

MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
DEPARTAMENTO DE CIÊNCIA E TECNOLOGIA
INSTITUTO MILITAR DE ENGENHARIA
CURSO DE MESTRADO EM SISTEMAS E COMPUTAÇÃO

PROPOSTA DE DISSERTAÇÃO DE MESTRADO

GABRIELA MENDES CORRÊA DE MIRANDA

ABORDAGEM MULTICRITÉRIO PARA AVALIAÇÃO E
SELEÇÃO DE ALGORITMOS CRIPTOGRÁFICOS
SIMÉTRICOS LEVES

Rio de Janeiro
2024

1 TÍTULO DA PROPOSTA DE DISSERTAÇÃO

Título da Proposta de Dissertação:

Abordagem Multicritério para Avaliação e Seleção de Algoritmos Criptográficos
Simétricos Leves

Área de Concentração:

Ciência da Computação

Linha de Pesquisa:

Sistemas de Computação

2 INTRODUÇÃO

Internet das Coisas (IoT) refere-se a uma rede em expansão de objetos físicos cotidianos que estão conectados à Internet (HARBI et al., 2021). Um dos objetivos principais da IoT é permitir que dispositivos habilitados para Internet, em um ecossistema interconectado, possibilitem que dados digitais estejam acessíveis em qualquer lugar e a qualquer momento. Os sistemas de IoT oferecem uma gama diversificada de serviços, incluindo sistemas de transportes, redes, cidades inteligentes e sistemas de monitoramento de saúde (KHANNA; KAUR, 2020). Sistemas de Controle Industrial (ICS), como os utilizados em usinas nucleares, também encontram-se sob o guarda-chuva da IoT e, por sua natureza crítica, tais infraestruturas estão sujeitas a medidas de defesa substanciais e mecanismos complexos de segurança (MOMENI et al., 2023). Com o advento da Internet das Coisas Militares (IoMT) ou Internet das Coisas do Campo de Batalha (IoBT), um número crescente de dispositivos de detecção e computação são usados e incorporados em equipamentos passando a coletar uma variedade de dados biométricos como impressões digitais e frequência cardíaca, assim como dados de contexto operacional e geolocalização.

Quando bilhões de dispositivos inteligentes, operando em diversas plataformas, estão conectados à Internet, eles introduzem novos riscos e desafios de segurança como autorização e autenticação destes dispositivos, garantia de privacidade e integridade dos dados, e detecção e gerenciamento de vulnerabilidades (SEVIN; MOHAMMED, 2023). Dispositivos IoT são facilmente acessíveis e expostos a muitos ataques de segurança, pois interagem diretamente com o mundo físico para coletar dados confidenciais ou controlar variáveis do ambiente (SINGH et al., 2017). Aplicar mecanismos de segurança em um sistema de IoT é mais desafiador do que em uma rede tradicional devido à heterogeneidade dos dispositivos e protocolos, restrições de recursos, privacidade e sua grande escala (BINTI MOHAMAD NOOR; HASSAN, 2019). Ao se considerar as limitações e especificidades desse ambiente, combinando práticas tradicionais de proteção com novos paradigmas, soluções mais leves são sugeridas a fim de garantir a segurança e a eficiência energética, sem comprometer o desempenho.

Soluções criptográficas são consideradas uma solução de segurança importante para proteção de dados garantindo a confidencialidade e integridade tanto de dados em trânsito quanto de dados armazenados, podendo também realizar a autenticação de remetentes, de destinatários e de uns aos outros para proteção contra repúdio, garantindo assim a

irretratibilidade (WILLIAMS et al., 2022). Dispositivos IoT comerciais e industriais são vulneráveis a ataques específicos de IoT e, ainda que existam numerosas ferramentas criptográficas disponíveis, nem todas são adequadas para estes ambientes (DUTTA et al., 2019). Comunicações seguras por meio de redes sem fio, vulneráveis a espionagem e outros tipos de ataque, são uma das principais questões que devem ser abordadas no projeto de sistemas habilitados para IoT, especialmente, para aplicações militares (KANNAN et al., 2023).

A maioria dos dispositivos de IoT são pequenos e com recursos limitados como pouca memória para armazenar e executar aplicativos, baixo poder de computação para processar os dados e pouca ou nenhuma bateria (THAKOR et al., 2021). Algoritmos criptográficos clássicos tendem a utilizar muitos recursos durante sua implementação em dispositivos IoT, tornando o processamento mais custoso. Diante disso, a utilização de algoritmos leves, que garantam recursos criptográficos seguros e que reduzam a sobrecarga na utilização de recursos, tem se tornando cada vez mais significativa (RADHAKRISHNAN et al., 2024).

A criptografia leve (do inglês, *Lightweight Cryptography*) é uma abordagem criptográfica que lida com algoritmos especialmente projetados para uso em ambientes restritos, o que inclui etiquetas RFID, cartões inteligentes, sistemas embarcados, dispositivos de saúde, redes de sensores, drones, veículos militares autônomos e assim por diante (BLANC et al., 2022). Esses algoritmos são caracterizados pelo fato de que o tamanho do bloco, o tamanho da chave, o poder computacional dos microprocessadores ou microcontroladores, o consumo de memória e o consumo de energia foram significativamente reduzidos (SEVIN; MOHAMMED, 2023). Tais primitivas têm mostrado um desempenho superior em ambientes restritos quando comparadas aos algoritmos convencionais, mesmo com suas limitações inerentes.

2.1 CARACTERIZAÇÃO DO PROBLEMA

Em um ambiente com recursos limitados, não é possível maximizar simultaneamente o desempenho e a segurança. Melhorar a segurança geralmente implica aumentar o uso de recursos, o que pode não ser viável em dispositivos restritos. Por outro lado, otimizar o desempenho pode exigir a redução da complexidade do algoritmo, o que pode comprometer sua segurança. Maximizar um dos aspectos geralmente implica sacrificar o outro e é necessário encontrar um equilíbrio que atenda às necessidades específicas da aplicação.

Implementações de algoritmos criptográficos leves não são idênticas porque a com-

plexidade das operações das cifras são diferentes em plataformas de *software* e *hardware* (KERCKHOF et al., 2012) e as métricas que avaliam o desempenho e a segurança variam amplamente. Devido a essa condição comparações justas entre diferentes algoritmos torna-se uma tarefa complexa. Em cenários que exigem máxima segurança, pode ser necessário sacrificar algum desempenho para garantir maior proteção. Em cenários com dispositivos de requisitos de baixa energia e processamento, a eficiência e o tempo de resposta geralmente são priorizados, mas isso pode deixar os sistemas vulneráveis a ataques mais sofisticados (SONG et al., 2017).

Diante do contínuo avanço na pesquisa de soluções criptográficas leves uma gama de algoritmos foi desenvolvida, surgindo o desafio de se avaliar corretamente um algoritmo criptográfico adequado para proteção dos dados e dos dispositivos IoT. Ao selecionar um algoritmo criptográfico leve é importante avaliar cuidadosamente critérios essenciais que garantam que o algoritmo apropriado se alinhe com as necessidades e restrições específicas dos dispositivos e dos cenários em que serão utilizados. Considerações a serem feitas ao se avaliar o algoritmo leve ideal para aplicações IoT incluem:

- Considerações de segurança e requisitos necessários de cada cenário; e
- Avaliação de desempenho, levando-se em conta fatores como complexidade computacional, uso de memória, consumo de energia, segurança e requisitos de interoperabilidade.

Selecionar o melhor algoritmo criptográfico é crucial uma vez que impacta a segurança, eficiência e confiabilidade dos sistemas criptográficos, dependendo de um equilíbrio entre a eficiência dos recursos, a complexidade, requisitos da aplicação e o nível de segurança pretendido.

2.2 TRABALHOS RELACIONADOS

Os principais trabalhos relacionados ao tema de avaliação e seleção de algoritmos criptográficos leves realizam uma análise de desempenho das cifras com base no consumo de energia e memória, taxa de transferência e tempo de execução, com tamanhos variados de chaves e de comprimento de mensagem (PANAHI; BAYILMIŞ, 2023), (WENG, 2023) e (RAHUL et al., 2024). Esses estudos apresentam ideias inovadoras para melhoria de desempenho, porém utilizam parâmetros simples e de maneira isolada para a avaliação, tornando desafiador verificar se as métricas utilizadas relacionam-se umas com as outras.

Estudos como os realizados por (MOHD et al., 2015), (HATZIVASILIS et al., 2018) e (SEVIN; MOHAMMED, 2023) medem os parâmetros de desempenho avaliando implementações em *hardware* e implementações em *software*. As implementações em *hardware* e *software* possuem características diferentes e que tornam uma comparação direta difícil, assim sendo, os trabalhos apresentados possuem resultados alcançados por meio de avaliações isoladas levando-se em conta somente uma das arquiteturas.

A análise apresentada em (QASAIMEH et al., 2018) fornece avaliações de desempenho e consumo de energia fornecendo ainda uma investigação da aleatoriedade de textos cifrados baseado em métricas do conjunto de testes estatísticos do *National Institute of Standards and Technology* (NIST) para aplicações criptográficas. A introdução de aleatoriedade no processo de cifragem aumenta a segurança, principalmente ao evitar que padrões previsíveis possam ser explorados, ainda assim, embora a aleatoriedade seja um fator essencial para tornar os sistemas criptográficos mais robustos, não deve ser o único aspecto a ser considerado. O referido trabalho não avalia, por exemplo, as possíveis restrições impostas em determinados cenários de aplicação das cifras leves.

Alguns trabalhos como os realizados por (BLANC et al., 2022), (SREEHARI et al., 2023) e (RADHAKRISHNAN et al., 2024) analisam o desempenho e a eficiência de diferentes algoritmos criptográficos leves por meio do benchmarking e envolvem a medição de métricas como tempo de execução, uso de memória e consumo de energia de diferentes algoritmos. Novamente, uma avaliação da relevância das métricas que afetam tanto o desempenho quanto a segurança e o modo que elas se inter-relacionam não é elaborada.

