Internet Industrial das Coisas: Principais vulnerabilidades e uso de Blockchain

Carlos Alexandre Rodrigues Bernardino

carlos.bernardino@fatec.sp.gov.br

Faculdade de Tecnologia Santana de Parnaíba (FATEC) – SP – Brasil

Resumo

Este artigo visa à elaboração de uma análise transparente sobre um dos pilares da Industria 4.0 a Internet das Coisas Industrial (IIoT) e as possíveis implicações de segurança que ela pode trazer. Essa tecnologia por estar em constante evolução cresce o número de ameaças quando dispositivos conectados podem ser usados de outras maneiras que não a sua originalmente projetada. Com isso abordando aspectos de segurança foi implantado uma rede blockchain para mitigação de vulnerabilidades e ataques. O final da elaboração deste trabalho, observou-se que o tema escolhido é de grande importância, principalmente no ambiente empresarial devido a comunicação entre as máquinas, garantindo confidencialidade, integridade e disponibilidade.

Palavras Chaves: Ataques; IIoT; Blockchain; Segurança; Vulnerabilidades.

Abstract

This article aims to provide a transparent analysis of one of the pillars of Industry 4.0 the Industrial Internet of Things (IIoT) and the possible security implications it can bring. As this technology is constantly evolving, the number of threats increases when connected devices can be used in ways other than the way they were originally designed. With that, addressing security aspects, a blockchain network was deployed to mitigate vulnerabilities and attacks. At the end of the elaboration of this work, it was observed that the chosen theme is of great importance, mainly in the business environment due to the communication between the machines, guaranteeing confidentiality, integrity and availability.

Keywords: Attacks; IIoT; Blockchain; Safety; Vulnerabilities

Introdução

O ambiente da Industria 4.0 é definido por um de seus pilares a automação industrial decorrente de dispositivos IIoT que vão desde de simples sensores até complexos robôs (Costa et al, 2020) e com o constante avanço dessa tecnologia as questões de segurança das informações trafegadas se torna um desafio a ser tratado pelo fato das ameaças e vulnerabilidades crescerem também.

A Internet das Coisas (do inglês Internet of Things (IoT)) emergiu dos avanços de várias áreas como sistemas embarcados, microeletrônica, comunicação e sensoriamento. De fato, a IoT tem beneficiado o ambiente doméstico quanto industrial, devido ao seu potencial de uso nas mais diversas áreas e inúmeras aplicações (Kadow e Camargo, 2016).

Neste contexto se insere o projeto FASTEN, um framework para a Industria 4.0 responsável pela integração de dispositivos IIoT com ferramentas de análise e de otimização (Costa et al. 2020). E o uso do Hyperledger Fabric uma plataforma projetada

para o ambiente empresarial, baseada na premissa de contratos inteligentes (chaincode), em uma rede blockchain privada para uma camada extra de segurança.

Como visto, são vários os desafios para a implantação definitiva da IoT e pode se afirmar que a segurança da informação é o principal obstáculo dentre eles, pois é o que oferece maior dificuldade de ser resolvido, já que não existem sistemas e dispositivos 100% seguros (Moraes, 2010). Porém o entendimento das vulnerabilidades e a forma como os ataques são realizados, possibilitam planejar a implantação da IoT de forma a maximizar a proteção dos dados coletados e minimizar os riscos de ataques e vulnerabildades.

2. Referencial teórico

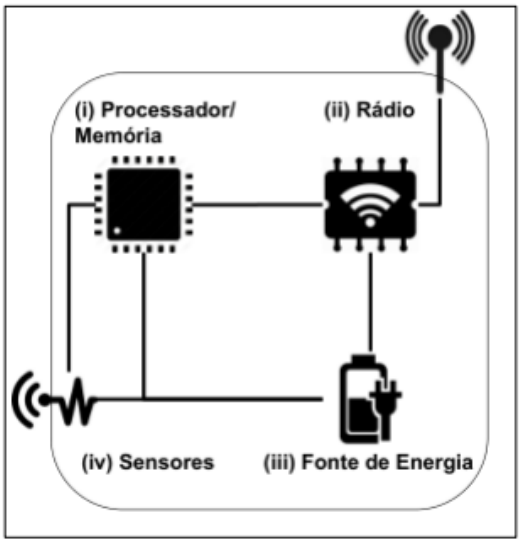
2.1 IIoT

A Indústria 4.0 está trazendo um de seus pilares a internet industrial das coisas (IIoT) para as empresas, consiste em máquinas que variam de sensores a complexos robôs industriais conectadas à internet, interagindo entre si, coletando e analisando dados, podendo armazená-los em nuvem, permitindo ainda, identificar e solucionar problemas sem a interferência humana, tomando decisões eficientes sozinhas (Costa et al, 2020).

