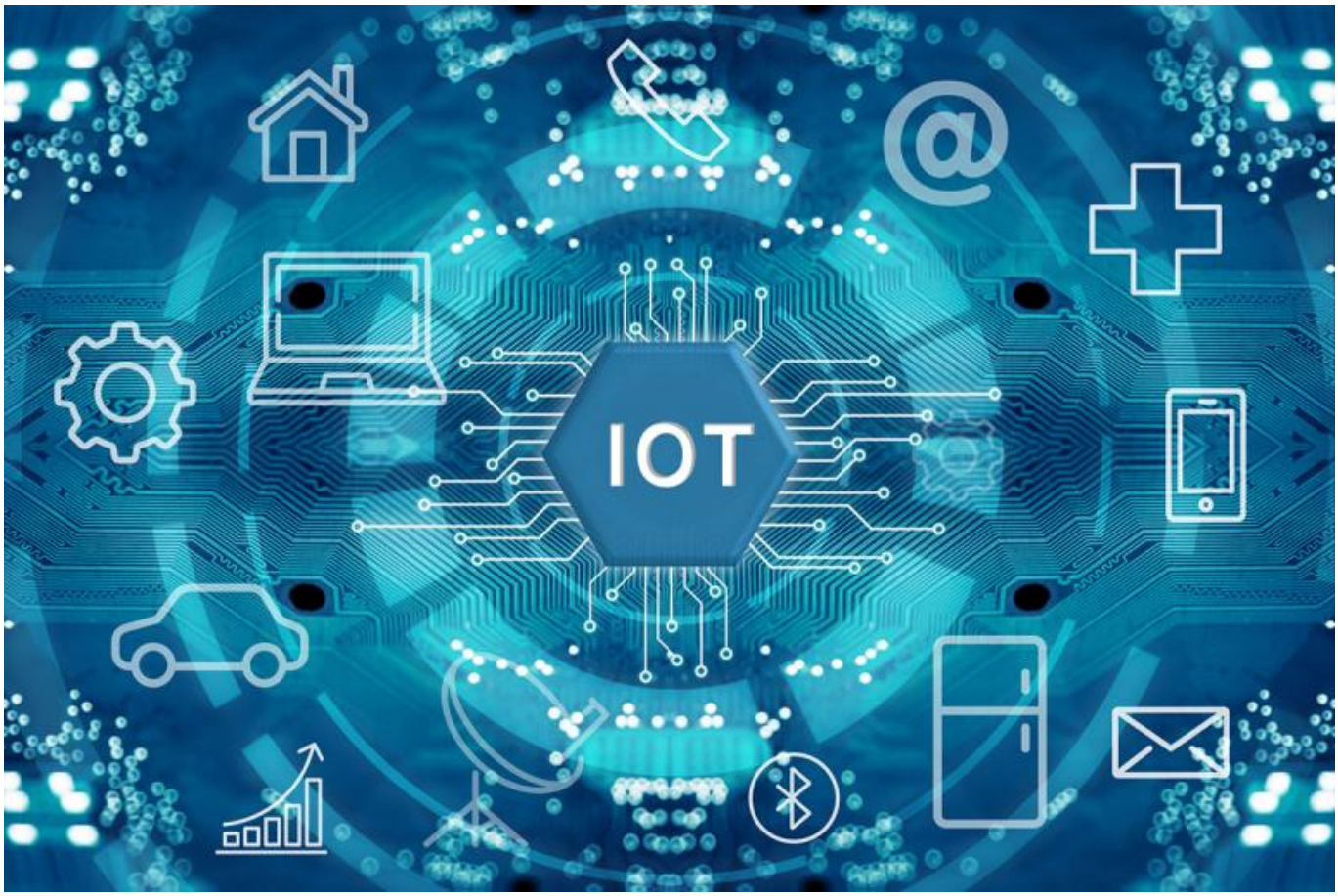
[Biztonságos megoldások a dolgok internetére (https://digital-strategy.ec.europa.eu/hu/policies/secure-internet-things)]

A Bizottság azon dolgozik, hogy szilárdabb és ellenállóbb biztonsági kereteket biztosítson az IoT-eszközök és azon hálózatok számára, amelyeknek részét képezik.