(NING et al., 2020) e (DAMAJ et al., 2023), realizam a avaliação de cifras leves adequadas a ambientes como o de Internet das Coisas da Saúde (do inglês, *Internet of Health Things* - IoHT) com base em múltiplos critérios (do inglês, *Multi-Criteria Decision Making* - MCDM). Métodos MCDM permitem a integração de critérios qualitativos e quantitativos e que levem em conta a complexidade das decisões. Esses estudos são complementares e contribuem significativamente na avaliação dos algoritmos leves, porém apresentam algumas limitações como a ausência de métricas robustas de segurança e a falta de critérios específicos de acordo com os diferentes cenários IoT e que levem em consideração suas particularidades.

A oportunidade de melhoria nos referidos trabalhos permite a expansão do escopo e a aplicabilidade dos estudos, através de uma análise mais completa e precisa para o uso de algoritmos criptográficos leves em diferentes ambientes de IoT que considere métricas mais robustas e os seus cenários de aplicações.

2.3 OBJETIVO

O problema na escolha de uma cifra leve apropriada para uma aplicação específica é difícil de ser completamente caracterizado por métricas simples como taxa de transferência, tamanho da chave e latência. Tal abordagem pode falhar em exibir as implicações existentes entre indicadores e a maioria das pesquisas sobre cifras leves se concentra em um subconjunto de métricas de classificação simples, onde nem sempre os cenários e o balanceamento entre desempenho e segurança são considerados.

Medidas, métricas e indicadores estão no cerne de qualquer avaliação. Indicadores são variáveis, fatores qualitativos ou quantitativos que podem fornecer uma maneira adequada de medir o sucesso (DAMAJ et al., 2023). Um indicador qualitativo é um recurso descritivo que reflete uma perspectiva, um valor ou uma característica específica. Em contraste, um indicador quantitativo é uma medição numérica obtida por meio de contagem, soma, média ou outros cálculos matemáticos. Nesse contexto, há uma ausência de pesquisa realizada sobre o estabelecimento de estruturas analíticas que classifiquem algoritmos criptográficos leves com base em suas características heterogêneas, quantitativa e qualitativamente, e que levem em consideração o cenário de aplicação da solução criptográfica.

Diante disso temos como objetivo o desenvolvimento de uma metodologia de avaliação multidimensional da segurança, desempenho e eficiência energética, que integre indicadores qualitativos e quantitativos, para auxiliar na seleção de cifras leves.

2.4 JUSTIFICATIVA

De acordo com a Política Nacional de Defesa (BRASIL, 2020), o setor cibernético é estratégico para a Defesa do País devendo, portanto, ser fortalecido. Para se opor a possíveis ataques cibernéticos, é essencial aperfeiçoar os dispositivos de segurança e adotar procedimentos que minimizem a vulnerabilidade dos sistemas que possuem suporte de tecnologia da informação e comunicação.

No setor cibernético, o Ministério da Defesa e o Ministério da Ciência Tecnologia e Inovação, por intermédio do Departamento de Ciência e Tecnologia do Exército, são responsáveis por promover ações que contemplem a proteção das infraestruturas estratégicas, com ênfase para o desenvolvimento de soluções nacionais inovadoras, dentre elas, aquelas relacionadas a algoritmos criptográficos e de autenticação próprios.

Documentos norteadores, como o Plano Estratégico do Exército (BRASIL, 2023), preveem o aprimoramento da atuação no espaço cibernético através do incremento da capaci-

dade cibernética de defesa e de cooperação para a proteção de infraestruturas estratégicas críticas. Tais objetivos devem ser alcançados por meio de projetos e desenvolvimento de soluções para obtenção de independência tecnológica, multiplicando o poder de combate nos níveis de atuação da defesa e da guerra cibernética.

Dispositivos IoT vêm sendo empregados em operações militares, desde drones até sistemas de comunicação e sensores. Algumas das aplicações podem ser vistas na Figura 2.1. Desse modo, surgem novas possibilidades para a coleta de informações e a execução de ações remotas, ampliando também a superfície de ataque para os adversários. A chamada Internet das Coisas Militares (IoMT) ou Internet das Coisas de Campo de Batalha (IoBT), passa a ser um componente crítico das estratégias militares, com ações focadas na proteção de infraestruturas, na coleta de dados de contexto operacional e no monitoramento e ataque a sistemas adversários.

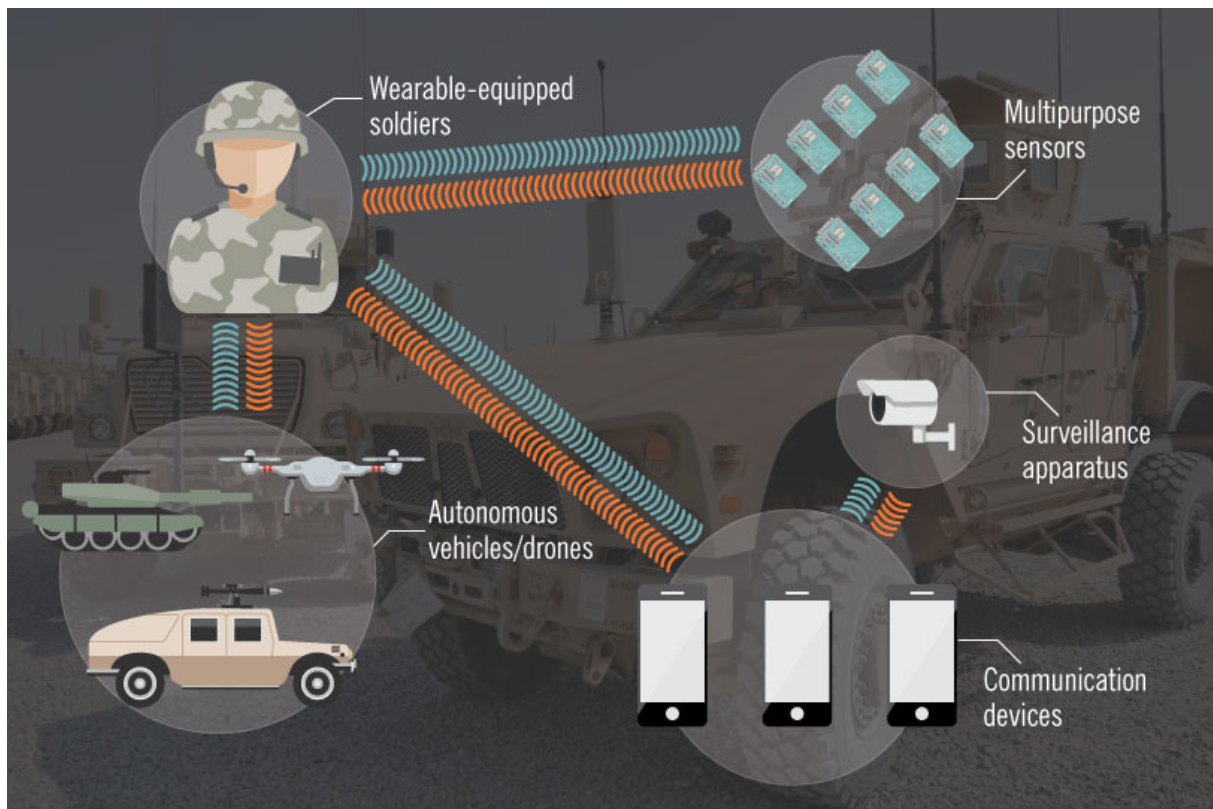


FIG. 2.1: Aplicações Internet das Coisas Militares. Fonte: Página do LinkedIn¹

A utilização de sistemas IoT em aplicações militares permitiu uma melhor consciência situacional e a identificação de potenciais ameaças, passando também a ser utilizada em exercícios de treinamento e simulação. No entanto, é essencial que a comunicação entre esses sistemas seja protegida contra acessos e intervenções ilegais. Existem limitações

<https://www.linkedin.com/pulse/internet-battlefield-things-cian-o-flaherty/>

técnicas que precisam ser superadas para a aplicação da IoT em um ambiente militar: infraestruturas descentralizadas para análise de dados, interoperabilidade, utilização de sensores e dispositivos, confiança e segurança são alguns desses entraves (SURI et al., 2016). A pesquisa nessa área se concentra em proteger as comunicações, garantir a integridade, confidencialidade e disponibilidade dos dados, e desenvolver estratégias para proteção contra ataques.

Utilizar métodos criptográficos para proteger a confidencialidade e a integridade de dados e operações é o princípio fundamental por trás da comunicação segura em sistemas embarcados habilitados para IoT e projetados para aplicações militares (KANNAN et al., 2023). Escolher uma solução criptográfica que seja ao mesmo tempo leve e segura é essencial para garantir um equilíbrio entre desempenho, segurança e viabilidade econômica, especialmente em contextos onde os recursos são limitados e os dados sensíveis.

Diante do contexto apresentado, justifica-se a necessidade de pesquisa de métodos de avaliação de segurança, desempenho e eficiência energética dos algoritmos criptográficos leves, candidatos a serem utilizados em ambientes de recursos limitados, como os de campos de batalha. Selecionar o algoritmo criptográfico ideal, em que pese os critérios da aplicação e dos cenários de utilização, busca prover soluções robustas e seguras impulsionando assim as estratégias cibernéticas de defesa nacional.

2.5 ESTRUTURA DO TEXTO

O texto é estruturado em cinco capítulos. O Capítulo 3 apresenta a Fundamentação Teórica, onde conceitos importantes são definidos. No capítulo 4 a proposta é apresentada através da questão de pesquisa, objetivos, hipótese e contribuições esperadas. Por último, o Capítulo 5 dispõe sobre o plano de ação, metodologia e cronograma da proposta de dissertação.

3 FUNDAMENTAÇÃO TEÓRICA

3.1 SEGURANÇA PARA DISPOSITIVOS COM RECURSOS LIMITADOS

A segurança visa preservar, restaurar e garantir a proteção das informações nos sistemas computacionais contra ataques e ameaças maliciosas (KOUICEM et al., 2018). Garantir um nível adequado de segurança dos dados em aplicações com recursos limitados é crítico e apresenta diversos desafios como a sobrecarga de implementação, o consumo de energia e o desempenho da segurança (Fan et al., 2013).

