SECRETARIA DE EDUCAÇÃO E CIÊNCIA
INSTITUTO POLITÉCNICO DE BRAGANÇA
ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO

LICENCIATURA EM ENGENHARIA DE INFORMÁTICA
6° PERÍODO

FERNANDO SOUZA FURTADO CARRILHO
JOSÉ RAFAEL SOARES BORGES

# **RELATÓRIO PRÁTICO 05**:
# SEGURANÇA NA INTERNET DAS COISAS

BRAGANÇA
2023

FERNANDO SOUZA FURTADO CARRILHO
JOSÉ RAFAEL SOARES BORGES

# **RELATÓRIO PRÁTICO 05**:
# SEGURANÇA NA INTERNET DAS COISAS

Este relatório objetiva a obtenção de nota na disciplina de Internet das Coisas dos graduandos no curso de Engenharia de Informática da Escola Superior de Tecnologia e Gestão do Insitutito Politécnico de Bragança. Seu conteúdo é composto pela observação, descrição e aplicação sobre segurança na Internet das Coisas.

BRAGANÇA
2023

# Sumário

# Lista de Figuras

# 1 SEGURANÇA NA INTERNET DAS COISAS

É fundamental a segurança das informações em meio à glabalização e aos avanços no meio tecnológico mundial. E isso, devido ao grande volume de dados transmitidos, compartilhados e acessados em milésimos de segundos, na grande rede. E diante disso vem a pergunta: como manter esses dados seguros, ou dizer que o acesso é seguro?

Nesse viés, antes de responder esta pergunta, é valido entender que com o aumento da automatização, em carros, aeronaves, casas e semelhantes, entra em questão a segurança dos dados recebidos, enviados e transmitidos nestes meios. Dessa forma, a automatização dos elementos que não tem internet e passa a ter a tratar dados, é chamado de Internet das Coisas, do inglês, Internet of Things - IoT.

Sendo assim, responde-se a pergunta acima dada, entra com a implementação da segurança, no universo digital, para a segurança dos dados envolvidos, a qual é provida de três pilares fundamentais: confidencialidade, integridade e disponibilidade. Logo, é com base nisso que se dá a apresentação de suas definições nos tópicos a seguir.

## 1.1 CONFIDENCIALIDADE DE DADOS

A confidencialidade de dados para Telium N. (2018) tem a ver com a privacidade dos dados da companhia. Para ele, o conceito da confidencialidade é intrínseco relacionada às ações tomadas para assegurar que informações confidenciais e críticas não sejam coletados indevidamente dos sistemas organizacionais.

Prontamente, compreende-se por confidencialidade, a capacidade de se reguardar de ciber-ataques, espionagem, entre outras práticas de terceiros que buscam o ganho próprio, dos dados da companhia.

## 1.2 INTEGRIDADE DE DADOS

A Integridade de dados, para Telium N. (2018), por sua vez, corresponde à preservação da precisão, consistência e confiabilidade dos dados, informações e sistemas pela companhia ao percorrer dos processos ou de seu ciclo de vida útil.

Protamente, é válido apontar que, para que exista a integridade, é indispensável ga-

rantir que os dados circulem ou sejam armazenados, do mesmo modo como foram criados, sem que exista interferência externa para corrompê-los, danificá-los ou comprometê-los.

### 1.3 DISPONIBILIDADE DE DADOS

A disponibilidade de dados, para Telium N. (2018), está intrinsecamente vinculada ao tempo e à acessibilidade que se têm dos dados e sistemas de uma companhia. Isto é, o quanto esses dados encontra-se disponíveis para serem consultados, a qualquer momento, pelos colaboradores, intermediários e/ou clientes.

## 2 DADOS CRIPTOGRAFADOS

Para se entender o universo de **Dados Criptografados**, também nomeado de **Dados Encriptados**, em primeira instância é válido compreender o significado de criptgrafia e em seguinte o motivo e o que são os dados criptografados.

