

**SAPIENTIA ERDÉLYI MAGYAR TUDOMÁNYEGYETEM
MAROSVÁSÁRHELYI KAR,
INFORMATIKA SZAK**



SAPIENTIA
ERDÉLYI MAGYAR
TUDOMÁNYEGYETEM

Nyitott ajtók az ember-gép interfész használatával: a
jelszómentes biztonságos beléptetés új megközelítése

DIPLOMADOLGOZAT

Témavezető:
Dr. Iclănzan Dávid,
Egyetemi docens

Végzős hallgató:
Bakó László - Mihály

2023

UNIVERSITATEA SAPIENTIA DIN CLUJ-NAPOCA
FACULTATEA DE ȘTIINȚE TEHNICE ȘI UMANISTE,
SPECIALIZAREA INFORMATICĂ



UNIVERSITATEA
SAPIENTIA

Deblocarea ușilor cu ajutorul interfeței om-mașină: o nouă
abordare a accesului securizat fără parolă

LUCRARE DE DIPLOMĂ

Coordonator științific:
Dr. Iclănzan Dávid,
Conferențiar universitar

Absolvent:
Bakó László - Mihály

2023

**SAPIENTIA HUNGARIAN UNIVERSITY OF
TRANSYLVANIA
FACULTY OF TECHNICAL AND HUMAN SCIENCES
COMPUTER SCIENCE SPECIALIZATION**



SAPIENTIA
HUNGARIAN UNIVERSITY
OF TRANSYLVANIA

Open doors with human-machine interface: a new approach to
password-free secure access

BACHELOR THESIS

Scientific advisor:
Dr. Iclănzan Dávid,
Associate professor

Student:
Bakó László - Mihály

2023

LUCRARE DE DIPLOMĂ

Coordonator științific:
dr. Iclanzan David

Candidat: **Bakó László**
Anul absolvirii: 2023

a) Tema lucrării de licență: Utilizarea interfețelor om-mașină ca alternativă la sistemele de control al accesului fără parolă, bazată pe principiul „dead man switch”.

b) Problemele principale tratate:

- Studiul literaturii de specialitate și investigarea posibilității de utilizare a interfețelor om-mașină ca alternativă la sistemele de control al accesului fără parolă.
- Studiu bibliografic și analizarea funcționării interfețelor om-mașină și a principiului "dead man switch". Identificarea potențialelor aplicații și domenii în care interfețele om-mașină ar putea fi implementate cu succes.
- Evaluarea aspectelor de securitate asociate utilizării interfețelor om-mașină.
- Examinarea opțiunilor tehnologice și soluțiilor disponibile pentru implementarea interfețelor om-mașină.
- Proiectarea și implementarea a cel puțin două soluții.
- Testarea sistemelor în diferite condiții pentru a evalua fiabilitatea și siguranța acestuia.
- Compararea interfețelor dezvoltate cu sistemele de control al accesului bazate pe parole în ceea ce privește siguranța și conveniența.
- Analizarea avantajelor și limitărilor utilizării interfețelor om-mașină în sistemele de control al accesului.
- Propunerea unor recomandări și concluzii privind utilizarea interfețelor om-mașină ca alternativă la sistemele de control al accesului bazate pe parole.
- Documentarea adecvată a stadiilor de proiectare, implementare și testare a aplicațiilor.

c) Desene obligatorii:

- Schema bloc a sistemului
- Diagrame de proiectare, implementare și testare pentru aplicațiile software realizate.

d) Softuri obligatorii:

- Backend pentru managementul accesului și a comunicării cu sistemele client ce încorporează o componentă, conexiune activă om-mașină.
- Cel puțin două soluții, implementări client, bazate pe interfețe om-mașină diferite.

e) Bibliografia recomandată:

Wiklund, M., Ansems, K., Aronchick, R., Costantino, C., Dorfman, A., van Geel, B., ... & Tilliss, J. (2019). Add a “dead man’s switch”. In *Designing for Safe Use* (pp. 63-64). CRC Press.

Lennick, D. (2020). *Kill switch design pattern for microservice architectures on internet of things devices* (Doctoral dissertation).

Nicolas-Alonso, L. F., & Gomez-Gil, J. (2012). Brain computer interfaces, a review. *Sensors*, 12(2), 1211-1279.

Tarkhani, Z., Qendro, L., Brown, M. O. C., Hill, O., Mascolo, C., & Madhavapeddy, A. (2022). Enhancing the security & privacy of wearable brain-computer interfaces. *arXiv preprint arXiv:2201.07711*.

Platschek, A. (2015). A Harmonized Threat/Hazard Modeling Method for Safety Critical Industrial Systems. In *Proceedings of the 17th Real Time Linux Workshop, 2015* (pp. 51-62).

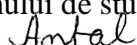
Hadid, A., Evans, N., Marcel, S., & Fierrez, J. (2015). Biometrics systems under spoofing attack: an evaluation methodology and lessons learned. *IEEE Signal Processing Magazine*, 32(5), 20-30.

f) Termene obligatorii de consultații: săptămânal, preponderent online
g) Locul și durata practicii: Universitatea „Sapientia” din Cluj-Napoca,
Facultatea de Științe Tehnice și Umaniste din Târgu Mureș, sala / laboratorul 413
Primit tema la data de: 25.04.2022
Termen de predare: 06.07.2023

Semnătura Director Departament



Semnătura responsabilului
programului de studiu



Semnătura coordonatorului



Semnătura candidatului



Declarație

Subsemnatul/a BAKO LASZLO-MIHALY, absolvent(ă) al/a specializării
INFORMATICA, promoția...2023... cunoscând
prevederile Legii Educației Naționale 1/2011 și a Codului de etică și deontologie profesională a
Universității Sapientia cu privire la furt intelectual declar pe propria răspundere că prezenta
lucrare de licență/proiect de diplomă/disertație se bazează pe activitatea personală,
cercetarea/proiectarea este efectuată de mine, informațiile și datele preluate din literatura de
specialitate sunt citate în mod corespunzător.

Localitatea, TÂRGU MUREȘ
Data: 14.06.2023

Absolvent

Semnătura...[Signature].....

Kivonat

A dolgozatban az ember-gép interfészek alkalmazásának lehetőségét vizsgáltuk, mint egy új megközelítést a jelszómentes biztonságos beléptetésre és felhasználói hitelesítésre. Az ajánlott megközelítésben az aktív kapcsolat, amely valamilyen biometrikus folyamatot monitorizál, egy biztonságosan működő „dead man switch” elvén alapuló, átruházhatatlan hitelesítési tokenként szolgál. Ha a kapcsolat megszűnik, a rendszer automatikusan visszavonja a jogosultságokat és kijelentkezteti a felhasználót. A hamisítás és megszemélyesítés elkerülése érdekében a rendszer egyszer használatos kulcsokkal védett kommunikációs protokollt használ a kliensek és az erőforrásokhoz való hozzáférést igazgató szerver között.

A kutatás során a biztonság, kényelem és költséghatékonyság kritériumai mentén elemeztük a lehetséges megoldásokat, majd implementáltunk egy kényelmesen viselhető látókéreg aktivitását monitorizáló és egy olcsón kivitelezhető pulzusfigyelésen alapuló rendszert. Az elkészült rendszereket teszteltük a megbízhatóságuk és biztonságuk felmérésére.

A kutatás eredményei alapján az átruházhatatlan hitelesítési token, a biometrikus adatok és a kommunikációs protokoll kombinációja ígéretes alternatívát nyújt a jelszó vagy egyszerű token alapú beléptető rendszerekhez képest, mivel javítja a biztonságot és lehetővé teszi a rugalmasabb, például az ideiglenesen felhatalmazott biztonsági szerepkörök létrehozását, kezelését.

Rezumat

În această teză, am explorat posibilitatea de a utiliza interfețele om-mașină ca o nouă abordare a accesului securizat fără parolă și a autentificării utilizatorilor. În abordarea propusă, interfața activă, care monitorizează un anumit proces biometric, servește ca un token de autentificare netransferabil bazat pe un "comutator de om mort" securizat. În cazul în care conexiunea este întreruptă, sistemul revocă automat privilegiile și deconectează utilizatorul. Pentru a evita falsificarea și uzurparea identității, sistemul utilizează un protocol de comunicare protejat de o cheie unică între clienți și serverul care gestionează accesul la resurse.

În cadrul acestei cercetări, am analizat soluțiile posibile pe baza criteriilor de securitate, comoditate și rentabilitate și am implementat un sistem bazat pe un monitor confortabil de activitate a cortexului vizual portabil și pe un sistem de monitorizare a ritmului cardiac cu costuri reduse. Sistemele finalizate au fost testate pentru a le evalua fiabilitatea și siguranța.

Rezultatele cercetării arată că combinația de jetoane de autentificare netransferabile, biometrie și protocol de comunicare oferă o alternativă promițătoare la sistemele de control al accesului bazate pe parole sau pe simple jetoane, deoarece îmbunătățește securitatea și permite roluri de securitate mai flexibile, cum ar fi rolurile de securitate autorizate temporar.

Abstract

In this thesis, we have explored the possibility of using human-machine interfaces as a new approach to password-free secure access and user authentication. In the proposed approach, the active interface, which monitors some biometric process, serves as a non-transferable authentication token based on a secure “dead man switch”. If the connection is terminated, the system automatically revokes the privileges and logs the user out. To avoid forgery and impersonation, the system uses a one-time key protected communication protocol between the clients and the server managing access to resources.

In this research, we analyzed possible solutions based on the criteria of security, convenience and cost-effectiveness, and implemented a system based on a comfortable wearable visual cortex activity monitor and a low-cost heart rate monitoring system. The completed systems were tested to assess their reliability and safety.

The results of the research show that the combination of non-transferable authentication tokens, biometrics and communication protocol offers a promising alternative to password or simple token-based access control systems, as it improves security and allows for more flexible security roles, such as temporary authorised security roles.

Tartalomjegyzék

1. Bevezető	11
2. Szakirodalmi áttekintés	13
2.1. Bevezetés	13
2.2. Történeti háttér a BCI világában	13
2.2.1. Nicolas-Alonso, L. F., & Gomez-Gil, J. (2012). Brain Computer Interfaces, a Review.	13
2.2.2. Parmar, P., Joshi, A., & Gandhi, V. (2018). Brain Computer Interface: A Review. International Journal of Advanced Research in Computer Science and Software Engineering	14
2.2.3. Saha, S., Mamun, K. A., Ahmed, K., Mostafa, R., Naik, G. R., Darvishi, S., ... & Baumert, M. (2021). Progress in Brain Computer Interface: Challenges and Opportunities. Frontiers in Neuroscience.	14
2.2.4. Zahra Tarkhani, Lorena Qendro, Malachy O'Connor Brown, Oscar Hill, Cecilia Mascolo, Anil Madhavapeddy (2022). Enhancing the Security & Privacy of Wearable Brain-Computer Interfaces, Cambridge University	14
2.3. Dead Man's Switch-en alapozó dolgozatok és azok fontosabb pontjai	15
2.3.1. Platschek, A. (2018). A Harmonized Threat/Hazard Modeling Method for Safety Critical Industrial Systems. Computers & Security	15
2.3.2. Lennick, D. (2018). Kill Switch Design Pattern for Microservice Architectures on Internet of Things Devices.	16
2.3.3. Összegzés	16
2.4. Szoftverek, könyvtárak	17
2.4.1. Unity	17
2.4.2. .NET	18
2.4.3. Azure	18
2.4.4. Angular	19
3. A rendszer specifikációja	20
3.1. Felhasználói követelmények	21
3.2. Rendszerkövetelmények	22
3.3. Példa	22
3.3.1. Ember-gép közötti monitorizálható kapcsolatok lehetőségei	25
3.3.2. Optimális virtuális környezet előállítása	29
3.4. Helymeghatározás	30

3.5.	Dead Man Switch szerepe	31
3.5.1.	Kill switch design pattern	31
3.6.	Jelszómentes beléptetés	32
3.7.	NextMind előnyei és hátrányok	33
3.8.	Impulzust mérő telefonkamera	34
3.9.	Biztonság tesztelése	35
4.	Tervezés	37
4.1.	Osztályok	37
5.	Mérések, eredmények	47
5.1.	Agy-számítógép interfész eredménye	47
5.2.	Impulzust mérő telefonkamera eredménye	48
5.3.	Hasonlat	48
6.	Következtetések	49
6.1.	Kutatás korlátai	49
6.2.	További kutatási lehetőségek	49
	Ábrák jegyzéke	51
	Táblázatok jegyzéke	52
	Irodalomjegyzék	54

1. fejezet

Bevezető

A jelszóalapú beléptető rendszerek használatakor előfordulhat, hogy az illetéktelenek birtokába jutnak a jelszavak, vagy a feljogosultak kényszer alatt ezeket feltárják. Továbbá, a token alapú beléptető átruházhatóak, és bár nehezebben, a biometrikus azonosítókat is ellopják, hamisíthatják az ellenséges szereplők. Az érzékeny adatok biztonsága, vagy a fizikai területek védelme érdekében érdemes olyan rendszert alkalmazni, amely minimalizálja ezeket a kockázatokat.

A „dead man switch” (magyarul: „halott ember kapcsolója”) [WAA⁺19] olyan mechanizmus, amely egy eszközt, folyamatot vagy rendszert automatikusan leállít, ha a felhasználó nem tartja fenn az aktív állapotot. A halott ember kapcsolója gyakran alkalmazható a biztonságos működés és a katasztrófák megelőzése érdekében. Például egy vonatban a dead man switch azért felel, hogy detektálja ha a vonatvezető meghal vagy elveszti az eszméletét, és ilyenkor a rendszer automatikusan megállítja a vonatot, hogy elkerülje az esetleges baleseteket, illetve riasztja a központot. A halott ember kapcsolója alkalmazása a különböző iparágakban széles körben elterjedt, beleértve az autóipart, a légiközlekedést, a katonai és űrkutatási területet.

A kutatás során megtervezett és kidolgozott rendszer egy olyan token alapú, jelszó megosztását nem igénylő megoldás, amely egy halott ember kapcsolója szerepet betöltő aktív ember-gép kapcsolat jelenlétére épít. Az ember-gép kapcsolat megszakítása esetén, a rendszer azonnal visszavonja a jogosultságokat.

Ezen irányelvek mentén, ebben a dolgozatban két megvalósítást is javasoltunk. Az első megvalósítás szerint, a jogosultsággal felhatalmazott felhasználók egy agy-számítógép interfész eszközt kapnak, amelynek segítségével a „gondolataikkal” nyithatják az ajtókat, vagy hozzáférhetnek más erőforrásokhoz. Ha a felhasználók leveszi a tokent a fejéről, a készülék már nem detektálja az agyhullámokat, a jogosultságok azonnal deaktiválódnak, megszűnnek. Ez az átruházhatatlan token biztosítja, hogy a rendszer teljesen biztonságos legyen, és csak a megfelelő személyek használhassák a jogosultságokat.

