Revisão Sistemática sobre Segurança Adaptativa Ciente de Contexto para a Internet das Coisas

Ricardo Borges Almeida[1], **Adenauer Corrêa Yamin**[1], **Ana Marilza Pernas**[1]

[1]Programa de Pós-Graduação em Computação (PPGC)
Universidade Federal de Pelotas (UFPel), Pelotas – RS – Brasil

{rbalmeida,adenauer,marilza}@inf.ufpel.edu.br

Resumo. *Este documento apresenta uma versão completa, incluindo um detalhamento sobre os trabalhos identificados, da revisão sistemática da literatura desenvolvida como parte da tese de doutorado de Ricardo Borges Almeida.*

1. Introdução

Uma materialização da Computação Ubíqua (UbiComp) que vem ganhando destaque é a Internet das Coisas, do inglês *Internet of Things* (IoT). Apesar das inúmeras contribuições que a IoT tem proporcionado, a decorrente proliferação de dispositivos conectados criou novas demandas na segurança da informação. Este mercado tem inspirado novas tecnologias, no entanto, na tentativa de manterem-se competitivos, os fabricantes buscam diminuir o tempo de produção destes dispositivos, o que torna questionável o nível de segurança no ciclo de vida do desenvolvimento KLIARSKY; LEUNE (2017).

Adicionalmente, as organizações muitas vezes implementam tecnologias de propósitos específicos para promover a segurança de seus ambientes computacionais, no entanto, elas se limitam a analisar informações contextuais específicas, não fornecendo um contexto holístico para análise de risco, resultando em decisões inadequadas de adaptação para mitigação AMAN (2016). Esses desafios, visões e vantagens impulsionam a investigação por soluções de segurança efetivas para os ambientes da IoT, uma vez que os atuais controles de segurança tradicionais são ineficientes e insuficientes para essa rede dinâmica e heterogênea em desenvolvimento.

Este trabalho concentra-se especialmente na exploração dos mecanismos de adaptação aplicados para promover a segurança de ambientes da IoT, ou seja, na segurança adaptativa para IoT. Observa-se que, especialmente devido as características da IoT, a aplicação dos conceitos de ciência de contexto e a integralização das diferentes soluções de segurança se mostram demandas oportunas.

Os objetivos deste trabalho consistem em: (i) sistematizar e apresentar os conceitos sobre adaptação ciente de contexto para IoT, incluindo a sua relação com a segurança da informação; (ii) realizar uma revisão sistemática da literatura buscando identificar o estado da arte em segurança adaptativa ciente de contexto baseada em eventos para IoT; e (iii) desenvolver uma análise crítica sobre os trabalhos identificados em um esforço para elencar as lacunas existentes nesta área.

Este trabalho foi organizado em 7 seções. Nesta primeira seção foi apresentada uma breve introdução ao tema central da pesquisa, suas motivações e objetivos. Na sequência, nas seções 2, 3 e 4 são discutidos os conceitos em torno da segurança adaptativa ciente de contexto para IoT. A seção 5 apresenta o estado da arte, para na seção

6 serem discutidos os trabalhos selecionados e as oportunidades de pesquisa. Por fim, a seção 7 discute as considerações finais.

2. Internet das Coisas

A Internet das Coisas consiste da onipresença de vários objetos ou coisas, incluindo tecnologias de sensores e dispositivos móveis físicos, sem e com fio, que interagem uns com os outros para cumprir objetivos comuns GIUSTO et al. (2010). A IoT é entendida como um ambiente inteligente que pode reagir às mudanças ou eventos que ela percebe em seu ecossistema.

A IoT, ao menos na teoria, visa tornar o cotidiano das pessoas mais simples, prático e produtivo, o que justifica a sua crescente popularidade. Desde a introdução de RFID como uma das tecnologias no âmbito da IoT, uma infinidade de outros sensores e objetos móveis são introduzidos para ampliar sua visão. Para exemplificar alguns dos dispositivos associados a esta afirmação é possível citar os relógios inteligentes, carros, cafeteiras, geladeiras, robôs aspiradores, entre outros. Este ambiente permite uma integração dos objetos físicos, móveis e de sensoriamento na infraestrutura tradicional, criando assim novas oportunidades de negócio. A eHealth[1], os edifícios inteligentes, as redes inteligentes e os sensores de meio ambiente são alguns exemplos de serviços e aplicações habilitadas pela IoT em diferentes campos AMAN (2016).

Para fornecer suporte a este ambiente dinâmico, considerando o escopo deste trabalho e, em especial, a necessidade de segurança em torno da IoT, exemplos de recursos que devem ser almejados incluem MIORANDI et al. (2012): suporte à heterogeneidade de dispositivos em diferentes níveis da arquitetura (protocolos, eventos, aplicação); escalabilidade, permitindo o tratamento de um crescente volume de dados, e; autonomia, uma vez que a complexidade, a dinâmica e as especificidades que muitos cenários da IoT apresentam implicam na necessidade de que os dispositivos (ou parte deles) sejam capazes de reagir de maneira autônoma às diferentes situações, buscando minimizar a intervenção humana.

Apesar dos benefícios fornecidos, algumas questões ainda não foram abordadas, como a visibilidade global, o gerenciamento autônomo em tempo real, a regularização, a padronização, a interoperabilidade dos sistemas, o consumo de recursos, a distribuição, o suporte à QoS, a privacidade dos dados e a segurança MIORANDI et al. (2012). Algumas dessas preocupações, como as questões de QoS e os consumos de recursos, são, em última instância, um problema de segurança, pois influenciam ou são influenciados direta ou indiretamente. Assim, pode-se estabelecer que a segurança é um dos problemas críticos que precisa ser adequadamente abordado MIORANDI et al. (2012); SICARI et al. (2015).

3. Segurança Adaptativa

A adaptação, dinâmica ou em tempo de execução, consiste na capacidade de um sistema em monitorar e regular, de forma autônoma, seu comportamento de acordo com as situações de interesse ou alterações sob observação AMAN (2016). Esta propriedade auxilia na complexidade dos ambientes computacionais compostos pela IoT, utilizando a tecnologia para gerenciar a tecnologia, buscando-se minimizar a necessidade de

[1] Uso de tecnologia da informação para saúde.

intervenção humana. Com isto, a segurança adaptativa é a capacidade de um sistema observar os ambientes sob sua gerência, analisar quaisquer potenciais ameaças de segurança e responder de forma autônoma aos riscos que estas representam e as falhas dos sistemas que compõem o ambiente, visando reduzir seus possíveis impactos AMAN (2016).

Muitas equipes de segurança da informação operam sob um comportamento alinhado à "resposta a incidentes", o que é importante para área. No entanto, com os atuais ambientes computacionais, em especial devido as mudanças consequentes da IoT, é necessário operar seguindo uma "resposta contínua", onde os sistemas são assumidos como comprometidos e exigem monitoramento e correção contínua, em tempo de execução.

A literatura defende o uso de métodos formais para fornecer evidências de que as mudanças nas situações do ambiente monitorado satisfaçam os objetivos de segurança de um sistema AMAN (2016). Uma abordagem promissora para segurança adaptativa considerando os ambientes da IoT é o emprego de um ciclo de *feedback*.

Em uma tentativa de lidar com as complexidades dos sistemas modernos de computação a *International Business Machines* (IBM) sugeriu o modelo *Monitor-Analyze-Plan-Execute plus Knowledge* (MAPE-K), conforme apresentado na Figura 1. O MAPE-K utiliza as atividades Monitorar, Analizar, Planejar e Executar empregando um ciclo de controle em conjunto com o componente Conhecimento que fornece as informações necessárias para realizar a adaptação AMAN (2016).

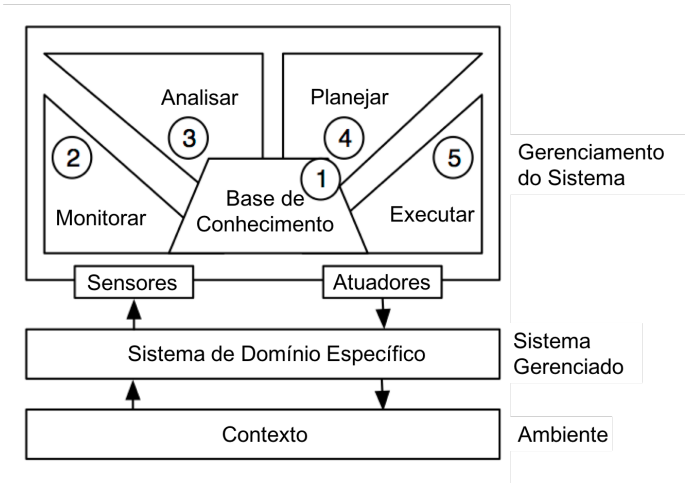

Figura 1. MAPE-K - Modelo para sistemas adaptativos
Fonte: IGLESIA; WEYNS, 2015

O componente Monitor coleta os dados apropriados dos recursos gerenciados por meio dos sensores. Os dados são correlacionados, filtrados e/ou agregados e o sintoma descoberto é passado para o componente Analisar. Sintomas e outros dados também podem ser armazenados em uma base de conhecimento compartilhada. O analisador determina se uma mudança precisa ser feita com base no conhecimento compartilhado (potencialmente uma política) e nos sintomas. Caso pertinente, uma solicitação de mudança no ambiente é passada para o componente Planejar. O planejador gera os comandos ou fluxos de trabalho necessários na forma de um plano de alteração que é passado para o componente Executar. O executor aplica o plano de mudança no recurso de gerenciamento usando os atuadores. Caso necessário, a base de conhecimento pode ser atualizada,

fornecendo dados do impacto da adaptação para serem aplicados como *feedback* para o próximo ciclo.

Em EVESTI (2014), os autores mencionam dois atributos oportunos para promover a segurança adaptativa, a autoconsciência (*self-awareness*) e a ciência de contexto (*context awareness*). A autoconsciência é a capacidade do sistema em conhecer seu próprio estado, seus componentes, capacidades, limites, recursos e comportamento. Já a ciência do contexto, consiste do conhecimento sobre o ambiente operacional ao qual o sistema está inserido.

4. Ciência de Contexto na Segurança Adaptativa

A ciência de contexto está presente nas pesquisas relacionadas a UbiComp, sendo um dos grandes desafios no desenvolvimento de aplicações nesta área. Para entender o seu significado, primeiramente é necessário definir **contexto**, que de acordo com Dey (2001) é qualquer informação que pode ser usada para caracterizar a situação de uma entidade (pessoa, local ou objeto) que seja considerada relevante para a interação entre o usuário e a aplicação, incluindo o próprio usuário e a aplicação. Contexto é o que contribui para a correta interpretação de uma ação ou evento, sem, no entanto, ser parte dessa ação/evento.

A ciência de contexto vem sendo foco de um grande número de pesquisas em diferentes áreas, consequentemente assumindo diferentes significados. Dessa forma, neste texto entende-se por **ciência de contexto** a capacidade de um sistema em usar o contexto para prover serviços e/ou informações relevantes para o usuário DEY (2001).

Ao se construir e executar aplicações cientes de contexto há uma série de funcionalidades que devem ser providas, envolvendo desde a aquisição de informações contextuais, a partir do conjunto de fontes heterogêneas e distribuídas, até a representação dessas informações, seu processamento, armazenamento, e a realização de inferências para seu uso em tomadas de decisão BELLAVISTA et al. (2012). Tais tarefas se alinham ao ciclo de *feedback* empregado na formalização da segurança adaptativa.

Os sistemas cientes de contexto devem ser flexíveis, se adaptarem, e serem capazes de atuar automaticamente para ajudar o usuário na realização de suas atividades, o que está diretamente associado às necessidades das soluções para segurança da informação. Algumas motivações para usar a ciência de contexto são: auxilia na compreensão da realidade; facilita na adaptação de sistemas; auxilia no processo de transformação dos dados em informação, e; apoia a compreensão de eventos e de situações.

No que tange a segurança adaptativa, caso os contextos relevantes para a identificação das situações a serem avaliadas não sejam adequadamente considerados, pode haver uma influência adversa no ambiente impactando nos serviços oferecidos. A ciência de contexto é especialmente crítica nos cenários da IoT, em particular na adaptação, pois esta consiste em uma comunicação máquina para máquina, a priori sem a inteligência (envolvimento direto) dos humanos. Caso sejam empregados contextos irrelevantes, incorretos ou insuficientes, a adaptação pode não ser eficiente AMAN (2016).

5. Estado da Arte

Esta seção tem como objetivo apresentar o estado da arte em pesquisas que empregam ciência de contexto para segurança adaptativa na IoT. Para isto, foi realizada uma revisão

sistemática da literatura sobre o tema. Desta forma, na subseção seguinte é apresentado o protocolo executado para posteriormente discutir os trabalhos selecionados.

A revisão sistemática adotada neste trabalho é baseada no processo proposto por Petersen et al. (2008), o qual estabelece uma série de atividades a serem executadas e registradas, permitindo que o estudo realizado seja reproduzido por outros pesquisadores. Como primeira etapa seguindo o processo mencionado, as seguintes questões de pesquisa foram propostas para guiar a revisão:

- (Q1) Quais os atuais desafios de segurança adaptativa em IoT?
- (Q2) Quais as estratégias utilizadas para avaliação das propostas?
- (Q3) Quais as informações contextuais utilizadas para realizar as adaptações?
- (Q4) Quais os mecanismos para tomada de decisões considerando diferentes opções para adaptação, bem como diferentes contextos?

Na pesquisa para identificação de estudos primários, inicialmente foram estabelecidos os seguintes critérios para seleção das fontes de artigos:

- disponibilidade na web, preferivelmente em bibliotecas digitais e bases científicas;
- artigos publicados em periódicos ou conferências focados em IoT, UbiComp, ciência de contexto e segurança da informação;
- utilização de mecanismos de pesquisa avançados que considerem os termos e sinônimos utilizados na *string* de busca.
- disponibilidade dos artigos completos;
- estarem escritos em inglês.

