UNIVERSIDADE FEEVALE

PATRICK PEREIRA FAGUNDES

Eficácia de algoritmos de criptografia leve em dispositivos de IOT

(Título Provisório)

Anteprojeto de Trabalho de Conclusão

Novo Hamburgo
2020

PATRICK PEREIRA FAGUNDES

Eficácia de algoritmos de criptografia leve em dispositivos de IOT

(Título Provisório)

Anteprojeto de Trabalho de Conclusão de Curso, apresentado como requisito parcial à obtenção do grau de Bacharel em Ciência da Computação pela Universidade Feevale

Orientador: Paulo Ricardo Muniz Barros

Novo Hamburgo
2020

RESUMO

Na última década o mundo tem se deparado com um crescimento vertiginoso de dispositivos de IOT nos mais diversos setores da sociedade, e ao que tudo indica este número deve continuar a crescer. Em geral podemos denominar estes aparelhos como pequenas peças que executam tarefas simples, mas que podem desempenhar um papel extremamente importante no que diz respeito a automatização e comunicação de dados. Setores como o da saúde tem se beneficiado muito com esta tecnologia, potencializando os cuidados médicos com os pacientes. Mas se por um lado estes dispositivos trazem praticidade e versatilidade, por outro lado, eles levantam um alerta em relação a segurança. Devido ao tamanho reduzido de certos dispositivos de IOT, seu processamento é extremamente lento em comparação a computadores convencionais, e esta característica torna muito difícil agregar segurança, como executar métodos de criptografia convencional, como AES, nestes equipamentos em função da sua baixa potência de processamento. Porém existem diversas bibliotecas e algoritmos de criptografia leve voltados para dispositivos de baixo poder de processamento. Algumas destas soluções são mais robustas em segurança, outras menos, algumas demandam um pouco mais de poder de processamento, ou consumo de memória. Mas em geral não existe um padrão, uma classificação destes algoritmos de criptografia para os hardwares de IOT. E é neste ponto que se apresenta a proposta desta pesquisa, identificar a melhor solução de criptografia para garantir segurança na comunicação de dispositivos de IOT, identificando os diferentes algoritmos que possam indicar e garantir os requisitos de confidencialidade frente a baixa capacidade computacional presente em dispositivos de IOT.

Palavras-chave: IOT. LightWeight Cryptography. Criptografia leve. Segurança.

SUMÁRIO

MOTIVAÇÃO

Nesta última década a sociedade vem se deparando cada vez mais com a inserção de dispositivos de IOT em seu cotidiano, seja tanto em tarefas simples para a casa, quanto em tarefas industriais e até mesmo em outros setores como saúde (Gomes, 2019), esta tecnologia tem tido um papel importante na automatização de processos e/ou comunicação de dados (S Pinto Junior et al., 2017). Para se ter uma ideia, somente neste ano de 2020 a base destes dispositivos pode chegar a 30 bilhões em todo o mundo, e com previsão de crescimento para 75 bilhões até o final de 2025 (Carrion & Quaresma, 2019).

Conforme apresentado por Gomes (2019), em seu trabalho, unidades de saúde tem se beneficiado com a inserção desta tecnologia em seu processo de trabalho, pois foca-se na redução de custos, uma vez que a monitorização passa a ser feita em tempo real, dispensando o deslocamento de um profissional de saúde ao enfermo. Ele também aborda uma pesquisa realizada pela GE Healthcare com dez mil pessoas, em dez países, conclui que 90% dos entrevistados apoiam o uso de tecnologias para monitorar a saúde a distância. Indicando que a IOT tende a crescer bastante nesta área. O que contribui para a popularidade destes dispositivos é a sua portabilidade, e em grande parte, o baixo consumo de energia e dissipação de calor. Porém essa portabilidade tem um preço, segundo Haroon (2016), mesmo com o avanço da nanotecnologia nos últimos anos, softwares mais pesados podem não serem suportados em grande parte dos hardwares de IOT, assim como um Linux com todas suas features, como Graphical user interface, Multiuser capability etc. Outro aspecto destacado em seu estudo é a limitação da energia, frente ao seu armazenamento, como mais um dos fatores que limitam o uso dessa tecnologia.

Esta limitação de hardware presente nos dispositivos pode levantar um alerta para a segurança destes em relação a cyber ataques, que vem aumentando consideravelmente nos últimos anos, como mostra os dados do CERT.br (2020). No ano de 2010 o total de ataques relatados ao órgão foi de 142844, em 2020 até a metade do ano o número foi de 318697, mais que o dobro do ano 2010 em apenas metade do período. Mas grande parte destes ataques podem ser evitados com o uso de cifras e códigos de autenticação de mensagens (Teixeira et al., 2014).