A második megvalósítás egy alternatív megközelítést képvisel: a jogosultsággal felhatalmazott felhasználók egy mobiltelefon alkalmazást kezelnek, amely a kamerára helyezett felhasználó ujjának segítségével monitorizálja a pulzusukat. Ha a felhasználó pulzusa már nem detektálható, a jogosultságok ugyancsak visszavonásra kerülnek, és a felhasználók hozzáférést az adott erőforráshoz a rendszer azonnal megvonja. Bár ez kényelmetlenebb megoldás, az előnye, hogy nem szükségesek speciális hardverek, mivel a pulzus figyelése és

monitorizálása, valamint a beléptetés aktiválása egy egyszerű mobiltelefon alkalmazással történik.

2. fejezet

Szakirodalmi áttekintés

2.1. Bevezetés

A BCI (Brain-Computer Interface) technológiák és az IoT (Internet of Things) eszközök összekapcsolódása új lehetőségeket kínál a biztonság és a rendszerek megbízhatóságának javításában. A következő szakirodalmi áttekintésben összefoglalom azokat a cikkeket, amelyek a BCI technológiák fejlődésére, alkalmazására és kihívásaira összpontosítanak, majd áttekintjük, hogyan lehet ezeket az ismereteket felhasználni a kill switch felügyeleti szerepben.

2.2. Történeti háttér a BCI világában

2.2.1. Nicolas-Alonso, L. F., & Gomez-Gil, J. (2012). Brain Computer Interfaces, a Review.

[[LF12](#)]

A cikk áttekintést nyújt a BCI-ről, amelyek olyan hardveres és szoftveres kommunikációs rendszerek, amelyek lehetővé teszik, hogy az agyi tevékenység számítógépeket vagy külső eszközöket vezéreljen. A BCI-kutatás célja, hogy kommunikációs képességeket biztosítson a súlyosan fogyatékos, bénult vagy neurológiai neuromuszkuláris rendellenességek miatt „bezárt” emberek számára.

A cikk a szabványos BCI különböző lépéseit tárgyalja, beleértve a jelgyűjtést, az előfeldolgozást vagy jeljavítást, a jellemzőkivonást, az osztályozást és a vezérlőfelületet. Emellett áttekinti a jelgyűjtés során használt különböző neuroképalkotási módokat, például az elektroencefalográfiát (EEG), a magnetoencefalográfiát (MEG), az elektrokortikográfiát (ECoG) és az intrakortikális neuronfelvételt. A szerzők tárgyalják az egyes modalitások előnyeit és hátrányait, és áttekintést nyújtanak a különböző eszközöket vezérlő BCI-alkalmazásokról.

A cikk kitér továbbá az agyi aktivitásban észlelhető különböző elektrofiziológiai vezérlőjelekre, valamint a jelerősítésben alkalmazott technikákra, amelyekkel a vezérlőjelekben megjelenő artefaktumok kezelhetők. Emellett áttekinti a jellemzők kinyerésére és osztályozására használt matematikai algoritmusokat, amelyek a vezérlőjelekből származó információkat a számítógépet vagy más eszközt működtető parancsokká alakítják.

Összességében ez az áttekintés átfogó áttekintést nyújt a BCI-kről és azok lehetséges alkalmazásairól. Értékes forrás mindazok számára, akik többet szeretnének megtudni erről az izgalmas kutatási területről.

2.2.2. Parmar, P., Joshi, A., & Gandhi, V. (2018). Brain Computer Interface: A Review. International Journal of Advanced Research in Computer Science and Software Engineering

[PP18]

Ebben a cikkben Parmar, Joshi és Gandhi áttekintést nyújtanak a BCI technológiák legújabb fejlesztéseiről és alkalmazási lehetőségeiről. A szerzők bemutatják a BCI kutatás különböző területeit, például a szenzorok és elektrodák fejlődését, a jelátviteli technikák előrehaladását, valamint a BCI rendszerek különböző típusait és alkalmazásait. A cikk rámutat a BCI technológiák jövőbeli kutatási irányaira és lehetőségeire is.

2.2.3. Saha, S., Mamun, K. A., Ahmed, K., Mostafa, R., Naik, G. R., Darvishi, S., ... & Baumert, M. (2021). Progress in Brain Computer Interface: Challenges and Opportunities. Frontiers in Neuroscience.

[SMA⁺18]

A cikk összefoglalja a BCI területén az elmúlt évtizedekben elért legújabb fejleményeket és kiemeli a kritikus kihívásokat. A kulcsszavak között szerepel az agy-számítógép interfész, hibrid/többszörös BCI, neuroimaging technikák, neuroszensorok, elektromos/-hemodinamikai agyi jelek és kognitív rehabilitáció.

A cikk részletesen tárgyalja a BCI rendszerek jellemzőit és azt is megvizsgálja, hogy milyen tényezők befolyásolják a BCI teljesítményét. Emellett a pszichofiziológiai és neurológiai kihívásokat is tárgyalja.

Összességében ez az oldal egy átfogó áttekintést nyújt az agy-számítógép interfész fejlődéséről és jelenlegi állapotáról.

2.2.4. Zahra Tarkhani, Lorena Qendro, Malachy O'Connor Brown, Oscar Hill, Cecilia Mascolo, Anil Madhavapeddy (2022). Enhancing the Security & Privacy of Wearable Brain-Computer Interfaces, Cambridge University

[TQB22]

A tanulmány a viselhető agy-számítógép interfészek (BCI) biztonsági és adatvédelmi veszélyeit tárgyalja, és bemutatja az Argus nevű rendszert, amely ezeket a veszélyeket enyhíti.

A dokumentum elmagyarázza, hogy a hordozható BCI-berendezések jellemzően egy fejre szerelt érzékelőt tartalmaznak, amely egy mobil eszközhöz csatlakozik, és a használt hardver-, szoftver- és hálózati stackek támadhatóak. Ezek a támadások kiszivárogtathat-

ják a felhasználók agyhullám-adatait, vagy átadhatják a BCI-alapú eszközök irányítását távoli támadóknak. A szerzők operációs rendszer és támadói gépi tanulás szempontjából elemzik a meglévő viselhető BCI-termékek egész rendszerre kiterjedő biztonsági és adatvédelmi fenyegetéseit.

A szerzők bemutatják az Argus-t, mint az első olyan információáramlás-ellenőrző rendszert a viselhető BCI-alkalmazásokhoz, amely enyhíti ezeket a támadásokat. Az Argus úgy tervezték, hogy könnyű legyen, és alkalmas legyen a meglévő BCI-felhasználási esetekhez. A szerzők valós BCI-eszközökön (Muse, NeuroSky és OpenBCI) végrehajtott koncepcióvizsgálati támadásaik során több mint 300 sebezhetőséget fedeztek fel hat fő támadási vektor stackjein keresztül. Értékelésük azt mutatja, hogy az Argus rendkívül hatékonyan követi az érzékeny adatáramlásokat, és elfogadható memória- és teljesítménytöbbletköltséggel ($< 15\%$) korlátozza ezeket a támadásokat.

A tanulmányban tárgyalt támadási vektorok egyike például a Sniffing, Spoofing & Man-in-the-middle a BCI host eszközökkel való titkosítatlan és nem biztonságos BLE (Bluetooth Low Energy) kapcsolatok miatt. A szerzők az összes vizsgált BCI-eszközben több sniffers-t is implementáltak, hogy rögzítsenek és elmentsék minden átvitt csomagot, MAC-címet és kapcsolati paramétert. Ezen információk megszerzése megkönnyíti az összetettebb támadások, például a MITM (Man in the middle) elindítását. A MITM-támadás révén könnyen elfoghatják és rögzíthetik a headset és az eszköz között küldött összes adatot, és az adatok megváltoztatásával veszélyeztethetik az eszköz integritását.

2.3. Dead Man's Switch-en alapozó dolgozatok és azok fontosabb pontjai

2.3.1. Platschek, A. (2018). A Harmonized Threat/Hazard Modeling Method for Safety Critical Industrial Systems. Computers & Security

[Pla18]

Andreas Platschek ebben a cikkben egy harmonizált veszélyelemzési és biztonsági modellezési módszert mutat be az ipari rendszerek számára. A módszer alapjául a HAZOP (Hazard and Operability Study) elemzés szolgál, amelyet biztonsági célú veszélyelemzésre használnak.

Ez a cikk a biztonságkritikus ipari rendszerek fenyegetés/veszély modellezésének harmonizálására szolgáló módszert tárgyalja. A szerző, Andreas Platschek, egy, a biztonság területén már alkalmazott módszer újrafelhasználását és a biztonságra való adaptálását javasolja. Ez a módszer megfelel a biztonsági szabványoknak, és építhet a biztonságtechnikai mérnökök jól megalapozott kompetenciájára. Ennek a megközelítésnek az az előnye, hogy a fejlesztőcsapatnak csak egy elemzési módszert kell ismernie.

A cikkben említett egyik példa egy "digital dead man's switch" rendszer. Ez a rendszer a mechanikus DMS (Dead man's switch), az üzemi padlóba ágyazott RFID (Radio Frequency Identification) olvasóval helyettesíti. Minden munkás két RFID-címkével rendelkezik, egy-egy csizmában. Ha a munkás használni akarja a gépet, biztosítani kell, hogy a bal lába a bal RFID-olvasón, a jobb lába pedig a jobb RFID-olvasón legyen.

A gépvezérlő csak akkor engedélyezi a működést, ha mindkét RFID-olvasóról érvényes leolvasás érkezik.

Ez a digitális DMS számos előnnyel jár a mechanikus kapcsolóval szemben. Bonyolultabbá teszi a biztonsági funkció becsapását, és további ellenőrzéseket tesz lehetővé, például a kezelő nézési irányának érzékelését és annak ellenőrzését, hogy a kezelő rendelkezik-e a gép használatához szükséges képzettséggel. Bizonyos mértékig kikényszeríti a védőfelszerelés viselését is.

Összességében ez a cikk egy érdekes megközelítést mutat be a biztonságkritikus ipari rendszerek fenyegetés/veszély modellezésének harmonizálására, és részletes példát ad arra, hogy ez a megközelítés hogyan alkalmazható a gyakorlatban.

2.3.2. Lennick, D. (2018). Kill Switch Design Pattern for Microservice Architectures on Internet of Things Devices.

[[Len22](#)]

David Lennick szakdolgozata egy „kill switch” tervezési mintát javasol az Internet of Things (IoT) eszközein működő mikroszolgáltatás-architektúrákhoz. A minta motivációja az IoT-eszközök gyors elterjedéséből és a folyamatos szoftvertámogatás elvesztése miatt közismerten bizonytalan természetükből adódó biztonsági aggályok kezelése. A szerző azt javasolja, hogy a mikroszolgáltatás-alapú virtualizált alkalmazáskomponensek és a hozzájuk tartozó kommunikációs útvonalak működési szintjeinek meghatározásával az alkalmazásfunkciók dinamikusan módosíthatók egy alapvető állapotba, hogy segítsenek megelőzni a károkat.

A dolgozat a virtualizált mikroszolgáltatásos alkalmazások javasolt tervezési mintájának formalizált definícióját és a működési szint üzemmódváltás kezelésére szolgáló algoritmust adja meg. Tartalmazza továbbá a minta elemzését és előnyeit mind az eszközgyártók, mind a végfelhasználók számára. Az eszközgyártók számára a minta megkönnyítené az eszközök karbantartását a mikroszolgáltatás-architektúra által meghatározott szolgáltatások dekompozíciója miatt, egyértelmű függőségi nyomkövetést biztosítana, és lehetővé tenné az általános célú konténerek telepítését. A végfelhasználók számára a minta lehetővé tenné az alapszolgáltatások folytatását még akkor is, ha az intelligens funkciók meghibásodnak, és lehetővé tenné az általános célú szolgáltatások telepítését, amelyek könnyebben frissíthetők.

A szerző a minta három példamegvalósítását is bemutatja: egy általános mikroszolgáltatás-alapú model-view-controller alkalmazást, egy példarendszert, amely a Suricata behatolásérzékelő rendszert használja események generálására, valamint egy módosított Docker Engine implementációt. Ezek a példák annak illusztrálására szolgálnak, hogy a kill switch minta hogyan alkalmazható különböző forgatókönyvekben.

2.3.3. Összegzés

Összefoglalva, a fent áttekintett cikkek a BCI technológiák fejlődését és az IoT eszközökkel való összekapcsolás lehetőségeit mutatják be. A BCI eszközök és IoT technológiák integrációja lehetővé teszi a kill switch felügyeleti szerepben történő alkalmazásukat is. Az ilyen alkalmazások lehetővé teszik a biztonság javítását és az adatvesztés megelőzését a BCI és IoT technológiák összetett és összekapcsolt rendszereiben. Bár a cikkek nem

foglalkoznak közvetlenül a BCI eszközök kill switch felügyeleti szerepével, a bemutatott technológiák és megközelítések alapot nyújtanak az ilyen megoldások fejlesztéséhez és alkalmazásához.

Az IoT eszközök és BCI technológiák kombinációja lehetővé teszi, hogy új szintre emeljük az ember-gép interfész képességeit és biztonságát. A BCI eszközök használata kill switch felügyeleti szerepben hatékony vészhelyzeti leállási mechanizmusokat és gyors válaszidőt biztosíthat az IoT eszközökben. Ez segít csökkenteni a kiberbiztonsági kockázatokat és a nemkívánatos incidenseket, valamint javítja az ember-gép interakció minőségét és megbízhatóságát. Ennek egy lehetséges megvalósításáról szól a jelenlegi kutatás.

2.4. Softwerek, könyvtárak

2.4.1. Unity

A Unity vagy Unity Game Engine egy olyan szoftverplatform, amely lehetővé teszi a 2D és 3D játékok, alkalmazások és élmények létrehozását és futtatását különböző platformokon, mint például a Windows, a Mac, az iOS, az Android, a VR és az AR. A Unity Game Engine segíti a játékefejlesztőket a grafikus, fizikai, hang- és mesterséges intelligencia elemek integrálásában és optimalizálásában. A Unity Game Engine széles körben elterjedt a játék- és szórakoztatóiparban, valamint más területeken, mint például az autóipar, az építészet és az oktatás.

A Unity Game Engine fontos a jelenlegi kontextusban, mert a dolgozat egy olyan ember-gép interfész megoldást vizsgál, amely a BCI (Brain-Computer Interface) technológiát használja. A BCI lehetővé teszi az agyi jelek felismerését és átalakítását olyan vezérlő jelekké, amelyeket a számítógépek vagy más elektronikus eszközök értelmezni tudnak. A dolgozatban bemutatott egyik megoldás szerint a felhasználók egy BCI eszközt viselnek a fejükön, amely monitorozza a látókéreg aktivitását. A látókéreg felelős a vizuális információk feldolgozásáért. Ha a felhasználók valamire néznek egy virtuális környezetben, akkor a BCI eszköz érzékeli az agyi aktivitást és átküldi azt egy számítógépnek vagy más eszköznek. Ezáltal a felhasználók "gondolataikkal" nyithatják az ajtókat vagy hozzáférhetnek más erőforrásokhoz.

