Projeto final de curso

Licenciatura em Engenharia Eletrónica e Telecomunicações e de Computadores

Uso e aplicação de algoritmos criptográficos em cloud computing

Aluno: Pedro Costa (Nº49944)

Orientador: Valderi Leithardt

2º Semestre letivo 2023/2024

29 de fevereiro de 2024

Índice

1.INTRODUÇÃO **3**

2.COMO A CRIPTOGRAFIA FUNCIONA? **4**

3.PROBLEMA A RESOLVER **5**

4.DESCRIÇÃO DO PROJETO **6**

5.CALENDARIZAÇÃO **7**

REFERÊNCIAS **8**

Lista de figuras

figura 1 – Exemplo de criptografia **4**

Lista de tabelas

Tabela 1 – Calendarização do projeto **7**

1. Introdução

Primeiramente o que que é criptografia. Criptografia é um método que converte textos em códigos abstratos conhecidos como textos cifrados, o propósito da criptografia é ocultar dados sensíveis, de forma a prevenir que usuários não autorizados acessem e roubem os dados. Nos dias de hoje a maioria dos sites e aplicativos utilizam a criptografia para proteger a transmissão de dados na internet, por exemplo, plataformas de armazenamento digital de dados, como a google cloud, usam a criptografia para adicionar uma camada extra de segurança aos seus serviços. A cloud é uma rede vasta de servidores remotos em todo mundo que estão interligados, sendo usados para armazenar e gerir dados, executar aplicações ou fornecer conteúdos ou um serviço. Por outro lado, cloud computing trata-se da tecnologia que permite o acesso direto e remoto a infraestruturas e recursos informáticos.

Tendo em conta aquilo que foi dito anteriormente este projeto para final de curso de engenharia Eletrónica e telecomunicações e computadores, tem o objetivo principal de explorar e implementar algoritmos criptográficos, considerando variáveis como o tamanho de pacotes e algoritmos diversos bem como a sua utilização juntamente com a cloud. A análise desses elementos permitirá a adaptação e otimização da criptografia para ambientes específicos, levando em consideração as demandas computacionais e as restrições de recursos dos dispositivos IoT.

2. Como a criptografia funciona?

A criptografia é realizada através de uma chave criptográfica que é uma string ou uma sequência de texto. Esta chave reordena e codifica dados que inicialmente são legíveis em textos cifrados ilegíveis, portanto no processo de transmissão de dados, o usuário que está a enviar os dados utiliza uma chave para realizar a codificação dos mesmos enquanto que o usuário que recebe os dados utiliza a mesma chave para os descodificar.

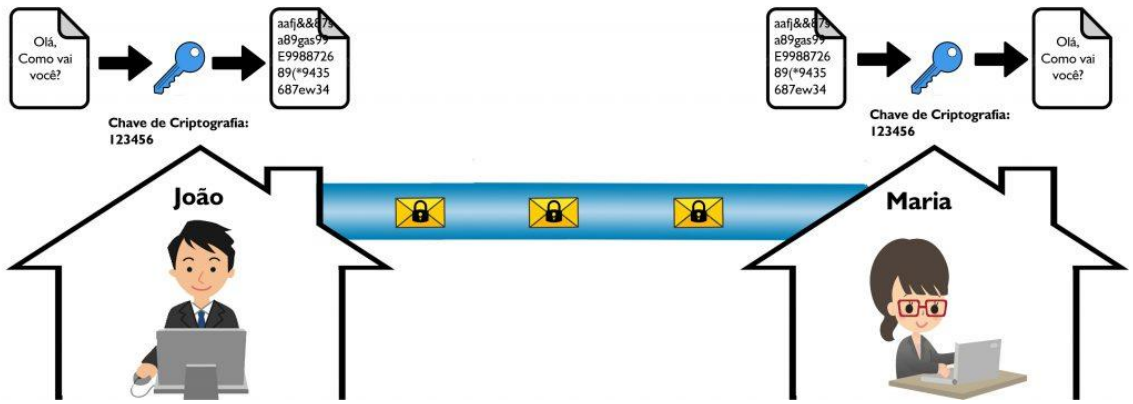

Figura 1 – Exemplo de criptografia

A força da criptografia depende do tamanho da chave utilizada, sendo esta em bits, chaves mais curtas possuem menos combinações e são menos seguras, no entanto apesar das chaves mais longas serem mais seguras, os algoritmos também cumprem um papel importante a nível de segurança.