Estimativas indicam que até 75 bilhões de dispositivos estarão conectados até 2030 (PLOENNIGS et al., 2018). Ainda de acordo com essa previsão, a IoT oferecerá receita econômica de US\$ 11 trilhões por ano até 2025 e, como resultado, esse crescimento já provoca problemas de segurança que exigem atenção. Vulnerabilidades e heterogeneidade das tecnologias de comunicação, sensibilidade e privacidade dos dados, limitações de recursos, mobilidade, falta de normatização e segurança são alguns dos desafios.

Diferentes tecnologias como a computação em nuvem, redes de comunicação sem fio e a inteligência artificial evoluem como componentes facilitadores para a evolução do paradigma da IoT (HASSIJA et al., 2019), conforme mostrado na Figura 3.1. Essas tecnologias facilitam a interconexão, o processamento de dados e a automação de sistemas, criando uma infraestrutura robusta e eficiente para os dispositivos IoT.

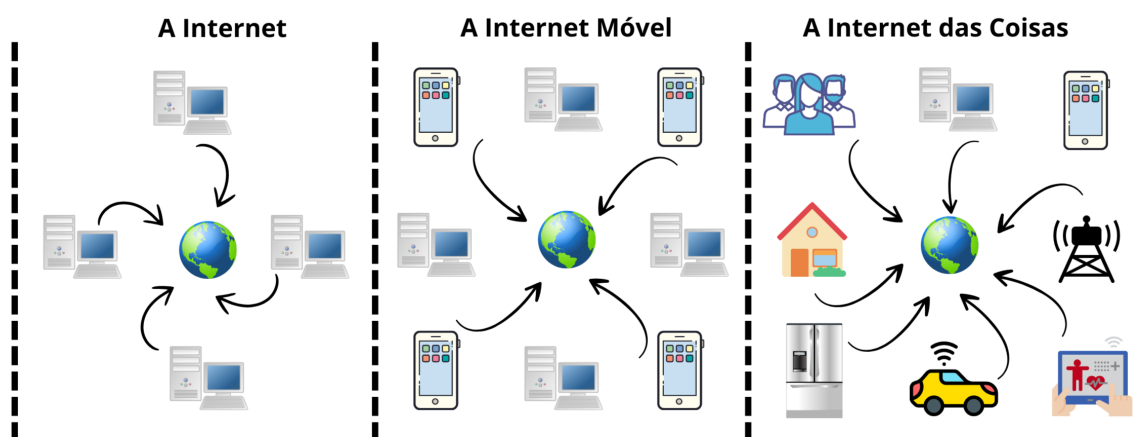


FIG. 3.1: Evolução da Internet.

Aplicações IoT operam em ambientes altamente distribuídos com o uso de objetos, sensores e atuadores inteligentes heterogêneos e que são limitados. Uma grande parcela

TAB. 3.1: Abordagens Leves para Segurança em Ambientes Restritos

Técnica	Aplicações de Segurança
<i>Fog Computing</i>	Processamento de dados locais, detecção de intrusão, controle de acesso
Aprendizado de Máquina	Detecção de anomalias, previsão de ameaças, identificação de <i>malware</i>
Blockchain	Controle de acesso distribuído, registro de <i>logs</i> imutáveis, contratos inteligentes
Radio Definido por Software	Mitigação de ataques em tempo real, segmentação de rede, políticas de segurança centralizadas
Criptografia Leve	Algoritmos de criptografia, técnicas de autenticação e funções de <i>hash</i>

dos dispositivos são vulneráveis a ataques de segurança devido aos seus recursos limitados e à falta de métodos de proteção. Por exemplo, ataques de negação de serviço e ataques de repetição levam ao esgotamento da bateria do sensor, resultando em baixo desempenho das aplicações de detecção. Em casos mais graves, o vazamento de informações desses dispositivos pode inclusive expor dados confidenciais para fora da rede (HASSIJA et al., 2019).

Para mitigar os riscos de segurança em dispositivos com recursos limitados, diversas abordagens foram desenvolvidas, adaptando as técnicas tradicionais de segurança para um contexto mais restrito. Soluções baseadas em *Fog Computing*, em Aprendizado de Máquina, em *Blockchain*, em Rede Definida por *Software* e em Criptografia Leve oferecem proteção avançada com o uso eficiente de recursos, ajudando a garantir a segurança em ambientes de IoT e sistemas embarcados, como mostrado na tabela 3.1. Soluções baseadas em Criptografia Leve tornaram-se fundamentais pois foram especificamente projetadas para proporcionar segurança suficiente com baixo consumo de energia, processamento e uso de memória e incluem algoritmos de criptografia, técnicas de autenticação e *hashes*.

3.2 CRIPTOGRAFIA LEVE

Criptografia leve é um grupo de primitivas, métodos e cifras criptográficas destinadas a fornecer soluções para dispositivos com recursos limitados, como IoT e tecnologia RFID (PATEL; MISTRY, 2015). Algoritmos criptográficos leves têm sido utilizados em muitas aplicações para garantia da segurança, privacidade e integridade de dados e são escolhidos por fornecerem baixo consumo de energia, processamento, capacidade de armazenamento

e uso de memória (SEVIN; MOHAMMED, 2023).

Esses algoritmos possuem características específicas que os tornam ideais para ambientes com restrições. Dentre as principais, compreende-se tamanhos reduzidos de chave e de blocos, economia de energia e memória, resistência a ataques específicos ao ambiente das aplicações (A.MOHAMMED; HUSSEIN, 2023). As primitivas criptográficas leves incluem cifras de bloco, cifras de fluxo, funções *hash*, e cifras autenticadas.

Cifras de bloco leves criptografam blocos de dados fixos, geralmente de 64 ou 128 bits, usando operações que foram simplificadas para menor consumo de recursos. Cifras de fluxo geram um fluxo contínuo de bits que são combinados com os dados para criptografá-los, sendo adequadas para transmissão de dados em tempo real. Funções *hash* leves garantem a integridade e autenticidade dos dados com baixo consumo de recursos, sendo ideais para verificar integridade de mensagens ou dados em dispositivos leves. As cifras autenticadas leves combinam criptografia e autenticação em uma única operação, garantindo tanto a confidencialidade quanto a integridade dos dados transmitidos.

Pesquisadores de criptografia leve têm explorado algoritmos criptográficos assimétricos, porém os resultados mostram-se não tão estáveis e promissores quanto os dos algoritmos criptográficos simétricos, como os que utilizam cifras de bloco ou de fluxo (THAKOR et al., 2020). Algoritmos criptográficos assimétricos leves são complexos em termos de operação e, como resultado, geralmente são menos eficientes em termos de área e/ou energia mesmo em versões otimizadas (LARA-NINO et al., 2018).

As primitivas têm apresentado desempenho superior em relação aos algoritmos convencionais quanto utilizadas em ambientes com restrições de recursos. Tal comportamento é razoável por algumas razões (GANIEV; KHUDOYKULOV, 2021):

- **Simplicidade das Operações:** Primitivas leves utilizam operações matemáticas mais simples, como XORs, rotações e deslocamentos, em vez de multiplicações complexas ou tabelas de substituição (S-Boxes) extensas;
- **Design Minimalista:** Ao contrário de algoritmos convencionais, que são projetados para rodar em uma ampla gama de sistemas, as primitivas leves são otimizadas para atender a um nível de segurança adequado em um ambiente específico;
- **Eficiência Energética:** As primitivas criptográficas leves foram desenvolvidas com foco na economia de energia, um fator crucial para dispositivos IoT e sistemas embarcados que dependem de baterias;

TAB. 3.2: Características dos Algoritmos Criptográficos Leves

Características		Algoritmos Leves
Físicas	Área	Tamanho de Bloco menor
	Memória	Tamanho de Chave menor
	Bateria/Energia	Rodadas simples
Desempenho	Poder de Computação	Geração de Chave simples
Segurança	Força de Segurança	Estrutura Forte
	Modelos de Ataque	
	Ataque de Canal Lateral	

- **Menor Uso de Memória:** Algoritmos convencionais geralmente requerem tabelas de substituição grandes e operações complexas, que ocupam muita memória. Primitivas leves são projetadas para ocupar o mínimo de espaço; e
- **Adequação para Hardware Específico:** Primitivas leves são frequentemente ajustadas para hardware específico, aproveitando as características da arquitetura do dispositivo, podendo garantir eficiência máxima.

Apesar de suas limitações em relação à robustez de segurança em comparação com algoritmos mais complexos, as primitivas criptográficas leves encontram um equilíbrio que permite desempenho superior em dispositivos com recursos limitados. Esses algoritmos leves precisam atender aos padrões de desempenho e eficiência energética, ao mesmo tempo em que oferecem um desempenho semelhante de segurança (THAKOR et al., 2021). As principais características dos algoritmos de criptografia leves e suas contribuições estão listadas na tabela 3.2.

3.3 MÉTRICAS

A criptografia leve apresenta um objetivo importante que é aumentar a segurança para dispositivos com restrições de recursos, respeitando ao máximo suas limitações. Para isso, três características principais devem ser levadas em consideração. De acordo com (THAKOR et al., 2021) um projeto de cifra criptográfica leve deve respeitar a tríade CPS (do inglês, *Cost, Performance and Security*) onde cada um desses componentes precisa ser considerado, como mostrado na Figura 3.2.

