Desafios e Soluções na Segurança da Internet das Coisas(IoT)

1st Fabrício Silva Dias
Sistemas de Informação - UFG
Senador Canedo, Brasil
fabricio_silva@discente.ufg.br

2nd Filipe Augusto Lima Silva
Sistemas de Informação - UFG
Goiânia, Brasil
filipe_augusto@discente.ufg.br

3rd Guilherme Pereira Fernandes
Sistemas de Informação - UFG
Goiânia, Brasil
guilherme_fernandes@discente.ufg.br

4th João Felipe Peres Lima
Sistemas de Informação - UFG
Goiânia, Brasil
joaofelipe2@discente.ufg.br

5th Philippe Augusto Monteiro Silva
Sistemas de Informação - UFG
Goiânia, Brasil
philippe_silva@discente.ufg.br

***Abstract*—A ampla adoção de dispositivos conectados à internet, utilizados para coletar, transmitir e/ou trocar dados, tem diversas consequências em nossa sociedade. Uma dessas ramificações refere-se à segurança de nossos dados. Para assegurar essa proteção, torna-se imperativo e urgente buscar soluções para enfrentar as vulnerabilidades presentes na Internet das Coisas (IoT).**

O texto a seguir define o conceito de IoT e destaca suas diversas áreas de aplicação na sociedade, evidenciando a existência de uma ampla gama de dispositivos associados à IoT. Esta pesquisa visa primariamente analisar os desafios encontrados na garantia da segurança dos dados, apresentando exemplos concretos de vulnerabilidades existentes. Discute-se a importância de garantir a integridade dessas informações por meio da implementação de camadas de segurança, práticas robustas de autenticação, e a aplicação de atualizações regulares de firmware. Além disso, destaca-se a necessidade de conscientizar os usuários sobre boas práticas de segurança.

***Index Terms*—IoT, Vulnerabilidade, Segurança, Ataques Cibernéticos.**

I. Introdução

A Internet das Coisas (IoT), ou "Internet of Things", é um conceito amplo criado por Kevin Ashton, pioneiro tecnológico britânico, em 1999. A comunicação entre objetos físicos por meio da internet, com o objetivo de coletar, transmitir ou trocar dados, teve início em 1990 com a criação do Internet Toaster por John Romkey.

A IoT tornou-se um tema emergente de importância tanto no âmbito social quanto econômico. Esses dispositivos estão transformando a forma como vivemos, realizamos atividades e trabalhamos. Presente em vários setores sociais, a IoT tem aplicações notáveis, tais como na saúde, possibilitando o monitoramento remoto de pacientes e gestão de medicamentos; em cidades inteligentes, otimizando o tráfego, melhorando a gestão de resíduos e promovendo a segurança pública; na agricultura, com sensores que monitoram condições climáticas e otimizam a irrigação; na indústria, contribuindo para a manufatura inteligente e manutenção preditiva. Essas aplicações, entre outras, destacam a versatilidade da IoT na transformação positiva de setores e na qualidade de vida.

Entretanto, conforme cresce o uso de IoT na sociedade, os ataques cibernéticos à estes dispositivos também cresce de maneira equivalente, segundo relatórios da Check Point Software Technologies, empresa de soluções de segurança digital, no ano de 2023 mais de 50% das organizações foram alvos de ataques direcionados a dispositivos IoT, como roteadores, câmeras IP e impressoras.

Além disso, tivemos um transformação tecnológica impulsionada pela pandemia da covid-19, onde redes de aprendizado e empresas aderiram a ambientes digitais de comunicação. Como consequência disto o uso de câmeras IP e demais dispositivos IoT tornaram-se mais comuns, aumentando as entradas possíveis para os cibercriminosos e dificultando mais as formas de garantir a integridade de informações. Entre os setores mais afetados, a educação e pesquisas estão entre os principais alvos de ataques, concentrando 131 ataques semanais.

A vasta quantidade de dispositivos conectados aumenta a exposição a ameaças, e na tentativa de mitigar esses riscos é necessário que usuários e fabricantes compartilhem da responsabilidade cabível a ambas as partes. O fabricante na garantia de um projeto seguro, atualizações de Firmware, implementação de fortes meios de autenticação e fornecer informações sobre práticas segura, as quais devem ser seguidas pelos usuários, além de seguir essas instruções devem também manter o seu dispositivo atualizado, colocar senhas fortes e monitorar atividades suspeitas.

II. Fundamentos Teóricos

Todo dispositivo conectado à internet está vulnerável a ataques cibernéticos, e existem diversas possibilidades e pontos visados em cada tipo de ataque, cada um utilizando uma vulnerabilidade diferente. Esses ataques podem ser divididos em três tipos:

- Ataques por Engenharia Social: Foco em manipular usuários para obtenção de informações confidenciais ou realizar ações prejudiciais (Phishing, Ransomware).