A critografia, para Kaspersky (2023), é a conversão de dados de um formato legível em um formato codificado, em semântica de interpretação, com uso de lebtra, números e até simbolos, dentre outros, de tal forma em que os dados encriptados só podem ser lidos ou processados após sua descriptografia.

À vista disso, a critografia de dados serve para manter seu conteúdo, ao máximo, inelegível a qualquer indivíduo que tente acessá-lo indevidamente. Logo, o percurso comum é que os dados sejam encriptados ao ser emitido e desencriptados no destino final, para que os dados cheguem devidamente ao endereço final.

### 2.1 NODE-RED BIBLIOTECA CRYPTO-JS

Para este tópico, sua finalidade dá-se à instalação ***Node-RED-contrib-crypto-js***, em seguida subscrever ao tópico MQTT *(IPB/IoT/Lab/AirQuality/Cripto)* e verificar se é possível interpretar os dados que obtém.

Consoante, o passo seguinte é subscrever ao Tópico (Cripto/AES) para descobrir qual a *secret-key* na qual está sendo usada para criptografar a mensagem. Após, pede-se que se apresente os valores criptografados e descriptografados bem como a *secret-key* obtida e que se confira se o valor corresponde ao dado obtido do tópico *(IPB/IoT/Lab/AirQuality)*.

Dito isso, é bom apontar que a proteção dos dados é um aspeto fundamental em sistemas IoT, especialmente quando se trata de informações sensíveis, como senhas, informações pessoais, bem como o processamento de dados críticos, como o caso de sistemas de energia ou transporte.

A criptografia é uma técnica importante para garantir a segurança das comunicações, tornando os dados ilegíveis para qualquer pessoa não autorizada.

Vista geral do sistema desenvolvido no Node-Red:

