Felhőben kapirgáló MI asszisztens

Tureczki Bence
MI - Biztonság - Blokklánc Tudásközpont
Óbudai Egyetem
tureczki.bence@uni-obuda.hu
+36 70 569 3207

Dr. Szenes Katalin
MI - Biztonság - Blokklánc Tudásközpont
Óbudai Egyetem
szenes.katalin@uni-obuda.hu
+36 1 666 5556

Kulcsszavak:
mesterséges intelligencia, blokklánc, felhő, kriptovaluta, arbitrázs

Absztrakt:
Az ügyfelek bizalma megrendült a gazdasági válságok és a bankcsődök miatt a bankokban. Ezért sokan szívesen tartják a vagyonukat olyan helyen, amelynek biztonsága attól függ, hogy elegendő ügyfél látja-e ugyanazt a vagyoni helyzetet. Ezt a koncepciót a kriptovaluta rendszerek blokklánc adatbázis alapon valósítják meg. A tranzakciók kezelésére egy AI asszisztenst készítettünk a Microsoft Azure felhő rendszer eszközkészletével. Digitális asszisztensünk, az eXpie, egy olyan blokklánc felhőt használ, amely a Monero kriptovaluta hálózat és a MODEX felhő erőforrásai között valós időben arbitrál.

1 Az MI asszisztensünk

Az Óbudai Egyetem MI-Blokklánc-Biztonság Tudásközpontjának egyik célja a “feltörekvő technológiák” minél teljesebb kihasználása[3]. A Tudásközpontban azt a technológiát tekintjük “feltörekvőnek”, amelyre igaz az, hogy létezik:

- olyan alkalmazás, amelyik a technológiát használja
- olyan profit-orientált vállalat, amelyik a technológiát használó alkalmazást üzleti értéknek tekinti, valamint
- a vállalat szerint üzleti előnyt jelent számára az alkalmazás a piacon

A definíciónk értelmében feltörekvő technológia lehet a:

- blokklánc adatbázis
- mesterséges intelligencia
- Merkle fa szerinti tranzakciókezelés
- felhő alapú infrastruktúra
- kriptovaluták

1.1 Egy új MI definíció

A tudásközpont “eXpie” nevű alkalmazása egy olyan “mesterségesen intelligens” digitális asszisztens, amelyiknek a forráskódja egy blokklánc adatbázisban van és a forráskódot egy felhőrendszer hajtja végre[3]. “Mesterséges intelligenciának” hívunk egy alkalmazást, ha olyan feladatot is meg tud oldani, amit még a saját készítője sem. Ebben a felfogásban mesterséges intelligencia a:

- Microsoft Cortana
- Apple Siri
- Amazon Alexa
- IBM Watson

Az említett MI alkalmazásokat digitális asszisztenseknek nevezzük, mert a digitális világban működnek és javarészt asszisztensi feladatokat látnak el.

2 Az MI asszisztens, mint zombi ügynök

A digitális asszisztensek különösen vonzó célpontok a hackerek számára, ugyanis nagymennyiségű személyes adathoz férnek hozzá és manipulálják a saját felhasználójukat. Tapasztalatunk szerint a három legjellemzőbb támadás a felhasználókkal szemben:

- a feladat végrehajtásának ellehetetlenítése
- a tudásbázis megszerzése
- az emberi felhasználó átverése

A fenti támadástípusok mindegyike történhet úgy, hogy a hacker az alkalmazást futtató számítógépet támadja meg. A feladatot a hacker legtöbbször hálózati leterheléssel (rosszindulató program telepítése nélkül) vagy valamilyen számítógépes vírussal lehetetleníti el. A támadás célja a következő kritériumok tetszőleges variációjának megsértése lehet:

- bizalmasság
- integritás
- rendelkezésre állás
- funkcionalitás
- hatásosság
- hatékonyság
- rend
- adateredet
- megbízhatóság
- megfelelőség[1, 2].

