Jämförelse av kontinuerliga autentiseringsmetoder för mobila enheter - med fokus på beteendebiometri

André Nordström
Kandidatavhandling i datateknik
Handledare: Marina Waldén
Fakulteten för naturvetenskaper och teknik
Åbo Akademi
2020

Abstract

I denna avhandling kommer olika kontinuerliga autentiseringssystem för mobila enheter att undersökas. Olika beteendebiometriska metoder för autentisering jämförs för att hitta fördelar och nackdelar med de olika systemen. Även sammanhangen för när de används kommer att tas i beaktande och undersökas om det finns bättre metoder att använda för vissa specifika sammanhang. Läsaren kommer att bli bekant med olika beteendebiometriska metoder och hur dessa kan användas inom dagens mobila enheter. Olika forskningsgruppers resultat kommer kritiskt att granskas, för att sedan jämföras med varandra. De väsentligaste begreppen inom beteendebiometrin tas först upp för att klargöra eventuella oklarheter och därefter jämförs de olika metoderna.

Innehållsförteckning

1. Introduktion

Autentisering är en process som användare går igenom dagligen för att verifiera sin identitet för att få tillgång till ett system. Sättet att autentisera en användare varierar beroende på vilken typ av system det är fråga om. Det vanligaste sättet att autentisera en användare har länge varit med hjälp av lösenord, där användaren identifieras med ett användarnamn som sedan passar ihop med rätt lösenord. Detta är en lätt metod att använda sig av för att autentisera användare men den har länge ansetts vara osäker. I och med ökat äventyrande av lösenord och ständigt ökande säkerhetskrav har organisationer börjat övergå till säkrare autentiseringsmetoder [1].

På senare tid har det även uppstått nya biometriska autentiseringsmetoder som använder sig av sensorer i mobila enheter och kontrollerar personers beteendemönster i användningen av dessa enheter [2], [3], [4]. De traditionella metoderna granskar användare endast vid inloggning till ett system, vilket lämnar säkerhetsbrister under inloggningssessionen däremellan. Flera studier som nämns i denna avhandling har undersökt nya beteendebiometriska metoder för att göra dessa system säkrare. Förutom att systemen blir säkrare kan vissa av dessa metoder användas utan att användaren behöver ingripa.

1.1 Kontinuerlig och statisk autentisering

Inom autentisering finns det två olika tillvägagångssätt för att autentisera en användare, närmare bestämt kontinuerlig autentisering och statisk autentisering [4]. Kontinuerlig autentisering kan även kallas för dynamisk autentisering eftersom den verifierar användaren under hela inloggningssessionen. Detta möjliggör för systemet att kontinuerligt kontrollera att det inte sker någon obehörig åtkomst. Statisk autentisering (även kallad ”one-shot”) däremot, kontrollerar användarens identitet endast vid specifika tillfällen (t.ex. vid inloggning) och ger åtkomst till system ända tills sessionen avslutas. Denna metod kan anses vara bristfällig eftersom systemet inte kontrolleras däremellan och kan bli utsatt för attacker [4].

1.2 Autentiseringsmetoder

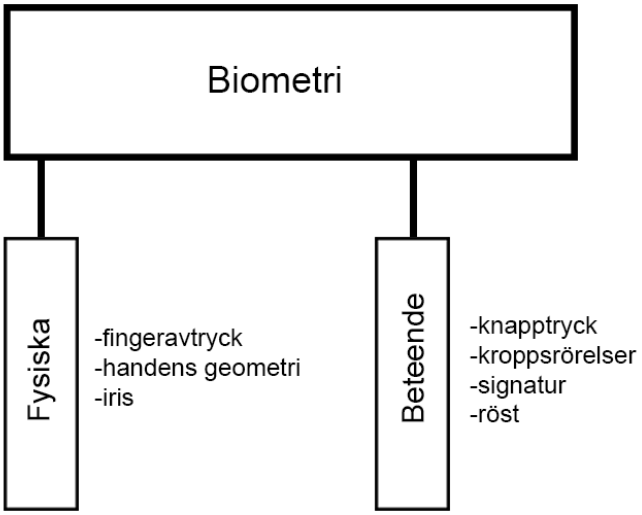
Det finns flera olika metoder för autentisering, men det brukar generellt talas om tre olika typer av autentiseringsmetoder som brukar användas vid autentisering av en användare: något som användaren vet (t.ex. ett lösenord), något som användaren har (t.ex. en säkerhetsdosa), och något som användaren är (t.ex. biometriska drag) [1], [5], [4]. Genom att kombinera åtminstone två av dessa metoder möjliggörs även flerfaktorautentisering (*eng. multi factor authentication (MFA)*). Ett exempel på detta är verifikation med en säkerhetsdosa efter att användaren har gett sitt användarnamn och lösenord [1].

1.3 Biometrisk autentisering

Användningen av biometriska data för igenkänning av en persons identitet kallas för biometrisk autentisering. De populäraste typerna inom biometrin (*eng. Biometrics*). är fysiska kännetecken och beteendekännetecken. I de fysiska dragen ingår fingeravtryck, handens geometri, iris eller retinaigenkänning osv., medan i beteende-kännetecken hittas knapptryck, kroppsrörelser, signatur, röst, osv [2]. De två olika kategorierna visas i *figur 1*.