2.1.1 Arquitetura

A arquitetura básica do IoT é composta por quatro elementos: processador/memória, comunicação, fonte de energia e sensores/atuadores (Santos et al, 2016). A Figura 1 apresenta esta arquitetura e a interligação entre seus componentes, os quais são descritos a seguir:

Figura 1 – Arquitetura dos Dispositivos IoT



Fonte: Santos et al (2016)

(i)Unidade(s) de Processamento/Memoria

Inclui a unidade de processamento como, por exemplo, microcontroladores, processadores e FPGAs, responsáveis por executar algoritmos locais nos objetos inteligentes (Santos et al, 2016).

(ii)Interface(s) de comunicação

Diz respeito às diversas técnicas utilizadas para conectar os dispositivos IoT. Também desempenha papel importante no consumo de energia dos objetos sendo, portanto, um fator crítico. Algumas das tecnologias usadas são WiFi, Bluetooth, Ethernet e RFID (Santos et al, 2016).

(iii)Fonte de energia

Responsável por fornecer energia aos dispositivos IoT, a função da fonte é converter a corrente alternada em corrente contínua que já está na tensão correta usada pelo dispositivo (Santos et al, 2016).

(iv)Unidade(s) de sensor(es)/atuador(es)

sensores coletam informações sobre o contexto onde os objetos se encontram e, em seguida, armazenam/encaminham esses dados para clouds ou centros de armazenamento. Atuadores podem manipular o ambiente ou reagir de acordo com os dados lidos (Santos et al, 2016).

2.1.2 Comunicação

Para que possa haver a interconectividade total entre todos os dispositivos “coisas”, é necessária a utilização de protocolos de comunicação e, seus padrões, permitindo uma comunicação transparente entre os dispositivos (Santos et al, 2016). Esta seção trata das principais tecnologias de comunicação utilizadas em IoT, identificando as características mais relevantes de cada uma delas.

2.1.2.1 Ethernet

O padrão Ethernet (IEEE 802.3) foi oficializado em 1983 pelo IEEE e está presente em grande parte das redes locais com fio existentes atualmente. Sua popularidade se deve à simplicidade, facilidade de adaptação, manutenção e custo. Atualmente, existem dois tipos de cabos: par trançado e fibra óptica, que oferecem taxas de comunicação diferentes. Os cabos de par trançado podem atingir taxas de até 1 Gbps (categoria 5), limitados a 100 m (para distâncias maiores é necessário o uso de repetidores). Os cabos de fibra óptica alcançam taxas de 10 Gbps, limitados a 2000 m (Tanenbaum, 2011). O uso do padrão Ethernet é sugerido para dispositivos fixos.

2.1.2.2 Wireless Fidelity (Wi-Fi)

A tecnologia Wi-Fi é uma solução de comunicação sem fio, popular no cotidiano residencial, industrial, comercial e até em espaços públicos das cidades. O padrão IEEE 802.11 (Wi-Fi) define um conjunto de padrões de transmissão e codificação. Desde o seu lançamento em 1997, já foram propostas novas versões do padrão IEEE 802.11 e, atualmente, a versão IEEE 802.11ac prevê taxas de comunicação de 600 Mbps ou 1300 Mbps (Tanenbaum, 2011).

O Wi-Fi possui algumas vantagens, como alcance de conexão e vazão, o que o torna adequado para navegação na Internet em dispositivos móveis, como smartphones e tablets. A principal desvantagem do Wi-Fi é o maior consumo de energia, quando comparado com outras tecnologias de comunicação sem fio (Santos et al, 2016).

2.1.2.3 3G/4G

Os padrões de telefonia celular 3G/4G também podem ser aplicados à IoT. Projetos que precisam alcançar grandes distâncias podem aproveitar as redes de telefonia celular 3G/4G. Por outro lado, o consumo energético da tecnologia 3G/4G é alto em

comparação a outras tecnologias (Santos et al, 2016). No Brasil, as frequências utilizadas para o 3G são 1900 MHz e 2100 MHz Universal Mobile Telecommunications System, ou "Sistema Universal de Telecomunicações Móveis" (UMTS), enquanto o padrão 4G Long Term Evolution (LTE) utiliza a frequência de 2500 MHz. A taxa de comunicação alcançada no padrão 3G é de 1 Mbps e no padrão 4G 10 Mbps (Santos et al, 2016).

2.1.3 Principais Desafios

A tecnologia IoT possibilita diversas variedades de aplicações podendo beneficiar tanto ambientes domésticos quanto industriais (Santos et al., 2016). Porém com o crescimento dessa tecnologia novos desafios surgem, assim se faz necessário conhecer e entender a fim de se obter um melhor planejamento para implantação e medidas de segurança.

