

UNIVERSIDADE FEDERAL DE PELOTAS
Centro de Desenvolvimento Tecnológico
Programa de Pós-Graduação em Computação



Tese

**Uma Proposta para Contextualização de Eventos em Segurança Adaptativa na
Internet das Coisas**

Ricardo Borges Almeida

Pelotas, 2021

Ricardo Borges Almeida

**Uma Proposta para Contextualização de Eventos em Segurança Adaptativa na
Internet das Coisas**

Tese apresentada ao Programa de Pós-Graduação em Computação do Centro de Desenvolvimento Tecnológico da Universidade Federal de Pelotas, como requisito parcial à obtenção do título de Doutor em Ciência da Computação.

Orientadora: Prof^a. Dr^a. Ana Marilza Pernas
Coorientador: Prof. Dr. Adenauer Corrêa Yamin

Pelotas, 2021

**Insira AQUI a ficha catalográfica
(solicite em <http://sisbi.ufpel.edu.br/?p=reqFicha>)**

Ricardo Borges Almeida

**Uma Proposta para Contextualização de Eventos em Segurança Adaptativa na
Internet das Coisas**

Tese aprovada, como requisito parcial, para obtenção do grau de Doutor em Ciência da Computação, Programa de Pós-Graduação em Computação, Centro de Desenvolvimento Tecnológico, Universidade Federal de Pelotas.

Data da Defesa: 30 de fevereiro de 2019

Banca Examinadora:

Prof^a. Dr^a. Ana Marilza Pernas (orientadora)

Doutora em Computação pela Universidade Federal do Rio Grande do Sul.

Prof. Dr. Adenauer Corrêa Yamin (coorientador)

Doutor em Computação pela Universidade Federal do Rio Grande do Sul.

Prof^a. Dr^a. Renata Hax Sander Reiser

Doutora em Computação pela Universidade Federal do Rio Grande do Sul.

Prof. Dr. Mario Antonio Ribeiro Dantas

Doutor em Computação pela University of Southampton.

Prof. Dr. Claudio Fernando Resin Geyer

Doutor em Informática pela Université Joseph Fourier.

RESUMO

ALMEIDA, Ricardo Borges. **Uma Proposta para Contextualização de Eventos em Segurança Adaptativa na Internet das Coisas.** Orientadora: Ana Marilza Pernas. 2021. 113 f. Tese (Doutorado em Ciência da Computação) – Centro de Desenvolvimento Tecnológico, Universidade Federal de Pelotas, Pelotas, 2021.

A Internet das Coisas (IoT) é uma materialização da Computação Ubíqua que vem ganhando cada vez mais destaque. Ela consiste de um ecossistema que combina redes de sensores sem fio, computação em nuvem, dados analíticos, tecnologias interativas, bem como dispositivos inteligentes. A IoT atualmente inclui uma gama diversificada de dispositivos, serviços e redes para se tornar uma internet de qualquer coisa, em qualquer lugar, de qualquer forma e a qualquer momento. Com isso, os desafios de segurança e privacidade se potencializam enquanto características necessárias e viabilizadoras para IoT. Promover a segurança sobre este ambiente dinâmico e heterogêneo com mecanismos de segurança pré-definidos e estáticos é uma tarefa que vem se mostrando inviável. Desta forma, são necessárias soluções de segurança adaptativa. Tendo isto em vista, os objetivos deste trabalho consistem em: (i) sistematizar e apresentar os conceitos sobre segurança adaptativa para IoT, incluindo a sua relação com os estudos em ciência de contexto; (ii) realizar um mapeamento sistemático da literatura buscando identificar o estado da arte em segurança adaptativa para IoT; (iii) desenvolver uma análise crítica sobre os trabalhos identificados em um esforço para elencar as lacunas existentes nesta área; e (iv) apresentar a concepção de uma proposta para segurança adaptativa considerando os desafios dos cenários da IoT, tendo como diferencial a aquisição de informações contextuais no momento oportuno e contemplando fontes heterogêneas.

Palavras-chave: Internet das Coisas. Segurança Adaptativa. Ciência de Contexto.

ABSTRACT

ALMEIDA, Ricardo Borges. **Titulo do Trabalho em Inglês.** Advisor: Ana Marilza Per-
nas. 2021. 113 f. Thesis (Doctorate in Computer Science) – Technology Development
Center, Federal University of Pelotas, Pelotas, 2021.

Proposal for Contextualization of Events in Adaptive Security considering the Internet of Things The Internet of Things (IoT) is a Ubiquitous Computing materialization that is gaining more and more prominence. It consists of an ecosystem that combines wireless sensor networks, cloud computing, analytical data, interactive technologies as well as intelligent devices. IoT currently includes a diverse range of devices, services and networks to become an internet of anything, anywhere, any way and anytime. As a result, the security and privacy challenges have become potentialized as a necessary and viable feature for IoT. Promoting security over this dynamic and heterogeneous environment with pre-defined and static security mechanisms is a unfeasible task. Therefore, solutions for adaptive security are required. The objectives of this work are: (i) systematize and present the concepts of adaptive security for IoT, including its relation with studies in context awareness; (ii) perform a systematic mapping of the literature striving to identify the state of the art in adaptive security for IoT; (iii) develop a critical analysis of the work identified in an effort to fill the gaps in this area; and (iv) present the conception of a proposal for adaptive security considering the challenges of IoT scenarios, offering as differential the contextual information acquisition in the opportune moment and contemplating heterogeneous sources. For the purpose of evaluating this proposal, two case studies were developed to validate the progressive contextualization of security events. Finally, the strengths and limitations of our approach are discussed, then followed by future works.

Keywords: Internet of Things. Adaptive Security. Context Awareness.

LISTA DE FIGURAS

1	Ciclo de <i>feedback</i> genérico	26
2	MAPE-K - Modelo para sistema adaptativos	28
3	String de pesquisa usada na revisão sistemática	33
4	Número de artigos publicados por ano em cada base considerada	34
5	Modelo proposto para gerenciamento de segurança adaptativa	40
6	Estudo de caso baseado em monitoramento de paciente	42
7	Estrutura da arquitetura de adaptação	43
8	Partes genéricas e específicas da implementação do monitoramento do nível de segurança	44
9	Dependências entre ontologias de segurança e de contexto	45
10	Framework de segurança ciente de contexto para IoT	46
11	Visão geral do Gerenciador de Contexto	47
12	Interações do <i>framework</i> para mecanismos de segurança adaptativa cientes de contexto	49
13	EDAS - modelo de referência	51
14	EDAS - ontologia para segurança adaptativa	53
15	EDAS - processo de segurança adaptativa	54
16	SARM - descrição do sistema autônomo	56
17	SARM - fundamentos do <i>framework</i> genérico para segurança adaptativa	57
18	Uma arquitetura para <i>framework</i> de segurança adaptativa baseada em ontologia integrada com a plataforma C2NET.	58
19	Ontologia de referência para segurança na IoT (65)	59
20	Modelo abstrato de diretrizes de segurança (51)	60
21	Componente projetado para o EXEHDA-SA Collector	67
22	Componente projetado para o EXEHDA-SA SmartLogger	68
23	Componentes do EXEHDA-SA mapeados sobre o ambiente ubíquo	68
24	Componente projetado para o EXEHDA-SA Manager	69
25	Adaptação Concebida do Ciclo de <i>feedback</i> MAPE-K com Enriquecimento Baseado em Contexto	70
26	Adaptação Concebida do Modelo de Endsley de Ciência de Situação com Enriquecimento Baseado em Contexto	72
27	Mapeamento do modelo MAPE-K proposto sob o EXEHDA-SA	72
28	Visão geral dos módulos do modelo arquitetural para segurança adaptativa ciente de contexto	73

29	Organização das tecnologias mapeadas para a abordagem modular do AS-ProCBE	85
30	Visão geral do ambiente de avaliação	87
31	Abstração da implantação do AS-ProCBE com perfil de Collector . .	89
32	Abstração da implantação do AS-ProCBE com perfil de SmartLogger	91
33	Evento após a contextualização por DNS, ASN e geolocalização . . .	92
34	Evento do NIDS após a contextualização por IOC	93
35	Regra de correlação e contextualização para evento com IOC . . .	93