Allt flera företag har börjat använda biometriska autentiseringsmetoder för att verifiera användare i olika system. År 2018 förväntades det att 90 % av alla större företag skulle använda sig av någon form av biometrisk autentisering år 2020 [6]. De huvudsakliga orsakerna för användning av biometrisk autentisering är [1]:

1. Risken för identitetsstöld är mycket mindre jämfört med andra autentiseringsmetoder eftersom mänskliga biologiska drag används.
2. Information som krävs vid autentisering måste inte läggas på minnet.
3. Hackare har svårt att gissa den biologiska informationen.
4. Det är omöjligt att dela biometrisk information med en annan person.



Figur 1: Olika typer inom beteendebiometri [2].

1.4 Beteendebiometri

Beteendebiometri är mätbart beteende som används för att verifiera en persons identitet. Autentiseringsmetoden fokuserar på beteendemönster istället för de fysiska dragen hos en person. Ofta används beteendebiometri i andra hand efter att en användare en gång identifierats med en annan traditionell autentiseringsmetod. Denna autentiseringsmetod kan kontinuerligt förhindra obehöriga personer att få tillgång till ett system genom att ständigt undersöka personens beteendemönster, genom att jämföra personens nuvarande mönster med ett mönster som finns lagrat i en databas. Redan under andra världskriget använde sig soldater av beteendebiometri för att identifiera sändare av morsekod. De använde sig av något som kallades för ”The fist of the sender” [7], där erfarna lyssnare kunde känna igen stilen hos den som sände koden.

2. Beteendebiometriska metoder

Beteendebiometriska metoder är olika sätt för en användare att kunna autentiseras med beteendebiometri. Av de olika beteendebiometriska metoderna skiljer sig en del märkbart från varandra medan vissa kan anses vara väldigt liknande. När det

gäller mobila enheter, kan knapptryck och pekrörelser användas för att skapa användarprofiler med endast mjukvara. För kroppsrörelser däremot, måste extra verktyg som en mobil enhets inbyggda sensorer användas. Detta är i praktiken inte ett problem eftersom de flesta av dagens smarttelefoner och klockor har dessa färdigt inbyggda.

2.1 Signatur

Eftersom varje människas signatur, och även handstil är unik kan denna metod även användas för autentisering. Med hjälp av apparater som överför personers signatur digitalt, kan signaturen sedan analyseras för att bestämma om det är rätt person som givit signaturen. Med hjälp av mera avancerade apparater blir igenkänningen även lättare och mera effektiv.

2.2 Knapptryck

Samma som att varje människas handstil är unik, är även varje människas sätt att skriva på ett tangentbord unikt. Genom att mäta tiden det tar mellan olika knapptryck på ett tangentbord och hur länge en knapp är nedtryckt, kan användaren identifieras genom att jämföra de pågående knapptrycken med en profil som finns lagrad. Denna metod är enbart baserad på mjukvara och kräver inga extra sensorer för att kunna användas. [8]

2.3 Pekrörelser

Med pekrörelser syftas det på de händelser som händer vid tryck på en pekskärm. Knapptryck och pekrörelser har mycket gemensamt och kan båda användas som beteendebiometriska autentiseringsmetoder. Pekrörelser för mobila enheter kan användas för att autentisera användare genom att vid början av en rörelse på pekskärmen, registrera tiden, positionen och hastigheten av rörelsen. [9]

2.4 Kroppsrörelser

Kroppsrörelser använder vi oss av hela tiden och är något som inte skall bortses inom biometrin. Varje människa har unika sätt att röra sig på och med hjälp av olika sensorer och mätverktyg kan detta mätas och användas för att autentisera en användare. Sensorer inbyggda i dagens smarttelefoner eller smartklockor kan användas för att bygga en profil av en person som rör på sig. Dessa profiler kan sedan användas vid autentisering. [2]

2.5 Röst

Varje människa har en unik röst som kan analyseras med hjälp av olika verktyg. Även om röster kan verka likadana för ett människoöra, hittas det flera små skillnader vid analys av röstens mönster. Dessa små skillnader kan sedan användas för att skilja åt olika människors röst och därmed kunna ge åtkomst åt endast behöriga personer. Röstigenkänning är inte alltid pålitligt eftersom till exempel bakgrundsbrus eller andra externa ljudkällor kan störa röstigenkänningen. [8]

Utöver dessa beteendebiometriska metoder finns även andra metoder som inte nämnts. De ovan nämnda metoderna är de som idag oftast används för att skapa ett beteendebiometriskt autentiseringssystem. I framtiden kan även andra metoder användas för att uppnå önskade resultat.

3. Biometriska mätnings-värden

Inom biometriska autentiseringssystem används generellt olika värden för att avgöra om en användare är den som den påstår sig att vara. Med hjälp av de olika värdena kan det till exempel avgöras med hur stor noggrannhet en användare accepteras till ett system.

