VI Simpósio de Iniciação Científica 2023
Ciência como ferramenta de transformação da sociedade

Análise de Vulnerabilidades em Redes IoT e Soluções no Contexto da IoMT

Ronys Wellington Rodrigues de Santana[1] (IC), Otávio de S. M. Gomes (PQ)[1]
[1]*Universidade Federal de Itajubá (UNIFEI).*

Palavras-chave: Segurança, Internet das Coisas Médicas, IoMT, vulnerabilidades, dispositivos médicos.

Introdução

Objetivo: apresentar maneiras eficazes de proteção de dados sensíveis na área da IoT e IoMT. A saúde é uma área fundamental de qualquer nação e nos dias atuais testemunhamos grandes avanços nesse setor. Técnicas e dispositivos de tecnologia foram desenvolvidos com o objetivo de melhorar o bem-estar físico e mental dos indivíduos. Com o crescimento populacional, aumento da longevidade, avanço das tecnologias médicas e a tendência de digitalização dos negócios, as organizações de saúde precisam se adaptar às novas condições[1]. A tecnologia desempenha um papel crucial nos hospitais, seja auxiliando em cirurgias ou acompanhando de perto a recuperação dos pacientes por meio de dispositivos "vestíveis" também conhecidos como wearables. No entanto, a crescente adoção da IoT na área médica também traz consigo desafios significativos em termos de segurança. A IoMT vem sendo cada vez mais alvo de ataques cibernéticos e o setor de saúde não está imune a essa realidade preocupante. De acordo com a HIPAA (Health Insurance Portability and Accountability Act)[2] os ataques a sistemas de saúde aumentaram 60% no ano de 2022. Esses ataques podem resultar em sérias consequências comprometendo a confidencialidade, integridade e disponibilidade dos dados e sistemas médicos, dados apresentados em seu site oficial.

Um exemplo alarmante das vulnerabilidades na Internet das Coisas Médicas foi revelado por um estudo conduzido pelo site UNIT-42. Nessa pesquisa foi constatado que 52% das bombas de infusão analisadas apresentavam vulnerabilidades classificadas como críticas[3].

Vulnerabilidades encontradas: estouro de buffer baseado em pilha, estouro de buffer baseado em heap, restrição inadequada de operações dentro dos limites de um buffer de memória, condição de corrida, injeção de argumento, dereferência de ponteiro nulo[4]. Essas brechas de segurança podem ser exploradas por indivíduos mal-intencionados com o intuito de acessar, controlar ou até mesmo interromper dispositivos médicos vitais para a saúde e segurança dos pacientes.

Diante desse contexto, é crucial dedicar atenção adequada às questões de segurança dos dados pessoais e sistemas médicos.

Metodologia

Neste artigo, foi conduzida uma análise de dados seguindo uma abordagem de revisão sistemática de literatura nas bases de dados: IEEE, no site ResearchGate e artigos com as palavras-chave cibersegurança em sistemas médicos (IoMT) e cibersegurança em internet das coisas (IoT), visando compreender as necessidades de segurança desses ambientes. Primeiramente, foram examinados artigos relacionados às falhas conhecidas em redes IoT identificando as ameaças mais comuns e suas implicações. Em seguida, uma investigação detalhada foi realizada para explorar os tipos de tecnologias empregadas na (IoMT). Essa análise permitiu uma compreensão aprofundada das especificidades e desafios de segurança na IoMT.

Resultados e discussão

A Internet é um sistema global de redes de computadores interconectadas que utilizam o conjunto padrão de protocolos da Internet (TCP/IP) para atender bilhões de usuários em todo o mundo. É uma rede de redes que consiste em milhões de redes privadas, públicas, acadêmicas, empresariais e governamentais, de âmbito local a global, que estão ligadas por uma ampla gama de tecnologias de redes eletrônicas, sem fio e ópticas [5].