A dolgok internete (IoT) eszközök kulcsszerepet játszanak a hálózatok ellenálló képességének biztosításában, valamint az adatok magán- és biztonságos megőrzésében. A kiberbiztonsági fenyegetések egyre összetettebb tendenciája azonban szilárdabb biztonsági kereteket tesz szükségessé az IoT-eszközök és -hálózatok számára.

E kérdés megoldása érdekében az Európai Bizottság 2020 decemberében átfogó kiberbiztonsági stratégiát terjesztett elő a digitális évtizedre vonatkozóan (https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade), felvázolva a biztonságos dolgok széles körű internete felé vezető utat.

Az IoT-projektek biztonsági klasztere az eszközök és hálózatok hiányosságaival foglalkozik. Ezt olyan biztonságos és moduláris keretek kialakításával teszi, amelyek integrálhatók az életvitel, az egészségügy, a gyártás, az élelmiszer-ellátás, az energia és a közlekedés területén az új és meglévő megoldásokba. Ez a klaszter 8 projektből áll, amelyek 40 millió EUR (egyenként körülbelül 5 millió EUR) uniós finanszírozást tesznek ki.

A klaszter figyelemre méltó eredményeket hozott a célágazatokban. Bár az alkalmazások specializáltak, a projektek által alkalmazott nyílt forráskódú moduláris fejlesztési megközelítés lehetővé teszi a modulok más megoldásokban történő újrafelhasználását az alkalmazások szélesebb köréhez.

Projektek

SecureIoT: Prediktív biztonság IoT-platformok és intelligens objektumok hálózatai számára (https://secureiot.eu/)

A SecureIoT az IoT-szolgáltatások és a kiberbiztonság globális vezetőinek közös erőfeszítése a decentralizált IoT-rendszerek következő generációjának biztosítása érdekében. Ezek az intelligens objektumok több hálózatát ölelik fel, és számos nyílt biztonsági szolgáltatást valósítanak meg.

A SecureIoT prediktív biztonsági szolgáltatásokat tervezett az IoT-alkalmazások élvonalbeli referenciaarchitektúráival összhangban, amelyek alapul szolgálnak a biztonsági építőelemek meghatározásához az IoT-rendszerek szélén és magjában egyaránt. A SecureIoT biztonsági adatgyűjtési, nyomon követési és prediktív mechanizmusokat biztosít, amelyek integrált szolgáltatásokat nyújtanak a kockázatértékeléshez, a megfelelőség ellenőrzéséhez a rendeletek és irányelvek (általános adatvédelmi rendelet (https://ec.europa.eu/info/law/law-topic/data-protection_en), a hálózati és információs rendszerek biztonságáról szóló irányelv (https://digital-strategy.ec.europa.eu/en/policies/nis-directive), az elektronikus hírközlési adatvédelmi irányelv (https://digital-strategy.ec.europa.eu/en/policies/digital-privacy)) és a fejlesztői támogatás tekintetében.

A SecureIoT szolgáltatásait piacvezérelt forgatókönyvekben, például az intelligens gyártás és a mobilitás területén megkérdőjelezték. Telepítésük nyíltan elérhető IoT-szolgáltatásokon és a platformok partnerközösségén alapult. Az intelligens életmód használata során a SecureIoT bemutatta az IoT-kompatibilis robotika támadásainak észleléséhez szükséges időt. Ezeknek a társadalmilag segítő robotoknak (https://secureiot.eu/assisted-living)a 80%-a a biztonsági tudásbázisban talált kritikus eszközök, így a SecureIoT kevesebb, mint 10 másodpercbe telt, hogy hatékonyan észlelje az anomáliákat, és kevesebb mint 5 percet vesz igénybe a kockázatértékeléshez.

Szemiotika: Smart End-to-end Massive IoT interoperabilitás, összekapcsolhatóság és biztonság (https://www.semiotics-project.eu/)

A Semiotics egy mintavezérelt keretrendszert fejlesztett ki, amely a meglévő IoT-platformokra építve garantálja a biztonságos és félautonóm viselkedést az ipari IoT-alkalmazásokban. Ezek a minták

kódolták az egyes intelligens objektumok biztonsága, magánélete, megbízhatósága és interoperabilitása közötti függőséget.

