Privacidade dos dados dos usuários na medição inteligente: analisando o desempenho e a viabilidade

Tiago Bornia de Castro * **Natalia Castro Fernandes** *

* *Midiacom - PPGEET - Escola de Engenharia, Universidade Federal Fluminense, RJ (e-mail: tiago_bornia@id.uff.br) (e-mail: nataliacf@id.uff.br)*

Abstract: Smart grids allow more connectivity between the end-user and the electric utility. Residential meters are replaced by smart meters, enabling near real-time communication between customer and company. The metering data serves to billing, monitoring, and service delivery. However, the interception of a malicious entity, or the misused by the utility, could expose customer privacy. With this comes the need to protect the privacy of end-users. Literature solutions discuss techniques such as data aggregation, homomorphic encryption, trusted third-party service, and blind signing to solve this problem. This article performs a qualitative and quantitative comparison of measurement models focused on operations data, considering the privacy aspect of user data. As a result, the blind signing model excelled in the security analysis and had 50% lower CPU usage than the partially homomorphic encryption model..

Resumo: Nas redes elétricas inteligentes, há uma maior conectividade entre o usuário final e a empresa de energia elétrica. Os medidores residenciais são substituídos por medidores inteligentes, possibilitando a comunicação quase em tempo real entre cliente e empresa. Esses dados de medição podem ser usados no faturamento, operações e prestação de serviços. Entretanto, a privacidade do cliente pode ser exposta se os dados forem interceptados por um indivíduo malicioso, ou se forem usados de forma indevida pela própria empresa de energia. Com isso, surge a necessidade de proteger a privacidade dos usuários finais. As soluções da literatura discutem técnicas como agregação de dados, criptografia homomórfica, serviço de terceiros confiáveis e assinatura às cegas para solucionar esse problema. Este artigo realiza a comparação qualitativa e quantitativa dos modelos de medição voltados para os dados de operações, considerando o aspecto da privacidade dos dados dos usuários. Como resultado, o modelo de assinatura às cegas se destacou na análise de segurança e apresentou o uso de CPU 50% menor que o modelo de criptografia parcialmente homomórfica.

Keywords: Privacy; Cybersecurity; *Blind* Signature; Cryptography; Smart Metering; Smart Grid.

Palavras-chaves: Privacidade; Cibersegurança; Assinatura às cegas; Criptografia; Medição Inteligente; Redes Elétricas Inteligentes.

1. INTRODUÇÃO

A rede elétrica inteligente é uma evolução da rede energia elétrica tradicional. Com sua implantação, as unidades consumidoras passam a ter um fluxo bidirecional de energia e de informação. E o ponto chave dessa comunicação é a instalação de medidores inteligentes nas unidades consumidoras.

Os medidores inteligentes reportam dados de medição dos usuários para a empresa de energia quase em tempo real. Os dados de medição podem ser usados para faturamento, operações da rede elétrica e para prover serviços, como mostrado em (Asghar et al. (2017)), permitindo que a empresa tenha mais informações sobre o comportamento dos usuários, e que o usuário tenha informação mais detalhada sobre o seu próprio consumo. Assim, a empresa pode monitorar a qualidade da energia da rede, oferecer programas de gerenciamento de energia pelo lado da demanda ou até mesmo melhorar o *forecast* da demanda de energia elétrica (nos casos em que os consumidores enviam a previsão de consumo para a próxima hora).

Entretanto, esses benefícios também trazem riscos. A privacidade do usuário pode ser exposta se os dados de medição forem interceptados por um agente malicioso, ou se forem usados de forma indevida pela própria empresa de energia elétrica. E quanto maior a granularidade dos dados reportados, mais informações se pode extrair sobre os hábitos de consumo do usuário (Eibl and Engel (2014)). Reportar os dados em um intervalo maior de tempo ajuda a camuflar os hábitos do usuário monitorado, entretanto, não protege integralmente a privacidade do usuário.

Diante desse cenário, surge o desafio de estabelecer uma comunicação segura e que preserve a privacidade dos usuários. Muitos trabalhos já foram propostos para ten-

tar solucionar esse desafio, e podem ser encontrados em *surveys* como (Finster and Baumgart (2015)), (Asghar et al. (2017)) e (Sultan (2019)). Os artigos relacionados frequentemente usam agregação de dados, onde os dados dos diversos clientes são agregados localmente, protegendo a privacidade dos usuários. Outra prática comum é o uso de múltiplos pseudônimos relacionados à um mesmo medidor, dificultando que um dado de medição seja associado à um cliente específico (Dorri et al. (2019)).

Apesar desses *surveys* apresentarem diversas soluções para segurança e privacidade, as propostas geralmente esbarram em um dos dois problemas: ou dependem de um terceiro confiável ou de um esquema de criptografia homomórfica, que possui um elevadíssimo custo computacional. Outras propostas utilizam sistemas de armazenamento de energia para camuflar a curva de energia do usuário e dificultar a identificação dos hábitos de consumo dos clientes. Entretanto, os sistemas de armazenamento têm um custo elevado e a capacidade de camuflagem é proporcional à capacidade do sistema de armazenamento, conforme relatado por (Guan et al. (2018)).