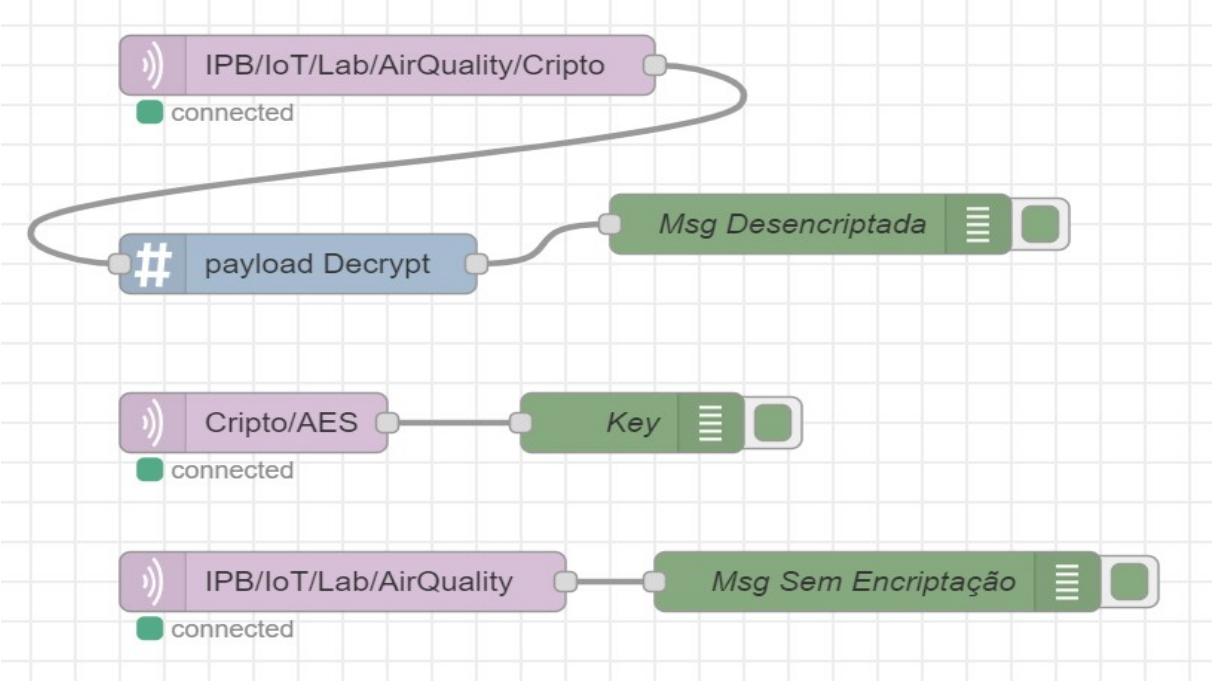


Figura 1: Esquema Node-Red

Primeiro, é necessário configurar o nó no Node-RED para subscrever o tópico "IPB/IoT/Lab/AirQuality/Cripto"para receber a mensagem que está criptografada usando o algoritmo de criptografia simétrica AES.

Este algoritmo AES, utiliza uma única chave para tanto encriptar como desencriptar os dados. Essa chave é compartilhada entre o emissor e o recetor da mensagem e deve ser mantida em segredo.

À vista disso, neste aspecto é preciso garantir que as mensagens sejam corretamente interpretadas e decodificadas, com o intuito de tal forma em que, se um terceiro interceptar a mensagem encriptada, esta incriptação o dificulte a saber sua informação.

Diante disso, para que seja possível conseguir o acesso à mensagem que chega nesse tópico (IPB/IoT/Lab/ AirQuality/ Cripto), é necessário descobrir qual a chave secreta está sendo utilizada na mensagem.

Para isso, utiliza-se o tópico “Cripto/AES”, com mostra a imagem 2 , para descobrir a secret-key utilizada para criptografar o seu conteúdo.

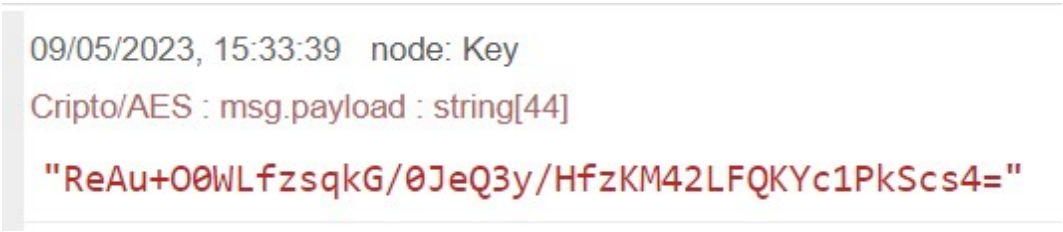


Figura 2: Chave Secreta utilizada

Com a chave secreta, utiliza-se o nó ”decrypt”do Node-RED com o algoritmo AES para desencriptar a mensagem que chega do tópico ”IPB/IoT/Lab/AirQuality/Cripto”.