Um algoritmo pode usar chaves criptográficas menores a fim de melhorar o desempenho e reduzir o custo, mas tal escolha pode comprometer a segurança tornando-o vulne-

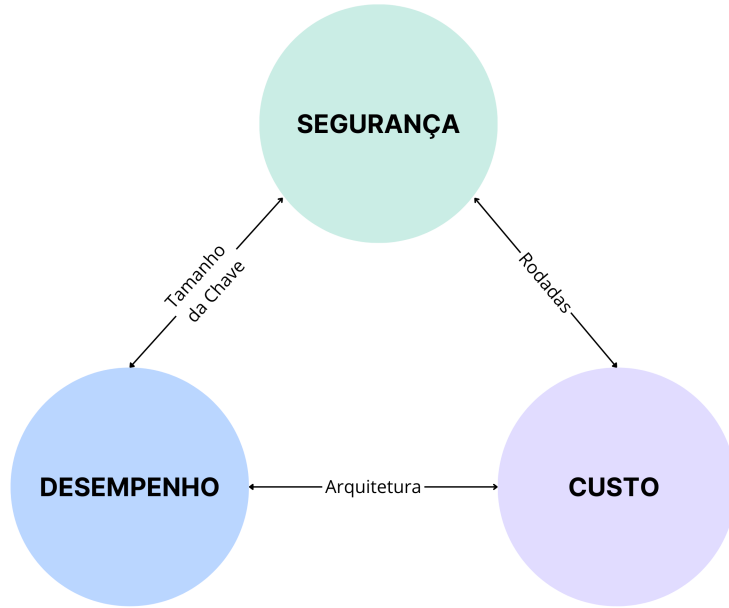


FIG. 3.2: Tríade Custo, Desempenho e Segurança.

rável a ataques de força bruta (EL GAABOURI et al., 2022). Algoritmos com estruturas mais complexas podem oferecer melhor segurança, mas a um custo elevado em termos de tempo de execução e uso de memória.

Alguns autores (SARAIVA et al., 2019) apresentam parâmetros que podem ser usados na comparação de diferentes cifras leves. Segurança, área do chip, latência, taxa de transferência, tecnologia CMOS (do inglês, *Complementary Metal Oxide Semiconductor*) são algumas das métricas discutidas. Outras métricas propostas, como FoM (do inglês, *Figure of Merit*) e consumo de energia/potência, também são empregadas para equilibrar segurança, eficiência computacional, e consumo de recursos (HATZIVASILIS et al., 2018).

As métricas para implementações de *software* e *hardware* de algoritmos criptográficos leves não são idênticas uma vez que a complexidade da implementação de operações de cifras é diferente em cada uma das plataformas (KERCKHOF et al., 2012). Enquanto que, em *software*, a complexidade está relacionada ao uso de memória e ciclos de processamento, tornando o desempenho dependente da arquitetura do processador e das otimizações no código, em *hardware* a complexidade é determinada pela quantidade de portas lógicas e a estrutura física necessária para realizar as operações, influenciando diretamente a eficiência energética e a latência (SALLAM; BEHESHTI, 2018).

Em contraste com os algoritmos clássicos, a criptografia leve difere ao assumir que primitivas leves não são projetados para uso em uma ampla variedade de aplicações e que não há necessidade de criptografar um grande número de dados. Para esses ambi-

TAB. 3.3: Métricas de desempenho de implementação de software.

Métrica	Definição
Consumo de memória	A quantidade de dados gravados na memória durante cada avaliação da função
Tamanho do código	A quantidade fixa de dados necessária para avaliar a função de forma independente
Taxa de transferência	Quantidade média de dados que são processados durante cada ciclo de clock
Ciclos/byte	Contagem de ciclos de criptografia e descriptografia, um bloco ciclos/byte
Energia consumida	Dado em μJ
Latência	O tempo necessário para o cálculo de um bloco de texto simples ou cifrado
Eficiência	Exigindo pouco armazenamento e consumindo pouca energia
Potência	Tempo de processamento x Potência média do dispositivo
Métrica combinada (CM)	Balanceamento entre tamanho da implementação e desempenho (tamanho do código x ciclo)
ST/A	(Segurança x Taxa de transferência) / Área

entes, implementações leves podem proporcionar um melhor equilíbrio entre segurança, desempenho e eficiência energética. A criptografia leve não deve ser associada a uma criptografia fraca e, para contextos criptográficos clássicos, continuam a ser recomendadas abordagens convencionais para garantir a segurança dos dados (FARHAN; KHAREL, 2018). As métricas que avaliam a segurança e as implementações de *hardware* e *software* variam amplamente e, devido a essa condição, comparações justas das diferentes implementações dos algoritmos são uma questão difícil.

Em geral, nenhum dos algoritmos leves atende a todos os critérios das métricas de segurança e de desempenho de *hardware* e *software*. Uma métrica leve e bem definida de custo e desempenho pode verificar a eficiência de uma cifra leve ou avaliar ainda sua segurança para uma determinada aplicação (RANA et al., 2024).

3.3.1 MÉTRICAS DE SEGURANÇA

Analisar a segurança de algoritmos criptográficos envolve diversas métricas e critérios que buscam garantir sua robustez contra ataques. A segurança depende da arquitetura do

TAB. 3.4: Métricas de desempenho de implementação de hardware.

Métrica	Definição
Área	A área ocupada pelo chip é medida em GE (<i>Gate Equivalents</i>)
Área/bit	O custo de área para um único bit
Taxa de transferência	Quantidade média de dados que são processados durante cada ciclo de clock
Eficiência	A proporção da taxa de transferência calculada em uma frequência de clock fixa sobre a área
FoM	$\text{FoM} = \text{Taxa de transferência} / GE^2$
FoAM	Combina a segurança fornecida por estruturas e componentes criptográficos com suas propriedades de implementação
Potência	Indica a taxa de consumo de energia. A potência depende da frequência de <i>clock</i> , medida em <i>Watts</i>
Energia por bit	Normaliza a energia em relação ao número de <i>bits</i> em um bloco da cifra
Energia x Área/Bits	Combina as duas restrições em uma expressão

algoritmo e de características como o processo de geração de chaves, comprimento da chave, tamanho do bloco e número de rodadas usadas para o processo de criptografia e descryptografia (HERCIGONJA, 2016). Esses fatores aumentam a complexidade do algoritmo dificultando ataques de força bruta, de criptoanálise diferencial ou linear, e a exploração de padrões estatísticos.

Outras propriedades fundamentais que fortalecem a segurança criptográfica estão relacionadas à entropia, à aleatoriedade e à avaliação do efeito avalanche (SANAP; MORE, 2021), que são propriedades intrínsecas do design matemático dos algoritmos. Entropia é um conceito originado na termodinâmica e amplamente aplicado em diversas áreas do conhecimento e mede o nível de desordem ou incerteza em um sistema (ZOLFAGHARI et al., 2022). (SHANNON; WEAVER, 1949) adaptou o conceito para medir a incerteza em processos de comunicação. Na criptografia, o conceito é usado para avaliar a segurança de sistemas criptográficos medindo o grau de aleatoriedade e imprevisibilidade das chaves criptográficas. Um algoritmo com alto efeito avalanche distribui a entropia uniformemente na saída, garantindo que cada bit tenha uma distribuição uniforme e independência estatística, dificultando ataques.

A conformidade com padrões reconhecidos e testes independentes realizados por especialistas possibilitam que os algoritmos sejam amplamente auditados, conferindo maior

segurança e credibilidade. Tais propriedades, quando combinadas, oferecem uma análise mais abrangente sobre a segurança e a adequação do algoritmo.

Para a avaliação da segurança de algoritmos criptográficos leves métricas específicas visam garantir que eles sejam seguros e eficientes no contexto de sua aplicação. Além da resistência a ataques criptoanalíticos clássicos, também é essencial considerar a resistência dos algoritmos a ataques específicos para implementações leves como ataques de canal lateral e ataques de injeção de falha (RAO; PREMA, 2021), particularmente relevantes em aplicações IoT e sistemas embarcados, onde os dispositivos são mais vulneráveis a ataques físicos.

A simplicidade e segurança do desenho do algoritmo permitem também sua implementação em *hardware* ou *software* leves sem comprometer sua segurança e facilitando a adaptação em dispositivos de recursos limitados (HASAN et al., 2022). Um algoritmo simples emprega operações aritméticas ou lógicas básicas como XOR, deslocamentos e rotações, em vez de operações matemáticas complexas como exponenciações ou multiplicações (GANIEV; KHUDOYKULOV, 2021). A simplicidade pode facilitar a análise de segurança do algoritmo uma vez que com menos elementos complexos a identificação e correção de vulnerabilidades pode se tornar mais simples.

3.4 MÉTODOS DE TOMADA DE DECISÃO MULTICRITÉRIO

A escolha da opção mais apropriada de um conjunto de alternativas possíveis em relação a requisitos, critérios ou indicadores predefinidos faz parte de atividades cotidianas. Em consequência, foram desenvolvidas técnicas conhecidas como Métodos de Tomada de Decisão Multicritério (do inglês, *Multi-Criteria Decision Making* - MCDM), que integram vários critérios e visam garantir uma análise objetiva e deliberada para gerenciar decisões com sucesso (ROY, 1996).

Portanto, a tomada de decisão pode ser definida como um esforço para resolver o dilema dos objetivos conflituosos, cuja presença impede a existência "solução ótima" e conduz à procura da "solução de melhor compromisso" (ZELENEY, 1982). A abordagem MCDM tem sido usada para IoT em vários campos, como prevenção de incidentes, segurança, gerenciamento de recursos, cadeia de suprimentos e planejamento de redes (ZAYAT; HASSAN, 2021).

A tomada de decisão multicritério pode ser abordada por meio de diversas metodologias que auxiliam na avaliação e seleção de alternativas, considerando múltiplos critérios que frequentemente entram em conflito.

TAB. 3.5: Métricas de segurança para implementações de algoritmos leves.

Métrica	Definição
Geração de Chaves	As chaves geradas devem ser imprevisíveis, garantindo entropia e segurança
Comprimento da Chave	Chaves mais longas aumentam o espaço de busca, dificultando ataques de força bruta.
Tamanho do Bloco	Define a quantidade de dados processados em cada rodada; blocos maiores reduzem padrões estatísticos.
Número de Rodadas	Rodadas adicionais aumentam a difusão e confusão
Entropia e Aleatoriedade	Geração de números aleatórios de alta qualidade para chaves e vetores de inicialização.
Avaliação de Avalanche	Pequenas mudanças na entrada causam mudanças significativas na saída.
Conformidade com Padrões	Algoritmos devem seguir normas para validação de segurança e desempenho.
Testes Independentes	Revisões conduzidas por especialistas e competições públicas.
Resistência a Ataques Criptoanalíticos Clássicos	Proteção contra criptoanálise diferencial, linear e de força bruta.
Resistência a Ataques Específicos para Ambientes com Restrições de Recursos	Minimiza vazamentos de informações físicas, como energia consumida ou ataques de injeção de falhas
Simplicidade e Segurança do Design	Design claro que facilita a implementação correta em <i>hardware/software</i> .