Uma outra técnica interessante, porém menos utilizada é a assinatura às cegas. Ela pode ser usada com objetivo de certificar de forma anônima o pseudônimo associado à um medidor inteligente, protegendo assim a privacidade do usuário (Finster and Baumgart (2013)). A assinatura às cegas também representa uma solução com custo computacional mais baixo que às propostas baseadas em criptografia homomórfica.

Esse artigo levanta os principais modelos para proteger a privacidade do usuário na medição inteligente e analisa o impacto de cada um em termos computacionais e em capacidade de proteger os dados dos clientes. Embora existam propostas com arquiteturas bem distintas na literatura para segurança na medição inteligente, faltam trabalhos que comparem os custos técnicos, de forma quantitativa e qualitativa. Assim, é desenvolvida uma análise de desempenho comparando as técnica de assinatura às cegas, criptografia homomórfica e os sistemas baseados em um terceiro confiável, considerando tanto o aspecto de custo computacional quanto de custo em rede de comunicação. O objetivo é avaliar a metodologia de cada proposta, ressaltando fragilidades em termos de segurança e o custo associado.

Na comparação dos modelos, o modelo de assinatura às cegas apresentou um desempenho intermediário em relação aos demais. O modelo de criptografia homomórfica apresentou o pior desempenho, enquanto o modelo de confiança em terceiro mostrou o melhor desempenho. Quanto à análise qualitativa, o modelo de confiança em terceiro apresentou o pior nível de segurança, e o sistema com assinatura às cegas foi o mais seguro.

O restante do trabalho está dividido da seguinte forma. A Seção 2 apresenta os trabalhos relacionados. A Seção 3 apresenta as técnicas de criptografia utilizadas nos modelos de medição. A Seção 4, exibe uma visão geral do sistema. A Seção 5, detalha os modelos de medição. A Seção 6, apresenta os testes e análises de resultados. E finalmente, a Seção 7 conclui o trabalho.

2. TRABALHOS RELACIONADOS

Guan et al. propõem o uso de uma blockchain privada para agregar e armazenar os dados de medição (Guan et al. (2018)). Para preservar a identidade dos usuários, cada medidor inteligente é capaz de gerar diversos pseudônimos. A cada momento o medidor pode registrar seu consumo na blockchain com um pseudônimo diferente, dificultando a associação entre um dado de medição a um usuário específico. Nesta solução, a agregação de dados é feita com privacidade e de forma descentralizada, dificultando o vazamento dos dados para agentes maliciosos externos. Entretanto, os autores utilizam um método baseado em terceiro confiável para realizar o faturamento com os dados coletados.

Zhang et al. apresentam um esquema descentralizado de preservação de privacidade de medição baseado em blockchain de consórcio (Zhang et al. (2020)). Uma bateria é utilizada para camuflar os hábitos dos usuários. Os medidores de uma região utilizam um esquema de assinatura em anel, desta forma o agregador da empresa de energia não consegue associar a mensagem de consumo ao medidor correspondente. Os *gateways* agregadores participam da blockchain e armazenam os dados de cada região. Neste trabalho, os autores também utilizam um método baseado em terceiro confiável, entretanto dividindo a responsabilidade do terceiro confiável entre duas entidades. Não há garantia que não haverá comunicação entre os dois equipamentos.

Tonyali et al. propõem uso de criptografia homomórfica em redes mesh sem fio (Tonyali et al. (2018)). Os protocolos propostos ocultam os dados de leitura dos medidores inteligentes criptografando-os ou computando seus compartilhamentos em um polinômio gerado aleatoriamente. Os dados criptografados/compartilhamentos computados são agregados em agregadores até o gateway da rede de forma hierárquica sem revelar o valor real das leituras.

Tabela 1. Técnicas dos trabalhos relacionados.

Proposta	Técnica
Guan et al. (2018)	Terceiro Confiável
Zhang et al. (2020)	Terceiro Confiável
Tonyali et al. (2018)	Criptografia Homomórfica

As metodologias utilizadas na privacidade dos dados de medição geralmente seguem os artigos relacionados nesta seção, conforme a Tabela 1. Criptografia homomórfica, com alto custo computacional, ou sistemas baseados na confiança de terceiros. A principal contribuição deste trabalho é a comparação das técnicas normalmente utilizadas com a técnica de assinatura às cegas. Realizando uma comparação tanto qualitativa quanto quantitativa. Levando em consideração aspectos de desempenho das técnicas e de segurança promovida por elas.

3. TÉCNICAS DE CRIPTOGRAFIA

Sultan divide as técnicas de privacidade em categorias (Sultan (2019)):

- Quanto ao tipo de dados: atribuíveis ou não atribuíveis. Para os dados atribuíveis há associação direta deles com um medidor.

- Quanto ao tipo de coleta dos dados: agregados ou não agregados. Para os dados agregados, um elemento da rede é responsável por agregar os dados antes de enviar para o núcleo da rede.
- Quanto ao modelo do sistema de medição: com criptografia homomórfica ou através de um terceiro confiável.

