

Mapeamento Sistemático Sobre Sistemas IoT no Domínio Smart Homes

Antônio Cézar Vieira



CENTRO DE INFORMÁTICA
UNIVERSIDADE FEDERAL DA PARAÍBA

João Pessoa, 2018

Antônio Cézar Vieira

Mapeamento Sistemático Sobre Sistemas IoT no Domínio Smart Homes

Monografia apresentada ao curso Ciência da Computação
do Centro de Informática, da Universidade Federal da Paraíba,
como requisito para a obtenção do grau de Bacharel em titulo

Orientador: Prof^a Dr^a Danielle Rousy Dias da Silva

Junho de 2018

**Catalogação na publicação
Seção de Catalogação e Classificação**

V658m Vieira, Antônio Cézar.

Mapeamento sistemático sobre sistemas IoT no domínio smart homes / Antônio Cézar Vieira. - João Pessoa, 2018.

31 f. : il.

Orientação: Danielle Rousy Dias da Silva.
TCC (Graduação) - UFPB/CI.

1. Internet das coisas. 2. Mapeamento sistemático.
3. Smart home. 4. IoT System. 5. Internet of Things. I.
Silva, Danielle Rousy Dias da. II. Título.

UFPB/CI

CDU 004.738.5:62-4



CENTRO DE INFORMÁTICA
UNIVERSIDADE FEDERAL DA PARAÍBA

Trabalho de Conclusão de Curso de Ciência da Computação intitulado ***Mapeamento Sistemático Sobre Sistemas IoT no Domínio Smart Homes*** de autoria de Antônio Cézar Vieira, aprovada pela banca examinadora constituída pelos seguintes professores:

Danielle Rousy C. Ricarte

Prof. D.ra Danielle Rousy Dias Ricarte
DI/CI/UFPB

Iury Rogério Sales de Araújo
Me. Iury Rogério Sales de Araújo

CI/PPGI /UFPB

Jessica Maciel de Castro

Ma. Jessica Maciel de Castro
CI/PPGI/UFPB

Coordenador(a) do Curso de Ciência da Computação
CI/UFPB

João Pessoa, 19 de junho de 2018

RESUMO

Com o propósito de apoiar o desenvolvimento de novas pesquisas em ambientes *Internet of Things* (IoT), este trabalho apresenta o processo e resultados de um mapeamento sistemático realizado sobre sistemas IoT para *Smart Homes*. O objetivo do mapeamento sistemático foi mostrar o estado atual do desenvolvimento dessa área e apontar lacunas nas diferentes abordagens utilizadas em sistemas IoT para *Smart Homes*, mais precisamente abordando questões sobre serviços oferecidos, tecnologias utilizadas, segurança, comunicação e limitações dos dispositivos. Este estudo foi realizado em três grandes bancos de dados: IEEE Xplore, Science Direct (Elsevier) e ACM Digital Library, e seguiu de forma rigorosa a metodologia de pesquisa proposta. Como resultado, este estudo se torna extremamente relevante por apontar lacunas presentes nas abordagens utilizadas nesses sistemas e constatar que há a necessidade de novas pesquisas, principalmente sobre abordagens de segurança utilizadas nesses sistemas.

Palavras-chave: Smart Home. Internet of Things. Mapeamento Sistemático. IoT System.

ABSTRACT

In order to support the development of new research in Internet of Things (IoT) environments, this work presents the process and results of a systematic mapping performed on IoT systems for Smart Homes. The objective of the systematic mapping was to show the current state of development of this area and to point out gaps in the different approaches used in IoT systems for Smart Homes, specifically addressing questions about services offered, technologies used, security, communication and device limitations. This study was carried out in three large databases: IEEE Xplore, Science Direct (Elsevier) and ACM Digital Library, and rigorously followed the proposed research methodology. As a result, this study becomes extremely relevant by pointing out gaps in the approaches used in these systems and finding that there is a need for further research, especially on safety approaches.>

Key-words: Smart Home. Internet of Things. Mapeamento Sistemático. IoT System.

LISTA DE FIGURAS

1	Distribuição dos resultados Retornados por Fonte de Pesquisa	18
2	Distribuição dos resultados Primários Selecionados por Fonte de Pesquisa .	19

LISTA DE TABELAS

1	Visão Geral da Seleção dos resultados Primários	20
2	Tecnologias utilizadas em sistemas IoT para <i>Smart Homes</i>	21
3	Serviços oferecidos por sistemas IoT para <i>Smart Homes</i>	22
4	Desafios para a segurança de sistemas IoT para <i>Smart Homes</i>	23
5	Requisitos de segurança utilizados em sistemas IoT para <i>Smart Homes</i> . . .	24
6	Protocolos utilizados para realizar a comunicação de dispositivos IoT para <i>Smart Homes</i>	25
7	Limitações dos dispositivos conectados a IoT em <i>Smart Homes</i>	26

LISTA DE ABREVIATURAS

IoT – Internet of Things

QP - Questão de Pesquisa

Sumário

1 INTRODUÇÃO	10
1.1 Definição do Problema	10
1.2 Objetivos	10
1.3 Estrutura da Monografia	11
2 REFERENCIAL TEÓRICO	12
2.1 Internet of Things	12
2.2 Smart Homes	12
3 METODOLOGIA	13
3.1 Questões de Pesquisa	13
3.2 Escopo e Restrições da Pesquisa	15
3.3 Seleção de Fontes	15
3.4 Identificação de Palavras-Chave e Sinônimos	15
3.5 Geração de Strings de Busca	16
3.6 Seleção dos Estudos Primários	16
4 APRESENTAÇÃO E ANÁLISE DOS RESULTADOS	18
4.1 Busca Primária	18
4.2 Seleção dos Resultados Primários	19
4.3 Extração do Dados	20
5 CONCLUSÕES E TRABALHOS FUTUROS	27
REFERÊNCIAS	27

