Avaliação experimental de uma camada de segurança implementada em dispositivo vestível cardíaco para Internet das Coisas Médicas

Vinícius Rodrigues Zanon[1], Eliel M. Rocha Romancini[2], Bianca de Espíndola Manoel[3], Jim Lau[3], Fabrício de O. Ourique[2,3], Analúcia Schiaffino Morales[2,3]

[1]Programa de Pós-graduação em Engenharia Elétrica (PPGEEL)
Universidade Federal de Santa Catarina – Florianópolis, SC – Brasil

[2]Programa de Pós-graduação em Energia e Sustentabilidade (PPGES)
Universidade Federal de Santa Catarina – Araranguá, SC – Brasil

[3]Curso de Graduação em Engenharia de Computação
Universidade Federal de Santa Catarina – Araranguá, SC – Brasil

{vinicius.zanon,eliel.romancini}@posgrad.ufsc.br,
bianca.espindola@grad.ufsc.br,
{jim.lau,fabricio.ourique,analucia.morales}@ufsc.br

Abstract. *There is a growing demand for new devices for medical applications due to the advancement of the Internet of Things in healthcare. This article aims to experimentally evaluate a security layer for a cardiac wearable designed to perform electrocardiogram exams in wireless and remote networks. Low computational cost algorithms for IoMT devices were analyzed in the scientific literature to improve the robustness against man-in-the-middle and eavesdropping attacks. Three algorithms were selected and implemented (AES-256 CBC, SPECK and CLEFIA). A series of load tests were applied to analyze the performance of the security layer of the chosen algorithms, observing the latency parameters and throughput variation in the transmission of the signals. All algorithms performed satisfactorily, demonstrating that adding a security layer to the IoMT device is feasible. However, the AES-256 CBC showed the best results, being the most suitable algorithm for a cardiac wearable security layer.*

Resumo. *Existe uma demanda crescente de novos dispositivos para a área médica, considerando a Internet das Coisas. Este artigo tem como objetivo avaliar de forma experimental uma camada de segurança para um vestível cardíaco projetado para realizar exames de eletrocardiograma sem fio e remoto. Para torná-lo menos suscetível aos principais ataques conhecidos, como homem-do-meio e espionagem, métodos de criptografia foram testados para analisar sua viabilidade. Três algoritmos de criptografia (AES-256 CBC, SPECK e CLEFIA) foram implementados e comparados em um ambiente de comunicação seguro e autenticado, a fim de analisar seu desempenho com relação à latência da rede e testes de carga do dispositivo. Foram feitas várias amostras de dados de medição e posteriormente, analisado graficamente e comparado. O AES-256 CBC apresentou melhores resultados, sendo o algoritmo mais indicado para uma camada de segurança do vestível cardíaco.*

1. Introdução

Com a pandemia de COVID-19, a área de saúde passou a ser o centro das atenções em uma esfera mundial, a partir de 2020. Os sistemas de saúde intensificaram o uso de tecnologias digitais e dispositivos eletrônicos para melhorar o atendimento aos pacientes. O Brasil abriu espaço para a telemedicina como recurso para atendimento remoto de seus pacientes [Firouzi et al. 2021]. Aliado a esta ferramenta, o uso de Internet das Coisas tem sido apontado como uma alternativa para reduzir custos com saúde pública e privada e melhorar o atendimento da população [Morales et al. 2021]. Trata-se de um novo paradigma que incorpora sensores, tecnologias de comunicação, sistemas pervasivos e armazenamento em nuvem, e têm sido amplamente pesquisados para aplicações em cuidados com a saúde e bem-estar [Qadri et al. 2020]. As aplicações têm sido inúmeras, desde o monitoramento contínuo em tempo real de doenças crônicas [Moses et. al. 2022], o uso como apoio a telemedicina [Yu and Zhou 2021], o acompanhamento de saúde mental [Hickey et al. 2021], o aprimoramento de exames médicos [Dang et al. 2020], entre outras.

No entanto, tem-se observado ausência de mecanismos de segurança em diversos dispositivos que têm sido propostos nos últimos anos, como é o caso do aparelho para o controle de glicose no sangue. As bombas de insulina sem fio, como são chamadas, possuem dosagens mínimas e máximas definidas pelo FDA (*Food and Drug Administration*), órgão regulatório do governo dos Estados Unidos, e têm sido amplamente empregadas. Contudo, um mau funcionamento de uma dessas bombas pode ser letal para os usuários. Pesquisadores resolveram demonstrar como estes dispositivos são vulneráveis sem a presença de uma camada de segurança, eles testaram dois tipos de ataques. O primeiro, foi um ataque único de sobredose de insulina e o segundo tipo de ataque foi a redução em uma quantidade insignificante sendo administrada por um longo período. Ambos os tipos de ataques foram bem sucedidos, devido à falta de segurança mínima no dispositivo [Hei et al. 2015]. Em 2017, a FDA emitiu uma nota sobre um marca-passo cardíaco que possuía inúmeras vulnerabilidades de segurança. Sendo necessária a visita dos cerca de 65.000 pacientes a seus médicos para estes poderem atualizar o *firmware* do dispositivo [Stellios et al. 2018]. Este artigo menciona ainda ataques de diversas naturezas a dispositivos vestíveis na área de saúde. Destaca-se o ataque à rede de monitoramento domiciliar de pacientes, em que é extraído o *firmware* dos dispositivos conectados ao corpo do paciente através da rede, e realizado uma engenharia reversa para explorar as vulnerabilidades. A vulnerabilidade dos dispositivos vestíveis e implantáveis foi apontada como fator preocupante, devido às implicações e os diferentes tipos de ataques que podem ser realizados com os pacientes devido a inadequada segurança observada nos dispositivos e falta de privacidade dos dados [Meneghello et al. 2019; Zheng et al. 2019].

