A Review of Privacy-Preserving Aggregation Schemes for Smart Grid

Lucas V. Dias, and T. A. Rizzetti

***Abstract*—Smart Grid aims to make the use of electricity reliable, sustainable, scalable, fault-tolerant, and efficient. For this purpose, it uses information and communication technologies. However, there are issues related to information security threats. For example, an adversary monitoring data metering from consumers could trace their habits. Traditional encryption techniques resolve this question against external attackers. However, the operation center still could trace the consumer's habits. Thus, to preserve consumer's privacy, even against internal threats, the data must be aggregated by groups of consumers, representing a geographic area. A usual way to make it possible is through the use of homomorphic cryptography, since it allows making arithmetic operation over encrypted data. Thus, this article reviews the literature on privacy-preserving data aggregation schemes against internal and external attackers. It also presents the information security requirements for Advanced Metering Infrastructure (AMI) and its operation.**

***Index Terms*—Smart Grids, Data privacy, Security, Information security, Cryptography, Meter reading, Power Distribution.**

I. Introdução

No final da segunda década do século XXI, o uso de tecnologia da informação tem abrangido diversas áreas dos setores produtivos como saúde [1], agricultura [2], automação residencial [3], entre outros. Os avanços em monitoramento, sensoriamento, controle e comunicação fazem com que a rede de energia elétrica tradicional seja substituída por um sistema inteligente e sustentável [4], [5]. A incorporação de mecanismos de comunicação bidirecionais, empregando integração entre os diversos componentes de uma rede de energia elétrica tradicional, assim como a incorporação de novas aplicações, permite a implementação do conceito de *Smart Grid* (SG) ou Redes Elétricas Inteligentes (REI) [6], [7].

A REI tem por objetivo tornar o uso de energia elétrica confiável, sustentável, escalável, tolerante a falhas e eficiente [8], [9]. Para isso, ela é dividida em sete domínios: geração, transmissão, distribuição, consumidor, mercado, centro de operações e provedor de serviço, conforme visto na Fig. 1 [10].

Os quatro primeiros domínios formam o modelo tradicional da rede de energia elétrica e nesse contexto, só existe fluxo de energia elétrica [11]. Todavia, no contexto de REI, há fluxos de energia elétrica e de informação entre eles. Por outro lado, entre os três últimos, ocorre apenas troca de informações [12]. Uma das principais diferenças entre a rede elétrica tradicional e a REI, é que a segunda consiste na capacidade de integração entre as informações provenientes dos diferentes segmentos e atores que compõem o sistema elétrico de potência [13], [14]. Desta forma, permitindo que diversas aplicações possam serem implantadas sobre ela, como resposta à demanda, tarifação dinâmica, entre outras [15]. Além disso, a REI aborda sistemas de uso final e recursos de distribuição de energia renováveis [16].

Um dos principais subsistemas que permitem o funcionamento da REI é a *Advanced Metering Infrastructure* (AMI) ou infraestrutura de medição avançada. Ela permite comunicação inteligente entre sistemas de operação e consumidores, dessa forma, sendo benéfica para ambos [17]. Adicionalmente, a AMI possibilita que o primeiro realize o monitoramento mais preciso do sistema, encontrando rapidamente falhas e fornecendo os meios técnicos necessários para a implementação de políticas de tarifação dinâmica, com vistas a melhorar a distribuição da curva de carga, entre outras questões [18]. A AMI permite que os dados de consumo de energia elétrica sejam medidos em tempo real ou quase real. Com isso, ela fornece as informações necessárias para que o sistema se adapte de forma a atender as condições correntes do sistema elétrico de potência [19].

A segurança cibernética para tais funcionalidades é crucial, uma vez que potencialmente podem tornar o sistema vulnerável. Um agente malicioso pode monitorar as medições de um alvo e traçar um perfil para uma diversidade de objetivos, como analisar os momentos em que se encontram pessoas em uma residência [20]. Para contornar esse tipo de problema é comum a utilização de técnicas de ofuscação, não permitindo nem mesmo a adversários com alcance aos dados da concessionária obterem acesso aos dados individuais de consumo instantâneo de um usuário. A criptografia homomórfica, que permite operações aritméticas sobre texto cifrado, junto a ofuscação de dados são tecnologias recorrentemente empregadas para esse propósito [11].

Além da privacidade, outros aspectos essenciais da segurança cibernética devem ser empregados em sistemas críticos como as REI, entre eles: confidencialidade, autenticidade, integridade, não-repúdio e disponibilidade [21], [22]. Dessa forma, o respectivo trabalho apresenta uma revisão de literatura sobre alguns esquemas propostos, especialmente voltados a AMI, que abordam a preservação de privacidade dos usuários.

O restante deste trabalho está divido nas seguintes seções: a Seção II apresenta os requisitos e funcionamento da AMI. Em sequência, modelos de adversários ou *adversary model* [23] e as propostas na literatura para preservação de privacidade são apresentadas na Seção III. Na Seção IV é abordada uma visão geral dos trabalhos. Por fim, as considerações finais e

Lucas Varga Dias is with Federal University of Santa Maria, Santa Maria, RS, Brazil, e-mail: lucas_dias@redes.ufsm.br.

Tiago Antonio Rizzetti is with Federal University of Santa Maria, Santa Maria, RS, Brazil, e-mail: rizzetti@redes.ufsm.br.

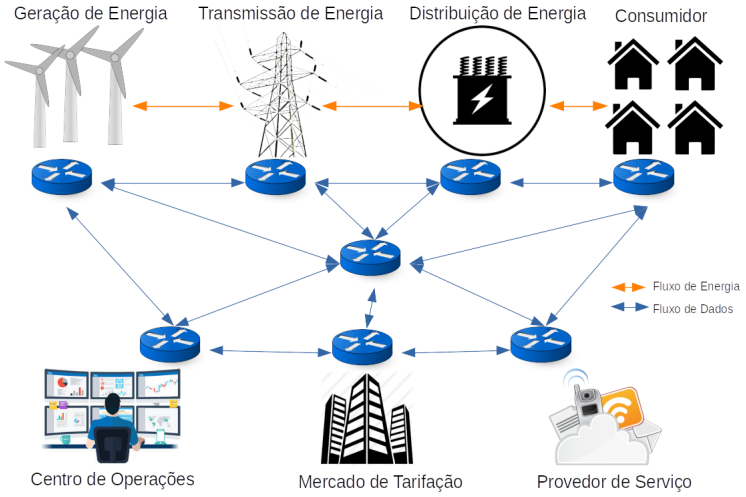


Fig. 1. Arquitetura da *Smart Grid*

trabalhos futuros são tratados na Seção V.

II. Requisitos de segurança da informação para AMI

A AMI é um subsistema fundamental para o funcionamento da REI. Ela é a integração de diversas tecnologias como *Smart Meters* (SM), enlaces de comunicação e sistemas de gerenciamento de informações. Dessa forma, permitindo troca de informações entre os dispositivos de medição e os sistemas de operação do sistema elétrico de potência [24]. Esse último é responsável por controlar a distribuição e transmissão de energia elétrica [11].

A importância da AMI se dá pela medição da energia elétrica através dos SMs de cada consumidor em intervalos de tempo curtos que podem variar de poucos milissegundos a minutos [25]. Isso permite aplicações de resposta à demanda, onde através de mecanismos de integração entre produção e demanda, empregam-se técnicas para equalizá-las [26]. Isso pode ser realizado através do incentivo ou penalização do consumo, bem como a produção ou inserção de energia armazenada, considerando os aspectos econômicos [27].

A AMI também permite a utilização de um sistema de tarifação dinâmica na qual o preço da energia elétrica varia com a carga da rede elétrica [28]. De acordo com [29], a AMI é formada pelos seguintes participantes.

- Fornecedor e operador da rede elétrica: É a entidade que controla a infraestrutura de distribuição e transmissão da energia elétrica e tem a responsabilidade de controlar armazenamento, geração distribuída, tarifação, e demais aspectos operacionais do sistema [30];
- Rede de comunicação: Responsável pela comunicação entre todas as entidades do sistema [7]. Deve-se empregar canais seguros de comunicação e/ou técnicas para cifração de dados.
- Produtor de energia elétrica: É uma entidade que vende energia elétrica aos consumidores através da infraestrutura de transmissão e distribuição. A tarifação da energia elétrica pode ocorrer através do ajuste da energia produzida. Por exemplo, quanto menor a demanda de uma região, menor o preço [31]. Ou ainda, sabendo o consumo total de energia consumida, aplica-se a tarifa que consumidor e o produtor estabeleceram em acordo;
- Consumidor: Usuário final que recebe a energia para consumo. Geralmente, tem acesso aos dados de medição, podendo serem agregados ou não, para administrar seus hábitos ou tirar vantagem da tarifação dependendo da política dela;
- SMs: Eles ficam nas instalações dos consumidores da rede elétrica, possuem a tarefa de medir a energia consumida em intervalo de tempo pré-definido e enviar ao agregador [32];
- Agregador ou *gateway*: Esse participante recebe os dados dos SMs e faz a agregação deles, pode realizar a estimativa da demanda de energia de uma determinada região [33]. É um dos elementos essenciais para a implementação do conceito de resposta à demanda ou *Demand Respose* (DR). Pode ser controlado pela mesma entidade que opera a rede [34].