1 INTRODUÇÃO

Mesmo sem considerar a velocidade dos avanços tecnológicos com o passar dos anos, foi estimado que no ano de 2020 a *Internet of Things* (IoT) terá no mínimo 50 bilhões de dispositivos conectados a internet [4]. Consequentemente, devido ao fato de *Smart Homes* serem um importante componente da IoT, fica claro que também haverá um enorme crescimento nessa área.

Sistemas de automação residencial são a base de uma *Smart Home*. Nos últimos anos esses sistemas tornaram-se cada vez mais sofisticados, sendo capazes de fornecer infraestrutura e métodos para trocar todos os tipos de informações de dispositivos e serviços [18]. Esses sistemas estão claramente ligados a IoT, que é a rede de dispositivos físicos que fornece conectividade eletrônica, de sensor, de software e de rede dentro de uma *Smart Home* [1].

Desde 2010, pesquisadores analisam sistemas IoT para *Smart Homes* utilizando várias abordagens. Os artigos de pesquisa existentes sobre o tema concentram-se nos desafios que impedem a plena utilização dos aplicativos de IoT em *Smart Homes*, e fornecem recomendações para reduzir esses problemas. A pesquisa sobre sistemas para *Smart Homes* é dinâmica e diversificada [1]. Por ser uma área considerada nova e que apresenta grande ascensão, faz-se extremamente necessário a realização de novas pesquisas utilizando diferentes abordagens, a fim de estimular cada vez mais o desenvolvimento de tecnologias inovadoras para esses ambientes.

1.1 Definição do Problema

Observando a relação entre sistemas IoT e *Smart Homes*, e tendo em vista a sua grande relevância na atualidade, é de fundamental importância que haja estudos capazes de observar e analisar como são tratadas as principais abordagens utilizadas nesses sistemas. Para se obter um aperfeiçoamento desses sistemas, primeiro é necessário saber o que precisa ser melhorado, e a análise detalhada de questões sobre segurança, tecnologias, e serviços tem um papel fundamental para promover o desenvolvimento de novas pesquisas.

1.2 Objetivos

Este trabalho tem como objetivo principal apresentar um mapeamento sistemático para identificar as principais abordagens utilizadas em termos de: segurança, tecnologias, comunicação, serviços e limitações dos sistemas IoT utilizados em *Smart Homes*. E, além disso, fazer uma categorização desses dados encontrados, com a finalidade de identificar lacunas e apontar a necessidade de novos estudos.

1.3 Estrutura da Monografia

Esta monografia apresenta cinco capítulos em sua estrutura. Após este capítulo de introdução, encontra-se o Capítulo 2, onde será apresentada a fundamentação teórica relevante para o desenvolvimento deste trabalho.

No Capítulo 3, é mostrado detalhadamente cada passo realizado no desenvolvimento do mapeamento sistemático. No Capítulo 4, encontra-se o processo de apresentação e análise dos resultados, onde são detalhados todos os passos efetuados para a realização das buscas, e por fim, são mostrados os resultados que foram obtidos por meio do mapeamento sistemático realizado. O Capítulo 5, é destinado as considerações finais acerca do desenvolvimento do trabalho e a perspectivas de trabalhos futuros.

2 REFERENCIAL TEÓRICO

2.1 Internet of Things

Como o próprio nome sugere, a IoT representa a interconectividade de objetos. Em uma definição mais específica, a IoT é uma interconexão de dispositivos de detecção e atuação que permite compartilhar informações entre plataformas por meio de um framework unificado, desenvolvendo um quadro operacional comum para permitir aplicações inovadoras. Isso é conseguido por meio de sensoriamento onipresente, análise de dados e representação de informações usando *Cloud computing* como framework unificador [29].

A IoT representa a próxima evolução da Internet, dando um grande salto na capacidade de coletar, analisar e distribuir dados que podem ser transformadas em informações, conhecimento e, por fim, sabedoria [4]. E com isso, está se tornando um fator importante em muitas áreas da nossa sociedade. A IoT traz inteligência para aspectos críticos como transporte, indústria, pagamentos, saúde e muitos outros. A interação entre dispositivos incorporados e serviços da Web baseados em nuvem é um cenário comum da implantação de IoT [2].

2.2 Smart Homes

Smart Homes estão ganhando grande popularidade como a aplicação mais promissora da emergente tecnologia da Internet das Coisas (IoT). Explorando o alto nível de conectividade presente em dispositivos eletrônicos atuais, como smartphones, tablets e sistemas multimídia, e oferecendo serviços inovadores, automatizados e interativos para seus residentes [22]. As *Smart Homes* são em resumo, casas automatizadas que possuem dispositivos de detecção e controle instalados, como ar-condicionado, aquecedor, ventilação, iluminação, hardware e sistemas de segurança. Esses sistemas e sensores geralmente são controlados por um sistema de controle, e esse sistema geralmente é apresentado na forma de um tablet, celular ou computador, apresentando uma interface de usuário que permita ao usuário usufruir das funcionalidades oferecidas pelos sistemas. A conectividade de rede desses sistemas é gerenciada pela IoT, mostrando claramente a forte relação entre essas duas áreas [1].