Com o avanço das novas tecnologias, praticamente todas as instituições estão sujeitas a ataques de segurança e privacidade de dados. Quando o assunto se referem aos dados médicos, a preocupação aumenta. Como por exemplo, um invasor pode fornecer informações falsas sobre usuários, de forma que pareçam reais, e como consequência, o impacto pode implicar na morte do paciente. Esta categoria de ataque pode comprometer a integridade física e mental do indivíduo [Ahmed and Barkat Ullah 2018]. Ataques de segurança podem ocorrer em qualquer camada de uma estrutura de Internet das Coisas. Na camada de rede, por exemplo, pode ocorrer um ataque homem-do-meio ou *man-in-the-middle*, em inglês [Salem et al. 2022], onde as informações verdadeiras são interceptadas do dispositivo antes de chegar na camada de rede, o atacante pode alterar

os dados e incluir dados falsos. Este tipo de problema pode ser evitado através de implementações de políticas de segurança, que bloqueiam ou ignoram as solicitações não autenticadas por meio de algoritmos criptográficos robustos e mecanismos de trocas de chaves [Firouzi et al. 2018].

Devido à natureza de informações confidenciais dos pacientes, garantir a segurança é uma questão fundamental. Especificamente, conforme a Sociedade Brasileira de Cardiologia, as doenças do coração lideram as causas de mortes desde 1960 em todo o território nacional [Oliveira et al. 2020]. Novas tecnologias têm sido aplicadas na prática clínica cardiovascular visando promover melhores diagnósticos, tratamentos mais precisos e redução de estatísticas. Embora já seja consolidado na área médica, melhorias vêm sendo agregadas ao exame de eletrocardiograma (ECG) a fim de promover conforto ao paciente e garantir a sua execução através de vestíveis e monitoramento remoto. Para que uma proposta de melhoria no ECG tradicional seja de fato usada no âmbito clínico, o sistema deve garantir que todas as informações geradas no exame, desde a aquisição, transmissão, armazenamento ou na associação aos dados pessoais do paciente, correspondam aos critérios mínimos de segurança. Dos requisitos de segurança a serem cumpridos, destacam-se: confidencialidade, integridade, autenticação e disponibilidade [Ghubaish et al. 2021].

O presente artigo tem como objetivo apresentar um estudo sobre a adaptação de um mecanismo de segurança para um vestível cardíaco. O protótipo vestível foi desenvolvido por Zanon et al. (2021) e não considerava nenhum tipo de segurança em seu desenvolvimento original. A questão a ser respondida é se uma camada de segurança pode afetar os dados do exame de ECG, considerando-se uma transmissão sem fio em tempo real. Ou seja, os testes foram direcionados ao desempenho do dispositivo acrescentando métodos criptográficos leves. Foram investigados na literatura científica, algoritmos de criptografia eficientes na proteção de dispositivos sensores para ataques do tipo homem-do-meio e de espionagem. A estratégia é garantir a troca de informações de forma segura empregando conceitos de autenticação por chaves criptográficas. Ao serem enviados ao servidor de aplicação, os dados da amostragem do sinal cardíaco passam por um processo de criptografia leve. Criando deste modo, uma camada de segurança entre o envio dos dados pelo dispositivo cardíaco e o recebimento pelo servidor. Essa comunicação é realizada apenas quando o servidor autentica o dispositivo usado e cria uma espécie de túnel de comunicação segura na rede. Após os dados chegarem ao servidor, os mesmos serão descriptografados e exibidos na página do sistema em tempo real. Foram testados três algoritmos diferentes: AES-CBC, SPECK e CLEFIA considerando as alterações de vazão e latência na rede, observando os impactos gerados durante a carga de realização dos exames.

O artigo foi estruturado em seis seções. Os aspectos relacionados à segurança em dispositivos de Internet das Coisas Médicas são discutidos na Seção 2. A Seção 3 apresenta os testes preliminares realizados para a escolha dos algoritmos de criptografia, uma breve discussão sobre o consumo de energia dos algoritmos e a implementação. A Seção 4 descreve os resultados obtidos e as discussões. Finalmente, seguem as conclusões e as referências bibliográficas.

2. Internet das Coisas Médicas

Apontada como uma área prioritária de Internet das Coisas, a Internet das Coisas Médicas (ou em inglês, *Internet of Medical Things* - IoMT), tem sido evidenciada pela literatura como uma alternativa para reduzir os custos e melhorar a saúde e bem-estar das pessoas.

O monitoramento contínuo de pacientes, sejam crianças ou idosos, tornou-se mais fácil com o uso de dispositivos não invasivos e sem fio, que podem medir dados do usuário como: pressão arterial, glicose, contagem de passos, sem que os mesmos se sintam incomodados e removam os dispositivos [Bhatia et al. 2020].

A demanda por sistemas de tempo real com alta acessibilidade e dispositivos que monitoram continuamente os parâmetros fisiológicos para o controle de doenças crônicas têm sido amplamente explorados [Qadri et al. 2020]. Diversos trabalhos sobre IoMT publicados em bases de dados reconhecidas (*IEEE Xplore, Pubmed, Google Scholar* e outras) têm características de protótipos, mas não mencionam nada a respeito de segurança e privacidade dos dados. Recentemente, foi publicado um artigo de revisão sistemática em que são discutidos os resultados das monitorações de pacientes cardíacos com o uso de diferentes dispositivos de IoMT, considerando dispositivos vestíveis e não vestíveis colocados diretamente na residência dos pacientes conectados à internet. Dos cinco trabalhos selecionados, apenas dois apresentam a avaliação por eletrocardiograma, os demais trabalhos avaliaram os pacientes através de outros parâmetros, como por exemplo, variação dos batimentos cardíacos, respiração, saturação de oxigênio, peso e postura corporal, e todos os trabalhos relacionados utilizaram a tecnologia *Bluetooth* para conectar com o *gateway* [Moses et. al. 2022]. Ainda com relação aos dispositivos de IoMT disponíveis no mercado para doenças cardiovasculares, o artigo de revisão publicado em 2022, apresenta diversos equipamentos que estão disponíveis comercialmente. O artigo relata as características dos produtos sobre uma perspectiva de certificação (aprovação pela FDA), tipos de sensores e parâmetros utilizados, a compatibilidade com sistemas operacionais, mas não apresenta questões relacionadas à segurança [Prieto-Avalos et al. 2022].

