risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Revista Ibérica de Sistemas y Tecnologías de Información

Recebido/Submission: 10/05/2022
Aceitação/Acceptance: 30/07/2022

Modelagem Bayesiana aplicada para cálculo da probabilidade de falha em Sistemas de Saúde IoT

Erika Midori Kinjo[1], André Felipe Henriques Librantz[1], Edson Melo de Souza[1], Fábio Cosme Rodrigues dos Santos[1]

midori.kinjo@gmail.com; librantzandre@gmail.com; prof.edson.melo@gmail.com; fcrsantos77@gmail.com

[1] Programa de Pós-graduação em Informática e Gestão do Conhecimento, Campus Vergueiro, Universidade Nove de Julho, 01525-000, Brasil

DOI: 10.17013/risti.47.87–108

Resumo: A implantação da tecnologia da Internet das Coisas (IoT) traz benefícios à vida, como controle remoto de pragas na agricultura, monitoramento da cadeia de suprimentos, melhoria na educação e monitoramento de pacientes. No entanto, apesar dos benefícios, existem desafios embutidos na implementação desta tecnologia. Um dos maiores desafios da área é a violação de privacidade e segurança de dados. Portanto, é necessário avaliar a probabilidade de falha dos elementos e, consequentemente, a causa desse problema. Assim, é neste contexto que este trabalho se propõe a identificar, modelar e calcular a probabilidade de falha através de uma análise sistemática, utilizando Redes Bayesianas. Os resultados mostraram que através do uso do modelo proposto foi possível avaliar diferentes cenários para o uso de redes de Internet das Coisas, bem como simular o efeito da probabilidade de falha nos elementos críticos do sistema.

Palavras-chave: Rede Bayesianas, Falha, Saúde, Internet das Coisas, *Noisy-OR*.

Bayesian modeling applied to calculate the probability of failure in IoT Health Systems

Abstract: The implementation of the Internet of Things (IoT) technology provides benefits to life, such as remote pest control in agriculture, monitoring the supply chain, improvement environment in education, and monitoring patients. However, despite the benefits, there are challenges embedded in the implementation of this technology. One of the biggest challenges in the area is the violation of privacy and data security. Therefore, it is necessary to assess the probability of failure of the components and, consequently, the cause of this problem. So, it is in this context that this work proposes to identify, model, and calculate the failure probability through a systematic analysis, using Bayesian Networks. The results showed that through the use of the proposed model it was possible to evaluate different scenarios for the use of Internet of Things networks, as well as to simulate the effect of the probability of failure in the critical components of the system.

Keywords: Bayesian Network, Failure, Health, Internet of Things, IoT, Noisy-OR.

1. Introdução

A Federação de Cientistas Americanos (FCA) listou a Internet das Coisas (IoT) como uma das seis tecnologias civis disruptivas. Segundo a Federação de Cientistas Americanos (2008), os pontos de internet poderão residir em coisas do cotidiano até 2025, como embalagens de alimentos, móveis, documentos em papel, entre outros.

A Internet das Coisas ou *Internet of Things* (IoT) é um conceito que reflete a interconexão de pessoas e objetos a qualquer hora e local, podendo impactar todo o negócio envolvido. Pode-se considerar como a interconexão de objetos e dispositivos inteligentes identificáveis dentro da infraestrutura de uma rede que proporciona benefícios para além da relação entre máquinas (Islam et al, 2015).

O uso dessa tecnologia percorre diversos setores da economia (Ray, 2017), como por exemplo no monitoramento da cadeia de suprimentos (Ben-daya et al, 2019), controle remoto de pragas no setor agrícola (Lin et al, 2019), acompanhamento preventivo de atletas (Wilkerson et al, 2018). A Internet das Coisas também é uma tendência mundial no ambiente educacional, impactando o ambiente físico e virtual de aprendizagem (Elsaadany e Soliman, 2017).

Desta forma, há aplicação em diversos contextos: dispositivos domésticos que proporcionam conveniência e eficiência energética (Wang, 2018), no monitoramento da qualidade da água (Sun et al, 2017) e no gerenciamento de um zoológico (Mali, 2019). Diante dos diversos setores existentes que a Internet das Coisas pode atuar, a área da saúde pode acarretar grande impacto. Segundo a Organização das Nações Unidas, 2020, os custos na área da saúde já representam 10 % do Produto Interno Bruto (PIB) mundial.

Além disso, a tecnologia IoT tem o potencial de melhorar as aplicações médicas, como o monitoramento remoto de saúde, programas de condicionamento físico, doenças crônicas e cuidados a idosos (Islam et al, 2015). Tudo isso acarreta melhoria da qualidade de vida dos cidadãos, além de proporcionar mobilidade e autonomia nas atividades diárias (Domingues et at, 2019).

Para melhorar os serviços médicos em hospitais, sistemas de tecnologia vestível (também chamados de *wearable*) são utilizados para detecção de casos de emergência no momento da triagem (Albahri et al, 2019). No contexto da mobilidade há trabalhos que utilizam sensores para captar a pressão na planta do pé e durante o caminhar pode-se identificar problemas de postura na coluna e lesões em pés diabéticos (Domingues et al, 2019). A prevenção do desenvolvimento de doenças crônicas corresponde a outra área de saúde. Ali et al (2018) sugeriram a supervisão do paciente, por meio de sensores, após a recomendação de dietas com alimentos e medicamentos específicos.

O assunto se caracteriza como emergente na academia e demanda estudos com aplicações práticas. Como visto no estudo da FCA, não foram encontrados estudos que abordassem a avaliação da probabilidade de falha usando a combinação de técnicas de redes bayesianas e *Noisy-OR*. Este estudo propôs avaliar cada elemento da rede IoT em vez da abordagem am camadas, permitindo a avaliação de fatores externos à rede.

2. Probabilidade de Falha em Redes IoT

Os problemas advindos da utilização de IoT necessitam ser superados, uma vez que a utilização dessa tecnologia é acompanhada de desafios, destacando a violação à privacidade e segurança dos dados pela a quantidade de estudos publicados. De acordo com Anjum et al (2018), a taxa de divulgação indevida dos dados de um indivíduo é de 87 %. Em contrapartida, a esse uso indevido dos dados há o compartilhamento, análise e processamentos das informações que são necessárias para agilizar os recursos de um sistema IoT.

Muhammed et al (2018) propôs abordar elementos da rede relacionadas ao protocolo, dispositivo/sensor e ao gateway para enfrentar esses desafios em sistemas IoT. Não obstante, Sharma et al (2018), optou por abordar os algoritmos desses sistemas.

Mittelstadt (2017a, 2017b) destacaram questões externas a rede, por exemplo, questões éticas. E as questões externas não foram abordadas por outros trabalhos de forma conjunta com outros elementos da rede. Alguns trabalhos que abordam a avaliação de probabilidade de falhas foram consolidados na Tabela 1.

Gyamfi et al (2019) utilizou a probabilidade de falha de um nó da rede, probabilidade de alteração do ambiente ao longo do tempo aplicando Bayes para evitar perda de pacotes e custos de energia altos. Além disso, propõe um solução que aborda um elemento da rede e o protocolo de transmissão de pulsação baseado no período ótimo de pulsação.

Zhang et al (2018) utilizou redes bayesianas dinâmicas no contexto de veículos inteligentes para propor uma solução no elemento algoritmo para análise do desempenho.

Sun et al (2017) e Qingping et al (2018), no sistema de controle de água, propõe um modelo de redes bayesianas baseado em camadas com o objetivo de obter mais segurança dos dados. Nota-se que o modelo proposto por utilizar apenas camadas não permite a inclusão de fatores externos à rede.