3 METODOLOGIA

Este trabalho busca identificar as diferentes abordagens utilizadas nos sistemas IoT para *Smart Homes*. Mais especificamente, deseja identificar abordagens relacionadas a: serviços oferecidos, tecnologias utilizadas, segurança, comunicação e limitações dos dispositivos. Após obter os resultados dessas questões, é esperado que seja realizada uma categorização desses dados encontrados, a fim de identificar lacunas nos resultados e mostrar o estado atual do desenvolvimento dessa área.

Com esse objetivo, a metodologia escolhida foi o mapeamento sistemático, visto que esse método é projetado para fornecer uma ampla visão geral de uma área de pesquisa, para estabelecer se existem evidências de pesquisa sobre um tópico e fornecer uma indicação da quantidade de evidências encontradas [20].

As etapas de pesquisa do mapeamento sistemático, foram divididas em seis seções. Na primeira seção, temos as **Questões de Pesquisa**, onde são mostradas as questões que foram utilizadas para obter-se os resultados do estudo. Na segunda seção, se encontra o **Escopo e Restrições de Pesquisa**, que apresentam os critérios utilizados na seleção de fontes de pesquisa e critérios de restrições da pesquisa. Na terceira seção, as **Seleções de Fontes**, onde são mostrados os bancos de dados utilizados na pesquisa. Na quarta seção, a **Identificação de Palavras-Chave e Sinônimos**, onde é detalhado o processo de identificação das palavras-chave e sinônimos que serão utilizadas na string de busca. A quinta seção, é a etapa de **Geração de Strings de Busca**, esta seção se destina a mostrar o processo de geração do string que foi utilizado para obter os estudos primários em cada banco de dados. Por fim, na sexta seção, encontra-se a etapa de **Seleção dos Estudos Primários**, onde é precisamente detalhado como se deu o processo de seleção dos estudos primários.

3.1 Questões de Pesquisa

Foram elaboradas seis Questões de Pesquisa (QP) relacionadas aos seguintes aspectos selecionados para o estudo de sistemas IoT para *Smart Homes*: Tecnologias, Serviços, Segurança, Comunicação e Limitações.

- **QP1:** Que tecnologias são utilizadas nos sistemas IoT para *Smart Homes*?
- **QP2:** Quais são os principais serviços oferecidos por esses sistemas?
- **QP3:** Quais são os principais desafios para a segurança de sistemas IoT para *Smart Homes*?
- **QP4:** Quais são os requisitos de segurança utilizados nesses sistemas?

- **QP5:** Quais são os principais protocolos utilizados para realizar a comunicação de dispositivos IoT em Smart Homes?
- **QP6:** Quais as principais limitações dos dispositivos conectados a IoT em Smart Homes?

3.2 Escopo e Restrições da Pesquisa

Com o propósito de evitar riscos a validade deste trabalho, foram utilizados critérios para a seleção de fontes, e restrições gerais da pesquisa. Como critérios de seleção de fontes, foram definidos os seguintes itens:

- **Estar disponível para consultas web.**
- **Ser uma fonte confiável.**

Já para critérios de restrições de pesquisa, foram definidos que só seriam aceitos trabalhos que atendessem aos seguintes itens:

- **Serão considerados apenas trabalhos encontrados nas fontes selecionadas para pesquisa.**
- **Serão considerados apenas trabalhos que respeitem os critérios de inclusão e exclusão.**
- **Os trabalhos não podem ter sido publicados antes do ano de 2013.**

3.3 Seleção de Fontes

Com o objetivo de aumentar a credibilidade dos resultados, foram utilizados estes três grandes bancos de dados para realizar a pesquisa:

- **IEEE Xplore;**
- **Science Direct (Elsevier);**
- **ACM Digital Library;**

3.4 Identificação de Palavras-Chave e Sinônimos

A identificação das palavras-chave, foi realizada a partir da análise das seis QP anteriormente apresentadas. Ao analisar as palavras mais importantes de cada questão, foram selecionadas as seguintes palavras: Serviços, Protocolos, Limitações, Segurança, Smart Home, IoT System, Internet of Things.

Como as fontes de pesquisa selecionadas apresentam em sua grande maioria conteúdos em inglês, para melhorar os resultados obtidos, as palavras selecionadas foram todas traduzidas para o inglês. Tendo como resultado final as seguintes palavras-chave: Service, Protocol, Limitation, Safety, Smart Home, IoT System, Internet of Things.

3.5 Geração de Strings de Busca

Uma String de busca sofisticada, pode ser construída usando os operadores Booleanos AND e OR [20]. Então, para a geração da string de busca, as palavras-chave foram agrupadas de maneira que o operador booleano AND fosse utilizado para separar as palavras-chave que devem ser o foco dos resultados, e o operador OR foi utilizado para separar as palavras-chave e sinônimos. Feito isso, foi obtido como resultado a seguinte string de busca:

(“Service” OR “Protocol” OR “limitation” OR “Safety”) AND (“Smart Home”) AND (“IoT System” OR “Internet Of Things”).