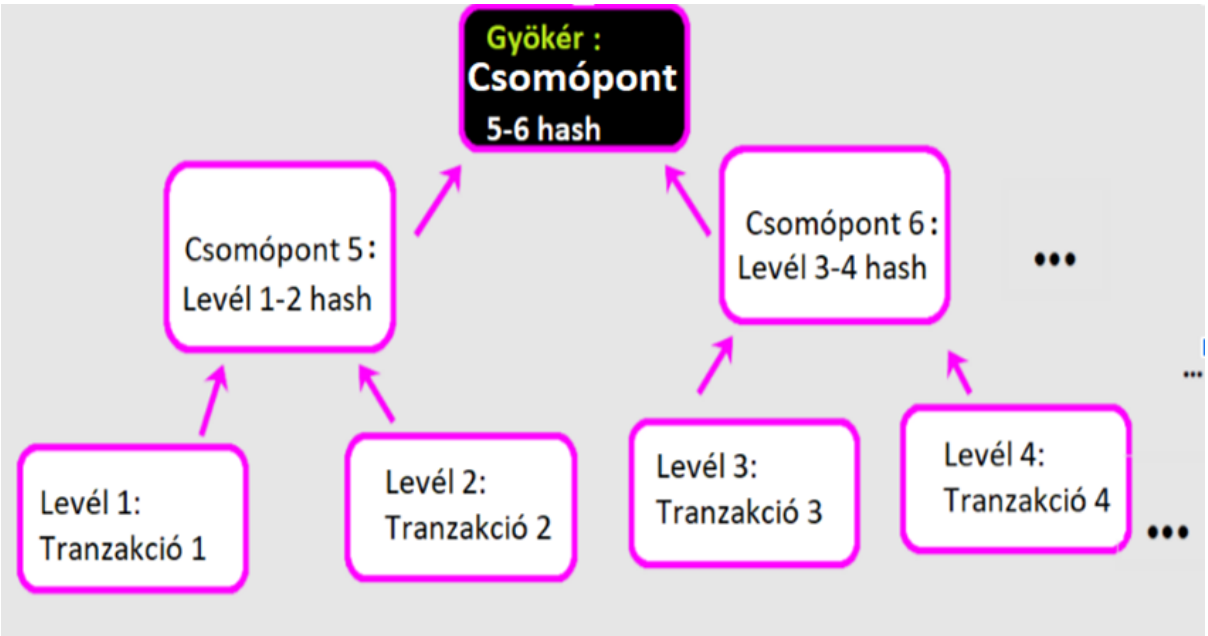
Például, ha a támadó kémalkamazást telepít a digitális asszisztenst futtató számítógépre, akkor az ott található tudásbázis adatainak bizalmasságát veszélyezteti. Ha rosszinduló alkalmazásával töröl az adatok közül, vagy módosítja azokat, akkor sérülhet a rend, az adatok integritása, sőt rendelkezésre állásuk is. Megfelelő adatok hiányában csorbulhat a funkcionalitás, ami rombolhatja az emberi felhasználó bizalmát az alkalmazásban. Más esetekben pedig éppen a bizalom az, ami segíti a támadót. Ha ugyanis nem ellenőrizzük az adatok eredetét, akkor a hacker, saját forrású adatokkal manipulálhatja a digitális asszisztens válaszait, azok pedig végső soron az emberi felhasználót[6]. Ahogy az 1. ábra mutatja, a mesterséges intelligencia ráveheti az embert arra - sokszor az áldozat tudomása nélkül-, hogy megtegyen a támadónak kedvező cselekedeteket, információkat adjon ki, egyszóval digitális asszistens helyett a hacker zombi ügynökeként működjön.

1. ábra: Hogyan lesz asszisztensből zombi?

3 MI asszistensünk kommunikációja Merkle fa alapon

Amikor MI asszisztensünk beszélget a felhasználóval, akkor mindkét fél válaszait tranzakciókban tároljuk el. A tranzakciókat egy Merkle fa leveleibe tesszük. Az egyes közbülső csomópontok az azokból a csomópontokból képzett hash kódot tartalmazzák, amelyekkel kapcsolatban vannak a fában. A 2. ábra azt mutatja, hogyan rendezzük Merkle fába a tranzakcióinkat. A levelektől legtávolabb eső csomópont, azaz a gyökér, egy olyan hash kódot tartalmaz, amelyre a fa összes csomópontjának tartalma hatása van. Tehát ha bármelyik csomópont tartalma megváltozik, az

kimutatható pusztán a gyökér ellenőrzésével, az egész fa feldolgozása nélkül. Így, a Merkle fa hatásos eszköz annak észrevételére, hogy módosítás történt valamelyik tranzakcióban, továbbá költséghatékony módszert biztosít a módosítás helyének megkeresésére, mert elegendő azokat az utakat bejárni, amelyek olyan csomópontokból állnak, amelyek megváltoztak a módosítás előtti Merkle fához képest.



