



SEGURANÇA E CONFIABILIDADE DOS DISPOSITIVOS E SISTEMAS QUE IMPLEMENTAM A INTERNET DAS COISAS - UM MAPEAMENTO SISTEMÁTICO DA LITERATURA

Trabalho de Conclusão de Curso

Engenharia da Computação

Iago Interaminense Gomes
Orientador: Prof. Dr. Sérgio Murilo Maciel Fernandes



**Universidade de Pernambuco
Escola Politécnica de Pernambuco
Graduação em Engenharia de Computação**

IAGO INTERAMINENSE GOMES

**SEGURANÇA E CONFIABILIDADE
DOS DISPOSITIVOS E SISTEMAS QUE
IMPLEMENTAM A INTERNET DAS
COISAS - UM MAPEAMENTO
SISTEMÁTICO DA LITERATURA**

Monografia apresentada como requisito parcial para obtenção do diploma de Bacharel em Engenharia de Computação pela Escola Politécnica de Pernambuco – Universidade de Pernambuco.

Recife - PE, Brasil Outubro de 2022.

INTERAMINENSE, Iago

SEGURANÇA E CONFIABILIDADE DOS DISPOSITIVOS QUE
IMPLEMENTAM A INTERNET DAS COISAS - UM MAPEAMENTO
SISTEMÁTICO DA LITERATURA / Iago Interaminense Gomes. - Recife - PE,
Brasil, Outubro de 2022- 48p.
xv, 48 f.: il. ; 29 cm.

Trabalho de Conclusão de Curso (Graduação em Engenharia de
Computação) Universidade de Pernambuco, Escola Politécnica de
Pernambuco Recife, 2021

Orientador : Prof. Dr. Sérgio Murilo Maciel Fernandes

Notas (opcional)

1. Mapeamento sistemático de literatura. 2. Internet das coisas.
3. Segurança e confiabilidade. I. SEGURANÇA E CONFIABILIDADE DOS
DISPOSITIVOS QUE IMPLEMENTAM A INTERNET DAS COISAS - UM
MAPEAMENTO SISTEMÁTICO DA LITERATURA. II. Prof. Dr. Sérgio Murilo
Maciel Fernandes. III. Universidade de Pernambuco.

MONOGRAFIA DE FINAL DE CURSO

Avaliação Final (para o presidente da banca)*

No dia 6/10/2022, às 13h15min, reuniu-se para deliberar sobre a defesa da monografia de conclusão de curso do(a) discente **IAGO INTERAMINENSE GOMES**, orientado(a) pelo(a) professor(a) **SÉRGIO MURILO MACIEL FERNANDES**, sob título **SEGURANÇA E CONFIABILIDADE DOS DISPOSITIVOS E SISTEMAS QUE IMPLEMENTAM A INTERNET DAS COISAS - UM MAPEAMENTO SISTEMÁTICO DA LITERATURA**, a banca composta pelos professores:

DANIEL AUGUSTO RIBEIRO CHAVES (PRESIDENTE)
SÉRGIO MURILO MACIEL FERNANDES (ORIENTADOR)

Após a apresentação da monografia e discussão entre os membros da Banca, a mesma foi considerada:

Aprovada Aprovada com Restrições* Reprovada

e foi-lhe atribuída nota: 8,0 (oito)

*(Obrigatório o preenchimento do campo abaixo com comentários para o autor)

O(A) discente terá 04 dias para entrega da versão final da monografia a contar da data deste documento.


AVALIADOR 1: Prof (a) **DANIEL AUGUSTO RIBEIRO CHAVES**


AVALIADOR 2: Prof (a) **SÉRGIO MURILO MACIEL FERNANDES**

AVALIADOR 3: Prof (a)

* Este documento deverá ser encadernado juntamente com a monografia em versão final.

Agradecimentos

Agradeço ao meu Deus, que por ele todas as coisas retornam eternamente.

Agradeço aos meus pais, mesmo eu sendo ruim em demonstrar.

Agradeço pela chance de poder estudar.

Agradeço aos meus professores.

Agradeço à Engenharia.

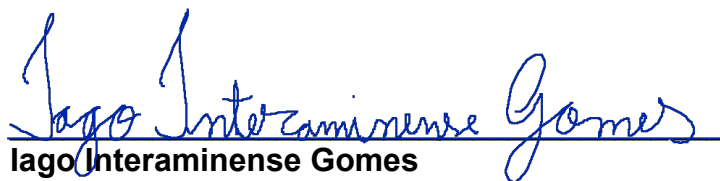
Agradeço à ela.

Agradeço.

Autorização de publicação de PFC

Eu, **Iago Interaminense Gomes** autor(a) do projeto de final de curso intitulado: **SEGURANÇA E CONFIABILIDADE DOS DISPOSITIVOS E SISTEMAS QUE IMPLEMENTAM A INTERNET DAS COISAS - UM MAPEAMENTO SISTEMÁTICO DA LITERATURA**; autorizo a publicação de seu conteúdo na internet nos portais da Escola Politécnica de Pernambuco e Universidade de Pernambuco.

O conteúdo do projeto de final de curso é de responsabilidade do autor.



Iago Interaminense Gomes



Orientador(a): **Sérgio Murilo Maciel Fernandes**

Coorientador(a):



Prof, de TCC: **Daniel Augusto Ribeiro Chaves**

Data: 6/10/2022

Resumo

Os dispositivos e sistemas IoT são um tema forte de pesquisa, a diversidade de escalas e a multiplicidade de lugares onde eles podem ser aplicados gera uma grande heterogeneidade de soluções para novos paradigmas de negócios. Essa quantidade e diversidade de sistemas sendo implantados sem padrões coesos, protocolos ou modelos, resulta na ausência de segurança e confiabilidade nos mesmos. Com o objetivo de expor no que as melhores equipes de pesquisadores tem trabalhado para sanar esse problema, o presente trabalho propõe fazer um mapeamento sistemático da literatura acerca da segurança e confiabilidade dos dispositivos e sistemas que implementam o IoT, utilizando diversas técnicas de seleção para garantir a qualidade dos trabalhos selecionados. A pesquisa se deu por meio da utilização de diferentes filtros de seleção automatizados, seleções elitistas através de métricas coletadas e trabalho de leitura. Os resultados obtidos são informações sobre quais são os problemas, as soluções e as áreas de aplicação onde segurança e confiabilidade dos sistemas e dispositivos IoT são a preocupação dos melhores pesquisadores da área.

Palavras-chave: Mapeamento sistemático; IoT; Segurança; Confiabilidade.

Abstract

IoT devices and systems are a strong research topic, the diversity of scales and the multiplicity of places where they can be applied generates a great heterogeneity of solutions for new business paradigms. This amount and diversity of systems being deployed without cohesive standards, protocols or models, results in the absence of security and dependability in them. With the objective of exposing what the best teams of researchers have been working on to solve this problem, the present work proposes to make a systematic mapping of the literature on the security and dependability of devices and systems that implement the IoT, using various selection techniques to ensure the quality of selected works. The research took place through the use of different automated selection filters, elitist selections through collected metrics and reading work. The results obtained are information about the problems, solutions and application areas where security and reliability of IoT systems and devices are the concern of the best researchers in the area.

Keywords: Systematic mapping; IoT; Safety; Reliability.

Lista de Figuras

Figura 1. – Processos aplicados nos dados coletados	25
Figura 2. – Processos de exclusão aplicados nos dados coletados	26
Figura 3. – Dados relacionando autores dos artigos com citações dos autores .	30
Figura 4. – Gráfico ordenado do número de citações por autor	31
Figura 5. – Tabela de autores ordenada por ocorrências de contribuições no conjunto de artigos	32
Figura 6. – Gráfico ordenado do número de contribuições em artigos do conjunto de dados por autor	33
Figura 7. – Gráfico ordenado do número médio de citações por autor em cada artigo	34
Figura 8. – Gráfico ordenado de número de citações por artigo	35
Figura 9. – Gráfico em pizza das áreas onde os artigos sobre segurança/confiabilidade são aplicados	37
Figura 10. – Gráfico em pizza das áreas onde os artigos sobre segurança/confiabilidade são aplicados, excluindo os IOT/SISTEMAS CYBER-FÍSICOS	38
Figura 11. – Gráfico em pizza dos atributos de segurança e confiabilidade que os grupos mais bem ranqueados de pesquisadores de sistemas IoT em 2020 deram atenção	39
Figura 12. – Gráfico em pizza das camadas arquitetônicas elencadas a partir dos artigos	40
Figura 13. – Gráfico em pizza dos problemas para obtenção de confiabilidade/segurança na <i>CLOUD</i>	41
Figura 14. – Gráfico em pizza dos problemas para obtenção de confiabilidade/segurança na <i>NETWORK</i>	42

Figura 15. – Gráfico em pizza dos problemas para obtenção de confiabilidade/segurança na <i>FOG/EDGE</i>	43
Figura 16. – Gráfico em pizza dos problemas para obtenção de confiabilidade/segurança na <i>DEVICE</i>	44
Figura 17. – Gráfico em pizza das tecnologias/técnicas garantidoras de confiabilidade e segurança mais utilizadas pelos trabalhos mais bem ranqueados de 2020	45

Lista de Tabelas

Tabela 1.	– Frase padrão de busca	22
Tabela 2.	– Conjuntos de palavras chaves derivadas	23
Tabela 3.	– Grupos unidos pelo conector lógico OR	23
Tabela 4.	– Frases de busca resultantes das permutações	24
Tabela 5.	– Sumário estatístico de métricas da base ACM	28
Tabela 6.	– Sumário estatístico de métricas da base SCIENCE DIRECT	28
Tabela 7.	– Sumário estatístico de métricas da base IEEEEXPLORE	28
Tabela 8.	– Sumário estatístico de métricas da base SPRINGERLINK	29

Lista de Símbolos e Siglas

CIA – *Confidentiality, Integrity, Availability*

GPS – *Global positioning system*

IoT – *Internet of Things*

MIoT – *Medical IoT*

Sumário

1	INTRODUÇÃO	13
1.1	Fundamentação Teórico-Methodológica	14
1.1.1	Revisões sistemáticas de literatura	15
1.1.2	Mapeamento sistemático de literatura	15
1.1.3	Internet das coisas (IoT)	15
1.1.4	Segurança da informação	16
1.1.5	Confiabilidade de sistemas computacionais	16
1.1.6	Fundamentação de termos	17
2	MAPEAMENTO SISTEMÁTICO DA LITERATURA	20
2.1	Metodologia de pesquisa	20
2.1.1	Perguntas de pesquisa	20
2.1.2	Estratégia de busca	21
2.1.2.1	Bases de pesquisa	21
2.1.2.2	Frase de busca	21
2.1.2.3	Período de busca	24

2.1.2.4	Critérios de inclusão	24
2.1.2.5	Critérios de exclusão	24
2.1.2.6	Conteúdo extraído	24
2.2	Processos aplicados	25
2.2.1	Processos de exclusão de artigo	25
2.2.1.1	Organizar e unificar a base de artigos	26
2.2.1.2	Reutilizar a frase de busca em filtro	27
2.2.1.3	Remover os estudos secundários	27
2.2.1.4	Remover os estudos duplicados	27
2.2.1.5	Remover os estudos com métricas relevantes desprezíveis	27
2.2.1.6	Remover artigos que fujam ao objetivo de pesquisa	29
2.2.2	Processos de adição de dados	30
2.2.3	Processos de exclusão de artigos	30
2.2.4	Processos de extração de dados	35
2.2.5	Processos de síntese de dados	36
2.3	Resultados	36
2.3.1	Resultados da pergunta de pesquisa 1	36
2.3.2	Resultados da pergunta de pesquisa 2	38
2.3.3	Resultados da pergunta de pesquisa 3	45
3	CONCLUSÕES E TRABALHOS FUTUROS	46
	REFERÊNCIAS	47

1 Introdução

A internet das coisas (**IoT** da sigla em inglês) é um dos principais motores de inovação e transformação nas sociedades participantes da economia globalizada. Sinônimo do conceito de computação ubíqua, o IoT já permeia vários aspectos do dia a dia de todas as pessoas. Essa infiltração no ambiente social permite uma coleta enorme de dados, uma vez que os dispositivos componentes dessa tecnologia podem estar repletos de sensores (GPS, proximidade, acelerômetro, câmera, microfone) capazes de capturar informações pessoais de participantes do ambiente onde o IoT está sendo implantado, fora isso, ainda existem os casos onde a informação sendo coletada é de posse privada de um indivíduo, como ocorre em várias aplicações do IoT aplicado à medicina (MIoT) [1], ou no uso de dispositivos sensores domésticos. Há ainda o caso dos dados coletados pela indústria, que, caso extraviados ou modificados, podem acarretar em danos na cadeia de produção.