LISTA DE TABELAS

1	Aplicação da string de busca nas bases acadêmicas	36
2	Número de artigos por critério	36
3	Artigos selecionados após a revisão sistemática	37
4	Artigos avaliados em profundidade após seleção inicial	38
5	Alinhamento da ISO/IEC 27005 ISMS, ISRM e ARM	39
6	Análise de Qualidade	62
7	Tabela comparativa	63
8	Tabela comparativa com o PROCEN-AS	83
9	Cronograma de atividades	99

LISTA DE ABREVIATURAS E SIGLAS

ARM *Adaptive Risk Management*

C2NET *Cloud Collaborative Manufacturing Networks*

CEP *Complex Event Processing*

CERP-IoT *Cluster of European Research Projects on the Internet of Thing*

CSGO *Cyber Security Guidelines Ontology*

EDAS *Event Driven Adaptive Security*

EXEHDA *Execution Environment for Highly Distributed Applications*

HP *Hewlett-Packard*

IBM *International Business Machines*

IDS *Intrusion Detection System*

IoT *Internet das Coisas*

IP *Internet Protocol*

IBM *International Business Machines*

ISMS *Information Security Management System*

ISRM *Information Security Risk Management*

LUPS *Laboratory of Ubiquitous and Parallel Systems*

MAPE-K *Monitor-Analyze-Plan-Execute plus Knowledge*

OSSIM *Open Source Security Information Management*

OWASP *Open Web Application Security Project*

PDCA *Plan-Do-Check-Act*

QoS *Quality of Service*

RBAC *Role-Based Access Control*

RFID *Radio Frequency Identification*

SARM *Security Adaptation Reference Monitor*

SNMP *Simple Network Management Protocol*

SMS *Short Message Service*

SQuaRE *Software product Quality Requirements and Evaluation*

UbiComp *Ubiquitous Computing*

UFPel Universidade Federal de Pelotas

XML *eXtensible Markup Language*

WAF *Web Application Firewall*

SUMÁRIO

1 INTRODUÇÃO	14
1.1 Motivações	16
1.2 Questões e Hipótese de Pesquisa	17
1.3 Objetivos	17
1.4 Estrutura do Texto	18
2 SEGURANÇA ADAPTATIVA PARA A INTERNET DAS COISAS	19
2.1 Internet das Coisas	19
2.2 Eventos para Segurança da Informação	21
2.3 Segurança Adaptativa	24
2.4 Ciência de Contexto na Segurança Adaptativa	29
2.5 Considerações sobre o Capítulo	31
3 ESTADO DA ARTE	32
3.1 Revisão Sistemática da Literatura	32
3.2 Trabalhos Selecionados	38
3.2.1 Risk-based Adaptive Security for Smart IoT in eHealth	38
3.2.2 Adaptive Security in Smart Spaces	42
3.2.3 Managing Context Information for Adaptive Security in IoT Environments	45
3.2.4 Adaptive Security in the Internet of Things	49
3.2.5 Efficient Security Adaptation Framework for Internet of Things	54
3.2.6 An Ontology-based Cybersecurity Framework for the Internet of Things	57
3.2.7 Ontology-based Automation of Security Guidelines for Smart Homes	60
3.3 Discussão dos Trabalhos Selecionados	61
3.4 Considerações sobre o Capítulo	64
4 AS-PROCBE: SEGURANÇA ADAPTATIVA BASEADA EM ENRIQUECIMENTO PROGRESSIVO DE CONTEXTO	66
4.1 Escopo do Trabalho: EXEHDA-SA	66
4.2 Proposta Concebida	69
4.2.1 Enriquecimento Baseado em Contexto	74
4.2.2 Percepção	76
4.2.3 Compreensão	77
4.2.4 Projeção	78
4.2.5 Tomada de Decisão	79
4.2.6 Execução de Ações	80
4.2.7 Comunicação	81
4.2.8 Repositório Híbrido de Informações Contextuais	82

4.3 Considerações sobre o Capítulo	82
5 MÉTODO DE AVALIAÇÃO	84
5.1 Objetivos da Avaliação	84
5.2 Tecnologias Utilizadas	84
5.3 Descrição do Ambiente de Avaliação	86
5.4 Cenários	86
5.4.1 Ataque de Injeção de Comandos	87
5.4.2 <i>Download</i> de Arquivo Suspeito	89
5.5 Considerações sobre o Capítulo	94
6 CONSIDERAÇÕES FINAIS	95
6.1 Contribuições	95
6.1.1 Com Relação ao Estado da Arte	96
6.1.2 Com Relação à Divulgação de Resultados Parciais	96
6.2 Cronograma de Atividades	98
REFERÊNCIAS	100
APÊNDICE A UM APÊNDICE	110
ANEXO A UM ANEXO	112
ANEXO B OUTRO ANEXO	113

1 INTRODUÇÃO

Com os avanços significativos das diversas tecnologias que permeiam as redes de computadores, especialmente aqueles proporcionados pelas pesquisas em torno da Computação Ubíqua (UbiComp), houve uma transformação na forma com que se busca, acessa e compartilha informações, tornando o ambiente mais interativo, adaptável e informativo (86). Uma materialização da UbiComp que vem ganhando destaque é a Internet das Coisas, do inglês *Internet of Things* (IoT), a qual consiste de um ecossistema que combina redes de sensores sem fio, computação em nuvem, dados analíticos, tecnologias interativas, bem como dispositivos inteligentes. Seu objetivo é prover soluções nas quais os objetos sejam primordialmente concebidos de forma a usufruir da conectividade da rede para coleta e troca de dados por meio de um identificador que busca melhorar as interações objeto-a-objeto.

O termo IoT foi cunhado em 1999 no *Massachusetts Institute of Technology* pelo analista britânico Kevin Ashton, sendo inicialmente proposto para conectar coisas específicas através da Internet usando dispositivos, como *Radio Frequency Identification* (RFID), para realizar a identificação e o gerenciamento inteligente de produtos (12). Desde então, esta visão foi expandida, contemplando características da UbiComp concebidas por Mark Weiser (1991), incluindo uma gama diversificada de dispositivos, serviços e redes para se tornar uma internet de qualquer coisa, em qualquer lugar, de qualquer forma e a qualquer momento.

As demandas deste mercado inspiraram novas tecnologias e protocolos, no entanto, na tentativa de manterem-se inovadores e 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. Com isso, os desafios de segurança e privacidade se potencializaram enquanto características necessárias e viabilizadoras para IoT, ou seja, o desenvolvimento da IoT é fortemente dependente do atendimento às preocupações de segurança (83; 52).

As ameaças e vulnerabilidades associadas à IoT são proporcionais às superfícies de ataque (52). Esses dispositivos sofrem ataques contra interfaces físicas, comunicação sem fio, protocolos de roteamento e ataques tradicionais vistos em redes

Internet Protocol (IP). Estudos realizados pela *Open Web Application Security Project* (OWASP) e pela *Hewlett-Packard* (HP) detalham uma série de vulnerabilidades que a IoT precisa abordar. Em relatório, as empresas destacam que: 60% das interfaces web disponíveis em dispositivos da IoT são propensas a ataques; 90% desses dispositivos coletam pelo menos uma informação pessoal; 70% se comunicam através de canais não criptografados; e 70% são suscetíveis a ataques de enumeração de contas (47; 71). Estas são algumas das preocupações graves especialmente para os serviços de saúde apoiados na IoT, onde o tipo de informação tratado é principalmente pessoal.