Esta seção descreve as diferentes técnicas de criptografia associadas a cada um dos modelos de medição. Criptografia Paillier para o modelo Parcialmente Homomórfico (PHE), criptografia AES para o modelo Baseado em Terceiro Confiável (BTC) e RSA às cegas para o modelo *Blind*, de assinatura às cegas.

3.1 Criptografia Homomórfica

A criptografia homomórfica é um tipo de criptografia que permite a realização de operações matemáticas entre valores criptografados sem precisar descriptografar os valores. Ela pode ser parcialmente homomórfica ou totalmente homomórfica.

Parcialmente Homomórfica. A criptografia parcialmente homomórfica realiza ou operação de soma ou a operação de multiplicação dos valores criptografados. Entre os diversos tipos, segundo (Tonyali et al. (2015)), a criptografia de Paillier é uma das mais usadas em redes elétricas inteligentes. A criptografia de Paillier consiste em três etapas: geração das chaves, criptografia e descriptografia.

Para gerar as chaves são escolhidos dois números primos bem grandes p e q. Calcula-se $n = pq$. O menor divisor comum da Equação 1 deve ser satisfeito. Define-se $L(x)$, conforme a Equação 2. O cálculo de λ segue a Equação 3. O g é um inteiro entre 1 e n^2. O cálculo de μ segue a Equação 4. A chave pública é (n, g) e a chave privada é λ.

$$mdc(n, (p-1)(q-1)) = 1 \tag{1}$$

$$L(x) = \frac{x-1}{n} \tag{2}$$

$$mmc(p-1, q-1) = \lambda \tag{3}$$

$$\mu = (L(g^{\lambda} mod(n^2)))^{-1} mod(n) \tag{4}$$

A criptografia segue a Equação 5, e a descriptografia segue a Equação 6, onde m é a mensagem e $0 \leq m < n$. Ainda nessas equações, r é um número aleatório, $0 < r < n$ e C é o valor criptografado, $0 < c < n^2$.

$$C = g^m r^n mod(n^2) \tag{5}$$

$$m = L(c^{\lambda} mod(n^2))\mu mod(n) \tag{6}$$

A propriedade homomórfica aditiva de Paillier está representada na Equação 7, onde E representa a criptografia com a chave pública e D representa a descriptografia com a chave privada.

$$D(E(m1)E(m2)mod(n^2)) = (m1 + m2)mod(n) \tag{7}$$

Totalmente Homomórfica A criptografia totalmente homomórfica pode realizar tanto a operação de soma como a operação de multiplicação com o texto criptografado. O primeiro sistema totalmente homomórfico foi proposto por (Gentry (2009)), entretanto o custo computacional desse tipo de sistema é tão alto que sua implantação se torna impraticável. No cálculo de sua propriedade homomórfica, utiliza-se uma variável de erro. A cada operação o erro é incrementado, e se ele ultrapassar um determinado limiar se torna impossível a descriptografia sem erros. Para contornar essa situação, Gentry introduziu uma técnica chamada *bootstraping* que atualiza o texto criptografado, descriptografando homomorficamente sem relevar a mensagem, conforme explicado em (Ducas and Micciancio (2015)). Entretanto ela deve ser repetida periodicamente, elevando assim o custo computacional. Por isso, iremos trabalhar apenas com a criptografia parcialmente homomórfica.

3.2 Criptografia AES

A criptografia AES (*Advanced Encryption Standard*) será utilizada para proteger os dados em um sistema baseado em terceiro confiável. A AES é uma criptografia simétrica, onde apenas uma chave é necessária para criptografar e descriptografar os dados. Ela possui chaves de diferentes tamanhos: 128, 192 ou 256 bits.

Na criptografia AES, a mensagem é alocada em uma matriz de 16 bytes. Esta matriz passa por quatro operações diferentes durante x rodadas. Onde x é determinado pelo tamanho da chave, para 256 bits são 14 rodadas.

Em cada rodada do AES, a matriz passa pelas seguintes operações, conforme (Heron (2009)):

- *Add Round Key*: a matriz passa por uma operação XOR com a chave gerada para aquela rodada.
- *Sub-Bytes*: utiliza a caixa de subtituição de Rijndael para mapear novo valor para cada um das células da matriz.
- *Shift Rows*: realiza a troca de elementos em uma mesma linha.
- *Mix Columns*: multiplica cada coluna por uma matriz constante para obter uma nova coluna.

A mensagem criptografada é resultado da matriz de entrada após passar todas rodadas por essas quatro operações.