Fora as preocupações com a privacidade e segurança das informações coletadas e transmitidas pelos dispositivos IoT, existem também receios no que compreende a confiabilidade e segurança desses sistemas, seja em um âmbito individual, como exemplifica o caso de um paciente diabético, dependente de um monitor de glicose contínuo que ativa uma sonda injetora de insulina [2]; seja no monitoramento de máquinas em ambientes de produção industrial através de redes IoT *wireless* [3]; ou ainda na parte de transporte e monitoramento de carga da cadeia de suprimentos [4], na qual vários negócios, com a ajuda da informação produzida por dispositivos IoT, precificam contratos futuros de materiais e produtos que são essenciais para o bom funcionamento da economia moderna. Em todos esses exemplos há a necessidade - crítica para os consumidores - de que o serviço entregue pela tecnologia esteja em concordância com a descrição do mesmo.

Para se obter os requisitos, que as tecnologias e dispositivos que abrangem o IoT demonstram precisar para sua adoção crescente ser sustentável, vários estudos, efetuados pela comunidade científica, sobre técnicas e métodos para alcançar um maior grau de confiabilidade nos dispositivos e sistemas; e segurança no uso,

transmissão e armazenamento dos dados, foram realizados desde o início da convergência das tecnologias que deram origem à área.

Esse trabalho se propõe a compreender quais são os desafios à confiabilidade e segurança de sistemas e dispositivos que implementam a internet das coisas, e quais são as técnicas e métodos que estão sendo, de forma relevante, mais pesquisados para saná-los. Efetuando-se no período de 2020 a 2021, a partir de um estudo secundário com regras bem definidas denominado mapeamento sistemático da literatura.

O resto dessa pesquisa é apresentada da seguinte forma: No capítulo 2 se encontra o desenvolvimento, que é separado em três partes - sendo a primeira parte para explicitar a metodologia utilizada pela pesquisa; a segunda para demonstrar os processos aplicados, a partir da metodologia, para a elicitação, refinamento e processamento dos dados; e a terceira expõe os resultados do processamento dos dados de forma organizada para a obtenção de conclusões sobre o tema de pesquisa. O capítulo 3 conclui a pesquisa, oferecendo uma visão geral sobre os resultados obtidos e fornece bases para trabalhos futuros que podem usufruir da metodologia utilizada para fazer análise derivadas sobre a área.

1.1 Fundamentação Teórico-Methodológica

1.1.1 Revisões sistemáticas de literatura

Revisões sistemáticas são estudos secundários ou meta-estudos, isso quer dizer que eles têm como objeto de pesquisa trabalhos científicos primários. Normalmente essas revisões buscam resumir temas de trabalhos relevantes que estão sendo publicados sobre um determinado domínio, eles fazem isso para sintetizar a vanguarda de uma área específica, mostrando para as pessoas que decidem ingressar em pesquisas semelhantes, como está o estado da arte dos trabalhos. Esses *checkpoints* da literatura funcionam como fotografias do que a comunidade científica está pesquisando e, dependendo da velocidade no avanço de pesquisas nas áreas sintetizadas, devem ser atualizados ou refeitos periodicamente.

Revisões sistemáticas de literatura surgiram como uma contraposição às tradicionais revisões narrativas [5], pois estas tiveram sua validade científica criticada por serem associadas à escrita e à autoridade de especialistas ou grupos de pesquisa específicos, com processos particulares e não analisáveis. A aplicação da metodologia científica sobre revisões é o que caracteriza as revisões sistemáticas, formalizando essa classe de meta-estudos e restringindo-a ao uso de regras que tornam esse tipo de contribuição replicável.

1.1.2 Mapeamento sistemático de literatura

O mapeamento sistemático da literatura faz parte de um conjunto de variações da revisão sistemática, que diferenciam-se de uma revisão comum, com características próprias e com um papel específico. A especificidade do mapeamento sistemático cumpre a tarefa de revisar um tema de pesquisa amplo, tentando compreender o que ocorre na área em aspectos gerais, necessitando de um volume grande de amostras como objeto de estudo, e evidenciando de forma visual o que foi identificado com a pesquisa [5].

1.1.3 Internet das coisas (IoT)

A IoT é um paradigma tecnológico caracterizado por um conjunto possivelmente heterogêneo de dispositivos espacialmente separados, que são capazes de conter funções de: identificação, sensorização, atuação, comunicação, processamento e análise de dados. Estando aptos a comunicar-se uns com os outros e com a internet, sem necessariamente requerer de interação humana, possibilitando a formação de uma rede de topologia dinâmica conectada globalmente [6].

Esses dispositivos são utilizados em diversas áreas, como:

- Produção industrial;
 - monitoramento [6][7];
 - transporte;
-

- rastreamento [6] e manutenção preventiva [6];
- abastecimento em tempo real da infraestrutura de cidades [7];
- saúde, por via de monitoramento e controle de sinais e indicadores de estado corpóreo, utilizando-se de dispositivos vestíveis ou mesmo dispositivos mantidos internos ao corpo [7].

1.1.4 Segurança da informação

A segurança da informação é caracterizada, primordialmente, pela manutenção ponderada da tríade confidencialidade, integridade e disponibilidade (**CIA**, da sigla em inglês) da informação [8]. Ela é necessária, pois a aplicação de tecnologia - que nunca será perfeita e sempre estará em mudança - sobre a informação causa riscos sobre os sistemas que se baseiam nessa tecnologia [9]. A obtenção de segurança da informação se dá através da aplicação de condutas que atentem a minorar riscos de que eventos de acesso indevido (quebra de confidencialidade); interrupção, deleção, corrupção, modificação (quebras de integridade); bloqueio de serviço (quebra de disponibilidade); etc. de dados que tenham criticidade sobre os sistemas os quais os utilizam[8].

1.1.5 Confiabilidade de sistemas computacionais

A confiabilidade de um sistema computacional é a qualidade do serviço entregue, de maneira a dependência ser justificavelmente empregada neste serviço [10]. A confiabilidade pode ser melhor descrita por meio de três conceitos: ameaças à obtenção de confiabilidade, meios de obtenção de confiabilidade e medidas de mensuração de confiabilidade.

Os fatores que ameaçam a obtenção de confiabilidade em sistemas podem ser encadeados no seguinte curso: falhas (*fault* do inglês), que podem ser ocorrências naturais, físicas ou intrínsecas do sistema. Tais ocorrências, quando ativas, se manifestam no sistema como erros, ou seja, o sistema contém um estado errôneo, que esse pode, subsequentemente, causar um defeito ou catástrofe (*failure* seria o termo usado para significar isso em inglês). Defeitos se caracterizam pela incapacidade do sistema de entregar o serviço proposto pelo mesmo de acordo com

sua descrição. Um exemplo desse encadeamento pode ser uma evento eletromagnético causar uma falha em um bloco de memória volátil, que se manifesta em um erro no estado da informação armazenada, causando uma falha no serviço descrito pelo fabricante do bloco de memória [11][12].

Os meios de obtenção de confiabilidade em sistemas computacionais são definidos por um conjunto de técnicas: a **prevenção de falhas**, que são formas de prevenir que o sistema admita a inserção de falhas, ou que elas ocorram. Tais prevenções são obtidas durante a fase de *design* e produção de sistemas; a **tolerância a falhas**: que são formas de fazer o sistema, mesmo com a presença de falhas, entregar o serviço correto de acordo com sua definição, é construída, em sistemas computacionais, a partir da detecção de erros e da posterior recuperação, do componente do sistema, de um estado errôneo para um estado correto; a **remoção de falhas**: caracteriza-se por maneiras de mitigar em número, ou em gravidade, as falhas. Ela é feita durante a vida útil dos sistemas através de manutenção preventiva ou corretiva, e também na fase de produção pelos processos de verificação, diagnóstico e correção; e a **previsão de falhas**: métodos que avaliam o sistema e estimam a quantidade presente e futura de falhas e as possíveis consequências da existência dessas. Tais métodos de avaliação se apresentam de maneira qualitativa e quantitativa [11][12].

A confiabilidade no sentido das medidas de mensuração é tida como um conceito “guarda-chuva” que agrega os atributos: disponibilidade, que é a prontidão da entrega do serviço correto; confiabilidade (no sentido restrito, *reliability* do inglês), que é a entrega contínua do serviço correto; segurança (para confiabilidade seria o termo inglês *safety*, e não o termo *security*), que é a ausência de defeito, de estados errôneos irrecuperáveis, de uma catástrofe para o ambiente ou o usuário do sistema; confidencialidade, que é o não extravio de informação; integridade, que é a ausência de alterações impróprias do estado do sistema; manutenibilidade, que é a habilidade de ser reparável e modificável [11][12].

1.1.6 Fundamentação de termos

- *Edge*: Paradigma de programação distribuída que aproxima a computação e o armazenamento de dados das fontes de dados.
 - *Fog*: (Nevoeiro do inglês) é uma camada do IoT onde o poder de processamento se aproxima do limite da rede.
 - *Confidentiality*: A confidencialidade é a propriedade da informação que limita seu acesso apenas a agentes autorizados.
 - *Availability*: A disponibilidade (definido em 1.1.5).
 - *Safety*: A segurança (definido em 1.1.5).
 - *Reliability*: A confiabilidade (definido em 1.1.5).
 - *Integrity*: A integridade (definido em 1.1.5).
 - *Device layer*: Camada IoT que trata dos dispositivos finais (sensores e atuadores).
 - *Fog/Edge layer*: Camadas intermediárias do IoT, ambas as camadas foram agregadas com uma só para 2.3.2, isso se deu por sua similaridade funcional.
 - *Network layer*: Camada de rede IoT. Para a classificação como camada *network*, foram consideradas as técnicas que possuem como alvo a comunicação, independentemente de qual camada para qual camada a comunicação é efetuada.
 - *Cloud layer*: A camada da "nuvem" IoT, onde processamento é alocado sob demanda para o processamento e o armazenamento de dados coletados e processados nas camadas inferiores (*Fog/Edge, Device*).
 - *Machine learning*: Termo que agrega técnicas de aprendizagem de máquina.
 - *Encryption scheme*: Termo que agrega esquemas de criptografia.
 - *Blockchain*: Tecnologia de registro distribuído que visa utilizar descentralização como meio de obtenção de segurança.
 - *Optimization*: Técnicas de computação que objetivam resolver um problema através da seleção do melhor elemento dentre um conjunto de alternativas de acordo com algum critério.
 - *Behavior monitoring*: Monitoramento de comportamento, técnicas utilizadas por sistemas detectores de intrusão.
-

1.2 Trabalhos relacionados

Com a IoT transitando para um período de maturidade do Ciclo de *Hype* tecnológico [13][14], a exploração especulativa amortece e o interesse em como tornar esse conjunto tecnológico mais resiliente e seguro aumenta para os pesquisadores e *stakeholders* com real interesse de longo prazo na área. Com um conjunto maior de publicações indo para essa direção, revisões sistemáticas começam a ser realizadas a efeito de comunicar o estado da arte, novidades, e termos novos que estão se agregando ao desenvolvimento de pesquisas na área.