A dolgozatban használt BCI eszköz a NextMind által készített eszköz. Ez az eszköz 9 elektródával rendelkezik, amelyeket a látókéreg régiója körül helyeznek el. A virtuális környezetben minden interaktív objektumra egy villogó mintát helyeznek el, amelyet NeuroTag-nek neveznek. Minden villanás aktiválja a látókéregre, és az eszközben mért impulzus frekvenciája alapján a rendszer következtet arra, hogy a felhasználó éppen mire néz.

A Unity Game Engine segítségével létrehozták ezt a virtuális környezetet és integrálták benne a BCI eszközt. A Unity Game Engine lehetővé tette a grafikus elemek létrehozását és animálását, valamint a NeuroTag-ek időzítését és szinkronizálását. A Unity Game Engine továbbá biztosította az alkalmazás kompatibilitását különböző platformokkal és eszközökkel.

Összegezve tehát a Unity Game Engine egy olyan szoftverplatform, amely lehetővé teszi a 2D és 3D játékok, alkalmazások és élmények létrehozását és futtatását különböző platformokon. A Unity Game Engine fontos szerepet játszik a dolgozatban bemutatott ember-gép interfész megoldásban,

2.4.2. .NET

A .NET egy szoftverfejlesztési platform, amelyet a Microsoft hozott létre, és lehetővé teszi a fejlesztők számára, hogy különböző típusú alkalmazásokat hozzanak létre, mint például asztali, webes, mobil és felhőalapú alkalmazások. A platform a Common Language Runtime (CLR) nevű futtatókörnyezeten alapul, amely a kód futtatását és kezelését végzi. A .NET fejlesztési környezet használata során a C# az egyik leggyakrabban használt programozási nyelv, amely a C, C++ és Java nyelvek kombinációjaként jött létre.

A C# egy objektumorientált, típusos nyelv, amely a .NET platformon fut. A C# sok olyan jellemzővel rendelkezik, amelyek megkönnyítik a fejlesztők számára az alkalmazások létrehozását és karbantartását, például a garbage collection, az automatikus memóriakezelés és a LINQ (Language Integrated Query) technológia, amely lehetővé teszi az adatlekérdezések integrálását a kódba.

Az ASP.NET Core egy korszerű, teljesítményoptimalizált és keresztplatformos webes keretrendszer, amely lehetővé teszi a fejlesztők számára, hogy webes alkalmazásokat hozzanak létre Windows, macOS és Linux platformokon. Az ASP.NET Core támogatja a RESTful API-k, valamint a MVC és a Razor Pages minták használatát, amelyek segítségével a fejlesztők hatékony és könnyen karbantartható webes alkalmazásokat hozhatnak létre.

Az ADO.NET egy adatelérési keretrendszer, amely lehetővé teszi a fejlesztők számára, hogy adatbázisokhoz csatlakozzanak és adatokat kezeljenek. Az ADO.NET támogatja a SQL Server, az Oracle és más népszerű adatbázis-motorok használatát, és képes kezelni az adatbázis-tranzakciókat és a kapcsolódó hibakezelést.

Az Entity Framework egy objektum-relációs leképező (ORM) keretrendszer, amely lehetővé teszi a fejlesztők számára, hogy adatbázis-struktúrákat és adatelérési logikát hozzanak létre anélkül, hogy közvetlenül SQL kódokat kellene írniuk. Az Entity Framework segítségével a fejlesztők a .NET objektumok és adatbázis-táblák közötti leképezést definiálhatnak, valamint LINQ lekérdezéseket használhatnak az adatok lekérdezésére és módosítására.

2.4.3. Azure

Az Azure az egyik legnépszerűbb felhőszolgáltatási platform, amelyet a Microsoft fejlesztett ki. Az Azure számos szolgáltatást kínál a felhasználóknak, beleértve a számítási erőforrásokat, az adattárolást, az adatbázisokat, az alkalmazások üzemeltetését, az IoT-t, a mesterséges intelligenciát és még sok más.

Az Azure .NET App Service egy olyan felhőszolgáltatás, amely lehetővé teszi a .NET alkalmazások gyors és egyszerű üzemeltetését a felhőben. Az App Service magas rendelkezésre állást, automatikus skálázást, folyamatos integrációt és telepítést biztosít, és támogatja a több verziós alkalmazásokat és azok verziókezelését.

Az App Service lehetővé teszi a felhasználók számára, hogy egyszerűen telepítsék és üzemeltessék az ASP.NET, az ASP.NET Core, a Node.js, a Python, a Java és a PHP alkalmazásokat. Az alkalmazásokat különböző méretű és típusú virtuális gépekbe telepíthetik, amelyek skálázhatóak és dinamikusan alkalmazkodnak a változó forgalomhoz.

Az Azure .NET App Service támogatja a különböző integrációs lehetőségeket, például a Visual Studio Team Services-t, a GitHub-ot és az Azure DevOps-ot, amelyek lehetővé teszik az alkalmazások folyamatos integrációját és telepítését.

Az Azure .NET App Service további előnyei közé tartozik a biztonsági funkciók, mint például a HTTPS támogatása, az SSL tanúsítványok, az Access Control (hitelesítés és engedélyezés) és az Active Directory integrációja. Az App Service továbbá lehetővé teszi a felhasználók számára, hogy egyszerűen használják a felhőben elérhető más Azure szolgáltatásokat, mint például az adattárolást, az adatbázisokat és az IoT-t.

Összességében az Azure .NET App Service egy nagyon hasznos felhőszolgáltatás, amely lehetővé teszi a .NET alkalmazások egyszerű és hatékony üzemeltetését a felhőben. A szolgáltatás számos előnnyel rendelkezik, beleértve a magas rendelkezésre állást, a skálázhatóságot, a folyamatos integrációt és telepítést, valamint a biztonsági funkciókat és az integrációt más Azure szolgáltatásokkal.

2.4.4. Angular

Az Angular egy nyílt forráskódú JavaScript keretrendszer, amelyet a Google fejleszt és karbantart. A keretrendszer célja, hogy megkönnyítse a fejlesztők számára a dinamikus, interaktív webes alkalmazások létrehozását és karbantartását. Az Angular különösen népszerű a Single Page Applications (SPA) terén, ahol az alkalmazások egyetlen HTML-oldalon futnak, és a tartalom dinamikusan frissül a felhasználói interakciók és a navigáció során.

Az Angular négy fő elemből áll:

- **Komponensek:** Az alkalmazás logikájának és a megjelenítendő tartalomnak a felosztása kisebb, újrafelhasználható részekre. A komponensek egy HTML-sablonból és a hozzájuk tartozó TypeScript osztályból állnak.
- **Modulok:** Az Angular alkalmazások komponenseit és szolgáltatásait logikai egységekbe szervezik, amelyeket moduloknak neveznek. A modulok lehetővé teszik az alkalmazás különböző részeinek egyszerűbb karbantartását és tesztelését.
- **Szolgáltatások és injekció:** Az Angular szolgáltatásokat használ a közös logika és funkciók különböző komponensek közötti megosztására. A szolgáltatások egyszerű osztályok, amelyeket a Dependency Injection (függőségi injekció) segítségével juttatnak el a komponensekhez.
- **Kötelező érvényű adatkötés (data-binding):** Az Angular egyik legnagyobb előnye a képessége arra, hogy automatikusan frissítse a nézetet, amikor a modellben változás történik. Ez az adatkötésnek köszönhető, amely kétféle irányú: egyirányú és kétkapcsolatos adatkötés. Az egyirányú adatkötés lehetővé teszi, hogy az adatok a modellből a nézetre frissüljenek, míg a kétkapcsolatos adatkötés mindkét irányban történő frissítést tesz lehetővé.

Az Angular előnyei közé tartozik a gyors fejlesztés, a kiterjedt dokumentáció, a nagy közösség és a könnyű tesztelhetőség. Továbbá az Angular alapvetően komponens-alapú architektúrára épül, ami elősegíti a kód újrafelhasználását és a projektek könnyebb karbantartását.

3. fejezet

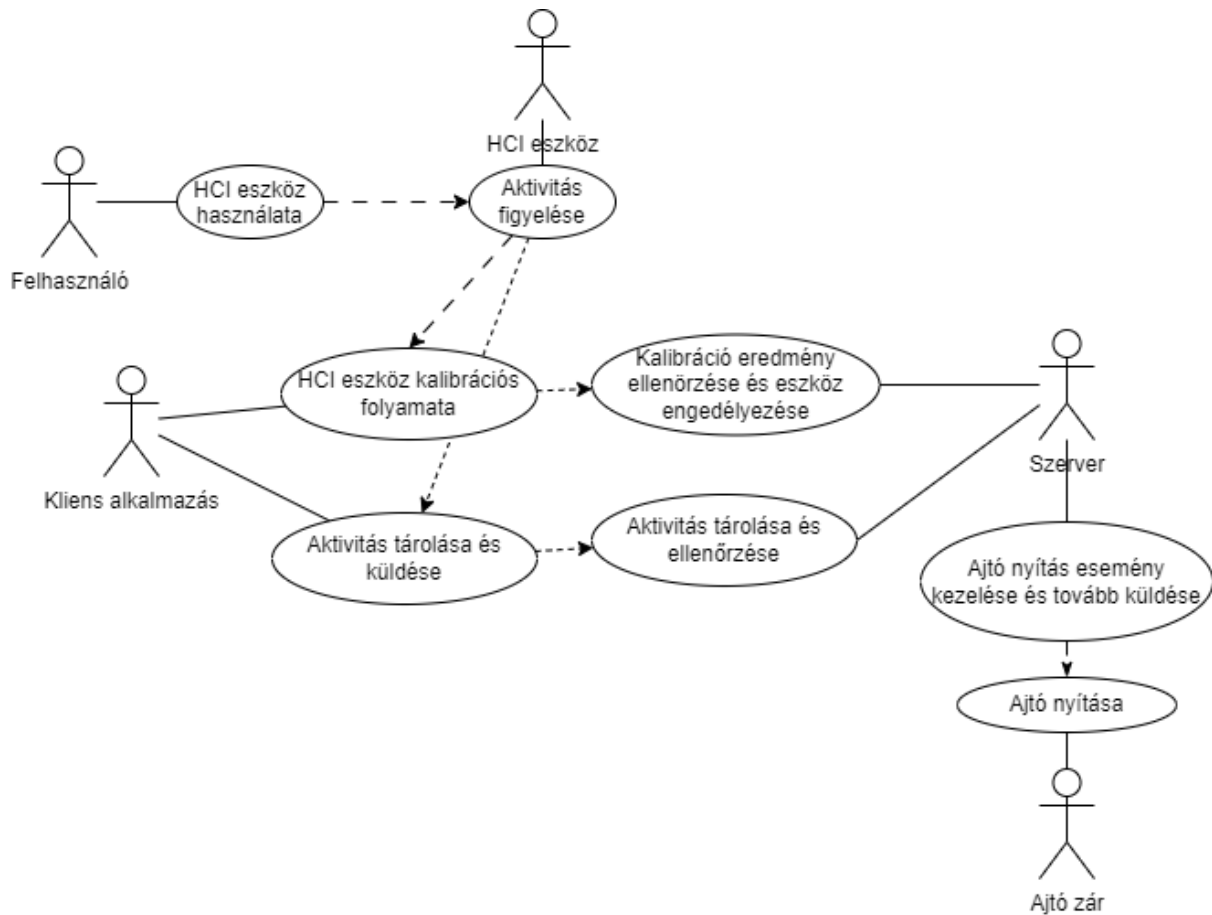
A rendszer specifikációja

A BCI eszköz egy olyan eszköz, amely lehetővé teszi az agyi jelek felismerését és átalakítását olyan vezérlő jelekké, amelyeket a számítógépek vagy más elektronikus eszközök értelmezni tudnak. Ezáltal az emberek közvetlenül tudnak kommunikálni a gépekkel, anélkül hogy hagyományos bemenetet használnának, mint például a billentyűzet vagy az egér. A dolgozatban használt BCI eszköz egy fejre szerelt érzékelőt tartalmaz, amely elektromos jeleket rögzít az agy látókéreg régiójából. Ezeket a jeleket egy „gazda” eszközre továbbítja, ahol egy szoftver elemzi és értelmezi őket. A szoftver képes felismerni, hogy a felhasználó mire néz a virtuális környezetben, és ez alapján vezérelheti az eszközöket.

A NeuroTag minta egy olyan minta, amelyet a virtuális környezetben lévő interaktív objektumokra helyeznek el. A minta villogó fényimpulzusokból áll, amelyek aktiválják a látókéregt. A BCI eszköz képes mérni az impulzusok frekvenciáját és időzítését, és ez alapján következtetni arra, hogy a felhasználó mire néz. Ez az információ lehetővé teszi az eszköz számára, hogy értelmezze és egy személyre szabott eseményt indítson el. A NeuroTag minta előnye, hogy nem igényel erős vagy zavaró villogó fényt, és nem függ a felhasználó szemmozgásától vagy pillantásától.

A kill switch mechanizmus egy olyan mechanizmus, amely automatikusan visszavonja a jogosultságokat és kijelentkezteti a felhasználót, ha az ember-gép kapcsolat megszűnik. Ez azt jelenti, hogy ha a felhasználó leveszi a BCI eszközt a fejéről, vagy elveszíti a kapcsolatot a mobil eszközzel, akkor a rendszer nem engedi tovább használni az eszközöket. Ez növeli a biztonságot és megakadályozza az illetéktelen hozzáférést.

3.1. Felhasználói követelmények



3.1. ábra. Use Case diagram

A 3.1. ábrán program egy többszereplős rendszert foglal magában, beleértve egy felhasználót, egy HCI eszközt, egy kliens alkalmazást, egy szervert és egy ajtó zárat. Ezek a szereplők különböző használati esetek végrehajtása érdekében működnek együtt, és kölcsönhatásaikat a köztük lévő kapcsolatok határozzák meg. A program áramlását az alábbiakban ismertetem:

A Felhasználó kezdeményezi a HCI eszköz használatát, amely lehetővé teszi számára a rendszerrel való interakciót.

A HCI eszköz részt vesz az aktivitás felügyeletében. A HCI eszköz nyomon követi a felhasználó tevékenységét, és rögzíti a vonatkozó információkat.

A HCI eszköz kalibrációs folyamaton megy keresztül, amelyet a kliens alkalmazás irányít. A kalibráció biztosítja az eszköz helyes és optimális működését.

Az kliens alkalmazás kommunikál a szerverrel, hogy ellenőrizze és engedélyezze a kalibrált HCI eszköz működését a rendszerben.

Ahogy a felhasználó interakcióba lép a HCI eszközzel, az eszköz továbbítja ezeket a tevékenységeket, és elküldi az adatokat a kliens alkalmazásnak.

Az kliens alkalmazás felelős a tárolási tevékenység kezeléséért és az adatok további feldolgozásra történő elküldéséért a szervernek.

A szerver ellenőrzi a tárolt tevékenységeket, és biztosítja, hogy azok érvényesek és követik a rendszer szabályait.