3.3 RSA às Cegas

A assinatura cega é uma técnica que permite que um elemento A assine uma mensagem gerada por um elemento B sem conhecer o conteúdo real da mensagem. E quanto um terceiro C recebe a mensagem assinada, ele pode verificar se a mensagem foi assinada pelo A, dificultando o rastreio de uma mensagem recebida ao usuário de origem. Está é uma técnica usada inicialmente em dinheiro virtual por (Chaum (1983)). Cheung et al. usaram ela para assinar credenciais para pedidos de compra de energia elétrica (Cheung et al. (2011)). Finster e Baumgart propuseram o uso de assinatura às cegas para assinar os pseudônimos associados aos medidores (Finster and Baumgart (2013)). Neste trabalho, usa-se a assinatura às

cegas com RSA para assinar os pseudônimos, conforme proposto por Finster and Baumgart.

A assinatura de uma mensagem no RSA às cegas ocorre da seguinte maneira. Um cliente gera uma mensagem, atribui a ela um fator de cegueira e envia para um servidor. O servidor assina a mensagem e devolve para o cliente. O cliente retira o fator de cegueira, e obtém a mensagem original assinada pelo servidor.

Partindo do princípio que d é a chave privada RSA, e é a chave pública e m a mensagem original. O cliente introduz na mensagem um fator de cegueira $r^e mod(n)$, conforme a Equação 8, tal que r obedeça à Equação 9. Ao receber m', o servidor assina conforme a Equação 10. O cliente recebe s', retira o fator de cegueira e obtém m assinada, Equação 11.

$$m' = mr^e mod(n) \tag{8}$$

$$mdc(r, n) = 1 \tag{9}$$

$$s' = (m')^d mod(n) \tag{10}$$

$$s = (s')r^{-1} mod(n) = m^d mod(n) \tag{11}$$

4. VISÃO GERAL DO SISTEMA

Neste artigo, o sistema de dados de medição para operações é composto por medidores inteligentes, agregador, gerenciador de chaves e central de controle, conforme a Figura 1. As demais entidades são utilizadas para faturamento e prestação de serviços. O papel de cada elemento do sistema é definido como:

- Medidor inteligente: realiza medições periódicas na unidade consumidora e envia para o agregador.
- Agregador: Responsável por coletar, agregar e enviar os dados de consumo para a a unidade de controle.
- Gerenciador de chaves: Responsável por gerar ou assinar as chaves do sistema.
- Central de controle: entidade pertencente à unidade controle. Responsável por tratar os dados coletados pelos agregadores, realizando análises e tomadas de decisões.

5. MODELOS DE MEDIÇÃO

Esta seção detalha a aplicação das técnicas de criptografia aos modelos de medição voltados para operações da rede elétrica. Cada uma possui sua particularidade e lógica de funcionamento.

5.1 Modelo Parcialmente Homomórfico (PHE)

O modelo PHE utiliza a criptografia de Paillier, em que a central de controle gera as chaves pública e privada. A chave pública é compartilhada entre os medidores, que criptografam os dados de medição com ela. Os agregadores recebem os dados criptografados e somam todos utilizando a propriedade homomórfica aditiva de Paillier. Ao receber

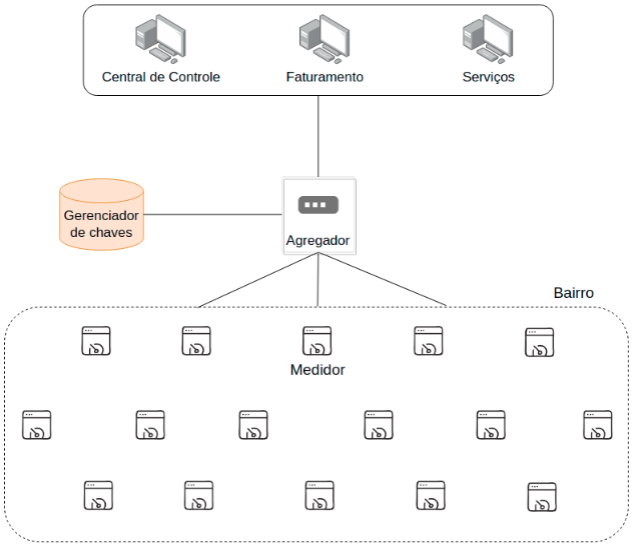

Figura 1. Visão Geral do Sistema.

os dados dos agregadores, a central de controle descriptografa e identifica o consumo de uma região. Entretanto, ela não consegue identificar o consumo específico de um medidor. A Figura 2 ilustra esta lógica funcionamento.

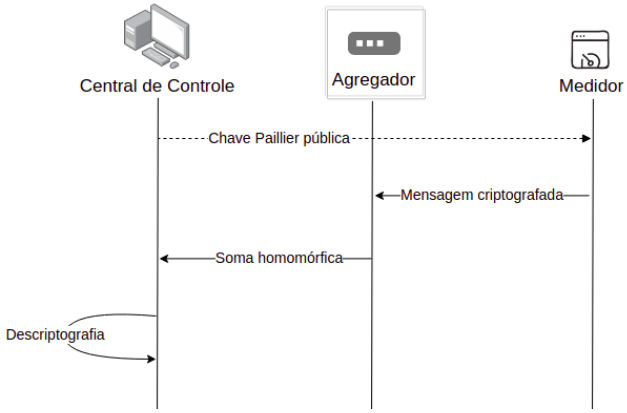

Figura 2. Modelo PHE.

