Imagem gerada pelo chatGPT

A Framework for Malicious Traffic Detection in IoT Healthcare Environment

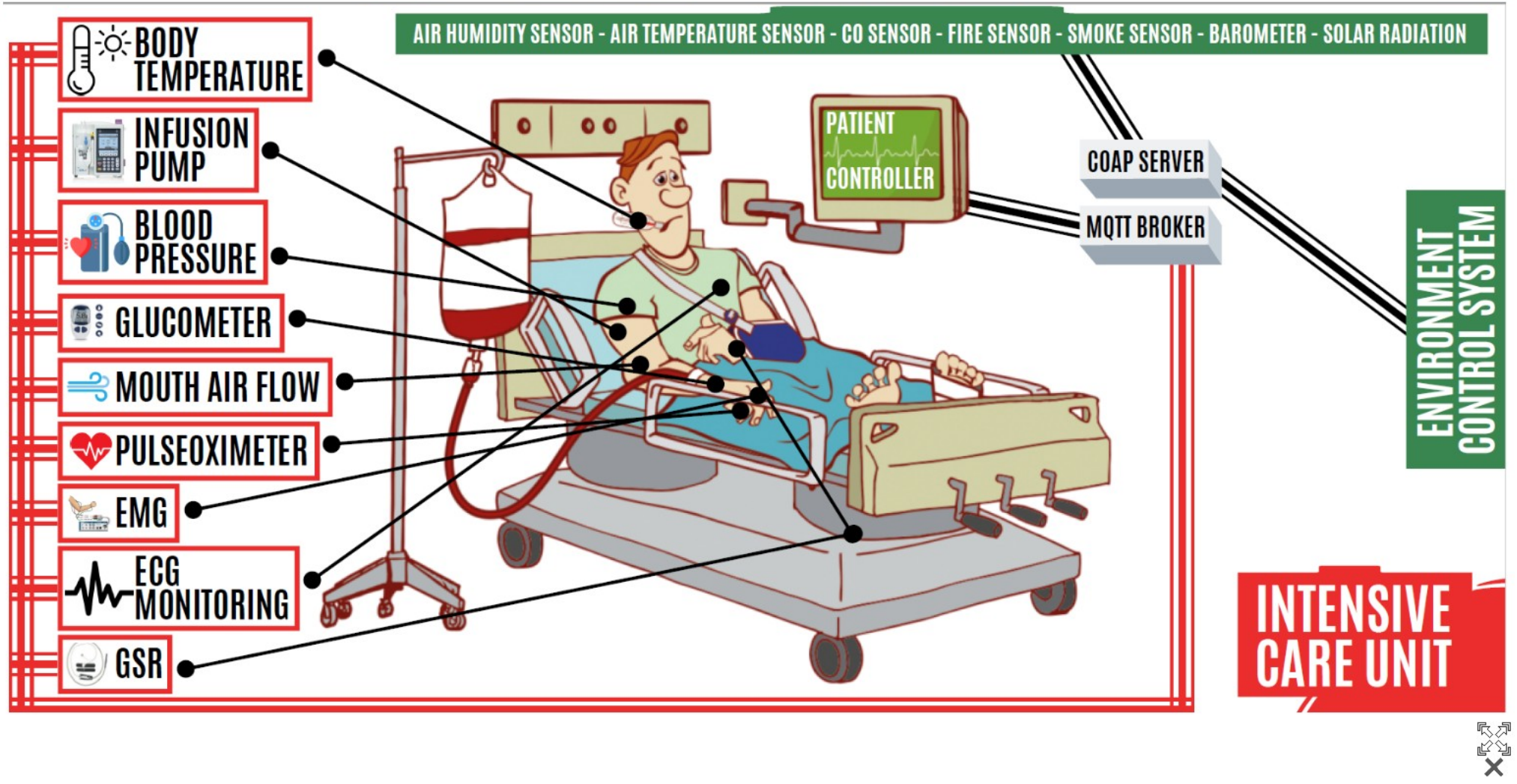
APRESENTAÇÃO ARTIGO 1

APRENDIZADO DE MÁQUINA NA SAÚDE
AUGUSTO CESAR DA F. DOS SANTOS

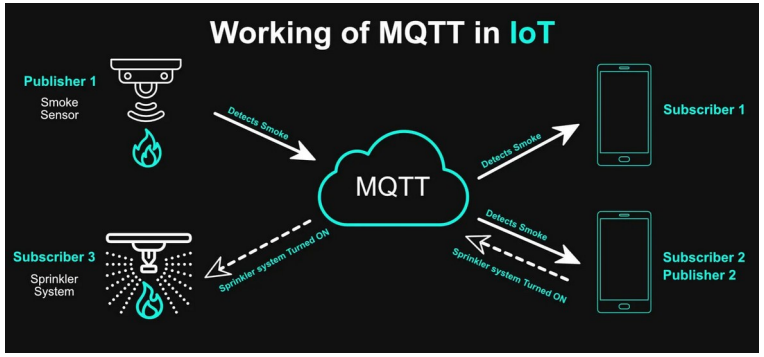
Sumário

“A fim de **dominar o mercado de IoT**, os fabricantes estão **atribuindo menos relevância à segurança dos dispositivos** [3]. Além disso, tais fabricantes criam ***backdoors*** para acessar os dispositivos remotamente para **manutenção ou para fins maliciosos**. A maioria dos dispositivos IoT implantados pelos consumidores está **conectado à rede sem nenhuma linha de defesa de segurança cibernética** [19]. Portanto, os dispositivos IoT podem ser subvertidos.”

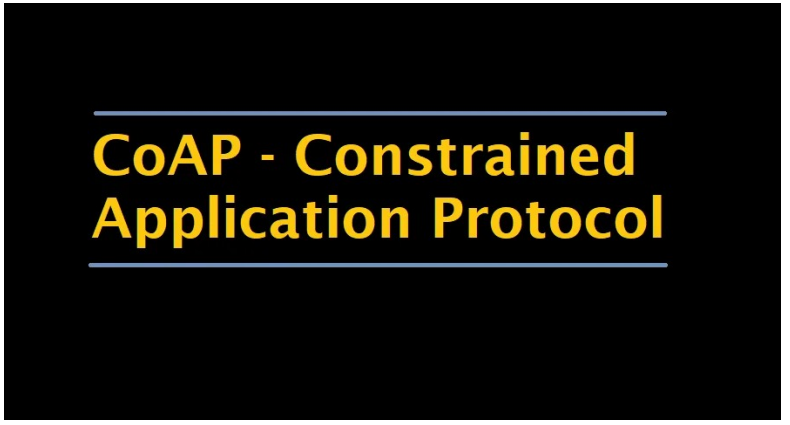
https://g1.globo.com/tecnologia/noticia/2024/10/16/hackers-invadem-aspiradores-robo-fazem-ofensas-racistas-e-observam-vitimas-pelas-cameras-diz-site.ghtml