A szemiotika támogatta a többrétegű adaptációt, beleértve az intelligens objektumokat, hálózatokat és felhőket, amelyek a terepen (szélen) és az infrastruktúra (backend) rétegek autonóm viselkedését célozták meg. A horizontális és vertikális területeken jelentkező komplexitási és skálázhatósági igények kielégítése érdekében a SEMIoTICS programozható hálózati és szemantikai interoperabilitási mechanizmusokat dolgozott ki. Gyakorlatiasságát az egészségügy, a megújuló energia és az intelligens érzékelés három felhasználási esetével validálták.

A konzorcium az európai iparban, a kkv-kban és a tudományos körökben érdekelt felekből állt, amely lefedte az IoT teljes értékláncát, a helyi beágyazott elemzéseket, valamint a felhőhöz való programozható kapcsolatukat a biztonsággal és a magánélettel.

DevOps beiktatása (https://cordis.europa.eu/project/id/780351)

A DevOps mozgalom olyan szoftverfejlesztési eszközöket támogat, amelyek biztosítják a szolgáltatás minőségét, miközben komplex rendszereket fejlesztenek ki, és elősegítik a gyors innovációs ciklusokat és a könnyű használatot. A DevOps széles körben elterjedt a szoftveriparban, de ma már nincs teljes körű támogatás a megbízható IoT rendszerekhez.

Hozzon létre olyan platformokat, amelyek lehetővé teszik a DevOps számára, hogy a megbízható IoT-rendszerek birodalmába léphessen, gazdagítva azt biztonsággal és rezilienciával, figyelembe véve az együttműködésen alapuló működéssel kapcsolatos kihívásokat. Megkönnyítette továbbá e koncepciók integrálását a DevOps olyan meglévő és új IoT-platformok számára történő kihasználása érdekében, mint a FIWARE (https://www.fiware.org/), a SOFIA (https://www.sophiaplatform.com/en/iot) és a TelluCloud (https://www.tellucloud.com/).

Ez a jelenlegi DevOps technikák kifejlesztésével valósult meg, amelyek támogatják az IoT-rendszerek működését, és olyan mechanizmusokat biztosítanak, amelyek biztosítják a megbízhatóságot. Ezzel az ENACT egy DevOps keretrendszert biztosított az intelligens IoT rendszerekhez.

Az intelligens közlekedésre (https://www.enact-project.eu/ucs.php) vonatkozó felhasználási esetben az ENACT értékelte a tárgyak internetének használatát a vonatok integritásának szabályozásában. Itt az infrastruktúra és az erőforrások drágaak, és a tervezés időigényes. A vasúti rendszerek használatát a biztonsági és védelmi irányelveknek megfelelően optimalizálták a terület kritikus és stratégiai jellemzői miatt, biztosítva a rakomány és az utasok megfelelő szállítását, és elkerülve a baleseteket.

IoT lánctalpas (https://cordis.europa.eu/project/id/779852)

A 2018 februárjában indított IoTCrawler a platformok közötti interoperabilitásra, az adatok és szolgáltatások integrálására szolgáló újrakonfigurálható megoldásokra, az adatvédelemre és a biztonságos algoritmusokra, valamint az IoT-rendszerek feltérképezésére, indexálására és keresésére

szolgáló mechanizmusokra összpontosított (https://iotcrawler.eu/).

Az IoTCrawler az Ipar 4.0-ra, az intelligens közösségekre és az intelligens (https://digital-strategy.ec.europa.eu/en/policies/smart-cities-and-communities) energiára összpontosító demonstrációkat nyújtott, amelyek a kutatás, az innováció és a technológiai fejlődés révén fejtenek ki hatást. A projekt a feltérképezés, a felfedezés, az indexelés, a szemantikai integráció és az IoT-ökoszisztéma biztonságának nyitott kihívásaival és kérdéseivel foglalkozott.