As principais tecnologias promotoras da IoT são consideradas objetos sensoriais que possuem limitações de processamento, memória e armazenamento, além de preocupações com o consumo de energia. Desta forma, as soluções de segurança atuais, como *firewall*, *Intrusion Detection System* (IDS), *Web Application Firewall* (WAF), até mesmo pequenos programas de antivírus, não são viáveis para essa rede de dispositivos de recursos reduzidos. Além disso, um incidente de segurança geralmente consiste em múltiplos vetores de ataque, com diferentes alvos visando explorar qualquer vulnerabilidade existente. Logo, essas soluções que se limitam a analisar informações contextuais específicas, por exemplo, informações do tráfego da rede ou de arquivos locais, não fornecem um contexto holístico para análise de risco, podendo produzir falsos positivos e negativos, resultando em decisões inadequadas de mitigação (11).

Promover a segurança sobre este ambiente dinâmico e heterogêneo com mecanismos de segurança pré-definidos e estáticos é uma tarefa muitas vezes inviável. Por isso, são necessárias soluções para segurança adaptativa, as quais utilizam um processo apoiado por um ciclo de *feedback* que permite que os sistemas tomem decisões de adaptação com mínima intervenção humana (53). A segurança adaptativa visa selecionar mecanismos de segurança e seus parâmetros em tempo de execução para preservar o nível de segurança requerido em um ambiente em mudança (38).

Em um âmbito geral, a adaptação, ou comportamento autônomo, é um problema importante para a IoT (9; 4; 72). Ela está relacionada à capacidade de dispositivos e aplicações em adaptarem seu comportamento como resposta às mudanças em seu ambiente de operação.

Com isso, a ciência de contexto torna-se um conceito chave para fornecer segurança adaptativa, ou seja, o sistema deve avaliar as diferentes informações contextuais provenientes das ameaças e vulnerabilidades percebidas no cenário para a situação corrente, selecionar as melhores contramedidas para minimizar o risco, e promover a adaptação do ambiente de acordo com as mudanças de contexto durante sua execução. Além disso, as aplicações cientes de contexto devem ser capazes de adaptar seus comportamentos ao ambiente em mudança com um mínimo de intervenção humana.

A construção de aplicações cientes de contexto apresenta uma série de etapas: aquisição de informações contextuais a partir de fontes heterogêneas e distribuídas; o processamento dessas informações na busca por situações de interesse; a respectiva atuação; e o armazenamento e a busca de informações para disseminação aos usuários (15). Esta pesquisa visa especialmente explorar a ciência de contexto no processamento de eventos promovendo a adaptação dos mecanismos de segurança em cenários de ambientes da IoT.

1.1 Motivações

O desenvolvimento desta pesquisa foi inicialmente motivado por questões gerais previamente descritas na seção anterior. Isto inclui o crescimento decorrente da IoT em tamanho, complexidade e distribuição das infraestruturas computacionais, o que implica que requisitos de desempenho, escalabilidade e flexibilidade sejam satisfeitos na concepção de uma arquitetura para segurança adaptativa (70; 57; 42; 48). Aspectos de suporte à heterogeneidade, dinamicidade e invisibilidade da comunicação nos ambientes da IoT também influenciaram este estudo.

Este panorama geral encaminhou o desenvolvimento de uma revisão sistemática para identificação das principais lacunas existentes no estado da arte em segurança adaptativa para IoT, avaliando também a sustentabilidade das abordagens existentes. Após a realização da revisão sistemática de literatura, as principais motivações para a concepção desta proposta incluem:

- muitas das abordagens propostas para segurança adaptativa foram concebidas para serem aplicadas em um único e específico campo de aplicação, o que se alinha com o observado em Yuan; Malek (2012), onde os autores destacam que, em termos arquiteturais, os trabalhos existentes possuem lacunas a serem consideradas;
- falta de propostas que definam todo o ciclo de *feedback*, especialmente apresentando informações que evidenciem o tratamento da heterogeneidade para o monitoramento contínuo do ambiente, contemplando desde a aquisição de informações contextuais em diferentes momentos, até a atuação no ambiente;
- a maioria dos projetos identificados não apresenta detalhes suficientes sobre a prototipação e a validação da proposta, inviabilizando a replicação dos cenários e a continuação da pesquisa por outros pesquisadores;
- falta de propostas que incluam a utilização de informações contextuais provenientes de plataformas para inteligência de ameaças, discutindo suas implicações, como por exemplo, as limitações quanto ao número de requisições;

- a correta utilização do volume de dados de contexto originados nestes cenários pode introduzir novas possibilidades para muitas aplicações, no entanto, caso a contextualização seja empregada de forma incorreta, ela pode ocasionar ou agravar diferentes problemas como o excesso de dados a serem analisados (56). Este desafio já tem impactado algumas organizações que citam a falta de visibilidade sobre os eventos de segurança como um dos principais impedimentos para uma eficaz resposta a incidentes (85).

1.2 Questões e Hipótese de Pesquisa

Considerando as motivações apresentadas, três questões foram elaboradas para encaminhar o esforço de pesquisa desenvolvido. Os escopos destas questões se interconectam, oferecendo um direcionamento com várias oportunidades sinérgicas de avanço.

- QP1: quais devem ser os componentes e sua organização, considerando um modelo arquitetural para contextualização de eventos em segurança adaptativa na IoT?
- QP2: quais características funcionais e não funcionais devem ser oferecidas por este modelo?
- QP3: quais estratégias devem ser empregadas no que diz respeito especificamente à etapa de contextualização dos eventos para lidar com o elevado volume de dados?

A hipótese defendida nesta proposta de tese consiste na convicção de que é possível explorar a ciência de contexto para prover segurança adaptativa empregando um modelo arquitetural que ofereça contextualização de eventos de forma distribuída, escalável e no momento oportuno.

1.3 Objetivos

O objetivo central deste trabalho é a concepção de um modelo arquitetural para segurança adaptativa na IoT, especificamente tratando o desafio de contextualização de eventos. Dentre os recursos a serem oferecidos pelo componente de contextualização do modelo, destacam-se: (i) suporte às etapas de um ciclo de *feedback* com suporte à heterogeneidade da IoT; (ii) flexibilidade no intuito de atender às demandas de diferentes cenários em segurança adaptativa que necessitem de ciência de contexto; (iii) capacidade de coleta de informações contextuais a partir de diferentes fontes; (iv) distribuição da contextualização em diferentes etapas; e finalmente, (v) um protótipo que possibilite a replicação dos estudos e a continuidade da pesquisa.

Com o intuito de atender o objetivo geral previsto, as seguintes metas devem ser contempladas:

- sistematização e apresentação dos conceitos sobre segurança adaptativa para IoT, incluindo a sua relação com os estudos em ciência de contexto;
- realização de uma revisão sistemática da literatura buscando identificar o estado da arte em segurança adaptativa para IoT que conte com desafios relacionados à ciência de contexto;
- concepção de uma proposta para suporte à ciência de contexto em segurança adaptativa para ambientes computacionais da IoT;
- especificação de componentes e funcionalidades a serem provados pelo modelo arquitetural proposto;
- instanciar a proposta no âmbito do grupo de pesquisa onde ela está sendo concebida, o *Laboratory of Ubiquitous and Parallel Systems* (LUPS) da Universidade Federal de Pelotas (UFPel), particularmente relacionando a proposta com o *middleware Execution Environment for Highly Distributed Applications* (EXEHDA).

1.4 Estrutura do Texto

Este trabalho foi organizado em 5 capítulos. Neste primeiro capítulo foi apresentada uma breve introdução ao tema do trabalho, suas motivações, a hipótese de pesquisa e os objetivos. Na sequência, são discutidos os conceitos em torno da segurança adaptativa ciente de contexto para IoT. O capítulo 3 apresenta a revisão sistemática realizada para identificação do estado da arte. No capítulo 4 é apresentada a proposta concebida, sendo discutidas suas principais características, seu modelo arquitetural e funcionalidades projetadas para contextualização dos eventos. Por fim, no capítulo 6 são apresentadas as considerações finais, bem como as atividades a serem desenvolvidas na continuidade desta pesquisa.