Nesse contexto, houve um trabalho de revisão com um espaçamento temporal maior (2008 - 2021) que resumiu as áreas envolvidas com IoT e os principais problemas relacionados à segurança em cada uma das camadas de uma generalização arquitetônica [15] especificada no trabalho; uma revisão sobre os desafios de modelagem de confiabilidade IoT em cada camada (percepção, comunicação, suporte e aplicação), destilando cada técnica utilizada em cada camada[16]; uma revisão sobre os desafios da quantificação de confiabilidade em IoT, baseando-se em disciplinas onde o conceito já é estabelecido, refinando a ideia de quantificação de confiabilidade ao ponto de defini-la para os componentes da IoT [17]; uma revisão focada em soluções de segurança para os componentes de software do IoT [18]; e uma revisão focada na confiabilidade da camada de arquitetura *Fog* proposta para IoT [19].

Diferentemente da literatura existente, este trabalho explora os temas de segurança e confiabilidade para IoT, de maneira geral, com uma metodologia baseada em processos facilmente replicáveis, além disso, enquanto alguns dos trabalhos citados utilizam intervalos de tempo maiores, esta pesquisa se concentra em um recorte anual. Outra característica distinta é este ser um mapeamento sistemático - o que exige uma quantidade superior de trabalhos, quando comparados com revisões - e difere em propósito de outras revisões, tendo o objetivo de estruturar a área de pesquisa [20].

2 Mapeamento sistemático da literatura

O objetivo deste estudo de mapeamento é determinar, a partir de extração de dados, as atuais adversidades e soluções mais relevantes pesquisadas em segurança e confiabilidade de sistemas IoT, destacando as áreas onde estes sistemas estão sendo aplicados, através de uma visão geral e expositiva. Dessa forma estruturando o conhecimento pesquisado na borda dessa subárea.

2.1 Metodologia de pesquisa

2.1.1 Perguntas de pesquisa

QP1: Em que áreas os sistemas IoT estão sendo empregados de forma essencial para o funcionamento?

QP2: Quais são as adversidades em nível de sistema (o agregado funcional de dispositivos IoT mais os sistemas que se comunicam com eles), e em nível de componente (cada dispositivo que compõe o sistema) para a obtenção de confiabilidade e segurança em sistemas IoT?

QP3: Quais são as principais tecnologias/técnicas garantidoras de confiabilidade e segurança que estão sendo pesquisadas para sistemas IoT?

2.1.2 Estratégia de busca

2.1.2.1 Bases de pesquisa

As seguintes fontes de pesquisa foram escolhidas por serem revisadas por pares e serem de comum busca quando os temas se relacionam com computação e tecnologia:

- ACM;
- IEEE;
- ScienceDirect;
- Springer.

Dessas bases foram extraídos os dados referentes a artigos; para dados dos autores dos artigos foi escolhido o Google Scholar.

2.1.2.2 Frase de busca

Para a formulação da frase de busca foram identificadas as seguintes palavras-chaves em inglês: *dependable*, *security*, *iot*, *system*. Essas foram agrupadas em três grupos de termos (*dependable*, *security*), (*iot*) e (*system*); conceitos e termos relacionados foram extraídos deles, respectivamente, formando a:

- lista 1: 'dependable', 'dependability', 'reliability', 'availability', 'maintainability', 'safety', 'reliable', 'qos', 'security', 'failure', 'fault', 'redundancy', 'fault tolerant', 'latent error', 'fault removal', 'fault forecasting', 'fault avoidance', 'fault tolerance', 'error removal', 'error forecasting', 'physical faults', 'human-made faults', 'design faults', 'interaction faults', 'elementary failure', 'corrective maintenance', 'preventive maintenance', 'error processing', 'error recovery', 'error compensation', 'error detection', 'error masking', 'confidentiality', 'integrity', 'availability', 'security attributes', 'information security', 'vulnerabilities', 'threats', 'authenticity', 'non-repudiation', 'privacy', 'auditability', 'authentication';
 - lista 2: 'iiot', 'fog', 'iot', 'm2m', 'wsn', 'iomt'; e a
-

- lista 3: 'systems', 'devices', 'system', 'device', 'software', 'hardware', 'middleware', 'component', 'components', 'computing', 'service'.

Simplificando palavras chaves na lista 1 (com junções e utilizando os operadores *OR* e *AND*), ligando as simplificações resultantes e as palavras chave das listas com o operador lógico *OR*, e conectando as três listas com *AND*, foi obtida a frase de busca expandida, que pode ser vista na tabela 1.

Tabela 1. Frase padrão de busca.

(dependable **OR** dependability **OR** reliability **OR** availability **OR** maintainability **OR** safety **OR** reliable **OR** fault tolerant **OR** qos **OR** security **OR** failure **OR** fault **OR** latent error **OR** fault-avoidance **OR** fault-tolerance **OR** fault removal **OR** fault forecasting **OR** error-removal **OR** error-forecasting **OR** fault avoidance **OR** fault tolerance **OR** error removal **OR** error forecasting **OR** redundancy **OR** ((physical **OR** human-made **OR** design **OR** interaction) **AND** (faults)) **OR** elementary failure **OR** ((corrective **OR** preventive) **AND** maintenance) **OR** (error **AND** (processing **OR** recovery **OR** compensation **OR** detection **OR** masking)) **OR** confidentiality integrity availability **OR** security attributes **OR** information security **OR** vulnerabilities **OR** threats **OR** authenticity **OR** non-repudiation **OR** privacy **OR** auditability **OR** authentication) **AND** (iiot **OR** fog **OR** iot **OR** m2m **OR** wsn **OR** iomt) **AND** (systems **OR** devices **OR** system **OR** device **OR** software **OR** hardware **OR** middleware **OR** component **OR** components **OR** computing **OR** service)

A adaptação da frase de busca para cada base de pesquisa ocorreu da seguinte forma: ACM,IEEE e Springer mantiveram a estrutura básica da frase padrão de busca (Tabela 1); enquanto a ScienceDirect, por uma restrição da sua ferramenta de busca que impunha um limite menor que oito operadores lógicos por frase de busca, necessitou de uma estratégia para a captura do intento da frase de busca original. Essa estratégia foi construída da seguinte maneira: na lista 1 foram aglutinados os termos da tríade *CIA*; as listas tiveram as palavras chave fixadas na ordem mostrada na tabela 2;

Tabela 2. Conjuntos de palavras chaves derivadas.

["dependable", "dependability", "reliability", "availability", "maintainability", "safety", "reliable", "fault tolerant", "qos", "security", "failure", "fault", "latent error", "fault removal", "fault forecasting", "fault avoidance", "fault tolerance", "error removal", "error forecasting", "redundancy", "physical faults", "human-made faults", "design faults", "interaction faults", "elementary failure", "corrective maintenance", "preventive maintenance", "error processing", "error recovery", "error compensation", "error detection", "error masking", "confidentiality integrity availability", "security attributes", "information security", "vulnerabilities", "threats", "authenticity", "non-repudiation", "privacy", "auditability", "authentication"]
["iiot", "fog", "iiot", "m2m", "wsn", "iiomt"]
["system", "device", "software", "hardware", "middleware", "component", "computing", "service"]

as palavras chave da primeira linha da tabela 2 foram separadas em sete grupos de seis palavras (obedecendo a ordem da lista), cada grupo teve suas palavras unidas com o operador lógico *OR* (tabela 3); cada um desses grupos foi permutado com o conjunto das palavras chaves da segunda linha, que foi permutado com as palavras chave da terceira linha, unindo cada elemento permutado do grupo resultante com o operador *AND* e separando-os com parênteses (tabela 4). Resultando, dessa permutação, em um total de 336 frases de buscas.

Tabela 3. Grupos unidos pelo conector lógico *OR*.

["dependable" OR "dependability" OR "reliability" OR "availability" OR "maintainability" OR "safety"], ["reliable" OR "fault tolerant" OR "qos" OR "security" OR "failure" OR "fault"], ...

Tabela 4. Frases de busca resultantes das permutações.

("dependable" OR "dependability" OR "reliability" OR "availability" OR "maintainability" OR "safety") AND ("iiot") AND ("system")
("dependable" OR "dependability" OR "reliability" OR "availability" OR "maintainability" OR "safety") AND ("iiot") AND ("device")
...
("dependable" OR "dependability" OR "reliability" OR "availability" OR "maintainability" OR "safety") AND ("fog") AND ("system")
("dependable" OR "dependability" OR "reliability" OR "availability" OR "maintainability" OR "safety") AND ("fog") AND ("device")
...
("reliable" OR "fault tolerant" OR "qos" OR "security" OR "failure" OR "fault") AND ("iiot") AND ("system")
("reliable" OR "fault tolerant" OR "qos" OR "security" OR "failure" OR "fault") AND ("iiot") AND ("device")
...

2.1.2.3 Período de busca

Foi estipulado o período de busca de um ano, entre 01/01/2020 e 31/12/2021.

2.1.2.4 Critérios de inclusão

Estudos primários; estudos revisados por pares; estudos do tipo artigo.

2.1.2.5 Critérios de exclusão

Estudos secundários; artigos duplicados; artigos não escritos em inglês; artigos com métricas irrelevantes (2.2.1.5); artigos que fujam ao tema de pesquisa.

2.1.2.6 Conteúdo extraído

O conteúdo extraído dos artigos que foi utilizado para o mapeamento se resume a: Título do artigo, título da publicação, DOI (*digital object identifier*), ano de publicação, URL (*universal resource locator*), tipo de conteúdo, autores, *abstract*,

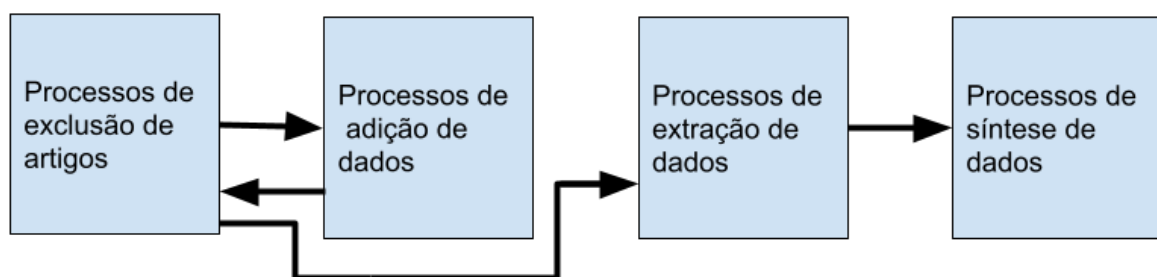
palavras chave, métricas (citações, downloads, acessos, métricas alternativas, visualizações, menções, leitores), base de onde foi extraído.

2.2 Processos aplicados

Para a obtenção de respostas para as perguntas feitas sobre o objeto de pesquisa (os dados coletados), é necessário que o mesmo seja sujeito a uma cadeia de processos que fará com que:

- Os dados utilizados estejam agregando conteúdo à pesquisa e não a diluindo, pois os processos empregados selecionam, a partir de filtros e leitura, apenas artigos que possam responder às questões de pesquisa;
- que métricas possam ser alavancadas para demonstrar de forma ponderada a importância de determinado artigo, conjunto de artigos relacionados, ou sub-área (2.2.2, 2.2.3);
- que termos possam ser retirados dos artigos para responder as perguntas.