A maioria dos problemas relacionados a segurança em uma rede de computadores também se aplicam aos dispositivos IoT, inclusive, maioria desses problemas é devido os dispositivos apresentarem limitações de hardware e o meio de comunicação que eles utilizam, geralmente sem fio (Andrea; Chrysostomou; Hadjichristofi, 2015).

O surgimento de novos dispositivos dedicados a IoT que podem ser comprometidos apresenta uma grande preocupação para os fabricantes, indústrias e consumidores. O problema se torna crítico quando dispositivos vulneráveis possam ser invadidos e utilizados em ***botnets*** prejudicando redes adequadamente protegidas. A fim de mitigar possíveis falhas de segurança para implantação e utilização da tecnologia IoT é necessário conhecer as vulnerabilidades presentes atualmente nos dispositivos (Paul, 2019).

Uma vulnerabilidade ou falha em uma rede ocorre por diversos fatores, como, por exemplo, problema em uma aplicação, serviço, vírus, erro humano ao divulgar senhas indiscriminadamente (CERT.BR, 2012). Há também ameaças mais perigosas como sabotagem ou espionagem de banco de dados para obter informações importantes da empresa (Moraes, 2010).

2.1.4 Principiais Vulnerabilidades

A Open Web Application Security Project (OWASP), ou “Projeto Aberto de Segurança em Aplicações Web” é uma comunidade online com o objetivo de ajudar fabricantes, desenvolvedores e consumidores a entender melhor as questões de segurança associadas à IoT, criando e disponibilizando de forma gratuita artigos, metodologias, documentação, ferramentas e tecnologias no campo da segurança de aplicações web, permitindo que os usuários, tomem as melhores decisões de segurança ao criar, implantar ou avaliar tecnologias de IoT (OWASP, 2018).

Em 2018, a OWASP (2018), divulgou uma lista com as 10 principais vulnerabilidades de IoT para 2019, descritas a seguir:

2.1.4.1 Senhas fracas, previsíveis ou codificadas

Senhas padrões que não podem ser modificadas e disponíveis publicamente são vulneráveis, fáceis de quebrar por técnicas de força bruta ou backdoors método de escapar de uma autenticação ou criptografia para entrada em sistemas, software, firmware, dispositivos etc. (OWASP, 2018).

2.1.4.2 Serviços de rede inseguros

Dispositivos expostos a internet com serviços de rede desnecessários ou inseguros executados no próprio dispositivo, especialmente aqueles expostos à Internet, que comprometem a confidencialidade, integridade, autenticidade ou disponibilidade de informações ou permitem o controle remoto não autorizado. (OWASP, 2018).

2.1.4.3 Interfaces inseguras

APIs insegura, APIs de back-end, nuvem ou interfaces móveis no ecossistema fora do dispositivo que permitem o comprometimento do dispositivo ou de seus componentes relacionados. Problemas comuns incluem falta de autenticação/autorização, falta ou criptografia fraca e falta de filtragem de entrada e saída. (OWASP, 2018).

2.1.4.4 Falta de mecanismos de atualização segura

Falta de capacidade de atualizar o dispositivo com segurança. Isso inclui a falta de validação de firmware no dispositivo, falta de entrega segura (não criptografada em trânsito), falta de mecanismos anti-reversão e falta de notificações de alterações de segurança devido a atualizações. (OWASP, 2018).

2.1.4.5 Uso de componentes inseguros, desatualizados ou obsoletos

Uso de componentes/bibliotecas de software obsoletos e/ou inseguros que podem permitir que o dispositivo seja comprometido. Isso inclui a personalização insegura da plataforma do sistema operacional e o uso de software de terceiros ou componentes de hardware de uma cadeia de suprimentos comprometida (OWASP, 2018).

2.1.4.6 Proteção da privacidade insuficiente

Informações pessoais do usuário armazenadas no dispositivo ou no ecossistema usadas de maneira insegura, imprópria ou sem permissão (OWASP, 2018).

2.1.4.7 Transferência e armazenamento de dados inseguros

Falta de criptografia ou controle de acesso para dados confidenciais que estão dentro do ecossistema, incluindo dados em repouso, em trânsito ou em processamento (OWASP, 2018).

2.1.4.8 Falta de controle de gerenciamento dos dispositivos

Falta de suporte de segurança em dispositivos liberados para produção, incluindo gerenciamento de ativos, gerenciamento de atualizações, desarme seguro, monitoramento de sistemas e recursos de resposta (OWASP, 2018).

2.1.4.9 Configuração insegura por padrão

Dispositivos ou sistemas com configurações padrão pouco seguras ou sem a possibilidade de tornar o sistema mais seguro, aplicando restrições com base nas alterações de configuração (OWASP, 2018).