É importante salientar que há dois aspectos distintos referentes a medição do consumo de energia:

- Faturamento ou tarifação: É responsável por identificar a quantidade de energia gasta pelo consumidor em um determinado intervalo de tempo, normalmente realizada mensalmente. É imprescindível a identificação do consumidor. Ela poderá ser realizada através de uma comunicação direta entre o SM e o sistema supervisório da concessionária.
- Mecanismos de resposta à demanda (DR): Necessitam de uma frequência de leitura mais intensa [25]. A resposta à demanda não deve identificar o consumidor, por questões de privacidade [20], mas deve computar a contribuição de cada um deles para a carga da região mensurada. No contexto de resposta à demanda a informação necessária consiste em determinar a carga requisitada em uma deter-

minada região composta por um grupo de consumidores. É especialmente neste segundo aspecto que se insere o conceito dos agregadores.

Para a interconexão entre os participantes, existem duas arquiteturas de medição. A centralizada onde os SMs tem apenas função de sensoriamento, enviando seus dados ao agregador [35]. Este, por sua vez, tem capacidade computacional maior que os SMs e armazena as medições recebidas em uma base de dados para envio ao centro de operações [36]. No centro de operações são gerenciadas as diversas aplicações, como cálculo de consumo, faturamento e processos de monitoramento e controle de carga. Essas informações podem ser recuperadas pelos consumidores proprietários delas [29].

Já na maneira descentralizada, os SMs também tem a função de agregador, normalmente implementando uma rede de comunicação *mesh*. Neste caso, além de realizar a sua própria medição, e participação no processo de faturamento, o SM poderá assumir a função de agregador. Assim, o gerenciamento da rede é desempenhado de maneira colaborativa pelos usuários através de interfaces sobre seu controle [37].

Uma representação da AMI, realizada de forma centralizada, é apresentada na Fig. 2. A *Home Area Network* (HAN) é composta pelo SM e pelos dispositivos eletrônicos inteligentes de cada consumidor. Cada residência consiste em uma HAN, já o conjunto de consumidores formam uma *Neighbor-Area Network* (NAN) [38]. Cada NAN possui um agregador, que é responsável por agregar os dados de medição da NAN e enviar a subestação de energia [39]. A subestação de energia envia esses dados ao sistema *Supervisory Control and Data Acquisition* (SCADA) da concessionária, o qual normalmente encontra-se no centro de operações [40].

O sistema SCADA é responsável pelo monitoramento e controle da distribuição de energia em tempo real [41], [42]. Em conjunto com aplicações de propósito específico, sistemas SCADA promovem as condições necessárias para implementação de mecanismos de adequação, de forma a manter a qualidade e disponibilidade do sistema [43]. Ele é formado pelos seguintes componentes.

- Servidores de Controle: Software de controle de hospedagem e acesso aos módulos de controle;
- Interface Homem-Máquina (HMI): Plataforma utilizada pelos operadores para monitorar o estado do sistema, modificar configurações de controle e sobrescrever operações de controle automático em momentos de emergência [44];
- Unidade Terminal Remota (RTU): Dispositivos de campo com interface de comunicação sem fio para encaminhar os dados de aquisição e controle [45];
- Controlador Lógico Programável (PLC): Dispositivos de campo que fazem funções de controle lógico executados pelo hardware elétrico [46];
- Dispositivo Eletrônico Inteligente (IED): Sensor e atuador inteligente que coleta dados, comunica-se com outros dispositivos e realiza controle e processamento local [47].

Na arquitetura do sistema SCADA, elementos como HMI, servidores de controle, estações de trabalho de energia e os dados históricos são mantidos no centro de controle. Eles são conectados através de uma *Local Area Network* (LAN). Já as informações recebidas dos RTUs, IEDs e PLCs são através da *Wide Area Network* (WAN) [48]. A AMI caracteriza-se pela troca de dados sensíveis e por ser um serviço de grande importância para o funcionamento da infraestrutura da rede de energia elétrica. Com isso, ela torna-se alvo de agentes maliciosos para diversos objetivos [49]. A seguir são apresentadas as prerrogativas de segurança da informação e exemplos de como um agente malicioso pode explorá-las [50].

- Não-repúdio: Essa prerrogativa deve tornar verificável evidências sobre as transações entre as entidades participantes. Ela evita que, por exemplo, os dados enviados por uma unidade consumidora, através do SM, possam ser desacreditados pelo agregador [51], [52], [53];
- Autenticação: trata de garantir que as entidades participantes de uma comunicação sejam quem dizem ser. Por exemplo, o SM garantir que o agregador para o qual ele envia seus dados de medições é o agregador da rede e, o segundo, garantir que as medições recebidas foram emitidas pelo SM [12]. Desta forma, realizando uma autenticação entre as duas partes da comunicação, ou seja, uma autenticação mútua [54];
- Disponibilidade: Essa prerrogativa tem por objetivo garantir o funcionamento do serviço aos elementos legítimos que o utilizam. Por exemplo, prevenir que ataques *black hole* sejam bem sucedidos [55]. Uma técnica comum de ataque é enviar pacotes de diversas fontes distintas para tornar indisponível um serviço, isso é denominado *Distributed Denial of Service*, um trabalho que aborda essa questão em AMI é apresentado em [56]. No contexto de AMI, deve ser garantido que um agregador esteja disponível para os SMs enviarem suas medições [57]. Esta prerrogativa trata, portanto, de empregar técnicas que garantam o menor consumo de recursos para o descarte de informações e/ou solicitações provenientes de fontes indevidas ou não autênticas [58];
- Integridade: Deve garantir que a mensagem enviada por um emissor seja a mesma entregue ao receptor [59]. Um agente malicioso poderia modificar informações de medição de consumo de energia emitidas por um SM [60]. As manipulações desses dados podem resultar em instabilidade na rede, incluindo degradação na qualidade da energia elétrica e, no pior cenário até mesmo um eventual *blackout* [15]. Além disso, poderia manipular a política de preços da energia elétrica [61]. Para atingir essa prerrogativa, muitas vezes, utiliza-se de técnicas baseadas em hash. Um algoritmo de hash, para ser seguro, deve ser aplicável a blocos de dados de qualquer tamanho, produzir uma saída de comprimento fixo, e deve ser fácil de computar para qualquer informação passada como entrada. Um algoritmo de hash também deve garantir que com apenas o resultado do hash, é inviável encontrar a mensagem original, bem como seja inviável duas mensagens iguais resultarem em hashes diferentes [62], e;
- Confidencialidade: Essa prerrogativa trata de garantir que apenas emissor e receptor tenham conhecimento das

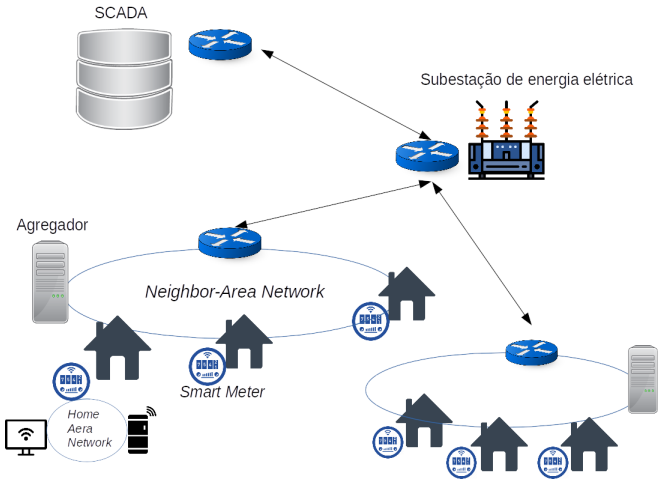


Fig. 2. Visão Geral da Arquitetura de Medição com arquitetura centralizada.

mensagens trocadas [63]. Um exemplo de utilização é em negociações entre concessionária e consumidores, os dados compartilhados são sensíveis e com isso é preciso garantir a confidencialidade da comunicação [57]. A prerrogativa de confidencialidade também aborda a privacidade das informações que pode ser definida como a garantia que um usuário tem de controlar e influenciar quais informações sobre eles podem ser armazenadas e coletadas. Além de controlar por quem e para quem elas podem ser reveladas [64]. No contexto de AMI, um consumidor não deseja que um agente malicioso consiga recuperar suas informações de medição de energia elétrica. Ele poderia usar essas informações para uma diversidade de objetivos como identificar os períodos do dia que se encontram indivíduos em uma residência [65]. Essa vulnerabilidade pode ser explorada em aplicações de resposta à demanda. Muitos trabalhos na literatura apresentam uma alternativa para contorná-la. Tendo em vista que a medição dos dados entregue a concessionária deve ser por região geográfica, sistemas criptográficos homomórficos, descritos na Subseção II-A, podem ser utilizados para promover a privacidade dos usuários.