- Ataques ao Sistema: Foco em comprometer a integridade do sistema ou sua disponibilidade (Ataque de Negação de Serviço(DoS), Ataques de Força Bruta, Injeção de Código(SQL, XSS)).
- Ataques a Dispositivo IoT: Foco em ter acesso/controle sobre um dispositivo conectado(Exploração de vulnerabilidade em dispositivo IoT).

Para lidar com os ataques cibernéticos aliados a vulnerabilidade do sistema, têm-se os seguintes mecanismos:

A. Ataques aos Sistemas

- Firewalls
- Sistema de Detecção de Intrusões(IDS)
- Sistemas de Prevenção de Intrusões

Esses mecanismos são mais utilizados na tentativa de prevenção dos ataques, atualizações em vulnerabilidades conhecidas e monitoramento contínuo são também medidas válidas.

B. Ataques por Engenharia Social

- Filtros de e-mail
- Software Antivírus

Ressalta-se também o treinamento de usuários para reconhecer e evitar ataques de phishing

C. Ataques a dispositivos IoT

- Atualizações de firmware
- Segmentação de rede
- Políticas de Segurança

Manter os dispositivos IoT atualizados com as últimas correções de segurança e patches de firmware é de suma importância, por corrigir as vulnerabilidades e melhorar a segurança global, junto com a implementação robusta, por meio de senhas fortes ou métodos multifatores dificultando a entrada de invasores. Firewall baseado em rede é também uma técnica válida, pois protege os dados assim que os mesmos entram na rede, permitindo também monitorar e bloquear o tráfego fora de sua VPN, muito útil principalmente em dispositivos M2M que possuem capacidade de processamento limitada.

Parte dos desafios encontrados, quanto ao assunto de segurança em dispositivos IoT se deve às particularidades únicas de cada ecossistema, visto a grande variedade de dispositivos, impossibilitando a criação de uma solução de forma universal. Além disso, muitos dos dispositivos são compactos e móveis, assim têm maiores limitações quanto a utilização de energia, capacidade de processamento e também armazenamento, o que faz necessário soluções de segurança que além de eficazes sejam otimizadas, para não comprometer o desempenho.

Assim, buscando lidar com tal problema, pesquisas e trabalhos desenvolvidos, vêm progredindo e com isso cada vez mais desenvolvendo uma solução, algoritmos que visão consumar menos poder computacional energético, visto as limitações de dispositivos IoT. A Lightweight Cryptography (LWC) ou criptografia leve é um campo de estudo focado no desenvolvimento de algoritmos criptográficos eficientes e otimizados, visando seu uso em IoT e sistemas embarcados. Não obstante, o fato de se ter um foco na eficiência de recursos, esses algoritmos não deixam a desejar quanto à garantia de segurança. Vários padrões de especificações foram desenvolvidos para orientar o uso da LWC em diferentes contextos, destaca-se o NIST (National Institute of Standards and Technology) e a ISO (International Organization for Standardization). A demanda por algoritmos de criptografia leve cresceu significativamente, visto a maior facilidade em aprimorar a segurança destes dispositivos, do que substituí-los por equipamentos de maior poder de processamento. Existem alguns modelos de criptografia, como SPECK, HIGHT e SIMON.

O AES (Advanced Encryption Standard) é também um algoritmo de criptografia, porém de criptografia simétrica, no entanto, é até hoje uma solução que satisfaça a necessidade de segurança e, recentemente, foi proposto uma versão otimizada deste algoritmo, por meio da simplificação de suas funções, com menos custo de desempenho e consumo de armazenamento, visando seu uso em aplicações em IoT.

III. Metodologia

Com o propósito de atingir os objetivos delineados neste trabalho, optou-se por realizar uma revisão narrativa de literatura, uma modalidade bibliográfica que possibilita uma busca não sistemática por informações, conforme destacado por Rother (2007). Essa abordagem envolve a escolha e seleção de bases de dados e periódicos científicos de maneira conveniente.

Em conformidade com o pressuposto acima e visando acessar um maior volume de trabalhos, os autores deste estudo conduziram a pesquisa no Google Acadêmico. Essa escolha foi motivada pela expectativa de encontrar uma quantidade significativa de artigos, uma vez que o Google Acadêmico é um agregador de bases de dados que engloba diversos periódicos.

O levantamento bibliográfico ocorreu no período de 15 a 22 de janeiro, utilizando os descritores ”Internet das Coisas (IoT)” e ”Segurança de dados”. A busca foi limitada a artigos e sites, todos pertencentes à língua portuguesa. Para inclusão na pesquisa, os estudos localizados precisavam abordar e enfatizar a segurança de dados associada à IoT. Foi dada especial atenção aos artigos que apresentavam dados sobre ataques a dispositivos da Internet das Coisas, pois esta pesquisa visa realizar uma análise comparativa entre anos anteriores e o ano presente.

