Este trabalho foi originalmente submetido em Agosto de 2022, na 24ª Jornada de Iniciação Científica na Universidade Católica de Pernambuco (UNICAP). Inicialmente entregue como o relatório final para o PIBIC 2021-2022, este trabalho foi orientado pelo professor Sérgio Murilo Maciel Fernandes. Esta versão foi resumida para conter apenas o conteúdo da pesquisa, descartando os demais itens presentes no relatório final de atividades.

Investigação de soluções de performance e de segurança em IoT

3.1 INTRODUÇÃO

As revoluções industriais foram eventos que marcaram a passagem entre diferentes fases da sociedade, representando evoluções e trazendo consigo avanços tecnológicos que atuam como agentes transformadores dos locais onde estão inseridos. A Terceira Revolução Industrial, também chamada de "Revolução Digital", teve seu início datado por volta de 1950 e foi responsável pelo constante desenvolvimento dos computadores e da automação industrial; fator decisivo para que o estado da arte da tecnologia tenha se expandido e esteja na atual fase, chamada de "Indústria 4.0", que possui foco na eficiência e produtividade dos processos.

Um dos conceitos responsáveis por garantir esses avanços e melhorias é o de *Internet of Things* (Internet das Coisas, abreviado nesta pesquisa como IoT) que consiste em conectar os chamados *smart objects* (objetos inteligentes – artefatos tecnológicos que simulam a forma de itens comuns do dia a dia, e que possuem a capacidade de captar, armazenar e/ou processar dados do meio físico) [1][2] através de uma rede (interna ou externa) a fim de trocar dados entre si [3]. A *International Telecommunication Union* define IoT como uma "infraestrutura global para a sociedade da informação, permitindo o avanço de serviços através da interconexão (física e virtual) de objetos" [4].

Para que seja justificado o desenvolvimento da cadeia de troca de dados entre dispositivos, é necessário que haja a obtenção de informações que, naturalmente, ocorre através do processamento dos dados coletados. Em [5], tem-se que os modelos de processamento de dados em IoT dividem-se em três níveis: *edge* (de ponta, também podendo ser chamado de local ou margem), *fog* (em névoa) e *cloud* (em nuvem), cada um com particularidades e vantagens de acordo com a aplicação desejada. Porém, apesar dos avanços nos últimos anos, dispositivos IoT, em sua maioria, são de pequeno porte e possuem limitações físicas que dificultam que o processo de obtenção e processamento de dados ocorra através de um único aparelho [2].

Os dados ou informações compartilhadas na rede podem variar desde relatórios de sensores até dados sensíveis de usuários (como geolocalização, identificadores de dispositivos, nomes ou outros que permitam rastreio de indivíduos). Logo, é imprescindível a investigação de possíveis alternativas de segurança (tais como criptografia, anonimização ou inserção de ruídos) que ocorram logo após a camada física, pois, segundo [6], a etapa seguinte é a de compartilhamento de dados através dos nós da rede, o que pode ocasionar uma brecha de segurança caso exista algum dispositivo infectado com um *malware* ou um *hacker* capaz de interceptar a troca de dados entre dois aparelhos. No entanto, a proteção de dados local requer um maior poder de processamento para a execução dos algoritmos.

Zahooor et al. [2] afirmam que uma maior força de processamento nesses dispositivos requer uma maior fonte de energia. Como alternativa, há a possibilidade de terceirizar o processamento de dados para servidores na nuvem ou outros aparelhos mais potentes que estejam conectados à rede, mas ao custo de causar latência na entrega da informação processada. Além disso, ainda segundo [2], mesmo com uma capacidade de processamento local, é preciso espaço para armazenar os algoritmos e os dados coletados. Logo, observa-se que não há solução única para resolver as diversas dificuldades presentes em soluções de implementação IoT.

Considerando as vantagens providas por este tipo de tecnologia, assim como as dificuldades apresentadas anteriormente, esta pesquisa tem por fim investigar possíveis soluções que possam impactar positivamente na performance de atuação de dispositivos presentes na Internet das Coisas, bem como formas de preservar a segurança dos dados coletados pelos mesmos.

3.1.1 *Internet of Things* (Internet das Coisas)

Consiste na conexão de dispositivos tecnológicos (comumente referenciados como *nodes* ou nós) a outros aparelhos externos e/ou servidores através de uma rede (interna ou externa) a fim de atividades de troca e envio de dados entre si, para obter informações relevantes acerca de uma determinada aplicação. Tecnologias que podem encaixar-se nesse conceito podem variar entre si, mas não se limitam a: sensores de uso específico, muitas vezes por radiofrequência (tais como medidores) até tecnologias usadas rotineiramente com outros propósitos (como câmeras) ou dispositivos vestíveis.