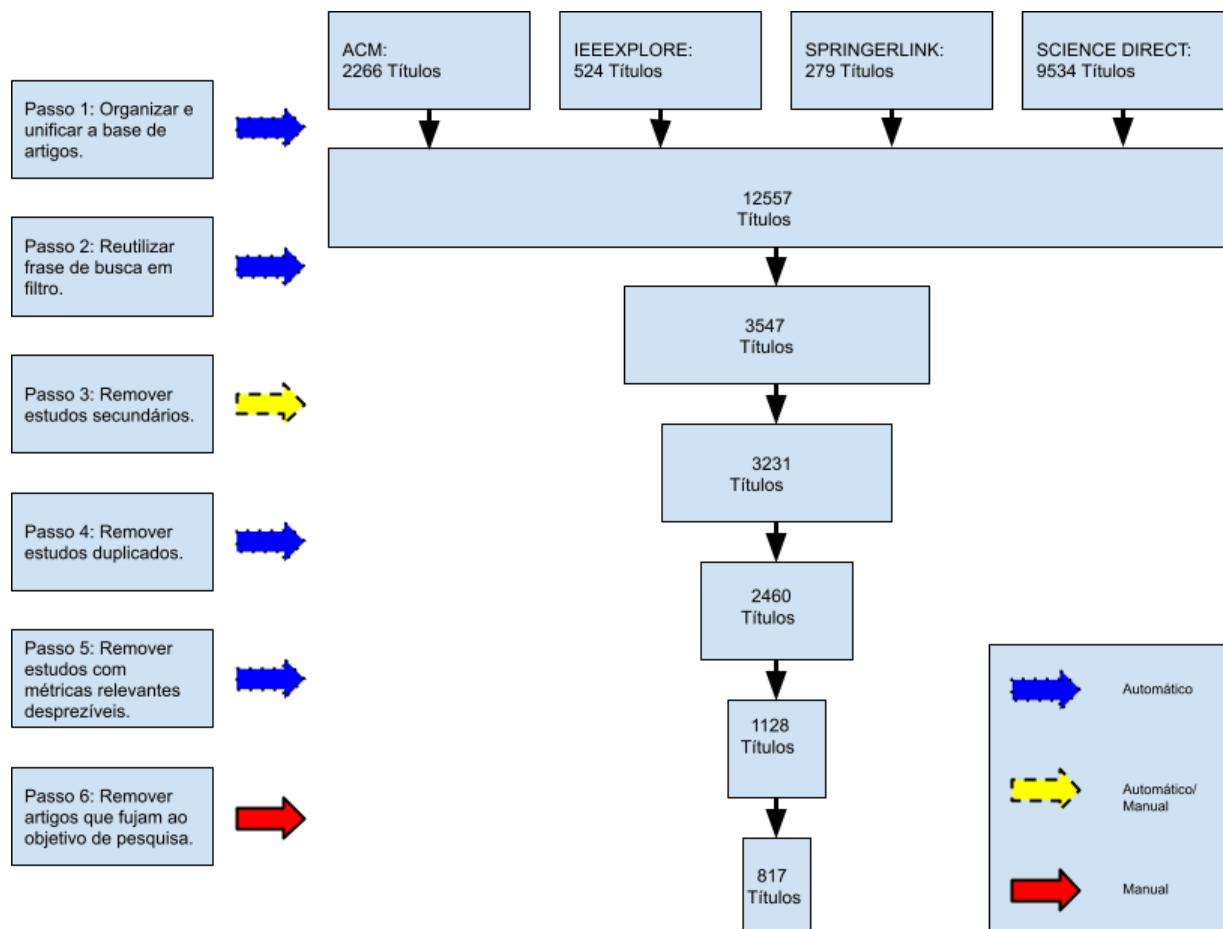
Figura 1. Processos aplicados nos dados coletados.



2.2.1 Processos de exclusão de artigos

Os dados coletados foram armazenados em arquivos csv. Tais arquivos foram processados - para a filtragem de apenas os artigos mais relevantes - com o uso de ferramentas como linguagens de programação, processadores de palavras e programas utilitários. Os processos realizados para exclusão podem ser observados na figura 2.

Figura 2. Processos de exclusão aplicados nos dados coletados.



2.2.1.1 Organizar e unificar a base de artigos

Nesse processo os dados de cada base foram unidos em uma única base. Como as bases possuem métricas diferentes entre si (**Tabela 5**, **Tabela 6**, **Tabela 7**, **Tabela 8**), todas as colunas de métricas de cada base foram mantidas para todas as linhas.

2.2.1.2 Reutilizar a frase de busca em filtro

Nesse processo, realizado para manter o conteúdo da pesquisa alinhado com o objetivo proposto, foi utilizado o filtro da tabela 1 em cada linha de dados, filtrando pelas colunas: título do artigo, *abstract* e palavras chave.

2.2.1.3 Remover os estudos secundários

Nesse processo foram elencadas listas de palavras relacionadas com estudos secundários, então, com elas, foi filtrado um conjunto de dados separados, onde foram manualmente retirados os estudos secundários. O restante foi recolocado no conjunto total de dados.

2.2.1.4 Remover os estudos duplicados

Nesse processo foram eliminadas as duplicatas de artigos utilizando como indexador de comparação: título do artigo, DOI, URL, *abstract*.

2.2.1.5 Remover estudos com métricas relevantes desprezíveis

Para a realização desse processo, de forma preparativa, foram extraídos resumos estatísticos dos dados agregados por base de pesquisa, vide tabelas 5, 6, 7, 8.

As tabelas estão segregadas por bases de pesquisa, e possuem sumários estatísticos das métricas de artigos apenas dessas bases. O sumário nos mostra, respectivamente, a média, o desvio padrão, o menor valor de métrica, os três primeiros quadrantes (quadrantes são formas de separar os dados de um conjunto ordenado), e o máximo valor da métrica encontrado no conjunto.

Tabela 5. Sumário estatístico de métricas da base ACM.

	citations	downloads	accesses	altmetric	views	mentions	readers
mean	0.934097	74.849570	-	-	-	-	-
std	2.316731	273.621200	-	-	-	-	-
min	0	0	-	-	-	-	-
25%	0	0	-	-	-	-	-
50%	0	0	-	-	-	-	-
75%	1	64	-	-	-	-	-
max	33	6055	-	-	-	-	-

Tabela 6. Sumário estatístico de métricas da base SCIENCE DIRECT.

	citations	downloads	accesses	altmetric	views	mentions	readers
mean	8.305110	-	-	-	-	0.017543	32.496567
std	16.547317	-	-	-	-	0.176038	48.911258
min	0	-	-	-	-	0	0
25%	0	-	-	-	-	0	7
50%	3	-	-	-	-	0	19
75%	9	-	-	-	-	0	42
max	261	-	-	-	-	4	772

Tabela 7. Sumário estatístico de métricas da base IEEEEXPLORE.

	citations	downloads	accesses	altmetric	views	mentions	readers
mean	0.611904	-	-	-	138.5	-	-
std	1.818586	-	-	-	131.181422	-	-
min	0	-	-	-	4	-	-
25%	0	-	-	-	68.75	-	-
50%	0	-	-	-	108.5	-	-
75%	0	-	-	-	170	-	-
max	19	-	-	-	1784	-	-

Tabela 8. Sumário estatístico de métricas da base SPRINGERLINK.

	citations	downloads	accesses	altmetric	views	mentions	readers
mean	4.354838	-	627.483871	0.354838	-	-	-
std	6.452639	-	915.456129	0.984831	-	-	-
min	0	-	67	0	-	-	-
25%	0	-	168	0	-	-	-
50%	1	-	429	0	-	-	-
75%	5.5	-	665	0	-	-	-
max	27	-	5060	5	-	-	-

A métrica *Altmetric* da base SPRINGERLINK e a métrica *mentions* da base SCIENCE DIRECT foram identificadas como métricas com pouca informação relevante para a finalidade dessa pesquisa e portanto foram desconsideradas e removidas.

As métricas que sobraram, podem ser identificadas para cada base como:

- *citations* para todas;
- *downloads* para a ACM;
- *readers* para a SCIENCE DIRECT;
- *views* para a IEEEEXPLORE; e
- *accesses* para a SPRINGERLINK.

Elas refletem a interação de usuários com o artigo exposto. Logo, nesse processo, qualquer artigo que teve essas métricas com valor igual a zero foi removido.

2.2.1.6 Remover artigos que fujam ao objetivo de pesquisa

Esse processo, assim como o 2.2.1.2, foi realizado para manter o conteúdo da pesquisa alinhado com o objetivo proposto, com a diferença de ter sido feita uma revisão manual, filtrando pelas colunas: título do artigo e *abstract*. O processo foi realizado da seguinte forma: foram analisados os títulos dos artigos para verificar a congruência dos mesmos com o tema do mapeamento e se poderiam ajudar a responder às perguntas de pesquisa. Caso um título fosse suspeito de ser

incongruente com o tema de pesquisa, seu *abstract* seria testado, se a incongruência se comprovasse, o registro do artigo seria removido.

2.2.2 Processos de adição de dados

Os dados resultantes do processo 2.2.1 possuem um conjunto de autores para cada artigo; Foram pesquisadas métricas para esses autores, porém a métrica "citações" foi a única que pôde ser encontrada para todos. Logo, foi criado um conjunto de dados relacionando cada autor com o seu número de citações para ser usado novamente na exclusão de artigos:

Figura 3. Dados relacionando autores dos artigos com citações dos autores.

	Author	Citations
0	Anying Chai	28
1	Farzam Mohammadi	3
2	Baoru Han	120
3	M Devi	0
4	Haoyu Yu	0
...
2932	Xiao Li	304
2933	Xueli Feng	9
2934	Yuanfan Yao	2
2935	Yueh-Tiam Yong	3
2936	Zhiran Yi	705

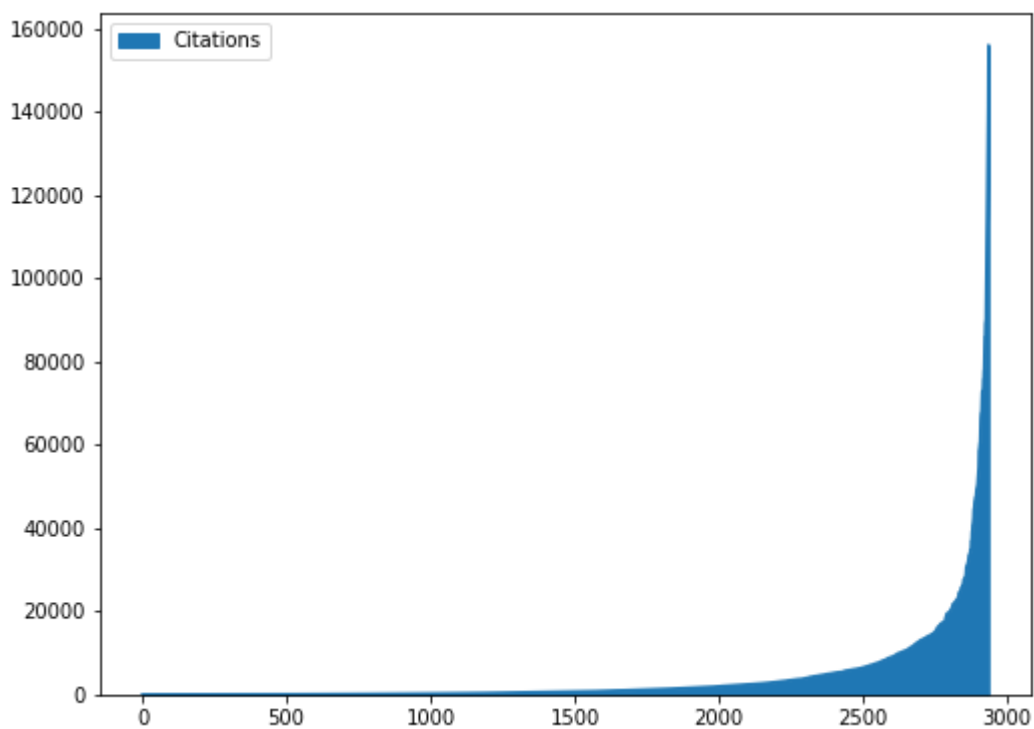
2.2.3 Processos de exclusão de artigos

A obtenção do conjunto de citações de autores no processo 2.2.2, possibilitou o relacionamento dessas citações com o conjunto de artigos, servindo assim para um novo processo de exclusão de artigos, que foi executado utilizando-se critérios que objetivam a seleção dos melhores trabalhos:

- Selecionar artigos que estejam relacionados com 1% dos autores com maior número de citações.

