# Instrumentos de Medição Seguros Baseados em Ambientes de Execução Confiáveis

**Eduardo V. A. Martins**[1], **Eduardo G. Machado**[1], **Gustavo de J. Martins**[1], **Wilson de S. Melo Jr.**[1]

[1]Instituto Nacional de Metrologia, Qualidade e Tecnologia (INMETRO)
CEP 25.250-020 – Duque de Caxias – RJ – Brasil

***Abstract.*** *We present an ongoing work that addresses a secure architecture for distributed measurement systems. In this paper, we explain how the sensing phase operates, which involves digital signatures in a trusted execution environment to ensure the authenticity of sensors in these systems. We evaluated the execution time of digital signatures for different key sizes, based on RSA. The time required for key generation and signing was 1 second for 1024 bits, 4 seconds for 2048 bits, and 45 seconds for 4096 bits. The next steps involve using lighter cryptographic algorithms and improving the existing algorithm.*

***Resumo.*** *Apresentamos um trabalho em desenvolvimento que aborda uma arquitetura segura para sistemas distribuídos de medição. Neste artigo demonstramos como funciona a fase de sensoriamento, que envolve assinatura digital em ambiente de execução confiável para promover autenticidade dos sensores desses sistemas. Avaliamos o tempo de execução de assinaturas digitais para diferentes tamanhos de chave, com base em RSA. O tempo para realizar geração de chaves e a assinatura foi de 1 segundo para 1024 bits, 4 segundos para 2048 bits e 45 segundos para 4096 bits. Os próximos passos envolvem a utilização de algoritmos de criptografia mais leves e no aprimoramento do algoritmo já existente.*

## 1. Introdução

Estamos presenciando um avanço tecnológico que revolucionou a maneira como vivemos, trabalhamos e interagimos [Wieczorowski and Trojanowska 2023]. Essa transformação está impulsionando moldando um futuro cada vez mais digital e interconectado. Sistemas distribuídos de medição são um conjunto de dispositivos computacionais que realizam diversos tipos de medições, como temperatura, pressão e consumo de energia, entre outros. Eles integram partes específicas de sensores e são acessíveis por meio de conexões de rede [Carnì et al. 2017]. Esses dispositivos têm a capacidade de coletar e armazenar uma grande quantidade de dados com uma baixa taxa de amostragem e armazenar esses dados na nuvem [Rizzi et al. 2017]. Eles são interconectados, compostos por várias unidades de medição ou processamento, e compartilham informações entre si por meio de uma rede [Lombardo 2022].

No entanto, um dos desafios ao lidar com eles é a dificuldade de garantir a consistência dos dados coletados e manter a segurança desses dados. Existe uma necessidade significativa de cibersegurança para evitar que atacantes possam alterar dados ou substituir sensores autênticos por sensores fraudulentos [Rytel et al. 2020, Snehi and Bhandari 2021], ocasionando distorções em relações comerciais que dependem de medições [Filho and Gonçalves 2016, Jr. et al. 2019]. Uma das soluções que propomos para esse problema é utilizar uma arquitetura que alia as garantias de autenticidade

do TEE com as primitivas de integridade das redes *blockchain* [Martins et al. 2023], por meio de três etapas: Sensoriamento, concretização da medição e armazenamento, como ilustrado na Figura 1.

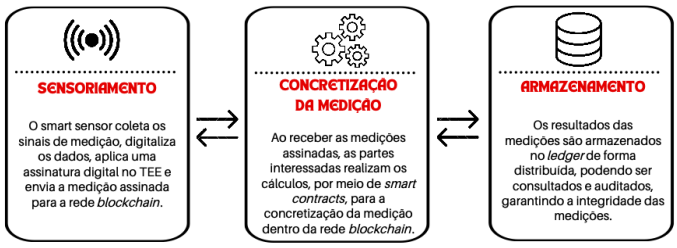


**Figura 1. Arquitetura Segura para Instrumentos Distribuidos de Medição**

A tecnologia TEE serve como um dos pilares para essa arquitetura, pois garante a imutabilidade dos *scripts* inseridos no sistema pelo sensor. O TEE divide o processador em dois ”mundos”sendo um deles o normal baseado em Linux, e um seguro, criptografado e inacessível pelo usuário [Valadares et al. 2021]. Dessa forma, os dados e *scripts* armazenados nele são protegidos de qualquer tentativa de acesso, principalmente por ser um sistema embarcado. Além disso, o usuário pode executar *scripts*, chamados *Trusted Applications*. Essas aplicações são assinadas e criptografadas pelo sistema operacional e possuem um UUID único atrelado a elas, o que permite a execução, mas também protege o código de qualquer leitura ou modificação e garantindo que ela apenas tenha a possibilidade de ser executada [TrustedFirmware 2024]. Por meio disso, o sistema pode assinar os dados recebidos do sensor usando um algoritmo de assinatura de chave pública. Esse passo promove a autenticidade do sensor e do sistema.