2. ábra: A Merkle fa

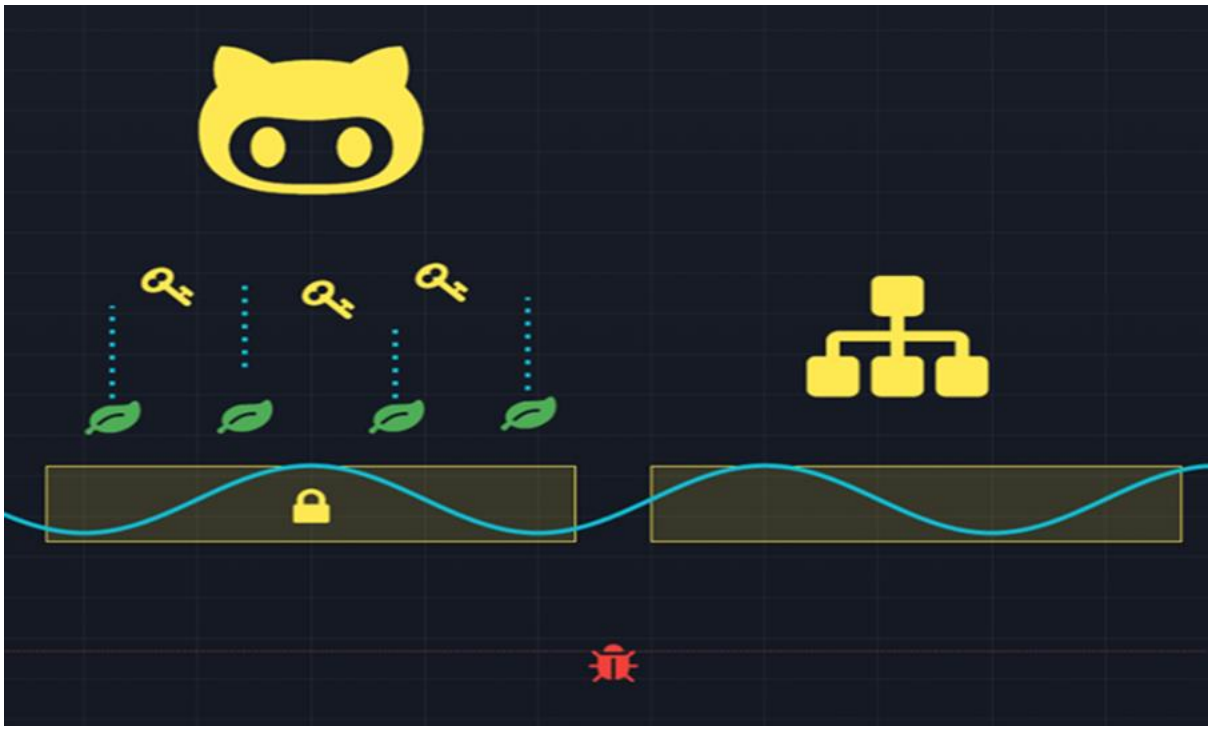
4 A rémisztő blokklánc

Az előző fejezet rávilágított arra, hogy miért érheti meg Merkle fában tárolni az MI asszisztens válaszait. Az MI azonban elveszíti ezeket az előnyöket, ha a második fejezetben leírt forgatókönyhöz hasonlóan, egy hacker hozzáfér a Merkle fáinkhoz, azaz az asszisztensünk tudásbázisához.

Ezért “eXpie” blokklánccal teszi a Merkle fák kezelését bizalmasabbá[3, 4, 5]. A 3. ábra azt mutatja, ahogy a blokkláncunk blokkjaiban eltároljuk a valamilyen szempont szerint készített Merkle fáinkat. Ilyen szempont lehet az azonos időpecsét. A blokklánc adatszerkezet jellemzője, hogy minden egyes blokk tartalmaz egy, az időben őt közvetlenül meglőző blokkból képzett hash kódot. Ilyen módon, minden blokk láncszerűen hivatkozik az őt megelőzőre. Ennek köszönhetően, ha egy hacker hozzáfér a Merkle fáinkhoz, azokat csak akkor tudja módosítani észrevétlenül, ha a blokklánc összes olyan blokkját módosítja, amely a módosítandó Merkle fát tartalmazó blokk után következik a láncban. Ennek hatalmas számítási igénye van, ezért nehéz feladatnak tekintjük.

Tapasztalatunk alapján, a hackerek sokszor szívesebben választanak könnyebb célpontot, mintsem hogy a blokkláncban tárolt adatokat írják át. Ha a támadó mégis megpróbálja módosítani az eltárolt adatokat, de nem írja át az összes releváns blokklánc blokkot és a Merkle fa csomópontot, akkor az illetéktelen

módosítás ténye hatásosan detektálható és a helyes állapot költséghatékonyan helyreállítható.



3. ábra: A blokklánc

5 Ki fűzi fel a blokkláncunk blokkjait?

Az előző fejezetben előnyként jelent meg a blokklánc működtetésének számítási igénye a támadókkal szemben. Ez az igény azonban akkor is drága, ha “eXpie” tisztességes használat során fűzi fel a válaszokat a blokkláncba. Ezért választottunk egy publikus blokkláncot. A publikus blokkláncban a költség mindig eloszlik a felhasználók között[5].

