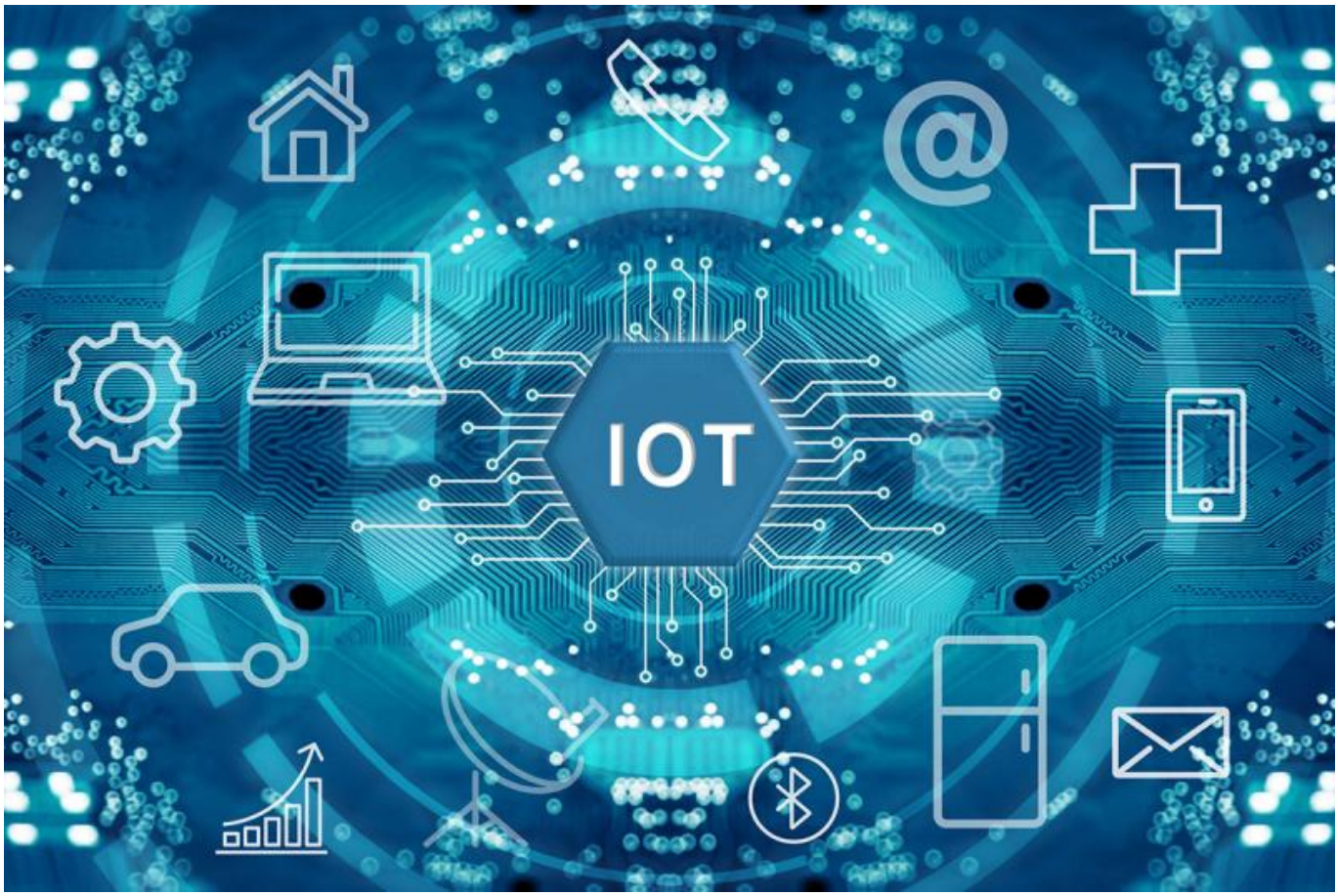
[Sikre løsninger til tingenes internet (https://digital-strategy.ec.europa.eu/da/policies/secure-internet-things)]

Kommissionen arbejder på at sikre mere robuste og modstandsdygtige sikkerhedsrammer for IoT-enheder og de netværk, som de er en del af.



© iStock by Getty Images -1184401187 Jae Young Ju

Tingenes internet (IoT)-enheder spiller en central rolle med hensyn til at sikre netværkenes modstandsdygtighed og holde data private og sikre. Men den stigende tendens i kompleksiteten af cybersikkerhedstrusler medfører et behov for mere robuste sikkerhedsrammer for IoT-enheder og -netværk.