2.1. Arquitetura IoMT

Até o momento não há um consenso sobre o número de camadas de uma arquitetura de IoMT, e também ainda não existe uma padronização internacional definida. Para o contexto do presente trabalho, uma arquitetura IoMT será composta pelas camadas propostas por Al-Turjman et al. (2020):

- Sensoriamento: corresponde a camada dos sensores, onde estão as “coisas” IoT. Consiste em sensores que detectam e coletam dados do usuário, por exemplo, sensores vestíveis coletando temperatura e sinal cardíaco de pacientes.
- Transporte: camada usada para a transmissão sem fio dos dados da camada anterior. Dependendo da arquitetura, suporta diversos protocolos de comunicação, como 5G, LTE, *Bluetooth*, *WiFi*, etc.
- Processamento: a camada executa o processamento dos dados do usuário, podendo realizar técnicas de segurança nas mensagens a fim de detectar dados suspeitos e emitir avisos a camadas superiores.
- Aplicação: fornece suporte baseado nas funcionalidades do usuário final do sistema, sendo o médico ou o próprio paciente. Essa camada pode permitir uma interatividade através dos protocolos e serviços da *Web*.
- Negócios: a camada de negócio lida com todo o sistema IoT, que inclui aplicativos, modelos de negócios e informações confidenciais dos usuários.

2.2. Dispositivos vestíveis

Na camada de sensoriamento podem ser encontrados diversos componentes eletrônicos capazes de converter informações físicas em impulsos elétricos. São empregados na

detecção de vários parâmetros, tais como, temperatura corporal, batimento cardíaco, saturação de oxigênio, nível de glicose, entre outros [Bhatia et al. 2020]. Com capacidade sem fio, os sensores permitem o monitoramento de dados fisiológicos de pacientes, podendo ser incorporados em *gadgets*, acessórios ou roupas. Além disso, apresentam definições sobre a energia consumida pelos dispositivos, podendo ser classificados como vestíveis de baixa, média e alta potência [Ometov et al. 2021].

Dispositivos de baixa potência possuem capacidades limitadas de processamento e precisam operar por longos períodos com foco em aquisição de dados. São exemplos, os anéis inteligentes ou pulseiras com bateria, rádio e alguns sensores auxiliares. Em geral, os dispositivos de média potência incluem *displays* para que seja possível interagir com o agente externo. São exemplos, os relógios *smartwatches* que fazem conexão com a internet e possuem múltiplos sensores a bordo. E por fim, os dispositivos de alta potência são caracterizados por apresentar alto poder de processamento (incluindo técnicas de aprendizado de máquina). Geralmente, não funcionam a bateria e comportam altas taxas de dados. São exemplos, os óculos de realidade virtual, câmeras térmicas, entre outros.

2.3. Segurança em IoMT e dispositivos vestíveis

Garantir a segurança e privacidade das informações de dispositivos para a saúde possuem desafios relacionados à quantidade de dados, processamento, memória, sensibilidade e o alto nível de segurança exigido pelas aplicações [Perwej et al. 2022]. No contexto de IoMT [Papaioannou et al. 2020], as premissas de segurança são similares à segurança de sistemas, mas existem limitações de recursos devido à natureza dos dispositivos. Destacam-se questões relacionadas a pouca memória, capacidade de processamento limitada e área física dos dispositivos [Thakor et al., 2021]. Além disso, torna-se desafiador garantir os requisitos de segurança para esse novo paradigma, pois existem as vulnerabilidades dos protocolos de comunicação, principalmente para monitoramento de doenças cardiovasculares que utilizam *Bluetooth Low Energy* (BLE) [Prieto-Avalos et al. 2022]. Trabalhos explorando confidencialidade, integridade, não repúdio, autenticação, autorização e disponibilidade podem ser encontrados em artigos científicos aplicados a cenários de dispositivos médicos interconectados [Saba et al. 2020], [Keerthika et al. 2021], [Wang et al. 2021], [Trnka et al. 2022] e [Papaioannou et al. 2020].

Devido a diversidade de dispositivos e muitas vezes a dependência do uso de equipamentos como *smartphones*, os dados gerados pelos vestíveis podem ser interceptados e adulterados. Os desafios de segurança de vestíveis em IoMT, podem ser relacionados aos aspectos de segurança tecnológica, gerenciamento de dados e legislação [Jiang and Shi 2021; Monteiro et al. 2021]. Estes desafios quando não resolvidos criam oportunidades para ataques cibernéticos, visto que os ataques são possíveis consequências de vulnerabilidades já existentes nas implementações, como é o caso do BLE, 6LowPAN e outros protocolos de comunicação [Meneghello et al., 2019]. As principais categorias de ataques são destinadas ao controle de dados, aos dispositivos e às redes [Strielkina et al. 2018; Zakaria et al. 2019]. Quando os ataques são focados na rede, os principais objetivos dos atacantes são a coleta de informações, sequestro de dados e injeção de *malwares* [Salem et al. 2022].

Nem todos os tipos de criptografias são adequados para os dispositivos médicos, devido à sua capacidade limitada de processamento, tamanho e memória. Criptografias leves, ou *Lightweight Cryptography* (LWC), são soluções destinadas ao uso de recursos limitados que vêm sendo investigadas para este fim [Dutta et al. 2019; Thakor et al. 2021;

Thakor et al., 2021]. Os autores Hatzivasilis et al. (2018) realizaram uma análise profunda de diferentes algoritmos de criptografia leve propícios para IoT, mas sem abordar o escopo de segurança. Já o artigo apresentado por Sevin e Mohammed (2021) foca em *blockciphers* para IoT, com vinte implementações de criptografias. Concluindo que a melhor *blockcipher* (equilibrando métricas de velocidade e custo de RAM/ROM) seriam os algoritmos PRESENT, SPECK , SIMON e CLEFIA.