De acordo com [6], os componentes que permitem a comunicação entre esse tipo de dispositivos são: método de comunicação local (o qual define por qual meio os aparelhos vizinhos se comunicam), protocolo de aplicação (estrutura definida através de um conjunto de códigos, que é responsável por definir como a informação deve ser transportada), *gateways* (portais responsáveis por transmitir, de fato, a informação, comumente conectando os dispositivos à internet), servidores (cuja função é aceitar e gerenciar os dados recebidos, geralmente constituindo centrais de dados na nuvem) e interface do usuário

(abstração, geralmente através de interface gráfica, na qual os usuários podem observar dados coletados e/ou processados, bem como interagir diretamente com os dispositivos, muitas vezes sem necessidade de conhecimentos em programação). No entanto, existe a possibilidade de os dados serem processados localmente, eliminando a necessidade de processamento em nuvem por parte dos servidores [2][5].

A arquitetura IoT é composta por cinco camadas [7], que, partindo-se da localizada mais à margem (ponta) até a nuvem, dividem-se em: (1) *perception layer* (camada de percepção, onde encontram-se os sensores ou objetos físicos, responsáveis pela coleta de dados), (2) *network layer* (camada de rede, responsável pela transmissão de dados, onde estão as tecnologias de comunicação), (3) *middleware layer* (camada intermediária, que pode possuir recursos como armazenamento, computação, entre outros, agindo como uma camada de suporte), (4) *application layer* (camada de aplicação, que envolve o gerenciamento das informações obtidas na camada intermediária, podendo ser utilizada para controlar o sistema como um todo) e (5) *business layer* (camada de negócios, estando relacionada à tomada de ação por parte das organizações, através de análise de ferramentas de visualização de dados, o que permite a montagem e refinamento de estratégias de negócio).

3.1.2 Coleta e armazenamento de dados

Os dados obtidos por dispositivos IoT comumente partem do meio físico, sendo heterogêneos e provenientes de múltiplas fontes, o que influencia em sua estrutura [5]. De acordo com [8], os dados coletados pelos aparelhos podem ser de natureza estruturada (tais como arquivos JSON ou XML), não estruturados (que não possuem organização, sendo de difícil interpretação) ou semiestruturados (que possuem marcadores para separar elementos, mas que não estão associados a regras de estruturas formais de modelos de dados), não existindo, atualmente, uma forma universal de tratamento e armazenamento.

Dados coletados por dispositivos podem ser armazenados localmente, na nuvem, em névoa ou seguir uma estratégia que procure englobar duas ou mais alternativas, sendo necessário levar em consideração fatores como volume de dados a serem armazenados, disponibilidade em rede e energia [8][9]. Ainda segundo [9], algumas aplicações podem ser beneficiadas pelo armazenamento em névoa, pois os sensores podem recuperar os dados que forem necessários sempre que preciso (requisitando acesso aos dispositivos intermediários) sem necessitar de maior capacidade de armazenamento e com baixa latência, que representa uma vantagem em relação à comunicação com a nuvem.

3.1.3 Processamento de dados

O processamento de dados na Internet das Coisas consiste em transformar os dados coletados através de sensores no meio físico em informações relevantes acerca da aplicação em que estão inseridos. De acordo com [5], existem três formas de processamento em IoT:

3.1.3.1 *Edge computing* (computação em ponta ou em margem)

Também chamado de computação local, refere-se ao processamento local dos dados coletados por um dispositivo. Somente os resultados são transmitidos pela rede, o que diminui o consumo de banda e latência [5]. No entanto, esse tipo de processamento não é recomendado para aparelhos que possuem localização e volume de dados dinâmico. Aplicações como carros autônomos, monitoramento de tráfego e *smart grids* (redes elétricas inteligentes) são exemplos de caso de uso de computação em margem [8].

3.1.3.2 *Fog computing* (computação em névoa)

Infraestrutura descentralizada, onde os recursos estão entre o dispositivo e o servidor na nuvem. Serve como um suporte para dispositivos que estão na ponta, permitindo atividades como processamento, armazenamento e serviços de rede, com uma latência menor do que quando compara aos serviços na nuvem [10]. Um exemplo de aplicação de computação em névoa é o de gerenciamento inteligente de resíduos, onde, através de sensores instalados em lixeiras, cidades podem monitorar o volume e estado atual dos resíduos, sendo possível traçar a rota dos caminhões somente para locais necessários (economizando em gasolina e desgaste do veículo) e monitorar questões de saúde pública antes que venham a se tornar um problema maior [11].

3.1.3.3 *Cloud computing* (computação em nuvem)

Servidores centralizados, em centrais que não necessariamente estão próximas do usuário ou dispositivo e necessitam ser acessados pela internet, podem realizar o processamento dos dados enviados pelos dispositivos de ponta ou névoa. A *Amazon Alexa*, aparelho da empresa *Amazon* que age como assistente de voz, realiza NLP (*Natural Language Processing* – processamento de linguagem natural) nos servidores na nuvem da *Amazon*, devido à falta de poder computacional do aparelho [12].