IV. Resultados e Conclusões

Um estudo realizado por Sevin e Mohammed (2021), trás teste comparativos no uso de blockchiphers para IoT, e como resultado, os algoritmos PRESENT, SPECK, SIMON e CLEFIA fazem melhor o papel custo-benefício, consumindo menos armazenamento RAM/ROM e sem grande perda de velocidade. Partindo deste, em uma avaliação experimental, Vinícius et al. (2022) trouxeram testes, feita a aplicação deste códigos em equipamentos IoT da área da saúde, utilizando métricas de vazão e latência para analisar o impacto desses

LWC. Foi concluído que dentre os algoritmos testados, o Present apresentou o menor desempenho satisfatível, apresentando uma baixa taxa de transferência, como consequência foi escolhido o descarte deste algoritmo. Por outro lado, o AES-256 CBC teve a melhor performance entre os testados, com maior velocidade tanto na encriptação como na desencriptação da mensagem. Os resultados apresentados por essa avaliação são os seguintes:

Criptografia	Vazão Encrypt ESP32	Vazão Decrypt ESP32	Vazão Servidor	Vazão Decrypt Servidor	Tamanho Chave	Tamanho Bloco	Uso Flash (ESP32)	Uso RAM (ESP32)	Otimizações (ESP32)	Segurança Quântica
AES CBC	7.03 MB/s	7.20 MB/s	300 MB/s	300 MB/s	256 bits	128 bits	0.51 kB	0.89 kB	Acelerado por *Hardware*	Sim
PRESENT	0.07 MB/s	0.07 MB/s	15 MB/s	15 MB/s	128 bits	64 bits	3.50 kB	1.30 kB	N/A	Não
SPECK	2.02 MB/s	1.88 MB/s	290 MB/s	290 MB/s	256 bits	128 bits	3.20 kB	1.10 kB	Operações 32 bits	Sim
CLEFIA	0.65 MB/s	0.65 MB/s	120 MB/s	120 MB/s	256 bits	128 bits	2.90 kB	2.50 kB	Lookup Tables	Sim

Fig. 1. Comparação Preliminar dos Algoritmos

Entretanto, quando analisados quanto ao consumo energético causado por estes algoritmos, não se tem uma conclusão, afinal, foram testados em diferentes aparelhos e a questão de hardware infere diferenças. Adiante, foram pontuadas diferentes formas de funcionamento, não chegando a concluir alguma semelhança entre os LWC.

Por fim, concluiu-se que os algoritmos AES-256 CBC, SPECK obtiveram os melhores resultados de desempenho, o SPECK, com menor variações abruptas nos quesitos de vazão e latência conforme maior demanda de transmissão, o AES-256 CBC obteve resultado semelhante mas com mudanças mais significativas conforme a crescente taxa de transmissão.

REFERENCES

[1] DE OLIVEIRA, Nairobi Spiecker et al. Segurança da informaçao para internet das coisas (iot): uma abordagem sobre a lei geral de proteçao de dados (lgpd). Revista Eletrônica de Iniciação Científica em Computação, v. 17, n. 4, 2019.

[2] CARVALHO, André Ferreira Almeida de; SANTOS, Christyan Matteus Lima; GONÇALVES, Lucas Vaz. Segurança em IoT. 2022.

[3] ABRANET. *Ataques a dispositivos da Internet das Coisas (IoT) crescem 41%*. ABRANET. 24/04/2023. Disponível em: https://www.abranet.org.br/Noticias/Ataques-a-dispositivos-da-internet-das-coisas-(IoT)-crescem-41%25-4300.html? Acesso em: 16 jan. 2024.

[4] Carlos Campo. *O que é Segurança em IoT? Riscos, Exemplos e Soluções*. EMNIFY. Disponível em: https://www.emnify.com/pt-br/glossario-iot/seguranca-iot#:~:text=Falta%20de%20criptografia&text=Muitos%20dispositivos%20IoT%20n%C3%A3o%20criptografam,transmitidas%20para%20e%20do%20dispositivo.. Acesso em: 16 jan. 2024.

[5] VAZ, Yuri Silva; MATTOS, Júlio CB; SOARES, Rafael Iankowski. AES Otimizado para Uso em Aplicações IoT. In: Anais Estendidos do XIII Simpósio Brasileiro de Engenharia de Sistemas Computacionais. SBC, 2023. p. 31-36.

[6] SEVIN, Abdullah; MOHAMMED, Abdu Ahmed Osman. A survey on software implementation of lightweight block ciphers for IoT devices. Journal of Ambient Intelligence and Humanized Computing, v. 14, n. 3, p. 1801-1815, 2023.

[7] ZANON, Vinícius Rodrigues et al. Avaliação experimental de uma camada de segurança implementada em dispositivo vestível cardíaco para Internet das Coisas Médicas. In: Anais do XXII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais. SBC, 2022. p. 97-110.