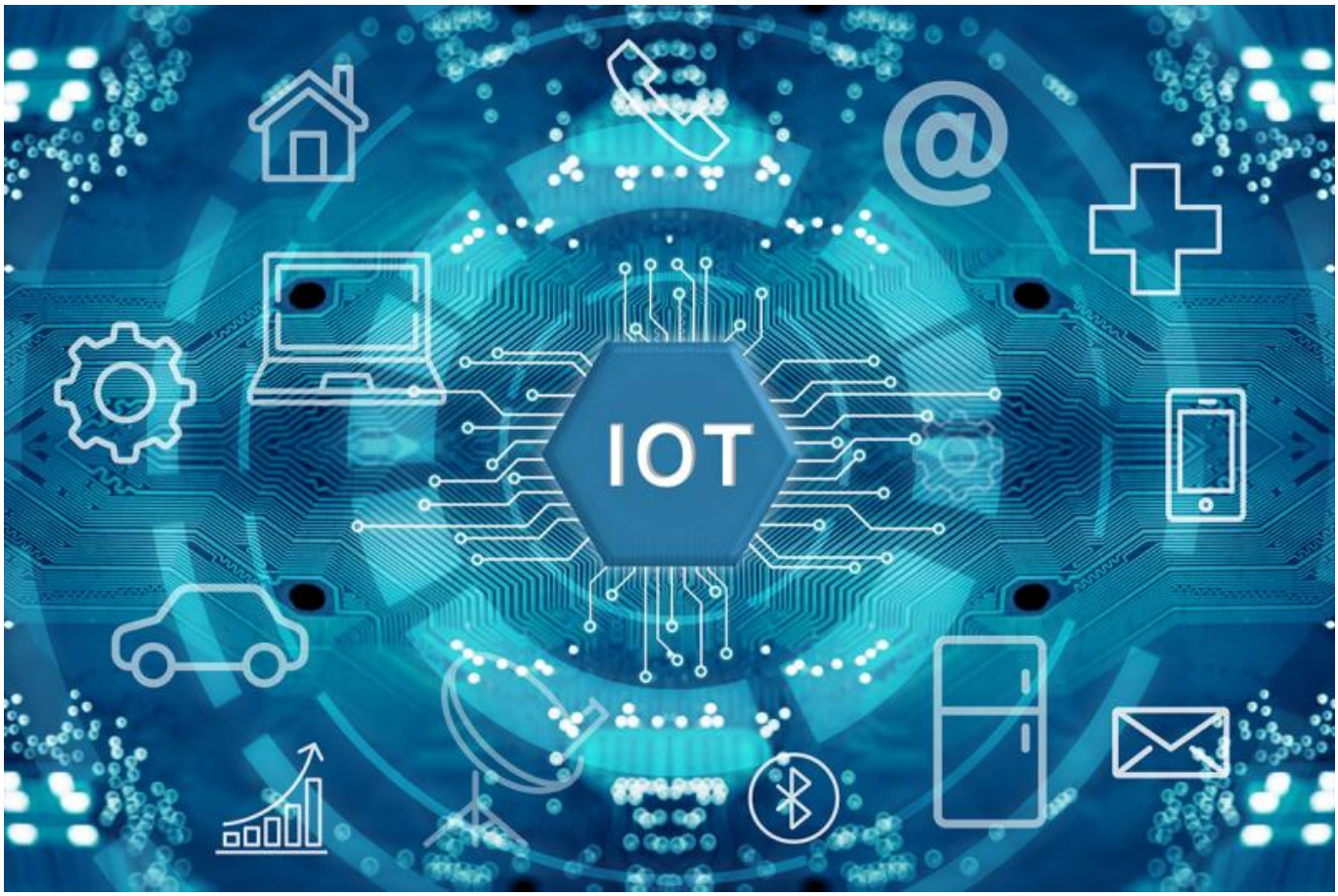
[Soluções seguras para a Internet das Coisas (https://digital-strategy.ec.europa.eu/pt/policies/secure-internet-things)]

A Comissão está a trabalhar no sentido de garantir quadros de segurança mais sólidos e resilientes para os dispositivos da Internet das coisas e as redes de que fazem parte.



© iStock by Getty Images -1184401187 Jae Young Ju

Os dispositivos Internet das Coisas (IdC) desempenham um papel fundamental para garantir a resiliência das redes e manter os dados privados e seguros. No entanto, a tendência crescente na complexidade das ameaças à cibersegurança traz a necessidade de estruturas de segurança mais robustas para dispositivos e redes de Internet das coisas.