A. *Criptografia Homomórfica*

Para um sistema criptográfico ser considerado homomórfico ele tem de satisfazer a (1) [66].

$$E(m1 \diamond m2, PK_{pubA}) = E(m1, PK_{pubA}) \diamond E(m2, PK_{pubA}) \quad (1)$$

Sendo que $\diamond$ representa qualquer operação aritmética, e `m1` e `m2` representam dois textos planos quaisquer. Com isso, a definição de criptografia homomórfica é de que as operações aritméticas em texto plano tem o mesmo resultado que operações aritméticas em texto cifrado equivalente [67].

Essa técnica criptográfica é em geral, formada por quatro funcionalidades. A primeira é a `KeyGen` que faz a geração do par de chaves pública e privada para a versão assimétrica ou a geração de um segredo compartilhado em uma versão simétrica [68]. A segunda é `Enc` que realiza a cifração dos dados, `Dec` que realiza a decifração e `Eval` que realiza as operações homomórficas específicas [69].

A criptografia homomórfica ainda se divide em *Fully Homomorphic Encryption* (FHE) e *Partially Homomorphic Encryption* (PHE). A primeira tem suporte a todas operações aritméticas e tem como exemplo o algoritmo de Gentry apresentado em [70]. Já a segunda pode ainda ser subdivida em PHE aditiva e PHE multiplicativa.

A primeira suporta apenas operações de soma sobre os dados encriptados [71]. Um exemplo de PHE aditiva é o cripto sistema de Paillier apresentado em [72]. Por outro lado, a segunda suporta apenas operações aritméticas de multiplicação sobre os dados encriptados, um exemplo de algoritmo que possui tal propriedade é o Rivest-Shamir-Adleman (RSA) [73].

O FHE tem desvantagem do tamanho de chaves em relação ao PHE [50]. Uma boa parte dos trabalhos apresentados na Seção III fazem uso de um dos tipos de criptografia homomórfica. Eles tratam da preservação de privacidade dos usuário em relação à ataques externos ou internos.

III. Esquemas Seguros para Preservação de Privacidades dos Dados de Medição Elétrica

Nessa seção são apresentados os trabalhos abordados na literatura que tratam da preservação de privacidade dos usuários em um sistema AMI. Alguns trabalhos tratam dessa questão, entretanto ignoram aspectos importantes de segurança, como as vulnerabilidades provocadas por um agente interno. Trabalhos que abordam apenas ataques externos da rede, ou seja, ataques realizados por um agente que não faz parte do processo de medição como visto na Fig. 3 são apresentados na Subseção III-A.

Um exemplo de ataque externo é um agente malicioso monitorando o tráfego de rede dos SMs e replicando os dados na rede para, por exemplo, realizar um ataque de negação de serviço no agregador [74]. Ou ainda, utilizar desses pacotes recuperados para inferir o consumo de energia elétrica de um consumidor [75]. Esses problemas podem, respectivamente, serem resolvidos através do uso de protocolos que empreguem

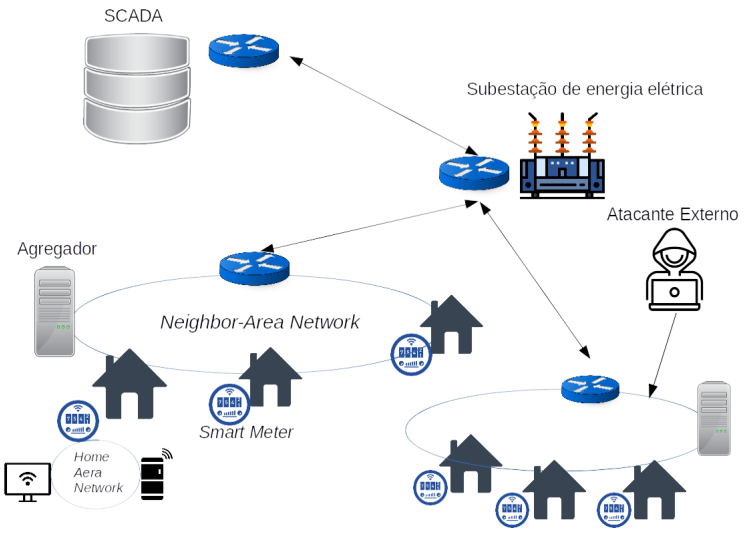


Fig. 3. Exemplo de localização de um adversário externo.

a técnica de desafio/resposta que utilizam números de uso único (*nonces*) e cifração de dados convencional.

No entanto, há outro tipo de ataque que as técnicas anteriores podem não serem suficientes, são os ataques provocados por agentes internos. Esse tipo de ataque é realizado por um agente que faz parte do processo de AMI como representado na Fig. 4. Os atacantes podem ser, ou ter subvertido, o centro de operações, os SMs ou os agregadores.

No caso do adversário ter subvertido o centro de operações, ele terá acesso à chave privada empregada na decifração das mensagens, ou seja, ele é capaz de realizar tanto a decifração de dados agregados, quanto dos dados individuais gerados por cada SM, já que todos empregam a mesma chave pública de um sistema homomórfico. Desta forma, a privacidade do consumidor pode ser comprometida, caso seja realizado o monitoramento de pacotes em conluio entre concessionária e agregador [76]. Vale ressaltar que muitas vezes o agregador é controlado pela própria concessionária.

Já os SMs agindo de maneira maliciosa podem, por exemplo, inserir dados de medição falsos na rede [77]. Outro exemplo que se encaixa como ataque interno consiste em um dispositivo legítimo comportando-se de forma inadequada, por exemplo, personificando outro cliente, de forma a afetar o sistema [78]. Além disso, um agregador agindo de maneira maliciosa poderia gerar dados de medição que não correspondem aos dados reais, dessa forma, uma instabilidade na rede elétrica pode ser causada [79]. Alguns trabalhos que tratam da prevenção de ataques internos são apresentados na Subseção III-B.

Em [80] a divisão é feita de maneira distinta. O trabalho divide esquemas AMI com preservação de privacidade em abordagens criptográficas e não-criptográficas. A primeira ainda é subdividida em agregação de dados, ofuscação e anonimização dos dados. Por outro lado, abordagens não criptográficas recaem em ocultação de carga com bateria e funções fisicamente não clonáveis. O primeiro trata da utilização de uma bateria recarregável para manipular a leitura do medidor, a fim de ocultar o consumo real de energia [81]. Por outro lado o segundo trata da autenticação baseada em hardware [82].

A. *Prevenção ou Detecção de Ataques Externos*

A prerrogativa de confidencialidade nesse contexto serve para garantir a privacidade dos usuários. Em [83] é proposto um esquema de agregação de dados que garante autenticidade e confidencialidade da mensagem. Em contrapartida, o agregador é considerado confiável. Isso é uma vulnerabilidade pelo fato de que caso a concessionária e agregador entrem em conluio, o segundo poderia enviar a medição de cada SM a concessionária. Com isso, a privacidade dos consumidores não é garantida.

Além disso, outro problema encontrado no trabalho é a forma de utilização do esquema *Boneh-Lynn-Shacham* (BLS) para assinatura digital das mensagens. O BLS permite verificação de assinatura de diversas mensagens de maneira eficiente [84]. Com isso, um atacante pode gerar duas mensagens assinadas que verificadas individualmente não correspondem. Contudo, o somatório das mesmas torna o conjunto válido devido a propriedades matemáticas do algoritmo [78]. Por exemplo, escolha duas assinaturas $\sigma'_1 = \sigma_1 + \mathtt{k}$ e $\sigma'_2 = \sigma_2 - \mathtt{k}$, sendo $\mathtt{k}$ uma constante qualquer. Se verificadas individualmente e($\mathtt{P}$,σ'_1)=e($\mathtt{Y}$,$\mathtt{M1}$) e e($\mathtt{P}$,σ'_2)=e($\mathtt{Y}$,$\mathtt{M2}$) são inválidas, entretanto, e($\mathtt{P}$,σ'_1) * e($\mathtt{P}$,σ'_2), torna a assinatura válida devido a característica do BLS [85]. $\mathtt{P}$ e $\mathtt{Y}$ formam um par de chave pública e privada. Por fim, uma desvantagem de [83] é o ponto único de falha. Se o agregador sofrer um ataque de negação de serviço, todo o sistema de AMI é comprometido.

Por outro lado, [86] tem como objetivo agregar os dados antes de enviar a concessionária, detectar e rejeitar pacotes repetidos e fornecer uma camada adicional para a montagem de pacotes. Para atingir os dois primeiros objetivos, o trabalho utiliza da criptografia homomórfica nos dados de medição para agregação e assinatura digital das mensagens de medição junto com um carimbo de tempo.