Com isto, as bases acadêmicas selecionadas para esta etapa foram: ACM Digital Library, Science Direct, IEEE Xplore, Web of Science e Scopus. A base Springer havia sido selecionada inicialmente, no entanto, por ela não possibilitar a pesquisa usando operadores lógicos nos campos título, resumo e palavras-chaves, ela foi excluída. Destaca-se que diversos trabalhos presentes na literatura aplicam a busca exclusivamente nos campos mencionados a fim de minimizar os falso-positivos da pesquisa quando ela é aplicada no texto completo DIKICI; TURETKEN; DEMIRORS (2018); HEEAGER; NIELSEN (2018); HOSSEINZADEH et al. (2018).

O processo de busca pelos artigos seguiu um fluxo de execução, onde inicialmente buscou-se definir uma *string* condicionada e delimitada pela inclusão obrigatória dos termos que melhor refletem os conceitos fundamentais desta pesquisa (segurança adaptativa, ciência de contexto e internet das coisas). Adicionalmente, foi realizado um esforço em tornar esta *string* suficientemente genérica para incluir variações dos termos referentes aos principais conceitos explorados (como por exemplo, “adaptation”, “adaptive”, “context-awareness”, “contextualization”, “contextual”) bem como alteração da ordem das palavras (tendo como exemplo “adaptive security” e “security adaptation”), e não restringir em aplicações específicas da IoT, como *Smart Home*, *eHeatlh*.

Posteriormente foram estabelecidas diferentes composições de termos para definição de uma *string* de busca. Neste momento, foram considerados sinônimos para “adaptive”, sendo avaliados os termos “automat*” e “orchestrat*”. No entanto, considerando os critérios a serem discutidos a seguir, estas variações não resultaram em artigos oportunos para serem utilizados na revisão.

Finalmente, após as alternativas exploradas e considerando as palavras-chave *adapt*, *security*, *context* e IoT, foi estabelecida a *string* de busca apresentada na Figura 2.

Figura 2. String de pesquisa usada na revisão sistemática

Destaca-se que para aplicação da string nos campos título, resumo e palavras-chaves, as seguintes particularidades de cada base devem ser observadas:

- na ACM é necessário inserir a string apresentada na restrição "recordAbstract:(...)" para aplicar a mesma no campo resumo, uma vez que não é possível pesquisar nos outros campos desejados;
- na IEEE a pesquisa deve utilizar a opção "Command search", (clicando em "Other search options") e selecionando a opção "Metadata Only", uma vez que a pesquisa padrão não utiliza os operadores lógicos;
- já na Science Direct, a opção de pesquisa avançada oferece a possibilidade de aplicar a string sobre os campos título, resumo e palavras-chave, no entanto, ela não suporta o uso de *wildcards*[2], os quais foram apenas removidos da *string*, o que é compensado pelo suporte à *stemming*[3] oferecido;
- e por fim, na Web of Science e na Scopus é necessário selecionar a opção "Tópico" e "Título, Resumo, Palavras-chave" respectivamente.

Para a triagem dos artigos, primeiramente a *string* de busca foi aplicada em cada base apresentada. A Figura 3 apresenta o número de artigos identificados por ano em cada base utilizada. Observa-se que neste gráfico, ainda constam artigos duplicados e documentos que não consistem de artigos de fato.

Com isso, os seguintes critérios de inclusão e exclusão foram aplicados, conforme a ordem apresentada:

- (E) artigo duplicado;
- (E) não é um artigo, por exemplo, consiste de resumo de eventos, *posters*, introdução de livros, entre outros;
- (E) não apresenta um modelo/*framework* para segurança adaptativa aplicada à IoT, o que inclui artigos que não possuem relação considerável com o objetivo desta tese, bem como revisões da literatura e aqueles voltados para segurança adaptativa mas focados em questões de avaliação ou de tomada de decisões;
- (E) segurança adaptativa voltada para campo específico como autenticação, autorização, entre outros;
- (E) artigo mais atual apresenta modificações deste artigo;
- (I) explora conceitos relacionados à ciência de contexto e segurança adaptativa;

[2]Um *wildcard* é um caractere especial que representa um ou mais outros caracteres. Um dos *wildcards* mais usados é o asterisco (*), que normalmente representa zero ou mais caracteres em uma sequência de caracteres ROUSE (2010).

[3]Em recuperação de informação *stemming* é o processo de reduzir palavras flexionadas (ou às vezes derivadas) ao seu tronco (*stem*), base ou raíz, geralmente uma forma da palavra escrita LOVINS (1968).

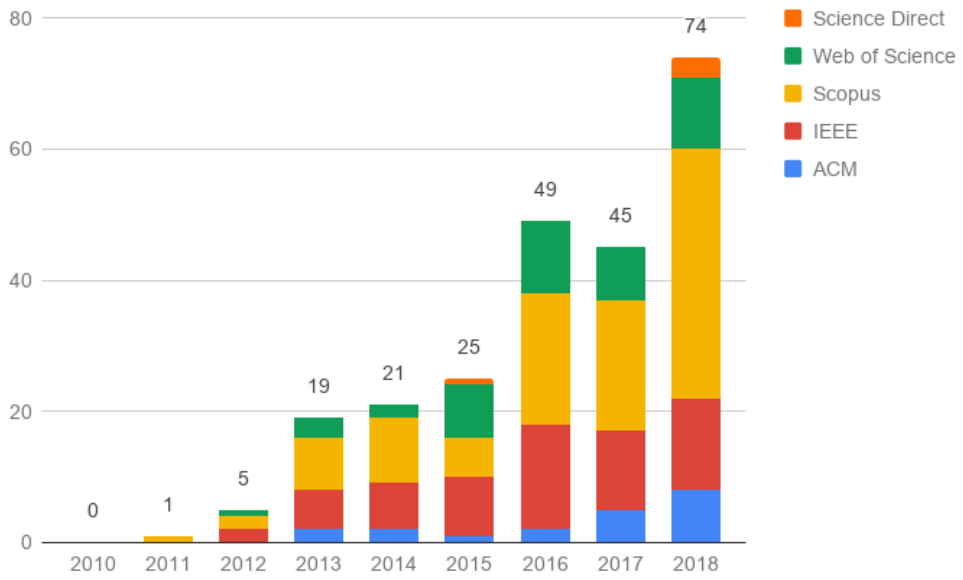

Figura 3. Número de artigos publicados por ano em cada base considerada

- (E) o artigo não possui nenhum dos critérios de inclusão.

Adaptações necessárias considerando as bases utilizadas foram empregadas para a aplicação da *string* nos campos título, resumo e palavras-chave. A Tabela 1 apresenta a *string* para cada base junto ao número de artigos retornados e um *link* para acesso rápido aos resultados. Observa-se que para acessar os *links* é necessário estar em uma rede com acesso às bases.

Com a submissão das *strings* para as bases, foi realizada a exportação dos metadados dos artigos retornados para o formato .bib e importação para a ferramenta StArt[4]. Um total de 465 documentos foram inicialmente identificados. O arquivo com o resultado da aplicação dos critérios, incluindo a razão pela qual cada artigo foi incluído ou excluído, pode ser importado no Start e está disponibilizado no Github[5].

A Tabela 2 apresenta o número de artigos incluídos ou excluídos, de acordo com os critérios apresentados. Primeiramente foram excluídos 52 documentos importados para o Start que não eram artigos, sendo a maior parte deles resumo de eventos ou sumários. Na sequência, 179 documentos foram identificados como duplicados e removidos da análise. Sendo assim, restaram 234 artigos para análise do conteúdo e aplicação dos demais critérios.

A aplicação dos critérios foi realizada primeiramente analisando o título e resumo, para posteriormente serem avaliados os capítulos de introdução, concepção do projeto e conclusão. Finalmente, os artigos que ainda restaram dúvidas quanto aos critérios, foram analisados por inteiro.

Visando minimizar a subjetividade da aplicação destes critérios, a revisão adotou

[4]http://lapes.dc.ufscar.br/tools/start_tool

[5]https://github.com/rborgesalmeida/doutorado-tese/raw/master/Seguranc\%CC\%A7a\%20Adaptativa\%20em\%20IoT\%20v3.start

Tabela 1. Aplicação da string de busca nas bases acadêmicas

Base	String	URL	Total de Artigos
ACM	[Abstract: adapt*] AND [Abstract: security] AND [Abstract: context*] AND [[Abstract: "internet of things"] OR [Abstract: iot]]	http://bit.ly/31DycJ9	63
IEEE	("All Metadata":adapt* AND security AND context* AND ("internet of things"OR iot))	http://bit.ly/3gpKIQT	114
Science Direct	TITLE-ABSTR-KEY(adapt AND security AND context AND ("internet of things" or iot))	http://bit.ly/2BY4u78	7
Web of Science	TÓPICO:(adapt* AND security AND context* AND ("internet of things" OR iot))	Em razão do gerenciamento de sessão utilizado pela base, a utilização de um link para a pesquisa não foi possível.	96
Scopus	TITLE-ABS-KEY (adapt* AND security AND context* AND ("internet of things" OR iot))	http://bit.ly/31I9eIG	185

um teste de confiabilidade entre avaliadores FINK (2010). O autor principal desta tese realizou a seleção dos artigos de forma completa, e uma amostra dos artigos resultantes do processo foi disponibilizada primeiramente ao colega de doutorado Roger da Silva Machado, e posteriormente discutida com os orientadores. Esta amostra consistiu de 21 artigos, os quais incluíram os 6 selecionados - a serem discutidos na sequência - e mais 15 que em um primeiro momento geraram dúvidas quanto à sua inclusão ou exclusão.

Tabela 2. Número de artigos por critério

Critério	Total de Artigos
(E) artigo duplicado	179
(E) não é um artigo	52
(E) não apresenta um modelo/*framework* para segurança adaptativa aplicada à IoT	212
(E) segurança adaptativa voltada para campo específico	13
(E) artigo mais atual apresenta modificações deste artigo	2
(I) explora conceitos relacionados à ciência de contexto e segurança adaptativa	6
(E) O artigo não possui nenhum dos critérios de inclusão	1

Os artigos que foram selecionados após o processo de revisão sistemática da lite-

ratura são apresentados na Tabela 3, onde pode ser visualizado os autores, o título, a base acadêmica que retornou o artigo e a conferência ou o periódico onde este foi publicado.

Tabela 3. Artigos selecionados após o revisão sistemática

Autores	Título	Base	Conferência/Periódico
ABIE; BALASINGHAM, 2012	*Risk-based Adaptive Security for Smart IoT in eHealth*	ACM	*European Conference on Software Architecture: Companion Proceedings*
AMAN; SNEKKENES, 2014	*Event driven adaptive security in internet of things*	Scopus	*International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies*
RAMOS; BERNABE; SKARMETA, 2015	*Managing Context Information for Adaptive Security in IoT Environments*	IEEE, Web of Science, Scopus	*International Conference on Advanced Information Networking and Applications Workshops*
EL-MALIKI; SEIGNE, 2016	*Efficient Security Adaptation Framework for Internet of Things*	IEEE, Web of Science, Scopus	*International Conference on Computational Science and Computational Intelligence*
MOZZAQUATRO et al., 2016	*An ontology-based security framework for decision-making in industrial systems*	IEEE, Scopus	*International Conference on Model-Driven Engineering and Software Development*
KHAN; NDUBUAKU , 2018	*Ontology-based automation of security guidelines for smart homes*	IEEE, Scopus	*World Forum on Internet of Things (WF-IoT)*

Em um esforço de aprimoramento da amplitude dos estudos identificados até esta etapa, foi realizada uma busca pela produção bibliográfica dos autores destes artigos junto à análise das principais referências utilizadas nos mesmos. Com isso, os documentos apresentados na Tabela 4 foram definidos como norteadores das análises posteriormente realizadas, sendo utilizados como critérios para suas escolhas a amplitude da discussão, neste caso sendo elencados principalmente as teses dos autores, e a atualidade do documento e aproximação com os critérios de inclusão.

Com isso, o primeiro trabalho apresentado na Tabela 3 foi substituído pela tese do autor, disposta na quarta linha da Tabela 4. O quarto artigo da Tabela 3 foi substituído por uma versão atual proposta pelos mesmos autores, apresentada na sexta linha da Tabela 4. E finalmente, o segundo trabalho na Tabela 4 foi adicionado em razão das referências analisadas nos demais estudos.

6. Trabalhos Selecionados

Com a realização da revisão sistemática da literatura, foram selecionados seis artigos, os quais são apresentados a seguir. Destaca-se que a análise destes trabalhos contemplou

Tabela 4. Artigos avaliados em profundidade após seleção inicial

Autores	Título	Base	Conferência/Periódico
ABIE; BALASINGHAM, 2012	*Risk-based Adaptive Security for Smart IoT in eHealth*	ACM	*European Conference on Software Architecture: Companion Proceedings*
EVESTI, 2014	*Adaptive Security in Smart Spaces*	Universidade de Oulu	Tese de Doutorado
RAMOS; BERNABE; SKARMETA, 2015	*Managing Context Information for Adaptive Security in IoT Environments*	IEEE, Web of Science, Scopus	*International Conference on Advanced Information Networking and Applications Workshops*
AMAN, 2016	*Adaptive Security in the Internet of Things*	Universidade de Ciência e Tecnologia da Noruega	Tese de Doutorado
EL-MALIKI; SEIGNE, 2016	*Efficient Security Adaptation Framework for Internet of Things*	IEEE, Web of Science, Scopus	*International Conference on Computational Science and Computational Intelligence*
MOZZAQUATRO et al., 2018	*An Ontology-based Cybersecurity Framework for the Internet of Things*	MDPI	*Special Issue - Security in IoT Enabled Sensors*
KHAN; NDUBUAKU , 2018	*Ontology-based Automation of Security Guidelines for Smart Homes*	IEEE, Scopus	*World Forum on Internet of Things (WF-IoT)*

não apenas os artigos dispostos na Tabela 4, mas sim toda a produção bibliográfica dos autores associadas aos modelos propostos.

6.1. Risk-based Adaptive Security for Smart IoT in eHealth

Este artigo propõem um *framework* de segurança adaptativa baseado em risco para a IoT em cenários de *eHealth* ABIE; BALASINGHAM (2012). O *framework* utiliza a teoria dos jogos e técnicas de ciência de contexto para estimar e prever o risco à segurança da informação. Os métodos e mecanismos de segurança do *framework* buscam adaptar as decisões de segurança sobre essas estimativas e previsões. O *framework* incorpora modelos de avaliação prática e sistemática que utilizam métricas de segurança para validação da adaptação.