Para abordar esta questão, a Comissão Europeia apresentou, em dezembro de 2020, uma estratégia global de cibersegurança para a Década Digital (https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade), que define um caminho rumo a uma Internet generalizada de coisas seguras.

O cluster de segurança de projetos de IoT aborda as deficiências de dispositivos e redes. Fá-lo através do desenvolvimento de quadros seguros e modulares que possam ser integrados em soluções novas e existentes para a vida assistida, os cuidados de saúde, a indústria transformadora, o abastecimento alimentar, a energia e os transportes. Este agregado é composto por 8 projetos, num montante de 40 milhões de EUR (cerca de 5 milhões de EUR cada) de financiamento da UE.

O agregado produziu resultados dignos de nota em setores-alvo. Embora as aplicações sejam especializadas, a abordagem de desenvolvimento modular de código aberto utilizada pelos projetos permite que os módulos sejam reutilizados em outras soluções para um espetro mais amplo de aplicações.

Projetos

SecureIoT: Segurança Preditiva para Plataformas de IoT e Redes de Objetos Inteligentes (https://secureiot.eu/)

SecureIoT é um esforço conjunto de líderes globais em serviços de IoT e segurança cibernética para proteger a próxima geração de sistemas de IoT descentralizados. Estes abrangem várias redes de objetos inteligentes, implementando uma gama de serviços de segurança abertos.

O SecureIoT projetou serviços de segurança preditivos em linha com arquiteturas de referência de ponta para aplicações IoT, que servem como base para especificar os blocos de construção de segurança tanto na borda quanto no núcleo dos sistemas IoT. O SecureIoT fornece mecanismos de coleta, monitoramento e previsão de dados de segurança, que oferecem serviços integrados de avaliação de riscos, auditoria de conformidade com regulamentos e diretivas (Regulamento Geral de Proteção de Dados (https://ec.europa.eu/info/law/law-topic/data-protection_en), Diretiva relativa à segurança das redes e sistemas de informação (https://digital-strategy.ec.europa.eu/en/policies/nis-directive), Diretiva Privacidade (https://digital-strategy.ec.europa.eu/en/policies/digital-privacy)Eletrônica) e suporte ao desenvolvedor.

Os serviços da SecureIoT foram desafiados em cenários orientados para o mercado em áreas como fabrico inteligente e mobilidade. Suas implantações foram baseadas em serviços de IoT disponíveis abertamente e na comunidade parceira de plataformas. Em um caso de uso em vida inteligente, o SecureIoT demonstrou o tempo necessário para detetar ataques em robótica habilitada para IoT. Com 80 % dos ativos críticos desses robôs (https://secureiot.eu/assisted-living)de assistência social encontrados em uma base de conhecimento de segurança, o SecureIoT demorou menos de 10 segundos para detetar efetivamente anomalias e menos de 5 minutos para uma avaliação de risco.

Semiótica: Interoperabilidade, conectividade e segurança maciças de IoT inteligentes de ponta a ponta (https://www.semiotics-project.eu/)

A semiótica desenvolveu uma estrutura baseada em padrões, com base em plataformas de IoT existentes para garantir um comportamento seguro e semiautonômico em aplicações industriais de

IoT. Esses padrões codificaram as dependências entre segurança, privacidade, confiabilidade e interoperabilidade de objetos inteligentes individuais.

A semiótica suportou a adaptação de camadas cruzadas, incluindo objetos inteligentes, redes e nuvens, abordando o comportamento autonômico em camadas de campo (borda) e infraestrutura (backend). Para atender às necessidades de complexidade e escalabilidade dentro de domínios horizontais e verticais, a SEMIoTICS desenvolveu mecanismos programáveis de rede e interoperabilidade semântica. Sua praticidade foi validada utilizando três casos de uso em saúde, energia renovável e sensoriamento inteligente.

O consórcio era constituído por partes interessadas da indústria europeia, das PME e do mundo académico, abrangendo toda a cadeia de valor da IdC, análises integradas locais e a sua conectividade programável à nuvem com segurança e privacidade.

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

O movimento DevOps defende um conjunto de ferramentas de engenharia de software para garantir uma qualidade de serviço enquanto evolui sistemas complexos e promovendo ciclos de inovação rápidos e facilidade de uso. DevOps tem sido amplamente adotado na indústria de software, mas não há nenhum suporte completo para sistemas de IoT fiáveis hoje.