Pode-se ver esta abordagem de cifras e criptografias sendo aplicadas em IOT através do uso de criptografias leves, conhecida como Lightweight Cryptography (LWC). Esta tecnologia já possui diversos tipos de algoritmos desenvolvidos para aparelhos com baixo poder de processamento e memória. Dentre os existentes, os da família Simon and Speck , criados pela NSA trazem bons resultados de criptografia leve. Sendo o Speck elaborado para obter

melhor desempenho em Softwares, enquanto Simon tem mais eficiência em implementações de hardware (DA SILVA, 2019).

Panasenko (Panasenko & Smagin, 2011) comenta que a LWC não determina critérios para classificar um algoritmo como leve, apenas que é preciso ter requerimentos muitos leves de hardware, como consumo de energia, memória etc. Já Albarello (2019) comenta a existência de bibliotecas Open Source de criptografia, com o objetivo de serem compatíveis com a maioria dos dispositivos embarcados, mas sem nenhuma garantia de desempenho para eles.

Diante deste cenário, a proposta deste trabalho visa estudar e testar algoritmos de criptografia leve para aumentar a privacidade e segurança na comunicação de dispositivos de IOT, servindo como um estudo balizador para escolha de algoritmos frente a ampla oferta de dispositivos de IOT, principalmente em áreas como a saúde, que necessitam de segurança no quesito que integra IOT e dados sensíveis de pacientes.

OBJETIVOS

Objetivo geral

Identificar a melhor solução de criptografia para garantir segurança na comunicação de dispositivos de IOT, identificando os diferentes algoritmos que possam indicar e garantir os requisitos de confidencialidade frente a baixa capacidade computacional presente nestes dispositivos.

Objetivos específicos

- Identificar os principais dispositivos de IOT utilizados no mercado que tenham conexão à rede e se comunicam com outros dispositivos.
- Identificar falhas de segurança na comunicação destes dispositivos;
- Identificar os principais algoritmos de criptografia leve existentes;
- Identificar se existem boas práticas para garantir segurança na comunicação entre estes dispositivos, bem como as métricas de avaliação;
- Realizar testes de vulnerabilidade em sua comunicação, com e sem a implementação de algoritmos de criptografia leve;
- Analisar e identificar os melhores algoritmos para tipos específicos de hardware destes dispositivos de IOT.

METODOLOGIA

A metodologia que será abordada neste trabalho baseia-se no método Design Science Research (DSR). Conforme DRESCH (Dresch et al., 2015), a DSR é uma forma de produção de conhecimento científico que envolve o desenvolvimento de uma inovação, com a intenção de resolver problemas do mundo real e ao mesmo tempo fazer uma contribuição cientifica de caráter prescritivo. Esta metodologia está classificada em seis etapas, conforme PEFFERS (2007) demonstra em seu trabalho. Seguindo sua classificação, cada uma destas etapas estão propostas da seguinte forma para esta pesquisa:

1. **Identificação do problema e motivação:** Pesquisar em banco de dados como Web os Science e Google Acadêmico, estudos relacionados a problemas que dispositivos de IOT com baixo poder de processamento possam ter em relação a segurança de dados. Identificar trabalhos que abordam boas práticas de segurança na área e realizar também pesquisa de algoritmos de criptografia leve (LWC).
2. **Definição dos Objetivos para solução:** Definir os principais algoritmos de criptografia leve existentes e quais serão usados na pesquisa. Também definir os tipos de hardware em IOT que possuem baixo poder de processamento que podem ser usados na pesquisa. De modo que possa ser encontrado os tipos de algoritmos mais eficazes para os tipos de Hardwares definidos.
3. **Projeto de desenvolvimento:** Preparar um ambiente de testes, de acordo com o que é abordado nos estudos identificados na etapa 1. De forma que seja possível implementar os algoritmos nos hardwares selecionados e depois testar a eficácia destes.
4. **Demonstração:** Executar os testes dos algoritmos nos dispositivos de IOT, seguindo a metodologia da etapa 3. Realizar testes de segurança, do tipo Man in the middle, como tentativa de quebra das criptografias e captura dos dados criptografados.
5. **Avaliação:** Aplicar as métricas de avaliação bem como a comparação dos resultados obtidos e classificar cada algoritmo como sendo eficaz ou não para os dispositivos, demonstrando a performance de cada um. De acordo com as principais abordagens encontradas na revisão da literatura na etapa 1.
6. **Comunicação final:** Apresentação do TC, bem como possível publicação dos estudos em eventos científicos.