Ha a szerver megállapítja, hogy az ajtónyitási tevékenység iránti kérelem érvényes és a HCI eszköz még engedélyezett, akkor elküldi a kérelmet az ajtó zárnak.

Az ajtó zár megkapja a kérést a szervertől, és végrehajtja az ajtónyitás használati esetet, lehetővé téve a felhasználó számára a kívánt területre való belépést.

Összefoglalva, a program áramlásában több szereplő dolgozik együtt a Felhasználó és a HCI eszköz közötti interakciók kezelése és feldolgozása, az eszköz kalibrálása, a tevékenységi adatok tárolása és hitelesítése, és végül az ajtó záron keresztül a biztonságos területre való belépés szabályozása érdekében.

3.2. Rendszerkövetelmények

a) Funkcionális követelmények

A dolgozatban bemutatásra kerülő rendszer egy olyan jelszómentes biztonságos beléptetési és felhasználói hitelesítési megoldás, amely egy ember-gép interfész (BCI) eszközön alapul. A rendszerben az ember-gép interfész egy átruházhatatlan hitelesítési tokenként szolgál, amely egy biometrikus folyamatot monitorizál. Ha a kapcsolat megszűnik, a rendszer automatikusan visszavonja a jogosultságokat és kijelentkezteti a felhasználót. A rendszer két megvalósítást is javasol: egy látókéreg aktivitását monitorizáló és egy pulzusfigyelésen alapuló rendszert. A dolgozatban a rendszer megbízhatóságát és biztonságát is tesztelték különböző feltételek mellett.

b) Nem funkcionális követelmények, megszorítások.

- Kliens alkalmazás tárhelye, 120 Mb
- Szerver alkalmazás tárhelye, 100 Mb (.NET runtime libraryt nem foglalja magában)
- Zár alkalmazás tárhelye, 3 Mb Ezek a tárhely követelmények nem tartalmazzák a forrás állományokat.

A projektben megvalósított operációs rendszer követelményen:

- A kliens alkalmazás csupán Windows platformon működik.
- A megvalósított rendszer többi alkalmazása multiplatform.

Az alkalmazás nem gyűjt adatot direkt módon a felhasználóról, csupán az aktivitásokat tárolja egy sesszió azonosítóhoz kötve.

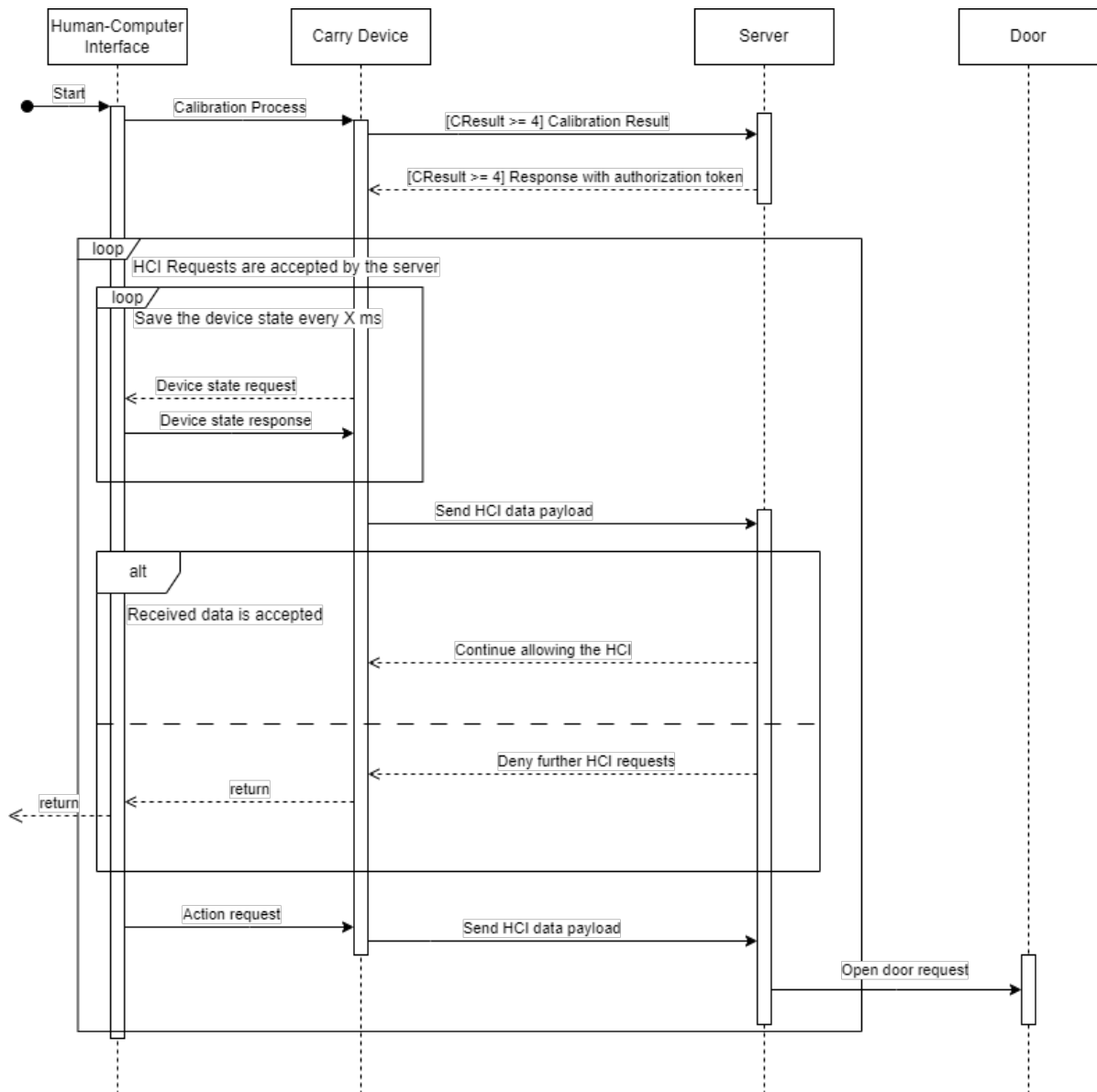
3.3. Példa

Az alábbi kép (3.2. ábra) a szoftver működésének absztrakt ábrázolását mutatja be, melyből kimaradnak bizonyos részletek. A diagram nem tartalmazza a titkosítási folyamatokat, az adatcsomagok ellenőrzését, valamint a folyamatos felügyeletet. A dolgozatban azonban ezek a részletek is tárgyalásra kerülnek. A diagram célja, hogy a főbb összetevők és műveletek kapcsolatát bemutassa, és a megértést elősegítse.

A kutatás során először is az ember-gép között, pontosan monitorizálható kapcsolatok lehetőségeit vizsgáltuk meg.

A kutatásban különös figyelmet kellett fordítani a biztonsági szempontokra, amelyek magukban foglalják a hackelés, spoofolás [HEMF15], becsapás stb., összességében az illetéktelen hozzáférés elleni védelmet [BG16]. A rendszer fejlesztése során a megfelelő kriptográfiai megoldásokat kellett alkalmazni az identifikációs adatok védelme érdekében.

Az utolsó lépés a rendszer teljes tesztelése, melynek célja felmérni, hogy az mennyire megbízható és biztonságos. A tesztelés során a rendszert különböző feltételek között kellett tesztelni, például szimulált támadások vagy belső és külső környezeti tényezők hatása alatt.



3.2. ábra. UML diagram

3.3.1. Ember-gép közötti monitorizálható kapcsolatok lehetőségei

Az ember-gép interfészek terén a kutatások és fejlesztések folyamatosan haladnak és az agy-számítógép interfész (BCI) egyike azon technológiáknak, amelyeket a kapcsolat javítására fejlesztenek. A BCI lehetővé teszi az agyi jelzések felismerését és azok átalakítását olyan vezérlő jelekké, amelyeket a számítógépek vagy más elektronikus eszközök értelmezni tudnak. Ezáltal az emberek közvetlenül tudnak kommunikálni a gépekkel, anélkül hogy hagyományos bemenetet használnának, mint például a billentyűzet vagy az egér. A BCI-t már alkalmazzák a rehabilitáció, a virtuális valóság, a játék és a protézisvezérlés területén.

A dolgozat keretén belül is egy BCI volt használva, ami nem más mint a NextMind által készített eszköz. Ez a BCI látókéreg aktivitás monitorizálja és képes felvenni az agyi aktivitást, amely segíthet a felhasználónak a gépi eszközökkel való kommunikációban.



3.3. ábra. NextMind headset elektródjai

Az eszköz 9 elektróddal rendelkezik (3.3. ábra), amelyeket a látókéreg régiója körül kerül elhelyezésre. A látókéreg felelős a vizuális információk feldolgozásáért. Ha egy személy valamire néz, akkor a látókéreg aktiválódik. Azonban, a generált jelek értelmezése, vagyis azok általános objektumokká való visszafejtése, külső segítség nélkül rendkívül nehéz, mivel a külsőleg érzékelt jel erősségét és forrását nem lehet 100%-osan helyreállítani. A NextMind csapata úgy döntött, hogy a probléma megoldása érdekében egy villogó mintát alkalmaz, úgynevezett NeuroTag-et. Minden villanás, minden villogó fényimpulzus aktiválja a látókéreget, és az eszközben mért impulzus frekvenciája alapján a rendszer következtet arra, hogy a felhasználó éppen mire néz. Ez az információ lehetővé teszi az eszköz számára, hogy értelmezze és visszaállítsa az általunk vizsgált tárgyakat.

A virtuális környezetben minden interaktív objektumra el tudjuk helyezni ezt a villogó mintát. A NextMind álltat kiadott SDK-val meg ezek a minták összhangban időzítve váltsák egymást. Két villanás közötti időkülönbséggel megtudja mondani nekünk, hogy melyik objektummal kívánunk mi interakciót végezni.

Emellett a villogó fénynek egyáltalán nem kell erősnek lennie. Mivel ezeknek a feldolgozása időigényes a válaszütem akár 2-3 másodperc is lehet, ami elég sok, így sok helyen alkalmatlannak bizonyult ez a eszköz. Az 3.5 ábrán látható felső számozás megmutatja



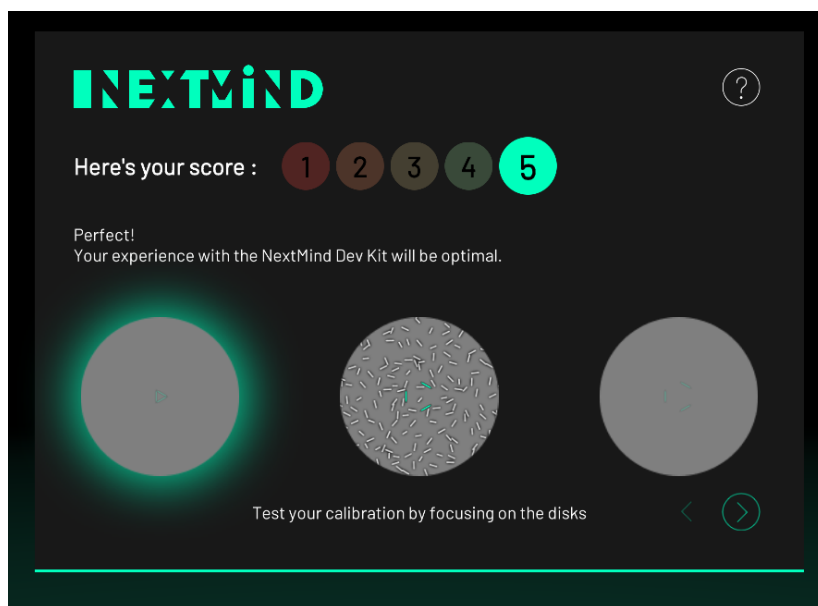
3.4. ábra. NextMind headset elhelyezve a látókéregen. (Kép forrása: [Cao20])

nekünk a véghez vitt kalibrációs értéket, minél nagyobb annál jobb. Az alatta lévő első kör balról jobbra nézve, egy aktivált objektum a vizuális válasza (feedback), a második kör egy villanásban lévő objektum míg az utolsó kör egy jelenleg passzív módban álló objektum.

Az ilyen technológiák azonban további kutatásra szorulnak, mivel a látókéreg aktivitás monitorizálása összetett folyamat, és a különböző emberek agyi aktivitása eltérő lehet.

Összességében azonban az ilyen technológiák nagy potenciállal rendelkeznek az ember-gép interfész terén, és lehetővé tehetik a felhasználók számára, hogy hatékonyabban és kényelmesebben kommunikáljanak a gépekkel. Azonban a biztonsági kockázatok és az egyéni különbségek miatt további kutatásokra és fejlesztésekre van szükség ahhoz, hogy ezek az eszközök széles körben elterjedjenek és biztonságosan használhatóak legyenek. Az egyik ilyen kutatás ami az BCI eszközök kommunikációs biztonságos protokolját figyelembe veszi nem más mint „Enhancing the Security & Privacy of Wearable Brain-Computer Interfaces” [TQB22] ahol több mint 300 sebezhetőséges fedeztek fel ezeknél. A BCI kommunikációs rétege fontos titkosítani különben kívülről bárki felhasználhatja az adatokat. A NextMind titkosítja a bluetooth álltal közvetített adatait.

A BCI technológiák mellett más ember-gép közötti monitorizálható kapcsolatok lehetőségai is felmerülnek, amelyek szintén elősegíthetik az emberek és a gépek közötti kommunikációt. Az egyik ilyen ötlet az impulzusmérő telefon kamera alkalmazása. Az impulzusmérő telefon kamera lehetővé teszi, hogy a felhasználók okostelefonjuk kameráját használva mérjék és monitorozzák pulzusukat, ami egy újabb kapcsolati lehetőség a felhasználó és a gép között.



3.5. ábra. NextMind headset kalibrációs eredménye, példa villogó objektumra

Kommunikációs csatornák és titkosítása

A beléptető rendszeren a megvalósított eszközök és softwareken a kommunikációs folyamat több titkosítási rétegen megy keresztül, hogy biztosítsa a maximális biztonságot.

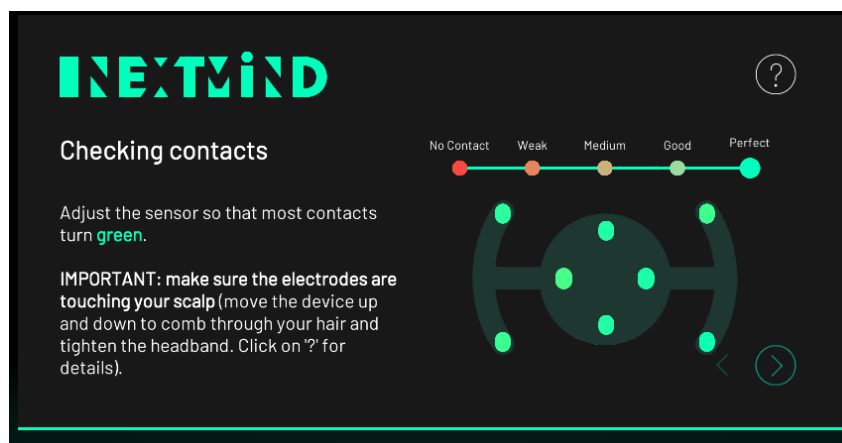
A NextMind eszköz a számítógéppel Bluetooth csatornán keresztül kommunikál, és az átvitt adatokat a küldő eszköz titkosítja.