BODY TEMPERATURE
INFUSION PUMP
BLOOD PRESSURE
GLUCOMETER
MOUTH AIR FLOW
PULSEOXIMETER
EMG
ECG MONITORING
GSR
AIR HUMIDITY SENSOR - AIR TEMPERATURE SENSOR - CO SENSOR - FIRE SENSOR - SMOKE SENSOR - BAROMETER - SOLAR RADIATION
PATIENT CONTROLLER
COAP SERVER
MQTT BROKER
ENVIRONMENT CONTROL SYSTEM
INTENSIVE CARE UNIT

https://psiborg.in/advantages-of-using-mqtt-for-iot-devices/



https://iotbyhvm.ooo/coap-protocol/



ZigBee®

https://mexico.newark.com/wireless-solutions-part-4-zigbee

Z-WAVE

https://en.wikipedia.org/wiki/Z-Wave

Bluetooth® Low Energy

Bluetooth® Classic

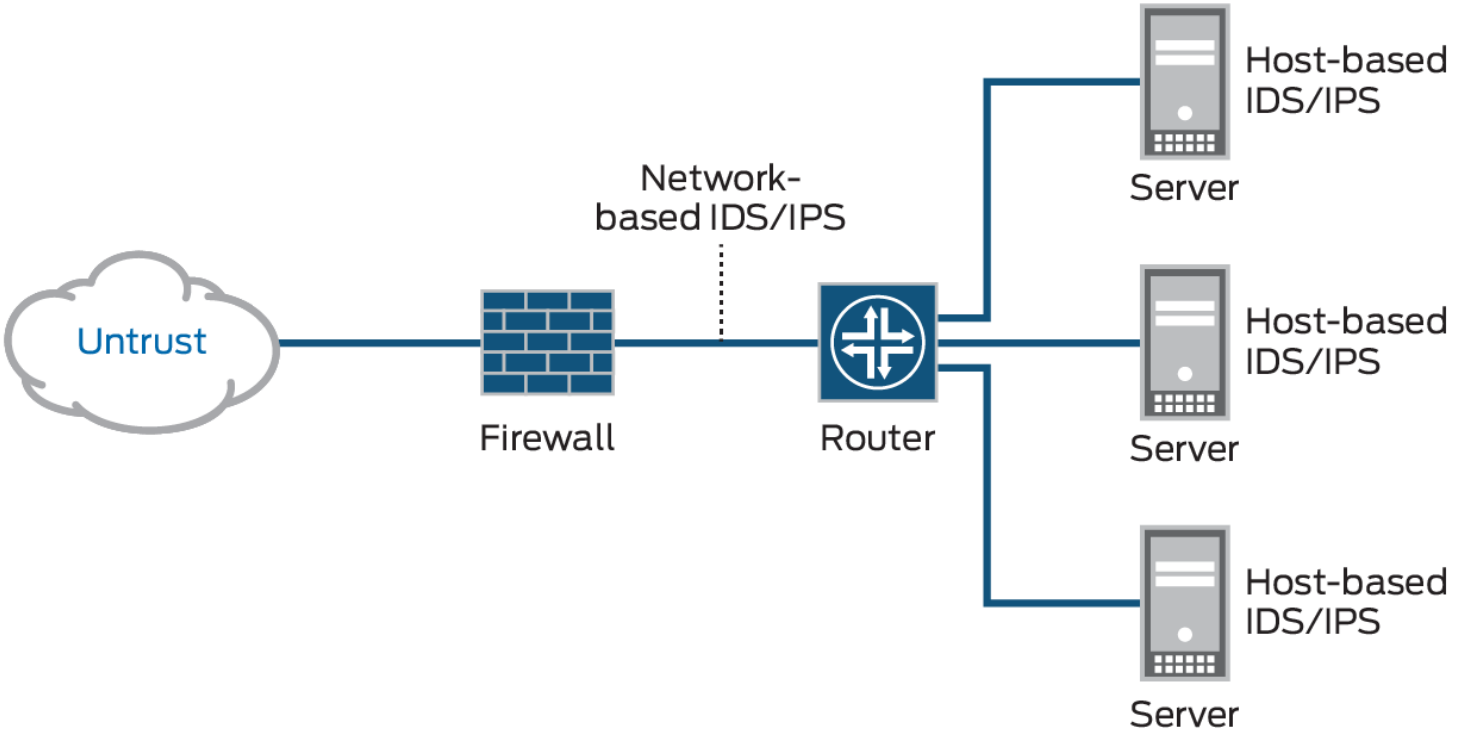
https://novelbits.io/bluetooth-low-energy-vs-bluetooth-classic-br-edr/