2 SEGURANÇA ADAPTATIVA PARA A INTERNET DAS COISAS

Para fornecer uma visão coerente sobre os temas tratados no trabalho, primeiramente são abordados neste capítulo conceitos de IoT, incluindo suas características e desafios para segurança. Na sequência, são discutidos os conceitos sobre eventos para segurança da informação. Posteriormente é apresentada a base conceitual em torno da segurança adaptativa. Finalmente, discute-se aspectos sobre a ciência de contexto, apresentando um exemplo de como ela pode ser aplicada para o provimento da segurança adaptativa.

2.1 Internet das Coisas

A Internet das Coisas, também chamada de IoT (proveniente do termo em inglês *Internet of Things*), consiste da onipresença de vários objetos ou coisas, incluindo tecnologias de sensores e dispositivos móveis físicos, sem fio e com fio, que interagem uns com os outros para cumprir objetivos comuns (43). Semanticamente, a IoT pode ser percebida como uma combinação entre a Internet e as coisas, e uma interligação mundial de objetos exclusivamente identificáveis com base em protocolos padrões de comunicação. A IoT é entendida como um ambiente inteligente que pode reagir às mudanças ou eventos que ela percebe em seu ecossistema.

Quanto à definição de “coisas”, adota-se neste texto a elaborada pelo *Cluster of European Research Projects on the Internet of Thing* (CERP-IoT), a qual define as “coisas” como participantes ativos em negócios, informações e processos sociais onde eles estão habilitados a interagir e se comunicar entre si e com o meio ambiente, trocando dados e informações sensoriados, enquanto reagem de forma autônoma aos eventos do “mundo real/físico”, influenciando a execução de processos que desencadeiam ações e criam serviços com ou sem intervenção humana direta (84).

A IoT, ao menos na teoria, visa tornar o cotidiano das pessoas mais simples, prático e produtivo, o que justifica a sua crescente popularidade. Embora RFID permaneça uma das principais 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 eHealth¹, edifícios inteligentes, redes inteligentes e sensores de meio ambiente são alguns exemplos de serviços e aplicações habilitadas pela IoT em diferentes campos (9).

Para fornecer suporte a este ambiente dinâmico, considerando o escopo deste trabalho e, em especial, a necessidade de segurança em torno da IoT, as seguintes características devem ser almejadas (61; 35; 9):

- Interoperabilidade: a IoT é caracterizada por apresentar uma considerável heterogeneidade de dispositivos, os quais apresentam capacidades diferentes dos pontos de vista computacional e de comunicação. As características de interoperabilidade estabelecem o gerenciamento dessa heterogeneidade dando suporte aos diferentes níveis da arquitetura (protocolos, eventos, aplicação). Adicionalmente, para transformar a quantidade considerável de dados produzidos pela IoT em informações úteis e para garantir a interoperabilidade entre diferentes aplicativos, é necessário fornecer dados com formatos adequados e padronizados. Isso permitirá que aplicações da IoT ofereçam suporte ao processamento de eventos. A interoperabilidade é um requisito essencial para lidar com a heterogeneidade e a dinamicidade, desafios exponenciais na IoT (?).
- Escalabilidade: na medida em que os objetos se conectam a uma infraestrutura de informação global, os problemas de escalabilidade surgem em diferentes níveis, incluindo: (i) endereçamento e nomeação, devido ao tamanho do sistema resultante; (ii) comunicação de dados e rede, em razão do alto nível de interconexão entre um grande número de entidades; (iii) gerenciamento de informações e conhecimento, pela possibilidade de construir uma base para qualquer entidade e/ou fenômenos, e; (iv) provisionamento e gerenciamento de serviços, em função da quantidade de serviços que podem estar disponíveis e a necessidade de lidar com recursos heterogêneos.
- Troca de dados baseada em redes sem fio: por sua comunicação ser fortemente baseada nas tecnologias de comunicação sem fio, isto pode representar problemas em termos de disponibilidade de espectro, ocasionando interferências e consequentemente erros de comunicação e indisponibilidade de serviço.
- Autonomia: a complexidade, a dinâmica e as especificidades que muitos cenários da IoT apresentam implicam na necessidade que os dispositivos (ou parte

¹Uso de tecnologia da informação para saúde.

deles) sejam capazes de reagir de maneira autônoma à diferentes situações, buscando minimizar a intervenção humana. Isso inclui a capacidade de executar a descoberta automática de dispositivos, recursos e serviços por eles oferecidos, além da necessidade de reação em casos adversos, como falhas ou lentidões, bem como a realização de ajustes do comportamento de protocolos, em especial os de segurança, para adaptação ao contexto atual.

Apesar do valor econômico estar aliado ao potencial de gerar impacto significativo na evolução e inovação da indústria, algumas questões ainda não foram abordadas para alcançar benefícios consistentes na IoT. Exemplos destas demandas incluem: a visibilidade global; o gerenciamento autônomo em tempo real; a padronização; a interoperabilidade dos sistemas; o consumo de recursos; a distribuição; o suporte à Qualidade de Serviço, do inglês *Quality of Service* (QoS); a privacidade dos dados; e a segurança (90; 61). 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 precisam ser adequadamente abordados (61; 77; 83). Fornecer segurança na IoT é uma tarefa complexa, uma vez que a rede é composta por diferentes dispositivos de detecção, computação e comunicação. Esta heterogeneidade, embora ofereça extensões de serviço e novos modelos de negócios, também introduz novos meios e oportunidades para que os adversários explorem ativos em diferentes níveis de uma arquitetura de serviço. Esses desafios, visões e vantagens impulsionam a investigação por soluções de segurança efetivas para proteger a IoT das ameaças emergentes, uma vez que os atuais controles de segurança tradicionais são ineficientes e insuficientes para proteger essa rede inteligente em desenvolvimento.

2.2 Eventos para Segurança da Informação

Para fornecer uma visão coerente sobre a relação entre a internet das coisas e a sua infraestrutura, a segurança adaptativa e a ciência de contexto, será abordado nesta seção o termo evento e, posteriormente, o que são os eventos de segurança e a importância de processamento de eventos complexos no âmbito desta tese.

O conceito de evento está diretamente associado com a capacidade de detecção de situações de interesse no âmbito da segurança adaptativa, uma vez que eventos são responsáveis por armazenar e tratar todas as mudanças sucedidas em qualquer situação que esteja ocorrendo em um determinado momento (17).

Considerando o escopo desta tese, **evento** é definido como uma ocorrência única dentro de um ambiente, geralmente envolvendo uma tentativa de mudança de situação. Inclui normalmente a noção de tempo, a ocorrência e os detalhes que pertencem

explicitamente ao evento ou ambiente que podem ajudar a explicar ou compreender as causas ou efeitos do evento (62).

Um evento pode ser dividido em campos que descrevem uma propriedade do evento. Exemplos de campos de um evento registrado por um WAF incluem: data; hora; endereço *Internet Protocol* (IP) de origem; padrão de correspondência; identificação da máquina do usuário; o objeto requisitado; entre outras informações. Termos sinônimos a registro de eventos incluem “registro de auditoria” e “entrada de log” (62).

Algumas vezes, eventos são utilizados para representar mudanças em situações, e esta abordagem é utilizada em algumas soluções de monitoramento (33). O sistema monitorado é representado por um grupo de sensores, sendo possível verificar os valores de cada sensor por meio de uma consulta, ou o próprio sensor emite um valor agindo como um produtor de eventos, possibilitando a identificação de uma mudança de situação por meio da avaliação do valor identificado.

Alguns eventos que acontecem ao redor do ambiente em análise não são eventos de interesse, ou seja, não representam algo relevante naquele determinado contexto, em contrapartida, outros são relevantes e podem causar uma mudança na situação atual. Nesta tese, há um interesse especial naqueles eventos que podem impactar na segurança do ambiente computacional, conhecidos como eventos de segurança.

Exemplos de eventos em computação incluem, a conexão de um usuário à um compartilhamento de arquivos, um servidor recebendo uma requisição de uma página web, um usuário enviando e-mail, e um *firewall* aceitando uma tentativa de conexão. Já os **eventos de segurança** são aqueles que, em geral, possuem consequências negativas na segurança da informação, podendo ou não consistirem de eventos computacionais, tais como falhas no sistema, violação da política de segurança da informação, uso não autorizado de privilégios do sistema, acesso não autorizado a dados sensíveis e execução de *malware* (93).