Az első titkosítási réteg a kommunikációs protokoll, amely a HTTPS-en alapul. A legelterjedtebb HTTPS használat a böngészőkben tekinthető meg. Az HTTPS működéséhez szükséges az SSL/TLS tanúsítványok használata. Az SSL/TLS tanúsítványok digitális tanúsítványok, amelyek azonosítják a weboldal tulajdonosát és a weboldal biztonságát biztosítják.

A tanúsítványokat általában a weboldal tulajdonosai igénylik és regisztrálják az egyik tanúsítvány kiadó (CA, Certification Authority) által, amelyek olyan megbízható harmadik felek, amelyek hitelesítik a weboldal tulajdonosát és igazolják a biztonsági protokoll betartását. A tanúsítványokat azután telepítik a weboldal szerverére, és azokat a látogatók böngészője automatikusan ellenőrzi azzal, hogy ellenőrzi a weboldal azonosságát, amikor az HTTPS-t használó weboldalra navigálnak.

A tanúsítványok tartalmazzák a következő információkat:

- A tanúsítvány kibocsátójának neve és információi.
- A weboldal tulajdonosának neve és információi.
- A tanúsítvány érvényességi ideje.
- A tanúsítvány digitális aláírása, amely garantálja, hogy az adatok hitelesek és biztonságosak.



3.6. ábra. NextMind headset elektrodák elhelyezkedési erősségük

Amikor egy felhasználó az HTTPS-t használó weboldalra navigál, a böngészője ellenőrzi a weboldal tanúsítványát a szerverrel való kapcsolat felépítése előtt. Ha a tanúsítvány érvényes és megbízható tanúsítvány kiadótól származik, a böngésző biztonságos kapcsolatot épít ki a weboldallal, és elkezd a titkosított kommunikációt.

Az SSL/TLS titkosítás és az HTTPS protokoll használata ajánlott az API (Application Programming Interface) végpontoknál (endpoints) is, mivel az API-k is titkosított kapcsolaton keresztül kommunikálnak az alkalmazások között. Az SSL/TLS titkosítás és az HTTPS protokoll használata biztosítja, hogy az adatok biztonságosan áramoljanak az alkalmazások között, és megakadályozza az illetéktelenek hozzáférését vagy a kommunikáció manipulálását.

Az API-k használata során a kliens oldal és a szerver oldal közötti kommunikáció titkosított kapcsolaton keresztül történik. Az API-k általában token vagy kulcs alapú hitelesítést használnak az ügyfél azonosítására és az illetéktelen hozzáférés megakadályozására. Az SSL/TLS tanúsítványok használata hozzájárul a biztonságos kommunikációhoz, mivel biztosítják, hogy a két fél közötti kapcsolat valódi és megbízható legyen.

Az API endpointok esetében az SSL/TLS tanúsítványokat a szerver oldalon telepítik, hogy biztosítsák a kommunikáció biztonságát az ügyfelek és a szerverek között. Az ügyfeleknek azonban szükségük lehet az SSL/TLS tanúsítványok érvényességének ellenőrzésére a kliens oldalon, hogy megakadályozzák az adathalász támadásokat és a biztonsági incidenseket.

Erre épült még egy One Time Pad (OTP) nevű titkosítási módszer, amely minden egyes kérés esetén használható egyszeri kulcsokat alkalmaz. Az OTP két fő feltétele az, hogy a kulcs hossza azonos legyen a tartalom hosszával, és a kulcsot titkosításra csak egyszer használjuk.

A megvalósítás során a Diffie-Hellman kulcscsere algoritmust alkalmazzák. Ha a kulcs mérete kisebb lenne, mint a küldeni kívánt adatsomag mérete, akkor egy kulcsderiválási funkció segítségével olyan derivált kulcsot hoznak létre, amely megegyezik a küldésre kívánt adatsomag hosszával. A kulcsderiválási funkció két paramétert használ: a seed-et és a kívánt hosszt. A seed a megosztott Diffie-Hellman kulcs lesz. Fontos megjegyezni, hogy azonos bemenetekre azonos eredményt ad a kulcsderiválási funkció.

Miután előállították a derivált kulcsot, azt az OTP módszerrel titkosítják az üzenetet. A szerveren ugyanez a folyamat zajlik visszafejtés során: a csomag hosszát megkapják, és a kulcs már rendelkezésre áll. A kulcsderiválással megkapják a kulcsot, amellyel visszaállíthatják a One Time Pad titkosítást. Ezt követően a szerver elkezd az érkező adatok ellenőrzését.

A JWT (JSON Web Token) használata további előnyöket és biztonsági réteget jelenthet a kommunikációs rendszerben. A JWT előnyei között szerepelnek az alábbiak:

Hitelesítés: A JWT használható a felhasználók hitelesítésére, vagyis annak ellenőrzésére, hogy a felhasználó jogosult-e hozzáférni az adott erőforráshoz vagy szolgáltatáshoz. A JWT a hitelesítési adatokat tartalmazza, így a szervernek nem kell minden egyes kérésnél ismételten ellenőriznie a felhasználói adatokat.

Hatékony: A JWT állapotmentes, vagyis a szervernek nem kell állapotot tárolnia a kliens oldalról, ami csökkenti a szerver oldali terhelést és egyszerűsíti a rendszert. A JWT-ben tárolt információk aláírás és/vagy titkosítás által védettek, így a szerver biztos lehet benne, hogy az adatok nem módosultak a tranzakció során.

Egyszerű: A JWT egyszerű és könnyen érthető formátumot használ (JSON), amely számos nyelven és platformon támogatott. Ennek köszönhetően a JWT-k könnyen integrálhatók a különböző rendszerekbe és alkalmazásokba.

Rugalmas: A JWT lehetővé teszi a felhasználói adatok és egyéb állítások (claims) tárolását a tokenben, ami rugalmasságot biztosít a rendszerben. A JWT-ben tárolható információkat a fejlesztők testreszabhatják az alkalmazás igényeinek megfelelően.

A JWT használata a már említett titkosítási rétegekkel együtt (HTTPS, OTP) egy erőteljes és biztonságos megoldást kínál a kommunikációs rendszerben. A JWT segítségével megakadályozhatók az illetéktelen hozzáférési kísérletek, miközben biztosítja az eszköz adatok védelmét és a hitelesítés hatékonyságát.

A weboldalakon tárolt „ajtók” csak engedélyezett domain nevektől érhetők el a tűzfal beállítások miatt. Ezáltal biztosítják, hogy a kommunikáció külső szempontból teljesen el legyen zárva. Így a NextMind eszköz és a számítógép közötti kommunikáció magas szintű biztonságot és adatvédelmet nyújt, míg a rendszer zárt marad a nem kívánt behatolásokkal szemben.

3.3.2. Optimális virtuális környezet előállítása

Az optimális virtuális környezet előállítása során a cél egy olyan környezet kialakítása, amely lehetővé teszi a felhasználók számára a rendszer hatékony és kényelmes használatát. Ennek érdekében több szempontot is figyelembe kell venni, mint például:

A lehető leggyorsabb választ megkapni a NextMind headsettől anélkül, hogy nagyban eltérjem a pontosságot. Számos kísérleti beállításokon mentem végig a dolgozat során, ezekhez tartoznak például a VSync bekapcsolása, felső FPS limit a renderre és sok apró finomítás amelynek összességében sikerült egy olyan konfigurációt elő állítani amiben az elvesztett pontosítás hanyagolhatóvá válik, ennek előnyére relatív gyors válasz időt sikerült előhozni, a válasz időt sikerült akár 1 másodperc alá csökkenteni.

A virtuális környezet ergonómiája: A környezet kialakítása során figyelembe kell venni a felhasználók kényelmét és a munkavégzés hatékonyságát. Ennek érdekében az interaktív elemek elhelyezése, a szövegek és a gombok mérete, valamint a felhasználói felület átláthatósága és könnyen érthetősége fontos szempontok.

A virtuális környezet teljesítménye: Az optimális teljesítmény érdekében a környezetben használt grafikai elemek és számítási igényű folyamatok optimalizálása szükséges, hogy a rendszer zökkenőmentesen működjön a felhasználó számára.

A virtuális környezet adaptálhatósága: A környezetnek képesnek kell lennie alkalmazkodni a különböző felhasználói igényekhez és eszközökhöz, amelyekkel a felhasználók hozzáférhetnek a rendszerhez. Ez magában foglalja a különböző képernyőméretek, operációs rendszerek és böngészők támogatását, valamint az esetleges akadálymentesítési igényeket.

A virtuális környezet biztonsága: Az optimális környezetnek biztonságosnak kell lennie a felhasználók számára, amely magában foglalja a rendszerbe való illetéktelen hozzáférés elleni védelmet, a személyes adatok védelmét és a rendszerben végrehajtott műveletek megbízhatóságát.

Az optimális virtuális környezet előállítása során a fenti szempontok figyelembe vételével lett megtervezve és fejlesztve a rendszer, hogy a felhasználók számára biztosított legyen a kényelmes és hatékony használat.

3.4. Helymeghatározás

A helymeghatározás a felhasználók aktuális földrajzi helyzetének meghatározása, amelyet több technológia segítségével lehet elérni. A helymeghatározás hasznos lehet a személyre szabott szolgáltatások nyújtásához, a navigációs alkalmazások működtetéséhez, valamint a biztonsági és vészhelyzeti esetek kezeléséhez.

Ebben az esetben fontos a helyet meghatározni, ugyanis a hozzánk legközelebbi „ajtó” lesz megnyitva.

A helymeghatározás megvalósítására több technológia létezik, mint például:

GPS: A globális helymeghatározó rendszer (GPS) műholdas technológiát használ a felhasználók pontos helyének meghatározásához. A GPS általában nagy pontossággal képes meghatározni a helyet, de a jel vételére negatív hatással lehetnek az épületek és a természetes akadályok.

Mivel ez egy kültérre alkalmas technológia és a dolgozat benti, titkos/magas biztonsággal rendelkező események kezelésére szolgáltat nem lesz használva GPS.

Ultra Wideband (UWB) technológia: Az UWB egy rádiófrekvenciás technológia, amely nagy sáv szélességű jeleket használ a felhasználók helyének nagy pontosságú meghatározásához. Az UWB előnye a nagy pontosság és a gyors reakcióidő, de hátránya, hogy korlátozott hatótávolsággal rendelkezik, és drágább, mint a többi helymeghatározási technológia.

Mivel a NextMind kiadói korlátozták a platformokat, illetve költséghatékonyságra is gondoltunk, ez nem alkalmazható.

Wi-Fi és mobilhálózatok: A felhasználók helyének meghatározására szolgáló technológiák, amelyek a közeli Wi-Fi hálózatok vagy mobilhálózati adótorony adatait használják. Ezek a módszerek általában kevésbé pontosak, mint a GPS, de előnyeik közé tartozik, hogy beltéri helyszíneken is működnek, ahol a GPS jel gyenge vagy nem érhető el.

Bluetooth alapú helymeghatározás: A Bluetooth alapú helymeghatározás olyan technológia, amely a közeli Bluetooth eszközök jelerősségét használja a felhasználók helyének meghatározásához. Ez a módszer általában kisebb pontossággal rendelkezik, mint a GPS, de előnye, hogy alacsony energiafogyasztású és beltéri helyszíneken is használható.

Amit a dolgozatban használunk az nem más mint a Wi-fi, mobilhálózatok és bluetooth alapú helymeghatározás kombinációja. Ahol egy mesterséges intelligencia dönti el, hogy hol vagyunk. A helyeket előre kell „felfedezzük” és elmondjuk az alkalmazásnak, hogy jelenleg hol is tartozkodunk, majd gépi tanulás segítségével az alkalmazás képes lesz megtanulni a jelenlegi helyzetünket a körülvevő jel erősségekre alapozva.

3.5. Dead Man Switch szerepe

A Dead Man Switch (DMS) egy biztonsági mechanizmus, amelyet arra terveztek, hogy aktiválódjon vagy deaktiválódjon, ha a felhasználó nem képes elvégezni egy előre meghatározott cselekvést egy adott időkeretben. A DMS használatának célja a felhasználók védelme és a rendszerek biztonságának fenntartása olyan esetekben, amikor a felhasználó elveszíti az ellenőrzést a rendszer felett, vagy olyan helyzetekben, amikor a felhasználó nem tudja biztonságban tartani a rendszert.

A DMS számos alkalmazása lehet, például:

Vészhelyzetek: A DMS használható vészhelyzetekben, amikor a felhasználó elveszíti az eszméletét, és a rendszernek automatikusan le kell állnia, vagy segélyhívást kell indítania.

Biztonsági alkalmazások: A DMS alkalmazható olyan biztonsági rendszerekben, amelyek védelmet nyújtanak a hackerek, a vírusok és más illetéktelen hozzáférések ellen. Ha a felhasználó nem tudja időben végrehajtani a szükséges cselekvéseket, a DMS aktiválódik, és leállítja a rendszert vagy visszaállítja a biztonsági beállításokat.

Adatvédelem: A DMS használható a felhasználók személyes adatainak védelmében. Például, ha a felhasználó elveszíti a mobiltelefonját, a DMS aktiválódhat, és távolról törölheti az összes érzékeny adatot a készülékről, megakadályozva az adatok illetéktelen hozzáférését.

Ipari és közlekedési alkalmazások: A DMS használható ipari és közlekedési rendszerekben, ahol a gépek és járművek biztonságos működését kell garantálni. Ha a felhasználó vagy működtető nem képes időben elvégezni a szükséges cselekvéseket, a DMS aktiválódhat, és leállíthatja a gépet vagy járművet, megelőzve a baleseteket és a károkat.

A DMS hatékonyan segíthet a biztonsági és adatvédelmi kockázatok minimalizálásában, és garantálhatja a felhasználók és rendszerek védelmét. A DMS beépítése a rendszerekbe lehetővé teszi, hogy a felhasználók biztonságban érezzék magukat, és csökkenti a biztonsági incidensek és adatvesztés esélyét.

A dolgozatban a BCI-ra kialakított DMS rendszer nagyon fontos szerepet tölt be, ugyanis a szerver állandóan figyeli az eszközök hordozóit és ha anomália lépne fel, akkor a rendszer kizárja az illetőt egy riasztót indítva.