Esse mecanismo tem sido utilizado em diversos setores, como o mercado financeiro, redes domésticas, casas inteligentes, e até mesmo redes internas de empresas. Dentro de um ambiente clínico-hospitalar, surge a Internet das Coisas Médicas (IoMT). Essa abordagem engloba uma rede que pode conter dispositivos de diferentes camadas de aplicação, desde sensores de monitoramento até máquinas de ressonância magnética e servidores que gerenciam os acessos dos usuários. De acordo com Matt Hatton o número de dispositivos de Internet das Coisas (IoT) continua aumentando. Até o final de 2030, o número de conectados espera-se que os dispositivos atinjam 24,1 bilhões, em comparação com cerca de 500 milhões de dispositivos em 2003, o que corresponde a cerca de 3,47 dispositivos IoT por pessoa [6], [7]. Um estudo da NOKIA revelou que em 2020, a taxa média mensal de infecção em redes móveis foi de 0,23%. Em fevereiro e março, no entanto, a taxa mensal de infecção móvel aumentou quase 30% em relação ao ano anterior nesses mesmos meses, em grande parte devido à escalada significativa de incidentes de segurança cibernética relacionados à pandemia do covid-19. Os dispositivos IoT são agora responsáveis por 32,72% de todas infecções observadas em redes móveis, que está acima de 16,17% em 2019, esta tendência está alinhada com o crescimento do número de dispositivos IoT que agora estão conectados a redes móveis[8].

A jornada do paciente é um termo que se refere à experiência do paciente ao longo de um episódio de atendimento, começando na admissão e terminando com a alta hospitalar[9], essa jornada segue várias etapas, incluindo consultas médicas, diagnóstico, tratamento hospitalar, cuidados pós tratamento e acompanhamento de saúde a longo prazo. Comunicação clara e apoio contínuo dos profissionais de saúde para garantir que os pacientes recebam a melhor atenção médica possível e tenham uma experiência positiva.

Através do estudo dos artigos foi possível identificar algumas práticas e ferramentas que podem atuar na manipulação e no monitoramento dos dados sensíveis das redes na questão da cibersegurança.

Camadas da rede IoMT

Uma classificação bastante utilizada no contexto da IoMT foi apresentada no artigo intitulado "A Survey: To Govern, Protect, and Detect Security Principles on Internet of Medical Things (IoMT)" [10]. Essa classificação divide os dispositivos com base em sua camada de aplicação. São elas:

1. Camada de coleta de dados: Nesta camada estão presentes os sensores responsáveis por coletar os dados dos pacientes.
2. Camada de gerenciamento de dados: Essa camada diz respeito ao armazenamento dos dados coletados.
3. Camada de serviço médico: Essa camada envolve as aplicações que permitem que os médicos se conectem aos seus pacientes para orientação ou em casos de emergência.

Através dessa classificação é possível saber onde estão os dados mais sensíveis para o seu sistema para aplicar um método de gerência de dados mais adequado, existem vários tipos de abordagem para os dados chamados de “soluções IoMT”, é possível utilizar o framework IoMT-SAF para auxiliar na escolha dessa solução.

IoMT-SAF (Security Assessment Framework)

Alsubaei em um estudo realizado em 2019 apresenta o IoMT-SAF (Security Assessment Framework) que desempenha um papel fundamental na garantia da segurança na Internet das Coisas Médicas (IoMT)[11]. Este framework, projetado para avaliar a segurança, privacidade e recomendações na rede IoMT, é uma ferramenta que tem como foco melhorar a qualidade dos cuidados médicos prestados tanto a pacientes quanto a profissionais de saúde.

Este framework é uma aplicação web desenvolvida em Python e oferece aos usuários a capacidade de avaliar a segurança das soluções IoMT, personalizando sua análise de acordo com o contexto específico de uso. Para atingir esse objetivo, o IoMT-SAF é dividido em dois módulos principais: o módulo de recomendação e o módulo de avaliação.

O módulo de recomendação funciona fornecendo uma lista de medidas de segurança recomendadas para cada cenário de uso da IoMT.

Isso permite que os usuários obtenham orientações valiosas sobre como proteger suas soluções em diferentes contextos.

Enquanto isso, o **módulo de avaliação** permite que os usuários realizem uma análise aprofundada da segurança de suas soluções IoMT. Isso é feito comparando as medidas de segurança implementadas com as recomendações fornecidas pelo framework. Assim, os usuários podem avaliar com eficácia o nível de segurança de suas soluções.

