” mechanism of the smartphone. Continuous authentication is a user authentication mechanism coined to enhance the security and privacy of the personal information stored in the smartphone. In contrast to entry-point authentication, continuous authentication extends the authentication process throughout the active session or till locks the smartphone’s touch-screen. Therefore, this survey believes that continuous authentication is an additional choice to improve the security and privacy of the confidential information stored in the smartphone.”*  
(Bansal and Ouda, 2024)  
“traditional methods of security are becoming increasingly inadequate. With the rise of sophisticated cyberattacks, it has become easier for hackers to gain access to systems and steal user identities. Even if an organization has a strong security system in place, employees may still inadvertently compromise security by sharing passwords or digital keys. As a result, businesses are facing significant losses due to weakened security systems that rely solely on static authentication methods. Research studies have shown that relying solely on static authentication methods, such as usernames and passwords, is no longer enough in preventing cyberattacks. In fact, according to the Verizon 2021 Data Breach Investigations Report, stolen credentials were the most common initial access vector in data breaches. This highlights the need for a more reliable and secure authentication system”

**Continuous authentication addresses these vulnerabilities** by constantly verifying the user's identity throughout their interaction with a system

• **Vulnerabilities of Traditional Authentication**

Traditional methods, like passwords or one-time biometric scans (such as fingerprint or facial recognition), authenticate users only at the start of a session

(Baig, Eskeland and Yang, 2023), (Adegbenle *et al.*, 2024), (Fereidooni *et al.*, 2023), (Bansal and Ouda, 2024), (Rayani and Changder, 2023)

After the initial login, the system doesn't re-verify the user's identity, leaving it vulnerable to security breaches if a device is left unattended or if an account is compromised (Baig, Eskeland and Yang, 2023), (Baig and Eskeland, 2021), (Rayani and Changder, 2023)

As a result, malicious actors may gain unauthorized access to sensitive information

(Baig, Eskeland and Yang, 2023), (Bansal and Ouda, 2024)

Stolen credentials are a common way for hackers to gain initial access to a system

(Bansal and Ouda, 2024)

• **Mitigation of Security Risks**

Continuous authentication addresses these vulnerabilities by constantly verifying a user's identity throughout a session (Baig and Eskeland, 2021), (Adegbenle *et al.*, 2024), (Bansal and Ouda, 2024), (Rayani and Changder, 2023)

It does so by analysing a user’s behaviour, such as keystroke dynamics or motion (Baig and Eskeland, 2021)patterns, in real time (Adegbenle *et al.*, 2024), (Bansal and Ouda, 2024), (Rayani and Changder, 2023)

This method of authentication is designed to be passive, operating in the background without requiring explicit user action or attention (Baig and Eskeland, 2021), (Stragapede *et al.*, 2022), (Abuhamad *et al.*, 2021)

This makes it less intrusive than traditional authentication methods (Yang *et al.*, 2019)

also makes it harder for malicious actors to capture and duplicate a user's patterns

(Adegbenle et al., 2024)

• **Protection Against Sophisticated Attacks:**Traditional authentication methods are vulnerable to sophisticated cyberattacks (Adegbenle *et al.*, 2024), (Fereidooni *et al.*, 2023), (Bansal and Ouda, 2024)

Continuous authentication provides an additional layer of security to prevent cyberattacks by monitoring user behaviour and identifying anomalies. This approach enhances security by continuously monitoring user behaviour and ensuring that the same person is accessing the system throughout the session

(Bansal and Ouda, 2024)

**• Usability and User Experience**

Unlike traditional authentication that requires explicit user interaction, continuous authentication is designed to be seamless and transparent (Baig and Eskeland, 2021), (Stragapede et al., 2022), (Abuhamad et al., 2021)

By running in the background and verifying a user's identity implicitly, it minimizes disruptions and enhances the overall user experience (Yang et al., 2019)

**• Real-time Monitoring**

Continuous authentication calculates the probability that the current user is the same one who initially logged in. This is done by analyzing user behaviour in real time without the need for external devices (Bansal and Ouda, 2024)