2.1.4.10 Segurança física insuficiente

Falta de medidas de fortalecimento físico, permitindo que potenciais atacantes obtenham informações confidenciais que podem ajudar em um futuro ataque remoto ou assumir o controle local do dispositivo (OWASP, 2018).

2.1.5 Principais Ataques

Com os avanços da tecnologia na exploração do IoT a quantidade de dispositivos conectados e que podem ser acessados tende aumentar, junto novas maneiras e oportunidades de ataques cibernéticos. Andrea, Chrysostomou e Hadjichristofi (2015), classificou os ataques a IoT em quatro categorias: ataques físicos, rede e software, descritos a seguir.

2.1.5.1 Ataques Físicos

Ataques que prejudicam diretamente o sistema de IoT, com o objetivo de impactar a disponibilidade do serviço, a vida útil ou o funcionamento do hardware e, ataques que envolvem engenharia social, pois o invasor precisa interagir fisicamente com os usuários da rede de IoT.

O invasor precisa ter acesso físico aos dispositivos para que os ataques sejam bem-sucedidos, focando nos componentes de hardware do sistema IoT, conhecidos também como NS (Nó Sensor) que são dispositivos autônomos equipados com capacidades de sensoriamento, processamento e comunicação.

2.1.5.2 Ataques de Rede

Nesta categoria, os ataques estão centralizados na rede do sistema de IoT onde o invasor obtém algumas informações sobre a rede, usando aplicações de sniffing, escaneamento de portas e sniffer de pacotes, assim pode detectar as informações confidenciais ou quaisquer outros dados provenientes das tecnologias RFID devido a suas características sem fio.

Ataques Main In The Middle (MITM) acontece quando dois usuários/dispositivos de um sistema IIoT trocam dados entre si o ataque MITM de alguma forma são interceptados, registrados e, possivelmente, alterados pelo atacante sem que as vítimas se percebam.

Um invasor pode falsificar sinais de RFID para ler e gravar uma transmissão de dados a partir de um dispositivo. Clonar um dispositivo RFID copiando os dados das vítimas para outros dispositivos RFID, mesmo os dados sejam idênticos, esse método não replica o ID original do RFID, tornando possível distinguir entre o original e o comprometido (Kadow e Camargo, 2016).

Ataque sinkhole (Buraco Negro) onde o invasor atrai todo o tráfego dos NS da RSSF, criando um "buraco negro", violando a confidencialidade dos dados e também nega serviço à rede descartando todos os pacotes em vez de encaminhá-los para o destino desejado.

2.1.5.3 Ataques de Software

Segundo Andrea, Chrysostomou e Hadjichristofi (2015), os ataques de software são a principal fonte de vulnerabilidade de segurança em qualquer sistema computadorizado. Esses ataques exploram o sistema usando trojans, worms, vírus, spyware e scripts maliciosos que podem roubar informações, adulterar dados, negar serviço e até danificar os dispositivos de um sistema de IoT.

Ataques de phishing o invasor obtém acesso a dados confidenciais falsificando as credenciais de autenticação de um usuário, geralmente através de e-mails infectados ou sites de phishing. Vírus, Worms, Trojans Spyware e Adwares pode infectar o sistema com software malicioso, ocasionando uma variedade de resultados como roubo de informações, adulteração de dados ou mesmo negação de serviço.

Dispositivos IoT geralmente conectadas à Internet onde o usuário que controla o gateway pode ser enganado ao executar scripts maliciosos, podendo resultar em um desligamento completo do sistema ou em roubo de dados.

Tabela 1 - Classificação dos Ataques a IoT

Ataques Físicos	Ataques de Rede	Ataques de Software
Adulteração de nós	Ataques de análise de tráfego	Ataques de phishing
Interferência por RF	Falsificação de RFID	
Bloqueio de nós	Clonagem de RFID	Vírus, Worms, Trojans, Spyware e Adwares
Injeção de nó malicioso	Acesso não autorizado a dispositivos RFID	
Danos físicos	Sinkhole	Scripts maliciosos
Engenharia social	Ataques man in the middle	
Ataques de negação de suspensão de atividade	Ataques de negação de serviço	Negação de serviço
Injeção de código malicioso		

Fonte: Adaptado de Andrea, Chrysostomou e Hadjichristofi (2015)

Ainda não há soluções definitivas para todos os ataques que a IoT pode sofrer, porém existem medidas de defesa que podem mitigar esses ataques e reduzir os impactos que eles possam causar (ANDREA; CHRYSOSTOMOU; HADJICHRISTOFI, 2015). Neste contexto, a proposta de solução foca na implementação de uma rede de blockchain para as validações de requisições de segurança de dados, mais especificamente o framework Hyperledger Fabric na versão 2.2.2 (ANDROULAKI et al. 2018) e seus paradigmas de segurança, para apoiar a segurança na comunicação entre os dispositivos, e assegurar que somente quem possui devida autorização possa acessar e operar os dispositivos e informações que compõem o ambiente.