Zhang & Xu (2020), na rede IoT utilizou redes bayesianas para definição da rota mais confiável e assim como os demais trabalhos já citados propões uma solução baseado em um elemento da rede, o algoritmo.

Ao contrário dos trabalhos correlatos espostos que utilizaram Redes Bayesianas, este estudo propõe a incluir fatores externos em uma abordagem sistêmica da rede, com foco em cada elemento em vez de camadas.

Autor	Desafio	Técnica
Lomotey et al (2017)	Rastreabilidade das rotas dos dados	Rede Petri
Gyamfi et al (2019)	Custo de energia/ Integridade dos dados	Redes Bayesianas
Chang et al (2020)	Governança da Rede/ Controle interno	Delphi
Sharma et al(2018) e Sareen (2017)	Privacidade dos dados	*Framework kHealth* (desenvolvido pela *Wright State University*)

Autor	Desafio	Técnica
Azimi et al (2019)	Integridade dos dados	Método de imputação múltipla
Wang et al (2020)	Privacidade e segurança dos dados, performance e intenção	Questionário/Análise dos dados
Zhang & Xu (2020)	Segurança dos dados	Redes Bayesianas
Sun et al (2017)	Identificação de intrusão	Redes Bayesianas
Vhaduri & Poellabauer (2019)	Privacidade e Segurança dos dados	Análise dos dados
Muhammed et al (2018)	Roteamento dos dados, confiabilidade dos dados	*Framework UbeHealth* (baseado em *deep learning*, *big data*, *high performance computing*)
Selvan et al (2019)	Confiabilidade dos dados	Lógica Fuzzy
Hou et al (2020)	Processamento de dados	*Machine Learning*
Guerrero-Rodriguez et al (2020)	Gerenciamento de energia	Análise dos dados
Gia et al (2018)	Custo de energia/ Integridade dos dados	Análise dos dados
Zhang et al (2018)	Segurança dos dados	Redes Bayesianas
Qingping et al (2018)	Segurança dos dados	Redes Bayesianas

Tabela 1 – Técnicas utilizadas nos trabalhos pesquisados

3. Rede Bayesiana

As Redes Bayesianas (RB) são modelos gráficos que mostram um conjunto de variáveis possíveis e suas dependências condicionais. De modo geral, uma RB é composta por partes quantitativas e qualitativas. A parte qualitativa é um DAG e a parte quantitativa são as probabilidades atribuídas aos nós que representam as variáveis. O fornecimento da relação de causa e efeito provém resultados animadores relacionados a diagnóstico, previsão e classificação de falhas (Librantz et al, 2020).

Esta abordagem permite que o conhecimento de especialistas sejam incluídos na modelagem (Librantz et al, 2020). Esta técnica representa uma boa estratégia para lidar com problemas que tratam incertezas. A RB é caracterizada por grafos acíclicos, no qual os vértices representam os nós e as ligações representam a relação de dependência entre esses nós, respectivamente são representados por elipse e setas. E os nós que não possuem dependência de outros nós, são denominados nós pais, conforme mostrado na Figura 1.

Essas variáveis podem ser valores observáveis, variáveis ocultas ou parâmetros desconhecidos. As bordas da RB representam as dependências. Cada nó tem uma função de probabilidade que consiste na probabilidade inicial (para nós sem pais) ou probabilidades condicionais relacionadas a diferentes combinações de nós pais.

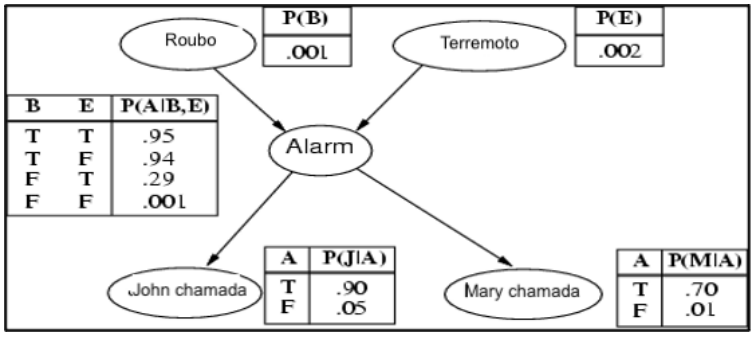

Figura 1 – Exemplo de rede bayesiana

A cada valor possível é chamado de estado. Quando há números finitos de estados, as dependências são definidas por Tabelas de Probabilidade Condicionais (TPC). De outra forma, a Tabela de Probabilidade Condicional consiste em um conjunto de distribuições de probabilidade indexadas pelas possíveis combinações de estados nós pais (Zagorecki & Druzdzel, 2013). O teorema de Bayes expressa a relação entre as variáveis dependentes, como segue:

$$P(H / E) = \frac{P(E / H).P(H)}{P(E)}$$

Na qual P (H/E) é uma probabilidade do evento H dado que o evento E ocorreu, P (E/H) é uma probabilidade do evento E dado que o evento H ocorreu, P (H) é uma probabilidade do evento H e P (E) é uma probabilidade do evento E. O teorema de Bayes usa um conhecimento probabilístico de uma hipótese antes de qualquer observação e, posteriormente, apresenta um número estimado para a hipótese após as observações. A primeira aplicação prática da RB foi o problema clássico do diagnóstico médico (Patterson et al, 1984). Empresas como a Microsoft(R) usaram essas redes para diagnóstico de falhas, principalmente solução de problemas de impressora (Heckerman, Mamdani & Wellman, 1995). As habilidades preditivas e diagnósticas das RB a tornam uma ferramenta poderosa para a tomada de decisão sob incerteza.

4. Materiais e métodos

O estudo proposto tem uma abordagem mista, conciliando características da abordagem qualitativa e quantitativa. A vantagem de utilizar a abordagem mista é obter resultados mais assertivos para o objetivo do estudo (Creswell & Clark, 2013). O trabalho foi dividido em três etapas para obtenção de um resultado mais consistente, conforme mostra a Figura 2.

As etapas expostas na Figura 2 são detalhadas a seguir:

- **Etapa Exploratória**

Primeiramente ocorreu a identificação das possíveis falhas na utilização de IoT na saúde e elementos associados, utilizando as palavras-chaves: (1) "IoT" *and* "*Failure Probability*" *and* "*Health*", (2) "*Internet of Things*" *and* "*Failure Probability*" *and* "*Health*", (3) "IoT" *and* "*Failure*" *and* "*Health*", (4) "*Internet of Things*" *and* "*Failure*" *and* "*Health*", (5) "IoT" *and* "*Evaluation*" *and* "*Health*", (6) "*Internet of Things*" *and* "*Evaluation*" *and* "*Health*", (7) "IoT" *and* "*Assessment*" *and* "*Health*" e (8) "*Internet of Things*" *and* "*Assessment*" *and* "*Health*" nas bases de dados: *Scopus*, *Web of Science*, IEEE e EBSCO, totalizando 75 artigos. Com a finalidade de compreender melhor os elementos que podem ocasionar falhas identificados na literatura, foi necessário que estes fossem avaliados em relação à probabilidade de falha e nível de impacto na rede IoT. Um formulário, no *Google Forms*(R), foi distribuído para 12 especialistas, cuja experiência média em projetos de automação que supera 10 anos, para que avaliassem a probabilidade de falha um valor entre 0 % e 100 % e a avaliação do nível de relevância, um valor de 0 a 10.