This constant monitoring enhances security by detecting imposters and unauthorized access attempts as they occur, not just at the beginning of a session

(Lu *et al.*, 2020),(Baig and Eskeland, 2021)

• **Adaptability and Flexibility**

Continuous authentication systems can adapt to a user’s behaviour over time, enhancing their accuracy and reliability. The system can adjust to changes in a user's typing, touch, or motion patterns (Bansal and Ouda, 2024)

• **Application Across Devices**

Continuous authentication can be applied to various devices such as smartphones, tablets, laptops, and wearable technologies (Saied *et al.*, 2020), (Stragapede et al., 2022), (Abuhamad et al., 2021)

It can be used to protect sensitive information on mobile platforms, in healthcare settings, and in financial institutions (Saied et al., 2020), (Stragapede et al., 2022), (Bansal and Ouda, 2024)

**CONCLUSION**  
In conclusion, continuous authentication is essential for improving security and user experience by providing constant and passive user verification, which traditional authentication methods cannot achieve. It is a critical component of modern security systems to protect against the ever-evolving landscape of cyber threats (Adegbenle et al., 2024), (Bansal and Ouda, 2024)

(Gorur, 2023) (Piugie *et al.*, 2022) (Baig*et al.*, 2023) (Hu *et al.*, 2020) (Oloyede and Hancke, 2016)

**03. Unimodal Vs. Multimodal**

Multiple sources emphasize the benefits of multimodal biometric systems over unimodal systems in terms of accuracy, robustness, and reliability (Ryu et al., 2021), (Stragapede et al., 2022), (Abuhamad et al., 2021), (Oloyede and Hancke, 2016)

1. **Increased Accuracy**Multimodal systems, which combine two or more biometric traits, generally achieve higher accuracy than unimodal systems (Ryu et al., 2021), (Abuhamad et al., 2021), (Oloyede and Hancke, 2016)  
     
   For example, one study found that combining voice and gait biometrics decreased error rates from 2.82%-43.09% and 13.7%-17.2% for individual voice and gait recognition to 1.97%-11.8% for the multimodal system. Similarly, a multimodal system combining face and voice biometrics decreased error rates from 4.29% for face and 34.72% for voice to 2.14%. Another study noted a decrease in error rates from 3.38%-29.87% to 0.56% when combining voice, face, and signature modalities (Abuhamad et al., 2021).
2. **Enhanced Robustness**Multimodal systems are more robust against noisy data and spoofing attacks (Ryu et al., 2021), (Abuhamad et al., 2021), (Oloyede and Hancke, 2016)  
     
   Unimodal systems can be easily compromised by spoofing a single biometric trait, whereas a multimodal system that uses multiple traits is more difficult to deceive (Oloyede and Hancke, 2016)  
     
   For example, a system using both face and voice features is harder to spoof than one relying on face or voice alone. Additionally, if one biometric modality is compromised, additional modalities can increase authentication confidence (Ryu et al., 2021)
3. **Improved Reliability**By using multiple sources of biometric information, multimodal systems are less sensitive to environmental factors and variations in data (Ryu et al., 2021), (Oloyede and Hancke, 2016)  
     
   For example, if a fingerprint scan is affected by a worn fingerprint, other modalities like voice or face can still authenticate the user. Multimodal systems also reduce the failure to enrol rate, as they do not rely on a single biometric identifier (Oloyede and Hancke, 2016)
4. **Performance Comparisons**Several studies directly compare the performance of unimodal and multimodal systems. For example, one study found that a fusion of mouse and gaze biometrics resulted in better accuracy and lower error rates than either modality alone (Kasprowski and Harezlak, 2018)  
     
   Another study showed that while keystroke biometric models were successful with a mean true positive proportion of 0.9381, eye-tracking biometric models had a lower rate of 0.6583, while a combination model achieved a rate of 0.7099 (Silver and Biggs, 2006) – Could be inappropriate for justifying multimodal.  
     