Outra definição importante a ser destacada para estabelecer a relação entre segurança da informação e processamento de eventos complexos é o de **incidente de segurança**, que consiste de qualquer evento ou conjunto de eventos de segurança correlacionados, confirmados ou sob suspeita, que impactam na segurança dos sistemas de computação ou das redes de computadores (22).

São exemplos de incidentes de segurança: tentativas de ganhar acesso não autorizado a sistemas ou dados; ataques de negação de serviço; uso ou acesso não autorizado a um sistema; modificações em um sistema, sem o conhecimento, instruções ou consentimento prévio do dono do sistema; desrespeito à política de segurança de uma empresa ou provedor de acesso. Por meio dos exemplos apresentados, percebe-se claramente que alguns dos incidentes são constituídos por um único evento de segurança, já outros, como o caso de ataques de negação de serviço, são normalmente detectados pela união de diversos eventos de segurança.

Normalmente, estes eventos mencionados são registrados em logs, atividade denominada de *logging*. Os eventos registrados em log são provenientes de sistemas, dispositivos, softwares, sensores, entre outros produtores de eventos, gerados a partir da resposta a algum estímulo. Este estímulo dependerá da origem do evento, por exemplo, em sistemas Unix, um estímulo pode ser o início ou a finalização de uma sessão por um usuário, em *firewalls* pode-se considerar a aceitação ou negação de um acesso, em sistemas operacionais, as falhas de armazenamento em disco também são estímulos responsáveis por gerar eventos que posteriormente devem ser analisados.

A definição de log adotada é também oriunda de (62), onde **log** é definido como uma coleção de registro de eventos. Termos como “registro de dados”, “registro de atividades”, “log de auditoria”, “trilha de auditoria”, “arquivo de log” e “log de eventos” são muitas vezes utilizados como sinônimos.

Em (25) a importância dos logs é evidenciada através da consideração de que logs são fontes de informações essenciais para manutenção de um sistema, visto que eles constituem a fonte básica de informação tanto para detecção e resolução de problemas quanto para informações de negócio, como métricas de acesso e comportamento de usuários. Além disso, logs são uma das principais fontes de evidência para a investigação de um crime cibernético (92). De acordo com (87), 84% das organizações que sofreram algum incidente de segurança possuíam evidências da violação em seus arquivos de log.

Para se obter sucesso no tratamento dos eventos de segurança registrados em log, e consequentemente nas estratégias de segurança adaptativa no escopo da IoT, é essencial estabelecer uma política concisa que esteja de acordo com as necessidades de quem estiver implementando. Os cenários são os mais diversos:

- Em uma certa empresa, é essencial registrar todas as atividades de acesso dos seus funcionários a websites. No entanto, uma outra empresa considera relevante armazenar somente as requisições a websites que não tiveram seu acesso permitido.
- Em um banco, é fundamental o registro de acessos ao banco de dados do núcleo bancário. No seu concorrente, adicionalmente, qualquer alteração no grupo de usuários administradores do servidor também é registrada.
- Em uma rede governamental, é fundamental o registro de todas as tentativas de ataque contra o seu perímetro de Internet.

Estas demandas devem ser refletidas em uma política que inclua desde a escolha de qual será o escopo de monitoração (aplicações, dispositivos, sistemas operacionais), até sua configuração, de modo que permita, assim, desde a geração correta

dos eventos e armazenamento dos logs que são pertinentes, até as correlações necessárias para que se obtenham as situações consideradas importantes, sejam as situações que se espera atuar sobre, ou os requisitos de auditoria que são exigidos para a empresa. Percebe-se assim que as soluções de segurança devem ser flexíveis para que as organizações possam adaptá-la às necessidades de seu ambiente.

Para fornecer esta flexibilidade, assim como a capacidade de unir vários eventos buscando oferecer um conhecimento de mais alto nível e possibilitar a tomada de uma determinada ação, é possível utilizar CEP (24).

Em linhas gerais, CEP trata-se da análise em tempo de execução de uma série de dados de múltiplas fontes para inferir eventos ou padrões que sugerem circunstâncias mais complicadas (81). Em geral, é uma operação feita em memória e a lógica é definida através de uma série de consultas feitas sobre o conjunto de dados recebidos. Para isto, o CEP considera operações que podem ser realizadas em eventos como parte de uma aplicação, incluindo filtragem, correlação, alteração e agregação, o que muitas vezes pode resultar em novos eventos. O objetivo é identificar situações significativas (como oportunidades ou ameaças) e responder a elas o mais rápido possível (14).

2.3 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 (41; 9). Esta propriedade auxilia na complexidade dos ambientes computacionais compostos pela IoT, utilizando a tecnologia para gerenciar a tecnologia, buscando-se minimizar a necessidade de intervenção humana. Com isto, a segurança adaptativa é a capacidade de um sistema em observar continuamente 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. Além disso, devem ser observados os requisitos funcionais e não funcionais (como tempo de resposta e desempenho) em conjunto com parâmetros estabelecidos pelo usuário (11).

Outro conceito importante a ser destacado é o de evento, o qual é uma das bases para a promoção da segurança adaptativa. Evento é definido como uma ocorrência única dentro de um ambiente, geralmente envolvendo uma tentativa de mudança de situação. Inclui normalmente a noção de tempo, a ocorrência e os detalhes que pertencem explicitamente ao evento ou ambiente que podem ajudar a explicar ou compreender as causas ou efeitos do evento (62).

Muitas equipes de segurança da informação dedicam uma parte considerável de

seus esforços na prevenção de ataques cibernéticos. Com isso, elas 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. De acordo com a Gartner, a segurança adaptativa é fundamentada em quatro elementos principais: prevenção; detecção; resposta e predição (60). Cada um destes elementos deve operar de maneira integrada, constituindo uma estratégia completa de proteção contra ameaças.

O conceito de segurança adaptativa foi elencado pela Gartner como uma das principais tendências de tecnologia estratégica, sendo um elemento vital de um negócio digital moderno (72). A adaptação dos controles e parâmetros de segurança considerando a avaliação do risco de maneira contínua, permite a tomada de decisão em tempo de execução, executando respostas que modificam o ambiente computacional, promovendo a segurança e consequentemente habilitando as empresas a expandirem e manterem seus negócios em operação (73).

Algumas das características da IoT, como a heterogeneidade, dinamicidade, espontaneidade, volatilidade e invisibilidade de como ocorre a comunicação nestes sistemas, implicam em uma maior complexidade no que tange a segurança da informação (54). Isso torna a utilização dos conceitos e mecanismos de adaptação um requisito importante para auxiliar no auto-gerenciamento deste ambiente. Além disso, considerando uma perspectiva evolutiva alinhada com o que percebe-se na indústria da IoT, a segurança adaptativa é um atributo a ser explorado visto o crescimento atual e potencial dos vetores de ataque e ameaças.

Este panorama dificulta a integração das abordagens de segurança tradicionais nos cenários de IoT, pois elas possuem uma visibilidade limitada e geralmente os mecanismos de resposta são manuais ou específicos (94; 96; 4). Logo, a flexibilidade é uma propriedade associada a segurança adaptativa relevante para a IoT, permitindo a integração das soluções de segurança em diferentes ambientes.

Para fornecer evidências de que as mudanças nas situações do ambiente monitorado satisfaçam os objetivos de segurança de um sistema, a literatura defende o uso de métodos formais (53; 11). Uma abordagem promissora para segurança adaptativa considerando os ambientes da IoT é o emprego de um ciclo de *feedback*. Um ciclo de *feedback*, conforme Figura 1, normalmente envolve quatro atividades principais: coletar; analisar; decidir e agir. Sensores coletam dados do ambiente e informações contextuais sobre seu estado atual. Os dados acumulados são então normalizados e armazenados para referência futura. A análise é então executada sobre os dados para inferir tendências e identificar sintomas. Posteriormente, de acordo com as situações identificadas, ocorre a decisão sobre como atuar no sistema em execução por meio

dos atuadores.