3.5.1. Kill switch design pattern

A kill switch design pattern egy olyan biztonsági mechanizmus leírása, amely a BCI eszközök működését szabályozza, és megakadályozza az illetéktelen hozzáférést és az adatokkal kapcsolatos visszaéléseket. Ebben a mintában az alábbi funkciókat és elveket alkalmazták:

Kalibráció ellenőrzése: A BCI eszközök pontos működésének alapja a megfelelő kalibráció (3.6. ábra). A kill switch rendszer gondoskodik arról, hogy az eszköz csak akkor

kapcsolódhasson a szerverhez és működhessen, ha a kalibrációs folyamat sikeresen befejeződött. Ezzel garantálva, hogy a felhasználó agyi aktivitását megfelelően rögzíti és értelmezi az eszköz. Ha a kalibráció sikertelen, a rendszer nem engedi tovább az eszközt, és a felhasználót értesíti a problémáról. Új kalibráció szükséges ilyenkor.

Folyamatos kommunikáció és adatellenőrzés: A BCI eszközök és a szerver közötti kommunikáció zavartalan működése elengedhetetlen a biztonságos és hatékony használat érdekében. A kill switch rendszer folyamatosan figyelemmel kíséri az adatátvitelt és ellenőrzi, hogy az megegyezik-e a várt értékekkel. Ha az adatátvitel megszakad, eltér a korábbiaktól, vagy a kommunikáció külső beavatkozást észlel, a rendszer azonnal leállítja az eszközt és aktiválja a riasztást.

Időzített ellenőrzés: A rendszer időközönként ellenőrzi a BCI eszköz állapotát és a kommunikációt a szerverrel, hogy biztosítsa a folyamatos és biztonságos működést. Az időzített ellenőrzés lehetővé teszi, hogy a rendszer rendszeresen felmérje a BCI eszköz teljesítményét és kommunikációját a szerverrel, így időben észlelheti a potenciális problémákat vagy biztonsági réseket. Ha a rendszer valamilyen problémát észlel, azonnal aktiválja a kill switchet és letiltja az eszközt.

Adatbiztonság és -integritás: A kill switch design pattern olyan technikákat alkalmaz, amelyek biztosítják az adatbiztonságot és -integritást. A rendszer különböző algoritmusokat és titkosítási technikákat használ, (3.1 fejezet) hogy megvédje az adatokat az illetéktelen hozzáféréstől és manipulációtól. Ezen felül a rendszer gondoskodik arról, hogy csak hitelesített és megbízható forrásból származó adatokat kezeljen. A rendszer továbbá rendszeresen ellenőrzi az adatok integritását, és amennyiben eltérést észlel, azonnal aktiválja a kill switchet, letiltja az eszközt és riasztást küld.

Visszaállítás: A BCI eszközök biztonságának és hatékonyságának megőrzése érdekében a kill switch rendszer visszaállítható a biztonságos állapotba, miután a problémát megoldották és az adott feltételek teljesülnek (pl. sikeres újra-kalibráció, személyes ellenőrzés maga biztonsági egységeinél). Ez a funkció lehetővé teszi a felhasználók számára, hogy gyorsan és egyszerűen folytathassák az eszköz használatát, minimalizálva a leállás időtartamát.

Proaktív riasztás és monitorozás: A kill switch rendszer proaktív módon figyeli a BCI eszközök működését és kommunikációját a szerverrel, és a rendszerben előre meghatározott feltételek alapján riasztásokat küld a felhasználóknak és a rendszergazdáknak. Ezzel a funkcióval a rendszer lehetővé teszi a gyors és hatékony reagálást a potenciális problémákra vagy biztonsági incidensekre.

Ezen funkciók és elvek kombinációja biztosítja, hogy a BCI eszköz csak akkor működjön, ha a kommunikáció a szerverrel zavartalan és a kalibráció megfelelő. Ha bármelyik feltétel nem teljesül, a kill switch azonnal letiltja az eszközt és aktiválja a riasztást, megakadályozva ezzel az illetéktelen hozzáférést és az adatokkal kapcsolatos visszaéléseket. Az ilyen kill switch design hozzájárul a BCI eszközök biztonságának növeléséhez, a felhasználói bizalom erősítéséhez és a BCI technológiák szélesebb körű alkalmazásának elősegítéséhez.

3.6. Jelszómentes beléptetés

A jelszómentes beléptetés [HH20] lehetővé teszi a felhasználók számára, hogy azonosítsák magukat és hozzáférjenek a rendszerhez jelszó használata nélkül. Ennek előnye

közé tartozik a felhasználói kényelem, a jelszólopás elleni védelem és a jelszókezelés költségeinek csökkentése.

A jelszómentes beléptetés megvalósítása több módon is lehetséges, például:

Biometrikus azonosítás: A felhasználók ujjlenyomat-, arcfelismerés- vagy írisz-felismerés-alapú azonosítása.

Egyszer használatos kódok: A rendszer által generált egyszer használatos kódok, amelyeket a felhasználók megkapnak, és beírva azonosíthatják magukat. Ezek a kódok általában e-mailben vagy SMS-ben érkeznek a felhasználóhoz.

Hardveres kulcsok: A felhasználók egy fizikai eszközt használnak az azonosításhoz, például egy USB-kulcsot vagy egy okostelefont, amely egy előre meghatározott biztonsági kódot tartalmaz.

Azonosítás több tényezővel: A jelszómentes beléptetés biztonságának növelése érdekében a felhasználók több tényezőt használhatnak az azonosításhoz, például a biometrikus adatokat és a hardveres kulcsokat kombinálva.

A jelszómentes beléptetés megvalósítása során fontos figyelembe venni a felhasználói kényelmet és a biztonsági szempontokat. Az alkalmazott megoldásnak biztosítania kell az illetéktelen hozzáférés elleni védelmet, miközben lehetővé teszi a felhasználók számára a gyors és egyszerű azonosítást.

A dolgozatban az eszköz maga szolgál tokenként, mivel egy BCI-ről van szó és a hardware-ben egyedi azonosítási széria szám van vésve, képesek vagyunk azokat használni mint belépési adat. Míg az elején inaktív az eszköznek a belépéshez hozzáférhető joga, ez megváltozhat a felügyelt kalibráció után. Minden használat előtt véghez kell vinni a kalibrációs folyamatot, mivel a szerver csakis ezután ismeri el az eszközt. Ezek után a BCI eszköznek továbbra is fent kell tartania a kapcsolatot a szerverrel, rendszerezett adat küldéssel. Fontos, hogy az eszköz a kalibráció utáni válasz alapján tárolja és továbbítsa az adatokat a szervernek, különben tiltásra kerül az eszköz aktiválva a DMS folyamatot. Ha az eszköz nem válaszol, megszakad a kapcsolat a látókéreggel vagy egy kicsit is eltérően küldi el az adatokat a szervernek akkor a szerver képtelen lesz az eszközt kitiltani és bekapcsolni a riasztást.

3.7. NextMind előnyei és hátrányok

A NextMind eszköz egy agy-számítógép interfész (BCI), amely a látókéreg aktivitásának monitorizálására használható. Annak ellenére, hogy a NextMind BCI úttörő technológia és számos előnnyel rendelkezik, vannak hátrányai is.

Előnyök

- Non-invazív: A NextMind eszköz egy non-invazív BCI, ami azt jelenti, hogy nem igényel sebészeti beavatkozást a használatához. Ez csökkenti a kockázatokat és lehetővé teszi a felhasználók számára, hogy könnyebben hozzáférjenek és használják az eszközt.
- Könnyű használat: A NextMind eszköz könnyen használható, és a felhasználók számára gyorsan megtanulható. Ez elősegíti a BCI technológiák elterjedését és alkalmazását.

- Széleskörű alkalmazási lehetőségek: A NextMind eszköz számos területen alkalmazható, mint például a rehabilitáció, a virtuális valóság és a protézisvezérlés. Ez lehetővé teszi a felhasználók számára, hogy széles körben alkalmazzák a BCI technológiát a mindennapi életben és a munkában.
- A biztonságos kommunikáció elérése érdekében a NextMind eszköz kiválóan alkalmazkodik a modern technológiákhoz és lehetővé teszi az alapvetően titkosított kommunikációt a párosított eszközzel. A kapcsolat létrehozása és fenntartása a bluetooth csatornán keresztül történik, így biztosítva a felhasználók és az eszközök közötti adatátvitel megbízhatóságát és biztonságát. Ezzel a megoldással a NextMind eszköz elősegíti a magas szintű adatvédelmet, miközben az eszközöket összekapcsoló hálózati kommunikáció minden szempontból hatékony és megbízható marad.

Hátrányok

- Válaszidő: A NextMind eszköz válaszüzeje jelenleg 2-3 másodperc, ami elég hosszú időtartamnak tekinthető. Ez a lassú válaszüze korlátozhatja a BCI technológia alkalmazását olyan területeken, ahol gyors válaszüze van szükség.
- Egyéni különbségek: A NextMind eszköz használata során a különböző emberek agyi aktivitása eltérő lehet, ami befolyásolhatja az eszköz hatékonyságát. Emiatt további kutatásra és fejlesztésre van szükség, hogy a BCI technológiák jobban alkalmazkodhassanak az egyéni különbségekhez.
- A platformfüggőség kihívást jelent ebben az esetben: a jelenlegi kutatás során az adott eszközt kezelő szoftverek kizárólag a Windows operációs rendszerrel működnek összhangban. Ez jelentősen korlátozza a hordozható eszközök és más népszerű operációs rendszerek, mint például az Android vagy az iOS használatát. Ezáltal szükségessé válik a kompatibilitás bővítése, hogy a felhasználók szélesebb körben élvezhessék az alkalmazások előnyeit és a különböző platformokon való integrációt.

3.8. Impulzust mérő telefonkamera

Az impulzust mérő telefonkamera egy olyan technológia, amely lehetővé teszi a felhasználók számára, hogy az okostelefonjuk kamerájával mérik a pulzusukat. Ez a módszer számos előnnyel jár, mint például a hordozhatóság, a könnyű hozzáférés és a nem invazív jelleg. A kamera segítségével a felhasználók gyorsan és egyszerűen ellenőrizhetik az egészségüket és a testmozgás hatékonyságát.

Az impulzust mérő telefonkamera működése a fényvisszaverődésen alapul, amelyet a bőrön áthaladó vér okoz. Amikor a telefon kamerája a bőrre irányul, a fényvisszaverődést a véráramlás változásai befolyásolják, és ezeket a változásokat a kamera rögzíti. A kamera képei alapján a telefon speciális algoritmusokat alkalmaz a pulzusszám meghatározására.

Előnyök

- Hordozhatóság: Az impulzust mérő telefonkamera lehetővé teszi a felhasználók számára, hogy bármikor és bárhol ellenőrizhessék a pulzusukat. Ez különösen hasznos

lehet azok számára, akik rendszeresen sportolnak vagy egészségügyi problémákkal küzdenek.

- Könnyű hozzáférés: Mivel a telefonkamera általában minden okostelefon része, a felhasználóknak nincs szükségük további eszközökre vagy alkalmazásokra a pulzus-méréshez.
- Nem invazív jelleg: Az impulzust mérő telefonkamera nem igényel semmilyen test-be juttatott eszközt vagy beavatkozást, így a felhasználók számára kényelmes és fájdalommentes módszert biztosít a pulzusszám mérésére.

Hátrányok

- Pontosság: Az impulzust mérő telefonkamera pontossága eltérhet a hagyományos pulzusmérő eszközöktől, mint például a mellkasi öv vagy a pulzoximéter. A környezeti fény, a bőr színe, a kamera minősége és a felhasználó mozgása mind befolyásolhatja a mérés pontosságát.

Összefoglalva, az impulzust mérő telefonkamera egy kényelmes és hordozható módszer a pulzusszám mérésére, amely számos előnnyel jár a felhasználók számára. Azonban a pontosság és az adatbiztonság kérdései miatt a felhasználóknak figyelmesen kell választaniuk az alkalmazásokat és a mérési körülményeket.

3.9. Biztonság tesztelése

A biztonság tesztelése során különböző módszerekkel vizsgáljuk meg a rendszer biztonsági réseit és sebezhetőségeit. A tesztelés fő célja annak ellenőrzése, hogy a rendszer megfelelően védi-e az adatokat és a felhasználókat az illetéktelen hozzáférés ellen.

A biztonsági tesztelés során főleg a Wireshark alkalmazást használtam.

A Wireshark egy hálózati protokoll analízátor, amely képes megjeleníteni és elemzésre a hálózaton közlekedő adatcsomagokat. A fent ismertetett kommunikációs rendszer biztonságának tesztelése során a program segítségével ellenőrizhetjük a kommunikáció titkosítását és integritását. A software segítségével a következő teszteket végeztem el:

Kommunikációs csatornák ellenőrzése: A program segítségével megfigyelhetjük a hálózati forgalmat, hogy biztosítsuk, hogy a rendszer a megfelelő kommunikációs csatornákat és protokollokat használja (például Bluetooth és HTTPS).

Titkosítás ellenőrzése: Ellenőrizhetjük, hogy az átvitt adatok valóban titkosítottak-e. A HTTPS kommunikáció esetén a Wireshark megmutatja az SSL/TLS kézfogást, amely a kommunikáció titkosítását biztosítja. A program képes dekódolni a HTTPS forgalmat amennyiben átadjuk a megfelelő kulcsokat, de még ígysem képes dekódolni az OTP által titkosított üzeneteket, ha nincs hozzáférése a megfelelő kulcsokhoz.

JWT tokenek ellenőrzése: Megfigyelhetjük a JWT tokenek jelenlétét és formátumát a kommunikáció során. Ezzel megbizonyosodhatunk arról, hogy a JWT tokenek megfelelően használatosak a hitelesítési folyamatban. A JWT módosítása hiába való, ugyanis egy aláírást tartalmaz amivel a szerver kiszurja ha bármilyen kicsiny módosítás van ejtve a JWT-n.

Tűzfal beállítások ellenőrzése: Ellenőrizhetjük a hálózati forgalmat, hogy megbizonyosodjunk arról, hogy a tűzfal beállítások megakadályozzák a nem engedélyezett domain nevek hozzáférését a rendszerhez. Ezzel biztosíthatjuk, hogy a kommunikáció csak a megfelelő és engedélyezett forrásokból származik, ami további védelmet nyújt a nem kívánt behatolásokkal szemben.

Diffie-Hellman kulcscsere ellenőrzése: Nyomon követhetjük a Diffie-Hellman kulcscsere folyamatát, és ellenőrizhetjük, hogy a kulcsok megfelelően keletkeznek-e és cserélődnek-e a két fél között de egy hallgató nem képes reprodukálni a megfelelő kulcsot. Ez biztosítja, hogy a kulcsok biztonságosan és helyesen létrejönnek a titkosításhoz és visszafejtéshez.

Véletlenszerűség tesztelése: Ellenőrizhetjük a generált OTP kulcsok és a Diffie-Hellman kulcscsere során előállított megosztott titkok véletlenszerűségét. A megfelelő véletlenszerűség biztosítása nélkülözhetetlen a titkosítás hatékonyságához, mivel előrejelezhető mintázatok esetén a titkosítás gyengébbé válhat.