3.6 Seleção dos Estudos Primários

A seleção dos estudos primários se deu em duas partes. Na primeira parte, foram definidos os critérios de inclusão e exclusão; estes critérios tiveram a função de selecionar apenas os resultados esperados para realizar o objetivo da pesquisa. Na segunda parte, é detalhado como foi o processo de seleção desses estudos.

O primeiro passo para um estudo primário ser selecionado, é verificar se ele respeita os critérios de seleção. Critérios de inclusão e exclusão devem ser utilizados para avaliar cada estudo primário em potencial. Os critérios de inclusão e exclusão servirão para selecionar de maneira precisa os estudos que serão utilizados no mapeamento sistemático [20].

Critérios de Inclusão:

- Os trabalhos devem estar escritos em inglês ou em português;
- Os trabalhos devem conter as palavras-chave, no resumo e/ou título e/ou nas palavras-chave do artigo selecionado;

Critérios de Exclusão:

- Trabalhos que estejam incompletos;
- Trabalhos que estejam indisponíveis para consulta nas fontes de pesquisa estabelecidas;
- Trabalhos de fontes sem credibilidade;
- Trabalhos que não respondem a pelo menos duas das questões da pesquisa;
- Trabalhos que não tenham foco em sistemas IoT para *Smart Homes*;
- Trabalhos feitos antes do ano de 2013;

- Trabalhos repetidos do mesmo autor;

Então, após definidos os critérios de inclusão e exclusão, o processo de seleção dos estudos primários se deu em três passos:

Passo 1: Primeiramente foram realizadas adaptações nas ferramentas de busca de cada fonte utilizada para pesquisa, de modo que todas as três buscas fossem realizadas da mesma forma. Após realizar as buscas iniciais de forma igual por todas as fontes, foram encontrados 100 artigos no IEEE Xplore; 160 artigos no ACM Digital Library; 158 artigos no Science Direct (Elsevier). Totalizando 418 artigos.

Passo 2: Os artigos que não apresentavam nenhuma das palavras-chave no título ou no resumo eram descartados. Após isso, artigos que apresentavam as palavras-chave no título e no resumo foram catalogados em um documento no Google Docs, totalizando 38 artigos.

Passo 3: E, por último, foram aplicados os critérios de inclusão e exclusão nos 38 artigos selecionados. Como resultado, restaram 23 artigos que tiveram seus dados extraídos por meio das questões de pesquisa propostas por este mapeamento sistemático.

4 APRESENTAÇÃO E ANÁLISE DOS RESULTADOS

Este capítulo foi dividido em três seções: Busca Primária, Seleção dos resultados Primários e Extração de dados. E tem como objetivo apresentar os resultados de cada fase da aplicação das técnicas do mapeamento sistemático que foi realizado.

4.1 Busca Primária

Para realizar as primeiras buscas, foi necessário fazer adaptações nas ferramentas de busca de cada fonte utilizada para pesquisa, com o objetivo de fazer com que a string de busca tivesse o mesmo papel em cada fonte. Essas mudanças foram realizadas da seguinte maneira:

- IEEE Xplore: foram encontrados 100 resultados utilizando o seguinte string de busca: (“Service” OR “Protocol” OR “limitation” OR “Safety”) AND (“Smart Home”) AND ((“IOT System” OR “Internet Of Things”), e incluindo ”Smart Home” no título.
- ACM Digital Library: foram encontrados 160 resultados utilizando o seguinte string de busca: (“Service” “Protocol” “limitation” “Safety” “IOT System” “Internet Of Things”) AND acmdlTitle:(+ “Smart +Home”).
- Science Direct: foram encontrados 158 resultados utilizando o seguinte string de busca: (“Service” OR “Protocol” OR “limitation” OR “Safety”) AND (“Smart Home”) AND (“IOT System” OR “Internet Of Things”), e incluindo ”Smart Home” no título.

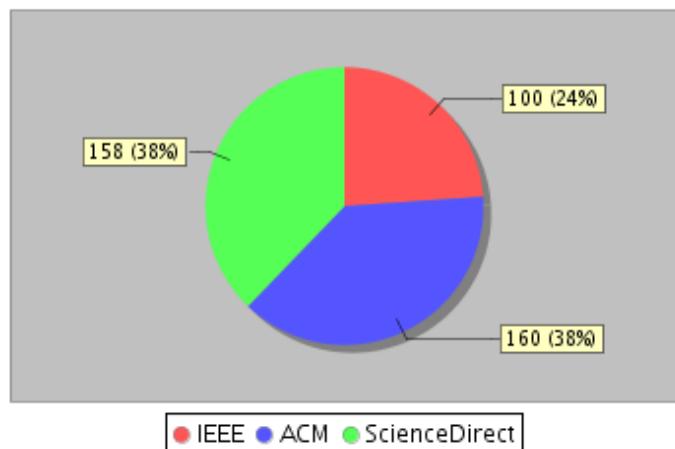


Figura 1: Distribuição dos resultados Retornados por Fonte de Pesquisa

4.2 Seleção dos Resultados Primários

Esta seção apresenta a descrição do processo de seleção dos resultados primários. Na busca primária, foram obtidos 418 resultados, após isso, foram descartados todos os resultados que não apresentavam as palavras-chave no título ou no resumo. Os resultados obtidos foram os seguintes:

- IEEE Xplore: Inicialmente apresentou 100 resultados, após esse processo, foram descartados 87, restando 13. E passando de 24% dos resultados totais, para 34%.
- ACM Digital Library: Inicialmente apresentou 160 resultados, após esse processo, foram descartados 147, restando 13. E passando de 38% dos resultados totais, para 35%.
- Science Direct: Inicialmente apresentou 157 resultados, após esse processo, foram descartados 146, restando 12. E passando de 38% dos resultados totais, para 32%.