A abordagem realiza um esforço para aumentar a segurança a um nível adequado, adaptando-se às condições dinâmicas de mudança da IoT, incluindo usabilidade, ameaças e heterogeneidade. O artigo também descreve um possível estudo de caso projetado para validação que propõem estratégias adaptativas para a interação dinâmica entre segurança e transmissão de dados em um sistema de monitoramento de pacientes móveis.

O *framework* emprega o ciclo de controle adaptativo, por meio da metodologia

Monitor-Analyze-Adapt, para gerenciamento de riscos de segurança e privacidade levando em consideração as informações de contexto necessárias para garantir a eficiência ao longo do tempo. A Tabela 5 mostra o alinhamento da metodologia Plan-Do-Check-Act (PDCA) apresentada na ISO/IEC 27005:2008 com os processos *Information Security Management System* (ISMS) e *Information Security Risk Management* (ISRM) com a *Adaptive Risk Management* (ARM) proposta.

Tabela 5. Alinhamento da ISO/IEC 27005 ISMS, ISRM e ARM

Processo ISMS	Processo ISRM	Processo/Metodologia ARM Proposto
Plan	*Establish the context; Risk assessment; Risk treatment planning; Risk acceptance*	*Analyze (plan): establish security*
Do	*Implementation of risk treatment plan*	*Adapt (Execute): adapt, implement and operate security*
Check	*Continual monitoring and reviewing of risks*	*Monitor: monitor and review security*
Act	*Maintain and improve the ISRM process*	*Adapt (learn): maintain, learn & improve security*

Os autores definem ARM como um modelo de gerenciamento de riscos capaz de aprender, adaptar, prevenir, identificar e responder a ameaças conhecidas e desconhecidas em tempo real. A principal função deste modelo é o desenvolvimento de métodos e mecanismos de segurança adaptativos baseados em risco para dispositivos inteligentes da IoT que estimam e prevêem danos de risco e benefícios futuros, integrando modelos de monitoramento adaptativo, analítico e preditivo, modelos de decisão adaptativa e modelos de avaliação e validação em um ciclo contínuo, permitindo que os métodos e mecanismos de segurança adaptem suas decisões sobre essas estimativas e previsões.

Para enfrentar esses desafios, o modelo ARM proposto considera as seguintes medidas necessárias: (i) identificação - capacidade de prever problemas, (ii) análise - capacidade de prever o impacto, (iii) planejamento para implementar ações planejadas, (iv) rastreabilidade - capacidade de manter o foco do gerenciamento em ações de mitigação de risco, e (v) controle - capacidade de reduzir a exposição ao risco. Estas medidas são alcançadas através da coordenação de diferentes modelos.

A Figura 4 descreve o *framework* de segurança adaptativa baseada em risco para a IoT. O *framework* consiste em (i) o modelo de gerenciamento de risco adaptativo, (ii) o modelo de monitoramento adaptativo, (iii) os modelos analíticos e preditivos, (iv) os modelos adaptativos de tomada de decisão e (v) os modelos de avaliação e validação.

O modelo de monitoramento de segurança adaptável (*Adaptive Monitoring*) empregado no *framework* foi proposto pelos autores em ABIE et al. (2010) e é utilizado para obter evidências técnicas automatizadas para fins de monitoramento de segurança operacional contínua. O modelo de monitoramento de segurança adaptável adapta a arquitetura seguindo um ciclo contínuo de monitoramento das informações de contexto e estado dos dispositivos inteligentes da IoT que são explorados em tempo de execução no processo de adaptação.

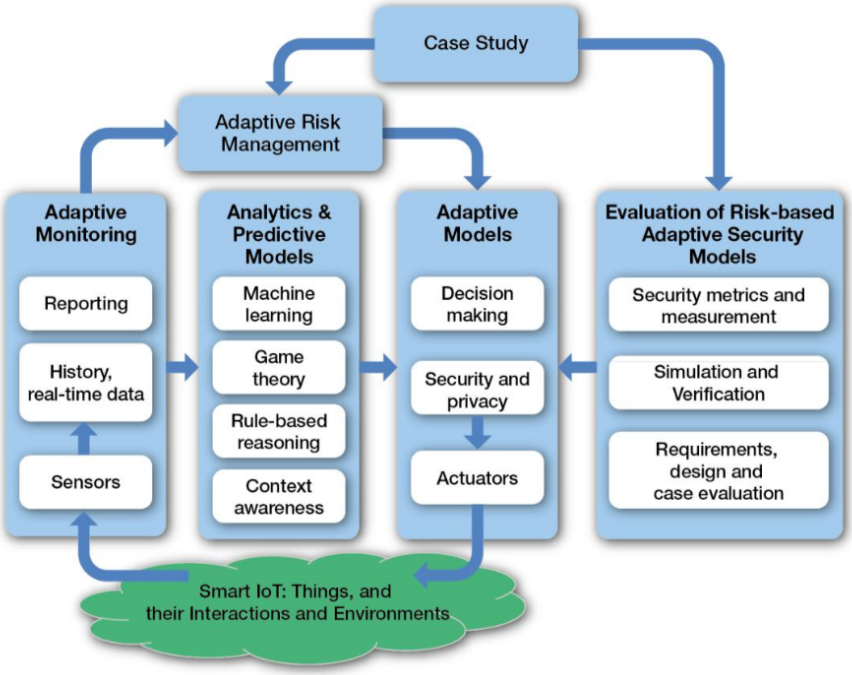

Figura 4. Modelo proposto para gerenciamento de segurança adaptativa
Fonte: ABIE; BALASINGHAM, 2012

Os modelos analíticos e preditivos analisam as informações coletadas a partir do modelo de monitoramento adaptativo usando a teoria dos jogos e a ciência de contexto para estimar e prever dinamicamente riscos de segurança e privacidade e benefícios futuros, visando compreender e priorizar as atividades de tomada de decisão e analisar a segurança socioeconômica da segurança adaptativa na IoT. A teoria dos jogos foi escolhida pois pode modelar o comportamento dinâmico das partes interessadas com interesses conflitantes, incluindo as estratégias dos adversários do mundo real. Os modelos também buscam aprimorar a precisão das estimativas aplicando métodos de aprendizado automatizado e algoritmos baseados em regras.

Na eHealth baseada na IoT, segurança adaptativa para tomada de decisão é necessária para adaptar os meios de proteção dos dispositivos envolvidos, suas interações e seu ambiente contra intrusos maliciosos e usuários autorizados. O modelo de tomada de decisão adapta-se ao dinamismo desses dispositivos, suas interações, ao meio ambiente e aos diversos graus de risco que o sistema da IoT para eHealth será confrontado. Isso é realizado determinando dinamicamente se as mudanças e a adaptação devem ser feitas ou não e, se for feita, selecionando o "melhor" modelo de segurança adaptativo para uma determinada situação para posteriormente aplicar as mudanças e adaptações identificadas garantindo a maior probabilidade de alcançar o maior benefício para o menor risco. O modelo geral de tomada de decisão adaptativa também aprende e se adapta a um ambiente de IoT em mudança em tempo de execução. Isso é feito (i) combinando modelos adaptativos de decisão baseado em risco, modelos adaptativos de segurança e privacidade e atuadores para fazer uma reação adaptativa efetiva, e (ii) integrando diferentes métricas para validação e verificação, avaliação adaptativa de risco e modelos de análise preditiva para estimativa e previsão de riscos e impactos de segurança e privacidade.

O artigo detalha ainda um possível estudo de caso baseado no fato de que os sistemas de monitoramento de pacientes são uma importante fonte de dados em ambientes de saúde. É ressaltado que esses sistemas devem manter um certo nível de disponibilidade, de QoS, de segurança e de proteção da privacidade do paciente. Com isso, os autores apresentam uma proposta de estudo de caso (vide Figura 5) baseado em um sistema de monitoramento de pacientes apoiado pela IoT . O paciente pode estar em casa ou no hospital, e os dispositivos da IoT incluem *smartphones*, *tablets*, sensores e atuadores.

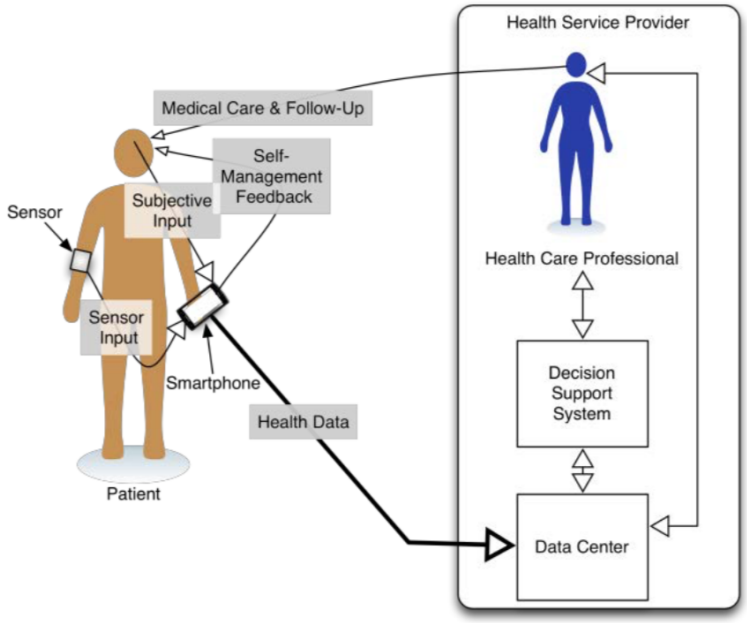

Figura 5. Estudo de caso baseado em monitoramento de paciente
Fonte: ABIE; BALASINGHAM, 2012

Como trabalho futuro os autores destacam: desenvolvimento e prototipação dos modelos para estimar e prever riscos e benefícios usando a teoria dos jogos e a ciência de contexto; definição da metodologia para medições de segurança e métricas para validar a eficácia da adaptação; bem como, a concepção de dispositivos inteligentes com mecanismos de baixo consumo de recursos que irão permitir a detecção de ameaças em tempo de execução, respondendo a elas e se adaptando ao meio ambiente, aprimorando o grau de segurança e privacidade. Também é incluído a necessidade de validação do cenário proposto.

6.2. Adaptive Security in Smart Spaces

A tese de doutorado de Evesti (2014) apresenta uma arquitetura para segurança adaptativa em espaços inteligentes. A abordagem combina um ciclo de adaptação, uma ontologia denominada *Information Security Measuring Ontology* (ISMO) e um modelo de controle de segurança para espaços inteligentes. O ciclo de adaptação inclui as fases de monitoramento, análise, planejamento e execução de mudanças no espaço inteligente. De acordo com os autores, a abordagem se diferencia por definir todo o ciclo de adaptação e o conhecimento necessário em cada etapa. As contribuições são validadas como parte do protótipo de um espaço inteligente. A abordagem oferece meios reutilizáveis e extensíveis

para alcançar a segurança adaptativa em espaços inteligentes EVESTI; SUOMALAINEN; OVASKA (2013).

Apesar de no artigo EVESTI; SUOMALAINEN; OVASKA (2013) a arquitetura ser explorada por meio de políticas dinâmicas de controle de acesso, o trabalho foi estendido em Evesti (2014), onde outros cenários de uso são expostos. Ou seja, a segurança adaptativa pode ser aplicada em vários domínios, sendo uma abordagem de adaptação genérica, consequentemente permitindo a adaptação à vários objetivos de segurança.

A estrutura da arquitetura proposta é apresentada na Figura 6, onde observa-se que a mesma está em conformidade com o modelo de referência MAPE-K. Consequentemente, os componentes *Monitor*, *Analyser*, *Planner* e *Executor* desempenham um papel fundamental na estrutura, ou seja, a arquitetura aplica o ciclo de adaptação MAPE completo para a segurança adaptativa e define cada fase separadamente. O conhecimento é oferecido a partir da ontologia no formato *Ontology Web Language* (OWL), a ISMO, a qual está conectada aos componentes *Monitor*, *Analyser* e *Planner* que utilizam o seu conhecimento.

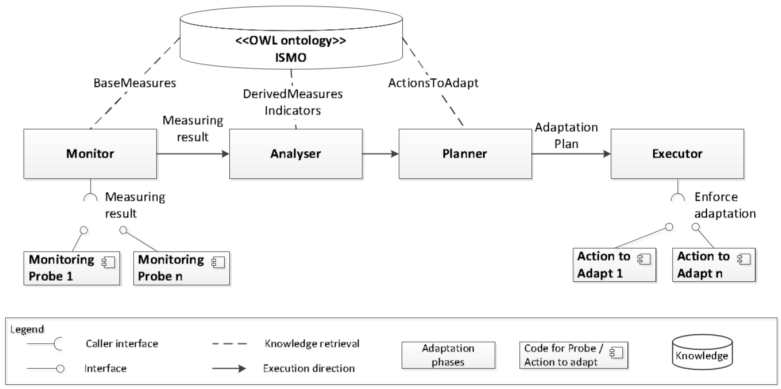

Figura 6. Estrutura da arquitetura de adaptação
Fonte: EVESTI, 2014

O componente *Monitor* está conectado aos componentes *Monitoring Probe*, ao *Analyzer* e ao ISMO. Da ISMO, o *Monitor* recupera as métricas base. Assim, apenas as métricas para os objetivos de segurança exigidos e os mecanismos de segurança utilizados são usadas. Cada métrica base possui sua própria abordagem de medição que descreve como realizar a medição. Os componentes *Monitoring Probe* são trechos de código que implementam os métodos de medição. O componente *Monitor* solicita a medição dos resultados dos componentes *Monitoring Probe* selecionados. A solução proposta utiliza métricas de segurança para monitorar o nível de segurança alcançado.

O componente *Analyzer* é chamado pelo componente Monitor. A Figura 7 mostra os componentes internos do componente *Analyzer* para calcular o indicador de nível de segurança. O *Analyzer* recupera medidas derivadas, indicadores e abordagens de medição relacionadas da ISMO. O componente analisa as regras dos modelos de análise que são utilizados no componente do combinador de métricas base (*Base measure combiner*) para calcular o indicador de nível de segurança. Posteriormente, o componente *Analyzer* compara os níveis de segurança alcançados e necessários com base em informações contextuais monitoradas e chama o componente *Planner* se a segurança necessária não tiver sido

alcançada.