A mensagem de monitoramento com Paillier obedece à seguinte estrutura. O consumo c é criptografado com a chave pública Paillier $E_{Paillier}$ e depois é concatenado com a informação do tempo de medição conforme Equação 12. Cada medidor gera um par de chaves RSA, onde o pseudônimo é a chave pública RSA, autenticada no gerenciador de chaves. A mensagem m é assinada com a chave privada RSA, $A_{RSA-priv}(m)$. A estrutura final da mensagem de medição está na Equação 13, onde $Pseud$ é a chave pública RSA do medidor (pseudônimo) .

$$m = E_{Paillier}(c)||t \tag{12}$$

$$M_{final} = E_{Paillier}(c)||t||A_{RSA-priv}(m)||Pseud \tag{13}$$

5.2 Modelo Baseado em Terceiro Confiável (BTC)

O modelo BTC usa a criptografia AES, onde inicialmente os pseudônimos RSA dos clientes são autenticados no

gerenciador de chaves. Através da criptografia RSA, conforme ilustrado na Figura 3, o medidor envia uma senha para o gerenciador de chaves, que gera uma chave AES. A chave AES é compartilhada entre o agregador e o medidor. Durante uma medição, o consumo é criptografado com a chave AES, enviado para o agregador e descriptografado para ser somado ao consumo dos demais medidores da região. Neste caso, a central de controle também recebe os dados agregados. Entretanto, o agregador conhece o consumo de cada mensagem recebida. A privacidade do usuário é estabelecida através do uso de pseudônimos apenas e o gerenciador de chaves conhece apenas o medidor associado à um pseudônimo.

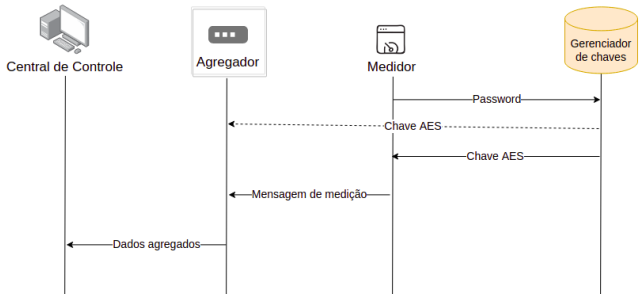

Figura 3. Modelo BTC.

No sistema de medição com auxílio do AES, a estrutura da mensagem é diferente da Paillier. O consumo c é concatenado com o tempo de medição, $c||t$, e criptografado usando a chave AES, Equação 14. A mensagem final corresponde a Equação 15, onde a mensagem criptografada é concatenada com o pseudônimo do medidor, chave pública RSA.

$$m = E_{AES}(c||t) \tag{14}$$

$$M_{final} = m||Pseud \tag{15}$$

5.3 Modelo Blind

O modelo *Blind* utiliza assinatura às cegas, em que o medidor autentica no gerenciador de chaves utilizando uma identidade conhecida. Entretanto, ele apresenta ao gerenciador uma chave pública RSA, que representa um pseudônimo, para ser assinado às cegas. A Figura 4 ilustra a lógica de funcionamento.

Primeiro, o medidor envia o pseudônimo com um fator de cegueira para ser assinado pelo gerenciador de chaves. Ao receber a mensagem assinada, ele retira o fator de cegueira e obtém o pseudônimo assinado. O pseudônimo será usado nas mensagens de medição enviadas ao agregador. Observe que desta vez nem mesmo o gerenciador de chaves conhece a associação entre um medidor e seu pseudônimo.

O consumo c é criptografado com a chave pública RSA do agregador E_{AG} e depois concatenado com o tempo de medição, Equação 16. A mensagem final corresponde a Equação 17, onde $A_{pseud}(m)$ é assinatura de m com a chave privada RSA do medidor, e $A_{Gen}(pseud)$ é assinatura do pseudônimo feita pelo gerenciador de chaves.

$$m = E_{AG}(c)||t \tag{16}$$

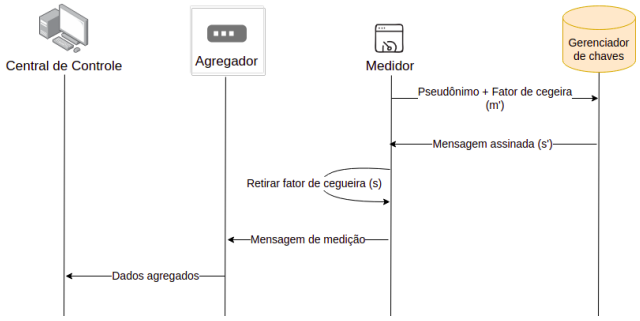

Figura 4. Modelo *Blind*.

$$M_{final} = m||A_{pseud}(m)||Pseud||A_{Gen}(pseud) \tag{17}$$

6. ANÁLISES E COMPARAÇÕES

As simulações foram modeladas em Python. Para a criptografia AES e RSA, foi utilizada a biblioteca PyCryptodome. Para a criptografia Paillier usamos a biblioteca python-Paillier. As chaves do AES usadas são de 256 bits. As chaves Paillier e RSA foram de 2048 bits. Os teste foram executados em notebook com processador Intel Core i5-7200U CPU 2.50GHz x 4, 8 GB de memória RAM. A análise de rede foi feita com o Wireshark, e o uso de CPU foi coletado com a biblioteca Psrecord. Esta seção contém a análise de comparação do desempenho e de segurança.