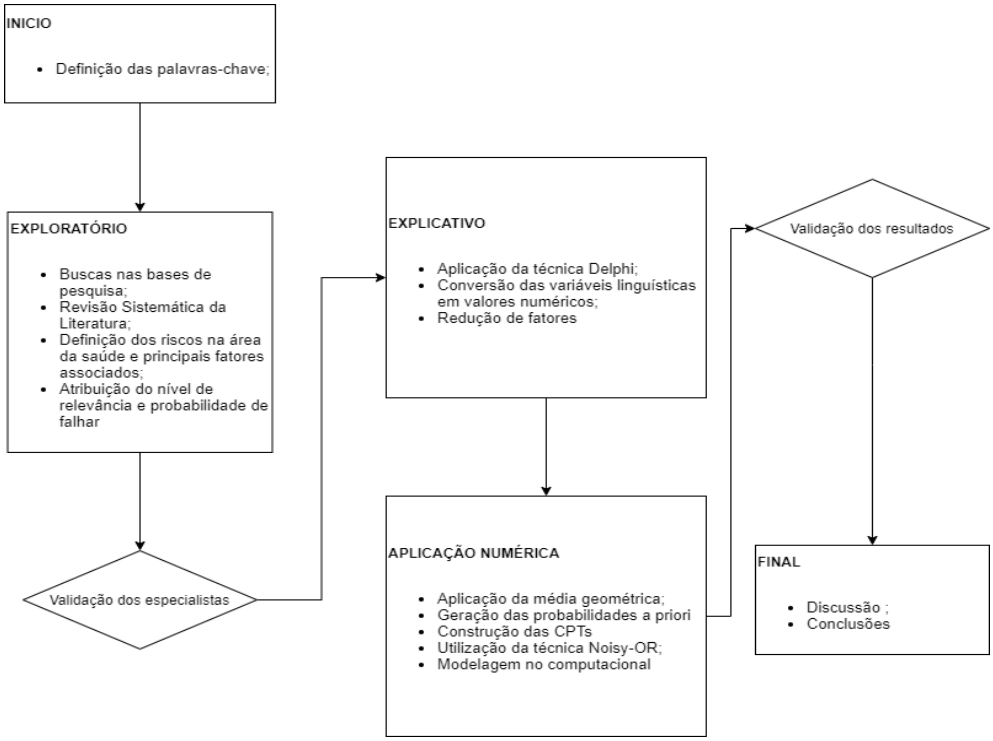

Figura 2 – Etapas de metodologia aplicada ao estudo

- **Etapa Explicativa**

A segunda etapa teve a finalidade de compreender os resultados encontrados na etapa anterior. A apliacação da técnica *Delphi* permitiu a identificação dos

elementos mais relevantes para o desafio de probabilidade de falha na violação à privacidade e segurança dos dados. Após a aplicação da técnica sobre os dados coletados das opiniões dos 12 especialistas convidados, o modelo demostrando os elementos e seus respectivos subelementos foi representado na Figura 3.

- **Etapa Aplicação Numérica**

  As opiniões dos especialistas foram consolidadas por meio da média geométrica e utilizados como probabilidade a priori. As Tabelas de Probabilidade Condicional (TPCs) foram desenvolvidas quando as probabilidades a priori foram definidas. Neste estudo, as TPCs foram geradas usando o método *noisy-OR*.

O método *noisy-OR* permite reduzir a complexidade decorrente da quantidade em demasia de distribuições de probabilidade, gerados de uma Rede Bayesiana (Pearl, 1986). Por fim, com a definição do grupo de elementos passíveis de falha e a relação de interdependência deles validada, foi possível modelar a Rede Bayesiana, utilizando o *software* Genie 3.0 Academic.

5. Resultados

Entre os resultados encontram-se:

5.1. Levantamento de fatores envolvidos

A Tabela 2 mostra os 8 elementos críticos de uma rede Internet das Coisas, de acordo com a literatura consultada. A tabela de levantamento dos elementos proposta por Woo et al (2017), destaca-se o dispositivo como fator essencial quando o monitoramento remoto no contexto da saúde foi considerado.

O *Gateway* foi elencado por Azimi (2019) como outro fator da rede. Este fator atua como uma ponte entre o dispositivo e o provedor de serviços, oferecendo toda a infraestrutura para o armazenamento dos dados e ampla quantidade de técnicas analíticas são responsabilidades do Provedor de Serviços. A contratação de uma infraestrutura de terceiros para este serviço está diretamente relacionada à forma como ser processado os dados, sendo este outro fator que pode influenciar a rede segundo Sharma et al (2018).

O Protocolo foi abordado na solução proposta por Muhammed et al (2018) para enfrentar os desafios enfrentados por essa tecnologia, tais como latência da rede, largura da banda e confiabilidade dos dados. O Algoritmo utilizado na rede foi destacado no trabalho de Sood e Mahajan (2017) como outro fator a ser abordado, uma vez que a combinação de algoritmos trouxe resultados interessantes para o controle e propagação do vírus da Chikungunya.

Segundo Tan et al (2018), a rede apresenta a Aplicação, no formato de Web sites, Chats, como o fator relevante para a rede. É por meio da aplicação que os usuários (médico e pacientes) visualizar os dados e informações obtidas.

O elemento ético (social) também foi abordado n as pesquisas de Mittelstadt (2017a, 2017b). Vale ressaltar que este elemento não foi considerado em nenhum outro trabalho como fator relevante para reduzir incertezas e falhas na rede, sendo considerado uma lacuna nos estudos já expostos.

Elemento	Conceito	Exemplo	Estudos que corroboram
Dispositivo/ Sensor	Responsável por coletar dados sobre sintomas relacionados à saúde e vários eventos dentro e ao redor do ambiente relacionados ao usuário. Os dados são coletados a partir dos dispositivos de hardware sem fio incorporados ao corpo do usuário, dentro e nos arredores do usuário.	*Wearable* e Dispositivo de Saúde Pessoal (PHD) vestível	Sood & Mahajan (2017), Wang (2018), Muhammed et al (2018), Woo et al (2017)
Gateway	Plataforma de gerenciamento de interconexão e serviços; portanto, o gateway é necessário para funcionar como tradutores de protocolo, dispositivos de correspondência de impedância e conversores de taxa entre eles.	*Access point*, *Wireless transmission* (SIM7000C) (NB-IoT)	Wang (2018), HU et al (2019), Azimi et al, (2019)
Algoritmo	Atua como uma ponte entre os sensores da IoT e os Serviços de Provedor. É usado para processamento e análise em tempo real de dados acumulados de sensores baseados em IoT.	Algoritmo incorporado, criptografia e algoritmo genético	Sood & Mahajan (2017), Wang (2018), Albahri et al (2019)
Protocolo	Permite a interoperabilidade nas redes heterogêneas e permita a troca de dados sem interrupções em todo o sistema da Internet das Coisas	Compartilhamento secreto Shamir, *LEACH protocol* (cluster), IKEv2, IPv6, oneM2M	Mittelstadt (2017a, 2017b), Sharma et al (2018), Wang (2018), Muhammed et al (2018)
Provedor de Serviços	Armazenamento dos dados (criptografados, perturbados ou anonimizados e sem nenhuma informação de identificação pessoal (PIIs)). Podendo optar por terceirizar dados e computação para um provedor de nuvem que fornece infraestrutura para armazenamento e análise.	Nuvem pública e privada	Sood & Mahajan (2017), Sharma et al (2018)
Processamento	Distribuição da carga de trabalho total de estruturas de preservação de privacidade para seus participantes em relação aos recursos disponíveis. Uma estrutura prática deve garantir que as partes com recursos limitados realizem tarefas de menor complexidade, enquanto as tarefas caras são paralelas à parte com recursos abundantes, como uma nuvem.	Paralelo e distribuído	Sharma et al (2018)
Social	Interação social através da distância geográfica, participação em grupos e localização. Está conectado à privacidade física.	Ética	Mittelstadt (2017a, 2017b)
Aplicação	Responsável pelo controle e gerenciamento dos dados transferidos para o servidor a partir dos elementos de processamento. [...] Para resolver a falta de comunicação entre pacientes e médicos no atual sistema de monitoramento de saúde	Website, Chat	Tan & Halim (2019), Hu et al (2019), Azimi et al, (2019)

Tabela 2 – Principais elementos que podem ocasionar falhas extraídos da literatura

Além disso, não foi encontrada na literatura pesquisas que abordassem diretamente um elemento específico da rede. De maneira geral, os autores dividiam o sistema IoT em camadas e analisavam apenas uma delas, destacando-se a camada física, comunicação e apresentação. Desta forma, os elementos externos a rede, por exemplo, questões éticas não eram avaliadas.