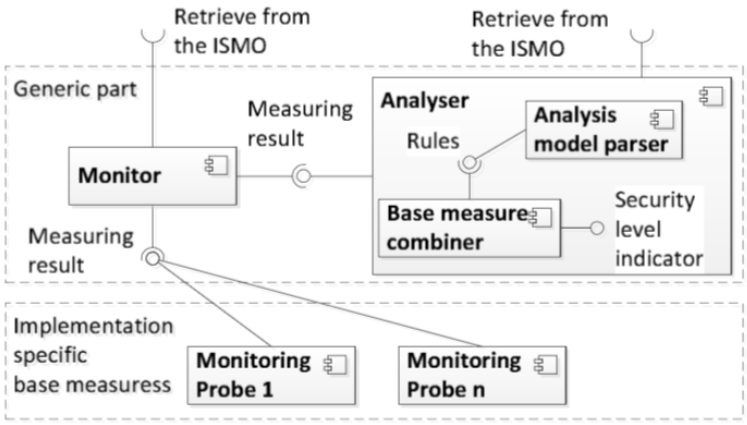

Figura 7. Partes genéricas e específicas da implementação do monitoramento do nível de segurança

Fonte: EVESTI, 2014

O objetivo do componente Planner é criar um plano de adaptação. O componente é conectado à ontologia ISMO para recuperar mecanismos ou atributos de segurança alternativos para alcançar a segurança necessária. O plano de adaptação é definido em tempo de modelagem e decidido em tempo de execução com base no conhecimento da ISMO, ou na pior situação, as instruções sobre como proceder são solicitadas ao usuário.

O *Executor* é o último componente no loop de adaptação. Seu objetivo é fazer cumprir o plano de adaptação recebido como entrada do componente *Planner*. Assim, ele está conectado aos componentes *Action to Adapt*, que são implementações para adaptar a segurança, ou seja, são mecanismos de segurança destinados a aplicar ou modificar os atributos dos mecanismos de segurança.

No que diz respeito a base de conhecimento ISMO, é ressaltado que a adaptação de segurança requer: i) conhecimento de segurança, ii) medição de conhecimento e iii) conhecimento de contexto. O conhecimento de segurança define objetivos de segurança, mecanismos, ameaças e como eles estão relacionados. Posteriormente, a medição do conhecimento descreve os atributos e a forma de medi-los. Por último, o conhecimento de contexto descreve o espaço inteligente e o papel dos dados, usuários e ações dentro do espaço inteligente. Essas três áreas de conhecimento são apresentadas na Figura 8.

De acordo com o projeto, a fase de monitoramento é definida em um nível detalhado, no entanto, as fases de análise e planejamento precisam de refinamentos. A fase de análise deve reconhecer o nível de segurança obtido com base nos resultados do monitoramento e deduzir o nível de segurança necessário das informações de contexto. Aprimorar estas duas tarefas garantiria a identificação dos requisitos de segurança e as necessidades de adaptação em diferentes situações. Além disso, a fase de planejamento da adaptação necessita de algoritmos de tomada de decisão mais sofisticados que considerem diferentes objetivos de segurança. Finalmente, Evesti menciona a necessidade de descentralização da abordagem, especialmente considerando o desenvolvimento das limitações aqui mencionadas que podem implicar em uma necessidade maior de poder computacional, seja de

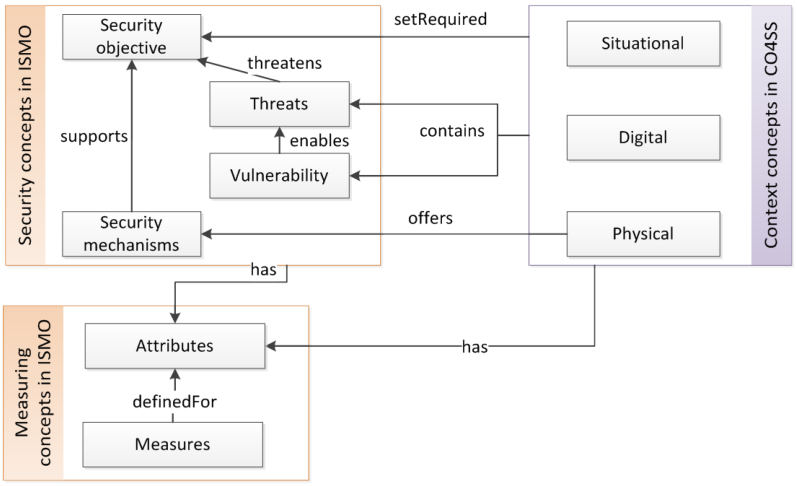

Figura 8. Dependências entre ontologias de segurança e de contexto
Fonte: EVESTI, 2014

armazenamento ou processamento.

6.3. Managing Context Information for Adaptive Security in IoT Environments

O trabalho de Ramos et al. (2015) visa abordar os desafios de modelagem e desenvolvimento de mecanismos de segurança cientes de contexto para a IoT por meio da definição de dois objetivos. O primeiro é fornecer uma visão geral das implicações de segurança para os estágios do ciclo de vida do gerenciamento de contexto na IoT. E o segundo é a concepção de um *framework* de segurança para IoT proposto em Bernabe et al. (2014) que tem como finalidade apresentar como as informações contextuais podem ser usadas por outros componentes deste *framework* para capacitar objetos inteligentes com ciência de contexto ao tomar decisões de segurança.

A Figura 9 apresenta o *framework* de segurança para IoT concebido em Bernabe et al. (2014), no qual o grupo funcional de segurança é detalhado. O *framework* amplia os componentes de segurança da *Architecture Reference Model* (ou seja, *Authentication*, *Authorization*, *KEM*, *Identity Management*, e *Trust && Reputation*) com a inclusão do *Group Manager* e do *Context Manager*. O primeiro pretende lidar com mecanismos de compartilhamento de dados mais flexíveis em que um grupo de objetos inteligentes podem ser envolvidos, enquanto a segurança e a privacidade são preservadas. O último é proposto para permitir a concepção de mecanismos de segurança cientes ao contexto para IoT, bem como para considerar as implicações de segurança durante as diferentes etapas do ciclo de vida do gerenciamento de contexto. Por outro lado, o *framework* de segurança propõe as principais interações entre esses componentes de segurança, de modo a permitir a modelagem de mecanismos de segurança inovadores e adequados, a serem explorados em cenários da IoT.

As pesquisas associadas à Ramos et al. (2015) possuem como foco o Gerenciador de Contexto (*Context Manager*), bem como as principais interações com outros componentes de segurança, a fim de tornar as decisões de segurança cientes de contexto. Além disso, são propostos diferentes estágios para o ciclo de vida do gerenciamento de contexto (incluindo aquisição, modelagem, organização, raciocínio, combinação e inferência

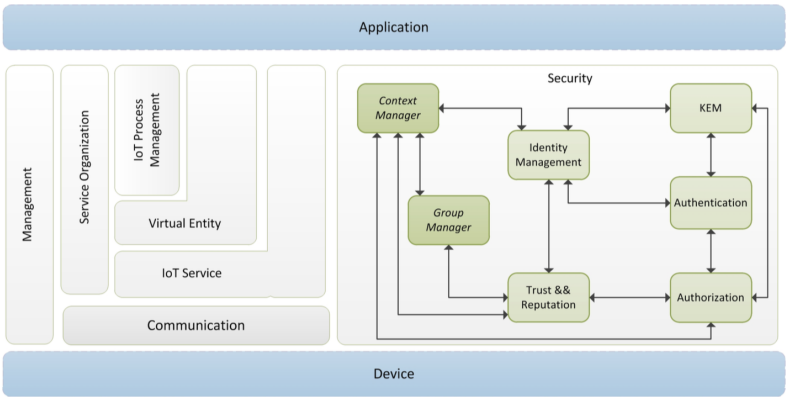

Figura 9. Framework de segurança ciente de contexto para IoT
Fonte: BERNABE et al., 2014

de informações contextuais), bem como um conjunto de diretrizes sobre implicações de segurança durante estes estágios.

A Figura 10 mostra os principais estágios considerados para o Gerenciador de Contexto do *framework* de segurança. Essas etapas são extraídas das fases do ciclo de vida do contexto, que são propostas em Perera et al. (2014). Antes de descrever essas etapas, deve-se destacar que o Gerenciador de Contexto pode ser instanciado de maneira diferente dependendo da entidade da IoT que está sendo considerada. Por exemplo, enquanto os *smartphones* atuais podem ser capazes de implantar toda a funcionalidade das diferentes etapas, outros dispositivos da IoT com mais restrições de recursos, só poderiam implementar um subconjunto. No caso de sensores ou atuadores, eles podem implantar um subcomponente do comunicador de contexto, mas não a funcionalidade de raciocínio.

O Gerenciador de Contexto é dividido em quatro etapas principais. Em primeiro lugar, durante a fase de aquisição, o *Context Acquirer* obtém informações de contexto a serem processadas. Esses dados podem ser provenientes de outras entidades internas (por exemplo, um acelerômetro no caso de um *smartphone*) ou de outros objetos inteligentes no ambiente monitorado (por exemplo, um sensor de temperatura). Nesse caso, as informações de contexto podem ser adquiridas através de diferentes protocolos de comunicação empregados na IoT, como o *Constrained Application Protocol* (CoAP), *Extensible Messaging and Presence Protocol* (XMPP) ou *Message Queue Telemetry Transport* (MQTT). Essas comunicações podem ser realizadas entre dispositivos com restrições de recursos, e precisam ser protegidas para que o Gerenciador de Contexto somente processe informações provenientes de objetos inteligentes legítimos. Enquanto alguns destes protocolos fornecem opções de segurança por meio de diferentes mecanismos (por exemplo, *Datagram Transport Layer Security* (DTLS) no caso do CoAP), atualmente, a implementação de mecanismos de segurança para esses protocolos é um tópico de pesquisa.

Depois que a informação contextual é adquirida, o conjunto de dados brutos é encaminhado para o componente *Context Modeller* para serem interpretados e modelados de acordo com um modelo de contexto comum. Para esse fim, o subcomponente *Context formatter* é responsável por traduzir dados brutos para um formato comum que pode ser interpretado pelas camadas superiores do Gerenciador de Contexto. Para a modelagem

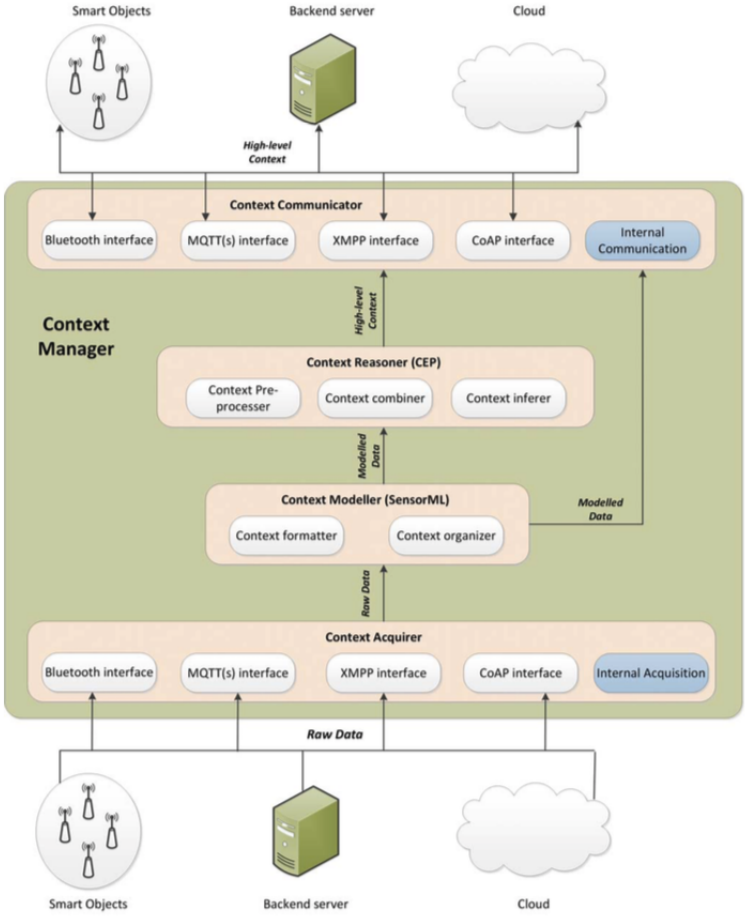

Figura 10. Visão geral do Gerenciador de Contexto
Fonte: PERERA et al., 2014

das informações contextuais nos ambientes da IoT, é necessário considerar um balanço entre o grau de expressividade do modelo e a viabilidade a ser implantada em certos tipos de dispositivos. Portanto, para o Gerenciador de Contexto proposto, foi selecionado o *Sensor Model Language* (SensorML) OCG (2018) (na versão *JavaScript Object Notation* (JSON)) como uma alternativa flexível e gerenciável para a representação de informações contextuais em dispositivos da IoT. SensorML fornece modelagem de informações com base em pares chave-valor e e marcações, o que permite uma representação simples de dados de contexto. Desta forma, uma vez que a informação contextual é modelada, o subcomponente *Context organizer* é responsável por validar o conjunto de dados modelados e adicioná-los ao repositório de informações contextuais do objeto inteligente.

Na próxima etapa, o *Context Reasoner* é responsável por deduzir informações de contexto de alto nível sobre os dados modelados fornecidos pela etapa anterior. Para isso, são realizadas três tarefas principais. Em primeiro lugar, os dados modelados são enviados para o *Context Pre-processer* que irá descartar dados ambíguos e imprecisos, ou provenientes de entidades não confiáveis e atribuir menor prioridade aos dados de contexto provenientes de objetos inteligentes com uma reputação questionável.

Uma vez que os dados de contexto foram pré-pré-processados, a informação con-

textual é combinada pelo *Context combiner* com dados de diferentes entidades levando em consideração a prioridade dos dados contextuais para criar uma visão de contexto mais completa.