Além disso, estamos desenvolvendo a integração entre duas tecnologias, usando um TEE, que manterá todos os *scripts* em um ambiente seguro e inacessível por qualquer pessoa conectada ao dispositivo, juntamente com a rede *blockchain*, responsável pelo aprimoramento da segurança de dados dos DMS. Após os dados receberem a assinatura digital, eles são encaminhados para a rede *blockchain*, onde podem ser processados e auditados pelos membros da rede.

Portanto, destacamos que as principais contribuições do presente trabalho consistem na apresentação da arquitetura segura, com destaque para a fase de sensoriamento, bem como a implementação e os testes realizados nessa etapa. Nas seções subsequentes deste artigo, explicaremos o funcionamento da camada de sensoriamento desenvolvida na arquitetura segura para DMS. No capítulo 2 fazemos uma revisão da literatura com os principais conceitos relacionados ao trabalho, o capítulo 3 explicita os a metodologia e os resultados preliminares obtidos, no capítulo 4 estão evidenciadas nossas conclusões e direcionamentos dos próximos passos.

## 2. Revisão da Literatura

### 2.1. Sistemas de Medição Distribuídos (DMS)

O conceito de DMS ainda não está universalmente definido na literatura e é frequentemente utilizado por diversos autores em diferentes contextos. Com o objetivo de esclarecer isso, são apresentadas aqui as definições contidas em diferentes pesquisas. Em

paralelo, nosso grupo de pesquisa está desenvolvendo um trabalho para harmonizar esse conceito e apresentar uma taxonomia que permita classificar os diferentes medidores distribuídos.

Os DMS podem ser caracterizados formalmente como um conjunto de nós distintos, com capacidades computacionais e de comunicação [Lamonaca et al. 2017]. Os DMS têm aplicações em diversos áreas como a aviação, astrofísica e sistemas de comunicação [Druzhinin and Sokolov 2017, Wiesner and Kovácsházy 2022]. Esses sistemas podem realizar a medição de diferentes grandezas, e de forma cooperativa, obtém o resultado quantitativo que representa essas grandezas [Lombardo 2022]. Alguns trabalhos [Jr. et al. 2019] [Santis et al. 2020] propuseram arquiteturas usando *blockchain* em contextos de DMS e IoT para aprimorar a integridade de medições críticas. Porém nenhum desses trabalhos visa garantir a autenticidade dos sensores dos DMS.

### 2.2. Ambientes de Execução Confiáveis (TEE)

O ambiente de execução confiável (TEE, do inglês Trusted Execution Environment) oferece um espaço no processador que é protegido contra manipulações. Ele opera em um kernel separado, utilizando uma abordagem com dois ambientes de execução: o mundo seguro e o mundo normal [Valadares et al. 2021]. No mundo seguro, as *Trusted Applications* (aplicações confiáveis) são protegidas e executadas sem a interferência ou acesso do mundo normal.

O mundo normal, por sua vez, é onde o sistema operacinal que permite a execução e interação entre *scripts* é executado. O OP-TEE é um sistema operacional de código aberto desenvolvido para fornecer acesso às funções do TEE. Inicialmente, o OP-TEE foi estruturado para ser usado com a tecnologia de hardware Arm TrustZone, mas também pode oferecer um ambiente de execução seguro para qualquer dispositivo compatível com os conceitos do TEE, como máquinas virtuais ou CPUs dedicadas[TrustedFirmware 2024]. Essa tecnologia é amplamente utilizada em dispositivos móveis para proteger informações sensíveis e realizar tarefas críticas, como pagamentos, de maneira isolada do restante do sistema.

## 3. Assinatura de Chave Pública em Ambiente de Execução Confiável

Propusemos uma arquitetura que associa o uso da *blockchain* e dos contratos inteligentes para melhorar a segurança dos dados dos DMS. Ela se baseia em três etapas: Sensoriamento, realização da medição e armazenamento. O TEE é usado para assinar digitalmente e criptografar os dados recebidos pelo DMS e enviados para a rede, garantindo tanto a validade da medição quanto a autenticidade do sensor. Até agora, esse tipo de arquitetura era inexplorado, e nosso objetivo é usar essa tecnologia a nosso favor. Em etapas subsequentes, uma rede *blockchain* realiza o processamento das medições com *smart contracts* e o armazenamento dos resultados de forma distribuída no *ledger*.

A arquitetura proposta aborda tanto a proteção física (hardware seguro) e como a virtual (software) do sistema. O DMS conecta seus elementos de forma inerente, o que permite a conexão com plataformas como a rede *blockchain*. A segurança da informação deve ser uma preocupação em cada um desses estágios, aplicando técnicas protetivas apropriadas.