Apesar de tratar da integridade e autenticidade das mensagens, o trabalho não trata da autenticação dos dispositivos. Já

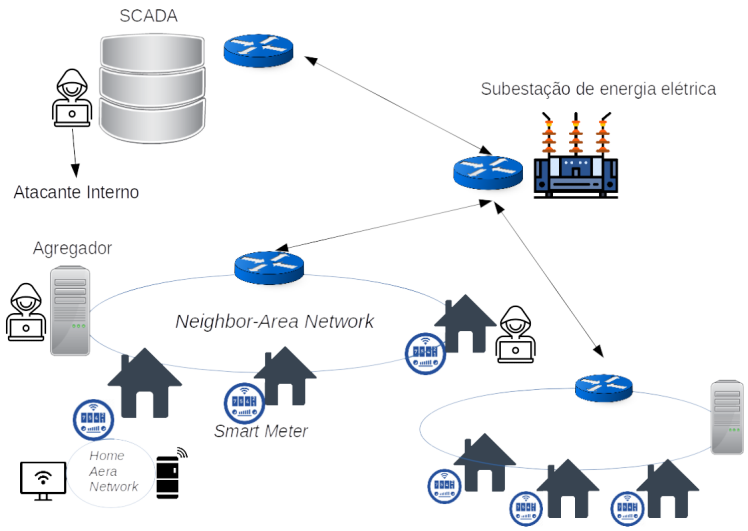


Fig. 4. Exemplos de atacantes internos.

para o terceiro objetivo, o trabalho implementa uma camada que fica entre transporte e aplicação para a montagem dos pacotes. Depois que um dado de medição inteiro for recebido, ele é repassado para a aplicação para agregação [86].

Em [87] é apresentado um esquema de agregação de dados que preserva a privacidade dos usuários. O cripto sistema de Paillier [72] é utilizado para isso. O trabalho faz uso da criptografia baseada em identidade (IBE) para gerar par de chaves público e privada utilizada na assinatura digital [88].

O trabalho parte do princípio que agregadores e centro de operações são confiáveis. O centro de operação gera o par de chaves para o agregador, e ele gera o par de chaves do SM, as quais são utilizadas na assinatura das mensagens [87]. Entretanto, caso esses elementos sejam subvertidos, podem personificar uns aos outros. Com isso, um agregador poderia gerar dados de medições, em nome dos SMs, de forma falsificada, e em consequência causar possíveis instabilidades na rede elétrica. Por exemplo, em um sistema amplamente conectado e integrado, a inserção de medições falsas, inferiores ao que de fato está sendo consumido, poderá disparar processos de adequação no sistema elétrico, como redução indevida na produção de energia por fontes geradoras, que irá afetar a qualidade da energia produzida, ou até mesmo causar disrupção do serviço.

Uma técnica bastante comum para evitar ataques internos como apresentados na Subseção III-B, é a utilização de fatores de ofuscação. Entretanto, apesar de utilizá-lo, [89] não trata da autenticidade e integridade das mensagens.

O trabalho descrito em [90] apresenta um mecanismo para a prevenção de atividade maliciosa de agregadores ou *gateway*, ambos responsáveis por entregar os dados de medição agregados a concessionária. Ao ingressar na rede, cada SM gera seu par de chave assimétrica. Ele utiliza a chave pública e um valor fornecido pelo centro de operações a todos os SMs aplicado a uma função de *hash* para gerar seu identificador.

Em seguida ele envia sua chave pública e tal identificador ao centro de operações. Esse por sua vez, devolve um segredo compartilhado pelos SMs de uma área para realizar o que os autores chamam de autenticação homomórfica no processo de medição [90]. Além disso, o SM também aplica a assinatura digital a mensagem ao agregador. Dessa forma, o agregador ou *gateway* não consegue forjar mensagens de medição da região. Para o processo de agregação, o trabalho utiliza o algoritmo de Paillier.

Entretanto, se o centro de operações, agregador ou *gateway* entrarem em conluio, o primeiro pode recuperar as medições dos usuários. Dessa forma, a privacidade dos usuários não é preservada. Além disso, o trabalho não aborda a prerrogativa de não-repúdio e disponibilidade do serviço.

Outra abordagem é proposta em [91]. O trabalho tem por objetivo evitar que agregadores e SMs consigam inferir dados uns dos outros, além de evitar que dados falsos sejam inseridos na rede. Entretanto, o trabalho pressupõe que a concessionária é confiável e pode recuperar as medições individuais de cada SM para gerenciamento de energia elétrica e preço.

Ainda assim, essa medição conhecida pela concessionária não é em tempo real pois, o agregador envia os dados da região a cada período de tempo `T`. Além disso, o trabalho propõe um algoritmo baseado no ElGamal que se demonstra menos custoso computacionalmente comparado ao trabalho de [78]. O tempo de agregação em [91] é menor. Por exemplo, considerando `n` intervalos de tempo, o SM realiza `n+1` operações de multiplicação e 4 de exponenciação, enquanto que em [78], os SMs necessitam de `n` operações de multiplicação e `2n` operações de exponenciação [91]. O trabalho utiliza de assinatura digital para garantir a autenticidade e integridade da mensagem [91], contudo, não aborda as prerrogativas de não-repúdio e disponibilidade.

B. Prevenção ou Detecção de Ataques Internos e Externos

Uma abordagem para prevenção de ataques internos e externos é apresentada em [78]. A arquitetura é formada por três partes, um agregador, os medidores inteligentes e uma terceira entidade confiável. Ao entrar na rede, os SMs e o agregador recebem um valor pseudoaleatório com tamanho

maior que 1024 bits. Esse valor é utilizado na cifração dos dados sobre consumo de energia elétrica onde também é aplicada a assinatura digital em cada SM.

Esse valor é chamado de fator de ofuscação. Dessa forma cada medidor inteligente possui um valor diferente e não há como forjar mensagens e assinaturas de medição. O dado agregado corresponderá a medição real apenas quando todos SMs enviarem as medições ao agregador. Isso se dá pela propriedade apontada que apenas quando juntado todos fatores de ofuscação, eles não terão influência sobre o dado encriptado [78]. Outro trabalho que também utiliza fator de ofuscação para prevenção de ataques internos é apresentado em [92]. Ambas propostas se assemelham bastante, entretanto, a proposta apresentada em [92] possui custo computacional menor. Ambos trabalhos tem crescimento linear, contudo, a constante multiplicativa em [92] é menor. Para agregação de dados, [92] tem custo de `3.33n + 103.4`, enquanto que [78], `52.58n + 54.15`, sendo `n`, a quantidade de intervalos de tempo de medição.

Em [93] é utilizada uma abordagem semelhante. Entretanto, também é realizada a contagem dos SMs que enviaram suas medições. Apesar dos trabalhos abordarem as questões de autenticidade, preservação de privacidade dos usuários e integridade das informações, os trabalhos não abordam a disponibilidade do agregador e a propriedade de não-repúdio dos dispositivos. Caso o sistema seja alvo de um ataque de negação de serviço, todo o sistema AMI é comprometido. Além disso, os trabalhos não tratam da autenticação dos dispositivos através de uma Infraestrutura de Chave Pública (ICP).

Já em [94] é apresentado um esquema de autenticação para dados agregados de forma eficiente, o esquema utiliza BLS para assinatura. Dessa maneira, o processamento para verificação de segurança diminui, tendo em vista que ele é uma assinatura agregada. Além disso, permite a rastreabilidade em mensagens incorretas, o esquema também define um mecanismo de redundância no caso do agregador falhar. Quando isso acontece, outro dispositivo na rede assume a função de agregador.

Outra abordagem é apresentada em [95], o trabalho utiliza da estrutura da *blockchain* para agregação dos dados. Além disso, para autenticação dos usuários, um filtro de Bloom é utilizado. O SM obtém seu identificador junto a uma terceira parte confiável através de uma prova de conhecimento zero. A terceira parte confiável gera um *hash* de uma chave pública gerada por ele que é aplicado em `mod n`, sendo `n` o tamanho do *array* que contém os identificadores, para encontrar a posição dele. Depois, ela devolve um par de chaves assimétrica ao SM, e envia a chave pública gerada para os demais SMs autenticarem o SM que deseja entrar na *blockchain* [95].

O nó minerador é escolhido a cada rodada de agregação, através da média do consumo da rodada anterior. Os autores do trabalho optaram pela *blockchain* pelo fato da dificuldade de um impostor injetar dados falsos. Para inserção de dados falsos, é necessário que mais da metade dos dispositivos que façam parte sejam comprometidos [96]. Cada nó verifica se o identificador de quem publicou a mensagem encontra-se no filtro de Bloom. A assinatura da mensagem é composta por identificador e chave pública. Esse identificador não corresponde ao identificador real dos SMs [95].

Uma desvantagem do trabalho apresentado em [95] é que caso a terceira parte confiável seja subvertida, ela poderia personificar um SM. Com isso, a prerrogativa de não-repúdio não é garantida.

Em [97] é apresentado um esquema de autenticação incremental ponto-a-ponto onde cada nó assina a mensagem e o receptor verifica a assinatura. Além disso, o receptor mantém salvo em uma tabela a assinatura das mensagens recebidas. O trabalho monta uma *Spanning-Tree* a partir de uma rede *Mesh*. Isso serve para rastreabilidade no caso do agregador encontrar um valor incorreto e desejar descobrir em que momento ocorreu problema na mensagem.

Com base nos trabalhos citados pode-se observar que a arquitetura geralmente é formada por três componentes: SMs, *gateway* ou agregador, e uma terceira entidade confiável, que é responsável por fornecer os valores públicos utilizados na aplicação. Já o trabalho de [98] apresenta uma arquitetura em que se elimina a necessidade da última entidade. Para ingressar no sistema, o agregador e SM utilizam de um protocolo de prova de conhecimento-zero em que o segundo se autentica ao primeiro sem a necessidade de uma terceira entidade confiável.