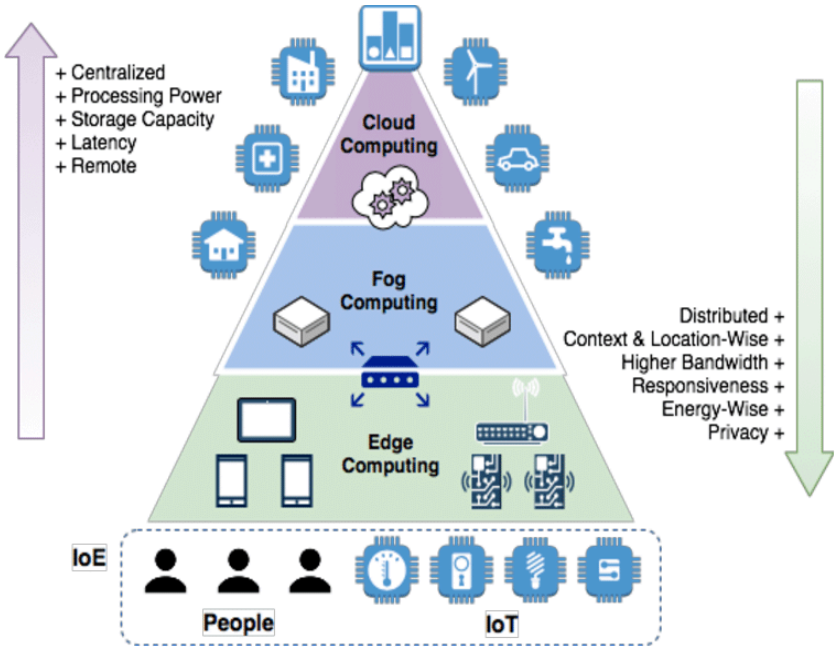

Figura 1: Exemplificação de um ecossistema para cidades inteligentes que inclui as três atuais formas de processamento. Disponível em: https://www.researchgate.net/figure/Osmotic-IoT-Computing-architecture-for-Smart-Cities_fig1_327571161

Na Figura 1, observa-se que aparelhos mais próximos à ponta apresentam vantagens como descentralização, maior responsividade e privacidade, ao custo de um maior gasto de energia para o dispositivo que estiver realizando o processamento, devido ao fato de que ele não está sendo delegado à uma entidade externa. A computação na nuvem, no entanto, traz maior latência, com a vantagem de possuir maior poder de processamento e maior capacidade de armazenamento (ambos por parte de servidores ou outros dispositivos que façam parte da rede, mas que não sejam os nós responsáveis por captar a informação).

3.1.4 Consumo de energia

O consumo de energia em dispositivos IoT está relacionado com a finalidade de sua aplicação, e deve ser planejado. No exemplo citado anteriormente sobre a utilização de computação de ponta para automóveis autônomos, apesar da problemática apresentada anteriormente por [2], espera-se que esse tipo de aplicação possua uma dependência constante de uma grande fonte de energia, visto que, sem a mesma, não haveria funcionamento do carro.

No entanto, é esperado que dispositivos de menor porte, tais como sensores *RFID* (*Radio Frequency Identification* – sensores por rádio frequência) operem continuamente através de baterias de pequeno porte [13]. Esta relação cria uma dependência onde tanto uma falha em uma bateria pode deixar

um aparelho indisponível quanto cria a necessidade de monitoramento e manutenção devido ao desgaste natural da bateria, sendo esta problemática trabalhada no âmbito de tolerância a falhas em software e hardware.

Como alternativa, há o conceito de *energy harvesting* (colheita de energia), que consiste em capturar energia de uma ou mais fontes renováveis para convertê-la em energia reutilizável [13][14]. No entanto, Georgiu et al. [15] afirma que dois problemas estão presentes nesse conceito, sendo eles o fato de que energias renováveis não podem ser fontes de alta dependabilidade devido à volatilidade de seu fornecimento e o conceito de *energy budget*, que diz respeito ao balanço da energia solar que chega à Terra, mas depois retorna ao espaço.

3.1.5 Segurança

Técnicas, métodos e protocolos de segurança dentro do contexto de Internet das Coisas dizem respeito não somente à proteção física do dispositivo, mas também aos dados que estão em processo de coleta ou que já foram coletados e possivelmente armazenados no aparelho ou sendo enviado à servidores externos.

Bertino [16] afirma que os dados provenientes desses dispositivos costumam incluir *meta-data*, ou seja, informações sensíveis (tais como localização, data, modelo do aparelho, dentre outros) que possibilitam relacionar um determinado dado à um usuário específico. De acordo com [17], ataques podem acontecer independentemente do nível da camada (*perception*, *network*, *middleware*, *application* ou *business*), e o *hacker* pode adentrar o dispositivo com sucesso mesmo que o aparelho esteja utilizando protocolos de segurança específicos para IoT. Fatores como confidencialidade (dados disponíveis somente para usuários autorizados), integridade (imutabilidade dos dados) e disponibilidade (dados disponíveis sempre que requisitados por usuários autorizados) são os ponto-chaves principais a serem levados em consideração no quesito de segurança em IoT [18][19].