Az Monero blokklánc blokkjait az Monero bányászok fűzik fel, akik az Monero nevű digitális valutában kapnak jutalmat a munkájukért[7]. A díjat az a felhasználó fizeti, akinek érdeke az adott blokk felfűzése, mert számára értékes tartalom van benne. Az egész világon bárki, bárhol, anonim módon használhatja a publikus blokkláncot. Nekünk csak akkor kell fizetnünk és csak azokért a válaszokért, amelyeket blokklánccal akarunk biztosítani. Ezt követően a feltöltött adat bárhová, bármikor, ingyen letölthető a MODEX felhőn keresztül, amelyik a digitális asszisztensünk és a Monero blokklánc között közvetít[7, 8]. További költsége nincsen számunkra. Ahhoz, hogy a bányászok el tudják végezni a munkájukat, letöltik a saját számítógépeikre a teljes Monero blokkláncot és ezt folyamatosan egyeztetik egymással.

Szóval, ha a támadó át akarja írni a blokkláncban tárolt adatok tetszőleges részhalmazát, akkor nemcsak a releváns hash kódokat kell újra kiszámolnia, hanem

a bányász számítógépek többségét is meg kell fertőznie. Tudomásunk szerint ezt a mai napig, soha, senki nem tudta sikeresen véghezvinni. A bemeneti/kimeneti adatok és forráskód módosítása nélkül pedig sokkal nehezebben lesz a digitális asszisztensünkből zombi ügynök.

Bibliográfia

[1] Katalin, Szenes ; Bence, Tureczki
Supporting Corporate Governance on a Blockchain basis
CYBER SECURITY REVIEW 2021 : 2 pp. 1-6. , 6 p. (2021)
Teljes dokumentum
Közlemény:31918301 Admin láttamozott Forrás Folyóiratcikk (Szakcikk) Tudományos

[2] Szenes, Katalin ; Tureczki, Bence
AI Supported Corporate Governance
In: Szakál, Anikó (szerk.) 2021 IEEE 19th World Symposium on Applied Machine Intelligence and Informatics (SAMI)
Budapest, Magyarország : IEEE Hungary Section (2021) 507 p. pp. 000465-000470. , 6 p.
Közlemény:31823932 Admin láttamozott Forrás Idéző Könyvrészlet (Konferenciaközlemény) Tudományos

[3] Tureczki, Bence ; Szenes, Katalin
Interdisciplinary Optimization of Security Operations Centers with Digital Assistant
In: Szakál, Anikó (szerk.) 15th IEEE International Symposium on Applied Computational Intelligence and Informatics SACI 2021
Budapest, Magyarország : Óbudai Egyetem, IEEE (2021) 539 p. pp. 397-402. , 6 p.
Közlemény:32073211 Egyeztetett Forrás Idéző Duplum Könyvrészlet (Konferenciaközlemény) Tudományos

[4] Katalin, Szenes ; Bence, Tureczki
Supporting Corporate Governance on a Blockchain basis
In: Nyikes, Zoltán; Kovács, Anna (szerk.) ICCECIP 2020 Absract book
Budapest, Magyarország : Óbudai Egyetem (2020) p. 37 , 1 p.
Közlemény:31918393 Admin láttamozott Forrás Könyvrészlet (Absztrakt / Kivonat) Tudományos

[5] Szenes, Katalin ; Tureczki, Bence
Blockchain basics, applications (2019)

Szóbeli előadás, Blockchain and deep learning workshop, 2019. szeptember 5., Számítástechnikai és Automatizálási Kutatóintézet,
Közlemény:31821002 Nyilvános Forrás Egyéb (Nem besorolt) Tudományos
Szenes, Katalin ; Tureczki, Bence
Blockchain basics, applications
In: Blockchain és deep learning : workshop
MTA SZTAKI (2019) pp. 1-40. , 40 p.
Közlemény:31820997 Nyilvános Forrás Egyéb konferenciaközlemény (Konferenciaközlemény) Tudományos

[6] Szenes, Katalin ; Tureczki, Bence
Az intézményi stratégia támogatása informatikai biztonsági és ellenőrzési módszerek továbbfejlesztésével; Hogyan rúgja fel a blokklánc az EU szabályozást? (2019)
Panel, "IT Law Specialist. IT jogi kérdések gyakorlati megközelítésben", IIR szakkonferencia, Budapest, 2019. szeptember 19-20., Szervező: IIR Magyarország Kft.,
Közlemény:31820977 Nyilvános Forrás Egyéb (Nem besorolt) Tudományos

[7] Monero, blokkláncszolgáltató, https://www.getmonero.org/ (2021.10.27.)

[8] MODEX, felhőszolgáltató, https://modex.tech/ (2021.10.27.)