Uma vez autenticado, o SM recebe suas credenciais do agregador que, por sua vez, armazena as informações em uma lista que contém todas as credenciais de SMs. Quando eles desejam enviar seus valores de medição ao agregador, utilizam das credenciais recebidas para gerar um desafio junto a mensagem e fazem assinatura dessa para garantir integridade e autenticidade [98].

Outro trabalho que tem como objetivo prevenir ataques internos e externos é apresentado em [99]. O trabalho tem como proposta uma arquitetura para agregação de dados que garante a privacidade dos usuários de maneira eficiente através de um algoritmo baseado em ElGamal com *Elliptic Curve Cryptography* (ECC). Além disso, para diminuir o processamento da decifração e verificação da autenticidade da mensagem, uma assinatura BLS é utilizada.

Ainda, o trabalho [99] considera três tipos de atacantes: (i) o primeiro é um agente malicioso que realiza o monitoramento das mensagens nos SMs para recuperar seus dados de medição. Isso é resolvido através de técnicas da cifração dos dados; (ii) o segundo tipo de atacante realiza a personificação de um ou mais SMs para enviar dados falsos em nome deles para o centro de operações, o que pode ser resolvido através do emprego de assinatura digital; (iii) E por fim, um atacante interno que pode ouvir o canal de comunicação entre SM e seu *gateway* ou agregador, o que pode comprometer a privacidade dos usuários, já que ele tem posse do par de chaves pública e privada utilizada no processo de cifração e decifração dos dados agregados. Para contornar esse problema, um fator de ofuscação é usado, onde cada SM tem um valor distinto e o utiliza no processo de cifração. O somatório de todos os fatores de ofuscação e o fator de ofuscação do centro de operações retira a influência dele sobre o dado em texto plano [99]. Entretanto, fatores de ofuscação tornam as propostas não-escaláveis tendo em vista que basta um SM não enviar seus dados de medição para que não possa ser recuperada a

demanda de energia elétrica de uma região.

Como alternativa aos métodos anteriores, a utilização de *Fog Computing*, que é uma camada entre a *Cloud* e os dispositivos, pode ser implantada para agregação dos dados [100]. Ao invés dos SMs enviarem suas medições ao agregador que pode ser um dispositivo de posse da concessionária, eles enviam para a *Fog* [101]. No trabalho proposto é utilizado o cripto sistema de Paillier para a agregação homomórfica dos dados. Para autenticação e integridade das mensagens, SMs assinam a mensagem que vai para a *Fog* e ela, por sua vez, faz o mesmo processo para enviar as medições agregadas para a concessionária.

Em [102] é proposto um esquema que garante a confidencialidade e autenticidade da mensagem gerada por um SM e enviada ao agregador. Entretanto, o último poderá recuperar as informações de medição de energia elétrica dos SMs. Dessa forma, o ataque realizado é passivo [103]. Isso significa que o agregador não modifica os dados de medição mas pode tentar recuperá-los. Para evitar isso, um fator de ofuscação é utilizado, e para evitar ataques de replicação, o agregador anuncia um identificador em cada rodada de medição que compõem a mensagem de medição do SM. Essa mensagem é assinada pelo SM para garantia de autenticidade. Diferente de alguns dos trabalhos apresentados anteriormente, o fator de ofuscação não é gerado por uma terceira entidade confiável, e utiliza um protocolo entre SM e concessionária [102].

Uma outra abordagem é apresentada em [104]. Cada SM envia uma chave `Ki` que está em um intervalo de 0 até um número primo `p`-1 para a concessionária. Essa por sua vez, após receber todas as chaves dos SMs, agregá-as, gerando uma chave que é utilizada no processo de decifração das medições recebidas. A concessionária devolve essa chave aos SMs. Onde ela é empregada para atualizar sua chave e no processo de encriptação. Para atualizar a chave, os SMs estabelecem um protocolo que compartilham sua chave atual e um número aleatório uns com os outros. Após, aplicam a soma da chave atual com o número aleatório gerado por ele, subtraído pelo número gerado por outro SM, gerando assim, a nova chave utilizada para encriptação [104].

Para o processo de encriptação, os SMs utilizam uma chave que a concessionária não conhece, pelo fato da utilização do processo de atualização. Entretanto, as chaves atualizadas não modificam a chave agregada. Os SMs aplicam um código de autenticação de mensagem baseada em *hash* ou *Hash Message Authentication Code* (HMAC), em que se utiliza de um segredo compartilhado combinado a funções de hash para autenticidade e integridade das mensagens [104]. A mensagem encriptada e o carimbo de tempo atual são aplicados ao HMAC para evitar que dados falsos sejam inseridos na rede e evitar ataques de replicação. Depois de receber todas as medições, a concessionária consegue recuperar os dados agregados, assim preservando a privacidade dos usuários [104]. Entretanto, o trabalho pressupõe que os SMs sempre estarão disponíveis. Dessa forma, a abordagem não se torna escalável. Um único dispositivo que tenha sofrido um ataque de negação de serviço ou ainda, esteja em mau funcionamento, faz com que a concessionária não consiga recuperar os dados de medição do conjunto de SMs. Além disso, o trabalho não trata da autenticidade da concessionária e dos SMs.

Outro trabalho proposto com a prevenção de ataques internos e externos é proposto em [105]. O objetivo do trabalho é construir uma arquitetura de agregação de dados com preservação de privacidade e tolerância a falhas. Para isso, o trabalho possui 4 componentes, uma autoridade confiável, um conjunto de SMs, um *gateway* ou agregador e um conjunto de servidores mantidos no centro de controle escolhidos de forma randômica a cada rodada de medição para decifração do dado agregado, além disso, o sistema criptográfico Paillier é utilizado.

A autoridade confiável ou *Trusted Authority* (TA) gera a chave privada dos SMs, eles utilizam o *hash* do tempo da rodada elevado na chave privada multiplicado pelo texto plano elevado na chave pública do Paillier para cifrar a medição. Portanto, o somatório das chaves privadas é utilizada para verificação se algum dos SMs não tenha enviado seus dados de medição. O centro de controle envia o dado para a TA fazer a verificação. Entretanto, o trabalho aponta que a TA apenas distribui as chaves privadas e os valores de inicialização do sistema e após fica offline, o que se torna uma contradição. Dessa forma, mesmo na presença de falhas de alguns dos SMs, o dado agregado pode ser recuperado, além disso, o adversário pode corromper metade dos servidores e ser o escolhido da rodada para inferir a privacidade dos usuários [105]. Apesar de o trabalho abordar a disponibilidade na presença de falha em alguns SMs e que alguns dos servidores sejam comprometidos, o trabalho não aborda a falha do *gateway* ou agregador. Adicionalmente, o trabalho não trata da autenticação dos dispositivos e da integridade das mensagens. Pressupõem-se que os dispositivos que contatam a TA são confiáveis [105].

IV. Discussão

Nessa seção é apresentada uma discussão geral sobre os trabalhos apresentados na Seção III. A Tabela I apresenta as prerrogativas de segurança cibernética que cada trabalho aborda. Além disso, apresenta se fazem uso do fator de ofuscação, previnem ou detectam ataques internos ou externos. A prerrogativa de confidencialidade diz respeito a um atacante externo recuperar as informações. Já a prerrogativa de integridade serve para garantir que um dado não foi modificado. Por exemplo, em [83], um atacante poderia inserir mensagens de medição falsas, entretanto, não conseguiria recuperar uma mensagem por não ter posse da chave privada utilizada na decifração da mensagem.

Para tratar dessa questão, a prerrogativa de autenticidade é utilizada. Para isso, a maioria dos trabalhos utiliza assinatura digital. Por outro lado, nenhum dos trabalhos utiliza ICP para autenticação dos dispositivos, dessa forma, a prerrogativa de não-repúdio não é tratada em nenhum dos trabalhos. Um agente malicioso tendo conhecimento do protocolo e funcionamento na rede poderia ingressar nela e injetar dados de medição como se fosse um SM.

Para a prerrogativa de disponibilidade foram considerados trabalhos que abordam redundância na falha de um agregador, portanto, a disponibilidade do serviço, tendo como exemplo os trabalhos [94] e [95]. Alguns trabalhos abordam a diminuição

TABELA I
COMPARAÇÃO DE CARACTERÍSTICAS DOS TRABALHOS

Trabalho	Confidencialidade	Integridade	Disponibilidade	Autenticidade	Não-repúdio	Ataques Externos	Ataques Internos	Fator de Ofuscação
[83]	V	V	X	V	X	V	X	X
[78]	V	V	X	V	X	V	V	V
[86]	V	V	X	V	X	V	X	X
[87]	V	V	X	X	X	V	X	X
[89]	V	X	X	X	X	V	X	V
[90]	V	V	X	V	X	V	X	X
[91]	V	V	X	V	X	V	X	X
[92]	V	V	X	V	X	V	V	V
[93]	V	V	X	V	X	V	V	V
[94]	V	V	V	V	X	V	V	X
[95]	V	V	V	V	X	V	V	X
[97]	V	V	X	V	X	V	V	X
[98]	V	V	X	V	X	V	V	X
[99]	V	V	X	V	X	V	V	V
[101]	V	V	V	V	X	V	V	X
[102]	V	V	X	V	X	V	V	V
[104]	V	V	X	V	X	V	V	X
[105]	V	X	X	X	X	V	V	X

de pacotes na rede ou a detecção em rejeição de pacotes repetidos, entretanto, não foi considerada a disponibilidade da rede. Contudo, essa é uma prerrogativa de alta relevância para o funcionamento da AMI. Caso o SM ou o agregador falhem, o sistema é comprometido, por exemplo, a concessionária não saberá a quantidade correta de energia requisitada em uma região.