For at løse dette problem fremlagde Europa-Kommissionen i december 2020 en omfattende strategi for cybersikkerhed for det digitale årti (https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade), der skitserede en vej mod et udbredt internet med sikre ting.

Sikkerhedsklyngen af IoT-projekter afhjælper manglerne ved enheder og netværk. Det gør den ved at udvikle sikre og modulopbyggede rammer, der kan integreres i nye og eksisterende løsninger til assisteret levevis, sundhedspleje, fremstilling, fødevareforsyning, energi og transport. Denne klynge består af 8 projekter, der beløber sig til 40 mio. EUR (ca. 5 mio. EUR hver) i EU-finansiering.

Klyngen har givet bemærkelsesværdige resultater i målsektorerne. Selv om applikationerne er

specialiserede, giver den open source-modulære udviklingstilgang, der anvendes af projekterne, mulighed for at genbruge modulerne i andre løsninger til et bredere spektrum af applikationer.

Projekter

SecureIoT: Prædiktiv sikkerhed for IoT-platforme og netværk af intelligente objekter (https://secureiot.eu/)

SecureIoT er en fælles indsats fra globale ledere inden for IoT-tjenester og cybersikkerhed for at sikre den næste generation af decentrale IoT-systemer. Disse spænder over flere netværk af smarte objekter, der implementerer en række åbne sikkerhedstjenester.

SecureIoT designede prædiktive sikkerhedstjenester i overensstemmelse med førende referencearkitekturer til IoT-applikationer, der tjener som grundlag for at specificere sikkerhedsbyggesten på både kanten og kernen i IoT-systemer. SecureIoT leverer mekanismer til indsamling, overvågning og forudsigelse af sikkerhedsdata, som tilbyder integrerede tjenester til risikovurdering, kontrol af overholdelse af forordninger ogdirektiver (generel forordning om databeskyttelse (https://ec.europa.eu/info/law/law-topic/data-protection_en), direktiv om sikkerhed i net- og informationssystemer (https://digital-strategy.ec.europa.eu/en/policies/nis-directive), e-databeskyttelsesdirektivet (https://digital-strategy.ec.europa.eu/en/policies/digital-privacy)) og udviklerstøtte.

SecureIoTs tjenester blev udfordret i markedsdrevne scenarier inden for områder som intelligent produktion og mobilitet. Deres implementeringer var baseret på åbent tilgængelige IoT-tjenester og partnerfællesskabet af platforme. I et brugstilfælde på smart living demonstrerede SecureIoT den tid, det tog at opdage angreb i IoT-aktiveret robotteknologi. Med 80 % af disse socialt hjælpende robotters (https://secureiot.eu/assisted-living)kritiske aktiver fundet i en sikkerhedsvidenbase tog det SecureIoT mindre end 10 sekunder at opdage uregelmæssigheder og under 5 minutter til en risikovurdering.

Semiotik: Smart end-to-end Massive IoT interoperabilitet, forbindelse og sikkerhed (https://www.semiotics-project.eu/)

Semiotik udviklede en mønsterdrevet ramme, der bygger på eksisterende IoT-platforme for at garantere sikker og semi-autonom adfærd i industrielle IoT-applikationer. Disse mønstre indkodede afhængigheden mellem sikkerhed, privatliv, pålidelighed og interoperabilitet af individuelle intelligente objekter.

Semiotik understøttede tilpasning på tværs af lag, herunder intelligente objekter, netværk og skyer,

der adresserer autonom adfærd i felt (kant) og infrastruktur (backend) lag. For at imødekomme behovet for kompleksitet og skalerbarhed inden for horisontale og vertikale områder udviklede SEMIoTICS programmerbare netværk og semantiske interoperabilitetsmekanismer. Dens praktiske virkning blev valideret ved hjælp af tre use cases inden for sundhedspleje, vedvarende energi og intelligent sensing.

Konsortiet bestod af interessenter i den europæiske industri, SMV'er og den akademiske verden, der dækkede hele værdikæden af IoT, lokale integrerede analyser og deres programmerbare konnektivitet til skyen med sikkerhed og privatliv.