3.1 True Acceptance Rate (TAR)

Korrekt godkännande av en behörig person till ett biometriskt system. Detta händer när allt har gått som det ska och en person som ska få tillgång till ett system verkligen får tillgång till systemet. I optimala fall händer det 100% TAR. Detta är förstås inte möjligt i praktiken men är ett bra mål att försöka nå.

3.2 False Acceptance Rate (FAR)

Felaktigt godkännande är den värsta säkerhetsbristen som kan hända i ett biometriskt system, eftersom det felaktigt beviljas åtkomst till användare efter autentisering. FAR vilket även kan ha namnet ”false match rate” (FMR), är mått på vad sannolikheten är för ett system att acceptera en obehörig användare och räknas ut enligt följande:

$$FAR(\mu) = \frac{Mängden\ av\ felaktigt\ lyckade\ försök}{Mängden\ gjorda\ försök}$$

μ = *säkerhetsnivån* [1]

3.3 False Rejection Rate (FRR)

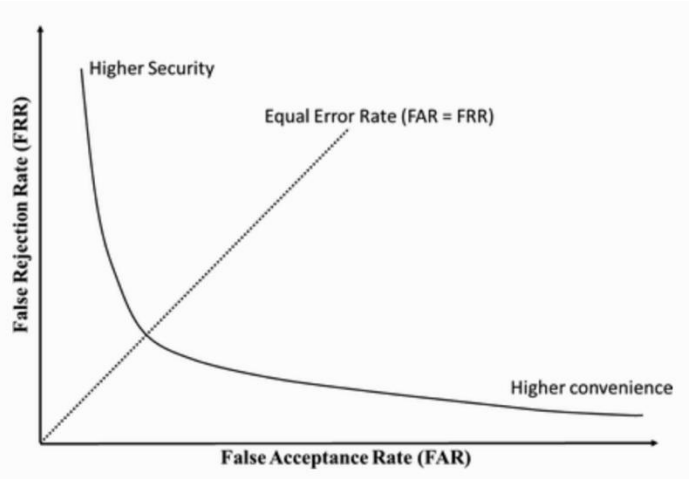
Felaktigt avslående är ett tillstånd där en behörig användare inte kan identifieras under autentiseringsprocessen. Detta händer då systemet misslyckas att hitta en träff mellan användarens indata och den biometri som finns lagrad i databasen. Är även känd som false non-match rate (FNMR)

$$FRR(\mu) = \frac{Mängden\ felaktiga\ avslag\ för\ behöriga\ användare}{Totala\ mängden\ autentiserings\ försök}$$

3.4 Equal Error Rate (EER)

Denna grad fås av övergångsvärdet som uppstår då FAR och FRR är lika. Om EER är lågt betyder det oftast att noggrannheten för systemet är högre och det motsatta

om EER är högre (se *figur 2)*. På marknaden existerar endast fåtal system som förser användaren med både ett användarvänligt system tillsammans med hög säkerhet [10]. Ofta leder det till att organisationer vill prioritera användarvänlighet framför säkerhet för att förhindra onödig kundbetjäning för system som inte accepterar korrekta användare.



Figur 2: Representationen av FAR, FRR och ERR som visar övergångsvärdet [1].

3.5 Failure to Enroll Rate (FTE)

Då systemet vid registreringsprocessen inte tar emot några giltiga data uppstår FER som betyder att det inte lades till något som kan användas vid autentisering. Detta kan hända av olika skäl. Personen kan vara utan dessa geometriska drag, kvaliteten på materialet som lades till kan vara otillräcklig, eller är det omöjligt att matcha med lagrade profilen vid autentisering.

3.6 Failure to Acquire Rate (FTA)

Detta händer då systemet inte kan inta eller hitta tillräckligt hög kvalitet av biometriska data. Oftast kan denna grad ändras med övergångsvärden i det biometriska systemet.

I alla biometriska system finns möjligheten att ändra på dessa värden och därmed välja hur känsligt ett system är. Till exempel, om noggrannheten för att acceptera

en användare höjs för att kräva nästan identiska jämförelser, betyder det att FRR ökar i samband med säkerheten. Samma sak händer även om säkerheten inte spelar någon stor roll och approximationer är godkända. Detta ökar på FAR. Ovan finns listade de vanligaste värdena som används inom biometrin. Det finns även andra värden som inte tas upp i denna text. Med hjälp av dessa värden kan det avgöras hur säkert ett system är och om det lönar sig att använda för ett visst specifikt syfte. [1]

4. Mobila sensorer

Moderna mobila enheter är fullpackade med olika sensorer som kan användas för att samla in data. Dessa sensorer kan användas inom beteendebiometrin för att läsa in beteendemönster som därefter kan bearbetas för användning inom olika autentiseringssystem. Moderna operativsystem för dessa mobila enheter ger utvecklare ofta möjlighet att lätt utnyttja sensorerna med hjälp av olika gränssnitt [2]. Mobila sensorer kan kategoriseras i tre olika typer, närmare bestämt rörelsesensorer, positionssensorer och omgivningssensorer [2].

4.1 Rörelsesensorer

Inom rörelsesensorer ingår accelerometrar, gyroskop, gravitations sensorer, osv. Dessa sensorer mäter acceleration och rotationer längsmed tre axlar.