   A study on mobile authentication found that individual modalities such as keystroke (12.19% EER) and magnetometer (14.98% EER) had higher error rates compared to their fusion, which achieved EER values below 10.00%, and with weighted coefficients, less than 4% (Stragapede et al., 2022)

**Specific Examples of Multimodal Systems Outperforming Unimodal Systems**

**• Eye and Mouse Movements** A system fusing eye and mouse movement data outperformed systems based on each modality individually, showing that the combination of the two modalities may lead to better results (Kasprowski and Harezlak, 2018)

• **Touchscreen and Background Sensors** Combining touchscreen data with background sensor data (such as accelerometer, gyroscope, and magnetometer) in mobile devices resulted in significantly enhanced discriminative ability, with EER values typically ranging from 4% to 9% within short interaction times. The magnetometer sensor was noted as being the best performing background sensor modality (Stragapede et al., 2022)

**• Keystroke Dynamics and Other Modalities**Combining keystroke dynamics with other modalities such as touchscreen data and background sensors improves overall system accuracy and robustness. (Abuhamad et al., 2021)

**Challenges and Considerations**

**Fusion Techniques -**  Choose a method and find justifications from the same papers.

The effectiveness of multimodal systems depends on the fusion techniques used. **Score level fusion**, where scores from different modalities are combined, is a common approach (Ryu et al., 2021), (Stragapede et al., 2022)

but other methods such as **feature level** fusion and **decision level** fusion exists (Ryu et al., 2021) (Stragapede et al., 2022) (Abuhamad et al., 2021) (Rayani and Changder, 2023) (Kasprowski and Harezlak, 2018)

The choice of fusion method can affect the system's performance (Ryu et al., 2021)

**Biometric Trait Selection**

There is no clear, proven process for choosing which biometric traits are best for a multimodal system, and further research is needed to explore the optimal combinations of different types of biometric traits (Ryu et al., 2021) (Abuhamad et al., 2021) (Oloyede and Hancke, 2016)

**Computational Complexity**

Multimodal systems may be more complex to implement and computationally intensive than unimodal systems, although they offer superior security and accuracy (Oloyede and Hancke, 2016)   
  
There is no clear guidance on the optimal number of modalities for use in a system, but adding more than three modalities might be useful (Ryu et al., 2021) - Could be inappropriate

**Standardization and Evaluation**

Lack of standardization in performance metrics and experimental setup makes comparisons across different studies challenging (Ryu et al., 2021) (Rayani and Changder, 2023) (Baig and Eskeland, 2021)   
  
Further, the performance can be affected by factors such as the type of device, the environment, and how the data are collected (Ryu et al., 2021) (Rayani and Changder, 2023) (Abuhamad et al., 2021) (Baig and Eskeland, 2021)

**CONCLUSION**in conclusion, the evidence from multiple sources strongly suggests that multimodal biometric systems offer significant advantages over unimodal systems, particularly in terms of accuracy, robustness, and reliability. The fusion of multiple modalities provides a more secure and dependable method for user authentication, addressing many of the shortcomings of traditional single-factor methods (Ryu et al., 2021) (Stragapede et al., 2022) (Abuhamad et al., 2021) (Oloyede and Hancke, 2016)

**04. Eyeblink pattern Justification for continuous authentication**

Several sources discuss the advantages of using eye-blink patterns for biometric authentication, sometimes in comparison to other ocular traits and other biometric modalities. Here's a breakdown of why **eye-blink patterns is considered a strong option**, with supporting evidence from the sources:

Advantages of Eye-Blink Patterns in Biometric Authentication

1. **Dynamic and Unique**Eye-blinking is a dynamic biometric that is unique to everyone. This makes it difficult to spoof or replicate. The patterns of eye-blinks are not static and can be captured as a sequence of movements, adding another dimension of security to the authentication process (Saied et al., 2020)
2. **Liveness Detection**Eye-blinking patterns (Which is an ocular biometric trait) inherently ensure liveness of the user, as they require a real-time, biological response, making it difficult for an attacker to use a recording of a user's face to bypass authentication (Taha et al., 2023)
3. **Non-Intrusive and Convenient**Capturing eye-blinks can be done remotely using a camera, without requiring any direct physical contact with a sensor (Saied et al., 2020) (Taha et al., 2023)  
     