3.4.1 MÉTODO CRITIC

CRITIC (do inglês, *Criteria Importance Through Intercriteria Correlation*) e foi introduzido por (?) e visa a determinação de pesos objetivos de importância relativa em problemas de método de decisão de múltiplos critérios. Segundo (PAN et al., 2021), o método CRITIC define os pesos baseado em dois conceitos: o tamanho do desvio padrão, que indica o tamanho da discrepância entre os valores de cada esquema dentro do mesmo indicador, e o caráter conflitante dos critérios de avaliação, com base na correlação entre índices.

3.4.2 MÉTODO TOPSIS

TOPSIS (do inglês, *Technique for Order Preference by Similarity to Ideal Solution*) foi apresentado por (HWANG; YOON, 1981) e é uma técnica de avaliação de performances de alternativas através da similaridade da mesmas com uma solução ideal. De acordo com essa técnica a melhor alternativa é aquela mais próxima da solução ideal e mais distante da solução não ideal. Ou seja, a solução ideal positiva é uma solução que potencializa os critérios de benefício e diminui os critérios de custo, ao contrário da solução ideal negativa, que é aquela que maximiza os critérios de custo e minimiza os critérios de benefício (KROHLING; SOUZA, 2011).

A variação do método TOPSIS num ambiente *fuzzy* é capaz de lidar com avaliações tanto quantitativas, quanto critérios qualitativos e selecionar a melhor alternativa de maneira eficiente (CHEN et al., 2006). Conforme o grau de proximidade, é possível definir não somente a ordem de classificação como também o status de avaliação das alternativas possíveis, demandando, assim, informações prévias a respeito da importância relativa dos critérios (BÜYÜKÖZKAN; ÇİFÇİ, 2012).

3.4.3 MÉTODO PROMETHEE

PROMETHEE (do inglês, *Preference Ranking Organization Method for Enrichment Evaluation*) (BRANS; VINCKE, 1982) é uma abordagem para tomada de decisão multicritério utilizada para determinar a melhor alternativa após a análise de alguns critérios especificados. O método é um modo de ordenação da avaliação multicritério e objetiva a construção de relações de sobreclassificação entre as alternativas, ranqueando-as da mais favorável até a menos propícia como forma de solução do problema (?).

O método em sua estrutura base, é destinado a avaliações de dados de natureza quantitativa, onde o decisor deve indicar a função de maximização ou minimização para

cada critério, juntamente com a função de normalização que mais se adequa ao critério em avaliação. Especificando os pesos para cada critério, são gerados os índices de preferência global, explicitando no contexto avaliado as relações de preferência entre as alternativas, obtendo ao final a sobreclassificação desejada (BRANS et al., 1986).

3.4.4 MÉTODO AHP

O Analytic Hierarchy Process (AHP) foi introduzido por (SAATY, 1990) e é um processo de classificação usado na tomada de decisões amplamente utilizado em uma variedade de campos, como o de negócios, governo, indústria, educação e saúde. O método se concentra em priorizar os critérios de seleção e distinguir os critérios mais importantes dos menos importantes.

O AHP é um método simples com foco em comparações em pares que são adequadas para avaliar o design qualitativo e quantitativo (TAN et al., 2014). Assumindo que há uma série de critérios e alternativas, os pesos dos critérios são primeiro calculados por meio de comparações pareadas usando a escala de Saaty. O método calcula os pesos dos critérios, verifica a consistência dos julgamentos e classifica as alternativas para identificar a melhor solução.

4 A PROPOSTA

De acordo com a Revisão Sistemática da Literatura realizada, observou-se:

- Embora haja um número crescente de algoritmos criptográficos leves desenvolvidos fatores como o ambiente de aplicação, o nível de ameaça e o custo computacional não são considerados na seleção do algoritmo mais adequado;
- Ausência de estudos comparativos consistentes, com critérios bem definidos e métricas padronizadas que dificultam a escolha de algoritmos que atendam de forma ideal às diversas exigências dos dispositivos e ambientes;
- Trabalhos anteriores utilizam apenas parâmetros baseados em *hardware* ou *software* na análise, desconsiderando os cenários ou avaliando isoladamente somente a segurança ou somente o desempenho das cifras; e
- Ausência de um conjunto de métricas consistentes e universalmente aceitas para avaliar e comparar algoritmos criptográficos leves, o que dificulta a padronização da seleção.

Da identificação de lacunas na área é possível verificar a oportunidade para o desenvolvimento de novos métodos na avaliação dos algoritmos leves, visando aprimorar a seleção e assim potencializando sua segurança, desempenho e eficiência energética, para ambientes de recursos limitados. A proposta será descrita nas seções subsequentes:

4.1 QUESTÕES DE PESQUISA

Medir o desempenho, a segurança e a eficiência energética é fundamental na avaliação concreta entre os algoritmos criptográficos simétricos leves. A avaliação e seleção de algoritmos criptográficos através de métricas isoladas, independentemente de ponderação da relevância dos parâmetros avaliados ou do cenário em que será utilizado, pode levar ao uso indevido de recursos ou ao comprometimento do nível de segurança.

Questão de Pesquisa 1. *Como uma metodologia de avaliação e seleção multi-critério pode ser desenvolvida para integrar diferentes métricas e critérios de segurança, desempenho e eficiência energética dos algoritmos criptográficos simétricos leves?*

4.1.1 HIPÓTESES

Hipótese 1. *Uma metodologia de avaliação e seleção multicritério pode identificar algoritmos criptográficos simétricos leves que ofereçam um equilíbrio otimizado entre segurança, desempenho e eficiência energética, atendendo às restrições de dispositivos IoT de forma mais eficiente do que abordagens unidimensionais focadas exclusivamente na segurança ou no desempenho.*

4.1.2 JUSTIFICATIVA DA HIPÓTESE

Muitos dispositivos IoT possuem limitações severas de recursos, como memória, processamento e energia, mas ainda precisam garantir um nível de segurança apropriado. Abordagens unidimensionais podem não ser adequadas pois não consideram a correlação entre os diversos requisitos. Em cenários reais, como redes de sensores sem fio, sistemas de controle industriais e dispositivos vestíveis, os algoritmos criptográficos utilizados precisam ser suficientemente seguros para a proteção dos dados, mas também rápidos e eficientes o suficiente para operar dentro das limitações dos ambientes em que são utilizados.

Uma abordagem multicritério pode fornecer parâmetros ajustáveis que atendam às diferentes necessidades de segurança, minimizando o comprometimento do desempenho e da eficiência energética, permitindo que o algoritmo selecionado seja o mais adequado para um determinado cenário.

4.2 OBJETIVOS

Uma avaliação multicritério de algoritmos criptográficos leves pode promover um balanceamento otimizado entre segurança, desempenho e eficiência energética, fornecendo uma base para a seleção de algoritmos que atendam de forma mais eficiente as necessidades específicas de aplicações IoT em diversos cenários.

Portanto, este trabalho tem como objetivo geral estabelecer uma metodologia de avaliação, através da identificação de métricas quantitativas e qualitativas, a fim de oferecer um equilíbrio entre segurança, desempenho e eficiência energética na seleção de algoritmos criptográficos leves.

Para atingir o objetivo geral são propostos os seguintes objetivos específicos:

- Identificação de algoritmos criptográficos leves existentes e suas aplicações;
- Análise dos mecanismos de segurança aplicados em cenários de IoT;

- Definição dos critérios de avaliação de segurança, desempenho e eficiência energética dos algoritmos e suas respectivas ponderações;
- Implementação de métodos de avaliação multicritério para comparação dos algoritmos; e
- Comparação dos resultados obtidos no trabalho com os apresentados na literatura.

4.3 CONTRIBUIÇÕES ESPERADAS

As contribuições esperadas para este trabalho são:

- (i) Definição de métricas qualitativas e quantitativas que permitam uma avaliação dos algoritmos criptográficos leves.
- (ii) Estabelecimento de uma metodologia de avaliação que permita a seleção eficiente de algoritmos criptográficos leves garantindo um equilíbrio entre segurança, desempenho e eficiência energética.

5 PLANO DE AÇÃO

O plano para o desenvolvimento da proposta de pesquisa inclui as atividades relacionadas abaixo:

- (i) Revisão Sistemática da Literatura;
- (ii) Escrita da dissertação, Identificação dos critérios de avaliação de segurança, desempenho e eficiência energética dos algoritmos criptográficos leves;
- (iii) Escrita da dissertação, Identificação dos métodos de tomada de decisão multicritério;
- (iv) Escrita da dissertação, Construção e validação dos cenários de execução dos algoritmos leves, seus critérios e seus respectivos pesos;
- (v) Escrita da dissertação, Configuração do modelo de tomada de decisão multicritério;
- (vi) Escrita da dissertação, Execução do modelo de tomada de decisão multicritério;
- (vii) Escrita da dissertação, Análise e comparação dos resultados;
- (viii) Escrita da dissertação, Escrita de artigo;
- (ix) Conclusão da escrita da dissertação; e
- (x) Defesa da dissertação.

5.1 METODOLOGIA

Nesta seção, será apresentada a metodologia, incluindo as fases para implantação da solução proposta, com a descrição detalhada de cada etapa. A metodologia para desenvolvimento do experimento se dará através da sequência descrita na Figura 5.1.