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

DevOps-bevægelsen går ind for et sæt softwaretekniske værktøjer til at sikre en servicekvalitet, mens de udvikler komplekse systemer og fremmer hurtige innovationscyklusser og brugervenlighed. DevOps er blevet bredt vedtaget i softwareindustrien, men der er ingen fuldstændig støtte til pålidelige IoT-systemer i dag.

Vedtage etablerede platformaktiveringer for at give DevOps mulighed for troværdige IoT-systemer og berige det med sikkerhed og modstandsdygtighed under hensyntagen til udfordringer i forbindelse med kollaborativ aktivering. Det lettede også integrationen af disse koncepter for at udnytte DevOps til eksisterende og nye IoT-platforme som FIWARE (https://www.fiware.org/), SOFIA (https://www.sophiaplatform.com/en/iot) og TelluCloud (https://www.tellucloud.com/).

Dette blev opnået ved at udvikle nuværende DevOps-teknikker til støtte for driften af IoT-systemer, der giver et sæt mekanismer til at sikre troværdighed. Gennem dette gav ENACT en DevOps-ramme for intelligente IoT-systemer.

I en brugssag om intelligent transport (https://www.enact-project.eu/ucs.php) vurderede ENACT brugen af IoT i togintegritetskontrol. Her er infrastrukturen og ressourcerne dyre, og planlægningen er tidskrævende. Anvendelsen af jernbanesystemer blev optimeret efter sikkerheds- og sikkerhedsdirektiver på grund af områdets kritiske og strategiske karakteristika, der sikrede korrekt transport af gods eller passagerer og undgåelse af ulykker.

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

IoTCrawler, der blev lanceret i februar 2018, fokuserede (https://iotcrawler.eu/) på interoperabilitet på tværs af platforme, rekonfigurerbare løsninger til integration af data og tjenester, privatlivsbevidste og sikre algoritmer og mekanismer til crawling, indeksering og søgning i IoT-systemer.

IoTCrawler leverede demonstrationer med fokus på Industri 4.0, intelligente fællesskaber (https://digital-strategy.ec.europa.eu/en/policies/smart-cities-and-communities) og intelligent energi, hvilket giver effekt gennem forskning, innovation og teknologiudvikling. Projektet behandlede åbne udfordringer og problemer i forbindelse med crawling, opdagelse, indeksering, semantisk integration

og sikkerhed for et IoT-økosystem.

Projektet udførte anomali påvisning i en vandforvaltning (https://iotcrawler.eu/index.php/project/iot-for-water-management-towards-intelligent-anomaly-detection/) anvendelse tilfælde. Analysen af data indsamlet af intelligente målere kan tilpasse feedback til kunderne, forebygge vandspild og opdage kritiske situationer. I forsyningsvirksomheder er anomali detektion ofte forsømt eller udføres af en tekniker, der ikke kan kontrollere alle meter på grund af mængden af data genereret. I dette scenario undersøgte IoTCrawler to metoder til tidsserieanomaliregistrering for at se, hvilke der passer bedst til vandforbruget.

Den første var en ARIMA-baseret (Auto Regressive Integrated Moving Average) ramme, der vælger som de punkter, der ikke passer til en ARIMA proces, og den anden var HOT-SAX (Heuristically Order Time serie ved hjælp af Symbolic Aggregate Approximation) teknik, som diskret repræsenterer data og diskriminerer det ved hjælp af en heuristisk. Begge metoder viste sig at være effektive til påvisning af uregelmæssigheder: 90 % blev fundet ved hjælp af ARIMA og 80 % ved hjælp af HOT-SAX.

Hjerne-IoT: Modelbaseret ramme for pålidelig sensing og aktivering i intelligente decentrale IoT-systemer (https://www.brain-iot.eu/)

Brain-IoT fokuserede på scenarier, hvor aktivering og styring understøttes af IoT-systemer. Målet var at etablere en metode til støtte for samarbejdsadfærd i decentrale sammenslutninger af heterogene platforme.

Brain-IoT tacklede forretningskritiske og privatlivsfølsomme scenarier, der er underlagt strenge krav om pålidelighed. I denne indstilling aktiverede BRAIN-IoT intelligent autonom adfærd, der involverer sensorer og aktuatorer, der samarbejder om komplekse opgaver. Dette blev opnået ved at anvende IoT-platforme, der er i stand til at understøtte sikker og skalerbar drift til forskellige use cases, understøttet af en åben decentraliseret markedsplads for platforme.