Após esse processo, restaram um total de 38 resultados, como pode ser visualizado no gráfico da Figura 2.

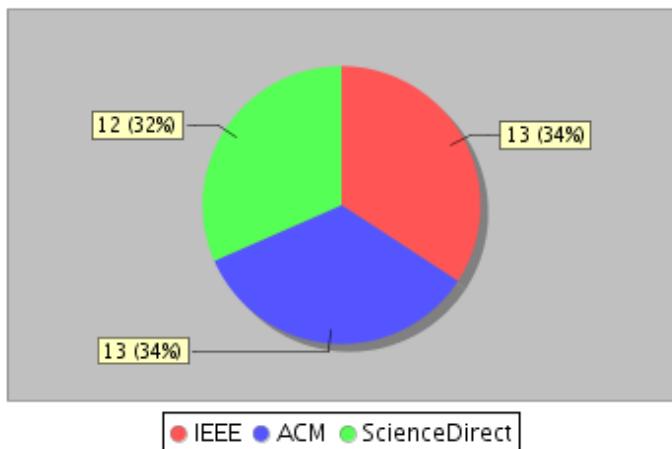


Figura 2: Distribuição dos resultados Primários Selecionados por Fonte de Pesquisa

Após isso, foram aplicados os critérios de inclusão e exclusão em cada um dos 38 resultados, tendo como motivo principal para a exclusão dos trabalhos, o fato de não estarem focados em Sistemas IoT para *Smart Homes*. Os resultados finais foram:

- **IEEE Xplore:** dos 13 resultados obtidos, 7 foram selecionados como resultados primários.
- **ACM Digital Library:** dos 13 resultados obtidos, 9 foram selecionados como resultados primários.

- Science Direct: dos 12 resultados obtidos, 7 foram selecionados como resultados primários.

Os resultados finais podem ser visualizados na Tabela 1.

Tabela 1: Visão Geral da Seleção dos resultados Primários

Fontes	Passo 1	Passo 2	Passo 3
IEEE Xplore	100	13	7
ACM	160	13	9
ScienceDirect	158	12	7
TOTAL	418	38	23

4.3 Extração do Dados

Esta seção é dedicada a apresentar os resultados finais obtidos pela realização do mapeamento sistemático. Esses resultados apresentam as respostas de cada uma das seis questões de pesquisa. E em seguida, mostra a categorização dos dados encontrados em forma de tabelas.

Essa pesquisa teve execução no mês de junho de 2018. Logo, esta seção apresenta somente resultados obtidos até essa data.

QP1: Que tecnologias são utilizadas nos sistemas IoT para *Smart Homes*?

Esse estudo apresentou uma grande variedade de tecnologias utilizadas nesses sistemas, tendo como foco principal os sensores. Esses sensores apresentaram várias funcionalidades, tais como: coletar, armazenar e analisar grandes quantidades de dados. Representando um papel fundamental na funcionalidade da grande maioria dos sistemas IoT para *Smart Homes*. Também pode-se perceber que no segundo e terceiro lugar, as tecnologias wireless de Radio Frequency IDentification (RFID) e Wireless Sensor Network (WSN), são citadas juntamente em quatro estudos, mostrando a sua relação e deixando claro a sua relevância nos sistemas atuais.

A Tabela 2 mostra o mapeamento das tecnologias utilizadas em sistemas IoT para *Smart Homes* retornados pela pesquisa.

Tabela 2: Tecnologias utilizadas em sistemas IoT para *Smart Homes*

Tecnologias	#	Referências
Wireless Sensor Network (WSN)	6	[16], [2], [8], [29], [7], [27]
Wireless Sensor and Actuator Network (WSAN)	2	[8], [5]
WPAN (Wireless Personal Area Network)	2	[27], [2]
SDK (Software Development Kit)	2	[29], [23]
Radio Frequency IDentification (RFID)	7	[16], [8], [29], [27], [5], [17]
Cloud Computing	3	[16], [12], [29]
5G	1	[27]
Body Area Network (BAN)	3	[7], [16], [27]
Home Area Network (HAN)	1	[27]
Wireless Automation Cells (WAC)	1	[2]
Controlador	4	[2], [22], [5], [25]
Microcontrolador	4	[26], [22], [5], [15]
Sensores	16	[16], [8], [24], [12], [29], [1],[7], [14], [13], [26], [10], [26], [11], [28], [15], [17]
Visão Computacional	1	[8]
Módulo de Visão Computacional	1	[8]
MEMS (Micro Electro Mechanical Systems)	1	[16]
Módulo Wi-Fi	5	[1], [14], [27], [23], [15]
Módulo ZigBee	4	[1], [27], [28], [5]
Raspberry Pi	3	[1], [14], [23]
Arduino Uno Board	2	[14], [11]
Digital Subscriber Line (DSL)	1	[27]
Decodificador de Satélite	1	[22]
Receptor Multimídia Digital	1	[22]
GPRS	1	[5]
EnOcean	1	[29]

QP2: Quais são os principais serviços oferecidos por esses sistemas?