4.1.1 Accelerometer

Accelerometern är den fysiska sensorn i mobila enheter som mäter accelerationen som påverkar på enheten ifråga. Med bland annat gravitationskraften går det att med de tre axlarna x, y och z att få ut accelerations data som sedan kan användas och bearbetas. När det är fråga om mobila enheter för personligt bruk är accelerationen ofta inte kontinuerlig i en och samma riktning, utan accelerations värdet har en tendens att ta sig tillbaka till 0. Accelerationen *A* som påverkar en

enhet, kan räknas ut med krafterna, inkluderande gravitationskraften g som appliceras på sensorn F med följande ekvation [2]:

$$A = -g\sum\frac{F}{massa}$$

4.1.2 Gyroskop

Gyroskopsensorn mäter enheters rotation och är till stor hjälp för accelerometern eftersom den hjälper förstå åt vilket håll enheten är vänd. Enheten för gyroskopsensorn är i rad/s, och mäts i de tre olika dimensionerna. Gyroskop är inte exklusiva för mobila enheter utan kan även hittas i t.ex. flygplan för att mäta lutningen och dess position [11].

4.1.3 Gravitationssensor

Denna sensor mäter gravitationskraften i tre olika riktningar och kan ange riktningen och styrkan av kraften som appliceras på enheten. Enheten för gravitationen är lika som för accelerometern i m/s^2 och mäts runt x, y och z axlarna. Tidigare har enheters lutning konstaterats med hjälp av accelerometern där värdena har filtrerats med ett låg-pass filter, men i dagens läge har de flesta enheter en inbyggd gravitationssensor som gör detta. [2]

4.2 Positionssensorer

För positionssensorer ingår orienterings och magnetometer sensorer som mäter den fysiska positionen av den mobila enheten. Både rörelse- och positionssensorer har tidigare visat sig vara effektiva för att särskilja användare och har redan använts i flera sammanhang för att autentisera användare. [2]

4.2.1 Orienteringssensor

Orienteringssensorn mäter värdena för vinklarna i en mobil enhet och mäter enhetens orientering runt tre axlar. Sensor använder dock ett annat koordinatsystem

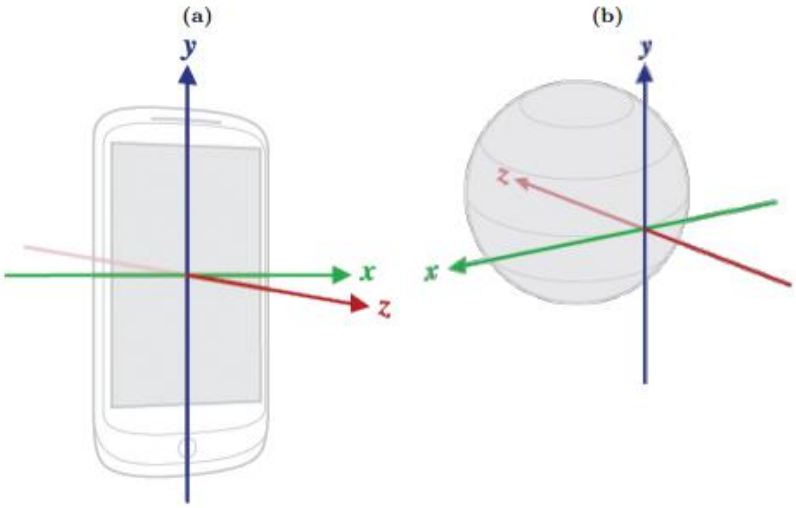
jämfört med accelerometern och kan användas till exempel för att avgöra om en enhet är i porträtt eller landskaps läge. [2]

4.2.2 Magnetometer

Magnetometern mäter styrkan och riktningen av magnetfältet runt de tre axlarna. Om en enhet är fri från andra magnetiska störningar kan magnetometern mäta jordens magnetfält. Jämfört med en kompass kan denna sensor inte ge den nordliga riktningen. [2]

4.3 Omgivningssensorer

Med omgivnings sensorer som till exempel barometer, termometer osv., mäts olika sorters fenomen som händer i omgivningen. Omgivningssensorer är inte de mest pålitliga för att användas som statiska autentiseringsmetoder eftersom deras data ofta förändras under en längre tid, men kan däremot vara utmärkta för kontinuerlig autentisering [2].



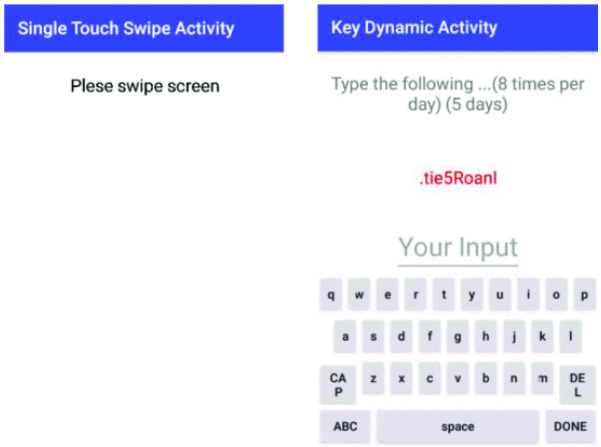
Figur 3: a. Koordinatsystem relativt till den mobila enheten. b. Koordinatsystem som används i orienteringssensorn. [2]

5. Autentiseringsprocessen

5.1 Insamling av data

Det första steget för användning av beteendebiometriska system är insamling av data. Detta sätt kan variera mycket beroende på vilken beteendebiometrisk metod som används. Råa data som blivit insamlade behöver därefter bearbetas på olika sätt beroende på vilka metoder som använts.