2.2 Projeto FASTEN

A arquitetura FASTEN é composta por três níveis. O nível de borda, onde se encontram os dispositivos IIoT, o nível da plataforma, que é composta pelos middleware de conexão dos rôbos à nuvem, de ordenação de cada solicitação e resposta da plataforma e os bancos de dados que armazenam as informações dos dispositivos IIoT e a terceira camada é responsável pelo nível empresarial, composta por diversos aplicativos, com a funcionalidade de gerenciar e analisar os dados e as informações (Costa et al, 2020). O projeto FASTEN trouxe avanços no uso de dispositivos IIot mas as questões de segurança das informações trafegadas ainda eram um desafio a ser tratado.

2.3 Blockchain

A blockchain é um livro-razão compartilhado e imutável que facilita o processo de registro de transações e o rastreamento de ativos em uma rede empresarial com um

banco de dados distribuído, consiste em uma lista de transações agrupadas juntas, criptografada em uma cadeia de blocos (IBM).

As transações são alterações de ativos que pode ser tangível (produtos ou documentos) ou intangível (intelectual), existem diversos frameworks para implementação da tecnologia blockchain. Dentre elas o Hyperlerdger Fabric (Fabric 2021). Praticamente qualquer item de valor pode ser rastreado e negociado em uma rede de blockchain, o que reduz os riscos e os custos para todos os envolvidos (IBM).

A blockchain utiliza o conceito de Proof-of-Work (prova de trabalho) para realizar a validações das transações feitas na rede. Este conceito é um protocolo criptográfico que requer que os membros de uma rede validem as transações emitidas (Hileman e Rauchs, 2017) garantindo que somente requisições válidas sejam realizadas.

Uma rede blockchain pode ser caracterizada com pública ou privada. A rede pública não requer nenhum tipo de autenticação para novos usuários. Já em rede privada, somente os usuários que forem autorizados a ingressar podem fazer parte da rede e emitir trasações (IBM), este modelo de rede é mais adequado a empresas que desejam manter um alto nível de governança.

O Hyperledger Fabric é uma plataforma de tecnologia de código aberto configurável, projetada para o ambiente empresarial, com o foco na construção de aplicações em cadeia de blocos privados e permissionados (Burle, 2019). A plataforma opera baseada na premissa de contratos inteligentes (chaincode), em uma rede blockchain privada.

Na rede do Hyperledger Fabric cada componente e atores possuem suas identidades e políticas que definem controle de acesso e governança na rede blockchain, permitindo que os membros aprovem ou rejeitem mudanças na rede, no canal ou no contrato inteligente. As aplicações do Hyperledger Fabric, utilizando o software development kit (SDK), oferecem suporte somente a efetuar um pedido de transação na rede e de consulta. As operações administrativas são executadas através das ferramentas command line input (CLI) (Fabric, 2021).

3. Metodologia

A metodologia principal utilizada nesse artigo foi a revisão de pesquisa bibliográfica (Andrea et al, 2015) com foco de transparecer os diversos tipos de vulnerabilidades dos dispositivos IIoT que são desde simples sensores a complexos robôs industriais. Porém o entendimento das vulnerabilidades e a forma como os ataques são realizados, possibilitam planejar a implantação da IIoT de forma a maximizar a proteção dos dados coletados e minimizar os riscos de ataques cibernéticos.