3. Materiais e métodos

A Figura 1 ilustra em alto nível de abstração a modelagem para a camada de segurança para o vestível cardíaco [Zanon et al., 2021, Zanon et al. 2022]. Ressalta-se que originalmente, o vestível não pertencia a uma arquitetura de IoMT, portanto durante este projeto foram consideradas as adaptações necessárias. Os fluxos de informações vão desde a camada de sensoriamento até a camada de aplicação. Na camada de sensoriamento os dados do paciente são coletados pelo dispositivo vestível, que faz o uso de um microcontrolador ESP32, e são submetidos para a camada de segurança modelada. Foi incluída uma etapa de validação de dispositivo com um servidor e, então, realizada a troca de chaves para efetuar a criptografia dos dados do paciente. Estes dados codificados são enviados para a camada de transporte onde serão descriptografados na camada de aplicação, acessada pelo médico ou paciente monitorado de forma remota. Este artigo, tem o foco em avaliar os diferentes algoritmos aplicados a camada de segurança projetada para o protótipo de vestível cardíaco adaptado. Ressalta-se que esse sistema foi pensado para o uso de vestível em clínica ou na residência dos pacientes, não sendo um ambiente com segurança e privacidade controlada.

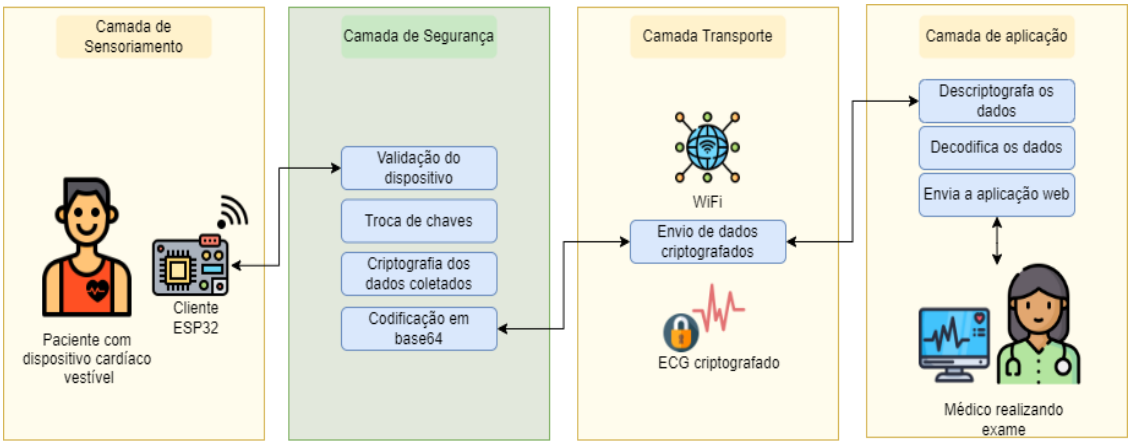

Figura 1. Modelagem da camada e interações com os dispositivos

A partir da investigação na literatura foram escolhidos para os testes os algoritmos de criptografia leve: AES-256 CBC (*hardware* ESP32), PRESENT (*software*), SPECK (*software*), CLEFIA (*software*). Além disso, foram definidas as métricas de vazão (*throughput*, em inglês) e a latência para avaliar o impacto da criptografia leve na execução dos exames. Na Tabela 1, são apontadas as principais características a partir de testes preliminares realizados com cada um dos algoritmos. O algoritmo PRESENT apresentou o pior resultado, obtendo a menor taxa de transferência entre todos os algoritmos testados, e não possui nenhum mecanismo para acelerar o processamento. Portanto, decidiu-se por descartá-lo dos demais testes para a camada de segurança do vestível.

Tabela 1. Comparação preliminar dos algoritmos

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

A criptografia AES-256 CBC integrada no microcontrolador ESP32, apresentou o melhor desempenho em comparação com os demais algoritmos considerados. Ou seja, a quantidade de dados transferidos foi muito superior aos demais, tanto para encriptar quanto para decriptar a mensagem. Já que se trata de uma unidade de *hardware* dedicado, é esperado que esta possua uma boa eficiência, no entanto, ela está limitada a um pequeno conjunto de algoritmos fixos, quaisquer outros que sua aplicação desejar usar, terá de ser implementado através de código em *software*.

Buscando analisar a influência do consumo energético pelos algoritmos selecionados, investigou-se trabalhos publicados na literatura científica que fizeram testes de consumo de energia. A Tabela 2 apresenta um resumo dos resultados de comparações entre os algoritmos criptográficos. Observa-se nos resultados valores totalmente diferentes, pois o consumo de energia é dependente do tipo de *hardware*, cenário de teste, bem como, o método matemático utilizado para extração dos valores [Makarenko et al., 2020]. Cada artigo apresentou um padrão de consumo distinto e não foi encontrada uma similaridade comportamental entre os algoritmos. Desse modo, não foram realizados os testes neste estudo levando em consideração o consumo de energia, apenas as métricas de avaliação vazão e latência.

Tabela 2. Consumo de energia dos algoritmos de criptografia leve

Refs.	AES CBC	PRESENT	SPECK	CLEFIA
[Makarenko et al., 2020]	56.80 mW	57.0 mW	56.80 mW	56.90mW
[Buhrow et al. 2015]	0.29 uJ/byte	-	0.12 uJ/byte	-
[Qasaimeh et al., 2021]	0.17 uW	0.10 uW	-	0.10 uW
[Banik et al., 2016]	350 pJ	172.3 pJ	-	-
[Thakor et. al, 2021]	42.38 uJ/bit (HW)	11.77 uJ/bit (HW)	73.67 uJ/bit (HW)	36.82 uJ/bit (HW)
	16.70 uJ/bit (SW)	43.10 uJ/bit (SW)	1.60 uJ/bit (SW)	114.50 uJ/bit (SW)
[Thorat & Inamdar, 2018]	6.4 pJ/bit	4.3 pJ/bit	-	4.7 pJ/bit

3.1 Implementação

Primeiramente, o dispositivo vestível (controlado pelo módulo ESP32) realiza a inicialização do seu sistema operacional e configura suas interfaces. Após este passo, conecta-se a uma rede *WiFi* previamente configurada. Ao conectar com sucesso adquire um IP através do protocolo DHCP. Caso o processo falhe, conectará em outra rede pré-configurada (se houver) e tentará novamente adquirir um IP. Com a rede e IP validados o dispositivo está apto para realizar a configuração de tempo. Nesta etapa, é realizada uma conexão com o servidor de tempo brasileiro (NTP), onde sincroniza com precisão a data e hora do seu relógio interno.