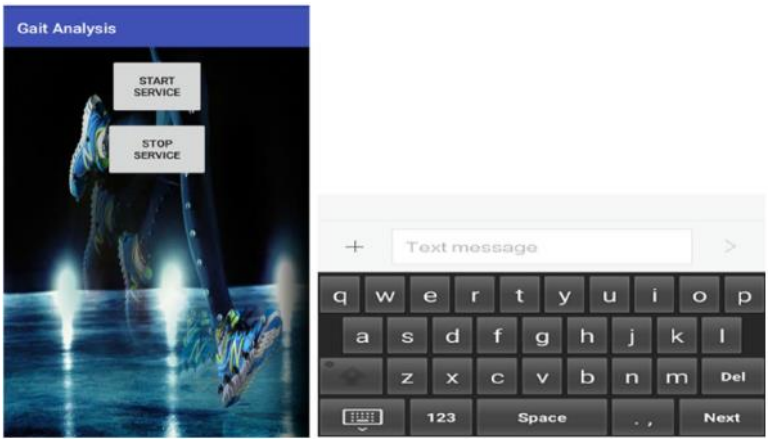
Inom en studie [9] användes en Android-baserad mobilapplikation för insamlingen av data i ett beteendebiometriskt system för knapptryck och pek-rörelser (*se figur 4*). Där måste användaren först utföra en pekrörelse på skärmen och sedan mata in ett komplext lösenord med enhetens inbyggda pekskärmstangentbord. Inom denna studie måste användarna utföra dessa operationer femtio gånger innan alla data som behövdes var samlade.



(a) Swipe stage. (b) Password typing stage.

Figur 4: Mobilapplikation för insamling av data från knapptryck och pekrörelser [9].

En annan studie [12] utförde en liknande insamling av data med en specialtillverkad Androidapplikation för att samla in data för knapptryck och kroppsrörelser (*se figur 5*). Denna applikation samlade in tre-dimensionella data runt de tre axlarna x, y och z med hjälp av accelerometern, när användaren för enheten rörde på sig. Data samlades därefter in genom att be användaren utföra realistiska scenarion med vardagliga aktiviteter. Även ett scenario där användaren både rörde på sig och skrev på tangentbordet utfördes.



Figur 5: Mobilapplikation för insamling av data för knapptryck och kroppsrörelser [12].

I en tredje studie [3] samlades data in från sensorer via både smarttelefoner och smartklockor. Där utförde personer aderton olika aktiviteter med en smarttelefon i deras högra byxficka och en smartklocka på deras dominanta hand. Här skedde den mesta delen av datainsamlingen under optimala labbförhållanden vilket kan ge avvikande resultat, men det var ansett viktigt för datakvaliteten. Även här användes en skräddarsydd Androidapplikation för uppsamling av data från enheternas accelerometer och gyroskop.

Ofta fås flera olika parametrar från sensorer, som alla måste tas i beaktande för att sedan kunna användas för att urskilja olika modeller. Exempelvis i den tredje studien [3] som nämns ovan, utvinns rörelsedata från sensorer som sedan sparas på separata rader i en datafil med följande format:

<subject-id, activity, timestamp, x, y, z>

Subject-id är personen som utför aktiviteten, *activity* står för den fysiska aktiviteten som utförs, *timestamp* är tidpunkten som data samlas in, medan x, y och z representerar sensorvärdena för de tre axlarna

5.2 Extrahering av särdrag

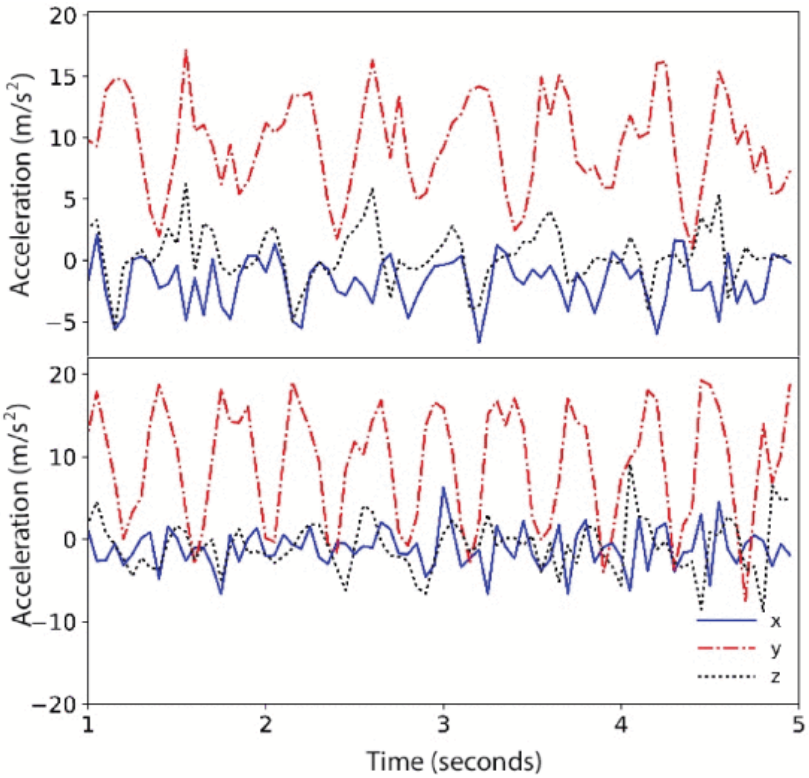
Extrahering av särdrag utförs efter att alla data som behövs blivit samlade. Detta är en obligatorisk process där alla råa data bearbetas och särskiljande drag fås fram