A projekt anomáliát észlelt egy vízgazdálkodási (https://iotcrawler.eu/index.php/project/iot-for-water-management-towards-intelligent-anomaly-detection/) esetben. Az intelligens fogyasztásmérők által gyűjtött adatok elemzése személyre szabhatja az ügyfelek visszajelzéseit, megelőzheti a vízpazarlást és észlelheti a kritikus helyzeteket. A közüzemi vállalatoknál az anomália észlelését gyakran elhanyagolják vagy elvégzik egy technikus, aki a generált adatok mennyisége miatt nem tudja ellenőrizni az összes métert. Ebben a forgatókönyvben az IoTCrawler két módszert vizsgált meg az idősorok anomáliájának észlelésére, hogy megtudja, melyik a legmegfelelőbb a vízfogyasztáshoz.

Az első egy ARIMA-alapú (Automatikus regresszív Integrált Moving Average) keretrendszer volt, amely olyan pontokat választ, amelyek nem illeszkednek egy ARIMA-folyamathoz, a másik pedig a HOT-SAX (Heuristically Order Time series with Symbolic Aggregate Enroximation) technika, amely diszkréten jeleníti meg az adatokat, és heurisztikus módon diszkriminálja azokat. Mindkét megközelítés hatékonynak bizonyult az anomáliák kimutatásában: 90%-uk az ARIMA-t, 80%-a pedig a HOT-SAX-ot használta.

Agy-IoT: Modellalapú keretrendszer az intelligens decentralizált IoT-rendszerek megbízható érzékeléséhez és működtetéséhez (https://www.brain-iot.eu/)

A Brain-IoT olyan forgatókönyvekre összpontosított, ahol a működtetést és az irányítást IoT-rendszerek támogatják. A cél egy olyan módszertan kidolgozása volt, amely támogatja a heterogén platformok decentralizált komposztálható szövetségeiben az együttműködő magatartást.

A Brain-IoT a szigorú megbízhatósági követelményeknek alávetett, üzleti szempontból kritikus és adatvédelmi szempontból érzékeny forgatókönyvekkel foglalkozott. Ebben a beállításban a BRAIN-IoT lehetővé tette az intelligens autonóm viselkedést, beleértve a komplex feladatokban együttműködő érzékelőket és aktuátorokat. Ezt az IoT-platformok alkalmazásával valósították meg, amelyek képesek támogatni a biztonságos és skálázható műveleteket különböző felhasználási esetekben, a platformok nyitott, decentralizált piacterének támogatásával.

Nyílt szemantikai modelleket használtak az interoperábilis műveletek kikényszerítésére, adatcserére és vezérlési funkciókra, amelyeket modellalapú fejlesztési eszközök támogatnak a prototípuskészítés és az interoperábilis megoldások integrációjának megkönnyítése érdekében. A biztonságos működést egy olyan keretrendszer biztosította, amely az elosztott IoT-forgatókönyvekben AAA funkciókat biztosít, az adatvédelmi tudatosság beágyazására szolgáló megoldásokkal együtt.

A megközelítések életképességét két felhasználási esetben, nevezetesen a szolgáltatási robotikában (http://www.brain-iot.eu/robotics/) és a kritikus infrastruktúra-gazdálkodásban (http://www.brain-iot.eu/scenarios/monitoring/), valamint a nagyszabású kísérleti kezdeményezésekkel együttműködésben végzett különböző koncepció-igazolási demonstrációk során bizonyították.

ITT VAN A SOFIE. Biztonságos nyílt föderáció az internet számára mindenhol (https://www.brain-iot.eu/)

A SOFIE projekt biztonságos és nyílt föderációs architektúrát és keretrendszert hozott létre. Megosztott főkönyvi technológiákat használt, hogy lehetővé tegye a működtetést, az auditálhatóságot, az intelligens szerződéseket, valamint az identitások és titkosítási kulcsok kezelését. Ez lehetővé tette a decentralizált megoldások szinte korlátlan skálázhatóságát.

A Sofie a föderáción keresztül foglalkozott az IoT széttagoltságával, ahol bármely IoT-platform csatlakozhat egy adapter létrehozásával. Az adatok a platformokon maradtak, és minden alkalmazásban felhasználhatók voltak a biztonsági politikák által meghatározott korlátokon belül. A projekt beépített adatvédelmet gyakorolt, biztosítva a végpontok közötti biztonságot, a kulcskezelést, az engedélyezést, az elszámoltathatóságot és az auditálhatóságot. A felhasználó az adatok feletti ellenőrzést akkor is megtarthatja, ha az adatokat a GDPR-nak megfelelő felhőben tárolják.