Wi Fi™

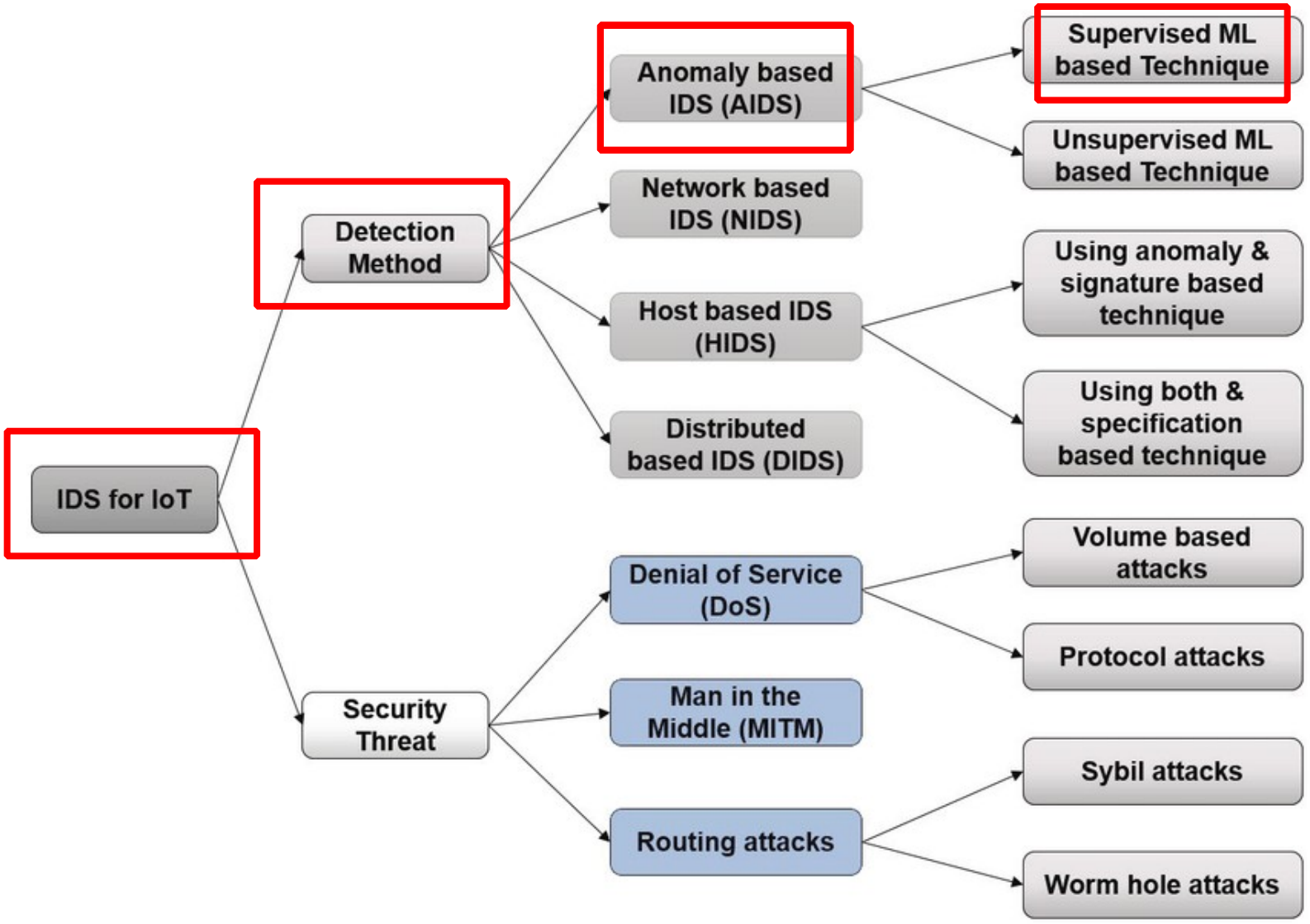
https://pt.wikipedia.org/wiki/Wi-Fi

LoRaWAN®

https://www.wattsense.com/blog/communication-protocols/what-is-lorawan/



https://www.juniper.net/br/pt/research-topics/what-is-ids-ips.html


IDS for IoT
Detection Method
Security Threat
Anomaly based IDS (AIDS)
Network based IDS (NIDS)
Host based IDS (HIDS)
Distributed based IDS (DIDS)
Denial of Service (DoS)
Man in the Middle (MITM)
Routing attacks
Supervised ML based Technique
Unsupervised ML based Technique
Using anomaly & signature based technique
Using both & specification based technique
Volume based attacks
Protocol attacks
Sybil attacks
Worm hole attacks

Motivação

63% of known exploited vulnerabilities found on healthcare networks

63% of Known Exploited Vulnerabilities Tracked by CISA are on Healthcare Organization Networks, Claroty's Team82 Finds

Report: Healthcare IoT, Devices Most Impacted by TCP/IP Vulnerabilities

IoT, Vulnerability Management

Zero-day vulnerabilities in temperature monitors could leak patient data

7 New Vulnerabilities Threaten Supply Chain, Medical Device Security

53% of Connected Medical Devices Contain Critical Vulnerabilities

IoT Malware Attack Volume Up 123% in Healthcare

Motivação

- O rápido crescimento da tecnologia **Internet das Coisas (IoT)** inaugurou o conceito de **dispositivos inteligentes, saúde inteligente, indústria inteligente, cidades inteligentes, redes inteligentes,** entre outros;
- A **segurança dos dispositivos IoT** tornou-se uma **séria preocupação**, **especialmente no domínio da saúde**, onde **ataques recentes expuseram vulnerabilidades de segurança prejudiciais** dos dispositivos IoT;
- Devido à **restrição de recursos** dos dispositivos IoT e ao **comportamento distinto dos protocolos**, os **mecanismos de segurança existentes não podem ser implantados diretamente** para proteger os dispositivos e a rede IoT contra **ciberataques;**
  - A **tecnologia IDS existente** é bem estabelecida, porém é **inadequada para redes IoT** devido à **capacidade limitada de processamento e armazenamento.**

Objetivo

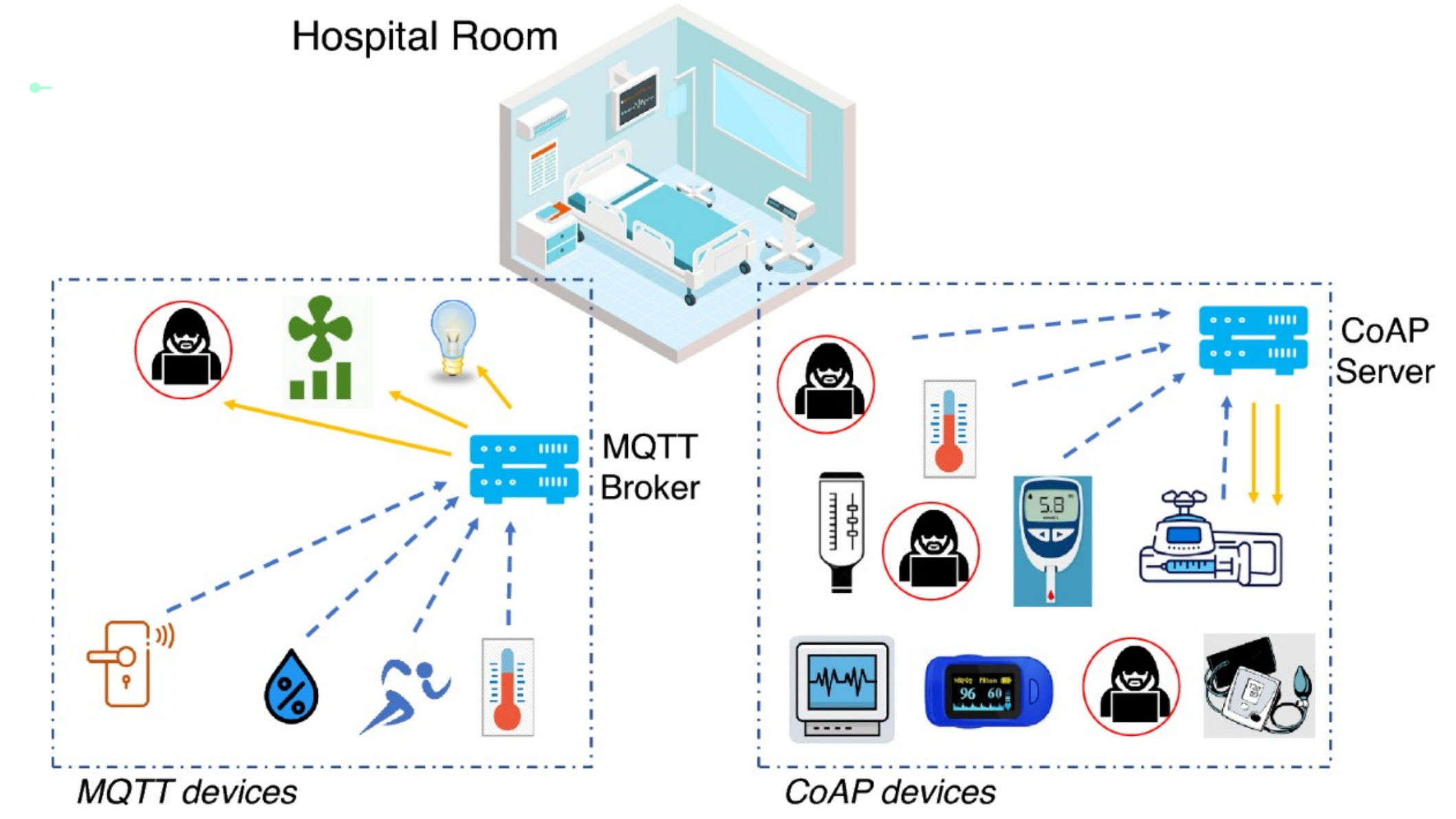
- Para **aumentar o nível de segurança para redes IoT**, são necessárias **ferramentas, métodos e conjuntos de dados específicos**;
- O **framework** proposto consiste em uma ferramenta recém-criada e de código aberto para **geração de dados IoT chamada IoT-Flock;**
- A ferramenta permite que os **pesquisadores desenvolvam casos de uso** compostos tanto por **dispositivos normais quanto maliciosos e gerem tráfego inerentes; e**
- O objetivo foi aplicar diferentes técnicas de **aprendizado de máquina (AM)** no intuito **detectar os ciberataques e proteger o sistema de saúde em** uma **Unidade de Terapia Intensivo (UTI).**