Segundo Tan et al (2018), a rede apresenta a Aplicação, no formato de Web sites, Chats, como o fator relevante para a rede. É por meio da aplicação que os usuários (médico e pacientes) visualizar os dados e informações obtidas.

As questões sociais também foram abordadas no trabalho de apresentado por Mittelstadt (2017a, 2017b). Destaca-se que o fator social não considerado em nenhum outro trabalho como fator relevante para reduzir incertezas e falhas na rede, sendo considerado uma lacuna nos trabalhos já apresentados.

A consulta na literatura resultou em nenhum estudo que aborde diretamente um elemento específico da rede. De maneira geral, os autores dividiam o sistema IoT em camadas e analisavam apenas uma dessas camadas. Entre essas camadas destacaram a camada física, comunicação e apresentação. Sendo assim, os elementos externos a rede, por exemplo, questões éticas não eram avaliadas.

Com o objetivo de detalhar os elementos mencionados anteriormente foram elencados 14 subelementos. A associação desses elementos e subelementos foi representada na Tabela 3. A relação do fator e seus respectivos subelemento foram utilizados como base para a construção do modelo.

5.2. Redução da quantidade de elementos do modelo

A coleta e análise desses dados permitiram, de acordo com a visão dos especialistas, excluir do modelo os elementos classificados como menor possibilidade de falha na violação à privacidade e segurança (dos dados).

Ao analisar a percepção dos especialistas, o Provedor de Serviços se mostrou o fato de maior relevância, seguido dos elementos Sociais e da Aplicação, corroborando o que foi destacado nos estudos correlatos de maior relevância, o qual o Provedor de Serviços apareceu entre os elementos mais citados.

Apesar de poucos trabalhos publicados sobre questões éticas no contexto deste trabalho, na percepção dos especialistas, trata-se de um dos elementos mais relevantes para o modelo. Os estudos avaliavam as questões internas dos sistemas IoT até então.

Após a aplicação da técnica do Índice de Validade de Conteúdo – IVC (Alexandre & Coluci, 2011; Bellucci Júnior & Matsuda, 2012) três subelementos foram considerados de menor importância e desconsiderados no modelo. Este resultado está de acordo com o encontrado na literatura, uma vez poucos trabalhos detalharam esses subelementos

No ranking de importância dos elementos, os três subelementos que foram excluídos do modelo por não atingirem o limite de IVC estabelecidos. O valor limite considerado nesta pesquisa foi de 60%, de modo que foram utilizado no modelo 11 subelementos. A partir desta etapa passou-se a implementação computacional do modelo bayesiano conforme descrito na sequência.

Elemento	Subelemento	Conceito	Exemplo(s)
Dispositivo/ Sensor	Quantidade	Número de dispositivos que coletam informações dos pacientes, que podem ser valores extrínsecos (temperatura, localização) e intrínsecos (pressão arterial, nível de glicose no sangue, batimento cardíacos.	1 sensor e 2 sensores
	Parâmetro	Refere-se à seleção do conjunto de dados e o que ele representa para o modelo.	Dados de localização, saúde, ambiente e meteorológicos
	Tipo	Classificação do sensor em relação a forma como é captado os dados.	Smartphone e *Weareable*
	Modelo	Atributos do dispositivo	Modelo, precisão/ acurácia (alta, média e baixa)
Gateway	Tipo	Desempenhar os papéis das infraestruturas físicas e também poderia desempenhar os papéis das infraestruturas de transmissão	SIM7000C
Algoritmo	Quantidade	Número de combinações de algoritmos para atingir o objetivo	
	Objetivo	Os algoritmos devem ser capazes de ajudar a identificar um problema específico e escolher a melhor técnica para isso	Criptografia
	Linguagem	Refere-se à linguagem de programação escolhida para o desenvolvimento da solução para atingir o objetivo	C e JAVA
Protocolo	Configuração	Refere-se ao padrão internacional para comunicação, especifica quando e como os dados são carregados para o servidor ou o comando é baixado pelos dispositivos de detecção e pode influenciar o consumo de energia	I2C de 7 bits.
Provedor de Serviços	Recursos	Refere-se aos recursos usados na arquitetura de rede IoT, como tipo, escalabilidade e investimento	*Cloud* e *On Premisses*
Processamento	Recursos	Refere-se à distribuição da carga de trabalho total de estruturas de preservação de privacidade para seus participantes em relação aos recursos disponíveis para eles.	Paralelo e Distribuído
Social	Ético	Refere-se a problemas éticos decorrentes das falhas inerentes à rede IoT, a sensibilidade dos dados relacionados à saúde e seu impacto na prestação de cuidados de saúde.	Direito de possuir e proteger o espaço pessoal, sentimento de intimidade/controle, autonomia

Elemento	Subelemento	Conceito	Exemplo(s)
Aplicação	Formato(tipo)	Refere-se a forma os usuários podem adquirir suas informações de interesse	API, Website e Chat
	Público-alvo	Refere-se a quem foi projetado para usar a interface, podendo ser um usuário comum ou o gerente do sistema.	Médicos, Hospitais e Pacientes

Tabela 3 – Elemento e Subelemento

5.3. Implementação Computacional do Modelo Bayesiano

O modelo foi implementado no software *Genie 3.0 Academic,* ou *GeNIe Modeler* que é uma interface gráfica de usuário (GUI), que permite a construção e aprendizagem de modelos interativos, conforme mostra a Figura 3. A principal vantagem da utilização dessa ferramenta é permitir a liberdade de modelagem completa, além de ter ampla aceitação tanto na academia quanto na indústria.