   This makes it a convenient option for continuous authentication systems, since it can be performed without the user's explicit action (Abuhamad et al., 2021) (Taha et al., 2023)
4. **Resistant to Spoofing**Unlike static face recognition, eye-blink patterns are difficult to spoof, as it is a dynamic biometric. The eye-blinking counter pattern method is noted to be novel and enhances security by requiring a different pattern each time. This dynamic challenge-response approach makes it difficult for attackers to use replay attacks. (Saied et al., 2020) - Could be inappropriate since, in our system, we will not be asking the user to give different blinking pattern each time. (Rad the paper for proper understanding)
5. **High Accuracy**Several studies show that eye-blink based systems can achieve high accuracy rates. One study achieved 98.4% accuracy for screen unlocks on smart devices (Saied et al., 2020)   
   Another study reported over **98% classification accuracy** using patterns of blinks processed by a Gated Recurrent Unit (GRU). Another research showed that EOG-based systems using voluntary eye blinks can achieve a high recognition accuracy of over 99.99% (Gorur, 2023)
6. **Complementary to Face Recognition -** Could be inappropriate   
   Eye-blink patterns can enhance face recognition systems by providing an additional layer of authentication. A system that combines face recognition with eye-blink authentication has been proposed to create a more robust system (Saied et al., 2020)   
   Eye blinking can be used to verify the liveness of the user (Taha et al., 2023)
7. **Feasibility in Various Applications** Eye-blink recognition is applicable to a variety of devices and contexts, including mobile phones, laptops, and access control systems. The method is effective even with lens reflection, thick glasses frames, and various face angles (Saied et al., 2020)  
     
   Justification for Eye-Blink over other Ocular Traits
8. **Eye-movement**- While eye movement is another viable biometric, it often requires more complex analysis of fixations, saccades, and scan paths (Silver and Biggs, 2006), (Taha et al., 2023)  
   - Some methods need specialized equipment to track eye movements accurately (Taha et al., 2023)  
   - In comparison, eye blink detection can be achieved with simpler methods based on the classification of open and closed eye states (Saied et al., 2020)  
   - Eye-blink patterns can also be extracted using EOG (electrooculography), which can be useful in situations where cameras are not feasible. (Gorur, 2023)
9. **Iris- Recognition  
   -** Iris recognition is another accurate biometric method, but it may require high-resolution images and specialized equipment (Oloyede and Hancke, 2016)  
   - Additionally, the enrolment process for iris recognition can be lengthy as it requires many images of the iris pattern (Oloyede and Hancke, 2016)  
   - Face recognition, iris recognition and fingerprint recognition are seen as highly reliable, but also require additional user action which makes them unsuitable for continuous authentication systems (Baig and Eskeland, 2021)  
   - Iris recognition can be affected by glasses and contact lenses (Oloyede and Hancke, 2016)
10. **EOG-Signals**- While EOG signals can be used for eye-blink detection, they are not practical for mobile continuous authentication systems that may require data capture via camera or device sensors. EOG signals also require special equipment to record the electrophysiological signals (Gorur, 2023)