Időbélyegzők és lejáratási idők ellenőrzése: A JWT tokenekben szereplő időbélyegzőket és lejáratási időket megfigyelhetjük. Ennek során megbizonyosodhatunk arról, hogy a tokenek csak a megfelelő időtartamig érvényesek, és a lejárt tokeneket a rendszer nem fogadja el.

A Wireshark segítségével tehát átfogó teszteket végezhetünk a kommunikációs rendszer biztonságára és integritására vonatkozóan. Az eredmények alapján szükség esetén további biztonsági intézkedéseket tehetünk, vagy módosíthatjuk a rendszer beállításait, hogy még erősebb védelmet biztosítsunk a rendszerben. A Wireshark egy hatékony és hasznos eszköz a hálózati kommunikáció és a titkosítás biztonságának tesztelésében, amely segíthet a rendszer sebezhetőségeinek azonosításában és kezelésében.

4. fejezet

Tervezés

4.1. Osztályok

A szerver oldali megvalósításhoz egy Model-View-Controllers-Service-Repository (MVCSR) arhitektúra volt használva. Részletezem is őket:

Modellek

Az alkalmazásban általában modellek alkotják az adatszerkezetet, amelyek reprezentálják az alkalmazás mögötti adatokat. A modellek lényegében C# osztályok, amelyek tulajdonságokat tartalmaznak, amelyek megfelelnek az adatbázis tábláinak oszlopainak. A modellek felelősek az adatok továbbításáért az alkalmazás különböző rétegei között.

- User:

User
+ Id : int + Username : string + PasswordHash : byte[] + PasswordSalt : byte[] + LastActive : DateTime + SessionId : string

Ez a modell jelképezi a felhasználót az adatbázis táblában, tulajdonságai egy „Id” ami primary key szerepet tölt be az adatbázisban és a kodban is egyedi azonosítóként van használva. Egy felhasználónév („Username”), amely a bejelentkezéshez szükséges. A jelszó hash („PasswordHash”) és a jelszó só („PasswordSalt”) tartalmazza a felhasználó titkosított jelszavát amely a program állítja elő. Illetve egy „SessionId” és egy egy „LastActive” tulajdonság amelyeknek célja az aktív felhasználók figyelése a kódban.

- PulseData:

PulseData
+ Pulse : float

A felhasználótól szerzett pulzus értékét tárolja magában a „Pulse” mezőben.

- SensorData:

SensorData
+ Id : int
+ SensorValues : float[]
+ RecordedTime : DateTime

A „SensorData” modell az érzékelőktől kapott adatokat reprezentálja. Három mezője van: az „Id”, amely egy adott érzékelő adatpéldányának egyedi azonosítója, a „SensorValues” ahol az érzékelő adatok tárolodnak egy tömbben (9 érzékelő van) és a „RecordedTime”, amely az adatok rögzítésének dátumát és idejét tárolja.

- SensorOnCalibrationEnd:

SensorOnCalibrationEnd
+ Id : int
+ SessionId : string
+ SensorValues : float[]

A „SensorOnCalibrationEnd” modell az érzékelő állapotát mutatja a kalibrációs folyamat végén. Az „Id” mezőket tartalmazza, amely a kalibrálás végpéldányának egyedi azonosítója, valamint a „SessionId” mezőket, amelyek egy adott munkamenethez/szesszióhoz kapcsolják, illetve a kalibráció végén szerzett érzékelő adatokat, „SensorValues”.

- SessionHistory:

SessionHistory
+ Id : int + SessionId : string + UserId : int + Created : DateTime + UpdateInterval : double

A „SessionHistory” modell az eddigi és a már elkezdett folyamatokat tárolják. Tartalmazza az „Id” mezőt, amely a munkamenet-előzmény példány egyedi azonosítója, a „SessionId” mezőt, amely a munkamenet egyedi azonosítója, a „UserId” mezőt, amely a munkamenethez tartozó felhasználót azonosítja, az „UpdateInterval” mezőt, amely meghatározza, hogy milyen gyakran frissül a munkamenet információ, és a „Created” mezőt, amely a munkamenet létrehozásának dátumát tárolja.

DTOK

DTO a Data Transfer Object rövidítése. Ez egy tervezési minta, amelyet azért hoztak létre, hogy az adatokat egyszerűbb módon lehessen átvinni az alkalmazás egyik rétegéből a másikba. A DTO-k segítenek az adatok összeszedésében és továbbításában a rétegek között. Általában csak adatokat tartalmaznak, és nem rendelkeznek viselkedéssel, kivéve az alapvető hozzáférési és beállítási metódusokat.

- UserDTO:

UserDto
+ Username : string + Password : string

Két mezőt tartalmaz: „Username” és „Password”, amelyeket a felhasználói regisztrációhoz és az alkalmazási rétegek közötti adatcseréhez használnak.

- LoginDTO:

LoginDto
+ Username : string + Password : string + SensorData : float[]?

A felhasználók bejelentkezésére szolgáló DTO. Tartalmazza a „Username” és „Password” mezőket, amelyeket hitelesítési célokra használnak, valamint egy opcionális „SensorData” mezőt, amely egy float tömb formájában tárolhatja az érzékelő adatait.

Repositoryk

A Repository egy olyan tervezési minta, amely a modell réteg és az adatbázis közötti kommunikációt kezeli. Ő felelős az adatok tárolásáért és lekérdezéséért, valamint a modell réteg és az adatbázis közötti műveletek implementálásáért.

A Repository egy köztes réteggént működik a modell és az adatbázis között, és elrejti az adatbázis specifikus részleteket a modellek elől. Ezáltal a modell osztályoknak nincs közvetlen kapcsolatuk az adatbázissal, és nem kell az adatbázis-specifikus kóddal foglalkozniuk. Ehelyett a modellek csak az absztrakt interfészre támaszkodnak, amelyet a Repository nyújt.

A Repositorynek számos előnye van. Először is, egységesített felületet biztosít az adatbázishoz való hozzáférésre, ami egyszerűsíti és rendszerezetté teszi az adatbázisműveleteket. Másodszor, a Repository segítségével könnyebb tesztelni a modellt, mivel a Repository interfészre épülő tesztek könnyen implementálhatók. Harmadszor, a Repository réteg lehetővé teszi az adatbázis-specifikus műveletek könnyű cseréjét, ha később más adatbázisrendszert szeretnénk használni az alkalmazásban.

- SessionRepository:

SessionRepository
- <code>_context : ApplicationDbContext</code> + <code>SessionRepository(context: ApplicationDbContext)</code> + <code>Add(session: SessionHistory) : void</code> + <code>Get(sessionId: string) : SessionHistory</code>

A „SessionRepository” egy az adatbázisban lévő SessionHistory modellhez. Módszereket biztosít munkamenet hozzáadásához az „Add” és munkamenet lekérdezéséhez a „Get” metódussal. A „_context” az adatbázissal létesít kapcsolatot és azon keresztül vannak az adatok módosítva.

- SensorOnCalibrationEndRepository:

SensorOnCalibrationEndRepository
- <code>_context : ApplicationDbContext</code> + <code>SensorOnCalibrationEndRepository(context: ApplicationDbContext)</code> + <code>Get(string sessionId) : SensorOnCalibrationEnd?</code> + <code>Add(sensorOnCalibrationEnd : SensorOnCalibrationEnd) : void</code>

A „SensorOnCalibrationEndRepository” interfészt biztosít az adatbázisban lévő SensorOnCalibrationEnd modellhez. Módszereket biztosít egy példány hozzáadásához az „Add” és egy példány kinyeréséhez a „Get” metódussal.

- SensorRepository:

SessionRepository
- __context : ApplicationDbContext
+ SessionRepository(context: ApplicationDbContext) + Add(session: SessionHistory) : void + Get(sessionId: string) : SessionHistory

A „SensorRepository” interfészt biztosít az adatbázisban lévő SensorData modellhez, amely magában foglalja a SensorData példányok hozzáadásához és lekérdezéséhez szükséges logikát.

Servicek

A Service egy olyan réteget jelent, amely a logikai üzleti folyamatokat és műveleteket valósítja meg. A Service réteg elválasztja az üzleti logikát (Business logic) a többi rétegtől, például a felhasználói felülettől és az adateléréstől (Model).

A Service komponens felelős a különböző üzleti műveletek végrehajtásáért, például adatok validálásáért, adatmanipulációért, külső szolgáltatások integrálásáért vagy tranzakciók kezeléséért. Ez a réteg koordinálja az alkalmazás üzleti folyamatait és közvetíti az adatokat a Model és Repository réteg segítségével.

A Service réteg előnye, hogy lehetővé teszi az üzleti logika újrafelhasználhatóságát és tesztelhetőségét. Az üzleti logika elkülönítése a többi rétegtől lehetővé teszi a könnyebb karbantarthatóságot és a fejlesztési folyamat nagyobb skálázhatóságát. Emellett segít a felelőségek szétválasztásában és a kód tisztaságának megőrzésében.

- CipherService:

CipherService
+ Cipher(ciphertext: byte[], sharedKey: byte[]): byte[] + DeriveKey(length: int, sharedKey: byte[]): byte[] - Concat(arrays: byte[]): byte[]

Ez az osztály az adatok titkosításáért és visszafejtéséért felelős szolgáltatást képviseli. A „Cipher” metódus elvégzi az adatok (rejtjelezett szöveg) titkosítását vagy visszafejtését egy megosztott kulcs segítségével. A „DeriveKey” metódus egy megadott hosszúságú biztonságos kriptográfiai kulcsot generál. A „Concat” meg egy-máshoz illeszti, segéd funkció a DeriveKey-nek.

- ValidatorService:

ValidatorService
- __sensorDataValidator : IValidator<SensorData> - __pulseDataValidator : IValidator<float>
+ ValidatorService(sensorDataValidator: IValidator<SensorData>, pulseDataValidator: IValidator<float>) + ValidateSensorData(data: List<SensorData>, sessionId: string) : bool + ValidatePulseData(data: List<float>, sessionId: string) : bool

Ennek a servicének a feladata a szenzoradatok és az impulzusadatok hitelesítése. A „ValidateSensorData” és a „ValidatePulseData” metódusok felelősek ezért az érvényesítésért, a SensorDataValidator és a PulseDataValidator segítségével.

- PulseDataValidator:

PulseDataValidator
- LOCKOUT_THRESHOLD : float
+ ValidateData(data: List<float>, __: string) : bool

Ez az általános IValidator interfész implementációja az impulzusadatok érvényesítésére. Tartalmazza a „ValidateData” metódust, amely ellenőrzi, hogy az impulzusból származó adatok érvényesek-e.

- SensorDataValidator:

SensorDataValidator
- __logger: ILogger<SensorDataValidator> - LOCKOUT_THRESHOLD: float - __sensorOnCalibrationEnd: ISensorOnCalibrationEndRepository - __session: ISessionRepository - __sensorService: ISensorRepository
+ SensorDataValidator(logger: ILogger<SensorDataValidator>, __sensorOnCalibrationEnd: ISensorOnCalibrationEndRepository, __session: ISessionRepository, __sensorService: ISensorRepository) + ValidateData(data: List<SensorData>, sessionId: string): bool - IsTimeDeltaValid(payload: List<SensorData>, sessionId: string): bool - IsSensorDataStillValid(sensorValues: float[], sessionId: string): bool

Ez az osztály az általános IValidator interfész implementációja az érzékelők érvényesítésére. A bejövő érzékelőadatokat egy sorozat ellenőrzés alapján érvényesíti az „IsTimeDeltaValid” és az „IsSensorDataStillValid” metódusok segítségével.

- SessionService:

SessionService
- __sessionRepository : ISessionRepository - __logger : ILogger<SessionService>
+ SessionService(sessionRepository: ISessionRepository, __logger: ILogger<SessionService>) + Check(sessionId: string): bool + Get(sessionId: string): SessionHistory? + Create(guid: Guid, userId: int, updateInterval: double): void

Ez a szolgáltatás felel a munkamenet-kezelésért. A „Create” metódus egy új munkamenet létrehozására szolgál. A „Check” metódus a munkamenet létezését ellenőrzi. A „Get” metódus egy SessionHistory objektumot kér le a munkamenet azonosítójával.

- ProcessingService:

ProcessingService
- __cipherService : ICipher - __sessionService : ISessionService - __validatorService : IValidatorService - __logger : ILogger<ProcessingService>
+ ProcessingService(cipherService: ICipher, sessionService: ISessionService, validatorService: IValidatorService, logger: ILogger<ProcessingService>) + ProcessPayload(request: HttpRequest, payload: byte[], payloadType: PayloadType): bool - HandlePulseData(request: HttpRequest, decipheredPayloadByte: byte[]): bool + HandleSensorData(request: HttpRequest, decipheredPayloadByte: byte[]): bool

Ez a service a végzi a fő kezelést. A „ProcessPayload” metódus a beérkező hasznos adatok feldolgozására szolgál, és a tényleges kezelést a hasznos adat típusától függően a „HandlePulseData” vagy a „HandleSensorData” metódusra delegálja.

Controllerek

A kontroller feladata, hogy fogadja a bejövő HTTP kéréseket a szerver részéről, feldolgozza azokat, és megfelelő választ generáljon. A kontroller felhasználja a serviceseket, hogy elvégezze a dolgát. A kontroller tehát közvetíti a kommunikációt a felhasználó és az alkalmazás többi része között.

A kontrollerek segítségével az alkalmazás logikája elkülönül a felhasználtól és az adatelérési rétegtől.

- AuthController:

AuthController
- __configuration : IConfiguration - __logger : ILogger<AuthController> - __context : ApplicationDbContext
+ AuthController(configuration : IConfiguration, context : ApplicationDbContext, logger : ILogger<AuthController>) + Register(request : UserDto) : Task<ActionResult<User>> + Login(request : LoginDto) : Task<ActionResult<string>> - CreateToken(user : User, guid : out Guid) : string - CreatePasswordHash(password : string, passwordHash : out byte[], passwordSalt : out byte[]) : void - VerifyPasswordHash(password : string, passwordHash : byte[], passwordSalt : byte[]) : bool

Ez az osztály kezeli a felhasználói hitelesítést és regisztrációt. A „Register” és a „Login” metódusok kezelik a felhasználók regisztrációját, illetve bejelentkezését. A vezérlő a „CreateToken” és „CreatePasswordHash” metódusokat használja a hitelesítési tokenek és a hashed jelszavak létrehozására, valamint a „VerifyPasswordHash” metódust a bejelentkezési kísérletek érvényesítésére.

- DHController:

DHController
- __cipher : ICipher
- public: IActionResult PostPublicKey([FromBody] string clientPublicBase64)

Ez a kontroller felelős a Diffie-Hellman kulcscsere protokoll megvalósításáért. A „PostPublicKey” metódus elfogadja az ügyfél nyilvános kulcsát. Majd a „Cipher” servicet használva kulcsot generál.

- LocationController:

LocationController
+ UpdateLocation([FromBody] location: LocationData) : IActionResult

A helyadatok kezeléséért felelős. Az „UpdateLocation” metódus frissíti a felhasználó helyadatait.