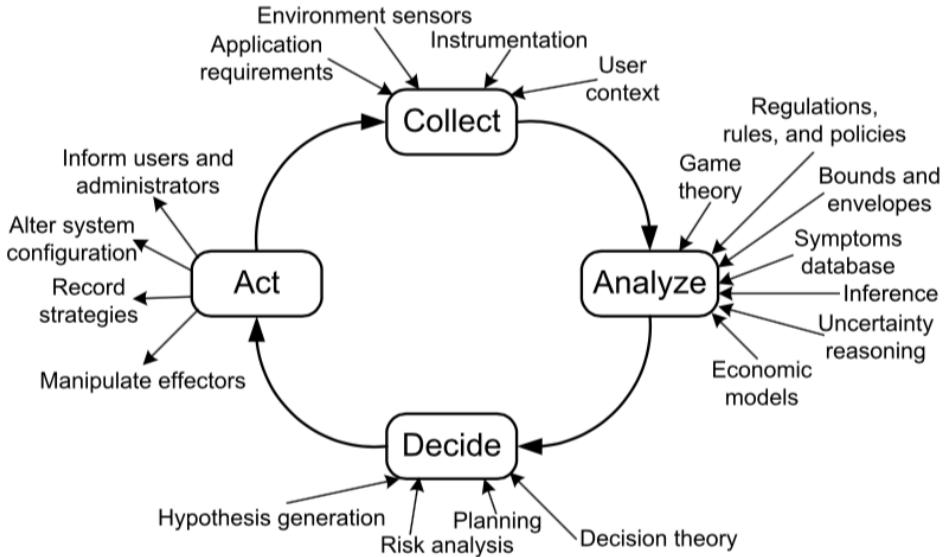


Figura 1 – Ciclo de *feedback* genérico

Fonte: 28, p. 227.

Um exemplo da aplicação do ciclo de *feedback* é discutido em Brun et al. (2009).

Os autores consideram que manter os serviços Web em funcionamento requer: (i) coletar informações que refletem o estado atual do sistema; (ii) analisar essas informações para diagnosticar problemas de desempenho ou para detectar falhas; (iii) decidir como resolver o problema (por exemplo, via balanceamento dinâmico de carga ou corrigindo falhas); e por último, (iv) agir para efetuar as decisões tomadas.

Ao conceber um sistema adaptativo, algumas questões sobre essas atividades tornam-se importantes. Estas questões relativas aos laços de *feedback* devem ser explicitamente identificadas, registradas e resolvidas durante o desenvolvimento de um sistema adaptativo. A seguir, serão apresentadas as atividades e as respectivas questões levantadas em Brun et al. (2009) e Lamprecht (2012):

- O ciclo de *feedback* começa com a coleta de dados relevantes de sensores disponíveis no ambiente e outras fontes que auxiliam na compreensão do estado atual do sistema. Algumas das questões que precisam ser respondidas aqui são: Qual é a taxa de amostragem necessária? Quão confiável é o dado do sensor? Existe um formato de evento comum entre os sensores? Os sensores fornecem informações suficientes para a identificação do sistema?;
- Na sequência, o sistema analisa os dados coletados. Nesta etapa existem inúmeras abordagens para estruturar e raciocinar sobre os dados brutos (por exemplo, usando modelos, teorias e regras). Algumas das questões aplicáveis aqui

são: Como o estado atual do sistema é inferido? Qual a quantidade/tempo de eventos passados podem ser necessários no futuro? Quais dados precisam ser arquivados para validação, verificação e/ou conformidade? Quão fiel será o modelo ao mundo real e se um modelo adequado pode ser obtido a partir dos dados de sensores disponíveis? Quão estável será o modelo ao longo do tempo?;

- Em seguida, uma decisão deve ser tomada para adaptar o sistema objetivando alcançar um estado desejável. Abordagens como análise de risco ajudam na escolha entre várias alternativas. Para esta atividade, as questões importantes são: Como o estado futuro do sistema é inferido? Como é alcançada uma decisão? Quais são as prioridades para a auto-adaptação em vários ciclos de *feedback* e em um único ciclo de *feedback*?;
- Finalmente, para implementar a decisão, o sistema deve agir por meio dos atuadores disponíveis. As questões importantes que surgem aqui são: Quando a adaptação deve e pode ser realizada com segurança? Como os ajustes de diferentes ciclos de *feedback* interferem um ao outro? Os *feedbacks* centralizados ou descentralizados ajudam a atingir o objetivo global? Uma importante questão aplicável adicional é se o sistema de controle tem autoridade de comando suficiente sobre o processo, ou seja, se os atuadores disponíveis são suficientes para conduzir o sistema nas direções desejadas.

O modelo genérico de um ciclo de *feedback* ilustrado na Figura 1, muitas vezes referido como o ciclo de controle autônomo, enfatiza as atividades que realizam *feedback*. Embora este modelo forneça um ponto de partida sobre os ciclos de *feedback*, ele não detalha o fluxo de dados e o controle em torno do ciclo (28). Ainda que esses ciclos de *feedback* tenham tido muito sucesso em diferentes ramos de engenharia, como na teoria de controle, ainda não está claro se os princípios gerais desta disciplina podem ser aplicados diretamente em sistemas adaptativos. Diferentemente da teoria de controle, os cenários da IoT possuem uma estrutura não totalmente conhecida (53).

Em uma tentativa de lidar com as complexidades dos sistemas modernos de computação a *International Business Machines* (IBM) assumiu os desafios mencionados e sugeriu o modelo *Monitor-Analyze-Plan-Execute plus Knowledge* (MAPE-K), conforme apresentado na Figura 2. 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 (11).

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 (53).

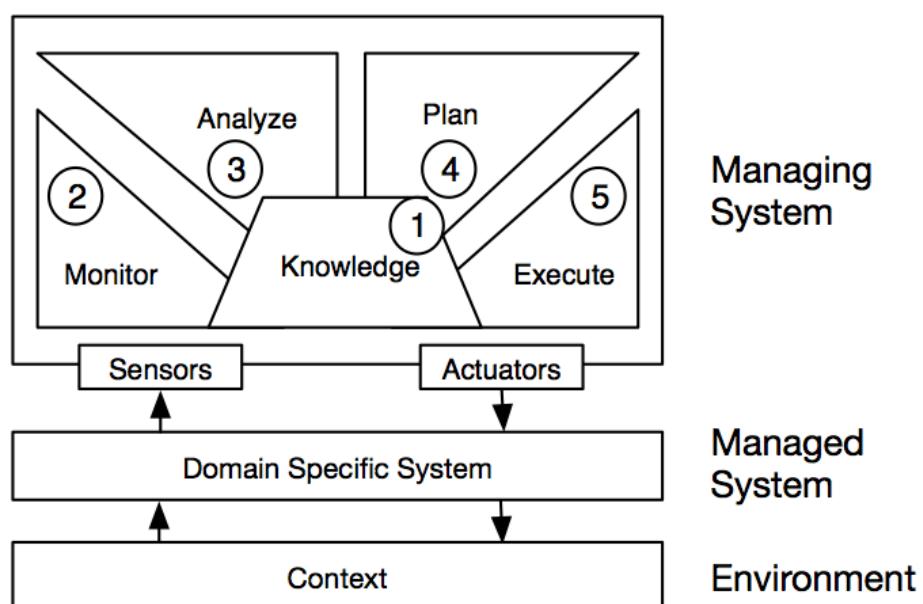


Figura 2 – MAPE-K - Modelo para sistema adaptativos

Fonte: 49, p. 7.