3. Problema a resolver

A criptografia envolve a aplicação de algoritmos matemáticos complexos para proteger os dados, sendo que o tempo necessário para criptografar um pacote de dados pode depender de vários fatores, nos quais se inclui o tamanho do pacote de dados e a complexidade do algoritmo de criptografia utilizado. Caso o pacote seja muito grande o tempo de codificação será maior, especialmente se o algoritmo utilizado não for otimizado para lidar com grandes volumes de dados. Para além disso, quanto maior for complexidade do algoritmo de criptografia maior será a exigência nos recursos computacionais, como por exemplo o poder de processamento (CPU), o que influenciará no tempo de aplicação do algoritmo.

Portanto o objetivo deste projeto como será mencionado no próximo capítulo, será encontrar um conjunto de algoritmos que permitam enviar o maior tamanho de pacote de dados no menor tempo possível juntamente com a utilização de cloud computing com intuito deste ser utilizado em conjunto com uma interface que virá a ser desenvolvida para demonstração de resultados. Diferenciado de certos projetos, este utilizará a cloud invés de um local host, visto que o cloud computing oferece como vantagens, acesso a tecnologias mais avançadas, maior velocidade de processamento, maior capacidade de integração, agilidade e garantia de cópias de segurança e entre outros.

4. Descrição do projeto

No contexto da utilização da cloud, a segurança e eficiência na transmissão de dados transformam-se em elementos cruciais. Este projeto visa otimizar a transferência de dados em quatro níveis diferentes, Guest, basic, Advanced e Admin em que a criptografia deve ser realizada na forma de complexidade crescente. Esta complexidade será implementada através de um encapsulamento de criptografias, isto é por exemplo, utiliza-se primeiramente um algoritmo de criptografia e no resultado é aplicado um outro algoritmo tornando assim os dados mais seguros.

A prioridade é encontrar combinações de algoritmos que permitam enviar pacotes substanciais de forma ágil. A otimização da transferência de dados será abordada em diferentes parâmetros, como já mencionados anteriormente. O tamanho dos pacotes, no cenário das redes 5G em que os pacotes podem ir até 10 gigabytes.
O tamanho dos pacotes enviados será influenciado pelo nível que o individuo possuí, aumentando de forma crescente. Por exemplo, um Guest possui um limite de um 1 gigabyte enquanto um Admin já pode enviar o valor máximo de 10 gigabytes.

Numa primeira fase será realizada, pesquisas sobre os diferentes tipos de algoritmos criptográficos e a análise de como estes funcionam de uma forma geral, bem como a realização dos testes das diversas combinações, tendo em conta as seguintes variáveis, tamanho do pacote, tempo de encriptação e decriptação e a complexidade dos algoritmos usados.

Por último será realizado uma interface interativa, utilizando uma linguagem à escolha, a qual permitirá testar as soluções encontradas, sendo estas soluções usadas juntamente com a cloud, através de um servidor que será criado através do Microsoft Azure, habilitando que um indivíduo possa aceder a interface desenvolvida em qualquer lugar e em qualquer altura.

5. Calendarização

Atendendo à complexidade do projeto proposto é necessário aplicar uma estratégia de forma a estruturar a calendarização das diferentes tarefas a cumprir, portanto propõe-se a seguinte calendarização de tarefas, que podem vir a ser alteradas consoante o avançar do projeto.

Atividade	inicio	duração	Termino
Pesquisa sobre o projeto	15/02/2024	3	18/02/2024
Relatório inicial	26/02/2024	7	04/03/2024
Pesquisa sobre os algoritmos	26/02/2025	17	15/03/2025
Testes dos algoritmos	13/03/2024	13	26/03/2024
Relatorio intercalar e poster	26/03/2024	29	24/04/2024
Pesquisa sobre o servidor Azure	10/04/2024	3	13/04/2024
Desenvolvimento da interface	13/04/2024	7	20/04/2024
teste da interface com o servidor	20/04/2024	9	29/04/2024
Relatório final	29/04/2024	44	12/06/2024

Tabela 1 – Calendarização do projeto

Referências

[1] https://www.hostinger.pt/tutoriais/o-que-e-criptografia?ppc_campaign=google_search_generic_hosting_all&bidkw=defaultkeyword&lo=1011749&gad_source=1&gclid=CjwKCAiA3JCvBhA8EiwA4kujZluvnyaHKzCIiM1E_hcXqQ796JRsUDXfgpk-m_dzUbj5BV65vuvATxoCI84QAvD_BwE

[2] https://azure.microsoft.com/pt-pt/resources/cloud-computing-dictionary/what-is-the-cloud/

[3] https://compuworks.pt/cloud-computing-beneficios-empresas/?gad_source=1&gclid=CjwKCAiA3JCvBhA8EiwA4kujZudcr791yAuhY6uXaMVmFsawkaSvs0fPKlGo_S0EkaCTVfDxyc1efhoChygQAvD_BwE

[4] https://www.apd.pt/vantagens-e-desvantagens-do-cloud-computing/