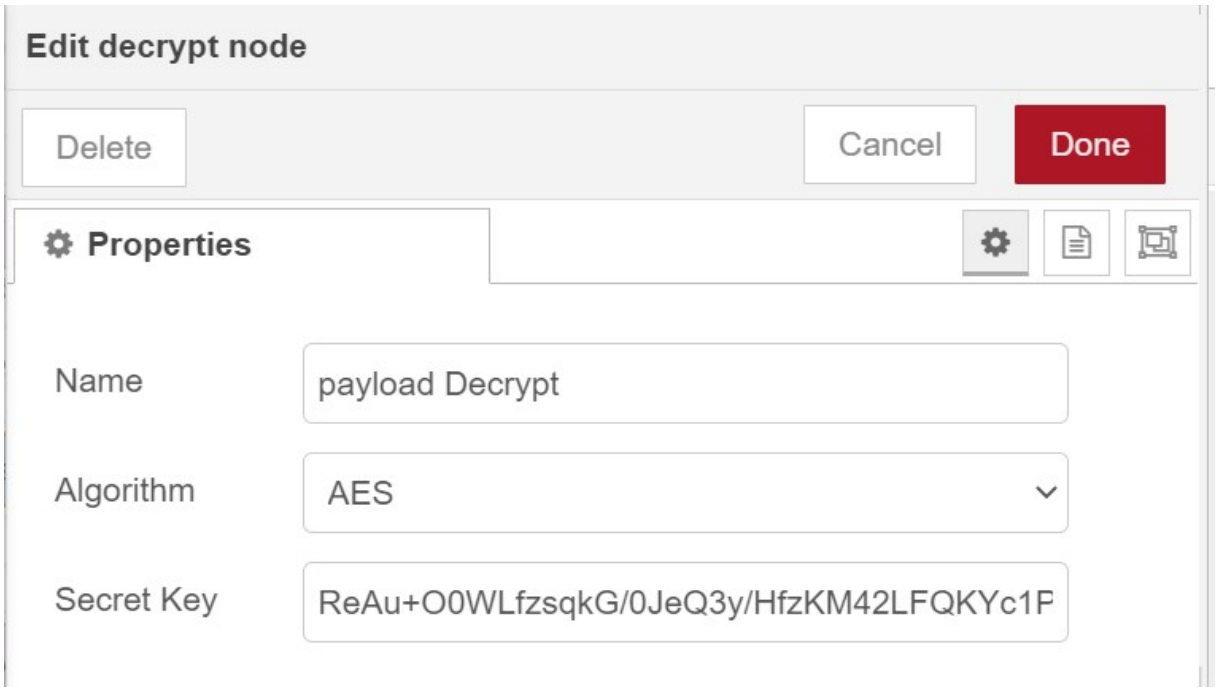


Figura 3: Configuração do nó decrypt

Depois de desencriptar e conseguir o acesso à mensagem, verificamos através da figura 4, que o valor obtido corresponde ao valor do tópico MQTT ”IPB/IoT/Lab /AirQuality”.