Este estudo apresentou uma grande variedade de serviços que poderiam ser agrupados em uma mesma categoria. O gerenciamento de eletrodomésticos, por exemplo, abrange o controle de vários tipos de eletrodomésticos em uma Smart Home.

Como resposta para a questão de pesquisa, os principais serviços oferecidos por sistemas IoT para *Smart Homes* foram: Serviços de Gerenciamento de Energia e Serviços de Gerenciamento de Eletrodomésticos. Os dois obtiveram 13 citações nos resultados finais, mostrando que ao mesmo tempo em que se busca desenvolver automação e conforto, há uma enorme preocupação com a energia gasta por esses dispositivos.

Outro ponto importantes a se observar é que os Serviços de Monitoramento de Atividade, e os Serviços de Gerenciamento de Dispositivos de Segurança também obtiveram destaque nos resultados do mapeamento. Tendo como foco o serviço de monitoramento de atividade, visto que, gerenciamento de dispositivos de segurança, abrange o controle de vários tipos de dispositivos.

A Tabela 3 mostra o mapeamento dos principais serviços oferecidos por sistemas IoT para *Smart Homes* retornados pela pesquisa.

Tabela 3: Serviços oferecidos por sistemas IoT para *Smart Homes*

Serviços	#	Referências
Gerenciamento de Energia	13	[16], [2], [24], [29], [1], [26], [10], [18], [28], [5], [15], [17], [25]
Monitoramento de Atividade	8	[8], [1], [30], [26], [11], [28], [22], [5]
Serviço de Notificação ao Usuário	2	[1], [10]
Detecção de Vulnerabilidade	1	[13]
Gerenciamento de Dispositivos de Segurança	8	[2], [1], [30], [13], [26], [28], [22], [5]
Gerenciamento de dados	7	[16], [1], [7], [10], [11], [23], [5]
Gerenciamento de Eletrodomésticos	13	[16], [2], [8], [24], [12], [1], [14], [30], [26], [10], [22], [5], [15]
Pet Care	1	[1]
HealthCare	3	[16], [1], [7]
Entretenimento	4	[26], [10], [28], [22]

QP3: Quais são os principais desafios para a segurança de sistemas IoT para *Smart Homes*?

Quanto aos desafios para a segurança nesses sistemas, foi percebido uma grande preocupação em identificar a autenticidade dos usuários dos sistemas, logo seguido por desafios relacionados a privacidade do sistema e a proteção contra ataques externos.

Essa sequência e variedade de problemas relacionados a segurança, mostra que esses sistemas precisam encontrar meios para fazer com que o usuário se sinta seguro, visto que esses sistemas armazenam informações pessoais que poderiam colocar a segurança do usuário em risco.

A Tabela 4 mostra o mapeamento dos principais desafios para a segurança desses sistemas.

Tabela 4: Desafios para a segurança de sistemas IoT para *Smart Homes*.

Desafios Para a Segurança	Detalhamento	#	Referências
Autenticação	Identificar Autenticidade do Usuário	11	[2], [12], [1], [7], [13], [11], [23], [18], [22], [4], [17]
Autorização	Autorização de Usuários	2	[2], [12]
Proteção de Dados	Proteção Física e do Sistema	4	[1], [7], [23], [17]
Pivacidade	Privacidade do Sistema	9	[24], [12], [29], [1], [13], [23], [18], [5], [17]
Ataques Externos	Ataques ao Sistema	8	[12], [1], [13], [11], [23], [18], [22], [5]
Integridade	Os dados transmitidos são idênticos aos dados recebidos	5	[29], [7], [13], [22], [17]
Confidencialidade	Tornar os dados ilegíveis para os outros	7	[29], [7], [13], [11], [23], [22], [17]
Confiabilidade	Confiabilidade do Sistema	5	[2], [12], [29], [1], [22]
Autenticidade	O dispositivo não é um objeto malicioso	2	[29], [23]
Atualizações Seguras	Verificação dos arquivos da atualização de firmware	2	[1], [23]
Disponibilidade	Capacidade de um usuário acessar informações ou recursos	4	[13], [18], [22], [17]

QP4: Quais são os requisitos de segurança utilizados nesses sistemas?

Quanto aos resultados dos requisitos de segurança utilizados nesses sistemas, pode-se perceber que só foram encontrados resultados em três artigos, e além disso, nenhum dos requisitos foi citado por mais de uma fonte. Levando isso em consideração e ligando aos resultados dos desafios de segurança na QP3, pode-se observar que os sistemas IoT para *Smart Homes*, apresentam uma grande lacuna em questões relacionadas a segurança. Isso mostra que há a necessidade de mais estudos relacionados a essa questão, visto que a segurança do usuário deve ser tratada como prioridade por esses sistemas.

A Tabela 5 mostra o mapeamento dos requisitos de segurança utilizados nesses sistemas.

Tabela 5: Requisitos de segurança utilizados em sistemas IoT para *Smart Homes*.

Requisitos de Segurança	#	Referências
Criptografia Dinâmica	1	[13]
Uso de IDS/IPS	1	[13]
Vincular o tipo de criptografia ao tipo de pacote	1	[23]
Autenticação de Usuário	1	[22]
Autenticação de Dispositivo	1	[22]
Network Monitoring	1	[22]
Secure Key Management	1	[22]
Physical Protection	1	[22]

QP5: Quais são os principais protocolos utilizados para realizar a comunicação de dispositivos IoT em *Smart Homes*?