6.1 Análise de Desempenho

Para a comparação de desempenho foram feitas três análises: Custo computacional relativo ao tempo de execução, custo computacional relativo ao uso de CPU, e a vazão da rede.

Para a análise de custo computacional relativo ao tempo de execução, os modelos de medição foram divididos em operações: inicialização do cliente, inicialização da empresa, criptografia e descriptografia. A inicialização do cliente é composta das operações de geração de chaves e troca inicial de informações entre o medidor do cliente e os elementos da rede da empresa de energia. Na inicialização da empresa está relacionada a geração de chaves e respostas à solicitações iniciais dos clientes. As operações de criptografia e descriptografia estão associadas ao monitoramento dos dados de medição, com a criação de mensagens, criptografias, descriptografia e o tratamento das mensagens para cada um dos modelos de medição.

Para esta análise foram executadas 20 rodadas por operação. Em cada rodada, as operações foram executadas 1000 vezes. A Tabela 2 apresenta as médias do tempo de execução por operação, e a Figura 5 nos permite uma análise visual destes dados.

Tabela 2. Custo computacional em segundos.

Modelo	Inic. Cliente	Inic. Empresa	Cripto	Descrip
Paillier	0,1005	0,1639	0,1022	0,0289
AES	0,1500	0,1527	0,0002	0,0498
Blind	0,1010	0,1017	0,0012	0,0020

Os modelos PHE e BTC apresentaram um custo computacional de tempo maior que o modelo *Blind*. Ao observar

o gráfico, a fase de inicialização dos modelos apresentaram um custo elevado, se comparada com a etapa de criptografia e descriptografia. Por usar uma criptografia homomórfica de Paillier, o alto custo do modelo PHE já era esperado. Quanto ao modelo BTC, apesar do uso do AES, a sua inicialização utiliza a criptografia RSA o que aumenta o custo com a geração das chaves. O modelos *Blind* possui um custo computacional de tempo de execução mais baixo na maior parte dos testes.

Para refinar o custo computacional, a segunda análise trabalha com o uso de CPU durante o monitoramento dos dados de medição. Nesta análise foram executados testes de troca de mensagens de medição variando o número de nós associados ao agregador. Cada nó enviou mensagens de medição em intervalos de 1 minuto. Foram realizadas rodadas de testes com duração de 10 minutos e calculada a média do uso de CPU do agregador durante a troca de mensagens. A Figura 6 ilustra o resultados desses testes.

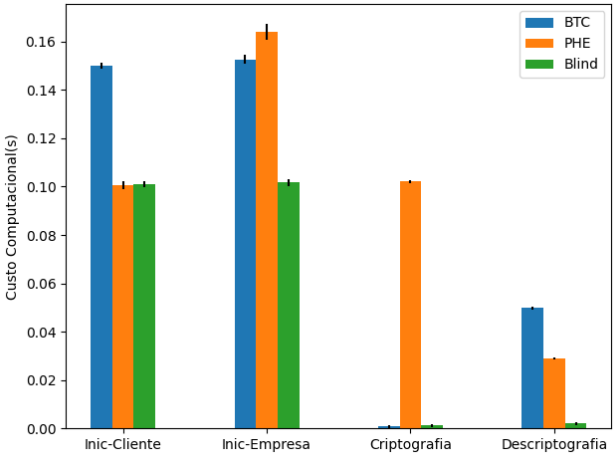

Figura 5. Média de custo computacional por operação.

Conforme o esperado, o uso de CPU do modelo PHE é extremamente elevado se comparado aos demais modelos, e o uso de CPU do modelo BTC é o mais baixo de todos. O modelo *Blind* obteve um custo computacional de uso de CPU intermediário, se comparado aos demais modelos. Em termos de custo computacional, tanto de tempo como de uso de CPU, o modelo *Blind* demonstrou ser uma alternativa totalmente viável.

A terceira análise quantitativa é o aumento da vazão da rede (kbps) de acordo com o número de nós. A Figura 7 ilustra o resultados desses testes.

Os modelos PHE e *Blind* apresentaram uma vazão mais elevada que o modelo BTC. Isto ocorre, em partes, pois o texto cifrado do AES possui um tamanho bem menor que o texto cifrado em Paillier ou RSA, do modelo *Blind*. Outro fator importante é a estrutura das mensagem de cada um dos modelos, descrita na Seção 4.