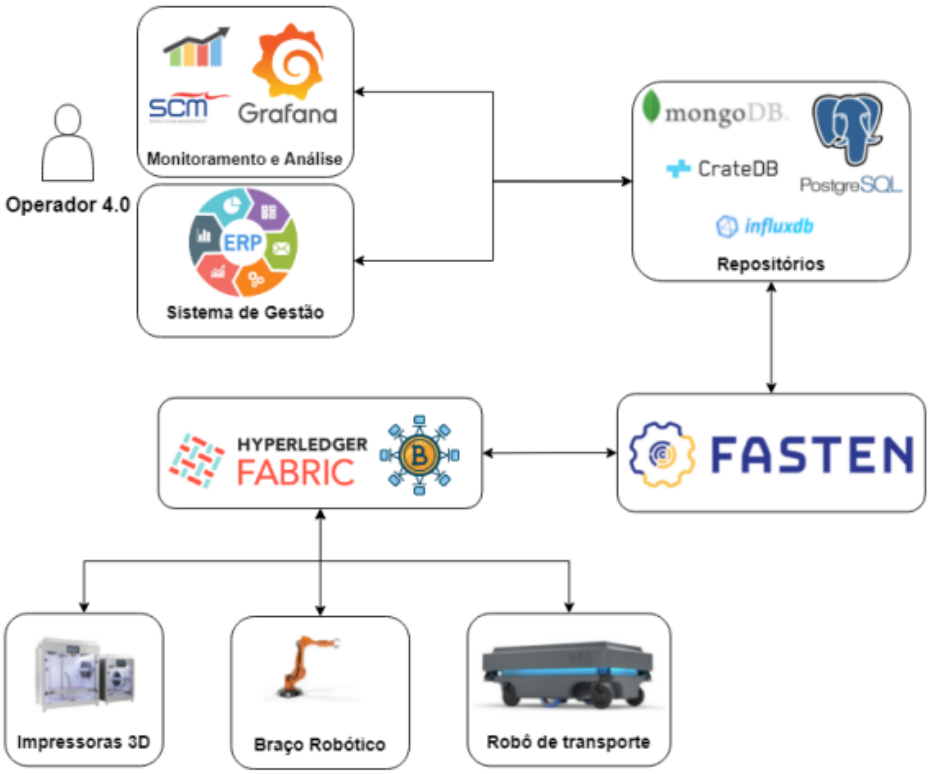
Como o objetivo implatar uma rede blockchain para mitigação de falhas de segurança para dispositivios IIoT (Costa et al, 2020) garantindo a disponibilidade, integridade, confidencialidade e autenticidade. Utilizado como coletas de dados frameworks, relatórios de documentos digitais, e outras bases de dados digitais para desenvolvimento do artigo.

4. Analise e interpretação dos resultados

Os membros da rede utilizam os contratos inteligentes (Smart Contract) para manter a integridade dos dados, através de uma arquitetura (executa-ordena-valida). A arquitetura permite a execução de uma transação e verifica sua validade através do protocolo de consenso, com a finalidade de ser inserida no livro-razão.

A Figura 2 mostra uma visão geral da arquitetura para a incorporação dos contratos inteligentes via Hyperledger Fabric no contexto do projeto FASTEN, de modo que o acesso aos dispositivos IIoT seja protegido pela camada de validação da rede blockchain. O Hyperledger Fabric age, impedindo que algum malware tenha acesso aos dados da rede, seja se passando por um operador ou um dispositivo IIoT. Dessa forma, garantimos que somente quem tem autorização possa trafegar dados no ambiente FASTEN. Para isso, utilizamos o processo de validação de transação, conhecido como Proof-of-Work (prova de trabalho), do Hyperledger Fabric, para que todas as transações de dados sejam validadas e não possuam nenhuma falha. Assim, só após a validação, as transações podem ser passadas para os dispositivos de IIoT presentes na rede.

Figura 2 – Arquitetura Proposta FASTEN – contrato Inteligentes

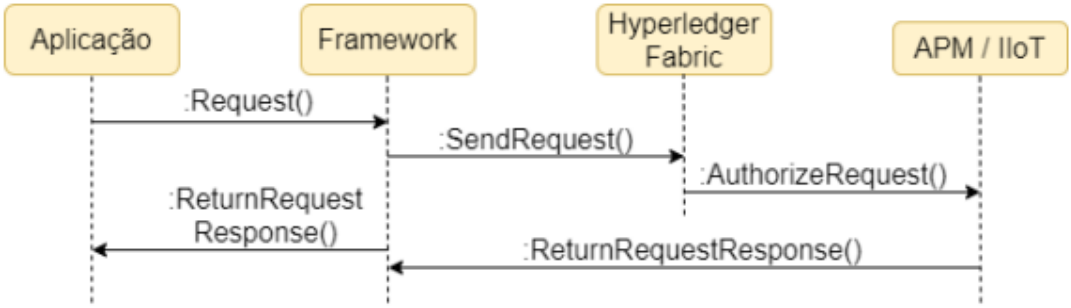


Fonte: Adaptado de Costa et al (2020)

Como resultado, e possível verificar que a integridade dos dados, por meio deste mecanismo de assinaturas digitais, certifica a disponibilidade e confidencialidade das informações (Fabric, 2021) presentes entre as comunicações dos dispositivos. Assim, todas as transações de uma rede blockchain são mantidas de forma distribuída pelos membros da rede.

A figura 3 apresenta uma representação do fluxo de dados no ambiente proposto pelo FASTEN com a incorporação do Hyperledger Fabric. Nele uma requisição é feita pelo usuário por meio de uma aplicação para utilização de um dispositivo IIoT. Esta requisição possui informações como identificação do requerente, localidade, data e hora, qual recurso será utilizado, e qual operação deve ser realizada (como uma impressão 3D). O framework FASTEN encaminha estes dados para a rede do Hyperledger Fabric que fara a autenticação da requisição. Se a requisição for válida, ela será encaminhada para execução no dispositivo, que retornará a resposta da tarefa, caso consiga realizá-la ou não.