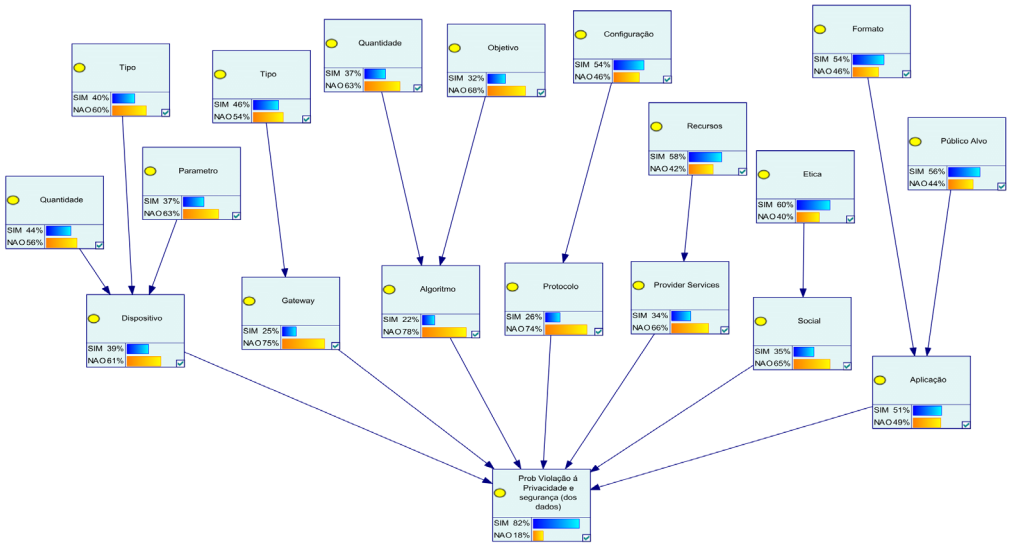

Figura 3 – Modelo da Rede Bayesiana produzido no Genie

5.3.1. Geração das probabilidades a priori

As informações prévias captadas dos especialistas sobre o problema abordado geraram, juntamente com aplicação da escala de conversão e a média geométrica, a probabilidade a priori que foi utilizada no modelo e estão representadas na Tabela 4.

Elemento	Subelemento	Esp. 1	Esp. 2	Esp. 3	Esp. 4	Esp. 5	Esp. 6	Esp. 7	Esp. 8	Esp. 9	Esp. 10	Esp. 11	Esp. 12	Probabilidade
Dispositivo/ Sensor	**Quantidade**	0,5	0,7	0,5	0,7	0,9	0,3	0,1	0,7	0,1	0,5	0,5	0,5	44%
	Parâmetro	0,5	0,1	0,5	0,3	0,5	0,3	0,3	0,7	0,1	0,5	0,5	0,5	37%
	Tipo	0,5	0,1	0,9	0,3	0,7	0,3	0,7	0,5	0,1	0,5	0,3	0,5	40%
	Modelo	0,5	0,1	0,3	0,5	0,7	0,3	0,7	0,7	0,1	0,5	0,3	0,3	39%
Gateway	**Tipo**	0,5	0,7	0,5	0,3	0,5	0,3	0,3	0,5	0,5	0,5	0,3	0,5	46%
Algoritmo	**Quantidade**	0,5	0,3	0,5	0,5	0,5	0,3	0,1	0,3	0,1	0,5	0,7	0,5	37%
	Objetivo	0,5	0,1	0,7	0,5	0,5	0,3	0,1	0,3	0,1	0,3	0,5	0,3	32%
	Linguagem	0,5	0,3	0,9	0,3	0,5	0,3	0,1	0,3	0,1	0,7	0,5	0,1	37%
Protocolo	**Configuração**	0,5	0,7	0,7	0,3	0,5	0,3	0,3	0,3	0,9	0,7	0,7	0,5	52%
Provedor de Serviços	**Recursos**	0,5	0,5	0,7	0,7	0,3	0,3	0,9	0,3	0,9	0,7	0,7	0,7	58%
Processamento	**Recursos**	0,5	0,5	0,3	0,3	0,5	0,3	0,3	0,3	0,5	0,5	0,5	0,5	43%
Social	*Ético*	0,5	0,7	0,5	0,7	0,9	0,3	0,5	0,3	0,9	0,9	0,5	0,3	60%
Aplicação	**Formato(tipo)**	0,5	0,5	0,7	0,5	0,9	0,3	0,3	0,3	0,9	0,5	0,7	0,3	54%
	Público-alvo	0,5	0,5	0,7	0,7	0,9	0,3	0,7	0,1	0,9	0,7	0,7	0,3	56%

Tabela 4 – Pesos atribuídos aos subelementos pelos especialistas

5.3.2. Construção das TPCs

A partir das probabilidades a priori, definidas anteriormente para cada nó do modelo foi construída uma tabela de probabilidade condicional. A Tabela 5 representa a TPC do nó Dispositivo. Cada Tabela de Probabilidade Condicional foi carregada no Genie.

	Dispositivo				
	Quantidade	**Parâmetro**	**Tipo**		
P(f)	**0,368408921**	**0,36580377**	**0,40087**		
Q(f)	**0,631591079**	**0,63419623**	**0,59913**	**Não existir**	**Existir**
	T	T	T	0,240	0,760
	T	T	F	0,401	0,599
	T	F	T	0,378	0,622
	T	F	F	0,632	0,368
	F	T	T	0,380	0,620
	F	T	F	0,634	0,366
	F	F	T	0,599	0,401
	F	F	F	1,000	0,000

Tabela 5 – TPC do Dispositivo/ Sensor

6. Validação do modelo

A validação do modelo possibilita uma considerável garantia da sua aplicabilidade. Há algumas abordagens para realizar estra etapa e em uma análise satisfatória necessita de dados históricos, compreendidos em longos períodos de tempo, o que pode tornar a validação completa muito difícil. Segundo Librantz et al (2020), a utilização de dois axiomas é utilizada para a validação parcial do modelo. Os axiomas são:

- Um ligeiro aumento/diminuição no nó pai resulta um aumento/diminuição no nó filho, ou seja, são diretamente proporcionais;
- A influência nas probabilidades de variações nos nós filhos no desafio de violação à privacidade e segurança dos dados deve ser maior que os parâmetros dos pais;
- O gráfico exibido na Figura 4 corrobora o Axioma 1, no qual a probabilidade de falha é diretamente proporcional à variação do Provedor de Serviços. Assim como diminuirá de acordo com a diminuição do nó pai.

A Tabela 6 apresenta os resultados do segundo experimento realizado para validação, mostrando que os elementos são acrescentados a variação da probabilidade de falha, que também aumenta. Além disso, quando outro elemento é adicionado, a probabilidade de falha é ainda maior do que o anterior. Esses resultados estão em boa concordância com o Axioma 2 descrito anteriormente, o que permitiu uma validação parcial do modelo proposto.

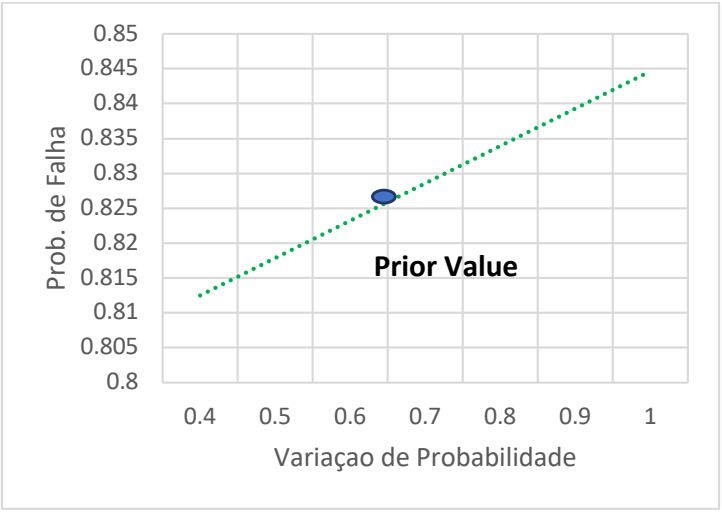

Figura 4 – Probabilidade de falha do elemento Recursos (do Provedor de Serviços)

	Desafio Violação à Privacidade e Segurança (dos dados)	**Variação (%)**
Elemento	0,82	0
Configuração (Protocolo)	0,83	1,2%
Configuração (Protocolo): Parâmetros (Dispositivo)	0,85	3,6%
Configuração (Protocolo): Parâmetros (Dispositivo):Recursos (Provedor de Serviços)	0,87	6,0%
Configuração (Protocolo): Parâmetros (Dispositivo):Recursos (Provedor de Serviços): Ética (Social)	0,89	7,1%