3.1.5.1 Protocolos de Comunicação

Segundo Jeddou et al. [20], dispositivos IoT costumam utilizar comunicação M2M (*Machine to Machine* – máquina para máquina). Ainda de acordo com o autor, esses aparelhos não dependem de um único protocolo de comunicação, mas de variados protocolos, de acordo com a aplicação. Alguns dos protocolos que podem ser utilizados, bem como uma breve descrição, são apresentados a seguir:

3.1.5.1.1 *Hyper Text Transport Protocol* (HTTP)

Protocolo padrão utilizado na Web. Bhola [21] afirma que, apesar de ser possível implementar, o HTTP não é recomendado para aplicações IoT devido à fatores como: não supre a necessidade de comunicação (HTTP funciona entre dois sistemas, enquanto IoT, geralmente, necessita de uma comunicação de um para muitos), unidirecionalidade (um cliente pode somente requisitar recursos de um servidor, e não requisitar e fornecer ao mesmo tempo), funcionamento síncrono, escalabilidade e consumo de energia.

3.1.5.1.2 *Message Queuing Telemetry Transport Protocol* (MQTT)

É um dos protocolos padrão utilizado em aplicações IoT [22], baseado na troca de mensagens *publish/subscribe* (publicar e inscrever-se) entre clientes e servidores (chamados de Brokers, que organizam o tópico das mensagens trocadas). Foi projetado levando em consideração dispositivos que fossem de baixa confiança, pouco poder de processamento e que operassem em redes com pouca banda e alta latência [23][24]. Por isso, é um protocolo cujos pacotes a serem transmitidos são menores e utilizam uma estrutura mais simplificada.

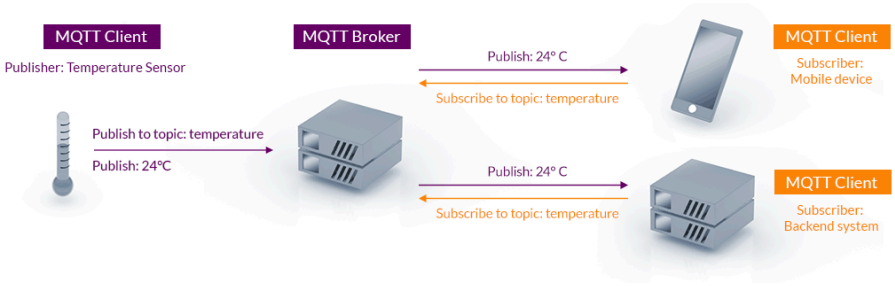

Figura 2: Exemplificação visual do funcionamento do protocolo MQTT. Disponível em: mqtt.org

Através da Figura 2, pode-se observar o seguinte fluxo de funcionamento: um sensor inteligente é responsável por captar os dados do meio físico e enviá-los para um MQTT Broker (entidade central responsável por receber mensagens de clientes MQTT [25]). Neste protocolo, um cliente consegue agir como *publisher*, *subscriber* ou ambos ao mesmo tempo [26].

3.1.5.1.3 *Simple/Streaming Text Oriented Messaging Protocol* (STOMP)

Também segue o paradigma de *publish/subscriber* utilizando-se de Brokers (chamados de STOMP *servers*). Assim como no MQTT, é possível que um cliente desempenhe papéis de *publisher*,

subscriber ou ambos ao mesmo tempo. Segue também o mesmo conceito de dividir as mensagens em tópicos, mas são nomeadas nessa aplicação por *destination* (destino). A estrutura das mensagens remete à uma sintaxe HTTP [26]. Uma das vantagens de utilização desse protocolo é que, segundo [27], é de simples implementação, e, além disso, a clientes STOMP customizados podem comunicar-se com quaisquer outros clientes STOMP devido ao conceito de interoperabilidade.

3.1.5.2 Segurança de dados

Segundo dados da Statista [28], haverá cerca de 29.4 bilhões de dispositivos IoT conectados à internet por volta de 2030. Aparelhos que variam desde lâmpadas inteligentes até carros autônomos estão inclusos nessa realidade. Levando este fato em consideração, é natural projetar que a quantidade e os modos de ataque a estes dispositivos aumentarão e serão mais refinados. Chunchun [29] afirma ainda que o crescimento constante no volume de dados pode aumentar a quantidade de dados públicos disponíveis, o que leva a riscos de rastreio de usuários específicos através de dados.