Para evitar ataques internos, é comum a utilização de fatores de ofuscação, entretanto, não é uma alternativa escalável. Para manter a propriedade do somatório dos fatores igual a zero, é montado um *array* com `n` valores. Se um novo dispositivo desejar ingressar na rede e fazer parte do processo de medição, os valores têm de ser redistribuídos. Além disso, o trabalho apresentado em [104], também não é escalável. Cada novo dispositivo inserido na rede teria de enviar sua chave para a concessionária, ela teria de recalcular a chave agregada e atualizá-la para todos dispositivos daquele grupo.

V. CONCLUSÃO

A *Smart Grid* aparece como um conceito difundido na literatura, entretanto, ainda há desafios com relação a segurança da informação. Um dos principais sistemas que a permitem seu funcionamento é a AMI [31]. Entretanto, existe alguns desafios nesse sistema. Por exemplo, como fazer a medição de energia elétrica de forma segura e que não prejudique o serviço?

Muitos trabalhos na literatura apresentam propostas que tratam da questão de preservação de privacidade. Entretanto, outras prerrogativas da segurança da informação como disponibilidade muitas vezes são tangenciadas. Por exemplo, se o agregador ou *gateway* parar de funcionar, a medição não pode ser realizada. Isso pode causar instabilidade na rede.

Além disso, a grande maioria dos trabalhos apresentados não utiliza da ICP que é utilizada para autenticação dos dispositivos [106]. Apesar dos SMs possuírem recursos computacionais limitados, há algoritmos que empregam chaves assimétricas, como ECC, que são computacionalmente menos onerosos que os sistemas tradicionais baseados e fatoração de números primos, como o RSA [107]. Além disso, também é preciso tratar da detecção de intrusão e falhas em SM.

Por fim, as principais contribuições deste trabalho consistem na revisão de literatura sobre os requisitos de segurança da informação para AMI. Adicionalmente, apresentação de algumas das arquiteturas propostas na literatura abordando diferentes tipos de ataques. Como trabalho futuro, fica a elaboração de um esquema para agregação de dados com preservação de privacidade dos usuários. Além disso, o trabalho faz a divisão entre os tipos de adversários, diferente de [80] que agrupa as propostas na literatura de acordo com o mecanismo de defesa.

REFERÊNCIAS

[1] Z. Baloch, F. K. Shaikh, and M. A. Unar, "A context-aware data fusion approach for health-iot," *International Journal of Information Technology*, vol. 10, no. 3, pp. 241–245, 2018.

[2] I. Mat, M. R. M. Kassim, A. N. Harun, and I. M. Yusoff, "Iot in precision agriculture applications using wireless moisture sensor network," in *2016 IEEE Conference on Open Systems (ICOS)*. IEEE, 2016, pp. 24–29.

[3] S. Anwar and D. Kishore, "Iot based smart home security system with alert and door access control using smart phone," *International Journal of Engineering Research & Technology (IJERT)*, vol. 5, no. 12, pp. 504–509, 2016.

[4] H. T. Haider, O. H. See, and W. Elmenreich, "A review of residential demand response of smart grid," *Renewable and Sustainable Energy Reviews*, vol. 59, pp. 166–178, 2016.

[5] M. Hossain, N. Madlool, N. Rahim, J. Selvaraj, A. Pandey, and A. F. Khan, "Role of smart grid in renewable energy: An overview," *Renewable and Sustainable Energy Reviews*, vol. 60, pp. 1168–1184, 2016.

[6] W. Fernandez and A. Rodriguez, "Analysis of the regulatory requirements for the smart grid in chile," *IEEE Latin America Transactions*, vol. 15, no. 1, pp. 13–20, 2017.

[7] Y. Lopes, N. C. Fernandes, and K. Obraczka, "Smart grid communication: Requirements and scada protocols analysis," in *2018 Simposio Brasileiro de Sistemas Eletricos (SBSE)*. IEEE, 2018, pp. 1–6.

[8] Mendel, Jacob and others, "Smart grid cyber security challenges: Overview and classification," *e-mentor*, vol. 68, no. 1, pp. 55–66, 2017.

[9] S.-K. Kim and J.-H. Huh, "A study on the improvement of smart grid security performance and blockchain smart grid perspective," *Energies*, vol. 11, no. 8, p. 1973, 2018.

[10] R. Zafar, A. Mahmood, S. Razzaq, W. Ali, U. Naeem, and K. Shehzad, "Prosumer based energy management and sharing in smart grid," *Renewable and Sustainable Energy Reviews*, vol. 82, pp. 1675–1684, 2018.

[11] S. Tan, D. De, W.-Z. Song, J. Yang, and S. K. Das, "Survey of security advances in smart grid: A data driven approach," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 397–422, 2017.

[12] W. Wang and Z. Lu, "Cyber security in the smart grid: Survey and challenges," *Computer networks*, vol. 57, no. 5, pp. 1344–1371, 2013.

[13] H. He and J. Yan, "Cyber-physical attacks and defences in the smart grid: a survey," *IET Cyber-Physical Systems: Theory & Applications*, vol. 1, no. 1, pp. 13–27, 2016.

[14] Z. El Mrabet, N. Kaabouch, H. El Ghazi, and H. El Ghazi, "Cyber-security in smart grid: Survey and challenges," *Computers & Electrical Engineering*, vol. 67, pp. 469–482, 2018.

[15] Z. Fan, P. Kulkarni, S. Gormus, C. Efthymiou, G. Kalogridis, M. Sooriyabandara, Z. Zhu, S. Lambotharan, and W. H. Chin, "Smart grid communications: Overview of research challenges, solutions, and standardization activities," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 1, pp. 21–38, 2012.

[16] N. Good, K. A. Ellis, and P. Mancarella, "Review and classification of barriers and enablers of demand response in the smart grid," *Renewable and Sustainable Energy Reviews*, vol. 72, pp. 57–72, 2017.

[17] R. Bayindir, I. Colak, G. Fulli, and K. Demirtas, "Smart grid technologies and applications," *Renewable and Sustainable Energy Reviews*, vol. 66, pp. 499–516, 2016.

[18] M. Emmanuel and R. Rayudu, "Communication technologies for smart grid applications: A survey," *Journal of Network and Computer Applications*, vol. 74, pp. 133–148, 2016.

[19] Y. Kabalci, "A survey on smart metering and smart grid communication," *Renewable and Sustainable Energy Reviews*, vol. 57, pp. 302–318, 2016.

[20] S. Sultan, "Privacy-preserving metering in smart grid for billing, operational metering, and incentive-based schemes: A survey," *Computers & Security*, vol. 84, pp. 148–165, 2019.

[21] M. A. Ferrag, L. A. Maglaras, H. Janicke, and J. Jiang, "A survey on privacy-preserving schemes for smart grid communications," *arXiv preprint arXiv:1611.07722*, 2016.

[22] M. Rogozinski and R. F. Calili, "Smart grid security applied to the brazilian scenario: A visual approach," *IEEE Latin America Transactions*, vol. 100, no. 1e, 2020.

[23] A. K. Sangaiah, D. V. Medhane, G.-B. Bian, A. Ghoneim, M. Alrashoud, and M. S. Hossain, "Energy-aware green adversary model for cyberphysical security in industrial system," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 5, pp. 3322–3329, 2019.

[24] M. L. Tuballa and M. L. Abundo, "A review of the development of smart grid technologies," *Renewable and Sustainable Energy Reviews*, vol. 59, pp. 710–725, 2016.

[25] R. Ullah, Y. Faheem, and B. Kim, "Energy and congestion-aware routing metric for smart grid ami networks in smart city," *IEEE Access*, vol. 5, pp. 13 799–13 810, 2017.

[26] M. H. Cintuglu, O. A. Mohammed, K. Akkaya, and A. S. Uluagac, "A survey on smart grid cyber-physical system testbeds," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 446–464, 2016.

[27] R. Deng, Z. Yang, M.-Y. Chow, and J. Chen, "A survey on demand response in smart grids: Mathematical models and approaches," *IEEE Transactions on Industrial Informatics*, vol. 11, no. 3, pp. 570–582, 2015.

[28] S. Nimbargi, S. Mhaisne, S. Nangare, and M. Sinha, "Review on ami technology for smart meter," in *2016 IEEE International Conference on Advances in Electronics, Communication and Computer Technology (ICAECCT)*. IEEE, 2016, pp. 21–27.

[29] Z. Erkin, J. R. Troncoso-Pastoriza, R. L. Lagendijk, and F. Pérez-González, "Privacy-preserving data aggregation in smart metering systems: An overview," *IEEE Signal Processing Magazine*, vol. 30, no. 2, pp. 75–86, 2013.