Tabela 6 – Validação do modelo (axioma 2)

6.1. Exemplos de Aplicação do modelo proposto

A eficácia do modelo proposto pode ser melhor verificada a partir de dois experimentos criados com a ajuda de um especialista. No primeiro deles, a estimativa de falha de 3 redes IoT é calculada a partir da estimativa de falha dos elementos pai, conforme os cenários abaixo:

6.1.1. Cenário 1: Monitoramento de sala climatizada

- Seis parâmetros são configurados, sendo que cinco deles definem os limites mínimos, máximos e o ideal para a temperatura e um para o controle de umidade;
- O ambiente conta com cinco sensores de temperatura e umidade integrados, modelo Am2315 com protocolo I2c;
- *Gateway*: Realiza a coleta dos dados dos sensores (supervisório) e faz a transmissão via protocolo UDP para o servidor;
- Algoritmo: São utilizados dois algoritmos um para processamento dos dados e outro para geração de alertas;
- Objetivo do Algoritmo: Verificar os dados coletados no intervalo de cinco minutos pelos sensores, realizar um cálculo sobre a média das cinco leituras e informar a necessidade de ajustes na temperatura e controle da umidade de acordo com os parâmetros definidos em um painel;
- Configuração do Protocolo: O protocolo utiliza configurações básicas, priorizando a velocidade na transmissão dos dados;
- Recursos do provedor de serviços: Utilização de firewall para proteção contra invasões e algoritmos de suporte para verificação de ataques do tipo DDoS;
- Éticas: Conscientização sobre a importância em seguir os protocolos de verificação de alertas e aplicação de correções quando necessárias;
- Formato de aplicação: Ocorre de forma automática por temporização, informando a necessidade de intervenção humana.

6.1.2. Cenário 2: Monitoramento de Polissonografia Home Care

- Sete parâmetros são configurados para receber os dados sobre atividade elétrica cerebral e muscular, movimento dos olhos, fluxo de ar pelo nariz e boca, esforço respiratório e saturação do oxigênio;
- Sete sensores são posicionados no corpo do paciente por meio de eletrodos e canolas para captura de ar;
- *Gateway*: Realiza a coleta dos dados dos sensores (supervisório) e faz a transmissão com o protocolo TCP para o servidor via internet;
- Algoritmo: São utilizados dez algoritmos para o processamento e checagem dos dados de cada um dos sensores;
- Objetivo do Algoritmo: Verificar a integridade das leituras, armazena localmente os dados para segurança, realizar encriptação e fazer a transmissão para um servidor;
- Configuração do Protocolo: Utiliza criptografia com os protocolos TLS/SSL, garantindo uma comunicação segura;
- Recursos do provedor de serviços: Utilização de firewall para proteção contra invasões e algoritmos de suporte para verificação de ataques do tipo DDoS;
- Éticas: Proteção à privacidade dos dados do paciente, tanto sobre as leituras quanto a sua identificação;
- Formato de aplicação: Ocorre de forma automática, coletando os dados e transmitindo para o centro de monitoramento.

6.1.3. Cenário 3: Monitoramento e Controle de Gotejamento de Medicação

- Seis parâmetros são configurados para verificação do volume da medicação, contagem de gotas e monitoramento dos sinais vitais (temperatura, frequência respiratória, frequência cardíaca e pressão arterial);
- Sete dispositivos são utilizados, sendo quatro sensores posicionados no corpo do paciente para monitoramento dos sinais vitais, dois acoplados no suporte que abriga a medicação e um atuador para regulagem do controle do fluxo da medicação;
- *Gateway*: Realiza a coleta dos dados dos sensores (supervisório) e faz a transmissão com o protocolo TCP para o servidor via internet;
- Algoritmo: São utilizados seis algoritmos para o processamento e checagem dos dados de cada um dos sensores e um para o atuador de controle de fluxo;
- Objetivo do Algoritmo: Verificar a integridade das leituras, armazenar localmente os dados para segurança, tomar a decisão de alterar o fluxo do gotejamento, realizar encriptação e fazer a transmissão para um servidor;
- Configuração do Protocolo: Utiliza criptografia com os protocolos TLS/SSL, garantindo uma comunicação segura;
- Recursos do provedor de serviços: Utilização de firewall para proteção contra invasões e algoritmos de suporte para verificação de ataques do tipo DDoS;
- Éticas: Proteção à privacidade dos dados do paciente, tanto sobre as leituras quanto a sua identificação, além do controle do acesso físico ao paciente quando necessário para a reposição ou ajustes de equipamentos e/ou medicação;
- Formato de aplicação: Ocorre de forma automática, coletando os dados para realização do monitoramento, atuação sobre a regulagem da aplicação da medicação e transmissão para o centro de monitoramento.

Os cenários acima citados foram resumidos nas probabilidades de falha, conforme mostra a Tabela 7.

		Probabilidade de Falha		
		Cenário 1	**Cenário 2**	**Cenário 3**
Dispositivo/Sensor	Quantidade	BAIXO	MUITO ALTO	ALTO
	Parâmetro	BAIXO	MÉDIO	ALTO
	Tipo	MÉDIO	ALTO	ALTO
	Modelo	BAIXO	MÉDIO	MÉDIO
Gateway	Tipo	ALTO	ALTO	MUITO ALTO
Algoritmo	Quantidade	BAIXO	MÉDIO	MÉDIO
	Objetivo	BAIXO	ALTO	MUITO ALTO
	Linguagem	BAIXO	BAIXO	BAIXO
Protocolo	Configuração	BAIXO	ALTO	ALTO
Provedor de Serviços	Recursos	BAIXO	ALTO	MUITO ALTO
Processamento	Recursos	BAIXO	MÉDIO	ALTO
Social	Ético	ALTO	ALTO	MUITO ALTO

		Probabilidade de Falha		
		Cenário 1	**Cenário 2**	**Cenário 3**
Aplicação	Formato (tipo)	MÉDIO	MÉDIO	ALTO
	Público-alvo	MÉDIO	ALTO	MUITO ALTO

Tabela 7 – Cenários de Aplicação

Para efeitos de análise de falha, valores até 60 % foram considerados toleráveis. Na Tabela 8 abaixo mostra os três sistemas foram classificados conforme a probabilidade de falha.

Sistema	Classificação
Cenário 3	1
Cenário 2	2
Cenário 1	3

Tabela 8 – Classificação dos Cenários

A análise dos cenários permitiu a verificação da aplicação do modelo proposto, uma vez que identificou corretamente as probabilidades de falhas envolvidas. No cenário três, ao envolver vidas humanas, foi classificada pelo modelo como nível 1. Essa classificação permitiu verificar que os elementos relacionados à coleta dos dados, *gateway*, atuadores, questões éticas e nível de aplicação são críticos. Em comparação com os outros dois modelos, verifica-se que neste cenário a intervenção de um profissional da área da saúde se faz necessária, bem como indica quais são os pontos vulneráveis e que devem ter maior atenção. O modelo proposto se mostrou efetivo e coerente nas situações onde foi aplicado e, se mostra útil para identificação de pontos críticos e na remediação dos mesmos.