Após validar a conexão e ajustar o relógio interno, o dispositivo inicia o processo para estabelecer uma comunicação com o servidor. Então, conecta-se ao IP do servidor e efetua transações HTTP para validar uma seção Socket.io. Com a conexão estabelecida,

o vestível envia o seu token interno (identificação do dispositivo), de modo a validar com o servidor que se trata de uma entidade conhecida. Ao verificar com sucesso, o servidor confirma para dar prosseguimento à comunicação.

Na primeira etapa do procedimento de troca de chaves o servidor e o dispositivo geram internamente um conjunto de chaves pública e privada. Na segunda etapa, ocorre a troca das chaves públicas, de forma que os dois derivam um segredo compartilhado. Ao combinarem as chaves recebidas com a chave privada, terão como resultado uma chave compartilhada que será usada para criptografar a comunicação entre dispositivos e avisar ao servidor que está apto para se comunicar através de mensagens criptografadas. Caso o processo de troca de chaves ocorra sem problemas, o servidor consegue descriptografar a mensagem e identifica que o procedimento ocorreu com sucesso. Com todo o processo de segurança validado, os dados podem ser trocados de forma segura. O dispositivo irá enviar todos os dados do paciente que necessita até finalizar o processo. A Figura 2 apresenta o fluxograma para a implementação dos algoritmos.

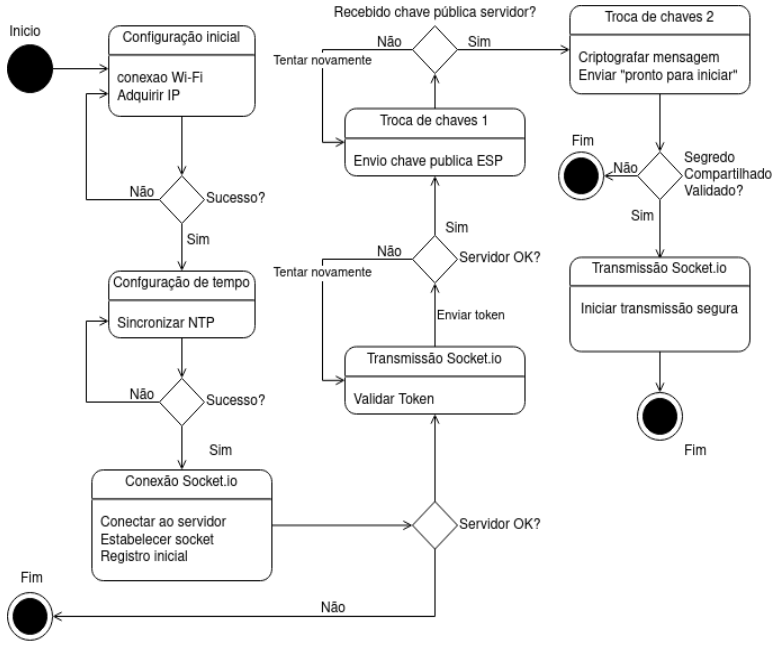

Figura 2. Modelagem da camada e interações com os dispositivos

3.2 Arquitetura cliente-servidor

Este modelo de arquitetura de rede possui duas entidades: os clientes que executam tarefas baseadas no usuário e os servidores que providenciam tarefas com base nos serviços requisitados pelo usuário. Existem dois clientes distintos neste modelo: a aplicação *web* interagida pelo usuário (médico) e o módulo ESP32 localizado no colete usado pelo paciente. As requisições entre a aplicação *web* e o servidor, são feitas através do protocolo HTTP. Para a troca de informação entre o vestível e o servidor é usada a comunicação baseada em cliente-servidor, *Websocket*.

3.3 Testes e experimentação

Para realizar a análise completa de todo o sistema em execução, foi criado um *script* de teste para ajustar alguns parâmetros, como: sincronização de relógios, ajuste de quantidade de amostras, ajuste de criptografia e armazenamento de resultados. Primeiro

é realizado todo o processo de inicialização e autenticação das entidades, neste momento ambos estão aptos para troca de mensagens. Em seguida, para mensurar a latência de comunicação, é realizado um processo de sincronização de relógios entre o módulo e o servidor, de modo a registrar nas mensagens o tempo inicial e final de transmissão. Além disso, o servidor configura o dispositivo para iniciar a transmissão dos dados e define a criptografia desejada. Após um período de teste recebendo os dados e gerando relatórios, o dispositivo pode ser configurado para transmitir outro conjunto de amostras.

A estrutura dos dados do teste, possui o formato JSON. O servidor ao receber este pacote, realiza a decriptação das amostras, utilizando a chave que compartilha com o dispositivo. No momento em que este dado é recebido também é registrado o *timestamp* com precisão de microssegundos, e comparado com o *timestamp* contido na mensagem. Desta forma é possível inferir a latência desde a criação do pacote até seu recebimento com sucesso no servidor. Os testes são executados por um tempo pré-definido, até que seja completo uma rodada de testes e uma ou mais variáveis do teste sejam modificadas, sendo elas a quantidade de amostras (de 100 a 1000 amostras por pacote) e a criptografia utilizada (sem criptografia, AES-256 CBC, SPECK e CLEFIA). A cada rodada são registradas as quantidades médias de bytes recebidos, pacotes e latência.

4. Resultados e Discussões

Uma série de testes foram realizados e os resultados obtidos são apresentados a seguir. Para mapear o comportamento de cada um dos algoritmos, dado um tamanho de amostra, o gráfico da Figura 3 ilustra os resultados dos testes comparando todos os algoritmos. As linhas contínuas são os resultados da vazão e as linhas pontilhadas são as latências. Conforme mencionado na seção 3, o algoritmo PRESENT foi descartado nos testes preliminares devido aos resultados apresentados.