A Sofie olyan meglévő nyílt szabványokon, interfészeken és komponenseken dolgozott, mint a FIWARE, a W3C Web of Things (https://www.w3.org/WoT/) és a oneM2M, (https://www.onem2m.org/) a meglévő komponensek kiválasztása, újak kifejlesztése és egy olyan keretrendszerbe való begyűjtése, amely adminisztratívlag decentralizált, nyílt és biztonságos üzleti platformokat hoz létre.

A Sofie három különböző ágazatban három pilótában bizonyította a megközelítés gyakorlatiasságát: az élelmiszerlánc, a szerencsejátékok és az energiapiacok. A pilóták számára három üzleti platform jött létre, és az eredményeket a fő teljesítménymutatók alapján értékelték.

Szekér: Kognitív heterogén architektúra ipari IoT-hez (https://www.brain-iot.eu/)

A Chariot kognitív számítástechnikai platformot biztosított az IoT-rendszerek adatvédelmére, biztonságára és biztonságára vonatkozó egységes megközelítés támogatására.

Három kísérleti helyszín Athénban (Görögország), Dublinban (Írország) és Velencében (Olaszország) valós megoldásokat mutatott be az iparág referenciaalkalmazásai révén, azzal a céllal, hogy bizonyítsa, hogy a biztonságos, a magánélet védelme által közvetített és a dolgok internetének

biztonságával kapcsolatos követelmények teljesülnek; mérföldkő a következő generációs IoT-platformokra vonatkozó uniós ütemtervhez.

Csakúgy, mint a fizikai fenyegetések, mint például a terrorcselekmények, a repülőterek egyre inkább ki vannak téve a kiberfenyegetéseknek, amelyek a jövőben helyettesíthetik a fizikai terrorizmust, vagy egy támadás során kombinálhatók. A repülőterek elleni kombinált kiber- és fizikai támadások pusztító következményekkel járhatnak. A hagyományos IKT-infrastruktúrák, mint például a repülőtereken használt szerverek, asztali számítógépek és hálózatok más rendszerekhez kapcsolódnak, mint például a küldetéskritikus rendszerek (poggyászkezelés, környezetvédelmi ellenőrzés, hozzáférés-ellenőrzés és tűzvédelem).

Az athéni nemzetközi repülőtér használati esete a repülőtéri infrastruktúrák biztonságával foglalkozott, fokozva a létesítmények fizikai és kiberfenyegetésekkel szembeni védelmét. A Chariot növelte a repülőtér képességét a veszélyes helyzetek korai felismerésére és előrejelzésére, ezzel párhuzamosan csökkentve a repülőtéri működést megzavaró téves pozitív riasztásokat

Seriot (https://seriot-project.eu/)

Az európai ipar, az otthonok és a társadalom megtapasztalja az IoT biztonsági kockázatait, amelyek napi rendszerességgel kísérik a nem tesztelt technológiát. A platformok tartalmára és szolgáltatásának minőségére irányuló támadások gazdasági, energetikai és fizikai következményekkel járhatnak, amelyek túlmutatnak a hagyományos internetes biztonság hiányán a számítógépeken és a mobiltelefonokon. A Seriot kulcsfontosságú volt a biztonságos IoT platformok és hálózatok megvalósításában, bárhol és mindenhol.

A projekt egy adaptív intelligens szoftver által definiált hálózaton alapuló IoT keretrendszert fejlesztett ki biztonságos útválasztókkal, fejlett elemzésekkel és felhasználóbarát vizuális elemzéssel. A Seriot holisztikus, többrétegű módon optimalizálta a platformok és hálózatok információbiztonságát. A pilóták különböző felhasználási esetekben tesztelték a SerIoT technológiáját. Ezek magukban foglalták az intelligens szállítást és felügyeletet, az Ipar 4.0-n belüli rugalmas gyártást és más feltörekvő területeket, például az élelmiszerlánc logisztikáját, az m-egészségügyet és az intelligens hálózaton keresztüli energiát. Ezeken a technológiai fejlesztéseken és tesztágyakon keresztül a projekt egyedülálló hordozható szoftveralapú hálózatot hozott létre, amely Európa IoT-vel kapcsolatos sikereinek élén áll.