Figura 3 – Fluxo de dados no ambiente FASTEN



Fonte: Pinto et al (2021)

A figura 4 apresenta uma tela de log de todas as transações que foram executadas na rede informando a chave do usuário (userPKI), a chave do dispositivo (IoTPKI), qual a operação realizada (task), o horario que foi realizada em timestamp e o status da transação. Como simulação, foram testados os seguintes conjuntos de entradas:

1. Usuário valido, dispositivo cadastrado e operação válida;

2. Usuário invalido, dispositivo cadastrado e operação válida;

3. Usuário valido, dispositivo não cadastrado e operação válida;

4. Usuário valido, dispositivo cadastrado e operação invalida;

Figura 4 – Log das transações em uma rede

Transactions

UserPki	IoTPki	Task	Timestamp	Status
c1eb3836-ef00-43a4-9f68-bbcc65ce7ecd	6eb28398-8698-46f0-8a94-78c67f8c04e7	print	1623981645473	invalid user
c1eb3816-ef00-43a4-9f68-bbcc65ce7ecd	6eb28398-8698-46f0-8a94-78c67f8c04e7	print	1623981660261	success
c1eb3816-ef00-43a4-9f68-bbcc65ce7ecd	6eb28398-8698-46f0-8a94-78c67f8c04e7	print	1623981661143	success
539a8b63-1747-441d-8e2f-927b6f12f193	6eb28398-8698-46f0-8a94-78c67f8c04e7	print	1623981697497	invalid user
ae3da5d0-a194-49cb-932b-9e7fdcf6c524	19b936dc-c8b1-402a-8eaf-55dd6c17b846	weld	1623981714942	success
c1eb3816-ef00-43a4-9f68-bbcc65ce7ecd	6eb28398-8228-46f0-8a94-78c67f8c04e7	print	1623981747939	iot/task not find
c1eb3816-ef00-43a4-9f68-bbcc65ce7ecd	6eb28398-8698-46f0-8a94-78c67f8c04e7	printt	1623981759343	iot/task not find
c1eb3816-ef00-43a4-9f68-bbcc65ce7ecd	6eb28398-8698-46f0-8a94-78c67f8c0447	print	1623981776673	iot/task not find
c1eb3816-ef00-43a4-9f68-bbcc65ce7ecd	68c99c30-567a-4225-b366-77418feaee98	print	1623981793043	success
c1eb3816-ef00-43a4-9f68-bbcc65ce7ett	6eb28398-8698-46f0-8a94-78c67f8c04e7	print	1623981846887	invalid user
c1eb3816-ef00-43a4-9f68-bbcc65ce7ecd	6eb28398-8698-46f0-8a94-78c67f8c04e2	print	1623981856247	iot/task not find

Fonte: Pinto et al (2021)

Para o caso 1 o sistema retorna um sucesso (success) e realiza essa transação na rede blockchain. Para os casos 2, 3 e 4 o sistema não realiza a transação, e retorna um erro de usuário invalido (invalid user), dispositivo não encontrado e operação invalida, respectivamente (iot/task not found). Com base nos resultados obtidos é possível verificar a segurança fornecida pelo Hyperledger Fabric, atestando que somente usuários e um dispositivos que atendam os requisitos executem transações na rede.

5. Conclusão

Como visto, são vários os desafios para a implantação de dispositivos IIoT e pode se afirmar que a segurança da informação é o principal obstáculo dentre eles, pois é o que oferece maior dificuldade de ser resolvido. Com isso a segurança de dados para processos IIoT relacionados a Industria 4.0 deve ser fundamental, assim, foi apresentada uma solução para segurança no contexto do projeto H2020 FASTEN, utilizando uma rede blockchain para mitigação de vulnerabilidades em dispositivos IIoT. Com base nos resultados obtidos, há evidências de que o Hyperledger Fabric fornece uma camada extra de validação para o meio de comunicação das indústrias.

Referencial bibliográfico

Costa, F. S.; Nassar, S. M.; Gusmeroli, S.; Schultz, R.; Conceição, A. G. S.; Xavier, M.; Hessel, F.; E Dantas, M. A. R. (2020). **FASTEN IIoT: An Open Real-Time Platform for Vertical, Horizontal and End-To-End Integration**. Sensors, 2020. <https://www.mdpi.com/1424-8220/20/19/5499> Acesso em: 15/10/2021

Santos, B. P.; Silva, L. A. M.; Celes, C. S. F. S.; Borges, J. B. N.; Peres, B. S.; Vieira, M. A. M.; Vieira, L. F. M.; Goussevskaia, O. N.; Loureiro, A. A. F. (2016). **Internet das Coisas: Da Teoria à Prática**. UFMG, Belo Horizonte, 2016. Disponível em: <https://homepages.dcc.ufmg.br/~mmvieira/cc/papers/internet-das-coisas.pdf> Acesso em:15/10/2021

Moraes, A. F. De. **Segurança em Redes: Fundamentos**. São Paulo: Érica, 2010.