Implemente facilitadores de plataforma estabelecidos para permitir que o DevOps entre no âmbito de sistemas de IoT fiáveis, enriquecendo-o com segurança e resiliência, tendo em conta os desafios relacionados com a atuação colaborativa. Ele também facilitou a integração desses conceitos para alavancar DevOps para plataformas de IoT existentes e novas como FIWARE (https://www.fiware.org/), SOFIA (https://www.sophiaplatform.com/en/iot) e TelluCloud (https://www.tellucloud.com/).

Isso foi conseguido através do desenvolvimento de técnicas atuais de DevOps para apoiar a operação de sistemas de IoT, fornecendo um conjunto de mecanismos para garantir a confiabilidade. Através disso, a ENACT forneceu um framework DevOps para sistemas inteligentes de IoT.

Num caso de utilização do transporte inteligente (https://www.enact-project.eu/ucs.php), a ENACT avaliou a utilização da IdC no controlo da integridade do comboio. Aqui, a infraestrutura e os recursos utilizados são caros e o planejamento é demorado. A utilização dos sistemas ferroviários foi otimizada, seguindo as diretivas de segurança e proteção devido às características críticas e estratégicas do domínio, assegurando o transporte adequado de carga ou passageiros e evitando acidentes.

Esteira rolante de**IoT** (https://cordis.europa.eu/project/id/779852)

Lançado em fevereiro de 2018, o (https://iotcrawler.eu/) IoTCrawler concentrou-se na interoperabilidade entre plataformas, soluções reconfiguráveis para a integração de dados e serviços,

algoritmos seguros e conscientes da privacidade e mecanismos de rastreamento, indexação e pesquisa em sistemas IoT.

IoTCrawler forneceu demonstrações com foco na Indústria 4.0, comunidades inteligentes (https://digital-strategy.ec.europa.eu/en/policies/smart-cities-and-communities) e energia inteligente, proporcionando impacto através da pesquisa, inovação e avanço tecnológico. O projeto abordou desafios e problemas abertos em rastreamento, descoberta, indexação, integração semântica e segurança para um ecossistema de IoT.

O projeto realizou a deteção de anomalias num caso de utilização da gestão da água (https://iotcrawler.eu/index.php/project/iot-for-water-management-towards-intelligent-anomaly-detection/). A análise de dados coletados por contadores inteligentes pode personalizar o feedback para os clientes, prevenir o desperdício de água e detetar situações críticas. Em empresas de serviços públicos, a deteção de anomalias é frequentemente negligenciada ou feita por um técnico que não pode verificar todos os metros devido ao volume de dados gerados. Neste cenário, o IoTCrawler examinou dois métodos para deteção de anomalias em séries temporais para ver quais são os mais adequados para o consumo de água.

A primeira foi uma estrutura baseada em ARIMA (Auto Regressive Integrated Moving Average) que seleciona como os pontos que não se encaixam em um processo ARIMA, e o outro foi a técnica HOT-SAX (heuristically Order Time usando Symbolic Aggregate Approximation), que representa discretamente dados e a discrimina usando uma heurística. Ambas as abordagens revelaram-se eficazes na deteção de anomalias: 90 % foram encontrados com ARIMA e 80 % com HOT-SAX.

IoT do cérebro: Estrutura baseada em modelos para deteção e atuação fiáveis em sistemas de IoT inteligentes e descentralizados (https://www.brain-iot.eu/)

Brain-IoT focada em cenários onde a atuação e o controle são suportados por sistemas de IoT. O objetivo era estabelecer uma metodologia de apoio ao comportamento cooperativo em federações descentralizadas e composíveis de plataformas heterogéneas.

A brain-IoT abordou cenários críticos para negócios e sensíveis à privacidade, sujeitos a rigorosos requisitos de confiabilidade. Nesta configuração, a BRAIN-IoT possibilitou um comportamento autônomo inteligente envolvendo sensores e atuadores cooperando em tarefas complexas. Isso foi conseguido empregando plataformas de IoT, capazes de suportar operações seguras e escaláveis para vários casos de uso, apoiadas por um mercado aberto e descentralizado de plataformas.