Finalmente, durante a fase de inferência, o conjunto de dados combinados é usado para produzir informações de contexto de alto nível através do *Context inferer*. Este processo também pode estar ciente das preferências de segurança e privacidade do objeto inteligente. Existe uma ampla gama de técnicas de raciocínio de contexto que podem ser aplicadas, como por exemplo, regras, lógica difusa, ontologias ou lógica probabilística. Nesse sentido, dado o alto grau de dinamismo e ubiquidade da IoT, a tecnologia de CEP, fornece meios para processar eventos derivados de informações contextuais provenientes de diferentes entidades. Especificamente, fornece um procedimento apropriado para filtrar, agregar e mesclar dados de diferentes fontes em tempo de execução. A CEP é uma tecnologia bem conhecida baseada em regras, fácil de estender e de menor uso de recursos do que outras técnicas de raciocínio (por exemplo, ontologias), o que favorece sua adoção para o paradigma da IoT.

Durante a última etapa, informações contextuais de alto nível são enviadas para outras entidades (por exemplo, outros objetos inteligentes, servidores ou nuvem para processamento posterior), usando o *Context Communicator*. Neste caso, as considerações de segurança do *Context acquirer* também devem ser levadas em consideração por este componente para proteger as informações que estão sendo disseminadas. Além disso, a comunicação de informações contextuais de alto nível deve basear-se nas especificações NGSI-9 e NGSI-10 O.M.A. (2012), permitindo uma interface comum para troca de dados de contexto com outras entidades. Outras considerações de segurança podem ser levadas em consideração quanto à freqüência ou granularidade desses dados, pois isso pode prejudicar a privacidade do objeto inteligente (ou do proprietário). Além das interfaces de comunicação externas, o comunicador de contexto mantém uma interface de comunicação interna para enviar informações de contexto de alto nível para outros componentes do *framework* de segurança. Essas interações destinam-se a criar uma visão de segurança adaptativa para o paradigma da IoT.

Após a descrição dos componentes do Gerenciador de Contexto, conforme observa-se na Figura 11, os autores apresentam as principais interações projetadas entre o gerenciador e outros componentes de segurança para gerar as decisões de segurança sobre os objetos inteligentes promovendo a segurança adaptativa.

O componente *Identity Management* (IdM) é responsável por gerenciar as identidades de um objeto inteligente de forma a preservar a privacidade. O *Authorization* é baseado em uma combinação de modelos e técnicas de controle de acesso sendo implantado para gerar tokens de autorização. O componente *Trust && Reputation* permite estabelecer um ambiente de IoT seguro e confiável, onde os usuários podem interagir com os serviços da IoT com segurança. Enquanto o *Group Manager* baseia-se no uso do esquema de criptografia *Ciphertext Policy Attribute Based Encryption* (CP-ABE) para permitir um mecanismo seguro de compartilhamento de dados com grupos de objetos inteligentes.

Finalmente, os autores discutem a necessidade de implementação das diferentes etapas do gerenciamento de contexto e das interações propostas com outros componentes de segurança, a fim de demonstrar a integração de mecanismos de segurança flexíveis,

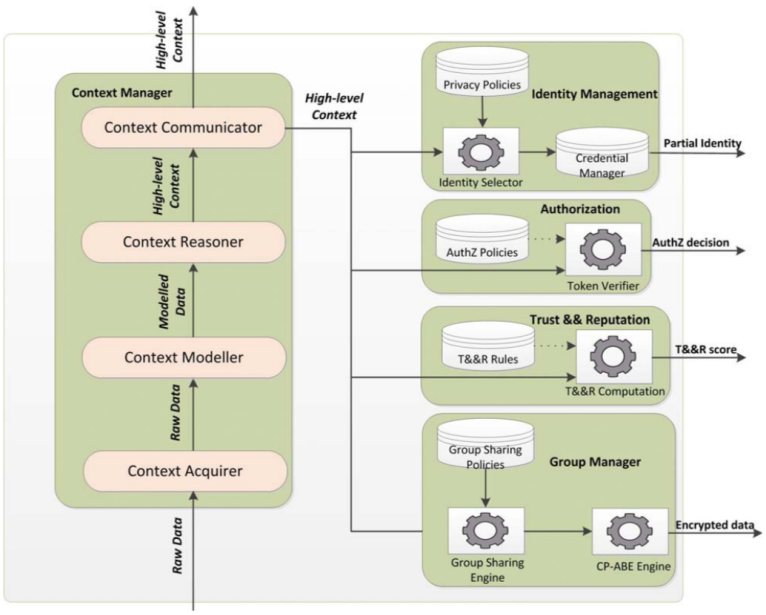

Figura 11. Interações do *framework* para mecanismos de segurança adaptativa cientes de contexto

Fonte: PERERA et al., 2014

leves e adaptativos em diferentes cenários.

6.4. Adaptive Security in the Internet of Things

A tese de Aman (2016) apresenta a concepção de uma solução autônoma para o gerenciamento de risco adaptativo para a IoT que permite analisar situações adversas em um contexto distinto e gerenciar o risco envolvido de forma inteligente para que as preferências do usuário final, a qualidade do serviço e a segurança estejam preservados. Com isto, em Aman e Snekkenes (2014) é apresentado o modelo de segurança adaptativa orientado a eventos para IoT, denominado *Event Driven Adaptive Security* (EDAS), o qual é aplicado em um cenário de eHealth para proteger o ambiente de ameaças em tempo de execução.

Para realizar o monitoramento dos eventos de segurança foi utilizada a solução *Open Source Security Information Management* (OSSIM) ALIENVAULT (2018). No que tange as adaptações das configurações de segurança, de modo que as preferências de usuários e serviços sejam preservadas, os autores propõem uma ontologia que aproveita as informações de risco da correlação de eventos. A ontologia permite que uma ação de mitigação seja selecionada de um conjunto de ações de forma que sua utilidade, em termos de usabilidade, QoS e confiabilidade de segurança, seja máxima entre as possíveis ações conforme os requisitos do usuário.

A principal contribuição deste artigo é a ontologia de adaptação autonômica à segurança. A OSSIM não fornece essa capacidade e depende de reconfigurações manuais que podem não atender aos requisitos do usuário e do serviço. Além disso, o OSSIM está focado no ambiente de computação tradicional, incluindo servidores, desktops e aplicações correspondentes, onde o processamento de eventos é relativamente uma tarefa comum. Este artigo amplia a segurança orientada à eventos para a IoT, onde o ambiente se torna mais complexo devido à diversidade e mobilidade dos dispositivos para as quais

os protocolos e ferramentas tradicionais são ineficientes para processar eventos.

O modelo apresentado, *Event Driven Adaptive Security* (EDAS), aborda a segurança adaptativa na IoT como uma *Event Driven Architecture* (EDA) na forma de um clico de *feedback*. O elemento básico de mudança disponível no ambiente monitorado é o evento gerado por várias aplicações e dispositivos registrados em arquivos de log. Eles fornecem um contexto primitivo sobre "quem, quando, onde e o que" provoca uma mudança e contém informações importantes, como data, origem, destino, atividade do usuário, níveis de gravidade, entre outras, necessárias para detectar situações de risco associadas a um evento. Um modelo de referência é apresentado na Figura 12, a qual inclui três principais componentes *Monitor*, *Analyzer* e *Adaptor*.

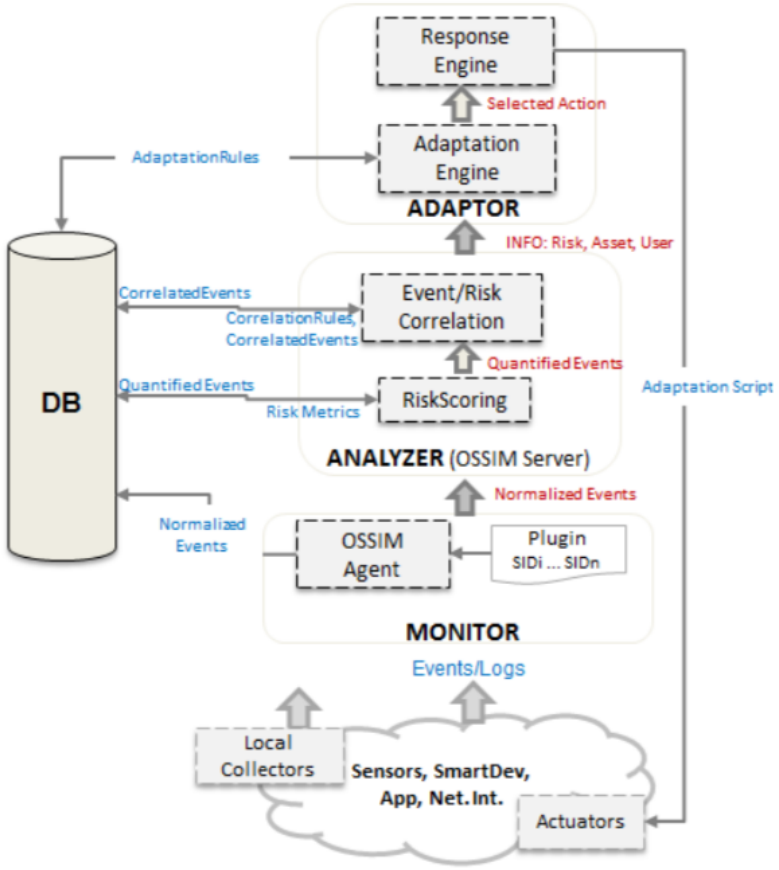

Figura 12. EDAS - modelo de referência
Fonte: AMAN, 2016

O componente *Monitor*, prototipado por meio do OSSIM Agent, coleta, filtra e normaliza eventos de diferentes dispositivos da IoT. Para a coleta, o EDAS faz uso tanto da bordagem com agente quanto sem agente (conhecida como *agent-less*), neste caso explorando protocolos como Syslog e *Simple Network Management Protocol* (SNMP). No que diz respeito aos dispositivos da IoT, os autores adotaram um agente baseado no *MQ Telemetry Transport* (MQTT), um protocolo de transporte de mensagens *Machine-To-Machine* M2M projetado especificamente para IoT independente de plataforma. O cliente do MQTT conecta-se à API de eventos do dispositivo para coletar eventos de segurança gerados e os transporta para o OSSIM Agent, onde eles são armazenados em um arquivo

de log específico.

A filtragem de eventos é realizadas através dos *plugins*, concebidos para fontes de eventos individuais. Escrever estes *plugins* requer algum conhecimento da fonte e dos eventos que estão sendo analisados. O *plugin*, identificado por um ID exclusivo e outros parâmetros necessários, é um arquivo de configuração que determina quais eventos da fila devem ser tratados e quais deles precisam ser filtrados. A OSSIM utiliza um mecanismo de lista branca (do inglês *white-listing*) baseado em expressões regulares onde apenas eventos de interesse são enviados para posterior processamento. Quando ocorre uma correspondência com as expressões um identificador único de segurança (SID) é atribuído ao evento, o qual é geralmente utilizado na correlação de eventos.

A normalização é realizada pois diferentes dispositivos da IoT produzem eventos em diferentes formatos. Logo, é necessário transformá-los em um único formato comum para correlação e análise. Este processo é realizado durante a extração de SIDs e visa também extrair atributos importantes de um evento. Os atributos variam de evento para evento dependendo do contexto primitivo que eles possuem.

O componente *Analyzer* é prototipado por meio do OSSIM Server. Inicialmente, antes dos eventos serem correlacionados, uma pontuação de risco é atribuída à eles. A OSSIM usa três métricas para calcular o risco do evento em tempo de execução:

- Valor do ativo (*asset value*): determina a importância da origem ou do destino dos eventos dentro do escopo monitorado. Varia de 0 a 5.
- Prioridade (*priority*): especifica o impacto do evento. Varia de 0 a 5.
- Confiabilidade (*reliability*): determina a probabilidade ou a confiança de que o evento corresponderá a um comprometimento do ativo. A confiabilidade varia entre 0-10.

Com isto, para cada evento X o risco é quantificado na função:

$$Risco(X) = (Prioridade \times Valordoativo \times Confiabilidade)/25$$

A divisão de 25 é feita para manter os valores de risco no intervalo de 0 a 10, o que reflete o nível de risco de cada evento. Esses valores são atribuídos à medida que chegam no mecanismo *Risk Scoring*, e são armazenados no banco de dados mantendo a relação com cada SID, podendo ser alterados manualmente conforme necessário. Já os valores de prioridade e confiabilidade podem ter valores diferentes configurados nas diretivas de correlação.

Na sequência, o mecanismo de correlação analisa os eventos usando diretrizes de correlação armazenadas em *eXtensible Markup Language* (XML). A correlação é disparada quando um SID específico é encontrado e, portanto, um novo evento é gerado com um novo valor de confiabilidade. O motor aumenta e diminui esse valor com os respectivos atributos definidos dentro das diretivas. Portanto, o risco é avaliado dinamicamente quando os SIDs são correlacionados ao longo do tempo. A correlação de eventos produz eventos de alto nível que vão para uma correlação detalhada ou são marcados como alarmes a serem gerenciados. Os alarmes são eventos correlacionados com o nível de risco acima do limite de aceitação de risco. As informações carregadas por um alarme incluem IDs de origem e de destino, o usuário envolvido, o nível de risco, os detalhes da ameaça e a diretiva de correlação responsável por gerá-lo. Esta informação é utilizada durante o processo de adaptação onde o risco confrontado é mitigado.

Para utilizar o conhecimento disponível de forma precisa e adaptar as configurações de segurança de forma otimizada, a ontologia de adaptação proposta é empregada. Para operar em tempo de execução, a ontologia considera todas as entidades e seus relacionamentos necessários para uma segurança adaptativa otimizada. O modelo proposto é utilizado em um cenário de *eHealth* habilitado para IoT, onde um paciente é gerenciado remotamente pela internet ou rede celular. Para isso, três contextos diferentes foram estabelecidos na ontologia proposta, conforme mostrado na Figura 13.