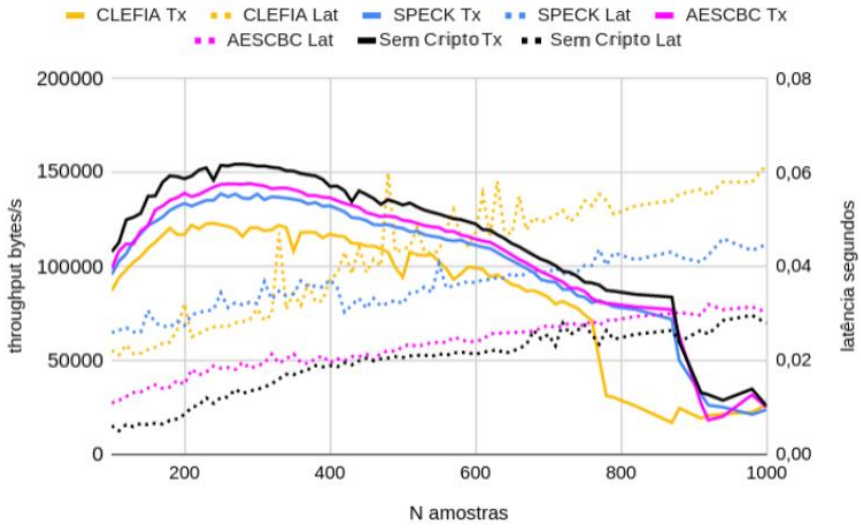

Figura 3. Resultados dos testes

Além disso, para fins de análise e de comparação, um teste foi realizado sem o uso de criptografia. Esta análise serviu para verificar o funcionamento dos dispositivos sem a função implementada e assim ter resultados de medição para comparar com os algoritmos que estão sendo avaliados. Ou ainda, avaliar se estes algoritmos alteram significativamente o desempenho na realização do exame cardíaco. Para este cenário entre o vestível e o servidor onde o dispositivo apenas envia as amostras sem criptografia

(linhas em preto), apresentou como resultado maior vazão e menor latência. Este é o resultado base que seria o melhor cenário para o experimento, isto é, sem a implementação da camada de segurança. É possível observar que o pico de vazão se encontra com o tamanho do pacote entre 200 a 400 amostras. Este pico de vazão de dados está relacionado à proximidade do tamanho do pacote em bytes com o valor do MTU (*Maximum Transmission Unit*) da rede, padrão de 1500 bytes. Quando os pacotes estão entre 1500 e 3000 bytes, a transmissão está num nível ótimo de fragmentação. Acima deste valor há uma perda de desempenho e um crescimento na latência, justificadas pelas dinâmicas de transmissão dos protocolos *WiFi* e TCP (*Transport Control Protocol*).

Também foram observadas as variações de vazão para cada tamanho de pacote. Ela apresenta maior oscilação quando o tamanho do pacote é menor (situação comum no uso da rede sem fio). Porém há uma redução nas variações quando o conjunto de amostras é maior, chegando abruptamente próximo de zero o valor da vazão.

Durante os testes o algoritmo AES-256 CBC (implementado em *hardware*), apresentou pouca influência na taxa de dados, no entanto é possível observar que a partir de 500 amostras a latência aumentou consideravelmente. Já o algoritmo de criptografia SPECK (baseada em *software*) teve um desempenho semelhante ao AES-256 CBC, porém a vazão máxima diminuiu e a latência manteve-se aumentando. Através do gráfico (Figura 3), observa-se que durante o período do teste obtiveram-se menos variações bruscas, tanto de latência quanto na vazão para o algoritmo SPECK. Além disso, com uma variação de dados entre 200 a 500 amostras, o algoritmo não afetou a capacidade de transmissão mesmo baseado em *software*.

Por fim, o algoritmo CLEFIA obteve o menor desempenho. Sua vazão ficou a menor entre todas as criptografias, não ultrapassando 125000 bytes por segundo. Apesar de apresentar maior latência, houve pouca diferença quando enviado menos de 400 amostras. Após este valor, a latência teve seu valor dobrado quando comparada ao algoritmo AES-256 CBC.

4.1. Análise dos resultados

Para auxiliar na construção da camada de segurança foi realizada a implementação de um canal de comunicação *WebSocket*, troca de chaves não fixas, autenticação e criptografia. Os resultados apresentaram valores de vazão suficientes para a realização de um exame em tempo real, conforme demonstrado por Zanon et al. (2021) com um ECG amostrado a uma taxa de 500Hz, ou ainda, 500 amostras por pacote a cada segundo.

Em um cenário onde um pacote contém 500 amostras (cerca de 3500 bytes) a vazão aproxima-se de 100000 bytes por segundo, levando em consideração o pior caso de implementação (algoritmo CLEFIA). Desse modo é possível que seja enviado até 28 pacotes do ECG por segundo, sem interferir na taxa de amostragem original do protótipo vestível cardíaco e garantir uma camada de segurança para o dispositivo. Para tornar a coleta de dados menos suscetível a ataques, fazer o uso do algoritmo de criptografia AES-256 CBC é uma opção viável para o caso estudado. Além disso, apresenta como vantagem a fácil implementação, já que está otimizado e acelerado em *hardware*. Estas características não prejudicam a comunicação, demonstrando uma capacidade de transmissão similar a implementação sem criptografia.

Caso o dispositivo de estudo não possua uma unidade de criptografia embarcada, é possível optar por uma solução utilizando o algoritmo SPECK. Apesar de possuir teoricamente um terço da velocidade do algoritmo AES-256 CBC, nos testes realizados

o impacto foi relativamente pequeno, garantindo ainda a capacidade de transmissão acima de 100000 bytes. Uma segunda solução seria a adoção da criptografia CLEFIA, a qual mostrou um desempenho reduzido. Sendo assim, uma opção viável para dispositivos que não enviam quantidades de dados elevadas e não demandam de aplicações em tempo real. Estes dados criptografados por quaisquer algoritmos possuem suas chaves seguras e únicas apenas para cliente e servidor. Isso se deve ao procedimento de autenticação segura, fazendo com que tentativas de adquirir dados ou chaves durante o processo de transmissão das mensagens seja dificultado. Criando, dessa forma, uma camada a mais de segurança para o paciente e a entidade que está realizando o exame cardíaco.

5. Considerações finais

Sem dúvidas, as questões relacionadas à segurança e a privacidade de dados são cruciais para a Internet das Coisas Médicas ou IoMT. Soluções escaláveis para os desafios encontrados na aquisição, transferência e armazenamento dos dados têm sido encontradas na literatura científica, mas poucos avanços em ambientes reais têm sido registrados. Muitas vezes, não são mencionadas as questões relacionadas à segurança de informação dos dispositivos, ou a privacidade dos dados dos pacientes. Neste contexto, sabe-se que os dados são considerados sensíveis e podem comprometer a integridade física, mental e emocional de um paciente (ao ser exposto) ou passar por uma experiência de ataque cibernético.

