



DESAFIOS E SOLUÇÕES NA SEGURANÇA DA IOT

Alunos:
Fabricio Dias
Philippe Augusto
João Felipe
Filipe Augusto Lima
Guilherme Fernandes

INTRODUÇÃO



Introdução à IoT:

- Conceito amplo por Kevin Ashton desde 1999.
- Comunicação entre objetos físicos via internet para coletar, transmitir ou trocar dados.

Importância da IoT:

- Emergente social e economicamente.
- Transforma a vida cotidiana em setores como saúde, cidades inteligentes, agricultura e indústria.

Impactos Positivos:

- Saúde: Monitoramento remoto, gestão de medicamentos.
- Cidades inteligentes: Otimização do tráfego, gestão de resíduos, segurança.
- Agricultura: Sensores para condições climáticas, otimização da irrigação.
- Indústria: Contribui para manufatura inteligente e manutenção preditiva.



BASE TEÓRICA

- Tipos de Ataques:

- Ataques por Engenharia Social (Phishing, Ransomware).
- Ataques ao Sistema (DoS, Força Bruta, Injeção de Código).
- Ataques a Dispositivos IoT (Exploração de Vulnerabilidades).

Mecanismos de Defesa:

Ataques aos Sistemas:

- Firewalls.
- Sistema de Detecção de Intrusões (IDS).
- Sistemas de Prevenção de Intrusões.

Ataques por Engenharia Social:

- Filtros de E-mail.
- Software Antivírus.

Ataques a Dispositivos IoT:

- Atualizações de Firmware.
- Segmentação de Rede.
- Políticas de Segurança.



BASE TEÓRICA

Desafios em Dispositivos IoT:

- Particularidades únicas em cada ecossistema.
- Limitações de energia, capacidade de processamento e armazenamento.
- Soluções de segurança eficazes e otimizadas são necessárias para não comprometer o desempenho.

Criptografia Leve (LWC):

- Foco em algoritmos criptográficos eficientes e otimizados para dispositivos IoT.
- Padrões de especificações desenvolvidos pelo NIST e ISO.
- Crescimento da demanda devido à facilidade de aprimorar a segurança em dispositivos IoT.
- Exemplos de modelos: SPECK, HIGHT, SIMON.

METODOLOGIA

Critérios de Inclusão:

- Estudos abordando e enfatizando a segurança de dados associada à IoT.
- Especial atenção a artigos que apresentam dados sobre ataques a dispositivos IoT para análise comparativa entre anos anteriores e o presente.

Ferramenta e Justificativa:

- Utilização do Google Acadêmico.
- Agregador de bases de dados abrangente, facilitando a busca por uma quantidade significativa de artigos.



Abordagem Utilizada:

- Revisão narrativa de literatura.
- Busca não sistemática por informações.
- Escolha e seleção de bases de dados e periódicos científicos de maneira conveniente.

Período e Descritores:

- Levantamento bibliográfico realizado de 15 a 22 de janeiro.
- Descritores: "Internet das Coisas (IoT)" e "Segurança de Dados".
- Busca limitada a artigos e sites em língua portuguesa.

RESULTADOS E SOLUÇÕES

Estudo Comparativo de Blockciphers para IoT:

- - Sevin e Mohammed (2021).
- - Algoritmos PRESENT, SPECK, SIMON e CLEFIA.
- - Melhor custo-benefício: Menos armazenamento RAM/ROM, sem grande perda de velocidade.

Avaliação Experimental em Equipamentos IoT da Saúde:

- - Vinícius et al. (2022).
- - Testes aplicando os algoritmos em equipamentos IoT da saúde.
- - Métricas de vazão e latência analisadas para avaliar o impacto dos Lightweight Cryptography (LWC).

RESULTADOS E SOLUÇÕES

- Resultados da Avaliação Experimental:

Algoritmos Testados:

- PRESENT: Menor desempenho satisfatório, baixa taxa de transferência, descartado.
- AES-256 CBC: Melhor performance, maior velocidade na encriptação e desencriptação.

03

RESULTADOS E SOLUÇÕES

Criptografia	Vazão Encrypt ESP32	Vazão Decrypt ESP32	Vazão Servidor	Vazão Decrypt Servidor	Tamanho Chave	Tamanho Bloco	Uso Flash (ESP32)	Uso RAM (ESP32)	Otimizações (ESP32)	Segurança Quântica
AES CBC	7.03 MB/s	7.20 MB/s	300 MB/s	300 MB/s	256 bits	128 bits	0.51 kB	0.89 kB	Accelerado por <i>Hardware</i>	Sim
PRESENT	0.07 MB/s	0.07 MB/s	15 MB/s	15 MB/s	128 bits	64 bits	3.50 kB	1.30 kB	N/A	Não
SPECK	2.02 MB/s	1.88 MB/s	290 MB/s	290 MB/s	256 bits	128 bits	3.20 kB	1.10 kB	Operações 32 bits	Sim
CLEFIA	0.65 MB/s	0.65 MB/s	120 MB/s	120 MB/s	256 bits	128 bits	2.90 kB	2.50 kB	Lookup Tables	Sim

RESULTADOS E SOLUÇÕES

- **Consumo Energético:**

- Diferenças significativas devido a testes em diferentes dispositivos.
- Diversas formas de funcionamento, sem conclusão sobre semelhanças entre os LWC.

Conclusões Finais:

- AES-256 CBC e SPECK obtiveram os melhores resultados de desempenho.
- SPECK mostrou menor variação nas métricas de vazão e latência com aumento da demanda de transmissão.
- AES-256 CBC apresentou resultados similares, com mudanças mais significativas com a crescente taxa de transmissão.

FIM