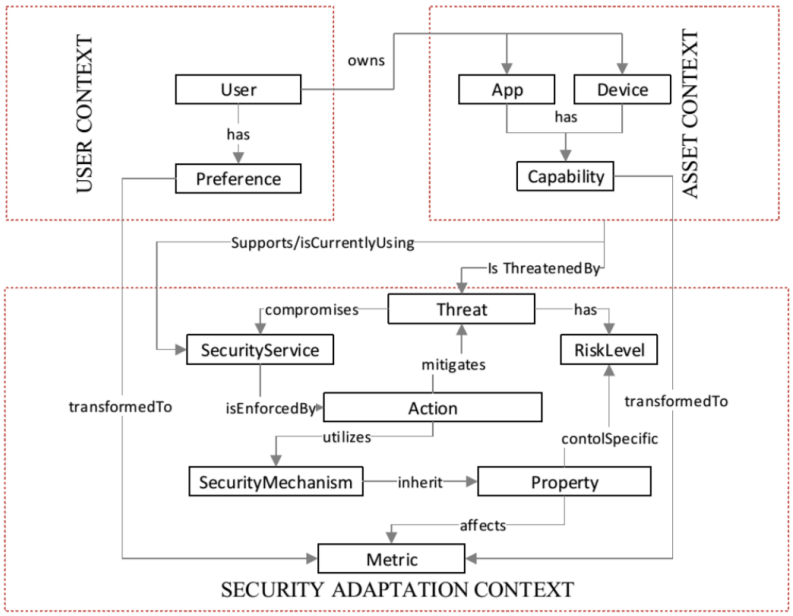

Figura 13. EDAS - ontologia para segurança adaptativa
Fonte: AMAN; SNEKKENES, 2014

O *User Context* corresponde às preferências do paciente e da equipe médica que devem ser consideradas antes da adaptação Cada usuário possui ou utiliza um conjunto de aplicativos, como o aplicativo *eHealth*, o Skype para comunicação paciente-médico, entre outros, e dispositivos, como sensores corporais, dispositivos inteligentes ou *desktop*/notebook, no escopo da infraestrutura da IoT-eHealth. As informações correspondentes, por exemplo, tipo, valor de ativos, etc., juntamente com suas capacidades, estão contidas em *Asset Context*. As entidades e as configurações associadas necessárias para a adaptação de segurança otimizada são agrupadas no *Security Adaptation Context*.

Uma ação de mitigação ideal é selecionada a partir do conjunto de ações seguindo o procedimento mostrado na Figura 14. O mecanismo de resposta (*Response engine*) envia uma mensagem usando o MQTT para um atuador (cliente MQTT instalado no dispositivo monitorado) com os detalhes da ação fornecida pelo mecanismo de adaptação. O atuador é conectado à API do dispositivo, por exemplo uma API de autenticação, e encaminha a mensagem como variáveis a serem reconfiguradas.

Uma função de predição escolhe a ação de adaptação com o máximo de utilidade. Os pesos subjetivos são atribuídos a métricas afetadas para cada propriedade, os quais correspondem à utilidade geral da propriedade (para ser usada na ação adaptada) para um usuário específico. As métricas refletem parâmetros, como usabilidade, confiabilidade, custo do serviço, entre outros, que podem ser influenciados negativamente ou positiva-

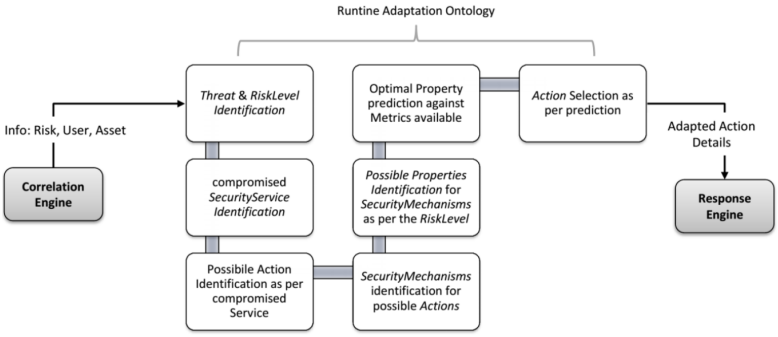

Figura 14. EDAS - processo de segurança adaptativa
Fonte: AMAN; SNEKKENES, 2014

mente por uma propriedade de segurança selecionada. As métricas são agrupadas em três categorias, *User*, QoS e *Security*, para capturar influências sobre preferências de usuários, QoS e confiabilidade de segurança.

Os autores descrevem um cenário da IoT-eHealth no qual um paciente residindo em casa, está equipado com vários sensores corporais. Seus sinais vitais são monitorados através desses sensores e são transmitidos através de uma rede sem fio ou celular para um local remoto do hospital para posterior diagnóstico. O paciente freqüentemente usa seu *smartphone*, parte dessa infraestrutura, instalado com um aplicativo de eHealth para acompanhar o estado de saúde, bem como para pagamentos de cobranças diversas além do uso pessoal. Com isto, um situação adversa é descrita onde um adversário com acesso ao *smartphone* tenta se autenticar no aplicativo de *eHealth*. Desta forma, a EDAS deve levar em consideração os diferentes contextos para escolha da melhor opção de mitigação.

É possível afirmar que ao utilizar o OSSIM, o suporte à heterogeneidade fica limitado, uma vez que é necessário criar as regras para normalização usando uma sintaxe similar a XML por meio da edição de arquivos. Além disso, o OSSIM é reconhecido por limitações quanto a estabilidade e escalabilidade ROCHFORD; KAVANAGH (2015); SHANKAR (2014). De acordo com o próprio autor, os componentes de adaptação são meramente compostos por um analisador de strings e chamadas à API, sendo necessária uma abordagem independente de plataforma para fornecer interoperabilidade na IoT. Finalmente, em Mozzaquatro et al. (2017), ao referenciar o EDAS, os autores destacam que o modelo não considera possíveis vulnerabilidades que possam impedir eventuais ameaças no ambiente.

6.5. Efficient Security Adaptation Framework for Internet of Things

O artigo EL-MALIKI; SEIGNE (2016) apresenta um *framework* genérico denominado *Security Adaptation Reference Monitor* (SARM) que emprega o paradigma autonômico, sendo desenvolvido especialmente para ambientes suportados por redes sem fio altamente dinâmicas. O SARM realiza os ajustes dos parâmetros de segurança levando em consideração o risco do ambiente atual e o desempenho do sistema, especialmente no que se refere à otimização do seu consumo de energia. Isto ocorre sob as políticas e as restrições de intervenção em tempo de execução dos usuários.

O SARM realiza os ajustes dos parâmetros de segurança levando em consideração

o risco do ambiente atual e o desempenho do sistema, especialmente no que se refere à otimização do seu consumo de energia. Isto ocorre sob as políticas e as restrições de intervenção em tempo de execução dos usuários. Assim, de acordo com os autores, o *framework* se difere dos outros por:

- utilizar um sistema de controle de feedback de segurança autônoma;
- empregar mecanismos de segurança dinâmicos e em evolução relacionados ao monitoramento de contextos;
- realizar o gerenciamento de energia explícita;
- lidar com a mobilidade dos atacantes.

O foco principal deste trabalho é a adaptação de segurança em ambientes de comunicação móvel e sem fio. Além disso, de acordo com autores, a melhor maneira de implementar o *framework* para cada programa de comunicação seria integrá-lo no *kernel* e, consequentemente, ter o controle geral da segurança do ambiente. Assim, todos os programas de comunicação teriam que interagir com o SARM para obter acesso aos recursos de comunicação.

O SARM foi proposto como um *framework* genérico pois os autores consideram que implementar e escolher um sistema de segurança adaptativa depende de alguns fatores que estão correlacionados, como: o custo de aquisição; custo de manutenção; usabilidade; e eficiência. Com isto, a proposta foi concebida seguindo uma metodologia de construção modular de blocos de modo a facilitar a integração e ocultar a complexidade interna do sistema. Além disso, essa abordagem permite uma expansão gradual para atender aos novos requisitos da IoT devido a sua constante evolução. Para reagir em tempo real a qualquer ameaça, o SARM baseia-se em informação de *feedback*, buscando reduzir a intervenção humana.

Três componentes principais do sistema autônomo, disposto na Figura 15 foram identificados no projeto: o primeiro é uma unidade funcional, o qual desempenha funções operacionais, sendo responsável por selecionar parâmetros de segurança adequados, como acesso eficiente à rede; o segundo é uma unidade de gerenciamento, que controla a unidade funcional; e o componente final consiste em entradas e saídas. Os parâmetros de segurança são definidos como qualquer algoritmo ou mecanismo que possa aprimorar a segurança, mas que também tenha a capacidade de não tomar medidas de segurança, a menos que seja realmente necessário. Isto inclui a escolha do acesso adequado à rede, uma vez que algumas tecnologias de comunicação de rede são mais seguras, porém com maiores níveis de consumo de energia, enquanto outras são menos seguras, e consequentemente possuem menores níveis de consumo de energia.

O SARM é descrito como uma quintupla: AS = (A,X,Q,Up,Uf). 'A' é composto por componentes do sistema e um conjunto de propriedades. Esses componentes pertencem a informações relacionadas ou não (como QoS, por exemplo) à segurança. O contexto 'X' refere-se à circunstância de qualquer interação entre um usuário e o sistema. As dimensões de adaptividade 'Q' são relacionadas à QoS ou segurança, e fornecem uma visão de alto nível dos usuários do sistema. As preferências do usuário, representadas pela sigla 'Up', expressam restrições e requisitos dos usuários. A função de utilidade 'Uf' expressa a qualidade da adaptação para um usuário ou rede. Os detalhes de implementação e experimentação do SARM junto à uma série de simulações e avaliações incluindo as

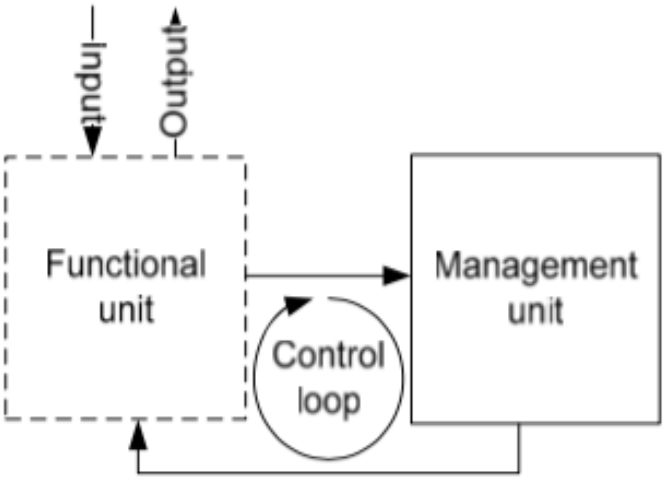

Figura 15. SARM - descrição do sistema autônomo
Fonte: EL MALIKI, 2014

métricas de avaliação, especialmente referentes ao consumo de energia, são expostas em El-Maliki (2014).

Após definir explicitamente os elementos de um sistema adaptativo, os autores realizam o mapeamento dos mesmos em um sistema autônomo, conforme observa-se na Figura 16. Para a unidade funcional, foram adicionadas as preferências de usuários e os parâmetros de segurança. Depois disso, foi adicionado um elemento sensorial para levar em consideração o contexto. Para a unidade de gerenciamento, fora definidas as políticas e logs para segurança de curto e longo prazo ou para análises de segurança e monitoramento de QoS. Os blocos de risco, vulnerabilidades e desempenho foram baseados no módulo de gerenciamento de risco.

Apesar do SARM ser proposto como um modelo genérico, a sua descrição é apresentada em um alto nível, não sendo especificados detalhes de como os blocos modulares são implementados, ou ainda, como eles se comunicam. Diferentemente da maioria dos trabalhos relacionados, os autores optaram pela utilização de simulação para a avaliação. Os autores ainda destacam que novas pesquisas são oportunas para suportar mais parâmetros de adaptação (como o processamento e uso de memória). Além disso, eles mencionam a possibilidade de desenvolvimento do SARM diretamente no sistema operacional, o que vai contra algumas das premissas da IoT. Funções alternativas para tomada de decisão, como funções fuzzy e não lineares, poderiam aumentar a flexibilidade do SARM. Aumentar o número de informações contextuais a serem processadas na função de tomada de decisão pode melhor a qualidade das adaptações, no entanto, aumentando o consumo energético. O autor também considera que qualquer contradição levantada pelas políticas, preferências do usuário e decisão do sistema deve ser abordada em tempo de execução, o que não é suportado completamente. Finalmente, questões de escalabilidade do SARM também devem ser consideradas com maior profundidade para melhorar a credibilidade do framework.

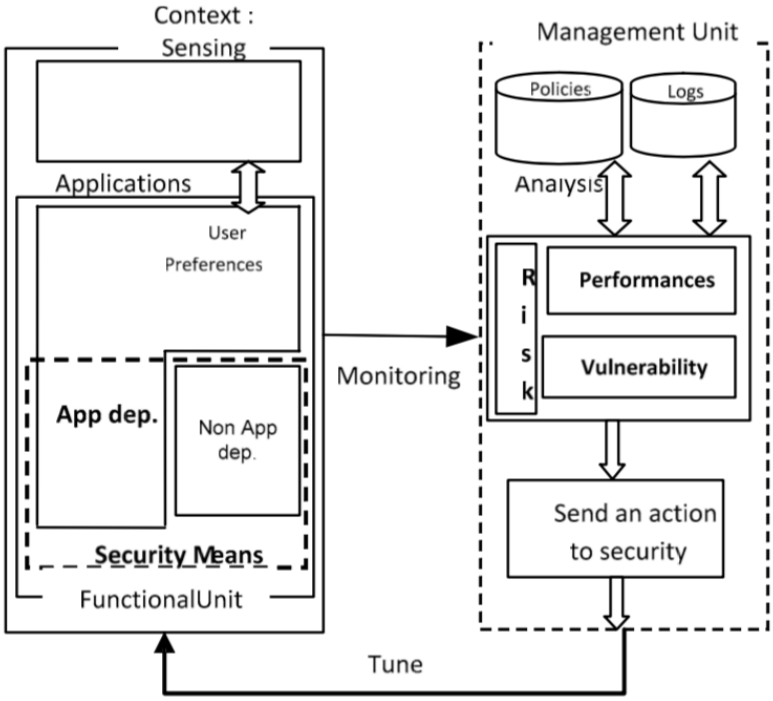

Figura 16. SARM - fundamentos do *framework* genérico para segurança adaptativa

Fonte: EL MALIKI, 2014

6.6. An Ontology-based Cybersecurity Framework for the Internet of Things

O trabalho de Mozzaquatro et al. (2016) propõe uma arquitetura para *framework* de segurança adaptativa (vide Figura 17) baseada no modelo MAPEK utilizando uma ontologia para a tomada de decisões visando melhorar a segurança da informação em sistemas industriais. O framework é adaptado em Mozzaquatro et al. (2018), contemplando duas abordagens: (1) em tempo de projeto, que fornece um método dinâmico para criar serviços de segurança por meio da aplicação de uma metodologia baseada em modelos, considerando os processos empresariais existentes; e (2) em tempo de execução, que envolve monitorar o ambiente da IoT, classificar ameaças e vulnerabilidades e atuar no ambiente, garantindo a adaptação correta dos serviços existentes.