Introdução

- Em uma **UTI** é fornecido **tratamento especializado aos pacientes críticos** que necessitam de **cuidados médicos intensivos**;
- Qualquer **falha de comunicação** devido a uma **violação de cibersegurança** pode causar **efeitos graves** e até mesmo **causar morte** em alguns casos;
- Qualquer **alteração (confidencialidade e integridade) no prontuário do paciente** podem levar a uma **morte** acidental, caso não seja percebida imediatamente pelo profissional médico;
  - **Exemplo de ataque:** Atacante **altera as configurações** da **bomba de infusão de insulina** de tal forma que comece a liberar mais quantidade que o necessário, causando hipoglicemia grave.

Introdução

- Os **protocolos IoT** comumente usados, como **MQTT** e **COAP não são suportados** pelas soluções tradicionais de IDS;
- O **treinamento e teste do IDS requerem** um **conjunto de dados** gerado com **tráfego específico em tempo real** que contenha **tráfego normal** e **malicioso em um ambiente de UTI**;
- A **ferramenta IoT Flock** foi utilizada para **gerar o tráfego IoT** criando uma **rede de ataque** e uma **rede normal típica** de dispositivos;
  - Foram **extraídos perfis de dados** baseada em **análises temporais, metadados da camada de rede e de aplicação**, além de características de ***payloads***.


Hospital Room
MQTT
Broker
CoAP
Server
MQTT devices
CoAP devices

Metodologia

- **Framework proposto:**

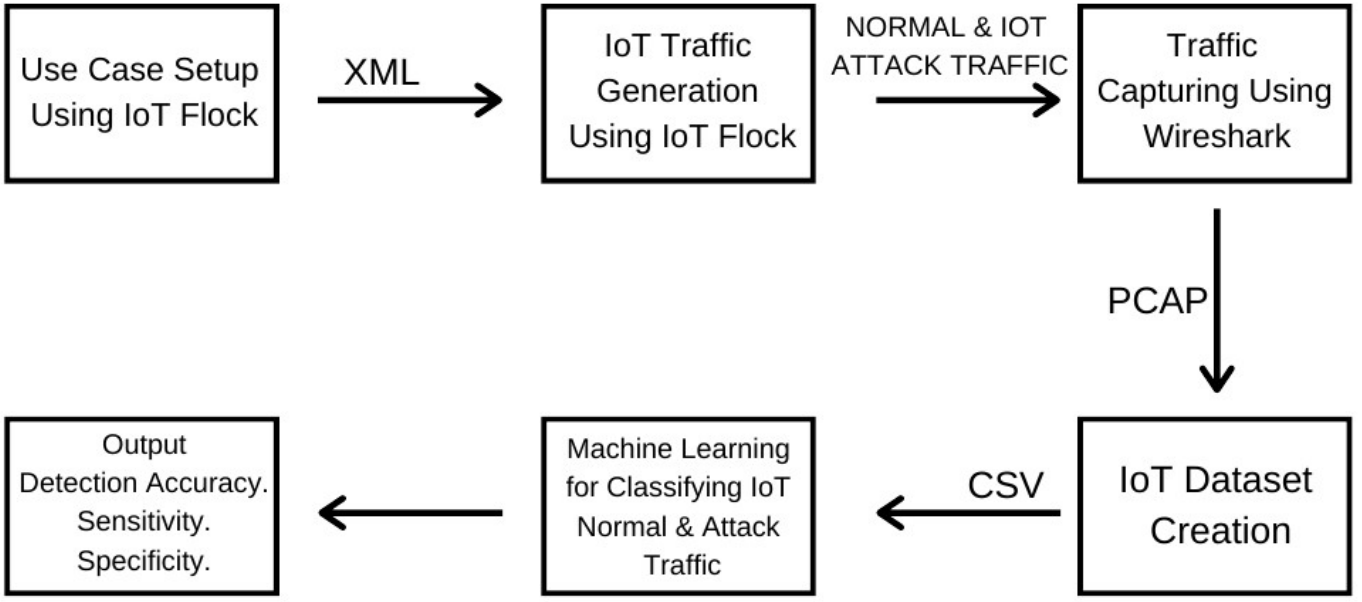


Figure 1. Framework for research in IoT health care security.