Os sensores inteligentes realizam a detecção, coletando e digitalizando as medições, que recebem uma assinatura digital no TEE do processador antes de serem enviadas para a rede *blockchain*. As partes interessadas processam esses dados usando contratos inteligentes dentro da nossa rede, que por ser permissionada, garante o acesso de qualquer orgão inspetor que seja acreditado. A escolha de um TEE permite que a autenticidade do sensor seja garantida por meio da assinatura digital dos dados capturados por ele. Além disso, a rede *blockchain* permite a consulta e auditoria das medições, reforçando a transparência e confiabilidade do sistema.

### 3.1. Experimento para realização das assinaturas digitais em TEE

Para validar a arquitetura, realizamos um experimento de assinatura de dados em um ambiente simulado e embarcado. Utilizamos um computador com sistema operacional Linux Ubuntu versão 22.04.4 LTS, processador Intel Core i3-7020U e 12GB de memória RAM, além de um Raspberry Pi 3B+ com processador ARMv8 e um cartão SD Sandisk de 16GB. No computador, instalamos o OP-TEE em um ambiente de simulação com QEMU, juntamente com todos os pré-requisitos necessários. Todos os passos para essa instalação, bem como os scripts desenvolvidos, estão disponíveis em nosso repositório público.[1]

O experimento foi executado com dados de medição reais providos por organismos de medição acreditados. Para que a simulação fosse realizada, utilizamos o OP-TEE em ambiente simulado e em ambiente embarcado, em um Raspberry Pi, para simular um sensor inteligente com hardware real. Em ambos os cenários, os dados foram direcionados ao kernel de execução confiável do processador para a execução de aplicações seguras. Para a assinatura dos dados, utilizamos um *script* de exemplo que está presente nos arquivos do OP-TEE, nomeado *acipher*.

Este script recebe uma string do usuário e um valor em bits, com o máximo de 4096 bits. Esses dados são usados em um *script* de criptografia de chave pública RSA, gerando uma chave com base no valor inserido pelo usuário e assinando os dados que foram recebidos. Após serem assinadas, as medições voltam ao mundo não protegido, onde podem ser conferidas pelo usuário e acessadas por uma aplicação cliente, que é responsável por enviá-la para a rede.

Esse processo assegura a integridade dos dados, já que a assinatura digital garante que qualquer alteração feita neles poderá ser detectada por meio das chaves. Por fim, testamos a eficiência do OP-TEE na realização dessas assinaturas e medimos o tempo necessário para executar o algoritmo com diferentes tamanhos de chaves, determinando se a eficiência dele é aceitável para os dispositivos de medição visados.

Quanto às etapas de concretização e armazenamento da medição foram tratados em outros trabalhos [Martins et al. 2023]. Como o foco deste trabalho é o sensoriamento das medições, estas etapas não serão abordadas.

### 3.2. Resultados preliminares e análise dos resultados

Os testes em ambiente de execução confiável foram realizados usando o OP-TEE no microcomputador Raspberry Pi 3B+. O tamanho mínimo das chaves geradas é de 1024 bits,

[1] https://github.com/edugmac/DMS

por uma característica do algoritmo *acipher*, que está baseado em RSA. O teste consistiu em gerar um par de chaves e assinar uma string padrão similar ao que seria um *hash* de um arquivo de medição. Os tempos de execução para realizar a geração das chaves de diferentes tamanhos e a assinatura digital no Raspberry Pi 3B+ estão apresentados na Figura 2.

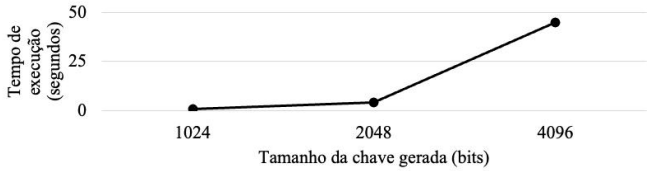


**Figura 2. Tempo da execução da assinatura digital no OP-TEE**

Consideramos que o tempo para realizar as assinaturas de chave pública não gera impacto significativo no processo de medição, principalmente considerando que um hardware dedicado a essa tarefa é capaz de manter resultados próximos aos do Raspberry. Percebemos que houve um aumento significativo no tempo para geração entre as duas chaves de maior tamanho. O presente trabalho ainda está em desenvolvimento e estamos separando o programa em dois *scripts* diferentes: um para gerar o par de chaves e o segundo para realizar as assinaturas digitais. Isso permite que as chaves sejam geradas no processo de fabricação dos sensores e distribuídas pelo fabricante dos sensores, conforme políticas próprias de segurança. Além disso, será possível realizar medições do desempenho da solução de assinaturas sem que seja computado o tempo de geração do par de chaves.