A abordagem em tempo de execução, foco desta análise, monitora os dispositivos da IoT com base em métricas e atributos de segurança para identificar comportamentos maliciosos no ambiente. Consequentemente, as configurações e/ou regras precisam ser adaptadas de acordo com a ontologia, quando os alertas são acionados por ferramentas de segurança. Para isso, a ontologia contribui para identificar as relações entre ameaças, ativos, vulnerabilidades, mecanismos e propriedades de segurança.

A ontologia aprensetada na Figura 18, denominada IoTSec, empregada na base de conhecimento, visa contribuir para sustentar o sistema usando consultas de informações contextuais coletadas no ambiente. A contribuição desta abordagem é validada por meio de duas abordagens: a validação da ontologia empregando a metodologia *Software product Quality Requirements and Evaluation* (SQuaRE); e um cenário industrial imple-

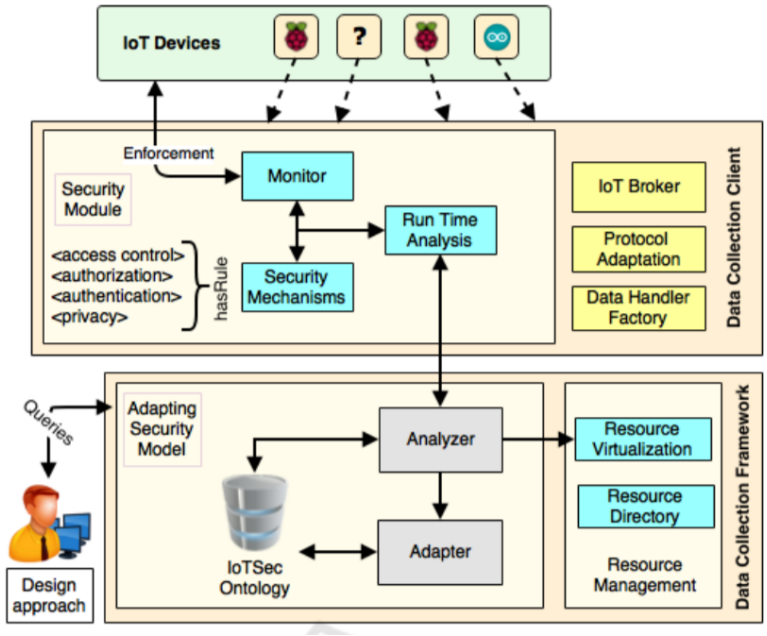

Figura 17. Uma arquitetura para *framework* de segurança adaptativa baseada em ontologia integrada com a plataforma C2NET.
Fonte: MOZZAQUATRO et al., 2016

mentado no âmbito do projeto *Cloud Collaborative Manufacturing Networks* (C2NET[6]) para verificar a adequação da aplicação do *framework* considerando algumas questões de cibersegurança.

A plataforma colaborativa C2NET tem como base a computação na nuvem permitindo que pequenas e médias empresas otimizem os seus recursos logísticos e de produção com base em dinâmicas colaborativas de procura, produção ou expedição. Um dos principais problemas das cadeias de abastecimento tradicionais está relacionado à centralização das abordagens de tomada de decisão, o que dificulta a reação das empresas considerando a dinamicidade dos mercados atuais. De acordo com isso, a plataforma C2NET é proposta para contribuir em vários aspectos da fabricação industrial, explorando a coleta de dados de dispositivos da IoT presentes nas empresas. No entanto, esses dispositivos são vulneráveis a várias ameaças e precisam ser abordados usando mecanismos de segurança. Além disso, alguns desses dispositivos usam diferentes tecnologias da IoT e a plataforma C2NET explora a interoperabilidade baseada em tecnologias da web semântica.

Para avaliação da proposta dois cenários foram desenvolvidos sobre o setor metalúrgico buscando aplicar a estrutura de segurança baseada em ontologia para melhorar os problemas de segurança entre os dispositivos da IoT e a plataforma C2NET. Os autores observam que o trabalho considera que os cenários são vulneráveis apenas à ameaças digitais, como divulgação de informações, ataques de repetição, *spoofing* e outros ataques a dispositivos inteligentes.

Apesar dos trabalhos MOZZAQUATRO; JARDIM-GONCALVES; AGOSTINHO (2015); MOZZAQUATRO et al. (2016, 2018) proporem a concepção de um *fra-*

[6]http://c2net-project.eu/

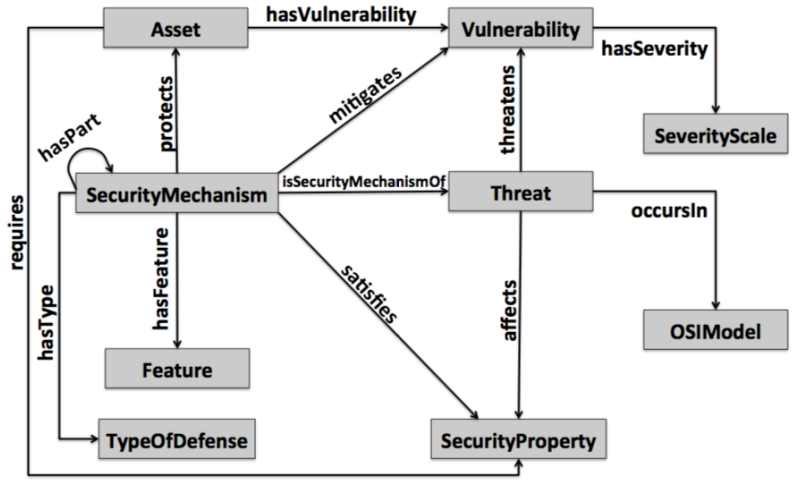

Figura 18. Ontologia de referência para segurança na IoT
Fonte: MOZZAQUATRO et al., 2016

mework integrado ao projeto C2NET, eles não detalham esta integração, comprometendo o ciclo MAPE-K, ou seja, é possível destacar que estes trabalhos são especialmente direcionados à base de conhecimento do ciclo. Os autores apenas mencionam que a utilização de ferramentas de segurança oferecem informações sobre diferentes tipos de alertas. Com isso, não são fornecidos detalhes sobre a implantação e interação entre as ferramentas. Consequentemente, não é possível afirmar maiores detalhes sobre os requisitos de escalabilidade e distribuição do *framework*. Reforçando isto, uma importante limitação destacada pelos autores em Mozzaquatro et al. (2018) é a incapacidade de lidar com desafios reais visto a necessidade de adoção de uma avaliação contínua de risco adaptativo que vise permitir a tomada de decisões em tempo de execução com respostas adaptativas. Finalmente, destaca-se que a proposta não considera diferentes fontes de informações contextuais, sendo focado apenas em questões de segurança.

6.7. Ontology-based Automation of Security Guidelines for Smart Homes

Em Khan; Ndubuaku (2018), uma ontologia é proposta para representar o conhecimento sobre as diretrizes de segurança para interoperabilidade e entendimento entre os usuários de casas inteligentes. Além disso, uma ontologia baseada em contexto é desenvolvida, a qual se adapta à mudanças de informações contextuais, como contexto do usuário e contexto do ambiente físico. Diferentes casos de uso criados com a linguagem de consulta SPARQL demonstram a aplicação de diretrizes de segurança em casas inteligentes e destacam como o contexto pode ajudar o usuário a executar essas diretrizes automaticamente.

A ontologia proposta, denominada *Cyber Security Guidelines Ontology* (CSGO), foi baseada no modelo abstrato de diretrizes de segurança ilustrado na Fig. 19. A CSGO apresenta uma maneira padronizada de representar o conhecimento sobre as diretrizes de segurança para a sua implementação na casa inteligente. A ontologia foi proposta seguindo uma investigação de diretrizes de segurança de várias fontes. Na sequência, visando automatizar o processo de agir sobre essas diretrizes para ajudar o usuário a executá-las, os autores apresentam a ontologia baseada em contexto para incorporar o contexto do usuário, fornecendo assim subsídio para a automação do gerenciamento de segurança e o envolvimento total do usuário para suportar uma modelagem incremental

das diretrizes de segurança.

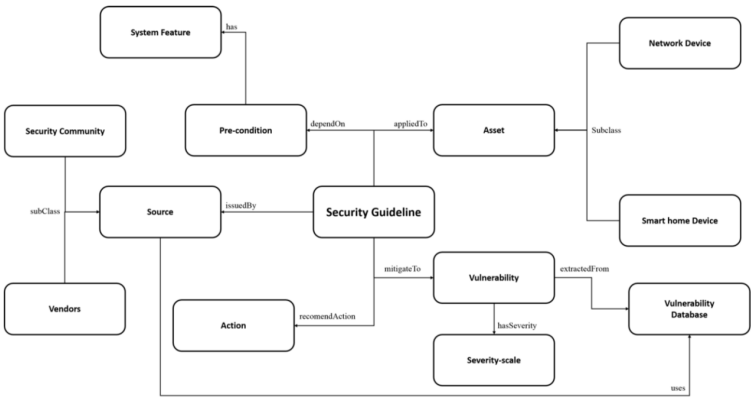

Figura 19. Modelo abstrato de diretrizes de segurança
Fonte: KHAN; NDUBUAKU, 2018

A diferença deste trabalho com relação à outras propostas ontológicas para segurança é evidenciada pela premissa de que a medida de controle é executada por um ator externo ao ativo, enquanto nos demais trabalhos esta ação é atribuída ao próprio ativo. As diretrizes de segurança para o usuário são classificadas em três diferentes níveis de envolvimento ao qual o usuário será submetido durante a execução: automático; semi-automático; e manual.

Ainda que seja prevista a execução automática e semiautomática de ações na ontologia, o trabalho não apresenta a integração da mesma em um *framework* para automação e análise em tempo de execução. Os autores ainda destacam a necessidade de implementar a automação proposta em um cenário real. Além disso, eles mencionam a possibilidade de integração da CSGO com ontologias existentes e banco de dados de segurança externos para aplicações mais abrangentes. No entanto, ao empregar ontologias, é necessário uma preocupação quanto a distribuição do *framework* a ser proposto visando possíveis limitações de escalabilidade.

7. Discussão dos Trabalhos Selecionados

As Tabelas 7 e 6 apresentam uma análise comparativa entre os projetos discutidos nesta seção. Visando otimizar o espaço ocupado pelas tabelas, os trabalhos foram identificados pelo sobrenome do primeiro autor e o respectivo ano de publicação.

A elaboração da Tabela 6 se deu por meio da pontuação resultante da análise de qualidade (AQ) da revisão sistemática que considerou os seguintes critérios e respectivas pontuações:

- C1 - os objetivos da pesquisa estão claramente definidos? (Sim - 1, Não - 0);
- C2 - a metodologia de avaliação é descrita em detalhes? (Sim - 1, Não - 0);
- C3 - existem informações que possibilitem a projeção da proposta em ambientes de produção da IoT? (Sim - 1, Não - 0);
- C4 - o artigo contempla detalhes que propiciam a replicação dos estudos? (pontuação de 1 à 3);

Tabela 6. Análise de Qualidade

	ABIE, 2012	EVESTI, 2014	RAMOS, 2015	AMAN, 2016	EL-MALIKI, 2016	MOZZA-QUATRO 2018	KHAN, 2018
C1	1	1	1	1	1	1	1
C2	0	1	0	1	1	1	1
C3	0	0	0	1	0	0	0
C4	1	2	1	3	2	2	1
C5	1	1	1	1	1	1	1
C6	1	3	2	3	2	2	1
AQ	4	8	5	10	7	7	5

- C5 - os resultados e contribuições estão claramente expostos? (Sim - 1, Não - 0);
- C6 - a arquitetura é descrita de maneira clara? (pontuação de 1 à 3).

Na sequência, a análise realizada na Tabela 7 visou identificar o suporte as seguintes características:

- R1 - suporte à heterogeneidade pelas propostas;
- R2 - a aderência ao ciclo de *feedback* MAPE-K;
- R3 - o provimento de estratégias para aplicação de adaptações no ambiente;
- R4 - a utilização de análise de risco como subsídio para tomada de decisão;
- R5 - a estratégia utilizada para escolha da adaptação entre diferentes opções;
- R6 - a área do estudo de caso;
- R7 - a escalabilidade do modelo ou *framework*;
- R8 - a possibilidade de distribuição da proposta;
- R9 - as fontes de informações contextuais consideradas.

Por meio da análise da tabela, bem como pela descrição dos trabalhos, percebe-se o suporte à heterogeneidade, ainda que contemplado por alguns trabalhos, apenas Aman (2016) apresenta detalhes suficientes que permitem replicar o estudo e identificar os pontos fortes e fracos da abordagem realizada, o que o destacou dos demais em sua pontuação na análise de qualidade. Neste sentido, existe uma lacuna nos *frameworks* para segurança adaptativa, especialmente na etapa de monitoramento do ciclo MAPE-K.

Reforçando esta afirmação, ao analisar o segundo requisito, aderência ao ciclo de *feedback*, ainda com exceção de Aman (2016), apesar da maioria dos trabalhos apresentarem em seu modelo as etapas MAPE, eles não fornecem especificações suficientes que permitam a replicação das avaliações ou ainda que possibilitem a prototipação fidedigna do modelo. É possível afirmar também que, em uma análise alto nível, visto até mesmo a profundidade da descrição dos modelos, eles se assemelham em grande parte. Além disso, a maior parte dos trabalhos se restringe a detalhar as ontologias propostas, as quais se referem exclusivamente à base de conhecimento do ciclo.