för att senare kunna användas för att identifiera användare. Eftersom olika klassificeringsalgoritmer har svårt att använda sig av råa data behöver den först behandlas.

5.2.1 Kroppsrörelsedata

Ett vanligt sätt för bearbetning av data från rörelsesensorer är att använda ett 10 sekunders fönster för dess insamlade data [3]. Ett 10 sekunder långt fönster används för att det anses vara tillräckligt långt för att få med nyckelelement från en persons rörelser, inkluderande repetitiva bas-rörelser från olika sorters gåendemönster. Inom dessa fönster kan det även uppstå mycket onödiga data. Exempel på ett fönster med data visas i *figur* 6. Inbyggda sensorer som accelerometrar i mobila enheter är ofta utsatta för brus eftersom deras funktionalitet styrs av enhetens inbyggda operativsystem [12]. Mycket av dessa brus kan elimineras med hjälp av specialdesignade filter. Till exempel användes det i den andra ovannämnda studien [12] ett FIR låg-pass filter designat i MATLAB på signalen från sensorerna. Vanliga särdrag som kan extraheras från givna data kan inkludera [12] [3]:

- **Medeltal**: medeltalet av sensorvärden för varje axel
- **Standardavvikelse**: standardavvikelsen för varje axel
- **Genomsnittlig absolut skillnad**: medeltalet av absoluta skillnaden mellan varje sensorvärde och medeltalet av alla sensorvärden
- **Korskorrelation**: korrelationen mellan värdena av två vektorer, till exempel mellan x och y axeln
- **Tid mellan toppar**: tiden mellan topparna om en sinusvåg formas inom givna data



Figur 6*:* Grafiskt representerade accelerometerdata från en mobil enhets tre axlar under en persons gående (övre grafen) och springande (nedre grafen) [3].

5.2.2 Tangenttryck och pekrörelsedata

Flera olika metoder används för extrahering av tangentryck och pekrörelsedata. För tangenttryck har det visat sig vara effektivt fokusera på information gällande tidpunkter för nedtryckning och släppande av knappar [12]. Pekrörelser däremot fokuserar för det mesta på koordinater och tiden mellan de olika koordinaterna. Data för tangenttryck och pekrörelser kan delas in i tre olika kategorier: temporära funktioner (t.ex. hur länge en knapp trycks ner och tiden mellan två knapptryck), lägesfunktioner (t.ex. x och y koordinaterna för den nedtryckta tangenten) och pekrörelsers funktioner (t.ex. pekrörelseriktning, längd och hastighet) [9]. Vanliga särdrag som kan extraheras från pekrörelser och tangenttrycks data kan förutom ovannämnda inkludera [9] [12]:

- **Ner-upp**: tidsintervallet mellan att trycka och släppa samma knapp
- **Ner-ner**: tidsintervallet mellan en knapptryckning och följande knapptryck
- **Upp-ner**: tidsintervallet mellan att släppa en knapp och trycka på nästa knapp

- **Upp-upp**: tidsintervallet mellan att släppa en knapp och släppa följande knapp
- **Tryckkraft**: kraften som används vid t.ex. knapptryck eller pekrörelse
- **Storleken av beröringsområdet**: Storleken av området som pekskärmen utsätts för
- **Skrivhastighet**: genomsnittliga tiden för ett knapptryck (ner-upp)

5.3 Klassificering

Dataklassificering är även en väsentlig del i autentiseringsprocessen och strävar efter att kategorisera objekt enligt indata. För att kunna generera autentisering och identifieringsmodeller används olika sorters klassificeringsalgoritmer. Inom de tre ovannämnda studierna har olika algoritmer använts och testats för att uppnå bästa resultat. Exempel på några av algoritmerna som använts i studierna är: Support Vector Machines [9] [12], Random Forest [12] [3], Random Tree [12], Naïve Bayes [9] [12], Multilayer Perceptron [9] [12], Decision Tree [9] [3] och K-Nearest Neighbors [9] [3]. För att veta hur effektiva de olika metoderna är, används EER värdet för att mäta prestandan på autentiseringssystemet. FAR och FRR värden används för att kontrollera hur stor andel av användare blivit korrekt och inkorrekt accepterade och avvisade.

