2025

Probleemanalyse

BIOMETRISCH TOEGANGSSYSTEEM

PIOTR TADRALA | INFORDB

O-PP-CMK

INHOUDSOPGAVE

1.0 INLEIDING

Traditionele toegangssystemen, zoals sleutels en toegangspassen, zijn kwetsbaar voor verlies, diefstal en misbruik. Biometrische technologieën, zoals gezichts- en vingerafdrukherkenning, bieden een verbeterde beveiliging, maar zijn niet volledig betrouwbaar. Door de groei in AI en deepfake-technologie wordt het steeds eenvoudiger om biometrische verificatiesystemen te omzeilen. Dit vergroot de noodzaak voor een beter toegangssysteem dat meerdere verificatiemethoden en algoritmes combineert

2.0 HUIDIGE SITUATIE

Momenteel worden biometrische verificatiemethoden, zoals gezichtsherkenning en vingerafdrukscanners, breed toegepast in toegangscontrolesystemen. Hoewel deze technieken een betere beveiliging bieden dan traditionele methoden, hebben ze ook enkele beperkingen:

SPOOFING

Gezichtsherkenning kan worden misleid door foto's, video's of deepfakes

GEBREK AAN LIVENESS-DETECTIE

Veel systemen controleren niet of de biometrische input afkomstig is van een echte persoon.

AFHANKELIJKHEID VAN ÉÉN VERIFICATIEMETHODE

De meeste biometrische systemen baseren hun response op één verificatiemethode, dit maakt het veel makkelijker om die te omzeilen.

3.0 PROBLEEMSTELLING

Huidige biometrische toegangssystemen zijn niet voldoende bestaand tegen misleidpogingen, zoals deepfakes en spoofing. Daarnast zijn er veel systemen afhankelijk van één enkele verificatiemethode waardoor de veiligheid beperkt blijft.

4.0 OORZAKEN VAN HET PROBLEEM

GROEI IN AI TECHNOLOGIE

Gezichtsherkenning wordt steeds gemakkelijker te misleiden.

BEPERKTE IMPLEMENTATIE VAN ANTI-SPOOFING

Relatief weining systemen implementeren anti-spoofing waardoor gebruikers een vals gevoel van veiligheid kunnen krijgen. Dit kan verder de leiden zijn aan het gebrek aan regelgeving rondom biometrische verificaties, waardoor bedrijven, om kosten te besparen, geen anti-spoofing implementeren.

FOCUS OP USER-EXPERIENCE

Veel systemen kiezen voor een eenvoudige verificatiemethode om de user-experience soepel te houden, wat ten koste gaat van het veiligheid

BEPERKTE REGELGEVING EN STANDAARDEN

Door het gebrek aan duidelijke richtlijnen voor biometrische verificatie kunnen bedrijven zelf bepalen in hoeverre ze anti-spoofingoplossingen implementeren, wat vaak tot minimale inzet leidt.

5.0 MOGELIJKE OPLOSSINGEN

- **Multi-factor verificatie:** Naast biometrische herkenning zou een extra verificatiestap toegevoegd kunnen worden, zoals een interactief element of een andere verificatiemethode.
- **Anti-spoofing technieken**: Implementatie van technieken die spoofing-attacks kunnen detecteren.
- **Dynamische verificatie:** Het integreren van een verificatiemethode die per gebruiker of context kan variëren.

6.0 BRONNEN

- Richard Carriere, (2023) As Biometrics adoption surges, anti-spoofing is non-negotiable
- 1kosmos, (2024) Combatting Biometric spoofing