Em uma primeira fase, foi realizada uma Revisão Sistemática da Literatura, com o objetivo de identificar características que qualificam um algoritmo criptográfico como leve e suas aplicações. Foram priorizados os trabalhos que exploram o balanceamento entre de segurança, desempenho e eficiência energética e que analisam os mecanismos aplicados em cenários de IoT. Algoritmos criptográficos leves são projetados para operar em cenários de recursos limitados e é importante identificar algoritmos adequados à estes ambientes. Da

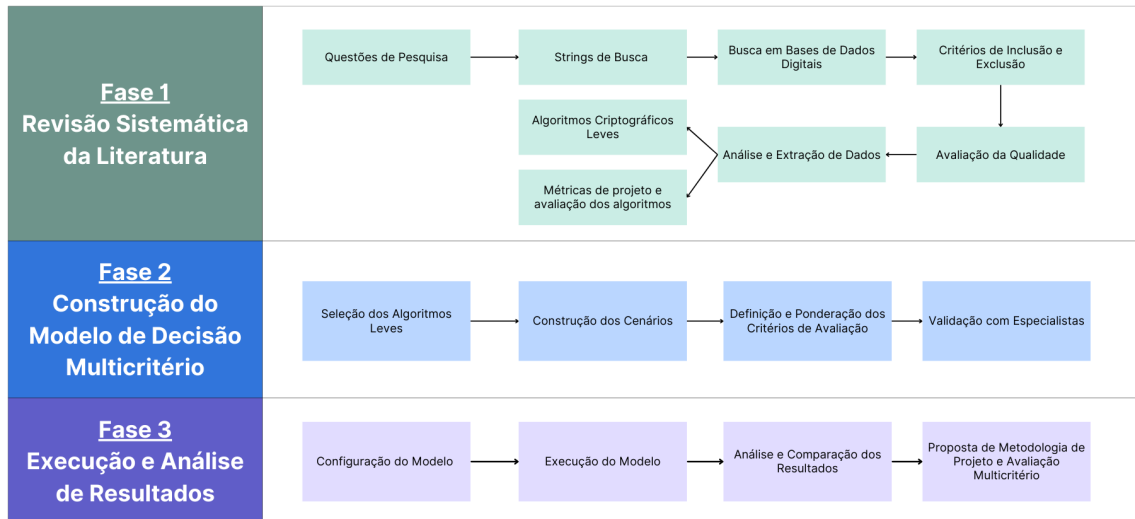


FIG. 5.1: Metodologia de Pesquisa Proposta.

mesma maneira, foram relacionadas as métricas mais utilizadas na literatura e que serão consideradas como critérios qualitativos e quantitativos para a avaliação dos algoritmos.

Durante a segunda fase, serão selecionados os algoritmos leves mais relevantes com base em sua popularidade na literatura, nível de segurança e uso em sistemas de recursos limitados. Nesta fase, os cenários de execução dos algoritmos serão construídos e a validados, e também serão definidos os critérios e subcritérios de segurança, desempenho e eficiência energética e seus respectivos pesos. A validação dos parâmetros relevantes a serem avaliados será realizada através de pesquisa com especialistas e gestores de segurança da informação (obs: a definir). O foco principal obter informações sobre os impactos dos algoritmos leves em cenários distintos e em termos de diferentes parâmetros como memória, latência, potência, energia, área do chip, tamanho do código fonte, tamanho da chave, e assim por diante.

Na última fase, uma vez configurado, o modelo de tomada de decisão multicritério será executado por meio de estudos de caso. Nesta fase, serão observadas como mudanças nos pesos dos critérios podem afetar a classificação final dos algoritmos, garantindo que os resultados sejam robustos e confiáveis. Por fim, os resultados dos estudos de caso serão analisados e comparados com estudos anteriores, com o objetivo final de propor uma metodologia de avaliação e seleção multicritério para algoritmos criptográficos simétricos leves.

5.1.1 PROVA DE CONCEITO

Objetivo: Demonstrar a viabilidade de utilização de métodos multicritério na avaliação de algoritmos criptográficos leves. Para isso, foi realizada a avaliação de 3 (três) algoritmos leves, citados na literatura como candidatos a serem utilizados em um cenário RFID. As métricas de consumo de Energia, Velocidade e Segurança foram avaliadas: em um primeiro contexto em que a Energia é a métrica mais importante; e em um segundo contexto em que a Segurança foi considerada mais importante. Os resultados finais apresentados demonstram que, para um mesmo rol de alternativas disponíveis, em que suas métricas são ponderadas de maneiras distintas, cada uma das avaliações apresentará resultados também distintos. O método utilizado nessa Prova de Conceito é o AHP, uma vez que tal método considera tanto métodos quantitativos quanto qualitativos, mais adequados à avaliação pretendida por essa pesquisa.

Métricas a serem avaliadas:

- a) Consumo de energia - critério quantitativo,
- b) Velocidade - critério quantitativo; e
- c) Segurança - critério qualitativo

Cenário de aplicação dos algoritmos: Etiquetas RFID

Algoritmos indicados: Grain, Trivium e DESL

Matriz de comparação de Pares (escala de Saaty):

Métrica	Energia	Velocidade	Segurança
Energia	1	3	5
Velocidade	1/3	1	4
Segurança	1/5	1/4	1

A escala considera 1 = igualmente importante; 9 = um é extremamente mais importante que o outro. Nesse exemplo, Energia é 3 vezes mais importante que Velocidade e 5 vezes mais importante que Segurança, enquanto Velocidade é 4 vezes mais importante que Segurança.

Normalização da Matriz e Cálculo dos Pesos

Cada coluna da matriz é normalizada dividindo-se cada elemento pelo somatório da coluna e, em seguida, calculamos a média de cada linha.

Métrica	Energia	Velocidade	Segurança	Média/Peso
Energia	0.652	0.706	0.500	0.619
Velocidade	0.217	0.235	0.400	0.284
Segurança	0.130	0.059	0.100	0.096

Resultado: Energia: 61,9%; Velocidade: 28,4%; e Segurança: 9,6%

Matriz de Comparação dos Algoritmos para cada Métrica

Os algoritmos são comparados em pares e em relação à cada métrica.

a) Energia

Algoritmo	Grain	Trivium	DESL
Grain	1	2	3
Trivium	1/2	1	2
DESL	1/3	1/2	1

b) Velocidade

Algoritmo	Grain	Trivium	DESL
Grain	1	1/3	2
Trivium	3	1	4
DESL	1/2	1/4	1

c) Segurança

Algoritmo	Grain	Trivium	DESL
Grain	1	1/2	1/4
Trivium	2	1	1/3
DESL	4	3	1

Cálculo dos Pesos para cada Métrica

Os pesos das métricas são calculados seguindo o processo de normalização das matrizes e de determinação dos pesos médios.

a) Energia:

Algoritmo	Grain	Trivium	DESL	Média/Peso
Grain	0.545	0.571	0.500	0.539
Trivium	0.273	0.286	0.333	0.297
DESL	0.182	0.143	0.167	0.164

Grain: 53,9%; Trivium: 29,7%; e DESL: 16,4%

O algoritmo Grain é o mais eficiente em termos de energia.

b) Velocidade:

Algoritmo	Grain	Trivium	DESL	Média/Peso
Grain	0.222	0.211	0.286	0.239
Trivium	0.667	0.632	0.571	0.623
DESL	0.111	0.158	0.143	0.137

Grain: 23,9%; Trivium: 62,3%; e DESL: 13,7%

O algoritmo Trivium é o mais eficiente em termos de velocidade.

c) Segurança:

Algoritmo	Grain	Trivium	DESL	Média/Peso
Grain	0.143	0.111	0.158	0.137
Trivium	0.286	0.222	0.211	0.239
DESL	0.571	0.667	0.632	0.623

Grain: 13,7%; Trivium: 23,9%; e DESL: 62,3%

O algoritmo DESL é o mais eficiente em termos de segurança.

Agregação dos Pesos

Os pesos das alternativas são multiplicados pelos pesos dos critérios e somado os resultados para cada algoritmo. Com as matrizes normalizadas de cada métrica e a Média/Peso também calculados, por fim, temos os pesos globais. Combinando a Média/Peso com os pesos das métricas principais (0.619 para Energia, 0.284 para Velocidade, e 0.096 para Segurança) temos que:

Para o Algoritmo Grain:

- Energia: $0.539 \times 0.619 = 0.334$
- Velocidade: $0.239 \times 0.284 = 0.067$
- Segurança: $0.137 \times 0.096 = 0.013$

- Peso Global: $0.334 + 0.067 + 0.013 = \mathbf{0.415}$

Para o Algoritmo Trivium:

- Energia: $0.297 \times 0.619 = 0.184$
- Velocidade: $0.623 \times 0.284 = 0.177$
- Segurança: $0.239 \times 0.096 = 0.023$
- Peso Global: $0.314 + 0.028 + 0.004 = \mathbf{0.384}$

Para o Algoritmo DESL:

- Energia: $0.164 \times 0.619 = 0.102$
- Velocidade: $0.137 \times 0.284 = 0.039$
- Segurança: $0.623 \times 0.096 = 0.060$
- Peso Global: $0.102 + 0.039 + 0.060 = \mathbf{0.201}$

Algoritmo	Energia (0.619)	Velocidade (0.284)	Segurança (0.096)	Final
Grain	0.334	0.067	0.013	0.415
Trivium	0.184	0.177	0.023	0.384
DESL	0.164	0.137	0.623	0.201

Resultado Final

- Grain é o algoritmo mais adequado, com uma pontuação total de 41,4%, devido ao seu equilíbrio entre eficiência energética e velocidade.
- Trivium ocupa o segundo lugar, sendo mais rápido, mas menos eficiente energeticamente.
- DESL é a alternativa menos adequada devido à sua menor eficiência em energia e velocidade.

Agora, em um segundo exemplo considera-se a métrica de **Segurança** como um critério de maior importância na avaliação dos algoritmos, consequentemente com maior peso. Nesse exemplo, a Segurança é 5 vezes mais importante que Velocidade e 7 vezes mais importante que Energia. Velocidade é 3 vezes mais importante que Energia.