Implementações de medidas de segurança em todos os níveis da arquitetura de IoMT tem sido pesquisada pela comunidade científica, foram encontrados artigos recentes que abordam o tema com bastante propriedade. Visando analisar a viabilidade de uma camada de segurança para os dados que são enviados a um servidor pelo dispositivo vestível durante o exame de eletrocardiograma proposto, este trabalho realizou a análise de três algoritmos de criptografia empregados nas mensagens enviadas entre o dispositivo e o servidor. A partir dos resultados apresentados é possível comprovar a viabilidade de implementação de uma camada de segurança para realizar uma solução de comunicação segura entre as entidades da arquitetura de IoMT aplicadas aos exames cardíacos. Apesar de ser um ponto importante, o consumo de energia não foi considerado nos testes, ficando como sugestão para trabalhos futuros uma comparação do consumo de energia de cada um dos algoritmos de criptografia estudados.

Referências

Ahmed, M. and Barkat Ullah, A. S. S. M. (2018). False Data Injection Attacks in Healthcare. *Communications in Computer and Information Science*, v. 845, p. 192–202.

Al-Turjman, F., Nawaz, M. H. and Ulusar, U. D. (15 jan 2020). Intelligence in the Internet of Medical Things era: A systematic review of current and future trends. *Computer Communications*, v. 150, n. December 2019, p. 644–660.

Banik, S., Bogdanov, A., Regazzoni, F. (2016). Exploring Energy Efficiency of Lightweight Block Ciphers. In: Dunkelman, O., Keliher, L. (eds) Selected Areas in Cryptography – SAC 2015. SAC 2015. Lecture Notes in Computer Science, vol 9566. Springer, Cham. https://doi.org/10.1007/978-3-319-31301-6_10

Bhatia, H., Panda, S. N. and Nagpal, Di. (2020). Internet of Things and its Applications in Healthcare-A Survey. *ICRITO 2020 - IEEE 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)*,

p. 305–310.

Buhrow, B., Riemer, P., Shea, M., Gilbert, B., Daniel, E. (2015). Block Cipher Speed and Energy Efficiency Records on the MSP430: System Design Trade-Offs for 16-Bit Embedded Applications. In: Aranha, D., Menezes, A. (eds) Progress in Cryptology - LATINCRYPT 2014. LATINCRYPT 2014. Lecture Notes in Computer Science, vol 8895. Springer, Cham. https://doi.org/10.1007/978-3-319-16295-9_6

Dang, V. B., Farahmand, F., Andrzejczak, M., et al. (2020). Implementation and Benchmarking of Round 2 Candidates in the NIST Post-Quantum Cryptography Standardization Process Using Hardware and Software/Hardware Co-design Approaches. *Cryptology ePrint Archive*,

Dutta, I. K., Ghosh, B. and Bayoumi, M. (2019). Lightweight cryptography for internet of insecure things: A survey. *2019 IEEE 9th Annual Computing and Communication Workshop and Conference, CCWC 2019*, p. 475–481.

Firouzi, F., Rahmani, A. M., Mankodiya, K., et al. (2018). Internet-of-Things and big data for smarter healthcare: From device to architecture, applications and analytics. *Future Generation Computer Systems*, v. 78, p. 583–586.

Gandhi, D. A. and Ghosal, M. (2018). Intelligent Healthcare Using IoT: A Extensive Survey. *Proceedings of the International Conference on Inventive Communication and Computational Technologies, ICICCT 2018*, n. Icicct, p. 800–802.

Ghubaish, A., Salman, T., Zolanvari, M., et al. (2021). Recent Advances in the Internet-of-Medical-Things (IoMT) Systems Security. *IEEE Internet of Things Journal*, v. 8, n. 11, p. 8707–8718.

Hatzivasilis, G., Fysarakis, K., Papaefstathiou, I. and Manifavas, C. (2018). A review of lightweight block ciphers. *Journal of Cryptographic Engineering*, v. 8, n. 2, p. 141–184.

Hei, X., Du, X., Lin, S., Lee, I. and Sokolsky, O. (2015). Patient Infusion Pattern based Access Control Schemes for Wireless Insulin Pump System. *IEEE Transactions on Parallel and Distributed Systems*, v. 26, n. 11, p. 3108–3121.

Hickey, B. A., Chalmers, T., Newton, P., et al. (2021). Smart devices and wearable technologies to detect and monitor mental health conditions and stress: A systematic review. *Sensors*, v. 21, n. 10, p. 1–17.

Makarenko, I. ; Semushin, S.; Suhai, S.; Ahsan Kazmi,S. M.; Oracevic, A. and Hussain, R. "A Comparative Analysis of Cryptographic Algorithms in the Internet of Things," *2020 International Scientific and Technical Conference Modern Computer Network Technologies (MoNeTeC)*, 2020, pp. 1-8, doi: 10.1109/MoNeTeC49726.2020.9258156.

Jiang, D. and Shi, G. (2021). Research on Data Security and Privacy Protection of Wearable Equipment in Healthcare. *Journal of Healthcare Engineering*, v. 2021.

Keerthika, N., Rai, R. S., Iyswariya, A., et al. (2021). IoT Secure Framework for Wearable Sensor Data for E-health System. *Proceedings of the 5th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), I-SMAC 2021*, p. 211–215.

Meneghello, F., Calore, M., Zucchetto, D., Polese, M. and Zanella, A. (2019). IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices. *IEEE Internet of Things Journal*, v. 6, n. 5, p. 8182–8201.

Monteiro, A., Soares, A., José, A., et al. (2021). Diretriz para o Registro de Dados de Pacientes na vigência da Lei Geral de Proteção de Dados (LGPD). p. 1–11.

Morales, A. S., Ourique, F. D. O., & Cazella, S. C. (2021). A Comprehensive Review on the Challenges for Intelligent Systems Related with Internet of Things for Medical Decision. Enhanced Telemedicine and e-Health, 221-240.