Foram utilizados modelos semânticos abertos para impor operações interoperáveis, trocar dados e

funcionalidades de controlo, apoiados por ferramentas de desenvolvimento baseadas em modelos para facilitar a criação de protótipos e a integração de soluções interoperáveis. Operações seguras foram garantidas por uma estrutura que fornece recursos AAA em cenários de IoT distribuídos, juntamente com soluções para incorporar a consciência de privacidade.

A viabilidade das abordagens foi demonstrada em dois casos de utilização, nomeadamente a robótica (http://www.brain-iot.eu/robotics/) de serviços e a gestão de infraestruturas críticas (http://www.brain-iot.eu/scenarios/monitoring/), bem como através de várias demonstrações de prova de conceito em colaboração com iniciativas-piloto em grande escala.

SOFIE: Federação aberta segura para Internet em todos os lugares (https://www.brain-iot.eu/)

O projeto SOFIE criou uma arquitetura e uma estrutura de federação seguras e abertas. Ele usou tecnologias de livro-razão distribuído para permitir atuação, auditabilidade, contratos inteligentes e gerenciamento de identidades e chaves de criptografia. Isso possibilitou soluções descentralizadas com escalabilidade quase ilimitada.

A Sofie abordou a fragmentação da IoT através da federação, onde qualquer plataforma de IoT poderia se juntar criando um adaptador. Os dados permaneceram nas plataformas e foram utilizáveis por todas as aplicações dentro dos limites estabelecidos pelas políticas de segurança. O projeto exercia a privacidade desde a conceção, fornecendo segurança de ponta a ponta, gestão de chaves, autorização, responsabilização e auditabilidade. O utente pode reter o controle sobre seus dados também após os dados terem sido armazenados na nuvem em conformidade com o GDPR.

A Sofie trabalhou em padrões, interfaces e componentes abertos existentes, como FIWARE, W3C Web of Things (https://www.w3.org/WoT/) e oneM2M (https://www.onem2m.org/), selecionando componentes existentes, desenvolvendo novos e coletando-os em uma estrutura para criar plataformas de negócios descentralizadas, abertas e seguras.

A Sofie demonstrou a praticidade da sua abordagem, utilizando-a em três projetos-piloto em três setores diferentes: a cadeia alimentar, o jogo e os mercados de energia. Foram realizadas três plataformas empresariais para os projetos-piloto e os resultados foram avaliados em função dos principais indicadores de desempenho.

Carruagem: Arquitetura cognitiva heterogênea para IoT industrial (https://www.brain-iot.eu/)

A Chariot forneceu uma plataforma de computação cognitiva para apoiar uma abordagem unificada em relação à privacidade, segurança e segurança dos sistemas de IoT.

Três locais-piloto em Atenas (Grécia), Dublim (Irlanda) e Veneza (Itália) demonstraram soluções realistas através de implementações de referência do setor, com o objetivo de demonstrar que são cumpridos os imperativos da IdC seguros, mediados pela privacidade e pela segurança; um trampolim para o roteiro da UE para as plataformas da próxima geração da IdC.

Para além das ameaças físicas, como os atos de terrorismo, os aeroportos estão a tornar-se cada vez mais vulneráveis às ciberameaças, que, no futuro, poderão substituir o terrorismo físico ou ser combinadas durante um ataque. Os ataques combinados cibernéticos e físicos aos aeroportos podem ter consequências devastadoras. As infraestruturas TIC tradicionais, como servidores, computadores de secretária e redes utilizadas nos aeroportos, estão ligadas a outros sistemas utilizados em áreas como sistemas de missão crítica (manuseamento de bagagem, controlo ambiental, controlo de acesso e controlo de incêndios).

O caso de utilização no aeroporto internacional de Atenas abordou a segurança das infraestruturas aeroportuárias, reforçando a proteção das instalações contra ameaças físicas e cibernéticas. A carruagem aumentou a capacidade do aeroporto de deteção precoce e previsão de situações perigosas, em paralelo com a redução de alarmes falsos positivos que perturbam as operações aeroportuárias

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

A indústria, os lares e a sociedade europeia enfrentam riscos de segurança da Internet das coisas que acompanham diariamente a tecnologia não testada. Os ataques ao conteúdo e à qualidade do serviço das plataformas podem ter consequências económicas, energéticas e físicas que vão além da falta de segurança da Internet tradicional em computadores e telemóveis. O SerIoT foi fundamental para implementar plataformas e redes de IoT seguras, em qualquer lugar e em qualquer lugar.