3.1.5.2.1 Anonimização de dados

É uma técnica utilizada como alternativa para as dificuldades mencionadas anteriormente. Costumam classificar-se em dois tipos: (1) técnicas baseadas em randomização (como permutação, que consiste em reorganizar os dados de acordo com um conjunto de regras preestabelecidas) e (2) técnicas baseadas em generalização [29]. Ainda segundo a autora, é possível utilizar a obfuscação de dados, consistindo em mascarar os dados através de processos como encriptação em tokenização, com o resultado final não sendo interpretável para o usuário a não ser que ele possua a chave correta para descriptografar o dado em questão.

3.1.6 Aplicações de IoT na área de saúde

Dispositivos vestíveis (tais como *smartwatches* – relógios de pulso inteligentes) são amplamente utilizados como forma de monitoramento em tempo real de funções vitais de pacientes. Esta é uma aplicação que se estende desde uso cotidiano até situações médicas aplicadas à área de *eldercare* (serviço de cuidado para idosos). Atualmente, IoT também é utilizado para aplicações de E-saúde, em campos de estudo como detecção e prevenção de doenças [30]. A utilização de dispositivos invasivos também é vista como uma tendência futura [31]. Segundo dados do *Mordor Intelligence* [32], tomando como base o valor obtido em 2020, espera-se que, até 2026, o mercado de IoT chegue próximo a duplicar.

Castro et al. [33] afirma que outra tendência futura é a de um prontuário eletrônico unificado e armazenado em serviços de *cloud*. Edoh et al. [34] trazem uma proposta de estudo para o monitoramento de pacientes com demência, o que consegue demonstrar, ainda mais, a volatilidade de ecossistemas IoT aplicados à área de saúde. Outras áreas de estudo da computação, como processamento de imagem digitais, também conseguem se beneficiar do avanço da Internet das Coisas para avançar em suas atuações [35].

3.2 OBJETIVO

3.2.1 Objetivo Geral

Investigar soluções que envolvam performance e segurança para os dispositivos de IoT.

3.2.2 Objetivos específicos

Investigar em IoT: soluções de armazenamento nos aspectos de consumo de energia em dispositivos, soluções que envolvam uma maior capacidade de processamento para os dispositivos de IoT (Performance) e investigação dos dispositivos de IoT com relação aos aspectos de dependabilidade: confiabilidade, disponibilidade, segurança do dispositivo contra defeitos e intrusão, confidencialidade e integridade dos dados.

3.6 MATERIAIS E MÉTODOS

Foi realizado um mapeamento sistemático acerca do tema de *IoT*, destrinchando-se em *IoT concepts*, *IoT challenges* e *IoT state of art*. As pesquisas foram realizadas através das seguintes strings de busca: *IoT storage*, *IoT data storage*, *IoT edge storage*, *IoT cloud storage*, *IoT device performance*, *IoT processing*, *IoT cloud computing*, *IoT fog computing*, *IoT edge computing*, *IoT energy consumption*, *IoT energy management*, *IoT security*, *IoT data security*, *IoT criptography*, *IoT privacy*, *IoT data privacy*, *IoT state of art*, *IoT healthcare*, utilizando sites como IEEE, Google Scholar e ResearchGate para obtenção dos artigos inclusos nesta pesquisa.

Foram inclusos ainda artigos e fontes de literatura cinzenta pertinentes ao tema geral estudado ou que oferecessem informações técnicas acerca do funcionamento e/ou estado da arte do tema de estudo. Somente fontes de literatura cinzenta que pertencesse a empresas de tecnologia já estabelecidas ou *newsletters,* com 5 anos ou mais de circulação, foram utilizadas. Os materiais inclusos neste trabalho

visam responder as seguintes questões de pesquisa, mas não limitando-se a: "como se dá o armazenamento em dispositivos *IoT*", "como se dá o processamento de dados em dispositivos *IoT*", "quais são os métodos e protocolos utilizados para proteger os dados em dispositivos *IoT*" e "como se dá a implementação de tecnologias *IoT* na área de saúde atualmente".

Quaisquer materiais anteriores à 2016 foram descartados tendo em vista um embasamento mais condizente com o estado da arte atual, salvo estudos de casos ou embasamentos teóricos. Os materiais inclusos foram divididos nas seguintes categorias, mas não limitando-se somente a uma única categoria:

Categoria	**Referências**
Armazenamento	[3], [8]
Processamento	[1], [2], [4], [5], [9], [10], [11], [12], [37]
Segurança	[16], [17],[18],[19],[20],[21],[22],[23],[24],[25],[26], [29], [38]
Saúde	[30], [31], [32], [33], [34], [35]
Energia	[2], [13], [14], [15]
Embasamento	[6], [7], [8], [25], [26], [28], [29]

3.4 RESULTADOS E DISCUSSÃO

É evidente que o conceito de Internet das Coisas modificou-se diversas vezes ao longo dos últimos anos, e, ao analisar tendências futuras, também fica claro que continuará sendo modificado. Mesmo com as dificuldades apresentadas ao longo desta pesquisa e várias outras dificuldades presentes em escopos de outras aplicações, é inegável que a sociedade atual caminha cada vez mais para utilizar o IoT no cotidiano, principalmente levando em consideração aplicações como Cidades Inteligentes, que já são realidade em diversos países.