Moses, J.C.; Adibi, S.; Angelova, M.; Islam, S.M.S. (2022). Smart Home Technology Solutions for Cardiovascular Diseases: A SystematicReview. *Appl. Syst. Innov.*,*5*, 51. https://doi.org/10.3390/asi5030051

Oliveira, G. M. M. De, Brant, L. C. C., Polanczyk, C. A., et al. (2020). Estatística Cardiovascular – Brasil 2020. *Arquivos Brasileiros de Cardiologia*, v. 115, n. 3, p. 308–439.

Ometov, A., Shubina, V., Klus, L., et al. (2021). A Survey on Wearable Technology: History, State-of-the-Art and Current Challenges. *Computer Networks*, v. 193, n. December 2020.

Papaioannou, M., Karageorgou, M., Mantas, G., et al. (2020). A Survey on Security Threats and Countermeasures in Internet of Medical Things (IoMT). *Transactions on Emerging Telecommunications Technologies*, n. June, p. 1–15.

Perwej, Y., Akhtar, N., Neha Kulshrestha and Mishra, P. (2022). A Methodical Analysis of Medical Internet of Things (MIoT) Security and Privacy in Current and Future Trends. *Journal of Emerging Technologies and Innovative Research*, v. 9, n. 1, p. d346–d371.

Prieto-Avalos, G., Cruz-Ramos, N. A., Alor-Hernández, G., Sánchez-Cervantes, J. L., Rodríguez-Mazahua, L., & Guarneros-Nolasco, L. R. (2022). Wearable Devices for Physical Monitoring of Heart: A Review. *Biosensors*, *12*(5), 292. https://doi.org/10.3390/bios12050292

Qadri, Y. A., Nauman, A., Zikria, Y. Bin, Vasilakos, A. V. and Kim, S. W. (1 apr 2020). The Future of Healthcare Internet of Things: A Survey of Emerging Technologies. *IEEE Communications Surveys and Tutorials*, v. 22, n. 2, p. 1121–1167.

Qasaimeh, M.; Al-Qassas, R.S.; Ababneh, M. Software Design and Experimental Evaluation of a Reduced AES for IoT Applications. *Future Internet* **2021**, *13*, 273. https://doi.org/10.3390/fi13110273

Saba, T., Haseeb, K., Ahmed, I. and Rehman, A. (2020). Secure and energy-efficient framework using Internet of Medical Things for e-healthcare. *Journal of Infection and Public Health*, v. 13, n. January, p. 1567–1575.

Salem, O., Alsubhi, K., Shaafi, A., et al. (2022). Man-in-the-Middle Attack Mitigation in Internet of Medical Things. *IEEE Transactions on Industrial Informatics*, v. 18, n. 3, p. 2053–2062.

Sevin, A. and Mohammed, A. A. O. (2021). A survey on software implementation of lightweight block ciphers for IoT devices. *Journal of Ambient Intelligence and Humanized Computing*, n. 0123456789.

Stellios, I., Kotzanikolaou, P., Psarakis, M., Alcaraz, C. and Lopez, J. (2018). A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services. *IEEE Communications Surveys and Tutorials*, v. 20, n. 4, p. 3453–3495.

Strielkina, A., Kharchenko, V. and Uzun, D. (2018). Availability models for healthcare IoT systems: Classification and research considering attacks on vulnerabilities.

Proceedings of 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies, DESSERT 2018, p. 58–62.

Thakor, V. A., Razzaque, M. A. and Khandaker, M. R. A. (2021). Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities. *IEEE Access*, v. 9, p. 28177–28193.

Thorat, C.G. and Inamdar, V.S. (2018), "Implementation of new hybrid lightweight cryptosystem", *Applied Computing and Informatics*, Vol. 16 No. 1/2, pp. 195-206. https://doi.org/10.1016/j.aci.2018.05.001

Trnka, M., Abdelfattah, A. S., Shrestha, A., Coffey, M. and Cerny, T. (2022). Systematic Review of Authentication and Authorization Advancements for the Internet of Things. *Sensors*, v. 22, n. 4, p. 1–24.

Vishnu, S. and Jino Ramson, S. R. (2021). An Internet of Things Paradigm: Pandemic Management (incl. COVID-19). *Proceedings - International Conference on Artificial Intelligence and Smart Systems, ICAIS 2021*, p. 1371–1375.

Wang, Z., Sun, P., Luo, N. and Guo, B. (2021). A Three-Party Mutual Authentication Protocol for Wearable IOT Health Monitoring System. *Proceedings - 5th IEEE International Conference on Smart Internet of Things, SmartIoT 2021*, p. 344–347.

Wu, T., Wu, F., Qiu, C., Redouté, J.-M. and Yuce, M. R. (2020). A Rigid-Flex Wearable Health Monitoring Sensor Patch for IoT-Connected Healthcare Applications. *IEEE Internet of Things Journal*, v. 7, n. 8, p. 6932–6945.

Yu, H. and Zhou, Z. (2021). Optimization of IoT-Based Artificial Intelligence Assisted Telemedicine Health Analysis System. *IEEE Access*, v. 9, p. 85034–85048.

Zakaria, H., Abu Bakar, N. A., Hassan, N. H. and Yaacob, S. (2019). IoT security risk management model for secured practice in healthcare environment. *Procedia Computer Science*, v. 161, p. 1241–1248.

Zheng, G., Shankaran, R., Yang, W., et al. (2019). A Critical Analysis of ECG-Based Key Distribution for Securing Wearable and Implantable Medical Devices. *IEEE Sensors Journal*, v. 19, n. 3, p. 1186–1198.

Zanon, V., Romancini, E., Ourique, F., and Morales, A. S. (2021). Dispositivo com Interface Vestível para a Aquisição, Processamento e Transmissão do Sinal Cardíaco em Exame de Eletrocardiograma. In *Anais do XXI Simpósio Brasileiro de Computação Aplicada à Saúde*, (pp. 48-59). Porto Alegre: SBC. doi:10.5753/sbcas.2021.16052

Zanon, V. R., Romancini, E. M. R., de Oliveira Ourique, F., and Morales, A. S. (2022). Wearable technology for electrocardiogram and vectocardiogram using the Dower Transformation. *Journal of Health Informatics*, *14*(1).