CRONOGRAMA

Trabalho de Conclusão I

Etapa	Meses				
	Ago	Set	Out	Nov	Dez
Escrita do anteprojeto					
Entrega do anteprojeto					
Levantamento bibliográfico					
Escrita do TC I					
Entrega do TC I					

Trabalho de Conclusão II

Etapa	Meses				
	Fev	Mar	Abr	Mai	Jun
Desenvolvimento de testes					
Testes					
Análise dos resultados					
Elaboração do TC II					
Entrega do TC II					
Apresentação do TC II					

BIBLIOGRAFIA

Albarello, R. H. (2019). *Avaliação de algoritmos de criptografia e implementação de um protocolo leve para troca de chaves em dispositivos IoT* [Universidade Tecnológica Federal do Paraná]. Disponivel em: <http://repositorio.roca.utfpr.edu.br/jspui/handle/1/16273>. Acesso em: 24 ago. 2020

Carrion, P., & Quaresma, M. (2019). Internet da Coisas (IoT): Definições e aplicabilidade aos usuários finais. *Human Factors in Design*, *8*(15), 49–66. Disponivel em: <https://revistas.udesc.br/index.php/hfd/article/view/2316796308152019049>. Acesso em: 25 ago. 2020

DA SILVA, C. L. (2019). *DESENVOLVIMENTO DE UM MÓDULO DE CRIPTOGRAFIA LEVE PARA FPGA UTILIZANDO O ALGORITMO SIMON AND SPECK* [Pontifícia Universidade Católica do Rio Grande do Sul]. Disponivel em: <https://www.inf.pucrs.br/moraes/docs/tcc/tcc_cristovam.pdf>. Acesso em: 24 ago. 2020

Dresch, A., Lacerda, D. P., & Júnior, J. A. V. A. (2015). *Design science research: método de pesquisa para avanço da ciência e tecnologia*. Bookman Editora.

Gomes, J. T. C. (2019). *Riscos e vulnerabilidades dos equipamentos IoT em unidades de saúde*. Disponivel em: <https://iconline.ipleiria.pt/handle/10400.8/4680>. Acesso em: 31 ago. 2020

Haroon, A., Shah, M. A., Asim, Y., Naeem, W., Kamran, M., & Javaid, Q. (2016). Constraints in the IoT: the world in 2020 and beyond. *Constraints*, *7*(11), 252–271. Disponivel em: <https://www.researchgate.net/profile/Munam_Shah/publication/311395059_Constraints_in_the_IoT_The_World_in_2020_and_Beyond/links/5845523b08ae2d2175677d3b/Constraints-in-the-IoT-The-World-in-2020-and-Beyond.pdf>. Acesso em 31 ago. 2020

Panasenko, S., & Smagin, S. (2011). Lightweight cryptography: Underlying principles and approaches. *International Journal of Computer Theory and Engineering*, *3*(4), 516. Disponivel em: <http://www.ijcte.org/papers/360-JG527.pdf>. Acesso em 24 ago. 2020

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems*, *24*(3), 45–77. Disponivel em: <https://www.tandfonline.com/doi/abs/10.2753/MIS0742-1222240302>. Acesso em 5 set. 2020

S Pinto Junior, J., e Silva, C. dos, Domingos Xavier, D., & others. (2017). SEGURANÇA EM INTERNET DAS COISAS: UM SURVEY DE SOLUÇÕES LIGHTWEIGHT. *Revista de Sistemas e Computação-RSC*, *7*(2). Disponivel em: <https://revistas.unifacs.br/index.php/rsc/article/view/5110>. Acesso em: 24 ago. 2020

Teixeira, F. A., Pereira, F., Vieira, G., Marcondes, P., Wong, H. C., Nogueira, J. M. S., & Oliveira, L. B. (2014). Siot--defendendo a internet das coisas contra exploits. *Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC)*. Disponivel em: <http://sbrc2014.ufsc.br/anais/files/trilha/ST14-1.pdf>. Acesso em: 31 ago. 2020

CERT.br, Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. *Estatísticas de Incidentes Reportados ao CERT.br. 2020*. Disponivel em: <http://www.cert.br/stats/incidentes/>. Acesso em: 31 ago. 2020