Åbne semantiske modeller blev brugt til at håndhæve interoperable operationer, udveksle data og kontrolfunktioner, understøttet af modelbaserede udviklingsværktøjer for at lette prototypedannelse og integration af interoperable løsninger. Sikre operationer blev garanteret af en ramme, der giver AAA-funktioner i distribuerede IoT-scenarier, kombineret med løsninger til integration af privatlivets fred.

Strategiernes levedygtighed blev demonstreret i to anvendelsestilfælde, nemlig servicerobotter (http://www.brain-iot.eu/robotics/) og forvaltning af kritisk infrastruktur

(http://www.brain-iot.eu/scenarios/monitoring/), samt gennem forskellige proof-of-concept-demonstrationer i samarbejde med omfattende pilotinitiativer.

HVAD ER SOFIE? Sikker åben føderation til internettet overalt (https://www.brain-iot.eu/)

SOFIE-projektet skabte en sikker og åben føderationsarkitektur og ramme. Det brugte distributed ledger-teknologier til at muliggøre aktivering, auditabilitet, smarte kontrakter og forvaltning af identiteter og krypteringsnøgler. Dette muliggjorde decentrale løsninger med næsten ubegrænset skalerbarhed.

Sofie tog fat på fragmenteringen af IoT gennem føderation, hvor enhver IoT-platform kunne deltage ved at oprette en adapter. Data forblev på platformene og kunne bruges af alle applikationer inden for de grænser, der er fastsat af sikkerhedspolitikker. Projektet udøvede privatlivets fred gennem design, ved at levere end-to-end sikkerhed, nøglestyring, godkendelse, ansvarlighed og auditabilitet. Brugeren kan bevare kontrollen over deres data, også efter at dataene er blevet gemt i skyen i overensstemmelse med GDPR.

Sofie arbejdede på eksisterende åbne standarder, grænseflader og komponenter, såsom FIWARE, W3C Web of Things (https://www.w3.org/WoT/) og oneM2M (https://www.onem2m.org/), vælge eksisterende komponenter, udvikle nye, og indsamle dem i en ramme for at skabe administrativt decentrale, åbne og sikre forretningsplatforme.

Sofie har demonstreret det praktiske i deres tilgang ved at bruge den i tre piloter inden for tre forskellige sektorer: fødevarekæden, spil- og energimarkederne. Der er gennemført tre forretningsplatforme for piloterne, og resultaterne er blevet evalueret i forhold til de centrale resultatindikatorer.

Vogn: Kognitiv heterogen arkitektur til industriel IoT (https://www.brain-iot.eu/)

Chariot leverede en kognitiv computerplatform til støtte for en samlet tilgang til privatlivets fred, sikkerhed og sikkerhed i IoT-systemer.

Tre pilotanlæg i Athen (Grækenland), Dublin (Irland) og Venedig (Italien) demonstrerede realistiske løsninger ved hjælp af branchereferenceimplementeringer med det formål at påvise, at sikre, privatlivsformidlete og sikkerhedsmæssige IoT-krav er opfyldt; et springbræt til EU's køreplan for næste generation af IoT-platforme.

Ud over fysiske trusler såsom terrorhandlinger bliver lufthavne i stigende grad sårbare over for cybertrusler, som i fremtiden kan erstatte fysisk terrorisme eller kombineres under et angreb. Kombinerede cyberangreb og fysiske angreb på lufthavne kan få ødelæggende konsekvenser. Traditionelle IKT-infrastrukturer såsom servere, stationære computere og netværk, der anvendes i lufthavne, er forbundet til andre systemer, der anvendes i områder som missionskritiske systemer (bagagehåndtering, miljøkontrol, adgangskontrol og brandkontrol).

Brugssagen i Athens internationale lufthavn omhandlede sikkerheden i lufthavnsinfrastrukturer og styrkede beskyttelsen af faciliteter mod fysiske trusler og cybertrusler. Vogn forbedrede lufthavnens evne til tidlig opdagelse og forudsigelse af farlige situationer parallelt med at reducere falske positive alarmer, der forstyrrer lufthavnsoperationer

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

Europæisk industri, hjem og samfund oplever IoT-sikkerhedsrisici, der dagligt ledsager uprøvet teknologi. Angreb på indhold og kvaliteten af tjenester på platforme kan have økonomiske, energiske og fysiske konsekvenser, der går ud over det traditionelle internets manglende sikkerhed på computere og mobiltelefoner. Seriot var nøglen til at implementere sikre IoT-platforme og -netværk, hvor som helst og overalt.