Eyeblink pattern is a better option because

1. **Simpler Implementation**Eye-blink detection can be performed with less complex algorithms than other ocular traits (Saied et al., 2020)  
   It does not require the detailed analysis of eye movements, such as fixations and saccades (Silver and Biggs, 2006)  
   The feature extraction for blink detection can be as simple as classifying open and closed eye states with a convolutional neural network (CNN) (Saied et al., 2020)
2. **Less Resource Intensive**The computations for eye-blink detection are generally less intensive, which makes it suitable for real-time applications, especially on mobile devices with limited processing power (Saied et al., 2020)  
   Some studies on EOG-based systems show that the processing times can be minimized by using small time segments for authentication (0.5 seconds). (Gorur, 2023)
3. **Suitable for Diverse Conditions**Eye-blink detection can be robust even with variations in lighting, head pose, and the presence of glasses (Saied et al., 2020) (Fodor et al., 2023)
4. **More Stable than Other Biometrics**Some sources indicate that voluntarily generated EOG responses from eye blinks are more stable than EEG signals over time and are less susceptible to fatigue and environmental factors, leading to more reliable authentication(Gorur, 2023)

Eyeblink Pattern vs. Other Biometric Traits

1. **Physiological vs. Behavioural**- Eye-blink is a behavioural biometric, which makes it more resistant to spoofing than some physiological traits(Gorur, 2023)(Ryu et al., 2021)- Physiological traits like fingerprints and facial recognition can be easily spoofed by using fake fingerprints or images and videos of faces (Gorur, 2023) (Baig and Eskeland, 2021)
2. **Complementary to Keystroke Dynamics**- Combining eye-blink patterns with keystroke dynamics provides a multimodal approach to authentication. Keystroke dynamics is a non-intrusive biometric that can be used in the background(Piugie et al., 2022)By combining the two, the continuous authentication system can be more reliable and secure. Keystroke dynamics can complement facial recognition when lighting or distance is an issue, while facial recognition can cover time gaps in keystroke capture (Ryu et al., 2021)

**CONCLUSION**

* Eye-blink patterns offer a unique combination of being dynamic, non-intrusive, and difficult to spoof.
* They can be captured using cameras without requiring direct user interaction, which is suitable for continuous authentication systems.
* Eye-blink detection can be implemented with less complexity and computational resources compared to other ocular traits like iris recognition and eye movement tracking
* The technology has proven to be accurate and reliable in various studies.
* Eye-blink patterns complement other biometric traits, such as keystroke dynamics, to enhance overall system security and robustness.

In conclusion, eye-blink patterns present a compelling option for biometric authentication due to their unique characteristics, ease of implementation, and robust performance. While other biometric traits offer various advantages, eye-blink patterns balance security, convenience, and practicality, making them a particularly strong option for continuous authentication systems, especially when paired with other modalities like keystroke dynamics.

**05. Keystroke Dynamics Justification for continuous authentication**

Keystroke dynamics is a behavioural biometric that analyses the manner and rhythm in which an individual types on a keyboard or keypad (Adegbenle et al., 2024). It is considered a valuable biometric trait for continuous authentication systems, especially when combined with other modalities such as eye-blink patterns. Here's a summary of the benefits of keystroke dynamics and how it complements eye-blink patterns, as supported by the sources:

**Benefits of Keystroke Dynamics**

1. **Non-Intrusive and Convenient**Keystroke dynamics is a non-intrusive method that collects data as users naturally type on a keyboard(Ryu et al., 2021)It doesn't require any additional hardware, making it convenient for implementation on existing systems like laptops and mobile devices(Ryu et al., 2021) (Fereidooni et al., 2023)  
   The data collection process is transparent to the user, operating in the background without requiring any explicit action (Fereidooni et al., 2023)
2. **Cost-Effective**Since keystroke dynamics uses existing keyboards, it avoids the need for specialized hardware, resulting in a cost-effective authentication solution (Ryu et al., 2021) (Fereidooni et al., 2023)
3. **Unique Typing Patterns**Every individual has a unique typing style, characterized by variations in key press durations, the time between key presses, and rhythm (Adegbenle et al., 2024) (Abuhamad et al., 2021) (Baig and Eskeland, 2021)  
   This makes it a viable biometric for user identification and authentication (Baig and Eskeland, 2021) (Lu et al., 2020)
4. **Continuous Authentication**Keystroke dynamics allows for continuous user authentication as long as the user is typing. This is unlike one-time authentication methods that verify the user only at login (Abuhamad et al., 2021) (Baiget al., 2023)
5. **Difficult to Mimic**  
   A user's typing style is hard to mimic, adding to the security of the system (Ryu et al., 2021)
6. **Enhanced Security**Keystroke dynamics provides an additional layer of security to traditional password-based authentication (Piugie et al., 2022)   
   It can verify the user based on how they type rather than just what they type (Adegbenle et al., 2024)
7. **Versatile Application**Keystroke dynamics can be used in various applications, including both mobile and desktop platforms (Piugie et al., 2022) (Abuhamad et al., 2021) (Baig and Eskeland, 2021)   
   It can be applied to free text as well as fixed text inputs (Lu et al., 2020)
8. **Low computational cost** Behavioural biometrics are less computationally complex as compared to physiological biometrics (Ryu et al., 2021)
9. **Variety of Features**Keystroke dynamics can use a variety of features like key press frequency, key release frequency, latency and hold times, error rate, and finger pressure to analyse unique typing patterns (Abuhamad et al., 2021)