6. Jämförelse av resultat

De tre olika studierna genomförs alla med beteendebiometriska metoder som kan mätas och jämföras. Olika tillvägagångssätt används och resultaten presenteras i liknande former.

6.1 Beteendebiometri med pekrörelser

I den första studien [9] behandlades ett beteendebiometriskt system med knapptryck och pekrörelser. Noggrannheten på klassificeringen och F1 värden mättes för att mäta prestandan. De olika klassificerings algoritmerna testades med en 10-faldig korsvalideringsmetod på modellerna. Med de resultat som åstadkoms i studien, kunde det noteras att prestandan med endast ett drag var märkbart sämre jämfört med om två olika drag kombinerades. Då de temporära funktionerna, lägesfunktionerna och pekrörelse funktionerna kombinerades, uppnåddes noggrannhets/F1 resultat varierande från 86.59% / 85.43% till 94.05% / 93.15%, medan system med endast ett drag varierade från 63.03% / 60.42% till 88.30% / 85.96%.

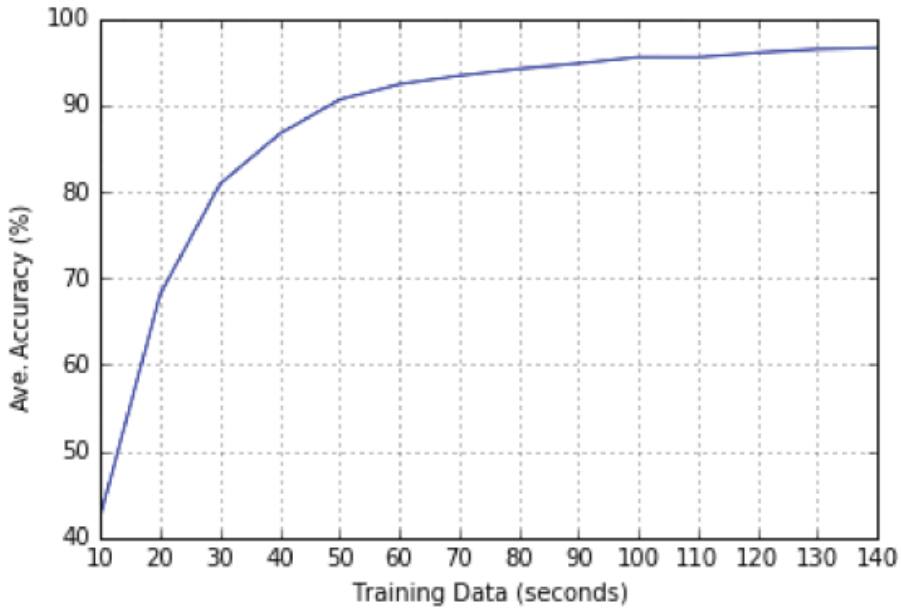
6.2 Beteendebiometri med rörelsemönster

I den andra studien [12] där beteendebiometri med rörelsemönster och tangenttryck behandlades, simulerades flera verkliga scenarion och höga noggrannhetstal uppnåddes med de kombinerade dragen. Även här användes en 10-faldig korsvaliderings teknik för att mäta prestandan på de olika modellerna. Flera olika resultat uppnåddes med de olika klassificerings algoritmerna, men vid det högsta uppnådda resultatet användes Multilayer Perceptron algoritmen. Den nådde en noggrannhets nivå på 99.11% med medeltals värden för FAR 0.684%, FRR 7% och EER 1%. Det har tidigare ansetts vara problematiskt att pålitligt använda tangenttryck som beteendebiometrisk metod på grund av att personer påverkas av trötthet under dagens gång. I denna studie har det inte påverkat resultaten särskilt mycket på grund av användningen av kombinerade drag (kroppsrörelser och tangenttryck).

6.3 Beteendebiometri med kroppsrörelser

Den tredje studien [3] som använde sig av kroppsrörelser för att autentisera användare har även nått optimala resultat. Den använde sig av sensorer i

smarttelefoner och smartklockor för att utvinna rörelsedata. Resultaten har även i vissa fall baserats på ett röstningssystem, som tar majoriteten av resultaten från fem tio sekunders data-fönster. Utgående från de resultat som studien åstadkommit vid jämförelse av klassificerings algoritmer, har Random Forest algoritmen presterat bäst för alla sensorer förutom för klockans gyroskop när röstningssystemet inte tillämpades. Genom att mäta EER värden från de olika aktiviteterna vid autentiserings resultaten, har de lägsta EER medelvärdena fåtts från accelerometrarna 11.3% och kombinationen av alla sensorer 11.5%. Identifierings resultaten nådde en noggrannhet på 94.7% med accelerometrarna, och om röstnings-metoden användes, nåddes perfekt noggrannhet på 100% vid de flesta av aktiviteterna. Det har även konstaterats att noggrannheten kan förbättrats genom att öka på tillgänglig tränings data, se *figur 7.* Figuren visar tydligt exempel på detta, men kan även konstateras att pålitliga resultat kan åstadkommas med under en minuts data.