Por mais que os teste quantitativos sejam importantes, eles não são definitivos por si só. Por serem técnicas voltadas à privacidade, a análise de segurança desempenha um papel com grande peso para a escolha da técnica que será utilizada em um sistema. A análise quantitativa pode desclassificar um modelo diante a inviabilidade de uso prático em um sistema real. Entretanto a análise de

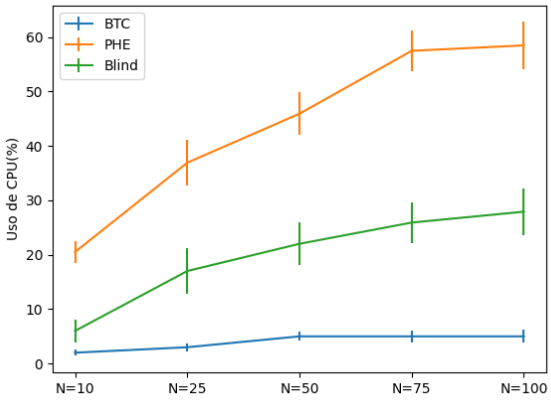

Figura 6. Média de uso de CPU por número de nós.

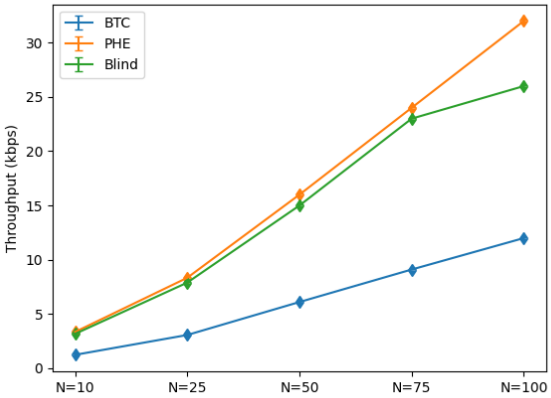

Figura 7. Vazão da rede de acordo com o número de unidades medidoras.

segurança será determinante na definição da solução. Não basta que o modelo tenha um bom desempenho, ele deve atender aos requisitos mínimos de segurança.

6.2 Análise de Segurança

Esta seção apresenta uma análise qualitativa dos modelos. Os requisitos mínimos de segurança foram baseados no trabalho (Asghar et al. (2017)), e estão relacionados abaixo:

- Confidencialidade: Os dados do medidor não devem ser expostos a indivíduos ou processos não autorizados. Garantir a confidencialidade dos dados é necessário para alcançar a privacidade criptográfica.
- Integridade: A precisão e exatidão dos dados do medidor devem ser mantidas, e quaisquer alterações feitas nos dados devem ser detectáveis.
- Autenticidade: O receptor dos dados do medidor deve ser capaz de verificar a origem dos dados.
- Não-Repúdio: A fonte dos dados do medidor não deve ser capaz de negar que originou os dados.

No modelo PHE, as mensagens são assinadas com a chave RSA privada do medidor. Atendendo assim os requisitos de autenticidade, não-repúdio e integridade. Se a mensagem

for adulterada, haverá falha na verificação da assinatura. A criptografia dos dados evita que agentes externos ao sistema tenha acesso aos dados dos usuários. A privacidade em relação à agentes internos é feita através da agregação dos dados de forma homomórfica. Os agregadores podem até saber a associação de um pseudônimo a um medidor específico, mas não têm acesso aos dados criptografados. Somente a central de controle possui a chave Paillier privada. Um ponto falho deste modelo é a confiança na integridade da empresa de energia, ou em seus agentes. Não há garantia que a empresa de energia, ou um de seus funcionários, não utilizará a chave privada de Paillier antes da agregação dos dados.

O modelo BTC apresentou um ótimo desempenho nos testes quantitativos. O modelo ganha bastante desempenho ao não assinar as mensagens. Entretanto, por este mesmo motivo ele não atende os requisitos mínimos de segurança. Ele não garante o não-repúdio ou autenticidade do usuário de origem. A chave de criptografia não é de conhecimento exclusivo do medidor, e o pseudônimo do medidor é conhecido pelos demais participantes da rede. Quanto à confidencialidade, este é um modelo baseado na confiança de terceiros. O agregador acessa a informação dos dados de consumo, mas a identidade do medidor é preservada com o uso de pseudônimos. Somente o gerenciador de chaves conhece a associação entre um pseudônimo e o seu medidor. Novamente a confiança está na integridade da empresa de energia e seus sistemas. Não há garantia que a empresa não acessará os dados do gerenciador de chaves. E se o terceiro confiável pertencer à outra empresa? Por se tratar de dados de alto valor, não há garantia que estas duas empresas não irão se associar. Permanece o grande desafio de encontrar um terceiro que seja realmente confiável.

No modelo *Blind*, de assinatura às cegas, as mensagens são assinadas com a chave privada RSA do medidor, assegurando a origem da mensagem. Os dados são criptografados com a chave publica RSA do agregador, garantindo que somente o agregador com sua chave privada tenha acesso aos dados de medição. O agregador tem acesso aos dados de medição. Porém, a identidade do usuário está protegida pelo uso de pseudônimo. Os pseudônimos são assinados às cegas, e nem mesmo o gerenciador conhece a associação entre um pseudônimo e seu respectivo medidor. A validade de um pseudônimo pode ser verificada através de sua assinatura feita pelo gerenciador de chaves e enviada junto com cada mensagem. Desta maneira, somente o usuário conhece a associação entre seu pseudônimo e sua identidade.