[30] H. H. Safa, D. M. Souran, M. Ghasempour, and A. Khazaee, "Cyber security of smart grid and scada systems, threats and risks," in *CIRED Workshop 2016*, 2016, pp. 1–4.

[31] M. Benmalek, Y. Challal, A. Derhab, and A. Bouabdallah, "Versami: Versatile and scalable key management for smart grid ami systems," *Computer Networks*, vol. 132, pp. 161–179, 2018.

[32] K. G. Di Santo, E. Kanashiro, S. G. Di Santo, and M. A. Saidel, "A review on smart grids and experiences in brazil," *Renewable and Sustainable Energy Reviews*, vol. 52, pp. 1072–1082, 2015.

[33] A. Ghosal and M. Conti, "Key management systems for smart grid advanced metering infrastructure: A survey," *IEEE Communications Surveys Tutorials*, vol. 21, no. 3, pp. 2831–2848, 2019.

[34] M. Shrestha, C. Johansen, J. Noll, and D. Roverso, "A methodology for security classification applied to smart grid infrastructures," *International Journal of Critical Infrastructure Protection*, vol. 28, p. 100342, 2020.

[35] V. Odelu, A. K. Das, M. Wazid, and M. Conti, "Provably secure authenticated key agreement scheme for smart grid," *IEEE Transactions on Smart Grid*, vol. 9, no. 3, pp. 1900–1910, 2016.

[36] R. R. Mohassel, A. Fung, F. Mohammadi, and K. Raahemifar, "A survey on advanced metering infrastructure," *International Journal of Electrical Power & Energy Systems*, vol. 63, pp. 473–484, 2014.

[37] N. Saputro and K. Akkaya, "Investigation of smart meter data reporting strategies for optimized performance in smart grid ami networks," *IEEE Internet of Things Journal*, vol. 4, no. 4, pp. 894–904, 2017.

[38] Y. Yoldaş, A. Önen, S. Muyeen, A. V. Vasilakos, and İ. Alan, "Enhancing smart grid with microgrids: Challenges and opportunities," *Renewable and Sustainable Energy Reviews*, vol. 72, pp. 205–214, 2017.

[39] E. U. Haq, H. Xu, L. Pan, and M. I. Khattak, "Smart grid security: threats and solutions," in *2017 13th International Conference on Semantics, Knowledge and Grids (SKG)*. IEEE, 2017, pp. 188–193.

[40] B. Gupta and T. Akhtar, "A survey on smart power grid: frameworks, tools, security issues, and solutions," *Annals of Telecommunications*, vol. 72, no. 9-10, pp. 517–549, 2017.

[41] E. Irmak and İ. Erkek, "An overview of cyber-attack vectors on scada systems," in *2018 6th International Symposium on Digital Forensic and Security (ISDFS)*. IEEE, 2018, pp. 1–5.

[42] W. Alves, D. Martins, U. Bezerra, and A. Klautau, "A hybrid approach for big data outlier detection from electric power scada system," *IEEE Latin America Transactions*, vol. 15, no. 1, pp. 57–64, 2017.

[43] V. K. Singh, H. Ebrahem, and M. Govindarasu, "Security evaluation of two intrusion detection systems in smart grid scada environment," in *2018 North American Power Symposium (NAPS)*. IEEE, 2018, pp. 1–6.

[44] K. R. Khan, A. Rahman, A. Nadeem, M. S. Siddiqui, and R. A. Khan, "Remote monitoring and control of microgrid using smart sensor network and internet of thing," in *2018 1st International Conference on Computer Applications Information Security (ICCAIS)*, 2018, pp. 1–4.

[45] M. Marian, A. Cusman, D. Popescu, and D. Ionică, "A dnp3-based scada architecture supporting electronic signatures," in *2019 20th International Carpathian Control Conference (ICCC)*, 2019, pp. 1–6.

[46] F. Espinoza, M. Mar, E. Ramirez, and J. Noel, "Control of real power in a synchronous machine using a scada system in a smart grid," in *2016 IEEE ANDESCON*, 2016, pp. 1–4.

[47] I. Colak, S. Sagiroglu, G. Fulli, M. Yesilbudak, and C.-F. Covrig, "A survey on the critical issues in smart grid technologies," *Renewable and Sustainable Energy Reviews*, vol. 54, pp. 396–405, 2016.

[48] Y. Zhang, L. Wang, Y. Xiang, and C.-W. Ten, "Power system reliability evaluation with scada cybersecurity considerations," *IEEE Transactions on Smart Grid*, vol. 6, no. 4, pp. 1707–1721, 2015.

[49] A. Anwar, A. Mahmood, and M. Pickering, "Estimation of smart grid topology using scada measurements," in *2016 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, 2016, pp. 539–544.

[50] A. O. Otuoze, M. W. Mustafa, and R. M. Larik, "Smart grids security challenges: Classification by sources of threats," *Journal of Electrical Systems and Information Technology*, vol. 5, no. 3, pp. 468–483, 2018.

[51] P. Kumar, Y. Lin, G. Bai, A. Paverd, J. S. Dong, and A. Martin, "Smart grid metering networks: A survey on security, privacy and open research issues," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2886–2927, 2019.

[52] S. Garg, K. Kaur, G. Kaddoum, J. J. P. C. Rodrigues, and M. Guizani, "Secure and lightweight authentication scheme for smart metering infrastructure in smart grid," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 5, pp. 3548–3557, 2020.

[53] C. Ruland and J. Sassmannshausen, "System-wide traceability of commands and data exchange in smart grids," in *2019 International*

Conference on Smart Energy Systems and Technologies (SEST). IEEE, 2019, pp. 1–6.

[54] K. Mahmood, S. A. Chaudhry, H. Naqvi, S. Kumari, X. Li, and A. K. Sangaiah, "An elliptic curve cryptography based lightweight authentication scheme for smart grid communication," *Future Generation Computer Systems*, vol. 81, pp. 557–565, 2018.

[55] T. Zhang, T. Zhang, X. Ji, and W. Xu, "Cuckoo-rpl: Cuckoo filter based rpl for defending ami network from blackhole attacks," in *2019 Chinese Control Conference (CCC)*, 2019, pp. 8920–8925.

[56] R. C. Diovu and J. T. Agee, "A cloud-based openflow firewall for mitigation against ddos attacks in smart grid ami networks," in *2017 IEEE PES PowerAfrica*, 2017, pp. 28–33.

[57] R. Mahmud, R. Vallakati, A. Mukherjee, P. Ranganathan, and A. Nejadpak, "A survey on smart grid metering infrastructures: Threats and solutions," in *2015 IEEE International Conference on Electro/Information Technology (EIT)*. IEEE, 2015, pp. 386–391.

[58] Ghosal, Amrita and Conti, Mauro, "Key management systems for smart grid advanced metering infrastructure: A survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2831–2848, 2019.

[59] R. K. Pandey and M. Misra, "Cyber security threats—smart grid infrastructure," in *2016 National Power Systems Conference (NPSC)*. IEEE, 2016, pp. 1–6.

[60] J. Giraldo, A. Cárdenas, and N. Quijano, "Integrity attacks on real-time pricing in smart grids: Impact and countermeasures," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2249–2257, 2017.

[61] S. Tan, W. Song, M. Stewart, J. Yang, and L. Tong, "Online data integrity attacks against real-time electrical market in smart grid," *IEEE Transactions on Smart Grid*, vol. 9, no. 1, pp. 313–322, 2018.

[62] Rizzetti, Tiago Antonio and others, "Novos métodos para prover segurança à comunicação no âmbito de redes elétricas inteligentes," Ph.D. dissertation, Universidade Federal de Santa Maria, 2018.

[63] M. Z. Gunduz and R. Das, "Analysis of cyber-attacks on smart grid applications," in *2018 International Conference on Artificial Intelligence and Data Processing (IDAP)*, 2018, pp. 1–5.

[64] A. Sanjab, W. Saad, I. Guvenc, A. Sarwat, and S. Biswas, "Smart grid security: Threats, challenges, and solutions," *arXiv preprint arXiv:1606.06992*, 2016.

[65] U. Ozgur, S. Tonyali, K. Akkaya, and F. Senel, "Comparative evaluation of smart grid ami networks: Performance under privacy," in *2016 IEEE Symposium on Computers and Communication (ISCC)*, 2016, pp. 1134–1136.

[66] A. Acar, H. Aksu, A. S. Uluagac, and M. Conti, "A survey on homomorphic encryption schemes: Theory and implementation," *ACM Computing Surveys (CSUR)*, vol. 51, no. 4, p. 79, 2018.

[67] J. H. Cheon, A. Kim, M. Kim, and Y. Song, "Homomorphic encryption for arithmetic of approximate numbers," in *International Conference on the Theory and Application of Cryptology and Information Security*. Springer, 2017, pp. 409–437.

[68] Chase, Melissa and Chen, Hao and Ding, Jintai and Goldwasser, Shafi and Gorbunov, Sergey and Hoffstein, Jeffrey and Lauter, Kristin and Lokam, Satya and Moody, Dustin and Morrison, Travis and others, "Security of homomorphic encryption," *HomomorphicEncryption. org, Redmond WA, Tech. Rep*, 2017.