Essa seleção resultou em 40 artigos.

Figura 4. Gráfico ordenado do número de citações por autor.



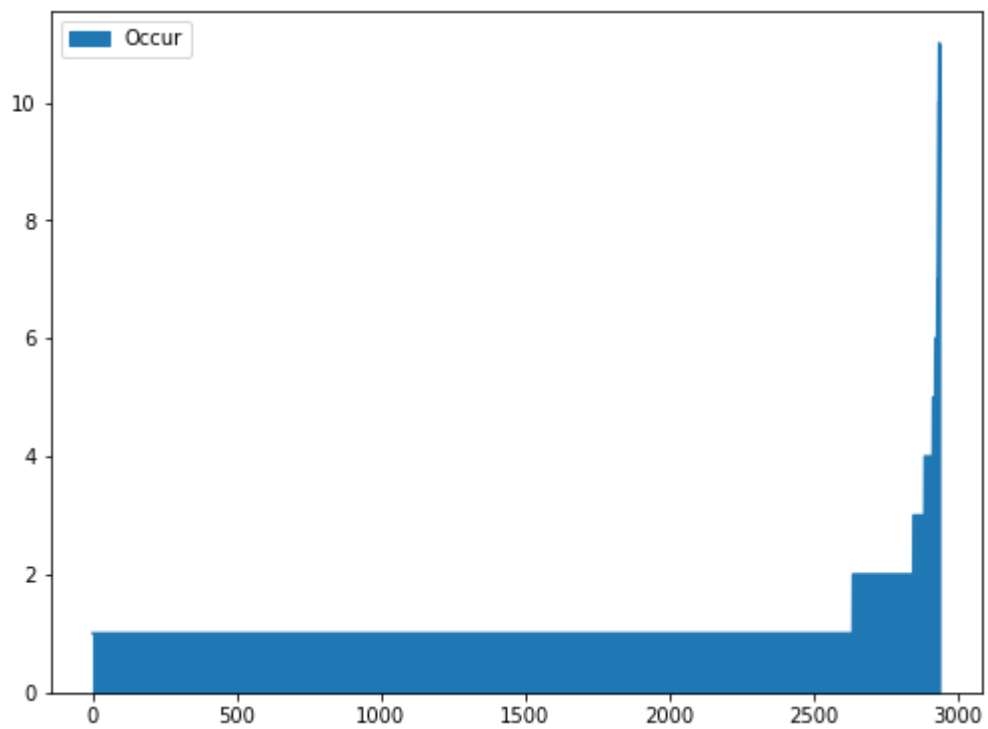
- Selecionar artigos relacionados com 1% dos autores que tenham mais contribuições no conjunto de artigos:

Essa seleção resultou em 111 artigos.

Figura 5. Tabela de autores ordenada por ocorrências de contribuições no conjunto de artigos.

	Author	Occur
0	Anying Chai	1
1891	Guanghai Wang	1
1892	Manuel Huber	1
1893	Dongkwan Kim	1
1894	Raffaele Bruno	1
...
2490	Mohsen Guizani	8
1875	Mamoun Alazab	9
1162	Gautam Srivastava	10
962	Kim-Kwang Raymond Choo	10
1966	Neeraj Kumar	11

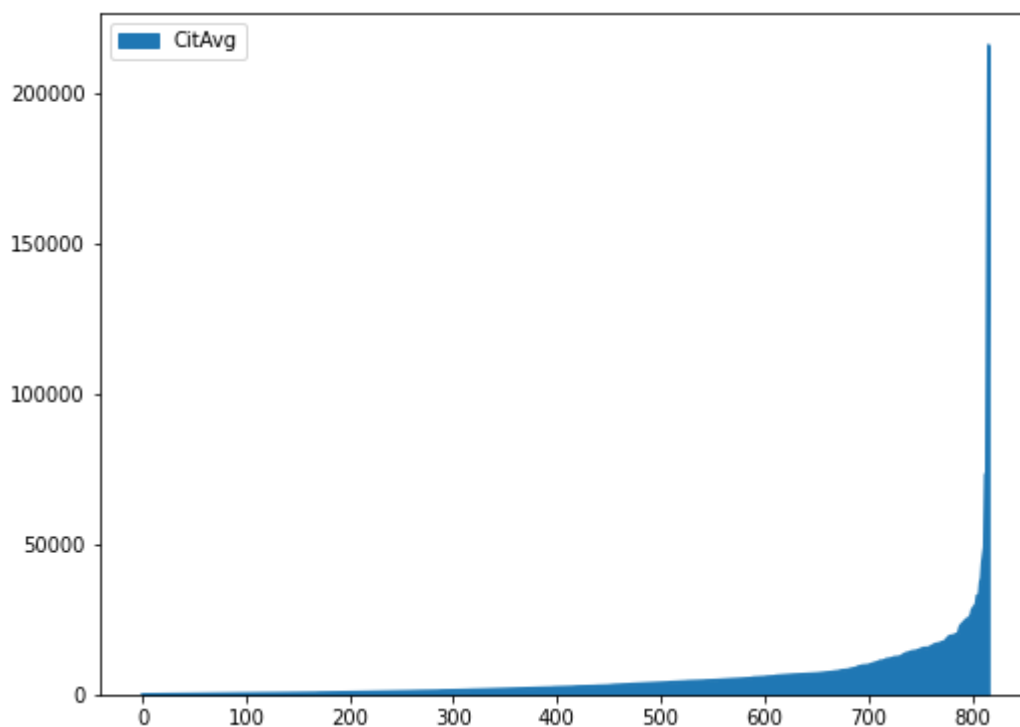
Figura 6. Gráfico ordenado do número de contribuições em artigos do conjunto de dados por autor.



- Selecionar os 5% artigos que possuam maior média de citações dos seus autores:

Essa seleção resultou em 39 artigos.

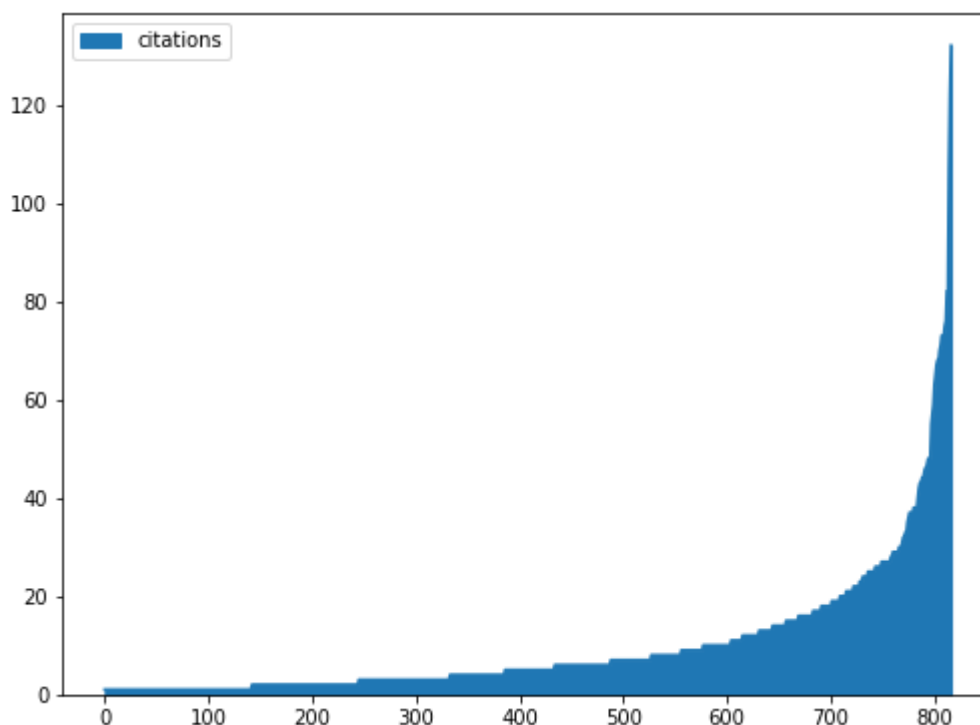
Figura 7. Gráfico ordenado do número médio de citações por autor em cada artigo.



- Selecionar os 5% de artigos com mais citações:

Essa seleção resultou em 8 artigos.

Figura 8. Gráfico ordenado de número de citações por artigo.



O conjunto de artigos resultante de cada exclusão foi então unido em um conjunto final, e as duplicatas foram retiradas, resultando em 143 artigos.

2.2.4 Processos de extração de dados

Os artigos resultantes do processo 2.2.3 serviram para o preenchimento das colunas da tabela de perguntas de extração de dados, que correspondem às perguntas de pesquisa. O preenchimento foi feito a partir da leitura dos dados de cada linha e, a partir desses dados, fazendo uma classificação da área de pesquisa que o artigo examina, dos problemas de segurança e/ou confiabilidade que ele se propõe a resolver e das técnicas ou meios utilizados para resolver os problemas propostos.

2.2.5 Processos de síntese de dados

Os dados resultantes do processo **2.2.4** foram sintetizados e agrupados em gráficos de pizza para demonstrar visualmente as respostas das questões de pesquisa.

2.3 Resultados

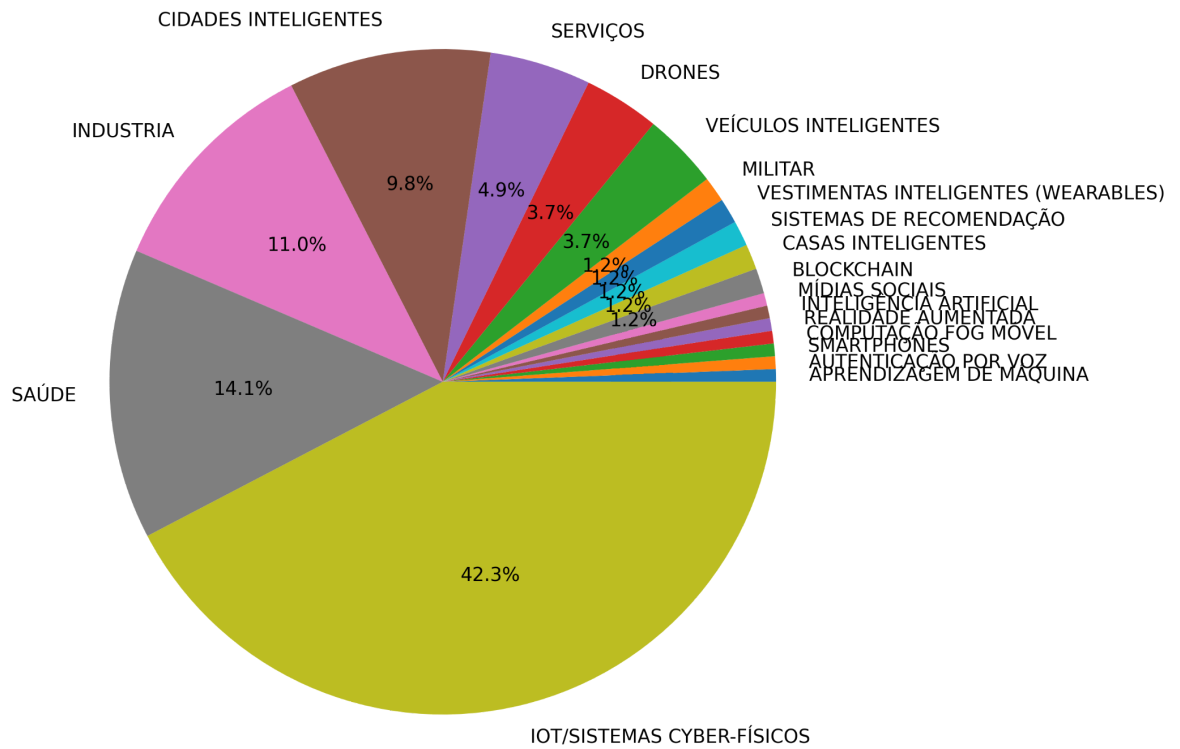
Retornando às perguntas de pesquisa, agora respondendo-as com os dados obtidos no mapeamento, que, após o longo processo de filtragem, possuem as publicações de artigos mais influentes do ano de 2020, dos autores mais citados e expostos às respectivas área de pesquisa, foram obtidos os seguinte resultados:

2.3.1 Resultados da pergunta de pesquisa 1

QP1: Em que áreas os sistemas IoT estão sendo empregados de forma essencial para o funcionamento?