3.4.1 Armazenamento em dispositivos IoT

Com a miniaturização tecnológica que vem ocorrendo ao longo das últimas décadas, não é natural considerar que um dispositivo, por menor que seja, não possua uma capacidade razoável de

armazenamento. Dispositivos de memória flash medem pouco mais do que alguns centímetros, e conseguem possuir capacidades de armazenamento na faixa de gigabytes.

No entanto, é necessário considerar que, dependendo do dispositivo em questão, não é necessário haver armazenamento local. Sensores inteligentes, por exemplo, não necessitam de espaço para guardar os dados coletados, pois, mesmo em situações de prototipagem, existirá uma entidade externa (neste exemplo é comum que sejam microcontroladores como Arduino) responsável por participar por mais uma etapa do fluxo que resultará na entrega da informação. Para dispositivos que operam no *edge*, e que precisam realizar processamento local, existem diversas soluções de armazenamento que consistem em guardar somente o que realmente for necessário ou então pedaços de dados (referidos por *blobs*), como na solução apresentada em [36].

3.4.2 Processamento de dados em dispositivos IoT

Uma dificuldade geralmente presente em dispositivos IoT é a falta de poder computacional. Esta restrição, no entanto, não se limita somente a dificuldades físicas, podendo, também, ser uma decisão de *design*, com o intuito de minimizar o dispositivo ou baratear um determinado produto para o usuário final. Alguns ecossistemas, como o apresentado no estudo de caso em [37], não precisariam de maior poder computacional no *edge*, pois, no fluxo apresentado, as atividades da ponta são simples o suficiente para serem reproduzidas por sensores inteligentes já presentes no mercado. Espera-se, por padrão, que os dispositivos de *fog* ou *cloud* possuam uma capacidade de processamento maior.

Outro ponto, que se estende para a área de segurança, é que dispositivos IoT, independente de porte, geralmente não podem depender de algoritmos de criptografia já estabelecidos por não conseguirem computar em paralelo ou por serem atividades dispendiosas.

3.4.3 Segurança em dispositivos IoT

Chunchun [29] apresenta uma implementação de um algoritmo de segurança voltado para dispositivos IoT, abrangendo tópicos como obfuscação de dados, permutação, *K-anonimity*, *L-diversity* e o conceito de *differencial privacy*.

Como já explicitado, parte das dificuldades de segurança na Internet das Coisas se dão devido à falta da capacidade de processamento dos dispositivos. Atualmente existem diversos estudos para operar algoritmos de encriptação (chamados *light-weight-cryptography*) em *low-energy devices* (dispositivos de pouca energia) como apresentado em [38]. Como é comum que a capacidade de processamento desses dispositivos também vá aumentando com o tempo, existe a possibilidade que, futuramente, os algoritmos

consigam ser mais poderosos do que os atuais, o que, consequentemente, irá aumentar a segurança dos dispositivos.

3.4.4 Energia em dispositivos IoT

Ao longo dos anos, vêm sendo apresentadas diversas soluções visando que dispositivos IoT deixem de depender de baterias ou de cabos de energia. Apesar de soluções como energia renováveis funcionarem para diversas aplicações, atualmente, como apresentado por Georgiu et al. [15], existem dificuldades que podem fazer com que esta não seja a melhor opção.

3.4.5 IoT aplicado à área de saúde e tendências futuras

A Internet das Coisas vem desempenhando um papel revolucionário na área de saúde. A área de monitoramento através de dispositivos vestíveis vem sendo cada vez mais comum, através de aplicações como: monitoramento de sono, monitoramento de batimento cardíaco (identificando picos ou casos de arritmia, por exemplo), acompanhamento de exercícios, dentre outros. Atualmente, como comentado em [39], existe uma área denominada HIoT (*Healthcare* IoT), com foco na aplicação de tecnologias de IoT e criação de ecossistemas para a área de saúde.

O estudo desenvolvido por Castro et al. [33] que considera prontuários eletrônicos é factível, e pode implementar outras tecnologias em alta (como *blockchain* e contratos inteligentes) para aumentar a segurança da aplicação. A proposta de monitoramento de pacientes com demência desenvolvida em [35] demonstra que a área consegue expandir-se não somente para saúde física, mas também mental.