[69] P. V. Parmar, S. B. Padhar, S. N. Patel, N. I. Bhatt, and R. H. Jhaveri, "Survey of various homomorphic encryption algorithms and schemes," *International Journal of Computer Applications*, vol. 91, no. 8, 2014.

[70] C. Gentry and D. Boneh, *A fully homomorphic encryption scheme*. Stanford University Stanford, 2009, vol. 20, no. 09.

[71] M. Alloghani, M. M. Alani, D. Al-Jumeily, T. Baker, J. Mustafina, A. Hussain, and A. J. Aljaaf, "A systematic review on the status and progress of homomorphic encryption technologies," *Journal of Information Security and Applications*, vol. 48, p. 102362, 2019.

[72] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 1999, pp. 223–238.

[73] G. Blakley and I. Borosh, "Rivest-shamir-adleman public key cryptosystems do not always conceal messages," *Computers & Mathematics with Applications*, vol. 5, no. 3, pp. 169–178, 1979.

[74] K. Wang, M. Du, S. Maharjan, and Y. Sun, "Strategic honeypot game model for distributed denial of service attacks in the smart grid," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2474–2482, 2017.

[75] S. Finster and I. Baumgart, "Privacy-aware smart metering: A survey," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 2, pp. 1088–1101, 2015.

[76] W. Tong, L. Lu, Z. Li, J. Lin, and X. Jin, "A survey on intrusion detection system for advanced metering infrastructure," in *2016 Sixth International Conference on Instrumentation Measurement, Computer, Communication and Control (IMCCC)*, 2016, pp. 33–37.

[77] B. Tang, J. Yan, S. Kay, and H. He, "Detection of false data injection attacks in smart grid under colored gaussian noise," in *2016 IEEE Conference on Communications and Network Security (CNS)*. IEEE, 2016, pp. 172–179.

[78] C.-I. Fan, S.-Y. Huang, and Y.-L. Lai, "Privacy-enhanced data aggregation scheme against internal attackers in smart grid," *IEEE Transactions on Industrial informatics*, vol. 10, no. 1, pp. 666–675, 2013.

[79] N. V. Abhishek, T. J. Lim, B. Sikdar, and A. Tandon, "An intrusion detection system for detecting compromised gateways in clustered iot networks," in *2018 IEEE International Workshop Technical Committee on Communications Quality and Reliability (CQR)*. IEEE, 2018, pp. 1–6.

[80] S. Desai, R. Alhadad, N. Chilamkurti, and A. Mahmood, "A survey of privacy preserving schemes in ioe enabled smart grid advanced metering infrastructure," *Cluster Computing*, vol. 22, no. 1, pp. 43–69, 2019.

[81] Y. Sun, L. Lampe, and V. W. S. Wong, "Ev-assisted battery load hiding: A markov decision process approach," in *2016 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, 2016, pp. 160–166.

[82] M. Nabeel, S. Kerr, X. Ding, and E. Bertino, "Authentication and key management for advanced metering infrastructures utilizing physically unclonable functions," in *2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm)*. IEEE, 2012, pp. 324–329.

[83] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, "Eppa: An efficient and privacy-preserving aggregation scheme for secure smart grid communications," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 9, pp. 1621–1631, 2012.

[84] M.-S. Lacharité, "Security of bls and bgls signatures in a multi-user setting," *Cryptography and Communications*, vol. 10, no. 1, pp. 41–58, 2018.

[85] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the weil pairing," in *International Conference on the Theory and Application of Cryptology and Information Security*. Springer, 2001, pp. 514–532.

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

[87] H. Li, X. Lin, H. Yang, X. Liang, R. Lu, and X. Shen, "Eppdr: An efficient privacy-preserving demand response scheme with adaptive key evolution in smart grid," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 8, pp. 2053–2064, 2013.

[88] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 2005, pp. 457–473.

[89] R. Lu, K. Alharbi, X. Lin, and C. Huang, "A novel privacy-preserving set aggregation scheme for smart grid communications," in *2015 IEEE global communications conference (GLOBECOM)*. IEEE, 2015, pp. 1–6.

[90] J. Ni, K. Alharbi, X. Lin, and X. Shen, "Security-enhanced data aggregation against malicious gateways in smart grid," in *2015 IEEE Global Communications Conference (GLOBECOM)*. IEEE, 2015, pp. 1–6.

[91] X. Dong, J. Zhou, K. Alharbi, X. Lin, and Z. Cao, "An elgamal-based efficient and privacy-preserving data aggregation scheme for smart grid," in *2014 IEEE Global Communications Conference*. IEEE, 2014, pp. 4720–4725.

[92] D. He, N. Kumar, and J.-H. Lee, "Privacy-preserving data aggregation scheme against internal attackers in smart grids," *Wireless Networks*, vol. 22, no. 2, pp. 491–502, 2016.

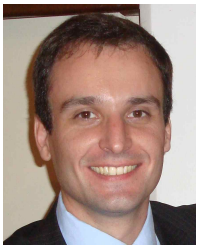
[93] S. Li, K. Xue, Q. Yang, and P. Hong, "Ppma: Privacy-preserving multisubset data aggregation in smart grid," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 2, pp. 462–471, 2017.

[94] D. Li, Z. Aung, J. R. Williams, and A. Sanchez, "Efficient authentication scheme for data aggregation in smart grid with fault tolerance and fault diagnosis," in *2012 IEEE PES Innovative Smart Grid Technologies (ISGT)*. IEEE, 2012, pp. 1–8.

[95] Z. Guan, G. Si, X. Zhang, L. Wu, N. Guizani, X. Du, and Y. Ma, "Privacy-preserving and efficient aggregation based on blockchain for power grid communications in smart communities," *IEEE Communications Magazine*, vol. 56, no. 7, pp. 82–88, 2018.

[96] I.-C. Lin and T.-C. Liao, "A survey of blockchain security issues and challenges." *IJ Network Security*, vol. 19, no. 5, pp. 653–659, 2017.
[97] F. Li and B. Luo, "Preserving data integrity for smart grid data aggregation," in *2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm)*. IEEE, 2012, pp. 366–371.
[98] F. Diao, F. Zhang, and X. Cheng, "A privacy-preserving smart metering scheme using linkable anonymous credential," *IEEE Transactions on Smart Grid*, vol. 6, no. 1, pp. 461–467, 2014.
[99] E. Vahedi, M. Bayat, M. R. Pakravan, and M. R. Aref, "A secure ecc-based privacy preserving data aggregation scheme for smart grids," *Computer Networks*, vol. 129, pp. 28–36, 2017.
[100] R. Mahmud, R. Kotagiri, and R. Buyya, "Fog computing: A taxonomy, survey and future directions," in *Internet of everything*. Springer, 2018, pp. 103–130.
[101] L. Zhu, M. Li, Z. Zhang, C. Xu, R. Zhang, X. Du, and N. Guizani, "Privacy-preserving authentication and data aggregation for fog-based smart grid," *IEEE Communications Magazine*, vol. 57, no. 6, pp. 80–85, 2019.
[102] X. Liu, Y. Zhang, B. Wang, and H. Wang, "An anonymous data aggregation scheme for smart grid systems," *Security and communication networks*, vol. 7, no. 3, pp. 602–610, 2014.
[103] G. Ohtake, R. Safavi-Naini, and L. F. Zhang, "Outsourcing scheme of abe encryption secure against malicious adversary," *Computers & Security*, vol. 86, pp. 437–452, 2019.
[104] M. Badra and S. Zeadally, "Lightweight and efficient privacy-preserving data aggregation approach for the smart grid," *Ad Hoc Networks*, vol. 64, pp. 32–40, 2017.
[105] L. Chen, R. Lu, and Z. Cao, "Pdaft: A privacy-preserving data aggregation scheme with fault tolerance for smart grid communications," *Peer-to-Peer networking and applications*, vol. 8, no. 6, pp. 1122–1132, 2015.
[106] V. Lozupone, "Analyze encryption and public key infrastructure (pki)," *International Journal of Information Management*, vol. 38, no. 1, pp. 42–44, 2018.
[107] C. Varma, "A study of the ecc, rsa and the diffie-hellman algorithms in network security," in *2018 International Conference on Current Trends towards Converging Technologies (ICCTCT)*, 2018, pp. 1–4.

Lucas Vargas Dias possui o título de Técnico em Informática pelo Instituto Federal de Educação Ciência e Tecnologia Farroupilha (IFFar) (2016), Tecnólogo em Redes de Computadores (2020) e atualmente é mestrando em Engenharia Elétrica na Universidade Federal de Santa Maria (UFSM). Tem interesse em segurança da informação, redes de computadores e redes elétricas inteligentes.



Tiago Antônio Rizzetti possui graduação em ciência da computação (2006), mestrado em computação (2009) e doutorado em engenharia elétrica (2018), pela Universidade Federal de Santa Maria (UFSM). Atualmente é professor adjunto da UFSM, e possui interesse nas áreas de smart grids, segurança cibernética, internet das coisas (IoT) e redes de computadores.