De acordo com a IBM, um sistema autonômico deve ter os seguintes auto-atributos (50; 49):

- Autoconfiguração (*self-configuration*): o sistema deve se configurar automaticamente de acordo com as políticas de alto nível pré-definidas. Este atributo também contempla a facilidade de se adaptar às mudanças causadas por configurações automáticas. A integração, instalação e configuração de dispositivos e softwares devem ser feitos eficientemente. Caso a nova configuração não proporcione para a rede o desempenho esperado, há a possibilidade de restauração da mesma;
- Auto-otimização (*self-optimization*): consiste da habilidade do sistema em controlar os recursos e os parâmetros de segurança para melhorar o desempenho e a eficiência, consequentemente aprimorando a QoS;

- Autocura (*self-healing*): é a capacidade do sistema detectar, diagnosticar e reparar falhas automaticamente sem que isto afete o funcionamento do sistema. A auto-cura é determinante na disponibilidade e na confiabilidade do sistema;
- Autoproteção (*self-protection*): este atributo envolve dois aspectos, a defesa contra ataques e a antecipação de ataques. A defesa deve ser realizada com o objetivo de proteger o sistema de ataques maliciosos ou falhas que não foram tratadas corretamente pela auto-cura. A antecipação de ataques é feita baseando-se em relatórios de sensores e, com essas informações, medidas devem ser adotadas para minimizar os problemas.

Em Evesti; Ovaska (2013), os autores mencionam outros dois atributos, a auto-consciência (*self-awareness*) e a ciência de contexto (*context awareness*). A auto-consciência 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.

2.4 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 é considerada relevante para a interação entre o usuário e a aplicação, incluindo o próprio usuário e a aplicação.

Contexto pode ser considerado também como uma descrição complexa de conhecimento compartilhado sobre circunstâncias físicas, sociais, históricas, entre outras, onde ações ou eventos ocorrem, percebendo assim a relação existente entre contexto e eventos. Contexto é o que contribui para a correta interpretação de uma ação ou evento, sem, no entanto, ser parte dessa ação/evento. Também pode ser considerado como sendo uma coleção de condições relevantes e influências que tornam uma situação única e compreensível (18; 56).

Existem seis questões básicas que podem ser realizadas para facilitar a compreensão do contexto, elas são conhecidas como 5W+1H (88). No entanto, para determinadas aplicações algumas são mais importantes que outras. A seguir as seis questões são apresentadas:

- quem (*who*): informação de presença e disponibilidade dos indivíduos no grupo, e de identificação dos participantes envolvidos num evento ou numa ação;

- o quê (*what*): informação sobre a ocorrência de um evento de interesse;
- quando (*when*): informação temporal sobre o evento, o momento em que o evento ocorreu;
- onde (*where*): informação espacial, de localização, o local onde o evento ocorreu;
- por que (*why*): informação subjetiva sobre as intenções e motivações que levaram à ocorrência do evento;
- como (*how*): informação sobre a maneira com que o evento ocorreu.

O contexto é relativo a um foco, onde foco pode ser uma tarefa ou um passo na resolução de um problema ou em uma tomada de decisão (19). Dessa forma, o foco determina onde está o contexto e o que pode ser considerado como importante, pois nem tudo que é contexto de uma situação é relevante para tal.

As áreas da UbiComp e Inteligência Artificial foram as pioneiras nos estudos e utilização do conceito de contexto e, com isso, foram as que demonstraram o potencial da aplicação desse conceito nos sistemas computacionais. Ultimamente, a ciência de contexto vem sendo foco de um grande número de pesquisas dentro da UbiComp. 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 (26).

Para a construção de aplicações cientes de contexto algumas funcionalidades devem ser providas. Dentre elas destaca-se (79): (i) suportar o tratamento de uma variedade de tipos de sensores; (ii) lidar com a natureza distribuída de informações contextuais, visto que os dados são provenientes de fontes diferentes e de naturezas de dados distintas; (iii) proporcionar uma interpretação transparente para as aplicações e uma abstração para os dados de contexto; (iv) disponibilizar o armazenamento desses dados e realizar a manutenção do seu armazenamento; (v) controlar o fluxo de dados de contexto. 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;

- apoia a compreensão de eventos e de situações.

Em Heimerl (2012), é discutida a importância de contexto à segurança da informação. Inicialmente, ele defende a ideia de que informação sem contexto é simplesmente um dado, e não informação. Logo, dados são mais valiosos quando contextualizados. Um cenário que exemplifica isto é apresentado em Aman; Snekkenes (2015), onde é descrito um médico, atualmente em férias, usando seu smartphone. O mesmo recebe autorização por um Sistema de Controle de Acesso Baseado em Função, do inglês *Role-Based Access Control* (RBAC), para acessar informações pessoais do paciente de um lugar incomum, em um fim de semana. Do ponto de vista do RBAC, esta atividade parece ser legítima, e o sistema deve conceder acesso. No entanto, se for analisado todo o contexto, isto é, o local incomum, o estado atual e a data de acesso, pode-se concluir que existe um risco envolvido se o acesso for concedido, ou seja, o smartphone pode ter sido comprometido. Portanto, para prover segurança adaptativa com eficiência deve-se avaliar a situação em uma visão holística.

No que tange a segurança adaptativa, caso os contextos relevantes para a identificação das situações a serem avaliadas não sejam adequadamente levados em consideração, pode haver uma influência adversa no ambiente impactando nos serviços oferecidos. Observa-se que a segurança adaptativa, é fortemente dependente do ambiente monitorado e da visão holística sobre o mesmo. Em outros termos, a contextualização deve ocorrer em diferentes níveis arquiteturas (desde a coleta do evento, passando pela normalização, análise de risco e assim por diante). A ciência de contexto torna-se fundamental nos cenários da IoT, em particular para realizar adaptação, pois esta consiste de uma comunicação máquina para máquina, a priori sem a inteligência (envolvimento direto) dos humanos. Uma vez que sejam levados em consideração contextos irrelevantes, incorretos ou insuficientes, a adaptação pode não ser eficiente (11).

2.5 Considerações sobre o Capítulo

Inicialmente neste capítulo foi apresentada a definição de IoT, sendo destacado que a segurança adaptativa é considerada um desafio importante e atual. Posteriormente, foram introduzidos os conceitos de evento e processamento de eventos, temas centrais nesta tese. Na sequência, a segurança adaptativa foi discutida, sendo exposto que o uso de um ciclo de *feedback* se faz necessário para apoiar a implantação deste conceito. Também foi descrito que a ciência de contexto é um atributo fundamental para a adaptação. Com isto, na seção seguinte foi analisada a ciência de contexto descrevendo como ela pode ser aplicada neste âmbito. No Capítulo a seguir é apresentada a pesquisa desenvolvida para identificar o estado da arte considerando os tópicos abordados nesta revisão conceitual.

3 ESTADO DA ARTE

Este capítulo 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 seção seguinte é apresentado o protocolo executado para, posteriormente, serem discutidos os trabalhos identificados.

3.1 Revisão Sistemática da Literatura

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 (27; 44; 46).

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*, *eHealth*.

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 3.

adapt* AND security AND context* AND ("internet of things" OR iot)

Figura 3 – 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*¹, os quais foram apenas removidos da *string*, o que é compensado pelo suporte à *stemming*² 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 4 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.

