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 hoger beveiligingsniveau, maar zijn niet volledig betrouwbaar. Door de snelle ontwikkelingen in AI en deepfake-technologie wordt het steeds eenvoudiger om biometrische verificatiesystemen te omzeilen. Dit onderstreept de noodzaak van een geavanceerder toegangssysteem dat meerdere verificatiemethoden en intelligente algoritmes combineert om de veiligheid te verhogen.

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.

PRIVACYRISICO'S EN ANGST VOOR DATALEK

Biometrische gegevens zijn zeer gevoelig. Wanneer deze gegevens worden gelekt of gestolen, zijn ze niet eenvoudig te wijzigen zoals wachtwoorden.

FOUTMARGES EN ONNAUWKEURIGHEID

Biometrische systemen zijn niet altijd 100% nauwkeurig. Slechte lichtomstandigheden, verouderde algoritmes of wijzigingen in het uiterlijk van de gebruiker kan leiden tot onnauwkeurigheid van het systeem.

HOGE KOSTEN

De implementatie van geavanceerde biometrische systemen, zoals die met liveness-detectie of geavanceerde sensoren, kan hoge initiële kosten en onderhoudskosten met zich meebrengen.

AFHANKELIJKHEID VAN TECHNOLOGIE BIJ STORINGEN

Storingen in het systeem, zoals netwerkproblemen of hardwarefouten, kunnen de toegang blokkeren of het systeem onbetrouwbaar maken. Er dient dus altijd een back-upmethode aanwezig te zijn

3.0 PROBLEEMSTELLING

Hoewel biometrische toegangssystemen een hoger beveiligingsniveau bieden dan traditionele methoden, zijn ze kwetsbaar voor misleidingspogingen zoals deepfakes en spoofing. Daarnaast vertrouwen veel systemen op slechts één enkele verificatiemethode, wat de veiligheid beperkt en de kans op ongeautoriseerde toegang vergroot. Bovendien brengen deze systemen privacyrisico's, foutmarges en hoge implementatiekosten met zich mee.

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

Door biometrische verificatie te combineren met een tweede of derde authenticatiemethode, zoals een pincode, een fysieke token (bijv. een smartcard) of gedragsbiometrie, wordt de beveiliging aanzienlijk verhoogd.

Voorbeeld: Een systeem vereist zowel gezichtsherkenning als een eenmalige code (OTP) via een mobiele app voordat toegang wordt verleend.

ANTI-SPOOFING TECHNIEKEN

Het integreren van (AI-gestuurde) liveness detection kan helpen om deepfake- en spoofing-aanvallen te herkennen. Dit kan door middel van:

- **3D-gezichtsdetectie:** controleert of het een echt gezicht is in plaats van een foto of video.
- **IR-scanning:** Detecteert warmte of specifieke lichtpatronen om te bepalen of het gezicht echt is en niet van een afbeelding of masker.
- **AI:** AI-modellen die getraind zijn voor het herkennen van deepfakes

DYNAMISCHE VERIFICATIE

In plaats van een statische biometrische scan, kan het systeem continu en adaptief controleren of de gebruiker legitiem is. Dit kan door:

- **Gedragsbiometrie:** analyse van unieke patronen zoals loopstijl.
- **Tijd- en locatiegebonden toegang:** verificatie afhankelijk maken van de context, zoals het tijdstip en de locatie, voorbeeld: Een werknemer die normaal alleen tijdens kantooruren toegang heeft, wordt extra gecontroleerd bij een inlogpoging midden in de nacht.

6.0 BRONNEN

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