Figur 7: Inlärningskurva för identifierings noggrannheter av de olika utförda aktiviteterna, med tiden för använd träningsdata på x axeln och noggrannheten på y axeln [3]**.**

6.4 Jämförelse av studierna

Studierna har använt sig av olika metoder för att uppnå högsta möjliga resultat. I den första och andra studien användes det även kombinerade metoder för autentisering, medan den tredje studien använde sig av en och samma metod men uppdelad med två enheter. Den första studiens resultat var höga och visade sig förstärka användarens autentisering, men de två andra studiernas resultat var på en helt annan nivå. Både i den första och andra studien bevisades det att med hjälp av att kombinera olika metoder, exempelvis kroppsrörelser och tangenttryck, kunde resultaten märkbart höjas. De olika studierna visade även att beroende på vilken typ av metod som användes, varierade även prestandan på klassificerings algoritmerna. Till exempel utförde Multilayer Perceptron algoritmen i den andra studien det bästa resultatet medan Random Forest var den vinnande algoritmen inom den tredje studien. Även pålitligheten behandlades i studie två och tre där det kom fram att datainsamlingen även testades under realistiska och påfrestande förhållanden med positiva resultat. Testnings förhållandena uppkom inte i den första studien. Utgående från resultaten kan det konstateras att höga noggrannhetstal inom mobila enheter lättare nås med biometriska system som involverar kroppsrörelser gentemot endast tangenttryck och pekrörelser.

7. Sammanfattning

I denna avhandling har olika typer av kontinuerlig autentisering med beteendebiometri behandlats och tre olika studier som fokuserat på detta inom mobila enheter har jämförts. För göra det lättare för läsaren har även centrala begrepp och metoder kort förklarats.

Beteendebiometriska metoder med kontinuerlig autentisering har visat sig vara effektiva för att förhindra obehörig åtkomst till system och förstärka säkerheten där traditionella autentiseringsmetoder används. Inom de ovan behandlade studierna har metoder med knapptryck, pekrörelser och kroppsrörelser använts tillsammans med smarttelefoner och smartklockor. Genom att kombinera beteendebiometriska metoder och använda sig av flera olika enheter har det visat sig att säkerheten märkbart ökat. Dock kan inte endast noggrannhet och säkerhet mäta hur lyckat ett

system är, utan även användarbarhet behöver tas i beaktande Detta görs inte i alla dessa studier och skulle kunna förbättras.

Dessa system som behandlats har alla utfört specifika aktiviteter för insamlingen av data och uppbyggnad av användarprofiler. I framtiden skulle även kontinuerliga system som baserar sig på användares alla dagliga aktiviteter kunna utvecklas vidare. Överlag finns det fortfarande mycket potentiella möjligheter för framtida kontinuerliga beteendebiometriska system.

Referenser

[1] D. Dipankar, R. Arunava ja N. Abhijit, Advances is User Authentication, Springer, 2017.

[2] B. Attaullah, ”Behavioral Biometrics for Smartphone User Authentication,” DISI, Trento, 2017.

[3] G. M. Weiss, ”Smartphone and Smartwatch-Based Biometrics Using Activities of Daily Living,” *IEEE Access*, 2019.

[4] N. A. Mahadi, M. A. Mohamed, A. I. Mohamad, M. Makhtar, M. F. A. Kadir ja M. Mamat, ”A Survey of Machine Learning Techniques for Behavioral-Based Biometric User Authentication,” tekijä: *Recent Advances in Cryptography and Network Security*, IntechOpen, 2018.

[5] Y. Li, J. Yang, M. Xie, D. Carlson, H. G. Jang ja J. Bian, ”Comparison of PIN- and pattern-based behavioral biometric authentication on mobile devices,” tekijä: *IEEE*, Tampa, 2015.

[6] Spiceworks, ”spiceworks,” 12 Mars 2018. [Online]. Available: https://www.spiceworks.com/press/releases/spiceworks-study-reveals-nearly-90-percent-businesses-will-use-biometric-authentication-technology-2020/.

[7] I. Deutschmann, P. Nordström ja L. Nilsson, ”Continuous Authentication Using Behavioral Biometrics,” IEEE, 2013.

[8] K. Chenigaram, ”Various Biometric Authentication Techniques: A Review,” *Journal of Biometrics & Biostatistics*, 2017.

[9] K.-W. Tse ja K. Hung, ”Behavioral Biometrics Scheme with Keystroke and Swipe Dynamics for User Authentication on Mobile Platform,” tekijä: *ICCAIE*, 2019.

[10] recogtech, ”recogtech,” [Online]. Available: https://www.recogtech.com/en/knowledge-base/security-level-versus-user-convenience.

[11] D. Nield, ”Gizmodo,” 23 07 2017. [Online]. Available: https://gizmodo.com/all-the-sensors-in-your-smartphone-and-how-they-work-1797121002.

[12] I. Lamiche, ”A continuous smartphone authentication method based on gait patterns and keystroke dynamics,” *Journal of Ambient Intelligence and Humanized Computing*, 2018.

[13] C. Perera, A. Zaslavsky, P. Christen, A. Salehi ja D. Georgakopoulos, ”Capturing Sensor Data from Mobile Phones using Global Sensor NetworkMiddleware,” tekijä: *PIMRC*, Sydney, 2012.