Foram obtidos diversos tipos de protocolos utilizados para realizar a comunicação de dispositivos IoT em *Smart Homes*, obtendo como destaque, os protocolos Wi-Fi, Bluetooth e ZigBee. Essa grande variedade de resultados mostra uma falta de padronização quanto aos protocolos de comunicação utilizados nesses dispositivos, podendo gerar problemas de incompatibilidade de diversas formas.

A Tabela 6 mostra o mapeamento dos principais protocolos utilizados nesses dispositivos.

Tabela 6: Protocolos utilizados para realizar a comunicação de dispositivos IoT para *Smart Homes*.

Protocolos	#	Referências
GPS	2	[16], [1]
Radio Frequency (RF)	5	[16], [8], [1], [14], [5]
Wi-Fi	9	[16], [2], [24], [12], [1], [26], [22], [15], [17]
Bluetooth	8	[16], [2], [29], [1], [26], [27], [22], [5]
ZigBee	8	[16], [2], [29], [1], [27], [23], [28], [22]
Bluetooth Low Energy (BLE)	3	[16], [2], [23]
ANT	1	[2]
HTTP	4	[8], [12], [13], [23]
Near Field Communication (NFC)	1	[8]
Message Queuing Telemetry Transport (MQTT)	1	[12]
Datagram Transport Layer Security (DTLS)	3	[12], [11], [18]
Constrained Application Protocol (CoAP)	3	[12], [1], [11]
X10	1	[29]
BACnet	1	[29]
Z-Wave	1	[29]
Insteon	1	[29]
Network Time Protocol (NTP)	1	[1]
Transmission Control Protocol (TCP)	1	[13]
EFEN_PROTO	1	[25]

QP6: Quais as principais limitações dos dispositivos conectados a IoT em *Smart Homes*?

Sobre as principais limitações dos dispositivos, obteve-se uma grande quantidade de resultados, focando principalmente nas limitações de processamento, energia e comunicação. Isso mostra que os dispositivos conectados a IoT para *Smart Homes* necessitam de grandes melhorias. Pode se observar que são limitações bastante contundentes para dispositivos com funções tão importantes, e que dependendo da intensidade dessa limitação, poderia facilmente comprometer todo o ambiente.

A Tabela 7 mostra o mapeamento das limitações dos dispositivos conectados a IoT em *Smart Homes*.

Tabela 7: Limitações dos dispositivos conectados a IoT em *Smart Homes*.

Limitações de Dispositivo	#	Referências
Problemas de Comunicação	6	[16], [1], [14], [27], [5], [15]
Problemas de Roteamento	2	[16], [2]
Capacidade de Processamento Limitada	8	[2], [8], [12], [29], [1], [27], [22], [17]
Limitações de Memória	4	[2], [8], [28], [16]
Limitações de Fonte de Energia	6	[2], [7], [14], [26], [18], [22]
Limitações de Armazenamento de dados	4	[24], [14], [22], [5]
Falhas de Hardware	1	[1]
Imprecisão	2	[8], [28]

5 CONCLUSÕES E TRABALHOS FUTUROS

Neste trabalho foi apresentado o resultado do estudo de um mapeamento sistemático realizado sobre os sistemas IoT para *Smart Homes*. O método utilizado na realização dessa pesquisa foi amplamente detalhado, apresentando grande eficiência e precisão na busca pelos resultados esperados.

Como resultado deste trabalho, analisando a Seção de Extração de Dados do capítulo 4, pode-se concluir que mesmo com a sua grande popularidade, os sistemas IoT para *Smart Homes* ainda apresentam grandes limitações e dificuldades em relação a segurança, o que é um fato preocupante, visto que esses sistemas lidam com informações pessoais e possuem dispositivos conectados que interagem diretamente com o usuário. Além disso, ainda foi observado uma grande quantidade de problemas vinculados aos dispositivos utilizados nas *Smart Homes*, principalmente relacionados a questões de processamento, comunicação e energia dos dispositivos. Esses problemas foram numerosamente citados pelos resultados primários encontrados na pesquisa, e tendo em vista que esses dispositivos estão diretamente ligados ao sistema, isso se mostra uma questão que merece atenção.

A contribuição deste trabalho encontra-se na grande quantidade de informações extremamente relevantes apontadas sobre esses sistemas. As informações obtidas mostraram que têm potencial para serem usadas como base em novas pesquisas, assim, como trabalhos futuros, tem-se a possibilidade de encontrar soluções para os problemas de segurança e limitações dos dispositivos utilizados nos sistemas IoT para *Smart Homes*.