Matriz de comparação de Pares (métrica de Segurança mais importante):

Métrica	Segurança	Velocidade	Energia
Segurança	1	5	7
Velocidade	1/5	1	3
Energia	1/7	1/3	1

Normalização da Matriz e Cálculo dos Pesos

Métrica	Segurança	Velocidade	Energia	Média/Peso
Segurança	0.745	0.789	0.636	0.724
Velocidade	0.149	0.158	0.273	0.193
Energia	0.106	0.053	0.091	0.083

Resultado: Segurança: 72,4%; Velocidade: 19,3%; e Energia: 8,3%

Agregação dos Pesos

Os pesos das alternativas são multiplicados pelos pesos dos critérios e somado os resultados para cada algoritmo. As matrizes de cada métrica já foram normalizadas anteriormente, e a Média/Peso também calculados. Nesse segundo caso os pesos globais serão calculados combinando a Média/Peso com os pesos das métricas principais (0.724 para Segurança, 0.193 para Velocidade, e 0.083 para Energia) temos que: :

Para o Algoritmo Grain:

- Energia: $0.539 \times 0.083 = 0.045$
- Velocidade: $0.239 \times 0.193 = 0.046$
- Segurança: $0.137 \times 0.724 = 0.099$
- Peso Global: $0.045 + 0.046 + 0.099 = \mathbf{0.190}$

Para o Algoritmo Trivium:

- Energia: $0.297 \times 0.083 = 0.025$
- Velocidade: $0.623 \times 0.193 = 0.120$
- Segurança: $0.239 \times 0.724 = 0.173$
- Peso Global: $0.025 + 0.120 + 0.173 = \mathbf{0.318}$

Para o Algoritmo DESL:

- Energia: $0.164 \times 0.083 = 0.014$
- Velocidade: $0.137 \times 0.193 = 0.026$
- Segurança: $0.623 \times 0.724 = 0.451$
- Peso Global: $0.014 + 0.026 + 0.451 = \mathbf{0.491}$

Algoritmo	Segurança (0.724)	Velocidade (0.193)	Energia (0.083)	Final
Grain	0.099	0.046	0.045	0.190
Trivium	0.173	0.120	0.025	0.318
DESL	0.451	0.026	0.014	0.491

Resultado Final

Em uma avaliação em que a Segurança é considerada como critério com maior peso em relação aos demais, temos um resultado distinto para o algoritmo mais adequado:

- DESL é o algoritmo mais adequado com 49,1%, principalmente devido à sua boa segurança e equilíbrio de velocidade e energia.
- Trivium ocupa o segundo lugar, com 31,8%, apresentando excelente velocidade, mas penalizado pela baixa segurança.
- Grain fica em terceiro lugar com 19%, devido ao menor valor atribuído à segurança.

5.2 CRONOGRAMA

O cronograma para o desenvolvimento das atividades relacionadas a esta proposta pode ser visto na Figura 5.2.

TAREFAS	2024		2025							
	NOV	DEZ	JAN	FEV	MAR	ABR	MAI	JUN	JUL	AGO
Revisão da Literatura	X	X	X	X	X	X	X	X	X	
Identificação dos critérios de avaliação		X								
Identificação dos métodos tomada de decisão multicritério		X								
Validação de cenários		X	X							
Configuração do modelo			X	X						
Execução do modelo				X	X	X				
Análise e comparação dos resultados					X	X	X			
Escrita de artigo							X	X	X	
Escrita da dissertação		X	X	X	X	X	X	X	X	
Defesa da dissertação										X



 Realizado
 Planejado

FIG. 5.2: Cronograma da Proposta de Dissertação.

6 REFERÊNCIAS BIBLIOGRÁFICAS

- A.MOHAMMED, Z.; HUSSEIN, K. A. Lightweight cryptography concepts and algorithms: A survey. In: 2023 SECOND INTERNATIONAL CONFERENCE ON ADVANCED COMPUTER APPLICATIONS (ACA), 2., 2023. **Anais...** [S.l.: s.n.], 2023, p. 1–7.
- BINTI MOHAMAD NOOR, M.; HASSAN, W. H. Current research on internet of things (iot) security: A survey. **Computer Networks**, v. 148, p. 283–294, 2019. Disponível em: <<https://www.sciencedirect.com/science/article/pii/S1389128618307035>>. Acesso em: 2023.
- BLANC, S.; LAHMADI, A.; GOUGUEC, K.; MINIER, M. ; SLEEM, L. Benchmarking of lightweight cryptographic algorithms for wireless iot networks. **Wireless Networks**, v. 28, 2022. Disponível em: <<https://doi.org/10.1007/s11276-022-03046-1>>. Acesso em: 2023.
- BRANS, J. P.; VINCKE, P. Promethee: A new method for ordinal classification. **Theory and Decision**, v. 12, n. 3, p. 219–245, 1982.
- BRASIL. **Política Nacional de Defesa**. [S.l.: s.n.], 2020.
- BRASIL. **Plano Estratégico do Exército**. [S.l.: s.n.], 2023.
- BÜYÜKÖZKAN, G.; ÇİFÇİ, G. A novel hybrid mcdm approach based on fuzzy dematel, fuzzy anp and fuzzy topsis to evaluate green suppliers. **Expert Systems with Applications**, v. 39, n. 3, p. 3000–3011, 2012.
- CHEN, C.-T.; LIN, C.-T. ; HUANG, S.-F. A fuzzy approach for supplier evaluation and selection in supply chain management. **International Journal of Production Economics**, v. 102, n. 2, p. 289–301, 2006.
- DAMAJ, I. W.; AL-MUBASHER, H. ; SAADEH, M. An extended analytical framework for heterogeneous implementations of light cryptographic algorithms. **Future Generation Computer Systems**, v. 141, p. 154–172, 2023. Disponível em: <<https://www.sciencedirect.com/science/article/pii/S0167739X22003673>>. Acesso em: 2023.

- DUTTA, I. K.; GHOSH, B. ; BAYOUMI, M. Lightweight cryptography for internet of insecure things: A survey. In: 2019 IEEE 9TH ANNUAL COMPUTING AND COMMUNICATION WORKSHOP AND CONFERENCE (CCWC), 9., 2019. **Anais...** [S.l.: s.n.], 2019, p. 0475–0481.
- EL GAABOURI, I.; SENHADJI, M. ; BELKASMI, M. A survey on lightweight cryptography approach for iot devices security. In: 2022 5TH INTERNATIONAL CONFERENCE ON NETWORKING, INFORMATION SYSTEMS AND SECURITY: ENVISAGE INTELLIGENT SYSTEMS IN 5G//6G-BASED INTERCONNECTED DIGITAL WORLDS (NISS), 5., 2022. **Anais...** [S.l.: s.n.], 2022, p. 1–8.
- FARHAN, L.; KHAREL, R. 1st. ed. Switzerland: Springer, Cham, 2018. p. 331–347. ISBN 9783319995397.
- GANIEV, S.; KHUDOYKULOV, Z. Lightweight cryptography algorithms for iot devices: Open issues and challenges. In: 2021 INTERNATIONAL CONFERENCE ON INFORMATION SCIENCE AND COMMUNICATIONS TECHNOLOGIES (ICISCT), 2021., 2021. **Anais...** [S.l.: s.n.], 2021, p. 01–04.
- HARBI, Y.; ALIOUAT, Z.; REFOUFI, A. ; HAROUS, S. Recent security trends in internet of things: A comprehensive survey. **IEEE Access**, v. 9, p. 113292–113314, 2021.
- HASAN, H.; ALI, G.; ELMEDANY, W. ; BALAKRISHNA, C. Lightweight encryption algorithms for internet of things: A review on security and performance aspects. In: 2022 INTERNATIONAL CONFERENCE ON INNOVATION AND INTELLIGENCE FOR INFORMATICS, COMPUTING, AND TECHNOLOGIES (3ICT), 2022., 2022. **Anais...** [S.l.: s.n.], 2022, p. 239–244.
- HASSIJA, V.; CHAMOLA, V.; SAXENA, V.; JAIN, D.; GOYAL, P. ; SIKDAR, B. A survey on iot security: Application areas, security threats, and solution architectures. **IEEE Access**, v. 7, p. 82721–82743, 2019.
- HATZIVASILIS, G.; FYSARAKIS, K.; PAPAEFSTATHIOU, I. ; MANIFAVAS, C. A review of lightweight block ciphers. **Journal of Cryptographic Engineering**, v. 8, p. 141 – 184, 2018. Disponível em: <<https://api.semanticscholar.org/CorpusID:19041116>>. Acesso em: 2023.

- HERCIGONJA, Z. Comparative Analysis of Cryptographic Algorithms. **International Journal of Digital Technology and Economy**, v. 1, n. 2, p. 127–134, 2016. Disponível em: <<https://ideas.repec.org/a/alg/jijdte/v1y2016i2p127-134.html>>. Acesso em: 2018.
- HWANG, C.-L.; YOON, K. Methods for multiple attribute decision making. In: _____. **Multiple Attribute Decision Making: Methods and Applications A State-of-the-Art Survey**. Berlin, Heidelberg: Springer Berlin Heidelberg, 1981. p. 58–191. ISBN 978-3-642-48318-9.
- KANNAN, B. M.; SOLAINAYAGI, P.; AZATH, H.; MURUGAN, S. ; SRINIVASAN, C. Secure communication in iot-enabled embedded systems for military applications using encryption. In: 2023 2ND INTERNATIONAL CONFERENCE ON EDGE COMPUTING AND APPLICATIONS (ICECAA), 2., 2023. **Anais...** [S.l.: s.n.], 2023, p. 1385–1389.
- KERCKHOF, S.; DURVAUX, F.; HOCQUET, C.; BOL, D. ; STANDAERT, F.-X. Towards green cryptography: A comparison of lightweight ciphers from the energy viewpoint. In: CRYPTOGRAPHIC HARDWARE AND EMBEDDED SYSTEMS – CHES 2012, 2012., 2012. **Anais...** Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, p. 390–407.
- KHANNA, A.; KAUR, S. Internet of things (iot), applications and challenges: A comprehensive review. **Wireless Personal Communications**, v. 114, p. 1–76, 2020.
- KOUICEM, D. E.; BOUABDALLAH, A. ; LAKHLEF, H. Internet of things security: A top-down survey. **Computer Networks**, v. 141, p. 199–221, 2018. Disponível em: <<https://www.sciencedirect.com/science/article/pii/S1389128618301208>>. Acesso em: 21 mar. de 2018.
- KROHLING, R.; SOUZA, T. Dois exemplos da aplicação da técnica topsis para tomada de decisão. **Revista de Sistemas de Informação da FSMA**, v. 8, p. 31–33, 2011.
- LARA-NINO, C. A.; DIAZ-PEREZ, A. ; MORALES-SANDOVAL, M. Elliptic curve lightweight cryptography: A survey. **IEEE Access**, v. 6, p. 72514–72550, 2018.
- MOHD, B. J.; HAYAJNEH, T. ; VASILAKOS, A. V. A survey on lightweight block ciphers for low-resource devices: Comparative study and open issues. **Journal of Network and Computer Applications**, v. 58, p. 73–93, 2015. Dispo-

nível em: <<https://www.sciencedirect.com/science/article/pii/S1084804515002076>>. Acesso em: 2023.