3.5 CONCLUSÃO

Sendo definido pela primeira vez em 1999 dentro do contexto da cadeia de suprimentos e na aplicação de tecnologias por radiofrequência, o termo veio sendo modificado e redefinido diversas vezes ao longo dos últimos 23 anos. A possibilidade de conectar esses dispositivos à internet viabilizou sua utilização como terminais, responsáveis por captar e enviar informações através de redes, beneficiando áreas como a de saúde, com sua utilização no monitoramento remoto de pacientes, e cidades inteligentes, em atividades como gestão de resíduos e gerenciamento de energia. Além disso, foram desenvolvidos diversos protocolos de comunicação e de rede que tem por finalidade garantir a segurança dos dados compartilhados.

Por fim, a implementação de um ecossistema IoT consiste em diversas decisões de projeto, pois é preciso entender as reais necessidades do sistema para saber se é necessário investir em formas de processamento de margem, névoa, nuvem, em mais de uma delas e quais as medidas de segurança de dados que precisam ser tomadas. São inegáveis os avanços e facilidades proporcionadas por essa tecnologia, e também que conceitos, hoje vistos como tendências futuras, teriam um progresso mais lento sem sua presença.

3.6 REFERÊNCIAS

[1] DHIRANI, Lubna L. NEWE, Thomas. LEWIS, Elfed. NIZAMANI, Shahzad. Cloud computing and Internet of Things fusion: Cost issues. Eleventh International Conference on Sensing Technology. Eleventh International Conference on Sensing Technology (ICST). 2017.

[2] ZAHOOR, Saniya. MIR, Roohie Naaz. Resource management in pervasive Internet of Things: A survey. Journal of King Saud University - Computer and Information Sciences. Volume 33, Issue 8. p. 921-935. 2021.

[3] MAO, W. et al. A Storage Solution for Massive IoT Data Based on NoSQL. IEEE International Conference on Green Computing and Communications. p. 50-57. 2012.

[4] SOUMYALATHA, Naveen. MANJUNATH, Kounte R. Key Technologies and challenges in IoT Edge Computing. p. 61-65. 2019.

[5] PENA, Lopez. ANGEL, Miguel. MUNOZ, Isabel Fernandez. SAT-IoT: An Architectural Model for a High-Performance Fog/Edge/Cloud IoT Platform. IEEE 2019 IEEE 5th World Forum on Internet of Things (WF-IoT'19) - Limerick, Irlanda. 2019.

[6] HOW Do IoT Devices Communicate? **Digi**. Disponível em: https://www.digi.com/blog/post/how-do-IoT-devices-communicate. Acesso em: 10 dez. de 2021.

[7] ANTÃO, Liliana. PINTO, Rui. REIS, João Pedro & Gonçalves, Gil. (2018). Requirements for Testing and Validating the Industrial Internet of Things.

[8] GERBER, Anna. KANSAL, Satwik. Making sense of IoT data. **IBM**. 26 mar. de 2020. Disponível em: https://developer.ibm.com/tutorials/IoT-lp301-IoT-manage-data/. Acesso em: 20 dez. de 2021.

[9] 10 Edge computing use case examples. **Partners**. Disponível em: https://stlpartners.com/articles/edge-computing/10-edge-computing-use-case-examples/. Acesso em: 20 dez. de 2021.

[10] DIFFERENCE Between Cloud Computing and Fog Computing. **GeeksforGeeks**. 06 mai. de 2020. Disponível em: https://www.geeksforgeeks.org/difference-between-cloud-computing-and-fog-computing/. Acesso em: 03 jan. 2022.

[11] PERERA, Charith. QIN, Yongrui. ESTRELLA, Juilio. REIFF-MARGANIEC, Stephan. VASILAKOS, Athanasios. Fog Computing for Sustainable Smart Cities: A Survey. ACM Computing Surveys. p. 50. 2017.

[12] GONFALONIERI, Alexandre. How Amazon Alexa works? You guide to Natural Language Processing (AI). **Towards Data Science**. 21 nov. de 2018. Disponível em: https://towardsdatascience.com/how-amazon-alexa-works-your-guide-to-natural-language-processing-ai-7506004709d3. Acesso em: 10 jan. 2022.

[13] ELAHI, Hassan. KHUSHBOO, Munir. EUGENI, Marco. ATEK, Sofiane. GAUDENZI, Paolo. Energy Harvesting towards Self-Powered IoT Devices. Energies 13, no. 21. 2020.

[14] GARG, N. GARG, R. Energy harvesting in IoT devices: A survey. 2017 International Conference on Intelligent Sustainable Systems (ICISS). p. 127-131. 2017.

[15] GEORGIOU, Kyriakos. XAVIER-DE-SOUZA, Samuel. EDER, Kerstin. The IoT energy challenge: A software perspective. Universidade Federal do Rio Grande do Norte. 27 jun. 2017.

[16] BERTINO, Elisa. Data Privacy for IoT Systems: Concepts, Approaches and Research Directions. Purdue University. 2016 IEEE International Conference on Big Data (Big Data). 2016.

[17] NOOR, Mardiana binti Mohamad. HASSAN, Wan Haslina. Current research on Internet of Things (IoT) security: A survey. Computer Networks. 6 ago. 2018.