- PhoneController:

PhoneController
- __logger : ILogger<PhoneController> - __processingService : IProcessingService
+ PhoneController(processingService: IProcessingService, logger: ILogger<PhoneController>) + PostPing(payload: List<float>): Task<ActionResult<bool>> - CheckPayload(payload: List<float>): bool

A felhasználó telefonjáról kapott impulzus adatok kezelésével foglalkozik. A „Post-Ping” metódus a telefontól érkező adatok fogadására szolgál. A „CheckPayload” metódus a kapott adatokat érvényesíti.

- PingsController:

PingsController
- __logger : ILogger<PingsController> - __processingService : IProcessingService
+ PingsController(logger: ILogger<PingsController>, processingService: IProcessingService) + PostPing(payload: string): Task<ActionResult<bool>> - CheckPayload(OTPMMessage: string): bool

Ez a vezérlő kezeli a NextMind használoktól érkező adatokat. A „PostPing” metódus az felhasználóktól érkező adatok kezelésére szolgál. A „CheckPayload” metódus validálja az felhasználótól kapott adatokat a „ValidatorService”-el. Szükség esetén kizárja, bekapcsolja a riasztót.

- TriggerController:

TriggerController
- __logger : ILogger<TriggerController>
+ TriggerController(logger: ILogger<TriggerController>) + Post()

Ez a vezérlő felelős bizonyos műveletek kiváltásáért. A „Post” metódus ezeket a műveleteket váltja ki. Pl. ajtó nyitás.

- UpdateController:

UpdateController
+ GetUpdates(cancellationToken : CancellationToken) : Task<IActionResult>

Ez a vezérlő felelős a frissítések kezeléséért. Az ajtók folyamatosan lekérlik a frissítéseket a „GetUpdate” metódussal.

5. fejezet

Mérések, eredmények

A kísérletek során a NextMind BCI és az impulzust mérő telefonkamera technológiák használatát vizsgáltuk „ajtónyitás” esetén. A két technológia eltérő előnyöket és hátrányokat mutatott a kísérletek során.

5.1. Agy-számítógép interfész eredménye

A NextMind BCI használata során a felhasználó először elhelyezte az eszközt a látókéregén, majd elindította a kalibrációs folyamatot a hozzá tartozó szoftver segítségével. Sikeres kalibráció után a felhasználó könnyedén végezhetett interakciókat a környezetben lévő objektumokkal, például ajtók nyitásával, pusztán a kijelölt képernyőre nézve és az interaktívvá váló objektumra fókuszálva. A kísérletek elején sokat kellett finomítani és hangolni a küszöbértékeket ami a DMS aktiválja, mivel sok fals pozitívum jött létre, ez inkább annak köszönhető, hogy a fejbőr elmozdul amikor a nyak mozog.

Az eredmények alapján a NextMind BCI gyors és intuitív interakciót tett lehetővé a felhasználók számára. A rendszer megbízhatósága és pontossága magas volt, és a felhasználók könnyen alkalmazkodtak a BCI használatához. Azonban a kalibrációs folyamat időigényessége és az eszköz helyes elhelyezkedésének fontossága némi nehézséget okozhat a felhasználóknak, különösen a kezdők számára. Ezenkívül a túlzott használat akár fájdalmat is okozhat az elektrodok nyomása miatt a látókéreg területén.

Az eredmények azt mutatták, hogy a NextMind BCI alapú hitelesítés hatékony és biztonságos módszer, amely a „dead man switch” elv alapján működik, és automatikusan visszavonja a jogosultságokat, ha a kapcsolat megszűnik vagy anomália lépne fel.

A tesztelés során a kapcsolat megszakításának észlelése 100%-os arányban sikerült. Az elektrodák már 2 méternél is kisebb távolságokra képesek voltak aktivitást kiváltani, viszont a képernyő mérete és a rajta megjelenő objektumok nagysága befolyásolhatja a hatótávolságot. Továbbá, a sűrű haj gátolhatja az elektrodák jeleinek érzékelését, ezért a felhasználónak szorosabban kell rögzítenie a NextMind eszközt és mélyebben kell illeszteni az elektrodákat egymást követő fel-le mozdulatokkal. Ugyanakkor ezek a mozdulatok károsíthatják a NextMind eszközt, mivel a haj beakadhat az elektrodákba és eltörheti azokat. Emellett a szoros viselet kényelmetlenséget okozhat már rövid idő alatt is. A sűrű és hosszú haj hátrányt jelent ennek az eszköznek a használata során.

5.1. táblázat. Felmért adatok

Művelet	Átlag idő (másodperc)	szórás (másodperc)
Belépési idő*	12.3	1.5
Kalibráció	55.49	1.10

Minta méret belépési időre: 843

Minta méret kalibrációra: 84

* A belépési idő pontos mérése nem volt lehetséges, mivel a résztvevő indította és állította le a stoppert a folyamat kezdeténél és végénél.

5.2. Impulzust mérő telefonkamera eredménye

Az impulzust mérő telefonkamera esetén a felhasználó először elindította az alkalmazást, majd az ujját a telefon kamerájára helyezte. Sikeres mérés után a felhasználó a telefonját egy NFC olvasóhoz közelítette, amellyel az ajtó kinyílt.

Az impulzust mérő telefonkamera előnyei között szerepel a gyors és egyszerű használat, valamint a széles körű elérhetőség a modern okostelefonokon. A rendszer megbízható volt, és a felhasználók könnyen alkalmazkodtak a technológia használatához. Azonban a hátránya az volt, hogy a felhasználó egyik kezét állandóan foglalta a telefon tartása és az ujj elhelyezése a kamerán, ami korlátozta a többkezes tevékenységek végzését. A legtöbben ezt egy hatalmas negatívumként fogták fel. Továbbá, a rendszer a telefon akkumulátorának gyorsabb merüléséhez vezetett az intenzív kamera- és szenzorhasználat miatt.

5.3. Hasonlat

Összehasonlítva a két technológiát, mindkettő előnyökkel és hátrányokkal rendelkezik egy jogokkal bíró ajtónyitási rendszerben.

A NextMind BCI előnyei közé tartozik a gyors és intuitív interakció lehetősége, valamint a kéz- és szabad mozgás biztosítása a felhasználó számára, ezenfelül gyakori használatnál jobb eredmények érhetőek el. Ugyanakkor a kalibráció időigényessége és az eszköz helyes elhelyezkedésének fontossága és kihívásai nehézségeket jelenthet egyes felhasználók számára.

Az impulzust mérő telefonkamera előnyei között szerepel a könnyű használat és a széles körű elérhetőség a modern okostelefonokon. Azonban a rendszer hátránya, hogy a felhasználó egyik kezét állandóan foglalja a telefon tartása és az ujj elhelyezése a kamerán, ami korlátozza a többkezes tevékenységek végzését és a telefon akkumulátorának gyorsabb merülését okozza.

A kísérleti eredmények alapján mindkét technológia alkalmas lehet a „ajtónyitási” rendszerben történő alkalmazásra, attól függően, hogy melyik előnyeit és hátrányait tartjuk fontosabbnak. A további kutatásokban érdemes lehet több technológiai kombinációt is vizsgálni, valamint a rendszer kialakítását és beállításait tovább optimalizálni a felhasználói igények és elvárások alapján. Mindkét rendszer alapja a „dead man switch” elv, amely átruházhatatlan hitelesítést nyújt és biztonsági szempontból előnyös.

Összességében, a kutatás során alkalmazott ember-gép interfészek új megközelítést jelentenek a jelszómentes biztonságos beléptetésre és felhasználói hitelesítésre.

6. fejezet

Következtetések

A kutatás során megállapítottuk, hogy az ember-gép interfészek, mint például a BCI és az impulzusmérő telefonkamera, új, hatékony lehetőségeket kínálnak a jelszómentes biztonságos beléptetés és felhasználói hitelesítés területén. Az eredmények azt sugallják, hogy az emberi biometrikus azonosítók felhasználása, mint az agyhullámok vagy a pulzus, olyan megközelítés lehet, amely csökkenti a jelszavakra és hagyományos beléptetési módszerekre jellemző biztonsági kockázatokat. Az ilyen típusú megoldások, amelyek az aktív ember-gép kapcsolatra építenek és amelyek az érzékelők által rögzített jeleket valós időben értelmezik, különösen előnyösek lehetnek olyan területeken, ahol az adatbiztonság és a fizikai védelem kiemelten fontosak, például a banki és kormányzati szektorban.

Az ajánlott rendszer egy másik nagy előnye, hogy a biometrikus minták nem tárolódnak, és nem társítjuk őket véglegesen egy felhasználóval. A „Cancelable Biometrics” [PRC15], magyarul „visszavonható biometria”, egy új kutatási irányzat, amely biztonsági rendszereket és protokollokat dolgoz ki az egyének magánéletének és anonimitásának megőrzése érdekében.

6.1. Kutatás korlátai

A jelenlegi kutatásnak több korlátja is van, amelyek befolyásolhatják az eredmények értelmezését és az alkalmazhatóságot. Az egyik ilyen korlát a minta mérete, amely korlátozza az eredmények általánosíthatóságát. Egy másik korlát a cyber-biztonság felmérése szakértők hiányában. Emellett az ember-gép interfészek jelenlegi technológiai korlátai, mint például a BCI kalibráció időigényessége, a NextMind használó softwarek egyedüli operációs rendszerrel való kompatibilitás és a telefonkamera alapú impulzusmérő kezdetleges felhasználói élménye, szintén korlátokat jelentenek a rendszerek széleskörű alkalmazásában.

6.2. További kutatási lehetőségek

A jelenlegi eredmények továbbfejlesztése és kiterjesztése érdekében számos lehetőség áll rendelkezésre a jövőbeni kutatások során. Az eredmények általánosíthatóságának javítása érdekében érdemes lenne növelni a minta méretét, és a különböző felhasználói csoportokat vizsgálni. A cyber-biztonság felméréséhez pedig érdemes biztonsági szakértőket bevonnunk a kutatási folyamatba.

A BCI és impulzusmérő telefonkamera technológiai korlátainak leküzdése érdekében lehetne olyan módszereket fejleszteni és tesztelni, amelyek csökkentik a kalibráció időigényét, javítják a felhasználói élményt, és fejlesztik a biztonsági protokollokat. Az új BCI technológiák is lehetőséget nyújtanak a korábbi problémák megoldására, mint például a Crown [Neu23].

Összefoglalva, az ember-gép interfészek jelentős lehetőségeket nyújtanak a jelszómentes biztonságos beléptetés és felhasználói hitelesítés területén. A jelenlegi kutatási eredmények bár korlátokkal rendelkeznek, a további kutatási lehetőségek és fejlesztések reményt keltőek a technológia széleskörű alkalmazását illetően.

A jövőbeli technológiai fejlesztések és az új biztonsági kihívások nyomán folyamatosan szükség lesz az ember-gép interfészek további kutatására és fejlesztésére. Az innováció és az új megközelítések által a biztonságos beléptetés és hitelesítés területén elért előrelépések hozzájárulhatnak a személyes adatok és a digitális erőforrások védelméhez, valamint az átfogó adatbiztonság védelmének javításához.

A fent említett megvalósított dolgok elérhetőek a személyes Github repositoryban:

Saját megvalósított dolgok:

- Backend: <https://github.com/bakolaszlo/NextMindBE>
- Frontend ("Ajtó"): <https://github.com/bakolaszlo/door-fe>
- NextMind alkalmazás: <https://github.com/bakolaszlo/NextMind-Client>

Módosított harmadfél alkalmazások és csomagok:

- Telefon alkalmazás módosított változata: <https://github.com/bakolaszlo/HeartBeat-1>

Harmadfél alkalmazások és csomagok:

- Telefon Alkalmazás eredeti változata: <https://github.com/berdosi/HeartBeat>
- Hely meghatározó alkalmazás eredeti változata telefon alkalmazás: <https://github.com/schollz/find3-android-scanner>
- Hely meghatározó alkalmazás: <https://github.com/schollz/find3>
- Diffie Hellman kulcs csere library: <https://github.com/MidLevel/MLAPI.Cryptography>

Ábrák jegyzéke

3.1. Use Case diagram	21
3.2. UML diagram	24
3.3. NextMind headset elektródjai	25
3.4. NextMind headset elhelyezve a látókéregben. (Kép forrása: [Cao20])	26
3.5. NextMind headset kalibrációs eredménye, példa villogó objektumra . . .	27
3.6. NextMind headset elektrodák elhelyezkedési erősségük	28

Táblázatok jegyzéke

5.1. Felmért adatok	48
-------------------------------	----

Irodalomjegyzék

- [BG16] Ioan Buciu and Alexandru Gacsadi. Biometrics systems and technologies: A survey. *International Journal of Computers Communications & Control*, 11(3):315–330, 2016.
- [Cao20] Sissi Cao. A New Headset That Uses Brainwaves To Control Things (It Works!) Is Now On Sale. <https://observer.com/2020/07/nextmind-ces-brain-sensing-interface-developer-kit-preorder-open/>, 2020. [Online; accessed 04-April-20223].
- [HEMF15] Abdenour Hadid, Nicholas Evans, Sebastien Marcel, and Julian Fierrez. Biometrics systems under spoofing attack: an evaluation methodology and lessons learned. *IEEE Signal Processing Magazine*, 32(5):20–30, 2015.
- [HH20] Morey J Haber and Morey J Haber. Passwordless authentication. *Privileged Attack Vectors: Building Effective Cyber-Defense Strategies to Protect Organizations*, pages 87–98, 2020.
- [Len22] David Lennick. Kill switch design pattern for microservice architectures on internet of things devices. 2022.
- [LF12] Jaime Gomez-Gil Luis Fernando, Nicolas-Alonso. Brain computer interfaces, a review. 2012.
- [Neu23] Neurosity. Crown. <https://neurosity.co/how-it-works>, 2023.
- [Pla18] Andreas Platschek. A harmonized threat/hazard modeling method for safety critical industrial systems. 2018.
- [PP18] Vaibhav Gandhi Parmar Prashant, Anand Joshi. Brain computer interfaces: A review. 2018.
- [PRC15] Vishal M Patel, Nalini K Ratha, and Rama Chellappa. Cancelable biometrics: A review. *IEEE signal processing magazine*, 32(5):54–65, 2015.
- [SMA⁺18] Simanto Saha, Khondaker A. Mamun, Khawza Ahmed, Raqibul Mostafa, Ganesh R. Naik, Sam Darvishi, Ahsan H. Khandoker, and Mathias Baumert. Progress in brain computer interface: Challenges and opportunities. 2018.
- [TQB22] Zahra Tarkhani, Lorena Qendro, and Malachy O’Connor Brown. Enhancing the security & privacy of wearable brain-computer interfaces. 2022.

- [WAA⁺19] Michael Wiklund, Kimmy Ansems, Rachel Aronchick, Cory Costantino, Alix Dorfman, Brenda van Geel, Jonathan Kendler, Valerie Ng, Ruben Post, and Jon Tilliss. Add a “dead man’s switch”. In *Designing for Safe Use*, pages 63–64. CRC Press, 2019.