Metodologia

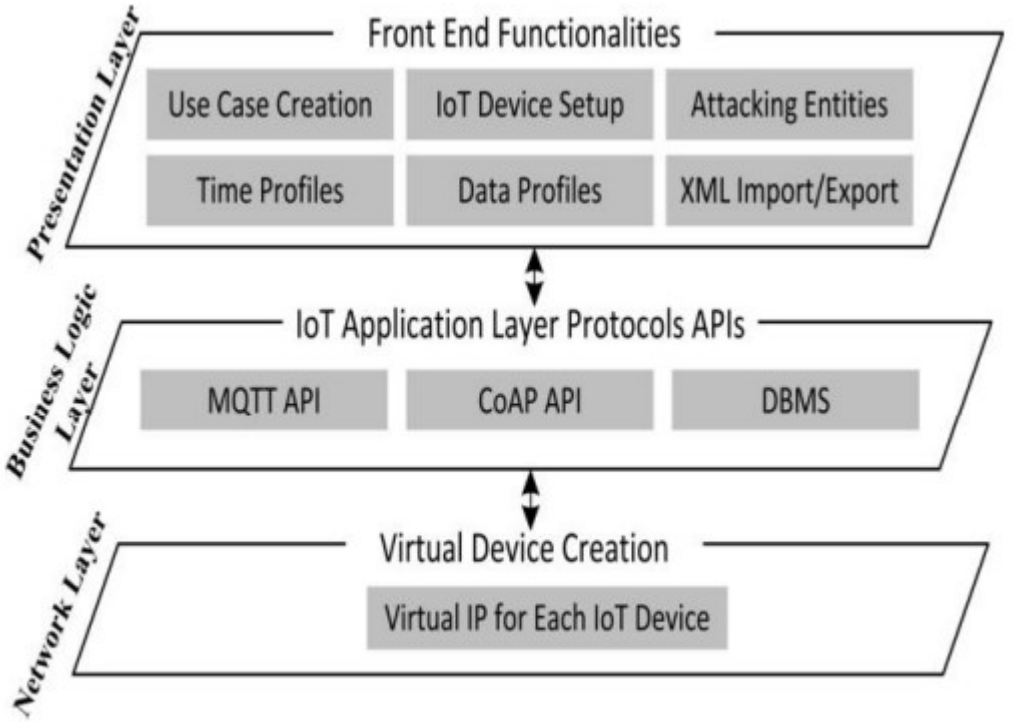


Fig. 1. Layer-wise Core Functionalities of IoT-Flock

Metodologia

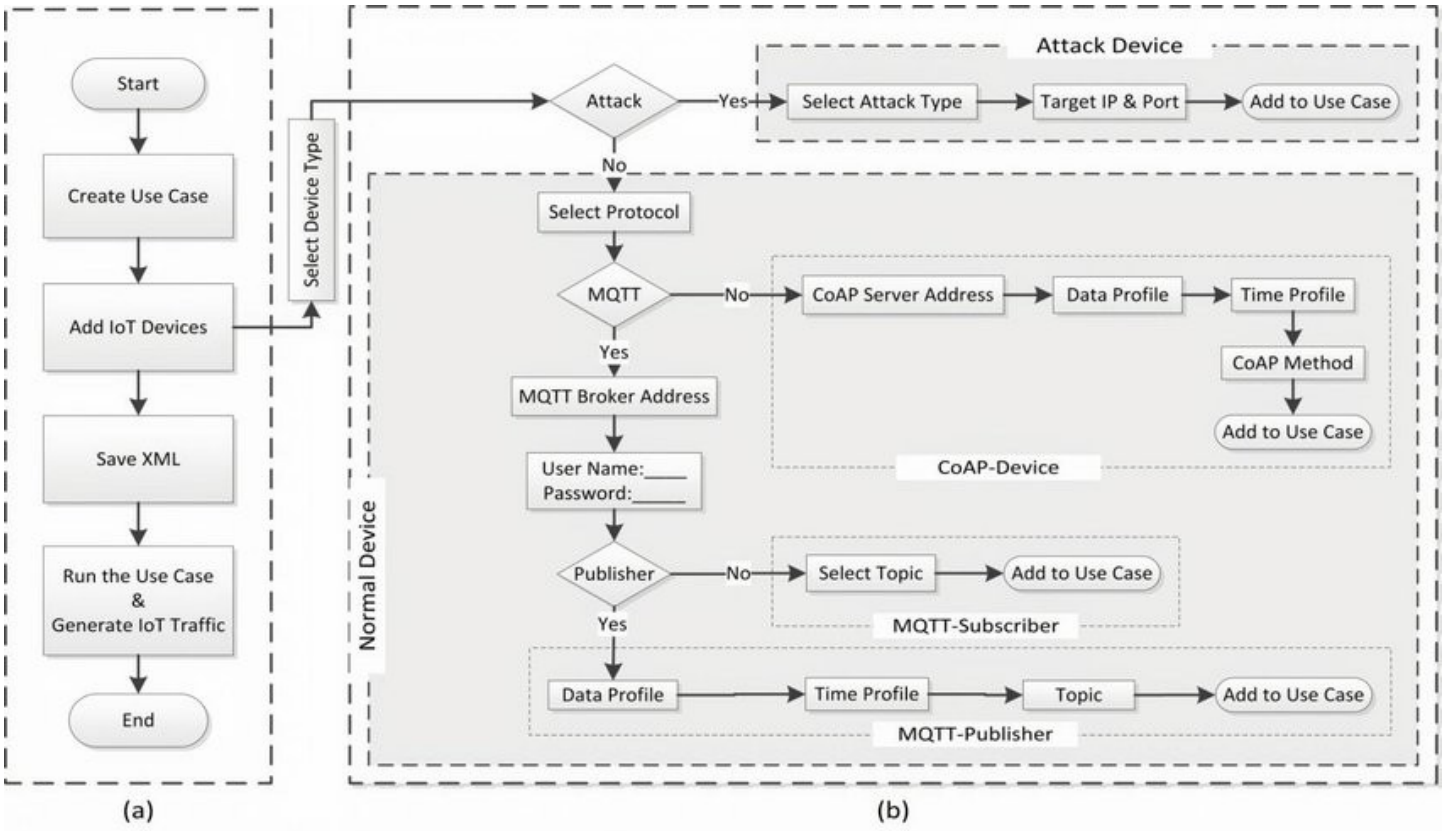


Fig. 2. Flow Diagram of IoT-Flock

Metodologia

- O IoT-Flock é **open-source**, encontra-se no **estado da arte, é escalável, flexível** e funciona nos **modos GUI** e **console**;
  - Permite a **simulação** de centenas de dispositivos e a **geração de tráfego (MQTT e COAP)**;
- Permite a **customização de cenário IoT para domínios de casos de uso reais** em uma única máquina física;
  - Com a funcionalidade de **exportação de cenários via XML** (modo console), o IoT-Flock permite que os usuários **criem e repliquem ambientes personalizados de simulação**; e
- Diferencia-se por permitir a **geração de tráfego legítimo e malicioso com anatomias de ataques específicas** para os protocolos MQTT e COAP.

Metodologia

- Os dispositivos adicionados podem **imitar o funcionamento em tempo real** provendo **informações funcionais e não funcionais** sobre cada dispositivo;
  - **Informações funcionais**:
    - Perfil **malicioso** ou **normal**, **protocolos** (MQTT e COAP), **perfil de dados** (digital ou analógico), **perfil de dados temporais** (peridódico ou randômico), **comandos e controles** (por exemplo, publish-subscriber no caso do MQTT e controle de post no caso do COAP);
  - **Informações não funcionais**:
    - **Distinção unívoca** entre dispositivos (IP, nome do dispositivo e número de dispositivos).