O IoMT-SAF utiliza uma abordagem orientada a stakeholders, o que significa que leva em consideração os diferentes atores envolvidos na IoMT, cada um com suas próprias responsabilidades e requisitos de segurança, isso ajuda a identificar problemas de segurança específicos para cada cenário e a recomendar contramedidas adequadas. Para avaliar o grau de segurança nas soluções IoMT, o IoMT-SAF emprega um método de avaliação quantitativa baseado no Processo Hierárquico Analítico (AHP). Essa abordagem oferece flexibilidade aos usuários, permitindo que comparem as soluções IoMT com base em sua segurança geral e em componentes específicos.

Sistema de Detecção de Intrusão IDS

Um Sistema de Detecção de Intrusão (IDS) monitora e analisa o tráfego malicioso para proteger os dispositivos de vários ataques . Em um ambiente IoT e sensores sem fio, o IDS verifica o tráfego de entrada e procura por invasões, se uma intrusão for identificada, o mecanismo apropriado é implantado para tomar a ação apropriada. O IDS pode ser dividido nas seguintes categorias [11]:

- Sistema de detecção de intrusão baseado em rede (NIDS): usado em uma rede para a prevenção e detecção de diferentes ataques à rede. Ele monitora toda a rede fazendo uma análise das atividades na rede.
- Sistema de detecção de intrusão baseado em host (HIDS): usado para monitorar um único host em busca de sinais de atividades maliciosas e analisar as atividades dentro do host.

Para que o IDS seja eficaz, deve-se garantir que não introduza novos pontos fracos, deve ser projetado de forma a exibir menos custos de computação e comunicação, deve ser confiável o suficiente para produzir menos números de falsos positivos e falsos negativos. Os IDS podem ser divididos em três grupos [12]:

- Detecção baseada em anomalias: baseada em métodos estatísticos de comportamento. Dois tipos de fluxos são definidos sob este, fluxo normal e anormal. Qualquer desvio do fluxo normal é detectado como uma anomalia. Esta é uma forma precisa e consistente de detecção com menos falsos negativos e positivos. Isso é perfeito para taxas desconhecidas, no entanto, o perfil para atividades normais precisa ser atualizado regularmente, pois as alterações ocorrem diariamente.
- Detecção baseada em uso indevido: também conhecida como baseada em regras ou baseada em assinatura. A assinatura de um ataque é gerada quando ele acontece, que é usada para detectar ataques futuros. Este método é perfeito para detectar ataques conhecidos com baixas taxas de falsidade.
- Detecção baseada em especificação: define as restrições e especificações que descrevem a exatidão do processo de detecção. O comportamento da rede é monitorado com base nas especificações e restrições. Essa técnica combina as vantagens da detecção baseada em anomalias e uso indevido, usando especificações e restrições desenvolvidas manualmente para identificar o comportamento anormal, com baixas taxas de falsos positivos. Essa técnica detecta ataques conhecidos e desconhecidos, mas pode ser demorada.

Com base nas informações coletadas, o artigo apresenta soluções e estratégias de segurança relevantes para abordar as vulnerabilidades identificadas em ambientes IoT, com foco especial na proteção de dispositivos e sistemas na área da saúde. As recomendações e abordagens propostas têm o objetivo de melhorar a integridade, confidencialidade e disponibilidade dos dados e sistemas em redes IoT e, ao mesmo tempo, garantir a segurança dos dispositivos e pacientes na IoMT.

Neste estudo, foi evidenciada a crescente necessidade de implementar medidas de segurança rigorosas para proteger redes de Internet das Coisas

Médicas (IoMT), a análise revelou que, devido à ampla adoção de diversos dispositivos e tecnologias de comunicação no contexto da IoMT, surgem desafios significativos em termos de segurança como apresentado no artigo[13].