O modelo que melhor atende aos requisitos de segurança é o modelo *Blind*, de assinatura às cegas. A associação entre um pseudônimo e seu medidor pode ser descoberta de outras formas. As mensagens associadas à um mesmo pseudônimo podem ser rastreadas e comparadas com o padrão de consumo de alguma casa que está sendo monitorada. Por isso, é comum também o uso de usar vários pseudônimos por um mesmo usuário para dificultar esse rastreamento.

7. CONCLUSÃO

Neste artigo, foram comparados os modelos de medição de dados de consumo da rede elétrica. Os modelos tradicionais, com criptografia homomórfica e baseados na confiança de terceiros, foram comparados com o modelo de assinatura às cegas, *Blind*. Os modelos propostos até o momento confiam na integridade da empresa de energia e de seus funcionários, onde a privacidade do usuário depende de terceiros. Já o modelo de assinatura as cegas propõe que a privacidade do usuário esteja nas mãos do próprio usuário.

O modelo *Blind* apresentou um bom desempenho nos testes de custo computacional e de rede. Ele demonstrou viabilidade de uso prático, apresentando um desempenho superior ao modelo PHE. E quanto aos requisitos de segurança, mostrou ser um modelo superior aos demais comparados.

Quanto a preservação da privacidade do usuário, o *Blind* não é uma solução completa. A identidade dos medidores podem ser revelada pela interface de comunicação, através do endereço de rede.

Como trabalho futuro, o modelo *Blind* deve ser analisado junto com outras técnicas para contornar a identificação pelo endereço de rede. Outra análise interessante é avaliar as técnicas propostas para privacidade dos dados não apenas em termos de medição do consumo de energia de usuários, mas também para outras finalidades, como manter a qualidade da rede e evitar fraudes. São válidas as análises para frequência de troca de dados e requisitos de cada uma dessas aplicações específicas.

REFERÊNCIAS

Asghar, M.R., Dán, G., Miorandi, D., and Chlamtac, I. (2017). Smart meter data privacy: A survey. *IEEE Communications Surveys & Tutorials*, 19(4), 2820–2835.

Chaum, D. (1983). Blind signatures for untraceable payments. In *Advances in cryptology*, 199–203. Springer.

Cheung, J.C., Chim, T.W., Yiu, S.M., Li, V.O., and Hui, L.C. (2011). Credential-based privacy-preserving power request scheme for smart grid network. In *2011 IEEE Global Telecommunications Conference-GLOBECOM 2011*, 1–5. IEEE.

Dorri, A., Luo, F., Kanhere, S.S., Jurdak, R., and Dong, Z.Y. (2019). Spb: A secure private blockchain-based solution for distributed energy trading. *IEEE Communications Magazine*, 57(7), 120–126.

Ducas, L. and Micciancio, D. (2015). Fhew: bootstrapping homomorphic encryption in less than a second. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, 617–640. Springer.

Eibl, G. and Engel, D. (2014). Influence of data granularity on smart meter privacy. *IEEE Transactions on Smart Grid*, 6(2), 930–939.

Finster, S. and Baumgart, I. (2013). Pseudonymous smart metering without a trusted third party. In *2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, 1723–1728. IEEE.

Finster, S. and Baumgart, I. (2015). Privacy-aware smart metering: A survey. *IEEE communications surveys & tutorials*, 17(2), 1088–1101.

Gentry, C. (2009). *A fully homomorphic encryption scheme*. Stanford university.

Guan, Z., Si, G., Zhang, X., Wu, L., Guizani, N., Du, X., and Ma, Y. (2018). Privacy-preserving and efficient aggregation based on blockchain for power grid communications in smart communities. *IEEE Communications Magazine*, 56(7), 82–88.

Heron, S. (2009). Advanced encryption standard (aes). *Network Security*, 2009(12), 8–12.

Sultan, S. (2019). Privacy-preserving metering in smart grid for billing, operational metering, and incentive-based schemes: A survey. *Computers & Security*, 84, 148–165.

Tonyali, S., Akkaya, K., Saputro, N., Uluagac, A.S., and Nojoumian, M. (2018). Privacy-preserving protocols for secure and reliable data aggregation in iot-enabled smart metering systems. *Future Generation Computer Systems*, 78, 547–557.

Tonyali, S., Saputro, N., and Akkaya, K. (2015). Assessing the feasibility of fully homomorphic encryption for smart grid ami networks. In *2015 Seventh International Conference on Ubiquitous and Future Networks*, 591–596. IEEE.

Zhang, S., Rong, J., and Wang, B. (2020). A privacy protection scheme of smart meter for decentralized smart home environment based on consortium blockchain. *International Journal of Electrical Power & Energy Systems*, 121, 106140.