Andrea, I.; Chrysostomou, C.; Hadjichristofi, G. (2015). **Internet of Things: Security Vulnerabilities and Challenges**, IEEE, 2015. Disponível em: <https://www.researchgate.net/profile/George_Hadjichristofi/publication/304408245_Internet_of_Things_Security_vulnerabilities_and_challenges/links/598188270f7e9b7b524b92ac/Internet-of-Things-Security-vulnerabilities-and-challenges.pdf>. Acesso em: 16/10/2021

Paul, F. **10 Principais Vulnerabilidades da Internet das Coisas**, 2019. Disponível em: <https://cio.com.br/10-principais-vulnerabilidades-da-internet-das-coisas/>. Acesso em: 16/10/2021

CERT.BR. **Cartilha de Segurança para Internet**. 4° ed. São Paulo: CERT.br, 2012. Disponível em: <https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Aceso em: 16/10/2021

Tanenbaum, A. (2011). **Computer Networks**. Prentice Hall Professional Technical Reference, 5° edition.

Open Web Application Security Project (OWASP, 2018). **OWASP Internet of Things Project**, 2018. Disponível em: < https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project>. Acesso em: 17/10/2021

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., Muralidharan, S., Murthy, C., Nguyen, B., Sethi, M., Singh, G., Smith, K., Sorniotti, A., Stathakopoulou, C., Vukolic, M., And Yellick, J. (2018). **Hyperledger fabric: A distributed operating system for permissioned blockchains**. EuroSys, Porto, Portugal, 2018. Disponível em: < https://dl.acm.org/doi/pdf/10.1145/3190508.3190538>. Acesso em: 17/10/2021

Fabric, H. (2021). **Hyperledger**. Disponível em: <https://hyperledger-fabric.readthedocs.io/en/release2.2/blockchain.html>.

IBM. **O que é a tecnologia blockchain?**. IBM. Disponível em: <https://www.ibm.com/br-pt/topics/what-is-blockchain?utm_content=SRCWW&p1=Search&p4=43700058887709639&p5=e&gclid=EAIaIQobChMI8Iyks8Pb8wIVBwaRCh1eug3sEAAYASAAEgLhOfD_BwE&gclsrc=aw.ds> Acesso em: 20/10/2021

Pinto, Carlos M., Santos. Mattheus S., Soares. Romulo L. A. S., David, José M. N., Braga, Regina., Dantas, Mário. (2021). **Uso de Blockchain na Industria 4.0: Uso do Hyperledger Fabric no projeto FASTEN.** SBC Open Lib, Rio de Janeiro, Brasil, 2021. Disponivel em: < https://sol.sbc.org.br/index.php/ersi-rj/article/view/16979/16817>. Acesso em: 20/10/2021

Burle, L. M. (2019). **Um estudo de caso em cadeias de blocos: principais mecanismos de consenso e a plataforma Hyperledger Fabric**. UFF (Universidade Federal Fluminense), Rio de Janeiro, Brasil. Disponível em: < https://app.uff.br/riuff/bitstream/handle/1/12585/Trabalho_de_Conclus_o_de_Curso_LeonardoMBurle.pdf?sequence=1&isAllowed=y>. Acessado em: 20/10/2021

Fiorenza, Maurício M., Kreutz, Diego., Escarrone, Thiago., Temp, Daniel. (2020). **Uma Análise da Utilização de HTTPS no Brasil.** SBC Open Lib, Brasil, 2020. Disponível em:< https://sol.sbc.org.br/index.php/sbrc/article/view/12338/12203>. Acesso em:04/11/2021

Hileman, G., Rauchs, M. (2017). **Global blockchain benchmarking study**. SSRN, University of Cambridge, 2017. Disponível em: <https://ssrn.com/abstract=3040224>. Acesso em: 04/11/2021

Kadow, André., Camargo, Carlos Eduardo Pires. (2016). **Internet das coisas: vulnerabilidade, privacidade e pontos de segurança,** ACADEMIA, Porto Alegre, Brasil, 2016. Disponível em: < https://www.academia.edu/33308880/INTERNET_DAS_COISAS_VULNERABILIDADE_PRIVACIDADE_E_PONTOS_DE_SEGURAN%C3%87A_INTERNET_OF_THINGS_VULNERABILITY_PRIVACY_AND_SECURITY_ISSUES>. Acesso em: 04/11/2021