Também é importante destacar que, embora existam ferramentas essenciais como o framework IoMT-SAF e o Sistema de Detecção de Intrusão (IDS), projetadas para melhorar a segurança e organização dos Smart Hospitals, a dinâmica da tecnologia na área médica evolui rapidamente. Conforme evidenciado no estudo "The Internet of Things How the Next Evolution of the Internet Is Changing Everything" [6][7], o cenário da Internet das Coisas Médicas (IoMT) continua a se expandir de forma exponencial. Essa rápida evolução apresenta desafios constantes para a manutenção da segurança em ambientes clínicos e hospitalares, tanto no espaço cibernético quanto fora dele.

A integração de dispositivos médicos e a coleta de dados sensíveis de pacientes tornam as redes IoMT alvos atrativos para ameaças cibernéticas. Com a proliferação dessas tecnologias, torna-se crucial estabelecer regras e diretrizes rigorosas de segurança para mitigar riscos potenciais.

Portanto, é fundamental que as instituições de saúde estejam sempre atualizadas e adotem uma abordagem proativa em relação à segurança, mantendo-se informadas sobre as mais recentes tendências e ameaças tecnológicas.

Conclusões

Conclui-se que a segurança em redes IoMT deve ser uma prioridade, dada a sua relevância para a qualidade da assistência médica e a proteção dos dados pessoais dos pacientes. As soluções propostas devem abordar as vulnerabilidades identificadas e garantir que os dispositivos e sistemas na IoMT sejam resilientes a ameaças cibernéticas.

Agradecimentos

Gostaria de expressar minha profunda gratidão às seguintes pessoas e instituições que desempenharam papéis fundamentais no desenvolvimento deste trabalho:

O professor Otávio de S. M. Gomes, meu orientador, pela orientação dedicada, insights valiosos e pelo constante apoio ao longo deste projeto.

Ao CNPq (Conselho Nacional de Desenvolvimento Científico e Tecnológico), pelo financiamento e apoio a esta pesquisa.

À Universidade Federal de Itajubá (UNIFEI), instituição à qual sou vinculado, por fornecer o ambiente acadêmico e os recursos necessários para a realização deste estudo.

Referências

[1] Solic. (2019). Awareness About Information Security And Privacy Among Healthcare Employees.

[2] Alder. (2017). 87% of Healthcare Organizations Will Adopt Internet of Things Technology by 2019. Thew HIPAA Journal, página. Disponível em: <https://www.hipaajournal.com/87pc-healthcare-organizations-adopt-internet-of-things-technology-2019-8712/> Acesso realizado em: Set/23.

[3] Das. (2/03/2023). Know Your Infusion Pump Vulnerabilities and Secure Your Healthcare Organization, UNIT 42, página. Disponível em:<https://unit42.paloaltonetworks.com/infusion-pump-vulnerabilities/>. Acesso realizado em: Set/23.

[4] NVD. (08/09/2019). CVE-2019-12255 Detail. Disponível em: <https://nvd.nist.gov/vuln/detail/CVE-2019-12255>. Acesso realizado em: Set/23.

[5] Madakam. (2015). Internet of Things (IoT): A Literature Review.

[6] Cisco. (2011). The Internet of Things How the Next Evolution of the Internet Is Changing Everything.

[7] Hatton. (2017).The IoT in 2030: Which applications account for the biggest chunk of the $1.5 trillion opportunity?. Transforma Insights, página. Disponível em: <https://transformainsights.com/blog/iot-24-billion-connected-things-15-trillion> Acesso realizado em: Set/23.

[8] NOKIA. (2020). Threat Intelligence Report 2020.

[9] Definitive Healthcare. (2017).The IoT in 2030: Patient Journey, página. Definitive Healthcare, Disponível em: <https://www.definitivehc.com/resources/glossary/patient-journey> Acesso realizado em: Set/23.

[10] ALHAJ. (2017). A Survey: To Govern, Protect, and Detect Security Principles on Internet of Medical Things (IoMT).

[11]ALSUBAEI, Faisal et al. IoMT-SAF: Internet of medical things security assessment framework. Internet of Things, v. 8, p. 100123, 2019.

[12] Pundir. (2019). Intrusion Detection Protocols in Wireless Sensor Networks Integrated to Internet of Things Deployment: Survey and Future Challenges.

[13] Naqvi. (2022). A Critical Review of IoT-Connected Healthcare and Information Security in South Africa.