Quanto ao fornecimento de estratégias que permitam a adaptação do ambiente à IoT, seja de forma automática ou semiautomática, nenhum dos trabalhos contempla de maneira satisfatória esta propriedade. Ou seja, apesar dos trabalhos possuírem como objetivo o fornecimento de segurança adaptativa, parte deles suporta este requisito de forma

Tabela 7. Tabela comparativa

	ABIE, 2012	EVESTI, 2014	RAMOS, 2015	AMAN, 2016	EL-MALIKI, 2016	MOZZAQUATRO, 2018	KHAN, 2018
R1	Não	Limitada	Sim	Sim	Não	Sim	-
R2	MAPE	MAPE-K	-	MAPE-K	MAPE	MAPE-**K**	K
R3	Não	Não	Não	Limitada	Limitada	Limitada	Prevista
R4	Não	Não	Não	Fórmula	-	Não	Não
R5	-	Conjuntos Fuzzy	-	Ontologia	-	Ontologia	Ontologia
R6	eHealth	Ambientes Inteligentes	Não	eHealth	Redes de Sensores sem Fio	Indústria Metalúrgica	Não
R7	Não	Não	-	Não	Não	-	-
R8	Não	Não	-	Sim	Não	-	-
R9	Usuário, QoS e Segurança	Segurança	Segurança	Usuário, QoS e Segurança	Usuário, QoS e Segurança	Segurança	Segurança

limitada, por meio de *scripts* personalizados como em Aman (2016) ou de códigos desenvolvidos especificamente para a avaliação EL-MALIKI; SEIGNE (2016); MOZZAQUATRO et al. (2018).

A análise de risco, a qual deve nortear as adaptações a serem realizadas, também é fornecida apenas em Aman (2016). Ainda assim, a mesma não contempla informações contextuais externas, restringindo-se apenas ao cálculo do risco com base nos eventos analisados e nas regras especificadas.

No que diz respeito a estratégia utilizada para decisão das diferentes opções de adaptação, a maior parte dos trabalhos tem empregado ontologias (regras ontológicas), a qual já é utilizada como base de conhecimento. Contudo, percebe-se que um dos principais benefícios teóricos do uso de ontologias, o reuso, não tem sido efetivamente explorado e na prática tem se tornado um problema na área CALDAROLA; RINALDI (2016); MOZZAQUATRO et al. (2018). A adoção de ontologias também implica em limitações de desempenho, o que pode inviabilizar a utilização das propostas em cenários da IoT.

De forma geral, percebe-se que não há um cenário específico para avaliação dos modelos, sendo geralmente utilizados os que mais se aproximam com a experiência dos grupos de pesquisa e parcerias dos mesmos em diferentes projetos.

Com relação às propostas, observa-se a necessidade de contemplarem a distribuição e a escalabilidade dos *frameworks*, possibilitando sua aplicação em cenários de crescente volume de dados, como na IoT. Finalmente, há a necessidade de propostas que propiciem a resolução de conflitos em diferentes requisitos, sejam eles de segurança, dos usuários, entre outros.

A tabela 7 e a discussão apresentada forneceu subsídio para responder de forma

objetiva as questões estabelecidas nesta revisão:

- "(Q1) Quais os atuais desafios de segurança adaptativa em IoT?" - considerando o escopo deste estudo, é possível afirmar que alguns dos desafios estão relacionados às limitações das propostas discutidas ao analisar a tabela 7, como por exemplo: o suporte à heterogeneidade, em especial na etapa de monitoramento do MAPE-K, o que contempla a aquisição de informações contextuais de fontes distintas; a aderência ao ciclo de *feedback* MAPE-K, visto que nem todos fornecem informações sobre a concepção de cada etapa; a possibilidade de replicação dos estudos, uma vez que os autores não disponibilizam seus protótipos, muito menos exploram tecnologias para facilitar esta tarefa; adoção de estratégias flexíveis que promovam a adaptação do ambiente da IoT; emprego de análise de riscos para direcionar as adaptações necessárias;
- "(Q2) Quais as estratégias utilizadas para avaliação das propostas?" - percebe-se que, em geral são utilizados estudos de caso em diferentes áreas da IoT;
- "(Q3) Quais as informações contextuais utilizadas para adaptações?" - além de considerar os requisitos de segurança, alguns estudos exploraram o uso de informações de QoS em conjunto com as preferências dos usuários, no entanto, o impacto do uso destas informações necessita de uma análise aprofundada, indicando esta como uma questão ainda em aberto para novas pesquisas;
- "(Q4) Quais os mecanismos para escolha da adaptação considerando diferentes contextos?" - alguns trabalhos apresentam o uso de ontologias, porém, este também permanece um tópico a ser estudado explorando novos algoritmos.

8. Considerações Finais

O presente capítulo buscou apresentar uma revisão sistemática sobre segurança adaptativa ciente de contexto para IoT. Através da metodologia aplicada foi possível perceber que atualmente existem várias abordagens para segurança adaptativa. No entanto, muitas propostas atualmente desenvolvidas se concentram em objetivos de segurança específicos FERRERA et al. (2016); VILLARREAL-VASQUEZ; BHARGAVA; ANGIN (2017); LE; MAPLE; WATSON (2018). Percebe-se também a falta no tratamento completo do ciclo de *feedback*, ou seja, as abordagens não definem todo o ciclo MAPE-K. No que diz respeito a aquisição de informações contextuais, não foi identificado um trabalho que caracterize uma contextualização oportuna para IoT, explorando os diferentes requisitos e desafios nessa infraestrutura distribuída. Além disso, as arquiteturas genéricas analisadas não detalham os métodos usados em cada componente, o que dificulta a reutilização e extensibilidade das abordagens propostas. Com a revisão sistemática realizada, foi possível identificar que apesar dos avanços nas pesquisas em segurança adaptativa em diferentes frentes, os desafios mencionados continuam em aberto, existindo ainda poucos modelos genéricos que detalhem a sua concepção, prototipação e estratégias de avaliação.

Referências

ABIE, H.; BALASINGHAM, I. Risk-based Adaptive Security for Smart IoT in eHealth. In: INTERNATIONAL CONFERENCE ON BODY AREA NETWORKS, 7., 2012, ICST, Brussels, Belgium, Belgium. **Proceedings...** ICST (Institute for Computer Sciences: Social-Informatics and Telecommunications Engineering), 2012. p.269–275. (BodyNets '12).

ABIE, H. et al. Self-Healing and Secure Adaptive Messaging Middleware for Business Critical Systems. **International Journal on Advances in Security**, [S.l.], v.3, 2010.

ALIENVAULT. OSSIM: The Open Source SIEM — AlienVault. Disponível em: ⟨https://www.alienvault.com/products/ossim⟩, acesso em: 11 feb 2018.

AMAN, W. **Adaptive Security in the Internet of Things**. 2016. Tese (Doutorado em Ciência da Computação) — Norwegian University of Science and Technology, Trondheim, Norway.

AMAN, W.; SNEKKENES, E. Event driven adaptive security in internet of things. **UBICOMM 2014 - 8th International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies**, [S.l.], p.7–15, 2014. cited By 6.

BELLAVISTA, P.; CORRADI, A.; FANELLI, M.; FOSCHINI, L. A survey of context data distribution for mobile ubiquitous systems. **ACM Comput. Surv.**, New York, NY, USA, v.44, n.4, p.24:1–24:45, Sept. 2012.

BERNABE, J. B.; HERNÁNDEZ, J. L.; MORENO, M. V.; GOMEZ, A. F. S. Privacy-Preserving Security Framework for a Social-Aware Internet of Things. In: UBIQUITOUS COMPUTING AND AMBIENT INTELLIGENCE. PERSONALISATION AND USER ADAPTED SERVICES, 2014, Cham. **Anais...** Springer International Publishing, 2014. p.408–415.

CALDAROLA, E. G.; RINALDI, A. M. An Approach to Ontology Integration for Ontology Reuse. In: IEEE 17TH INTERNATIONAL CONFERENCE ON INFORMATION REUSE AND INTEGRATION (IRI), 2016., 2016. **Anais...** [S.l.: s.n.], 2016. p.384–393.

DEY, A. K. Understanding and Using Context. **Personal and Ubiquitous Computing**, [S.l.], v.5, p.4–7, 2001.

DIKICI, A.; TURETKEN, O.; DEMIRORS, O. Factors influencing the understandability of process models: A systematic literature review. **Information and Software Technology**, ELSEVIER, v.93, p.112 – 129, 2018.

EL MALIKI, T. **Security adaptation in highly dynamic wireless networks**. 2014. Tese (Doutorado em Ciência da Computação) — Université de Genève.

EL-MALIKI, T.; SEIGNE, J. M. Efficient Security Adaptation Framework for Internet of Things. In: INTERNATIONAL CONFERENCE ON COMPUTATIONAL SCIENCE AND COMPUTATIONAL INTELLIGENCE (CSCI), 2016., 2016. **Anais...** [S.l.: s.n.], 2016. p.206–211.

EVESTI, A. **Adaptive Security in Smart Spaces**. 2014. Tese (Doutorado em Ciência da Computação) — University of Oulu.

EVESTI, A.; SUOMALAINEN, J.; OVASKA, E. Architecture and Knowledge-Driven Self-Adaptive Security in Smart Space. **Computers**, [S.l.], v.2, n.1, p.34–66, 2013.

FERRERA, E. et al. Adaptive security framework for resource-constrained internet-of-things platforms. **2016 8th IFIP International Conference on New Technologies, Mobility and Security, NTMS 2016**, [S.l.], 2016. cited By 0.

FINK, A. **Conducting Research Literature Reviews**: From the Internet to Paper. [S.l.]: SAGE Publications, 2010.

GIUSTO, D.; IERA, A.; MORABITO, G.; ATZORI, L. **The Internet of Things**: 20th Tyrrhenian Workshop on Digital Communications. [S.l.]: Springer New York, 2010.

HEEAGER, L. T.; NIELSEN, P. A. A conceptual model of agile software development in a safety-critical context: A systematic literature review. **Information and Software Technology**, ELSEVIER, 2018.

HOSSEINZADEH, S. et al. Diversification and obfuscation techniques for software security: A systematic literature review. **Information and Software Technology**, ELSEVIER, 2018.

IGLESIA, D. G. D. L.; WEYNS, D. MAPE-K Formal Templates to Rigorously Design Behaviors for Self-Adaptive Systems. **ACM Trans. Auton. Adapt. Syst.**, New York, NY, USA, v.10, n.3, p.15:1–15:31, Sept. 2015.

KHAN, Y.; NDUBUAKU, M. Ontology-based automation of security guidelines for smart homes. **IEEE World Forum on Internet of Things, WF-IoT 2018 - Proceedings**, [S.l.], v.2018-January, p.35–40, 2018. cited By 0.

KLIARSKY, A.; LEUNE, K. Detecting Attacks Against The Internet of Things. **SANS Institute. InfoSec Reading Room**, [S.l.], 2017.

LE, A.; MAPLE, C.; WATSON, T. A profile-driven dynamic risk assessment framework for connected and autonomous vehicles. **IET Conference Publications**, [S.l.], v.2018, n.CP740, 2018. cited By 0.

LOVINS, J. B. Development of a stemming algorithm. **Mechanical Translation and Computational Linguistics**, [S.l.], v.11, p.22–31, 1968.

MIORANDI, D.; SICARI, S.; PELLEGRINI, F. D.; CHLAMTAC, I. Internet of things: Vision, applications and research challenges. **Ad Hoc Networks**, [S.l.], v.10, n.7, p.1497 – 1516, 2012.

MOZZAQUATRO, B. A. et al. An Ontology-Based Cybersecurity Framework for the Internet of Things. **Sensors**, [S.l.], v.18, n.9, 2018.

MOZZAQUATRO, B. A.; JARDIM-GONCALVES, R.; AGOSTINHO, C. Towards a reference ontology for security in the Internet of Things. In: IEEE INTERNATIONAL WORKSHOP ON MEASUREMENTS NETWORKING (M N), 2015., 2015. **Anais...** [S.l.: s.n.], 2015. p.1–6.

MOZZAQUATRO, B. A.; MELO, R.; AGOSTINHO, C.; JARDIM-GONCALVES, R. An ontology-based security framework for decision-making in industrial systems. In: INTERNATIONAL CONFERENCE ON MODEL-DRIVEN ENGINEERING AND SOFTWARE DEVELOPMENT (MODELSWARD), 2016., 2016. **Anais...** [S.l.: s.n.], 2016. p.779–788.

MOZZAQUATRO, B.; AGOSTINHO, C.; MELO, R.; JARDIM-GONCALVES, R. A model-driven adaptive approach for IoT security. **Communications in Computer and Information Science**, [S.l.], v.692, p.194–215, 2017.

OCG. Open Geospatial Consortium. Sensor Model Language (SensorML). Disponível em: ⟨http://www.opengeospatial.org/standards/sensorml⟩, acesso em: 12 feb 2018.

O.M.A. **NGSI Context Management**. [S.l.]: Open Mobile Alliance, 2012.

PERERA, C.; ZASLAVSKY, A.; CHRISTEN, P.; GEORGAKOPOULOS, D. Context Aware Computing for The Internet of Things: A Survey. **IEEE Communications Surveys Tutorials**, [S.l.], v.16, n.1, p.414–454, First 2014.

RAMOS, J. L. H.; BERNABE, J. B.; SKARMETA, A. F. Managing Context Information for Adaptive Security in IoT Environments. In: AINA WORKSHOPS, 2015. **Anais...** IEEE Computer Society, 2015. p.676–681.

ROCHFORD, O.; KAVANAGH, K. M. **Magic Quadrant for Security Information and Event Management**. [S.l.]: Gartner Group, 2015.

ROUSE, M. What is wildcard character?. Disponível em: ⟨https://whatis.techtarget.com/definition/wildcard-character⟩, acesso em: 28 abr 2020.

SHANKAR, V. Clash of the titans - Arcsight vs QRadar. Disponível em: ⟨http://infosecnirvana.com/clash-titans-arcsight-vs-qradar/⟩, acesso em: 04 fev 2018.

SICARI, S.; RIZZARDI, A.; GRIECO, L.; COEN-PORISINI, A. Security, privacy and trust in Internet of Things: The road ahead. **Computer Networks**, [S.l.], v.76, p.146 – 164, 2015.

VILLARREAL-VASQUEZ, M.; BHARGAVA, B.; ANGIN, P. Adaptable Safety and Security in V2X Systems. In: IEEE INTERNATIONAL CONGRESS ON INTERNET OF THINGS (ICIOT), 2017., 2017. **Anais...** [S.l.: s.n.], 2017. p.17–24.