Kövesse a legújabb fejleményeket és tájékozódjon arról, hogyan vehet részt Ön is a folyamatokban!

- Kövesse a Bizottságnak a technológia és a digitális technológia terén végzett munkáját @DigitalEU (https://twitter.com/DigitalEU)

Legfrissebb hírek

PRESS RELEASE | 06 December 2022
EU to invest €13.5 billion in research and innovation for 2023-2024 (https://digital-strategy.ec.europa.eu/en/news/eu-invest-eu135-billion-research-and-innovation-2023-2024)

The Commission has adopted the main Horizon Europe work programme 2023-24, with around €13.5 billion to support researchers and innovators

in Europe to pursue breakthrough solutions for environmental, energy, digital and geopolitical challenges.

PRESS RELEASE | 09 Február 2022
A spektrum harmonizálása a jobb összekapcsoltság érdekében: készen áll az 5G-re és az innovációra (https://digital-strategy.ec.europa.eu/hu/news/harmonising-spectrum-enhanced-connectivity-ready-5g-and-innovation)

A Bizottság végrehajtási határozatokat fogadott el annak biztosítása érdekében, hogy az EU rádióspektrum-politikája megfeleljen a széles sáv és az innovatív digitális alkalmazások iránti növekvő keresletnek.

PRESS RELEASE | 02 Február 2022
Az EU új megközelítéssel törekszik arra, hogy az uniós szabványok világszerte meghatározóak legyenek, hirdessék az uniós értékeket, valamint előmozdítsák a reziliens, zöld és digitális egységes piacot (https://digital-strategy.ec.europa.eu/hu/news/new-approach-enable-global-leadership-eu-standards-promoting-values-and-resilient-green-and-digital)

A Bizottság ezen a héten új szabványosítási stratégiát terjesztett elő, amelyben felvázolja az egységes piacon belüli és globális szabványokkal kapcsolatos megközelítésünket.

PRESS RELEASE | 06 Szeptember 2021
A Bizottság tanulmányt tesz közzé a nyílt forrás európai gazdaságra gyakorolt hatásáról (https://digital-strategy.ec.europa.eu/hu/news/commission-publishes-study-impact-open-source-european-economy)

A Bizottság közzétette a nyílt forráskódú szoftverek és hardverek európai gazdaságra gyakorolt gazdasági hatását elemző tanulmány eredményeit.

Böngészés ebben a témában: Internet of Things

(https://digital-strategy.ec.europa.eu/hu/related-content?topic=125)

Kapcsolódó tartalom

Összkép

(https://digital-strategy.ec.europa.eu/hu/policies/internet-things-policy)
A dolgok internetére vonatkozó európai politika
(https://digital-strategy.ec.europa.eu/hu/policies/internet-things-policy)

Az EU aktívan együttműködik az iparral, a szervezetekkel és a tudományos körökkel annak érdekében, hogy kiaknázza a dolgok internetében rejlő lehetőségeket Európa-szerte és azon túl.

Lásd még

A dolgok következő generációja
(https://digital-strategy.ec.europa.eu/hu/policies/next-generation-internet-things)

A dolgok internete és az Edge Computing forradalmasíthatja a termelés és a folyamatok szervezésének és nyomon követésének módját a stratégiai értékláncokban.

(https://digital-strategy.ec.europa.eu/hu/policies/next-generation-internet-things)
A dolgok internetének feltérképezése innovációs klaszterek Európában
(https://digital-strategy.ec.europa.eu/hu/policies/iot-innovation-clusters)

A dolgok internete (IoT) európai klasztereiről készült tanulmány mélyebb megértést nyújt az e terület dinamikáiról, mozgatórugóiról és sikertényezőiről.

(https://digital-strategy.ec.europa.eu/hu/policies/iot-innovation-clusters)
Az európai mezőgazdasági ágazat digitalizálása
(https://digital-strategy.ec.europa.eu/hu/policies/digitalisation-agriculture)

Az európai mezőgazdasági ágazat digitalizációja képes forradalmasítani az ipart, előmozdítva a hatékonyságot, a fenntarthatóságot és a versenyképességet.

(https://digital-strategy.ec.europa.eu/hu/policies/digitalisation-agriculture)