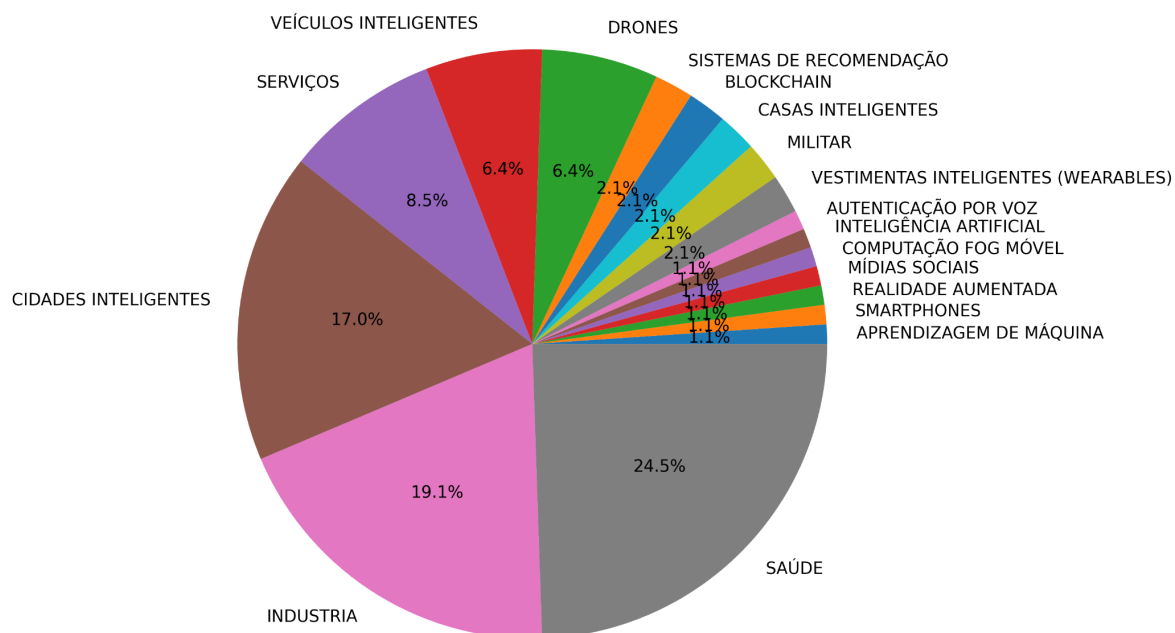
- Os dados apontaram que a maioria dos artigos trata da própria área como finalidade, ou não específica área alvo.
-

Figura 9. Gráfico em pizza das áreas onde os artigos sobre segurança/confiabilidade são aplicados.



- Para a melhor visualização das áreas alvo que foram especificadas, a **Figura 10** mostra o gráfico em pizza sem os artigos que tem como alvo o IOT/SISTEMAS CYBER-FÍSICOS:

Figura 10. Gráfico em pizza das áreas onde os artigos sobre segurança/confiabilidade são aplicados, excluindo os IOT/SISTEMAS CYBER-FÍSICOS.

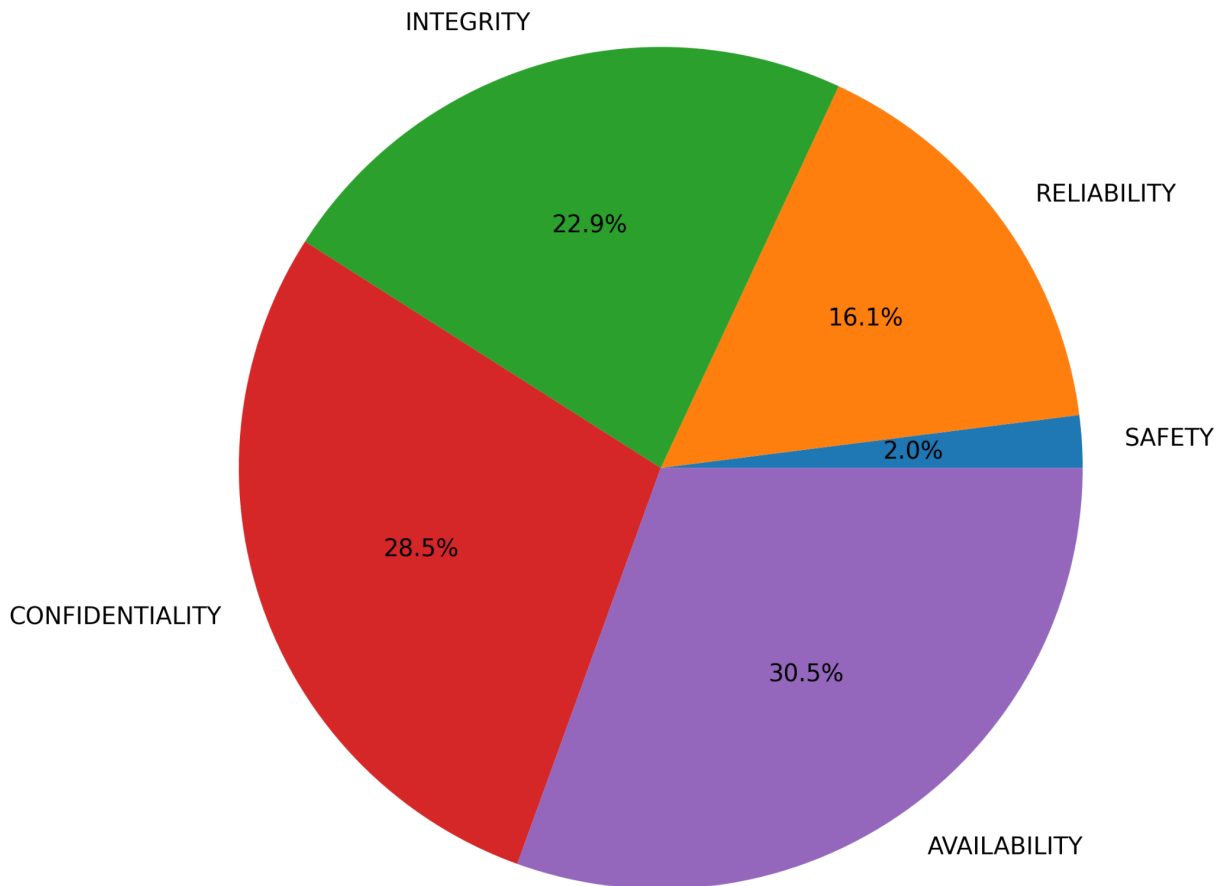


2.3.2 Resultados da pergunta de pesquisa 2

QP2: Quais são as adversidades em nível de sistema (o agregado funcional de dispositivos IoT mais os sistemas que se comunicam com eles), e em nível de componente (cada dispositivo que compõe o sistema) para a obtenção de confiabilidade e segurança em sistemas IoT?

- Adversidades para o agregado funcional:
 - O gráfico da **figura 11** demonstra que os atributos da tríade CIA da segurança da informação foram mais exploradas no ano de 2020:

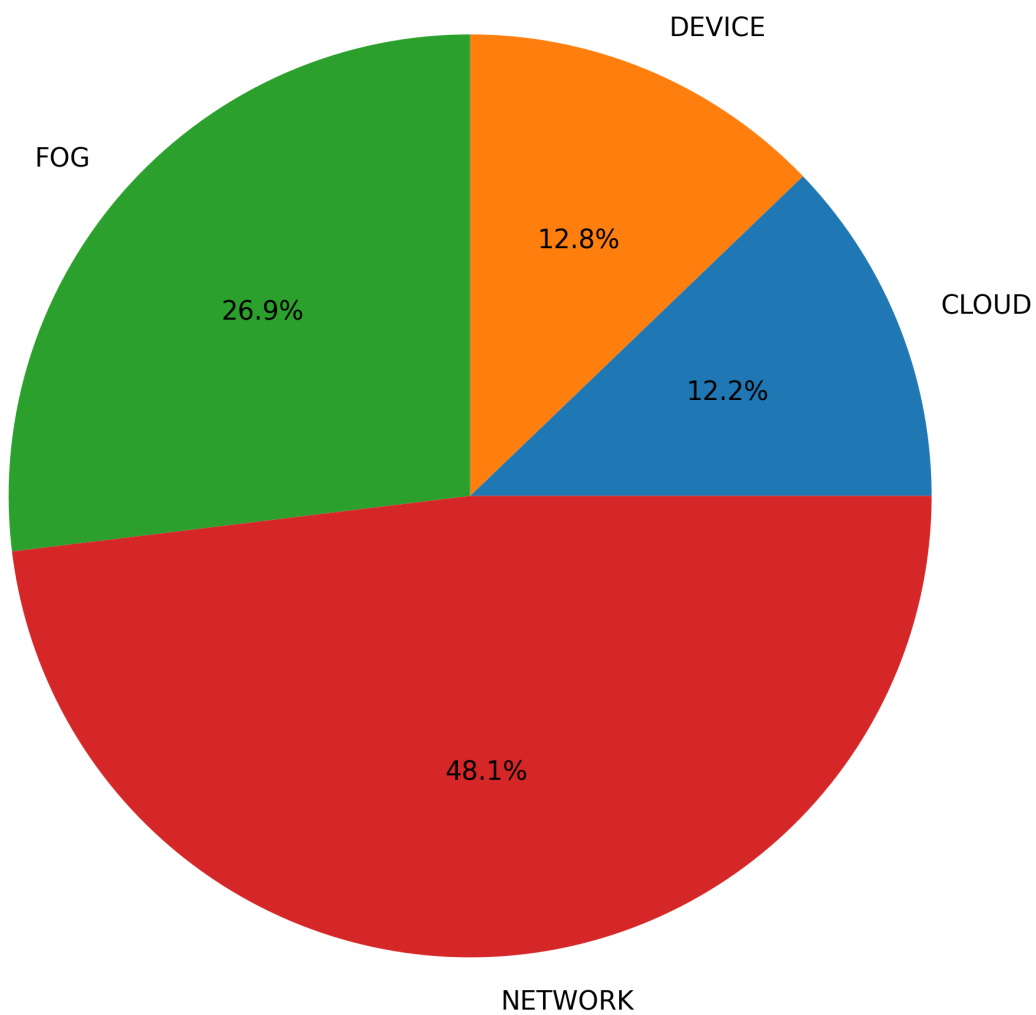
Figura 11. Gráfico em pizza dos atributos de segurança e confiabilidade que os grupos mais bem ranqueados de pesquisadores de sistemas IoT em 2020 deram atenção.