Baseando-se no cenário 2, uma alteração nos sensores pode provocar danos críticos ao sistema, na medida em que a leitura dos dados, uma vez não realizada ou realizada de forma inconsistente, prejudicará o resultado. Entretanto, podem ser anexados novos sensores para redundância, garantindo a coleta correta dos dados. Neste sentido, os algoritmos envolvidos devem ser aprimorados, tanto nas questões de controle sobre as redundâncias como na quantidade, a fim de garantir que os demais elementos funcionem adequadamente. Portanto, no segundo experimento o elemento algoritmo variou de 0 a 100%, simulando o efeito da variação deste fator na classificação de falhas dos sistemas, exibido na Figura 5.

No experimento 2, nota-se que a classificação dos sistemas não se altera, permanecendo Cenário 3, Cenário2, Cenário 1. Uma vez que na revisão da literatura há escassez de trabalhos incluindo o elemento social em uma análise sistêmica e também se trata de um fator classificado entre os mais impactantes após a aplicação da técnica *Delphi*. Este elemento foi escolhido também para o Experimento 2, mostra na Figura 6.

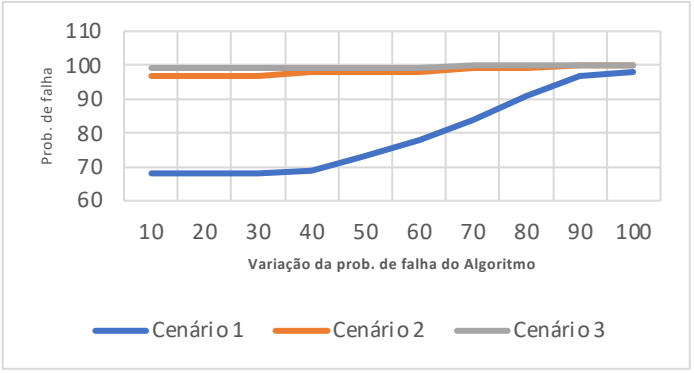

Figura 5 – Experimento 2 - Variação da probabilidade de falha do Algoritmo

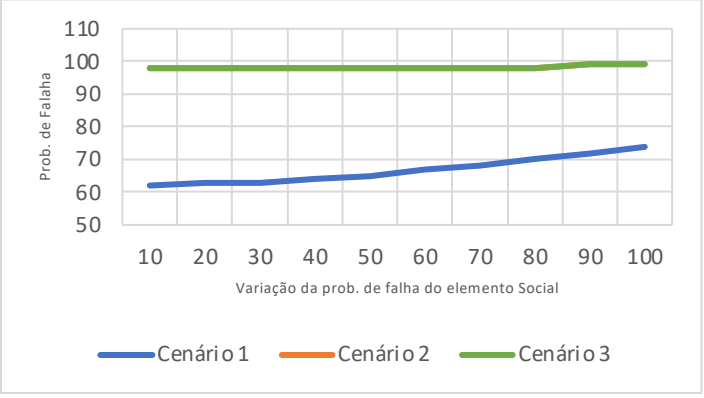

Figura 6 – Experimento 2 – Variação da probabilidade de falha do elemento Social

No experimento 2 reforçou o impacto para os cenários propostos, no cenário 2 e 3 o impacto fica próximo de 100%, demostrando a seriedade dos cenários.

7. Conclusão

Neste estudo a modelagem usando redes Bayesianas foi proposta para avaliar a probabilidade de falha em redes IoT. Os elementos foram identificados e validados por especialistas. Os primeiros resultados demonstram que o modelo proposto pode ser utilizado satisfatoriamente para avaliar a probabilidade de falha em sistemas IoT.

A aplicação de métodos numéricos facilita a variação da probabilidade de falhas do desafio abordado, principalmente no processo de verificação de falhas em sistemas complexos, pois se trata de uma tarefa árdua e onerosa. As técnicas *Delphi* e *noisy-OR* foram utilizadas para reduzir a complexidade do modelo. A principal vantagem dessa combinação de métodos é permitir a conciliação dos aspectos quantitativos e qualitativos para simulação de cenários característicos dos sistemas IoT.

A utilização de Redes Bayesiana mostrou a condição de que um dos elementos venha a sofrer modificações em seus parâmetros, é possível demostrar toda a relação de dependência entre os elementos, avaliando cada cenário.

A participação dos 12 especialistas proporcionou ao modelo uma visão real, permitindo a identificação de elementos relevantes. Da mesma maneira, os cenários simulados compreendem situações práticas que podem ocorrer no dia a dia desses sistemas de Internet das Coisas e os resultados obtidos certamente são pertinentes para analisar as falhas recorrentes e, consequentemente, darão suportarão decisões no segmento.

Como contribuição a teoria, este estudo permitiu abordar de forma sistêmica um conjunto de elementos inerentes às redes IoT por meio de uma combinação de técnicas até então não utilizadas para esse tema. Como limitação da pesquisa encontra-se a abordagem de apenas um dos desafios que cercam esses sistemas.

Visando trabalhos futuros, pretende-se incluir a análise de sensibilidade para avaliar a consistência dos resultados gerados. Uma outra opção para a continuidade do trabalho seria a inclusão do impacto no modelo desenvolvido, permitindo assim o cálculo de risco nas diferentes aplicações.

Referências

Anjum, A., Ahmed, T., Khan, A., Ahmad, N., Ahmad, M. A. M., Reddy, A. G., Saba, T. & Farooq, N. (2018). Privacy preserving data by conceptualizing smart cities using MIDR-Angelization. *Sustainable Cities and Society*, 40,326-334.

Alexandre, N. M. C. & Coluci, M. Z. O. (2011). Validade de conteúdo nos processos de construção e adaptação de instrumentos de medidas. *Ciência & Saúde Coletiva*, 16(7), 3061-3068.

Albahri, O. S., Albahri, A. S., Zaidan, A. A., Zaidan, B. B., Alsalem, M. A., Mohsin, A. H., Mohammed, K. I., Alamoodi, A. H., Nidhal, S., Enaizan, O., Chyad, M. A., Abdulkareem, K. H., Almahdi, E. M., Al Shafeey, G. A., Baqer, M. J., Jasim, A. N., Jalood, N. S. & Shareef, A. H. (2019). Fault-Tolerant mHealth Framework in the Context of IoT Based Real-Time Wearable Health Data Sensor. *IEEE Access*, 7, 50052-50080.

Ali, F., Khand, P., Kwak, D., Islam, S. M., Ullahe, N., Yoo, S. & Kwak, K. S. (2018). Type-2 fuzzy ontology-aided recommendation systems for IoT-based healthcare. *Computer Communications*, 119, 138-155.

Azimi, I., Pahikkala, T., Rahmani A. M., Niela-Vilén, H., Axelin, A. & Liljeberg, P. (2019). Missing data resilient decision-making for healthcare IoT through personalization: A case study on maternal health. *Future Generation Computer Systems*, 96, 297-308.

Bellucci Júnior, J. A. B. & Matsuda, L. M. (2012). Construção e validação de instrumento para avaliação do acolhimento com Classificação de Risco. *Revista Brasileira de Enfermagem*, 65(5),751–757.

Ben-Daya, M., Hassini, E. & Bahroun, Z. (2019). Internet of things and supply chain management: a literature review. *International Journal of Production Research*, 57, 15-16.

Chang, S-I., Chang, L-M. & Liao, J.-C. (2020). Risk factors of enterprise internal control under the internet of things governance: A qualitative research approach. *Information & Management*, 57(6),103335.

Creswell, J. W. & Clark, V. L. P. (2013). Pesquisa de Métodos Mistos (2ª Ed.). Editora Penso.