Também buscamos aprimorar o método utilizado tomando algumas ações: realizar mais experimentos visando avaliar a repetibilidade dos resultados apresentados, promover alterações na aplicação confiável, de forma a mostrar no *log* os carimbos de tempo do processador em cada etapa. E ainda planejamos utilizar a criptografia de curvas elípticas para a assinatura das medições, por conta da sua maior velocidade de processamento[Madeira et al. 2021], o que permite melhor execução em DMS que têm limitações de capacidade de processamento e consumo de energia.

## 4. Conclusão

O desenvolvimento atual do trabalho abrangeu a assinatura digital das medições, juntamente com testes na rede *blockchain* para armazenamento de dados e a implementação de contratos inteligentes. Além disso, conduzimos simulações do TEE no QEMU, assim como testes de assinatura dentro do mundo seguro. Também, instalamos o sistema operacional do TEE em um Raspberry Pi, que será responsável por capturar os dados de medição recebidos pelos sensores.

Buscamos implementar em trabalhos futuros aprimorar o algoritmo existente e gerar um algoritmo para que os dados recebam uma assinatura digital única desse sensor, baseado em um algoritmo de Curva Elíptica. O algoritmo de curva elíptica possui um desempenho consideravelmente superior ao RSA, portanto pode ser uma melhor escolha para a nossa abordagem.

## 5. Agradecimentos

Este trabalho foi parcialmente apoiado pelo CNPq, bolsa 151399/2023-9, e FAPERJ, bolsas E- 26/290.124/2021, E-26/205.266/2022, e E-26/260.179/2023

## Referências

Carnì, D., Grimaldi, D., Sciammarella, P. F., Lamonaca, F., and Martirano, L. (2017). *Towards a unified approach for Distributed Measurement System Technologies*. IEEE.

Druzhinin, Y. and Sokolov, V. (2017). Features of data collection at strict schedule in distributed measurement system with ring structure. In *2017 Tenth International Conference Management of Large-Scale System Development (MLSD)*, pages 1–5.

Filho, B. A. R. and Gonçalves, R. F. (2016). Measuring the economic impact of metrological frauds in trade metrology using an input-output model. *IFIP Advances in Information and Communication Technology*, pages 624–632.

Jr., W. S. M., Bessani, A., Neves, N., Santin, A. O., and Carmo, L. F. C. (2019). Using blockchains to implement distributed measuring systems. *IEEE Transactions on Instrumentation and Measurement*, 68:1503–1514.

Lamonaca, F., Carnì, D., Grimaldi, D., and Sciammarella, P. F. (2017). Mobile object to speed up the synchronization of iot network. pages 1–6.

Lombardo, L. (2022). Distributed measurement systems: Advantages and challenges of wireless sensor networks. *IEEE Instrumentation  Measurement Magazine*, 25:21–28.

Madeira, F. L., Canedo, E. D., Gondim, J. J. C., Caetano, M. F., and Veneziano, W. H. (2021). Aplicação prática de criptografia de curvas elípticas (ecc). *Instituto de Ciências Exatas Departamento de Ciência da Computação*, pages 1–59.

Martins, E. V. A., Machado, E. G., Gomes, R. T. B., and Melo, W. S. (2023). Blockchain-based architecture to enhance security in distributed measurement systems. pages 1–4.

Rizzi, M., Ferrari, P., Flammini, A., and Sisinni, E. (2017). Evaluation of the iot lorawan solution for distributed measurement applications. *IEEE Transactions on Instrumentation and Measurement*, 66:3340–3349.

Rytel, M., Felkner, A., and Janiszewski, M. (2020). Towards a safer internet of things—a survey of iot vulnerability data sources. *Sensors (Switzerland)*, 20:1–26.

Santis, L. D., Paciello, V., and Pietrosanto, A. (2020). Blockchain-based infrastructure to enable trust in iot environment. *I2MTC 2020 - International Instrumentation and Measurement Technology Conference, Proceedings*, pages 1–6.

Snehi, M. and Bhandari, A. (2021). Vulnerability retrospection of security solutions for software-defined cyber-physical system against ddos and iot-ddos attacks.

TrustedFirmware (2024). Op-tee documentation.

Valadares, D. C. G., Will, N. C., Caminha, J., Perkusich, M. B., Perkusich, A., and Gorgonio, K. C. (2021). Systematic literature review on the use of trusted execution environments to protect cloud/fog-based internet of things applications. *IEEE Access*, 9:80953–80969.

Wieczorowski, M. and Trojanowska, J. (2023). Towards metrology 4.0 in dimensional measurements. *Journal of Machine Engineering*, 23.

Wiesner, A. and Kovácsházy, T. (2022). Distributed measurement system for performance evaluation of embedded clock synchronization solutions. In *2022 23rd International Carpathian Control Conference (ICCC)*, pages 293–298.