[18] JOSE, DEEPA V. VIJYALAKSHMI, A. An Overview of Security in Internet of Things. Procedia Computer Science, vol. 143, p. 744-748. 2018.

[19] IN, Jie. YU, Wei. ZHANG, Nan, et al. Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications. IEEE Internet of Things Journal. 2017.

[20] SIDNA, Jeddou. AMINE, Baina. ABDALLAH, Najid. Analysis and evaluation of communication Protocols for IoT Applications. Proceedings of the 13th International Conference on Intelligent Systems: Theories and Applications. 2020.

[21] BHOLA, Siddharth. Why HTTP is not suitable for IOT applications. Cocurrency. 24 jun. 2019. Disponível em: https://www.concurrency.com/blog/june-2019/why-http-is-not-suitable-for-iot-applications. Acesso em: 13 jan. 2022.

[22] THOTA, Priyanka. Implementation and Analysis of Communication Protocols in Internet of Things. University of Nevada, Las Vegas. Mai. 2017.

[23] YEH, Chia-Shin. CHEN, Shang-Liang. LI, I-Ching. Implementation of MQTT protocol based network architecture for smart factory. Journal of Engineering Manufacture. 2021.

[24] V, Shilpa. A, Vidya. PATTAR, Santosh. MQTT based Secure Transport Layer Communication for Mutual Authentication in IoT Network. Global Transitions Proceedings, vol. 3, Issude 1, p. 60-66. Jun. 2022.

[25] MQTT Broker. Network Admin Guide, Chapter 6. Disponível em: https://www.catchpoint.com/network-admin-guide/mqtt-broker. Acesso em: 16 jan. 2022.

[26] WYTREBOWICZ, Jacek. CABAJ, Krzystof. KRAWIEC, Jerzy. Messaging Protocols for IoT Systems – A Pragmatic Comparison. Advances in Electronics, Signal Processing and Control Applied in Sensors and Systems. 18 out. 2021.

[27] Stomp: The Simple Text Oriented Messagign Protocol. Disponível em: https://stomp.github.io. Acesso em: 10 jun. 2021.

[28] VAILSHERY, Lionel Sujay. Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2030 (in billions). statista. Disponível em: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/. Acesso em: 20 jun. 2022.

[29] NI, Chunchun. CANG, Li Shan. GOPE, Prosanta. MIN, Geyong. Data anonymization evaluation for big data and IoT environment. Information Sciences, Volume 605, p. 381-392. Ago. 2022.

[30] SELVARAJ, Sureshkumar. SUNDARAVARADHAN, Suresh. Challenges and opportunities in IoT healthcare systems: a systematic review. SN Applied Sciences. 2020.

[31] Recreating Healthcare With Implantable IoT Devices. T Systems. Disponível em: https://www.t-systems.com/de/en/newsroom/expert-blogs. Acesso em: 22 jun. 2022.

[32] Internet of Things (IoT) In Healthcare Market - Growth, Trends, COVID-19 Impact, and Forescasts (2022-2027). Morder Intelligence. Disponível em: https://www.mordorintelligence.com/industry-reports/internet-of-things-in-healthcare-market. Acesso em: 26 jun. 2022.

[33] CASTRO, Diego. CORAL, William. CABRA, José, et al.Survey on IoT solutions applied to Healthcare. Universidad Nacional de Colombia. 12 out. 2017.

[34] DOMB, Menachem. ISMAIL, Yasser. DAUWED, Mohammed Ahmed, et al. Internet of Things (IoT) for Automated and Smart Applications. IntechOpen. 2019.

[35] KANSAL, ISHA. POPLI, Renu. VERMA, Jyoti, et al. Digital Image Processing and IoT in Smart Health Care - A review. 2022 International Conference on Emerging Smart Computing and Informatics (ESCI). 22 abr. 2022.

[36] Armazenar dados na borda com o Armazenamento de Blobs do Azure no IoT Edge. Microsoft. Disponível em:

https://docs.microsoft.com/pt-br/azure/iot-edge/how-to-store-data-blob?view=iotedge-2020-11&viewFallbackFrom=iotedge-. Acesso em: 28 jun. 2022.

[37] PERERA, Charith. QIN, Yongrui. ESTRELLA, Julio C, et al. Fog Computing for Sustainable Smart Cities: A Survey. ACM Computing Surveys. Mar. 2017.

[38] P., Prakasam. M., Madheswaran, P., Sujith K., et al. An Enhanced Energy Efficient Lightweight Cryptography Method for various IoT devices. ICT Express, Volume 7, Issue 4, p. 487-492. Dez. 2021.

[39] KASHANI, Mostafa Haghi. MADANIPOUR, Mona. NIKRAVAN, Mohammad, et al. A systematic review of IoT in healthcare: Applications, techniques and trends. Journal of Network and Computer Applications. Vol. 192. 15 out. 2021.