Domingues, F., Alberto, N., Leitão, C., Tavares, C., Lima, E., Radwan, A., Sucasas, V., Rodriguez, J., André, P. & Antunes, P. (2019). Insole Optical Fiber Sensor Architecture for Remote Gait Analysis-An e-Health Solution. *IEEE Internet of Things Journal*, 6(1),207-214.

Elsaadany, A. & Soliman, M. (2017). Experimental Evaluation of Internet of Things in the Educational Environment. *International Journal of Engineering Pedagogy*, 7(3),50-60.

Federação De Cientistas Americanos (FCA).(2020) Disruptive Civil Technologies: Six Technologies With Potential Impacts On Us Interests Out To 2025. https://fas.org/irp/nic/disruptive.pdf

Gia, T. N., Sarker, V. K., Tcarenko, I., Rahmani, A. M., Westerlund, T., Liljeberg, P. & Tenhunen, H. (2018). Energy efficient wearable sensor node for IoT-based fall detection systems. *Microprocessors and Microsystems*, 56,34-46.

Guerrero-Rodriguez, J. M., Cobos-Sanchez, C., Gonzalez-de-La-Rosa, J. J. & Sales-Lerida, D. (2019). An Embedded Sensor Node for the Surveillance of Power Quality. *Energies*. 12(8),1561.

Gyamfi K. S., Brusey J., Gaura, E. & Wilkins, R. (2019). Heartbeat design for energy-aware IoT: Are your sensors alive? *Expert Systems with Applications*. 128,124-139.

Heckerman, D., Mamdani, A. & Wellman, M. P. (1995). Real-World Applications of Bayesian Networks. *Communications of the ACM*, 38(3),24-25.

Hou, R., Kong, Y. Q., Cai, B. & Liu, H. (2020). Unstructured big data analysis algorithm and simulation of Internet of Things based on machine learning. *Neural Computing & Applications*. 32(10),5399-5407.

Hu, Z., Bai Z., Yang, Y., Zheng, Z., Bian, K. & Song, L. (2019). UAV Aided Aerial-Ground IoT for Air Quality Sensing in Smart City: Architecture, Technologies, and Implementation. *IEEE Network*, 33(2),14-22.

Islam, S. M. R., Kwak, D., Kabir, Md. H., Mahmud, H. & Kyung-Suo, K. (2015). The Internet of Things for Health Care: A Comprehensive Survey. *IEEE Access*, 3,678-708.

Librantz, A. F. H., Costa, I., Spinola, M. M., Oliveira Neto, G. C. & Zerbinatti, L. (2020). Risk assessment in software supply chains using the Bayesian method. *International Journal of Production Research*, 59(22),6758-6775.

Lin, Y-B., Lin Y-W., Lin, J-Y. & Hung, H-N. (2019). SensorTalk: An IoT Device Failure Detection and Calibration Mechanism for Smart Farmin. *Sensors*, 19(21),4788.

Lomotey, R. K., Pry, J. & Sriramoju S. (2017). Wearable IoT data stream traceability in a distributed health information system. *Pervasive and Mobile Computing*, 40,692-707.

Mali, A. D. (2019). Recent Domain-Specific Applications of Artificial Intelligence Using IoT. *International Journal on Artificial Intelligence Tools*, 28(7),1930003.

Mittelstadt, B. (2017a). Ethics of the health-related internet of things: a narrative review. *Ethics and Information Technology*, 19(3), 157-175.

Mittelstadt, B. (2017b). Designing the health-related internet of things: Ethical principles and guidelines. *Information*, 8(3),25.

Muhammed, T., Mehmood, R., Albeshri, A. & Katib, I. (2018). UbeHealth: A Personalized Ubiquitous Cloud and Edge-Enabled Networked Healthcare System for Smart Cities, *IEEE Access*, 6, 32258 – 32285.

Organização das Nações Unidas. (2021) OMS: custos com saúde já representam 10% do PIB mundial. https://news.un.org/pt/story/2019/02/1660781

Patterson, R. E., Eng, C., Horowitz, S. F., Gorlin, R. & Goldstein, S. R. (1984). Bayesian comparison of cost-effectiveness of different clinical approaches to diagnose coronary artery disease. Journal of The American College of Cardiology, 4(2),278-289.

Pearl, J. (1986). Fusion, Propagation and Structuring in Belief Networks. *Artificial Intelligence*, 29(3),241-288.

Ray, P. (2017). Understanding the role of internet of things towards smart e- healthcare services. *Biomedical Research India*, 28(4),1604–1609.

Selvan, N. S., Vairavasundaram, S. & Ravi, L. (2019). Fuzzy ontology-based personalized recommendation for internet of medical things with linked open data. *Journal of Intelligent & Fuzzy Systems*, 36(5),4065-4074.

Sood, S. K. & Mahajan, I. (2017). Wearable IoT sensor-based healthcare system for identifying and controlling chikungunya virus. *Computers in Industry*, 91,33-44.

Qingping S., Jian, K., Rong, W., Hang, Y., Yun, L. & Jie W. (2018). A Framework of Intrusion Detection System based on Bayesian Network in IoT. *International Journal Performability Engineer*, 14(10),2280-2288.

Rouse, W. B. (2021). Failure Management: malfunctions of technologies, organizations and society. OXFORD, United Kingdom.

Sareen, S., Sood, S. K. & Gupta, S. K. (2017). Secure Internet of Things-based Cloud Framework to Control Zika Virus Outbreak. *International Journal of Technology Assessment in Health Care*, 33(1),11-18.

Sharma, S., Chen K. & Sheth A. (2018). Toward practical privacy-preserving analytics for IoT and cloud-based healthcare systems. *IEEE Internet Computing*, 22(2),42-51.

Sun, F. F., Wu, C. & Sheng, D. (2017). Bayesian Networks for Intrusion Dependency Analysis in Water Controlling Systems. *Journal of Information Science and Engineering*, 33(4),1069-1083.

Tan, E. & Halim, Z. (2019). Health care Monitoring System and Analytics Based on Internet of Things Framework. *IETE Journal of Research*, 65(5), 653-660.

Vhaduri, S. & Poellabauer, C. (2019). Multi-Modal Biometric-Based Implicit Authentication of Wearable Device Users. *IEEE Transactions on Information Forensics and Security*, 14(12),3116-3125.

Wang, L. (2018). Environment supervision system for chemical industry park based on IOT. *Chemical Engineering Transactions*, 67, 481-486.

Wang, X., Mcgill, T. J. & KLOBAS, J. E. (2020). I Want It Anyway: Consumer Perceptions of Smart Home Devices. *Journal of Computer Information Systems*, 60(5),437-447.

Wilkerson, G., Gupta, A. & Colston, M. (2018). Mitigating Sports Injury Risks Using Internet of Things and Analytics Approaches. *Risk Analysis*, 38(7),1348-1360.

Woo, M. W., Lee, J. & Park, K. (2017). A reliable IoT system for Personal Healthcare Devices. *Future Generation Computer Systems*, 78(2),626-640.

Zagorecki, A. & Druzdzel, M. J. (2013). Knowledge Engineering for Bayesian Networks: How Common Are Noisy-MAX Distributions in Practice? *IEEE Transactions on Systems Man Cybernetics-Systems*, 43(1),186-195.

Zhang, H., Zhang, Q., Liu, J. & Guo, H. (2018). Fault Detection and Repairing for Intelligent Connected Vehicles Based on Dynamic Bayesian Network Model. *IEEE Internet of Things Journal*, 5(4),2431-2440.

Zhang, Q. & Xu, D. L. (2020). Security authentication technology based on dynamic Bayesian network in Internet of Things. *Journal of Ambient Intelligence and Humanized Computing*, 11(2),573–580.