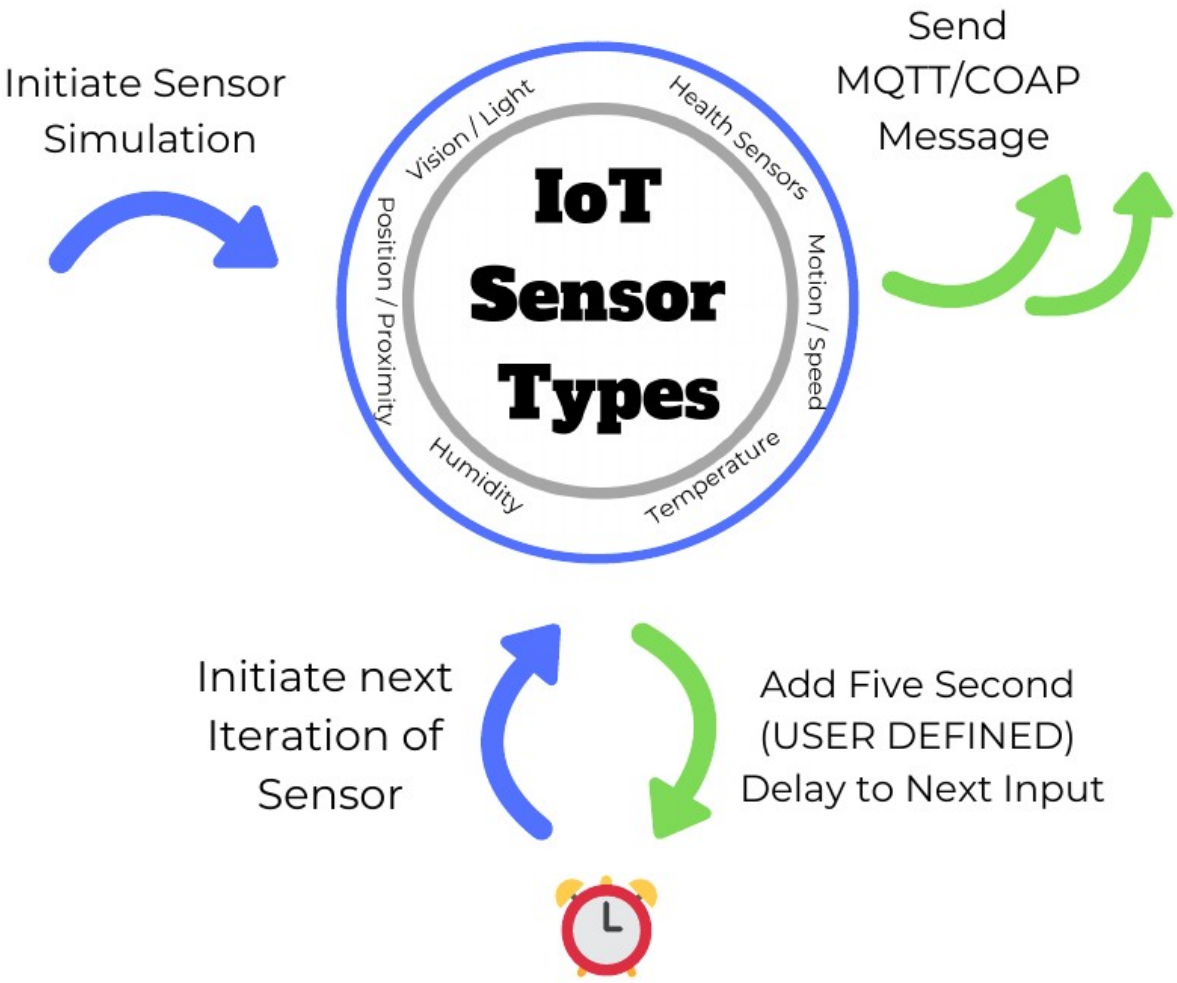


Figure 3. Time profile.

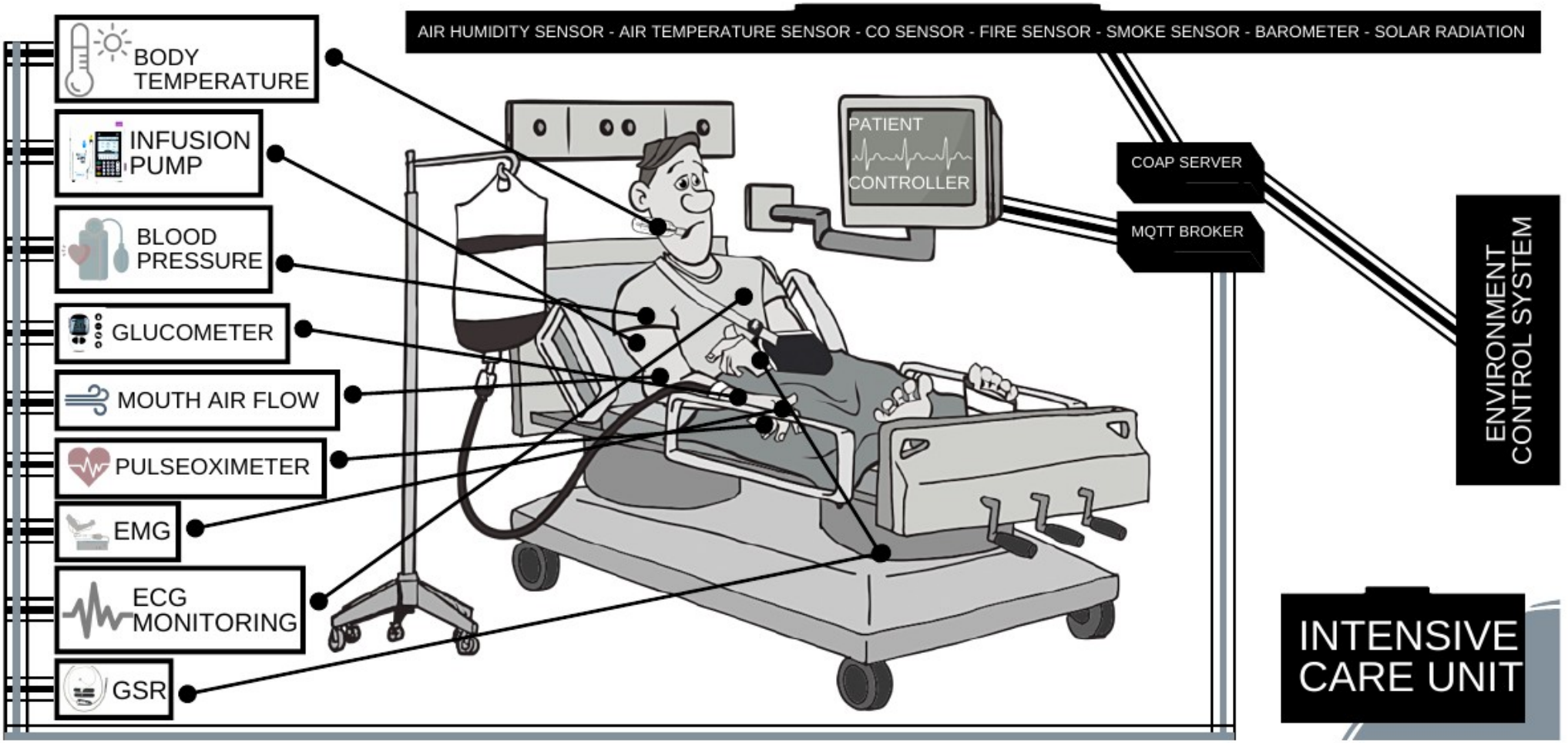


Figure 4. IoT ICU use case.

Table 1. Environment monitoring sensors.

Device Name	Description	Data Profile	Time Profile
Air Humidity Sensor	Measures the air humidity	0–100 % Rh (Relative Humidity)	5 s
Air Temperature Sensor	Measures the air temperature	−20–70 °C	5 s
CO Sensor	Measures the concentration of CO gas in Environment	0–2000 ppm	2 s
Fire Sensor	Detects the presence of fire and flame	Flame detected (0,1)	2 s
Smoke Sensor	Detects the smoke in the air	300–10,000 ppm	2 s
Barometer	Measures the atmospheric pressure	800–110 hPa	5 s
Solar Radiation Sensor	Measures the direct solar radiations by thermopile	Spectrum of radiation (0–2000 Watt/m^2)	5 s

Os dispositivos de monitoramento ambiental são usados para monitorar as condições ambientais da UTI para manter um bom ambiente na UTI.