O projeto desenvolveu um framework de IoT ganza em uma rede definida por software inteligente adaptável com roteadores seguros, análises avançadas e análises visuais fáceis de usar. A SerIoT otimizou a segurança da informação em plataformas e redes de forma holística e transversal. Os pilotos testaram a tecnologia da SerIoT em vários casos de uso. Estes incluíram transportes e vigilância inteligentes, fabrico flexível no âmbito da Indústria 4.0 e outros domínios emergentes, como a logística da cadeia alimentar, a saúde móvel e a energia através da rede inteligente. Através destes desenvolvimentos tecnológicos e bancos de ensaio, o projeto proporcionou uma rede portátil única baseada em software que pode liderar o sucesso da Europa na IdC.

Seguir os últimos progressos e informar-se sobre as possibilidades de participação

- Acompanhar o trabalho da Comissão em matéria de tecnologia e digital @DigitalEU (https://twitter.com/DigitalEU)

Últimas notícias

PRESS RELEASE | 06 Dezembro 2022
UE investirá 13,5 mil milhões de euros em investigação e inovação para 2023-2024 (https://digital-strategy.ec.europa.eu/pt/news/eu-invest-eu135-billion-research-and-innovation-2023-2024)

A Comissão adotou o principal programa de trabalho do Horizonte Europa para 2023-24, com cerca de 13,5 mil milhões de EUR para apoiar os

investigadores e inovadores na Europa na procura de soluções revolucionárias para os desafios ambientais, energéticos, digitais e geopolíticos.

PRESS RELEASE | 09 Fevereiro 2022
Harmonização do espetro para uma maior conectividade: pronto para a tecnologia 5G e a inovação (https://digital-strategy.ec.europa.eu/pt/news/harmonising-spectrum-enhanced-connectivity-ready-5g-and-innovation)

A Comissão adotou decisões de execução para assegurar que a política da UE em matéria de espetro de radiofrequências satisfaça a procura crescente de banda larga e de aplicações digitais inovadoras.

PRESS RELEASE | 02 Fevereiro 2022
Uma nova abordagem para garantir a liderança mundial das normas da UE promovendo os valores e um mercado único resiliente, verde e digital (https://digital-strategy.ec.europa.eu/pt/news/new-approach-enable-global-leadership-eu-standards-promoting-values-and-resilient-green-and-digital)

A Comissão apresentou esta semana uma nova estratégia de normalização que define a nossa abordagem em matéria de normas no mercado único, bem como a nível mundial.

PRESS RELEASE | 06 Setembro 2021
Comissão publica estudo sobre o impacto da fonte aberta na economia europeia (https://digital-strategy.ec.europa.eu/pt/news/commission-publishes-study-impact-open-source-european-economy)

A Comissão publicou os resultados de um estudo que analisa o impacto económico do software e do hardware de fonte aberta na economia europeia.

Percorrer por tema

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

Conteúdo relacionado

Visão geral

(https://digital-strategy.ec.europa.eu/pt/policies/internet-things-policy)
Política da Europa para a Internet das Coisas
(https://digital-strategy.ec.europa.eu/pt/policies/internet-things-policy)

A UE coopera ativamente com a indústria, as organizações e o meio académico para libertar o potencial da Internet das coisas em toda a Europa e fora dela.

Ver também

A próxima geração de Internet das Coisas
(https://digital-strategy.ec.europa.eu/pt/policies/next-generation-internet-things)

A futura Internet das Coisas e a Computação de Borda podem revolucionar a forma como a produção e os processos são organizados e monitorados através de cadeias de valor estratégicas.

(https://digital-strategy.ec.europa.eu/pt/policies/next-generation-internet-things)
Mapeamento dos polos de inovação da Internet das coisas na Europa
(https://digital-strategy.ec.europa.eu/pt/policies/iot-innovation-clusters)

Um estudo realizado sobre os agregados da Internet das Coisas (IdC) na Europa proporciona uma compreensão mais aprofundada da dinâmica, dos motores e dos fatores de sucesso neste domínio.

(https://digital-strategy.ec.europa.eu/pt/policies/iot-innovation-clusters)
A digitalização do setor agrícola europeu
(https://digital-strategy.ec.europa.eu/pt/policies/digitalisation-agriculture)

A digitalização do setor agrícola europeu tem potencial para revolucionar a indústria, promovendo a eficiência, a sustentabilidade e a competitividade.

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