- Adversidades para cada componente:

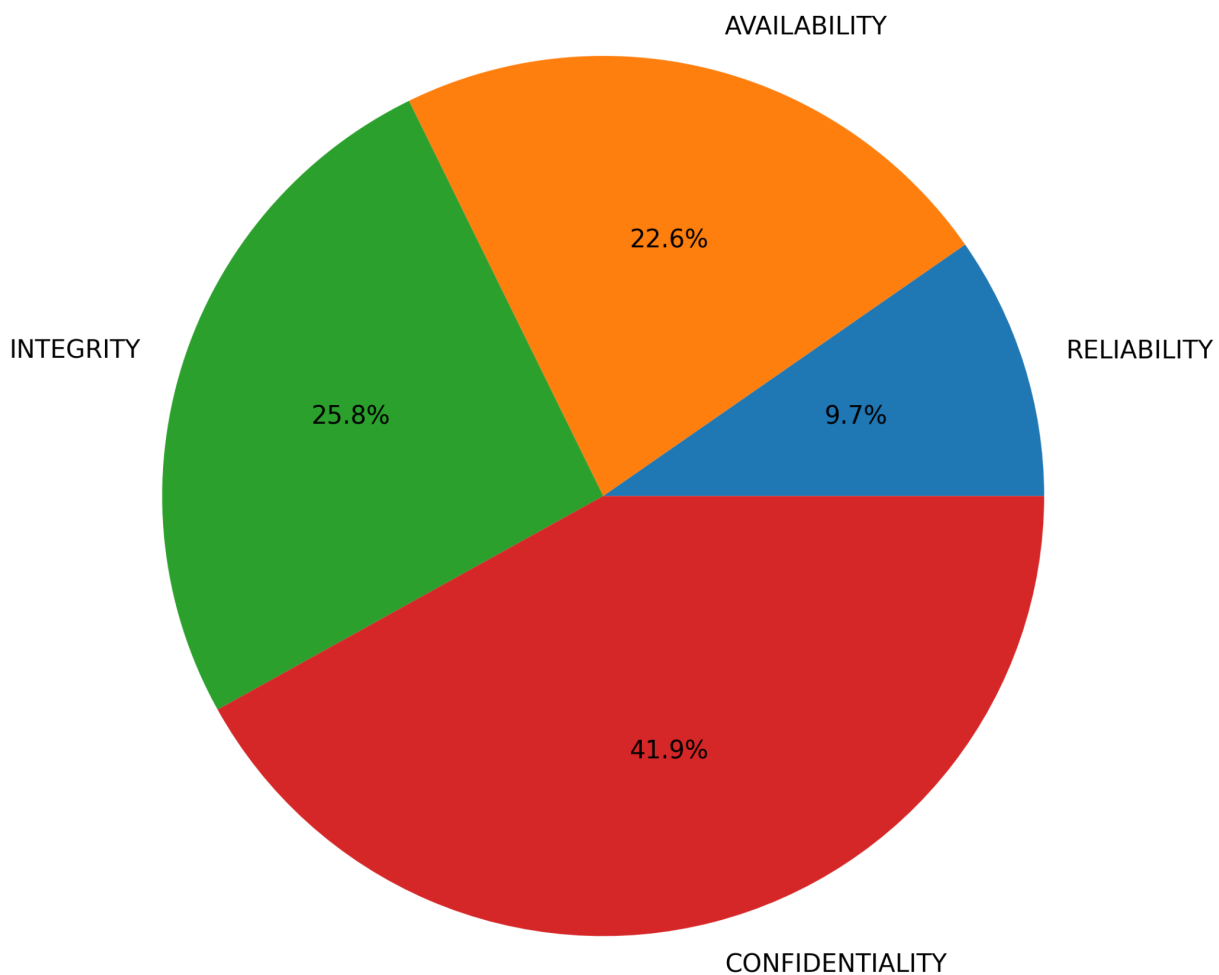
Os problemas que os artigos se propuseram a resolver no quesito de confiabilidade e segurança, foram agregados pela camada do IoT onde é aplicada a proposta de solução dos artigos:

Figura 12. Gráfico em pizza das camadas arquitetônicas elencadas a partir dos artigos.



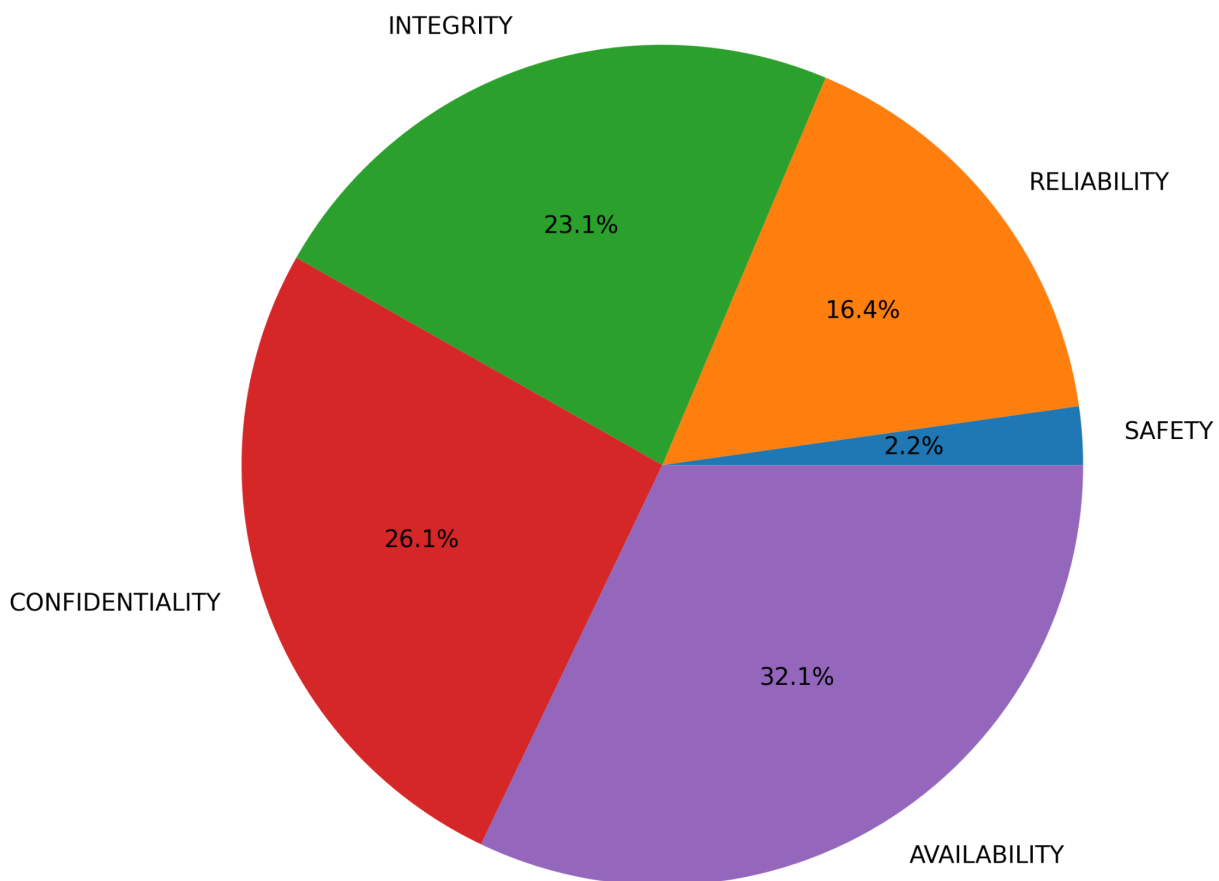
- CLOUD:

Figura 13. Gráfico em pizza dos problemas para obtenção de confiabilidade/segurança na *CLOUD*.



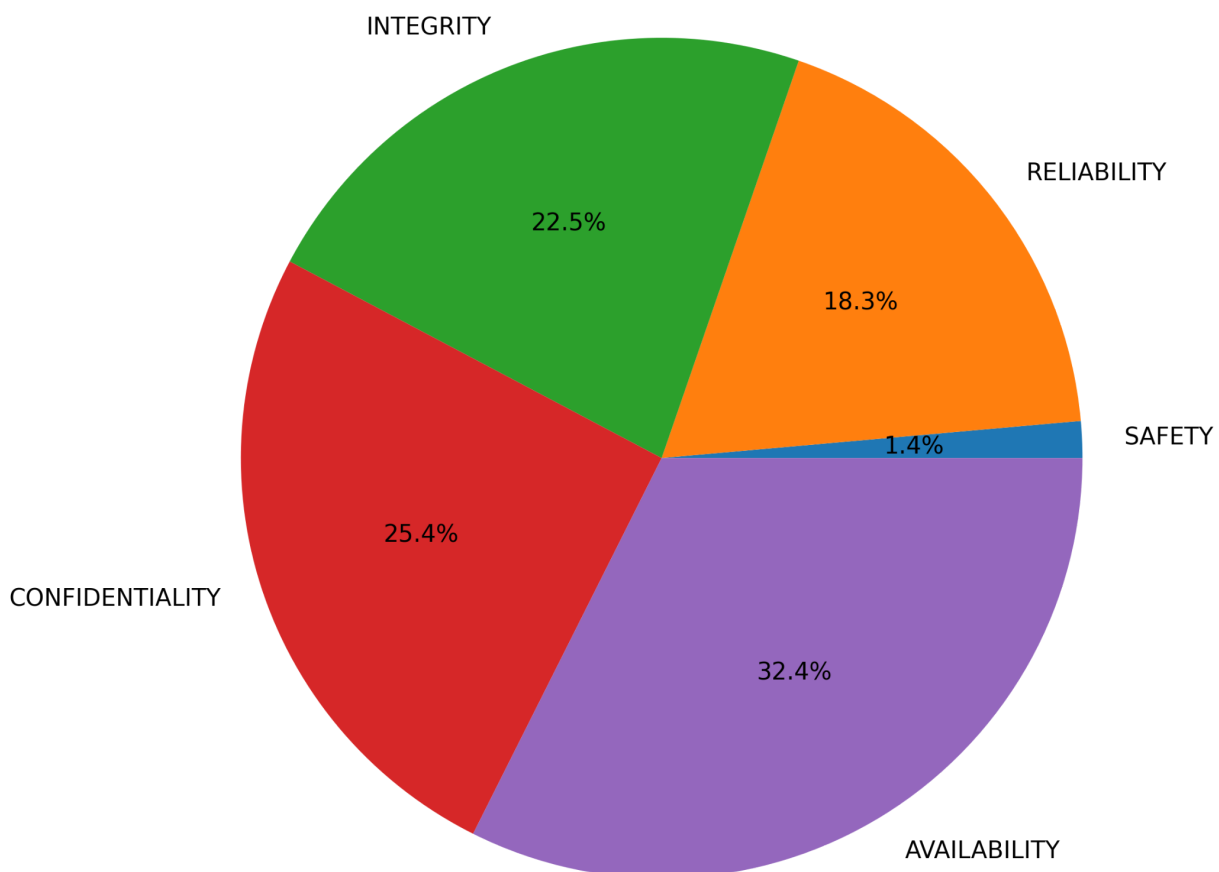
- NETWORK:

Figura 14. Gráfico em pizza dos problemas para obtenção de confiabilidade/segurança na *NETWORK*.