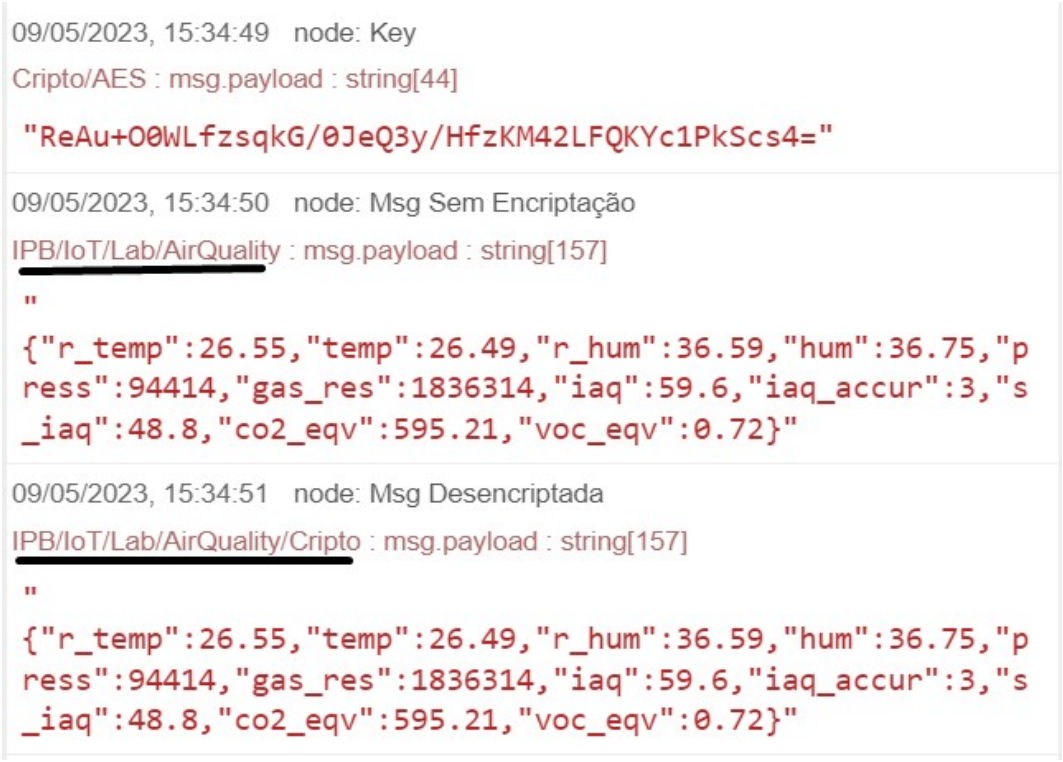


Figura 4: Valores obtidos

A implementação de um sistema de criptografia e descriptografia de mensagens utilizando a biblioteca "Node-RED-contrib-crypto-js"no Node-RED mostrou-se objetiva para garantir a segurança de comunicações em sistemas IoT. A técnica de criptografia é uma ferramenta importante para garantir a segurança de dados sensíveis e deve ser considerada em ambiente de Internet da Coisas.

## 2.2 NODE-RED BIBLIOTECA SENSE-RSA

Para esta atividade, é pedido que se instale no Node-RED a biblioteca **"sense-rsa"**, e que se crie uma chave publica, uma chave privada e que se criptografe e descriptografe uma mensagem qualquer.

Em seguida, pede-se também que se apresente qual a função da chave pública, qual a função da chave privada e o porque é uma abordagem relevante em Internet das Coisas.

Dessa forma, é com base neste contexto que o fluxo da Figura 5 expressa a forma de realizar a encriptação e descriptação de um texto, neste caso, ***Fernando Furtado***, no Node-RED.

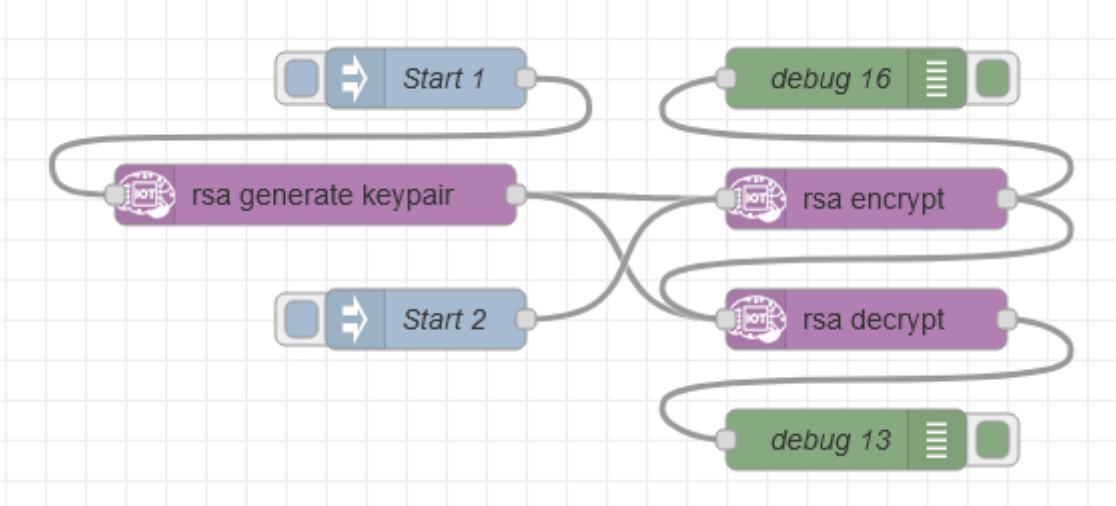


Figura 5: Fluxo de encriptação e descriptação de textos no Node-Red

Diante disso, como é visível na Figura 5, há dois nós azulados, de nomes *Start 1* e *Start 2*. Para que o fluxo acima percorra corretamente, é preciso acionar o nó *Start 1*, para que o nó *rsa generate keypair* gere as duas chaves para encriptação, chave pública e privada.

Por conseguinte, os nós seguintes, *rsa encrypt* e *rsa descrypt* recebem, respectivamente, a chave pública e chave privada. Nesse contexto, é válido apontar que é com base na chave pública que o texto é encriptado e pela chave privada que o texto é descriptado.