Table 2. Patient monitoring sensors.

Device Name	Description	Data Profile	Time Profile
Remote Electrocardiogram (ECG) monitoring	Test the electrical and muscular functions of the heart	Pulse Rate (0–200 bpm)	1 s
Infusion Pump	A generic device used to deliver the nutrients and drugs to patient at a controlled amount.	Dose (10–100 mL)	10 min
Pulsoximeter (SPO2)	A device that tells the oxygen saturation (i.e., amount of oxygen dissolved) in blood	Oxygen in blood (35–100%)	1 s
Nasal/Mouth AirFlow Sensor	Provides the (breathing) respiratory rate of a patient	Device Respiratory rate (0–60 ppm peaks/min)	1 s
Blood pressure monitor Sensor	Measure the pressure of the blood in the arteries when heart beats.	systolic & diastolic pressure (0–300 mm Hg)	2 s
Glucometer	A device used to determine the amount of glucose in the blood.	Glucose in Blood (10–150 mg/dL)	10 min
Body Temperature Sensor	Measures the temperature of the body	Temperature (0–120 F)	10 min
Electro- myography (EMG) Sensor	Measures the electric potential produced by the body muscles	Muscle rate (0–60 cpm) (contractions/min)	5 min
Galvanic skin response (GSR) Sensor	Measures the electrical conductance of skin.	Conductance (0–20 uS) (micro Semens)	5 min

Os dispositivos de monitoramento do paciente são montados em partes específicas do corpo para observar a condição física do paciente.

Cenário de Caso de Uso

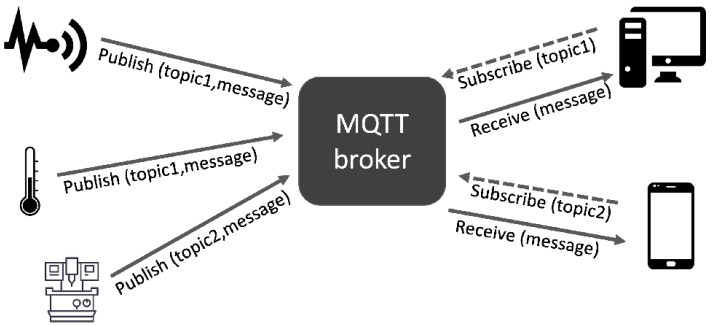
- **UTI com capacidade de dois leitos**, onde **cada leito está equipado com nove dispositivos de monitoramento de pacientes** (sensores) e **uma unidade de controle** (Unidade de controle de cama **Bedx**);
  - **x** representa o **número de cada cama**, ou seja, Unidade_de_controle_**Bed1** e Unidade_de_controle_**Bed2**; e
- A **Unidade de Controle Bedx** é responsável por **tomar ações específicas e definir limiares**, **perfil temporal de cada IoT**, a **quantidade da dose administrada ao paciente** (Ex.: bomba de infusão), **alarme de emergência** com base na condição física do paciente observada.

Cenário de Caso de Uso

- Também foi adicionada um **outra unidade de controle para dispositivos de monitoramento ambiental** chamada de **Unidade de Controle Ambiental;**
  - Responsável por **controlar as condições do ambiente da UTI,** como manter a **temperatura** específica, o nível de **umidade**, **detectar fumaça** e gerar um **alarme de emergência** em caso de condições de emergência para **manter o ambiente necessário da UTI**
- Nesse caso de uso, tanto os dispositivos de monitoramento de pacientes quanto os dispositivos de monitoramento ambiental são dispositivos baseados em MQTT;
  - O **protocolo MQTT é orientado a conexão** e garante que o pacote seja transmitido corretamente

Geração do Tráfego IoT

- A infraestrutura do ***testbed*** foi **dividida em duas redes** para desenvolver um **conjunto de dados extenso**, ou seja, uma **rede segura e uma rede atacante**;
  - **Na rede segura está o broker MQTT** implantado, além de **vários dispositivos** com o mesmo protocolo transmitindo e recebendo os dados;
  - **Na rede atacante existem entidades maliciosas** (clientes ou subscribers) originando diferentes tipos de ataques para outros clientes e para o broker;



Network sample representation of the Message Queue Telemetry Transport (MQTT) publish/subscribe approach.

Rede Segura – Tráfego Normal

- Rede projetada com a **ferramente IoT-Flock (rodando em estação Linux) populada com dispositivos MQTT de monitoramento de pacientes e do ambiente,** enviando e recebendo os dados de rede em **condições normais;**
- Para **cada dispositivo uma interface de rede virtual** foi criada pela ferramenta em uma única máquina física para intercomunicação; e
- Nesse cenário, **o broker MQTT e o COAP rodam em uma estação separada.**

Rede Atacante – Tráfego Malicioso

- Inclui **dez dispositivos atacantes** gerando **quatro tipos de ataques**, **DDoS MQTT, inundação MQTT, força bruta e ataque SlowITE** (tipo de DoS);
- **Outros** exemplos de **ataques suportados** pelo IoT-Flock:
  - **MQTT Publish Flood;**
  - **MQTT Authentication Bypass Attack;**
  - **COAP Replay Attack;**
  - **MQTT Packet Crafting Attack; e**
  - **COAP Replay Attack.**

Captura de tráfego

- Utilização do **Wireshark** para capturar o tráfego de rede;
- **Utilitário Python** para **rastreio dos pacotes e extração** da camada de aplicação recursos dos arquivos .pcap;
- Utilização da **biblioteca tshark** para **extração dos cabeçalhos da camada de rede, aplicação e payloads**;
  - Salvos posteriormente em formato CSV com **rótulos relevantes** para aplicação dos modelos de AM;

PDU	MODELO OSI	PROTOCOLOS
DADOS	APLICAÇÃO	HTTP, SMTP, FTP
DADOS	APRESENTAÇÃO	ASCCI, MPEG, JPEG
DADOS	SESSÃO	SSH, SAP, SDP
SEGMENTO	TRANSPORTE	TCP, UDP, SPX
PACOTE	REDE	IP, IPX, ICMP
FRAME	ENLACE	ETHERNET, FDDI
BITS	FÍSICA	MODEM, CABO DE REDE

Desenvolvimento do Modelo com AM

- O módulo de desenvolvimento de modelos de AM consiste em **três etapas principais:**
  - **Pré-processamento do conjunto de dados;**
    - O conjunto de dados foi criado capturando o tráfego no formato pcap, posteriormente convertidos em CSV usando um script python;
  - **Seleção de características;**
    - Foi aplicada Regrssão Logística (LR) para **selecionar as dez características mais significativas para treinar e testar** os modelos; e
  - **Treinamento e teste de modelos de ML;**
    - O modelos de AM utilizados foram: **Naive-Bayes, KNN, Random Forest, LR e árvores de Decisão.**