MOMENI, M. R.; JABBARI, A. ; FUNG, C. An energy-efficient multiple-factor authentication protocol for critical infrastructure iot systems. In: 2023 7TH CYBER SECURITY IN NETWORKING CONFERENCE (CSNET), 7., 2023. **Anais...** [S.l.: s.n.], 2023, p. 238–242.

NING, L.; ALI, Y.; KE, H.; NAZIR, S. ; HUANLI, Z. A hybrid mcsm approach of selecting lightweight cryptographic cipher based on iso and nist lightweight cryptography security requirements for internet of health things. **IEEE Access**, v. 8, p. 220165–220187, 2020.

PAN, X.; ZHANG, H. ; LI, X. An improved critic method for multi-criteria decision making. **Journal of Multi-Criteria Decision Analysis**, v. 28, n. 3, p. 123–135, 2021.

PANAHI, U.; BAYILMIŞ, C. Enabling secure data transmission for wireless sensor networks based iot applications. **Ain Shams Engineering Journal**, v. 14, n. 2, p. 101866, 2023. Disponível em: <<https://www.sciencedirect.com/science/article/pii/S2090447922001770>>. Acesso em: 2023.

PATEL, S. T.; MISTRY, N. H. A survey: Lightweight cryptography in wsn. In: INTERNATIONAL CONFERENCE ON COMMUNICATION NETWORKS (ICCN), 2015., 2015. **Anais...** [S.l.: s.n.], 2015, p. 11–15.

PLOENNIGS, J.; COHN, J. ; STANFORD-CLARK, A. The future of iot. **IEEE Internet of Things Magazine**, v. 1, n. 1, p. 28–33, 2018.

QASAIMAH, M.; AL-QASSAS, R. S. ; TEDMORI, S. Software randomness analysis and evaluation of lightweight ciphers: the prospective for iot security. **Multimedia Tools Appl.**, v. 77, n. 14, p. 18415–18449, 2018. Disponível em: <<https://doi.org/10.1007/s11042-018-5663-8>>. Acesso em: 2024.

RADHAKRISHNAN, I.; JADON, S. ; HONNAVALI, P. B. Efficiency and security evaluation of lightweight cryptographic algorithms for resource-constrained iot devices. **Sensors**, v. 24, n. 12, 2024. Disponível em: <<https://www.mdpi.com/1424-8220/24/12/4008>>. Acesso em: 2024.

- RAHUL, C.; KOUSARR, N.; YADAV, T.; KEERTHI, P.; HARIHARAN, S. ; KUKREJA, V. Analysis of resource utilization in lightweight cryptographic algorithms. In: 2024 INTERNATIONAL CONFERENCE ON COGNITIVE ROBOTICS AND INTELLIGENT SYSTEMS (ICC - ROBINS), 2024., 2024. **Anais...** [S.l.: s.n.], 2024, p. 884–889.
- RANA, M.; MAMUN, Q. ; ISLAM, R. Balancing security and efficiency: A power consumption analysis of a lightweight block cipher. **Electronics**, v. 13, n. 21, 2024. Disponível em: <<https://www.mdpi.com/2079-9292/13/21/4325>>. Acesso em: 2024.
- RAO, V.; PREMA, K. A review on lightweight cryptography for internet-of-things based applications. **Journal of Ambient Intelligence and Humanized Computing**, v. 12, p. 1–23, 2021.
- ROY, B. **Multicriteria Methodology for Decision Aiding**. Dordrecht, The Netherlands: Kluwer Academic Publishers, 1996. ISBN 978-0-7923-4212-2.
- SAATY, T. L. How to make a decision: The analytic hierarchy process. **European Journal of Operational Research**, v. 48, n. 1, p. 9–26, 1990. Disponível em: <<https://www.sciencedirect.com/science/article/pii/037722179090057I>>. Acesso em: Desicion making by the analytic hierarchy process: Theory and applications.
- SALLAM, S.; BEHESHTI, B. D. A survey on lightweight cryptographic algorithms. In: TENCON 2018 - 2018 IEEE REGION 10 CONFERENCE, 10., 2018. **Anais...** [S.l.: s.n.], 2018, p. 1784–1789.
- SANAP, S. D.; MORE, V. Performance analysis of encryption techniques based on avalanche effect and strict avalanche criterion. In: 2021 3RD INTERNATIONAL CONFERENCE ON SIGNAL PROCESSING AND COMMUNICATION (ICPSC), 3., 2021. **Anais...** [S.l.: s.n.], 2021, p. 676–679.
- SARAIVA, D. A. F.; LEITHARDT, V. R. Q.; DE PAULA, D.; SALES MENDES, A.; GONZÁLEZ, G. V. ; CROCKER, P. Prisec: Comparison of symmetric key algorithms for iot devices. **Sensors**, v. 19, n. 19, 2019. Disponível em: <<https://www.mdpi.com/1424-8220/19/19/4312>>. Acesso em: 2024.
- SEVIN, A.; MOHAMMED, A. A survey on software implementation of lightweight block ciphers for iot devices. **Journal of Ambient Intelligence and Humanized Computing**, v. 14, p. 1–15, 2023.

- SHANNON, C. E.; WEAVER, W. **The Mathematical Theory of Communication**. Champaign, IL, USA: The University of Illinois Press, 1949.
- SINGH, S.; SHARMA, P.; MOON, S. ; PARK, J. Advanced lightweight encryption algorithms for iot devices: survey, challenges and solutions. **Journal of Ambient Intelligence and Humanized Computing**, v. 15, p. 1–18, 2017.
- SONG, H.; FINK, G. A. ; JESCHKE, S. Lightweight crypto and security. In: _____. **Security and Privacy in Cyber-Physical Systems: Foundations, Principles, and Applications**. [S.l.: s.n.], 2017. p. 243–261.
- SREEHARI, B.; SANKAR, V.; LOPEZ, R. S.; K S, V. ; STUART, C. M. A review on fpga implementation of lightweight cryptography for wireless sensor network. In: 2023 INTERNATIONAL CONFERENCE ON POWER, INSTRUMENTATION, CONTROL AND COMPUTING (PICC), 2023., 2023. **Anais...** [S.l.: s.n.], 2023, p. 1–6.
- SURI, N.; TORTONESI, M.; MICHAELIS, J.; BUDULAS, P.; BENINCASA, G.; RUSSELL, S.; STEFANELLI, C. ; WINKLER, R. Analyzing the applicability of internet of things to the battlefield environment. In: 2016 INTERNATIONAL CONFERENCE ON MILITARY COMMUNICATIONS AND INFORMATION SYSTEMS (ICMCIS), 2016., 2016. **Anais...** [S.l.: s.n.], 2016, p. 1–8.
- TAN, R.; AVISO, K.; HUEL GAS, A. ; PROMENTILLA, M. Fuzzy ahp approach to selection problems in process engineering involving quantitative and qualitative aspects. **Process Safety and Environmental Protection**, v. 92, n. 5, p. 467–475, 2014. Disponível em: <<https://www.sciencedirect.com/science/article/pii/S0957582013000864>>. Acesso em: Process Systems Engineering.
- THAKOR, V. A.; RAZZAQUE, M. A. ; KHANDAKER, M. R. A. Lightweight cryptography for iot: A state-of-the-art. **ArXiv**, v. abs/2006.13813, 2020. Disponível em: <<https://api.semanticscholar.org/CorpusID:220041664>>. Acesso em: 2023.
- THAKOR, V. A.; RAZZAQUE, M. A. ; KHANDAKER, M. R. A. Lightweight cryptography algorithms for resource-constrained iot devices: A review, comparison and research opportunities. **IEEE Access**, v. 9, p. 28177–28193, 2021.
- WENG, D. Performance and energy evaluation of lightweight cryptography for small iot devices. In: 2023 IEEE 14TH ANNUAL UBIQUITOUS COMPUTING, ELEC-

TRONICS MOBILE COMMUNICATION CONFERENCE (UEMCON), 14., 2023.
Anais... [S.l.: s.n.], 2023, p. 289–295.

WILLIAMS, P.; DUTTA, I. K.; DAOUD, H. ; BAYOUMI, M. A survey on security in internet of things with a focus on the impact of emerging technologies. **Internet of Things**, v. 19, p. 100564, 2022. Disponível em: <<https://www.sciencedirect.com/science/article/pii/S2542660522000592>>. Acesso em: 31 nov. de 2023.

ZAYAT, M.; HASSAN, H. Multicriteria decision-making in iot applications. **Journal of Computational Intelligence in IoT**, v. 10, p. 78–89, 2021.

ZOLFAGHARI, B.; BIBAK, K. ; KOSHIBA, T. The odyssey of entropy: Cryptography. **Entropy**, v. 24, n. 2, p. 266, 2022. Disponível em: <<https://www.mdpi.com/1099-4300/24/2/266>>. Acesso em: This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

1º Ten Gabriela Mendes Corrêa de Miranda (SC 23201)

Aluno

Ten Cel José Antônio Moreira Xexéo, D.Sc.

Orientador

Maj Gabriela Moutinho de Souza Dias, D.Sc.

Coordenador de Pós-graduação

Concordo com a presente Proposta de Dissertação e declaro que as necessidades para sua execução serão garantidas pela Seção.

IME, em 10 de Dezembro de 2024.

Cel Julio César Duarte

CHEFE da SE/9