Projektet udviklede en IoT-ramme baseret på et adaptivt smart softwaredefineret netværk med sikre routere, avanceret analyse og brugervenlig visuel analyse. Seriot optimerede informationssikkerheden i platforme og netværk på en holistisk, tværlags måde. Piloter testede SerIoTs teknologi i forskellige use cases. Disse omfattede intelligent transport og overvågning, fleksibel produktion inden for Industri 4.0 og andre nye områder som fødevarekædelogistik, m-sundhed og energi gennem det intelligente net. Gennem disse teknologiske udviklinger og testbænke leverede projektet et unikt bærbart softwarebaseret netværk, der kan stå i spidsen for Europas succes inden for IoT.

Følg med i den seneste udvikling, og læs mere om, hvordan du kan deltage.

- Følg Kommissionens arbejde med teknologi og digital @DigitalEU (https://twitter.com/DigitalEU)

Seneste nyheder

PRESS RELEASE | 06 December 2022
EU investerer 13.5 mia. EUR i forskning og innovation i perioden 2023-2024 (https://digital-strategy.ec.europa.eu/da/news/eu-invest-eu135-billion-research-and-innovation-2023-2024)

Kommissionen har vedtaget det vigtigste Horisont Europa-arbejdsprogram for 2023-24 med ca. 13.5 mia. EUR til støtte for forskere og innovatorer i Europa med henblik på at finde banebrydende

løsninger på miljømæssige, energimæssige, digitale og geopolitiske udfordringer.

PRESS RELEASE | 09 Februar 2022
Harmonisering af frekvensressourcer med henblik på øget konnektivitet: klar til 5G og innovation (https://digital-strategy.ec.europa.eu/da/news/harmonising-spectrum-enhanced-connectivity-ready-5g-and-innovation)

Kommissionen har vedtaget gennemførelsesafgørelser for at sikre, at EU's radiofrekvenspolitik imødekommer den stigende efterspørgsel efter bredbånd og innovative digitale applikationer.

PRESS RELEASE | 02 Februar 2022
Ny tilgang til at muliggøre EU-standarders globale lederskab til fremme af værdier og et modstandsdygtigt, grønt og digitalt indre marked (https://digital-strategy.ec.europa.eu/da/news/new-approach-enable-global-leadership-eu-standards-promoting-values-and-resilient-green-and-digital)

Kommissionen har i denne uge fremlagt en ny standardiseringsstrategi, der skitserer vores tilgang til standarder både på det indre marked og globalt.

PRESS RELEASE | 06 September 2021
Kommissionen offentliggør en undersøgelse af Open Sources indvirkning på den europæiske økonomi (https://digital-strategy.ec.europa.eu/da/news/commission-publishes-study-impact-open-source-european-economy)

Kommissionen har offentliggjort resultaterne af en analyse af de økonomiske konsekvenser af open source-software og Hardware for den europæiske økonomi.

Søg på Internet of Things

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

Se også

Det store billede

(https://digital-strategy.ec.europa.eu/da/policies/internet-things-policy)
EU's politik om tingenes internet
(https://digital-strategy.ec.europa.eu/da/policies/internet-things-policy)

EU samarbejder aktivt med industrien, organisationer og den akademiske verden om at frigøre potentialet i tingenes internet i og uden for Europa.

Se også

Næste generation Internet of Things
(https://digital-strategy.ec.europa.eu/da/policies/next-generation-internet-things)

Fremtidens Internet of Things og Edge Computing kan revolutionere den måde, hvorpå produktion og processer organiseres og overvåges på tværs af strategiske værdikæder.

(https://digital-strategy.ec.europa.eu/da/policies/next-generation-internet-things)
Kortlægning af innovationsklynger på tingenes internet i Europa
(https://digital-strategy.ec.europa.eu/da/policies/iot-innovation-clusters)

En undersøgelse af tingenes internetklynger (IoT) i Europa giver en dybere forståelse af dynamikken, drivkræfterne og succesfaktorerne på dette område.

(https://digital-strategy.ec.europa.eu/da/policies/iot-innovation-clusters)
Digitalisering af den europæiske landbrugssektor
(https://digital-strategy.ec.europa.eu/da/policies/digitalisation-agriculture)

Digitaliseringen af den europæiske landbrugssektor har potentiale til at revolutionere industrien og fremme effektivitet, bæredygtighed og konkurrenceevne.

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