Resultados

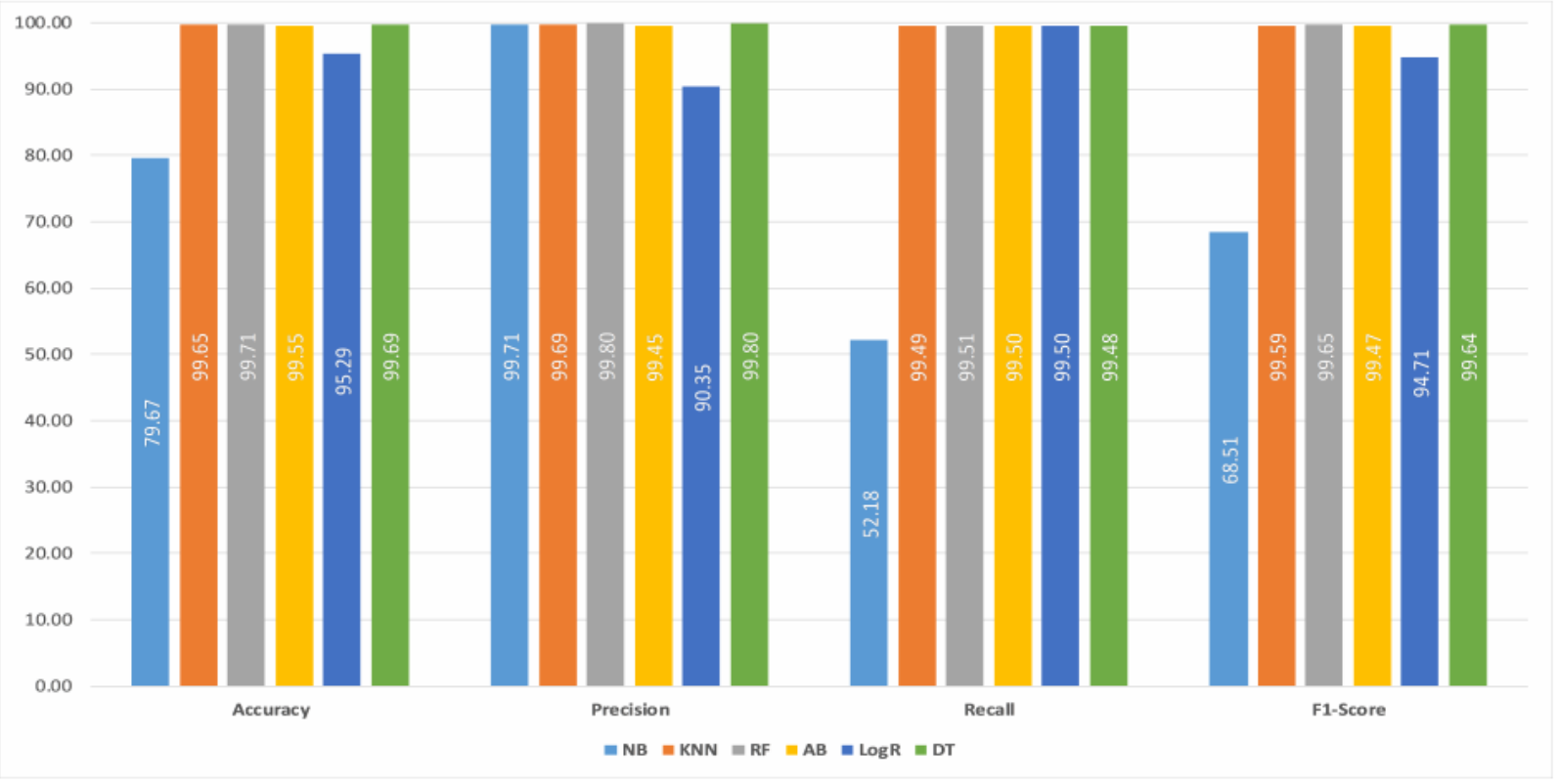


Figure 6. Performance comparison of six commonly used machine learning classifiers for malicious traffic detection over IoT healthcare dataset.

Oportunidades de Pesquisa

- **Desenvolvimento de mais modelos de Detecção de Intrusão** utilizando novas tecnologias como **computação hiperdimensional (HDC)** e outros modelos de **redes neurais** (RNN) e **redes neurais profundas** (DL);
- **Envidar esforço significativos através de mais pesquisas para defesa** dos protocolos da camada de aplicação IoT (COAP, MQTT) contra ataques DDoS;
  - A **principal razão** por trás da falta de atenção é a **indisponibilidade de conjuntos de dados de IoT** sobre o **tráfego de ataques na camada de aplicação de IoT; e**
- Portanto, **com esse framework é possível desenvolver cenários de detecção de intrusão para diferentes ambientes IoT**, além do domínio da saúde.

Conclusão

- O rápido **avanço da tecnologia IoT** tem concentrado a atenção de pesquisadores e técnicos no design de sistemas de saúde IoT;
- Muitos sistemas de saúde IoT foram propostos nos últimos anos, **porém muitos enfrentam vulnerabilidades de segurança;**
- A segurança dos sistemas de saúde IoT é crucial, pois **qualquer violação de segurança ou ciberataque pode ter um efeito mortal na vida humana;**
- Em virtude disso, **foi proposta uma estrutura para desenvolver um Sistema de Detecção de Intrusão em ambientes de saúde, o IoT-Flock**.

Referências

[1] - Hussain, F.; Abbas, S.G.; Shah, G.A.; Pires, I.M.; Fayyaz, U.U.; Shahzad, F.; Garcia, N.M.; Zdravevski, E. A Framework for Malicious Traffic Detection in IoT Healthcare Environment. Sensors 2021, 21, 3025. https://doi.org/10.3390/s21093025

[2] Ghazanfar, Syed & Hussain, Faisal & Rehman, Atiq & Ubaid, Usama & Shahzad, Farrukh & Shah, Ghalib. (2020). IoT-Flock: An Open-source Framework for IoT Traffic Generation. 10.21203/rs.3.rs-20786/v1.

[3] Sicato, Jose & Singh, Sushil Kumar & Rathore, Shailendra & Park, Jong. (2020). A Comprehensive Analyses of Intrusion Detection System for IoT Environment. Journal of Information Processing Systems. 16. 975-990. 10.3745/JIPS.03.0144.

[4] Vaccari I, Aiello M, Cambiaso E. SlowITe, a Novel Denial of Service Attack Affecting MQTT. Sensors (Basel). 2020 May 21;20(10):2932. doi: 10.3390/s20102932. PMID: 32455752; PMCID: PMC7285273.

Fontes

https://www.techtarget.com/healthtechsecurity/news/366593999/63-of-known-exploited-vulnerabilities-found-on-healthcare-networks

https://mqtt.org/

https://coap.space/

https://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2022_2/grupo_13/


IOT
IOT
IOT