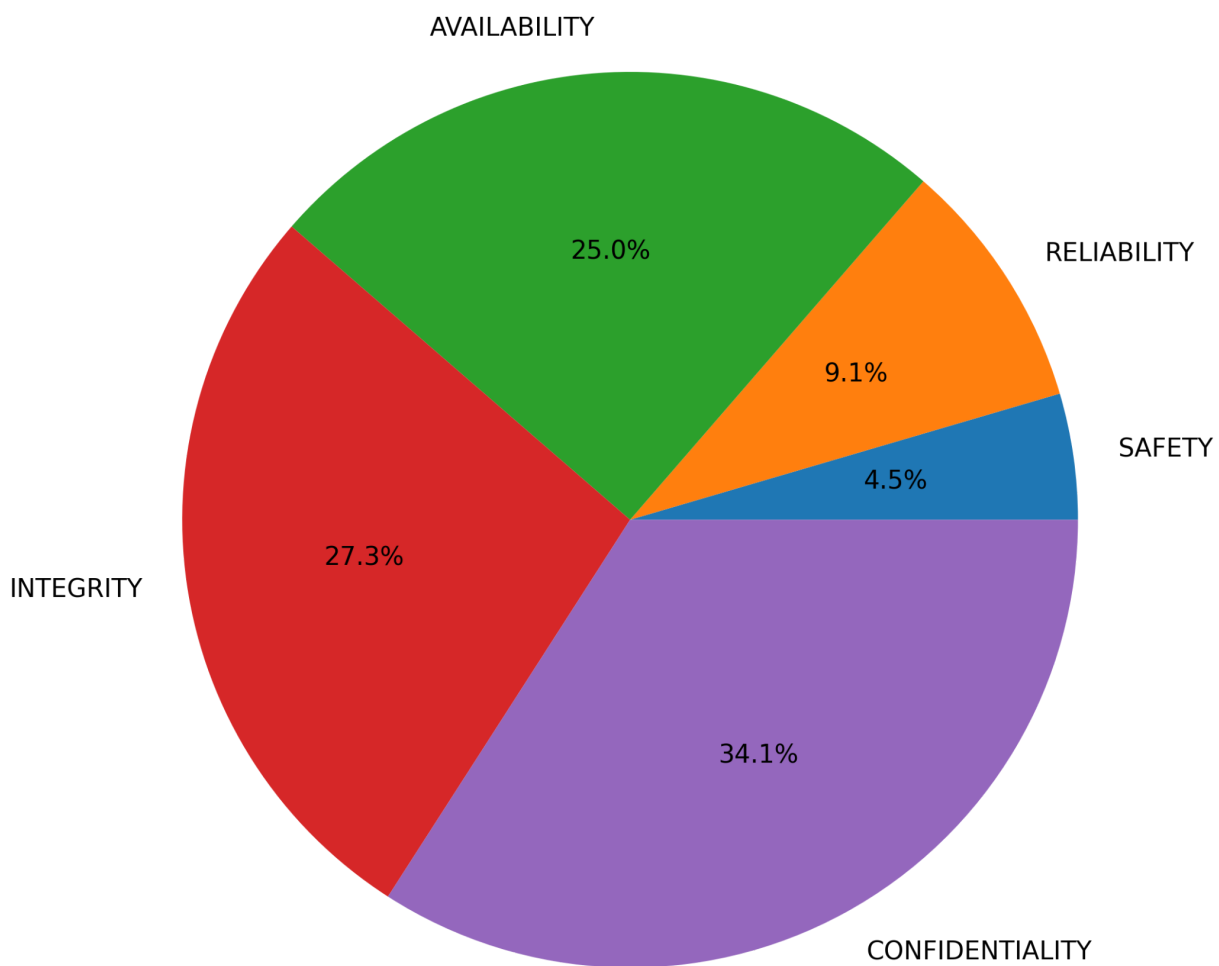
- FOG/EDGE:

Figura 15. Gráfico em pizza dos problemas para obtenção de confiabilidade/segurança na *FOG/EDGE*.



- DEVICE:

Figura 16. Gráfico em pizza dos problemas para obtenção de confiabilidade/segurança na *DEVICE*.

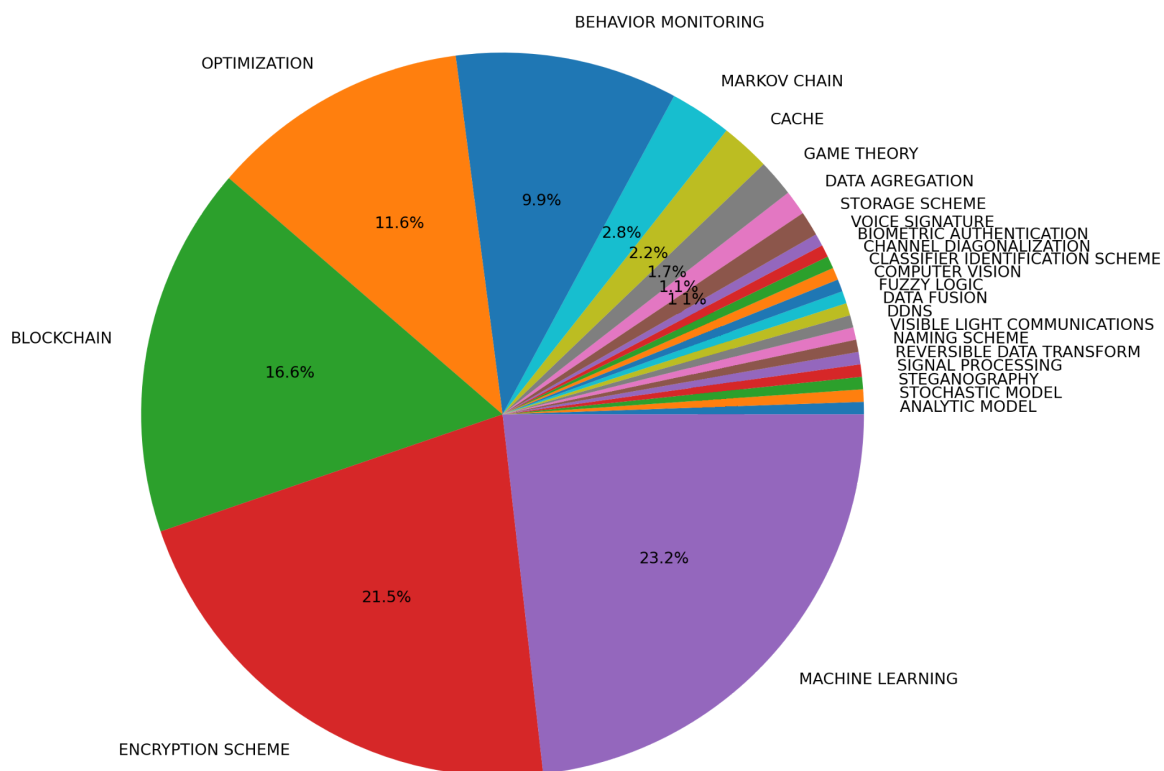


2.3.3 Resultados da pergunta de pesquisa 3

QP3: Quais são as principais tecnologias/técnicas garantidoras de confiabilidade e segurança que estão sendo pesquisadas para sistemas IoT?

- Na figura 17 é notável que esquemas de criptografia, aprendizagem de máquina, *blockchain*, monitoramento de comportamento por sistemas detectores de intrusão e algoritmos de otimização, foram as técnicas mais relevantes para os trabalhos mais relevantes em segurança e confiabilidade de dispositivos IoT em 2020:

Figura 17. Gráfico em pizza das tecnologias/técnicas garantidoras de confiabilidade e segurança mais utilizadas pelos trabalhos mais bem ranqueados de 2020.



3 Conclusão e Trabalhos Futuros

Os sistemas IoT são uma realidade, são pervasivos em vários ambientes onde a automação é essencial, são feitos úteis e ótimos com o montante de pesquisa que é feita para a sua adoção, recebem uma plethora de algoritmos e dispositivos que se combinam em novas aplicações.

Porém, para a grande quantidade de sistemas que é disponibilizada no mercado, há a necessidade de avaliações e propostas de melhoria na segurança e confiabilidade. Tarefa essa que necessita esforço de especialistas, esses necessitam priorizar quais técnicas estudar para obter o melhor resultado na sua pesquisa.

Ao realizar o mapeamento foi observado que existem lacunas nas áreas de pesquisa que recebem o enfoque dos pesquisadores mais citados, tais áreas não exploradas ficam sujeitas à objeto de estudo para novos trabalhos.

Os seguinte pontos podem ser melhorados ou abordados em trabalhos futuros:

- Aumentar a janela de análise para mais de um ano;
 - Automatizar o processo de filtragem manual;
 - Utilizar método inteligente para a extração dos dados ;
 - Utilizar um método mais acurado para a remoção dos dados dos autores ;
 - Retirar mais informação dos dados coletados, explorando mais combinações entre eles.
-

Referências

- [1] HEMPHILL, Thomas. **Wearable devices and healthcare: Data sharing and privacy**. An International Journal, vol. 34, p. 49-57, 2018.
 - [2] PIPETTI, Ryan. **Threat model for securing internet of things (IoT) network at device-level**. Internet of Things, vol. 11, 2020.
 - [3] FOUKALAS, Fotis. **Dependable Wireless Industrial IoT Networks: Recent Advances and Open Challenges**. 2019 IEEE European Test Symposium (ETS), p. 1-10, 2019.
 - [4] KOOT, Martijn. **A systematic literature review of supply chain decision making supported by the Internet of Things and Big Data Analytics**. Computers & Industrial Engineering, vol. 154, 2021.
 - [5] MOHER, David. **All in the Family: systematic reviews, rapid reviews, scoping reviews, realist reviews, and more**. Systematic Reviews, vol. 4, 2015.
 - [6] LEE, In. **The Internet of Things (IoT): Applications, investments, and challenges for enterprises**. Business Horizons, vol. 58, p. 431-440, 2015.
 - [7] MOLONEY, Patricia. **The Internet of Things (IoT): An Overview**. Congressional Research Service (CRS), 2020. Disponível em: <https://crsreports.congress.gov/product/pdf/IF/IF11239>
 - [8] FLETCHER, Martin. **An introduction to information risk**. The National Archives, 2016. Disponível em: <https://blog.nationalarchives.gov.uk/introduction-information-risk>
 - [9] BLAKLEY, Bob. **Information Security is Information Risk Management**. Association for Computing Machinery, p. 97–104, 2001.
 - [10] J.-C. Laprie, **DEPENDABLE COMPUTING AND FAULT TOLERANCE : CONCEPTS AND TERMINOLOGY**. Twenty-Fifth International Symposium on Fault-Tolerant Computing, 1995, ' Highlights from Twenty-Five Years', p. 2, 1995.
 - [11] J.-C. Laprie, **Fundamental Concepts of Dependability**. Technical Report, Department of Computing Science Technical Report Series, 2001. Disponível em: https://www.researchgate.net/publication/2408079_Fundamental_Concepts_of_Dependability
 - [12] J.-C. Laprie, **Basic Concepts and Taxonomy of Dependable and Secure Computing**. IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, vol. 1, 2004.
 - [13] AHMED, Bestoun S. **Aspects of Quality in Internet of Things (IoT) Solutions: A Systematic Mapping Study**. IEEE Access, vol. 7, p. 13758-13780, 2019.
-

-
- [14] PANETTA, Kasey. **5 Trends Emerge in the Gartner Hype Cycle for Emerging Technologies, 2018**. gartner, 2019. Disponível em: <https://www.gartner.com/smarterwithgartner/5-trends-emerge-in-gartner-hype-cycle-for-emerging-technologies-2018>
- [15] BEKKALI, Abla El. **Systematic Literature Review of Internet of Things (IoT) Security**. Advances in Dynamical Systems and Applications, vol. 16, p. 1671-1692, 2021.
- [16] XING, Liudong. **Reliability in Internet of Things: Current Status and Future Perspectives**. IEEE Internet of Things Journal, vol. 7, p. 6704-6721, 2020.
- [17] MOORE, S.J.. **IoT reliability: a review leading to 5 key research directions**. CCF Transactions on Pervasive Computing and Interaction. vol. 2, p. 147–163, 2020.
- [18] LIAO, Zitian. **Assessing Security of Software Components for Internet of Things: A Systematic Review and Future Directions**. Security and Communication Networks, vol.2021, 2021.
- [19] BAKHSHI, Zeinab. **Dependable Fog Computing: A Systematic Literature Review**. 2019 45th Euromicro Conference on Software Engineering and Advanced Applications (SEAA), p.395-403, 2019.
- [20] PETERSEN, Kai. **Guidelines for conducting systematic mapping studies in software engineering: An update**. Information and Software Technology, vol. 64, p. 1-18, 2015.
-