**How Keystroke Dynamics Complements Eye-Blink Patterns**

1. **Multimodal Approach**Combining keystroke dynamics with eye-blink patterns creates a robust multimodal biometric system. This approach leverages the strengths of both behavioural traits to enhance security and accuracy. Multimodal systems are more secure than systems relying on a single biometric. (Ryu et al., 2021) (Abuhamad et al., 2021)
2. **Continuous Authentication Coverage**While keystroke dynamics is effective when users are actively typing, eye-blink patterns provide a continuous authentication mechanism, regardless of the user's interaction with the keyboard (Baiget al., 2023) (Taha et al., 2023) (Gorur, 2023)  
   Thus, even when the user is not typing, eye-blink patterns can verify their identity.
3. **Independent Modalities**Keystroke dynamics and eye-blink patterns are independent modalities, meaning that they capture different aspects of user behaviour (Baiget al., 2023) (Ryu et al., 2021) (Abuhamad et al., 2021)   
   If one modality is compromised, the other can still ensure the system's security (Baiget al., 2023)   
   This independence reduces the chances of spoofing and improves overall system resilience.
4. **Enhanced Liveness Detection**Eye-blink patterns ensure liveness, while the typing pattern ensures that the user is engaging with the device (Baiget al., 2023) (Gorur, 2023) (Taha et al., 2023) (Stragapede et al., 2022) Together they provide a strong defense against replay attacks.
5. **Balanced Biometric Traits**Keystroke dynamics is a behavioural biometric while eye-blink pattern is a combination of behavioural and physiological (Adegbenle et al., 2024)   
   Using both can make the system secure and less prone to errors (Abuhamad et al., 2021)

**Specific Complementary Aspects**

1. **Temporal Gaps:** Keystroke dynamics data acquisition might have temporal gaps when a user is not typing. Eye-blink data can help cover such gaps with continuous authentication (Ryu et al., 2021)
2. **Contextual Awareness:** Keystroke patterns can vary based on the user's emotional or physical state and their activity (Abuhamad et al., 2021) Eye-blink patterns can add a layer of authentication when typing patterns might be unreliable, and vice versa.
3. **Covert and Frictionless Nature:** Both keystroke dynamics and eye-blink patterns are covert and frictionless (Adegbenle et al., 2024)  
   This implies they can be used without the user being aware of it and can provide continuous authentication without the need for an explicit user action (Baiget al., 2023) (Abuhamad et al., 2021) (Piugie et al., 2022)

**CONCLUSION**

Keystroke dynamics offers a cost-effective and convenient way to authenticate users based on their unique typing patterns. By combining it with eye-blink patterns, a more secure and robust continuous authentication system can be achieved. The two modalities compensate for the limitations of each other and offer a comprehensive solution that is difficult to spoof and convenient for users. Both modalities are non-intrusive and operate in the background, enabling continuous authentication without requiring explicit user action.

**06. Eyeblink / Ocular authentication Architecture.**