Feito isso, o passo seguinte é ativar o nó *Start 2*, o qual insere o texto ***Fernando Furtado***, de acordo com a Figura 6, para no nó *rsa encrypt* para ser encriptado; o texto encriptado pode ser visualizado no *debug 16*, conforme expressa a Figura 7.


Figura 6: Texto do nó *Start 2* no fluxo do Node-RED

Posto isso, diante do texto inserido no *Start 2*, da Figura 6, no *msg.payload*, o seu conteúdo é enviado ao nó *rsa encrypt* no qual o resultado, já criptografado é encaminhado ao nó *debug 16* e apresentado na Figura 7, abaixo expresso.


Figura 7: Texto encriptado no Node-RED

Paralelamente, ao ponto que o texto ***Fernando Furtado*** é encriptado, conforme é visível na Figura 7, acima apresentado, o texto sifrado, encriptado, é enviado ao nó *rsa decrypt*, o qual descriptografa o texto cifrado e envia seu resultado ao nó *debug 13*, como é expresso na Figura 8, abaixo.

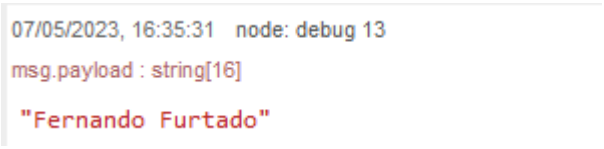


Figura 8: Texto descriptado no Node-RED

Com vista a isso, é válido apontar que ao clicar em *Start 2* e ativá-lo, no console do debug, os resultados dos debugs 16 e 13, são apresentados no console do debug instantaneamente, como expressa abaixo a Figura 6.

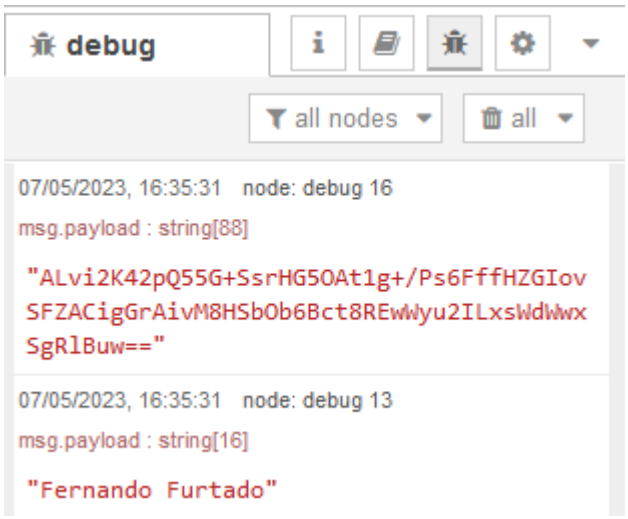


Figura 9: Saídas no Debug de encritação e descriptação no Node-RED

Ademais, com base no Fluxo da Figura 5, percebe-se que o objetivo da atividade foi

concluída, pelo fato do texto ***Fernando Furtado*** ter sido inserido, encriptado, conforme a Figura 7, e após, no destino final, descriptado.

Por fim, com base nesta atividade, percebe-se que o uso da encriptação é de fundamental importância, incluso no universo da *Internet das Coisas*, para que os dados sejam passados de um lado para o outro, origem à destino, crifrados, com o objetivo de que se um terceiro os capturar, isso o dificulte a usar os dados capturados para ganho próprio.

# Referências

[Kaspersky 2023] Kaspersky: *What is Data Encryption? Definition and explanation.* Disponível em: https://www.kaspersky.com.br/resource-center/definitions/encryption. Acesso em: 07 Mai. 2023. 2023

[Telium N. 2018] Telium N.: *Confidentiality, integrity and availability: the three pillars of information security.* Disponível em: www.telium.com.br/IoT. Acesso em: 07 Mai. 2023. 2018