REFERÊNCIAS

- [1] ALAA, M. et al. A review of smart home applications based on Internet of Things. *Journal of Network and Computer Applications*, v. 97, p. 48–65, 2017.
- [2] COLLOTTA, M.; PAU, G. Bluetooth for Internet of Things: A fuzzy approach to improve power management in smart homes. *Computers and Electrical Engineering*, v. 44, p. 137–152, 2015.
- [3] EVANS, D. A Internet das Coisas Como a próxima evolução da Internet está mudando tudo. Cisco, p. 1–13, 2011.
- [4] EVANS, D. A Internet das Coisas Como a próxima evolução da Internet está mudando tudo. Cisco, p. 1–13, 2011.
- [5] GAIKWAD, P. P.; GABHANE, J. P.; GOLAIT, S. S. A survey based on Smart Homes system using Internet-of-Things. *2015 International Conference on Computation of Power, Energy, Information and Communication (ICCPEIC)*, p. 0330–0335, 2015.
- [6] GALININA, O. et al. Smart home gateway system over Bluetooth low energy with wireless energy transfer capability. *Eurasip Journal on Wireless Communications and Networking*, v. 2015, n. 1, 2015.
- [7] GEBRIE, M. T.; ABIE, H. Risk-based adaptive authentication for internet of things in smart home eHealth. *Proceedings of the 11th European Conference on Software Architecture Companion Proceedings - ECSA '17*, p. 102–108, 2017.
- [8] GONZÁLEZ GARCÍA, C. et al. Midgar: Detection of people through computer vision in the Internet of Things scenarios to improve the security in Smart Cities, Smart Towns, and Smart Homes. *Future Generation Computer Systems*, v. 76, n. 2017, p. 301–313, 2017.
- [9] GUBBI, J. et al. Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, v. 29, n. 7, p. 1645–1660, 2013.
- [10] GUEBLI, W.; BELKHIR, A. TV Home-box Based IoT for Smart Home. *Proceedings of the Mediterranean Symposium on Smart City Application*, p. 12:1–12:7, 2017.
- [11] IBRAHIM, J. M. et al. A security authorization scheme for smart home Internet of Things devices. *Future Generation Computer Systems*, v. 44, n. 2017, p. 335–336, 2017.

- [12] IBRAHIM, J. M.; KARAMI, A.; JAFARI, F. A Secure Smart Home using Internet-of-Things. Proceedings of the 9th International Conference on Information Management and Engineering - ICIME 2017, p. 69–74, 2017.
- [13] JIA, X.; LI, X.; GAO, Y. A Novel Semi-Automatic Vulnerability Detection System for Smart Home. Proceedings of the International Conference on Big Data and Internet of Thing, p. 195–199, 2017.
- [14] KADIMA, M. N.; JAFARI, F. A Customized Design of Smart Home using Internet-of-Things. Proceedings of the 9th International Conference on Information Management and Engineering - ICIME 2017, p. 81–86, 2017.
- [15] KAMAL, M. S. et al. Efficient low cost supervisory system for Internet of Things enabled smart home. 2017 IEEE International Conference on Communications Workshops, ICC Workshops 2017, n. Scpa, p. 864–869, 2017.
- [16] KHAN, M. et al. Context-aware low power intelligent SmartHome based on the Internet of things. Computers and Electrical Engineering, v. 52, p. 208–222, 2016.
- [17] KIM, J. T. Analyses of secure authentication scheme for smart home system based on internet on things. 2017 International Conference on Applied System Innovation (ICASI), p. 335–336, 2017.
- [18] KIM, Y. P.; YOO, S.; YOO, C. DAoT: Dynamic and energy-aware authentication for smart home appliances in Internet of Things. 2015 IEEE International Conference on Consumer Electronics, ICCE 2015, p. 196–197, 2015.
- [19] KITCHENHAM, B. Procedures for performing systematic reviews. Keele, UK, Keele University, v. 33, n. TR/SE-0401, p. 28, 2004.
- [20] KITCHENHAM, B. et al. Systematic literature reviews in software engineering-A tertiary study. Information and Software Technology, v. 52, n. 8, p. 792–805, 2010.
- [21] KITCHENHAM, B.; CHARTERS, S. Guidelines for performing Systematic Literature reviews in Software Engineering Version 2.3. Engineering, v. 45, n. 4ve, p. 1051, 2007.
- [22] LEE, C. et al. Securing smart home: Technologies, security challenges, and security requirements. 2014 IEEE Conference on Communications and Network Security, CNS 2014, p. 67–72, 2014.
- [23] LIU, H. et al. Smart Solution, Poor Protection: An Empirical Study of Security and Privacy Issues in Developing and Deploying Smart Home Devices. Proceedings of the Workshop on Internet of Things Security and Privacy (IoTS&P), n. I, p. 13–18, 2017.

- [24] MATSUI, K. An information provision system to promote energy conservation and maintain indoor comfort in smart homes using sensed data by IoT sensors. Future Generation Computer Systems, v. 82, p. 388–394, 2018.
- [25] ORSI, E.; NESMACHNOW, S. Smart home energy planning using IoT and the cloud. Urucon 2017 Ieeee, n. Cc, 2017.
- [26] RAHMAN, A. A. A.; NAWI, A. H.; AZIZ, R. M. F. T. Improving Power Consumption of Wireless Home Automation System with Secured Smart Energy Controller. Proceedings of the 2017 International Conference on E-Society, E-Education and E-Technology, p. 33–36, 2017.
- [27] RAJAEI, H.; MIRZAEI, F. IoT, Smart Homes, and Zigbee Simulation. Proceedings of the Communications and Networking Symposium, p. 8:1–8:10, 2018.
- [28] RASHID, M. A.; HAN, X. Gesture control of ZigBee connected smart home Internet of Things. 2016 5th International Conference on Informatics, Electronics and Vision, ICIEV 2016, p. 667–670, 2016.
- [29] RISTESKA STOJKOSKA, B. L.; TRIVODALIEV, K. V. A review of Internet of Things for smart home: Challenges and solutions. Journal of Cleaner Production, v. 140, p. 1454–1464, 2017.
- [30] SIVARAMAN, V. et al. Smart-Phones Attacking Smart-Homes. Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks - WiSec '16, p. 195–200, 2016.