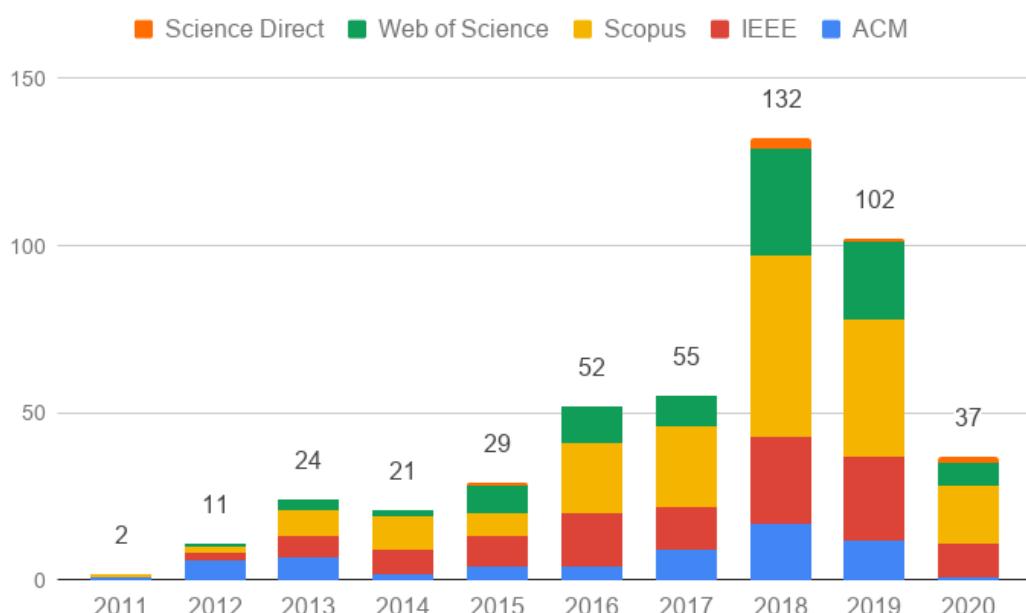


Figura 4 – Número de artigos publicados por ano em cada base considerada

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

- (E) artigo duplicado;

¹Um *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 (78).

²Em recuperação de informação *stemming* é o processo de reduzir palavras flexionadas (ou às vezes derivadas) ao seu tronco (*stem*), base ou raiz, geralmente uma forma da palavra escrita (58).

- (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;
- (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 StArt³. 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 Github⁴.

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 um teste de confiabilidade entre avaliadores (40). O autor principal desta tese realizou

³http://lapes.dc.ufscar.br/tools/start_tool

⁴<https://github.com/rborgesalmeida/doutorado-tese/raw/master/Seguranc%C3%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

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 literatura 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; BALA-SINGHAM, 2012	<i>Risk-based Adaptive Security for Smart IoT in eHealth</i>	ACM	<i>European Conference on Software Architecture: Companion Proceedings</i>
AMAN; SNEK-KENES, 2014	<i>Event driven adaptive security in internet of things</i>	Scopus	<i>International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies</i>
RAMOS; BER-NABE; SKAR-META, 2015	<i>Managing Context Information for Adaptive Security in IoT Environments</i>	IEEE, Web of Science, Scopus	<i>International Conference on Advanced Information Networking and Applications Workshops</i>
EL-MALIKI; SEIGNE, 2016	<i>Efficient Security Adaptation Framework for Internet of Things</i>	IEEE, Web of Science, Scopus	<i>International Conference on Computational Science and Computational Intelligence</i>
MOZZAQUATRO et al., 2016	<i>An ontology-based security framework for decision-making in industrial systems</i>	IEEE, Scopus	<i>International Conference on Model-Driven Engineering and Software Development</i>
KHAN; NDU-BUAKU , 2018	<i>Ontology-based automation of security guidelines for smart homes</i>	IEEE, Scopus	<i>World Forum on Internet of Things (WF-IoT)</i>

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.

Tabela 4 – Artigos avaliados em profundidade após seleção inicial

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

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

3.2.1 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* (1). 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	<i>Establish the context; Risk assessment; Risk treatment planning; Risk acceptance</i>	<i>Analyze (plan): establish security</i>
Do	<i>Implementation of risk treatment plan</i>	<i>Adapt (Execute): adapt, implement and operate security</i>
Check	<i>Continual monitoring and reviewing of risks</i>	<i>Monitor: monitor and review security</i>
Act	<i>Maintain and improve the ISRM process</i>	<i>Adapt (learn): maintain, learn & improve security</i>

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 5 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.

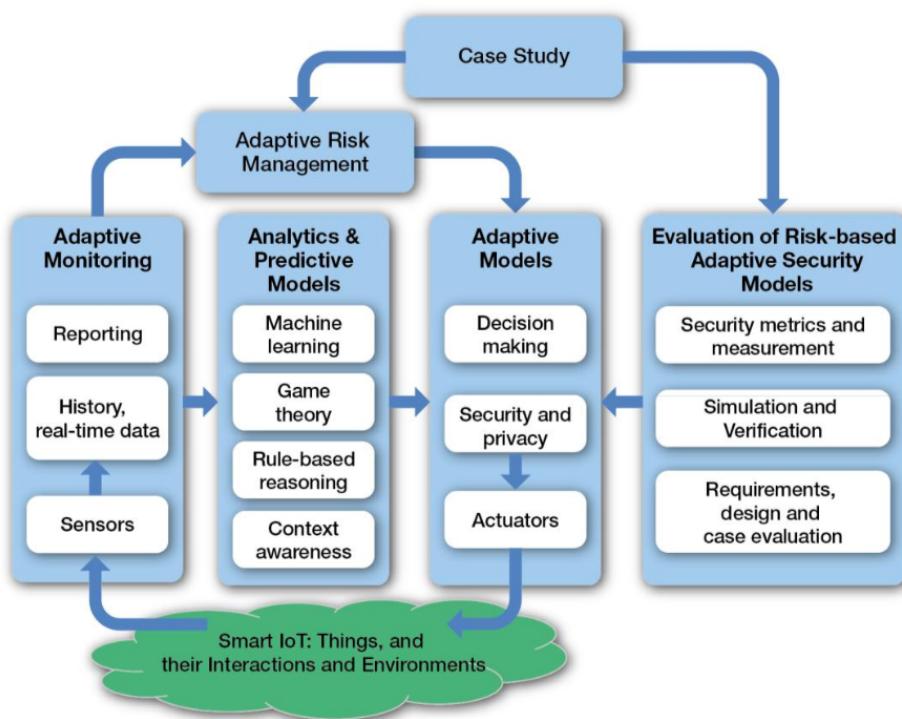


Figura 5 – Modelo proposto para gerenciamento de segurança adaptativa

Fonte: ABIE; BALASINGHAM, 2012

O modelo de monitoramento de segurança adaptável (*Adaptive Monitoring*) empregado no *framework* foi proposto pelos autores em (2) 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.

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 6) 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.

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.

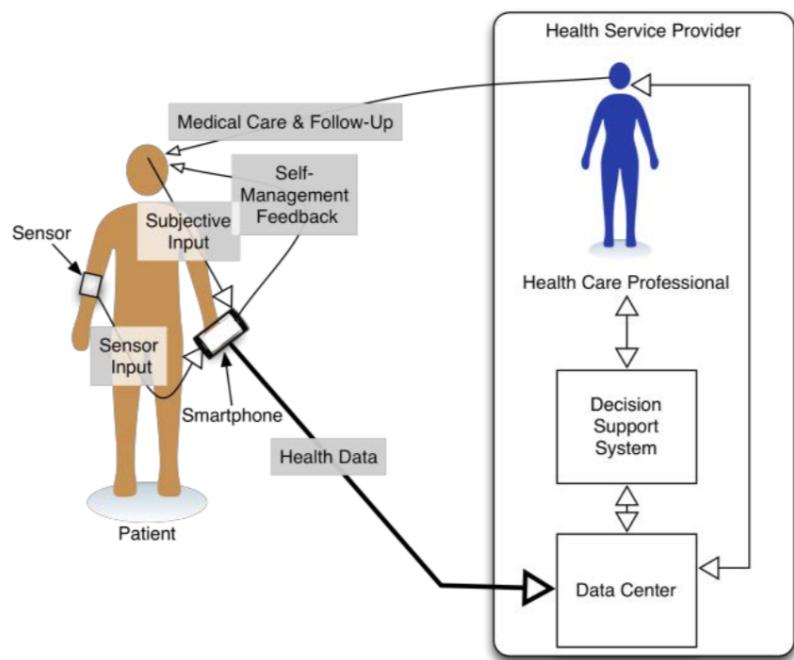


Figura 6 – Estudo de caso baseado em monitoramento de paciente
Fonte: ABIE; BALASINGHAM, 2012

3.2.2 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 (37).

Apesar de no artigo (37) 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 7, 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.

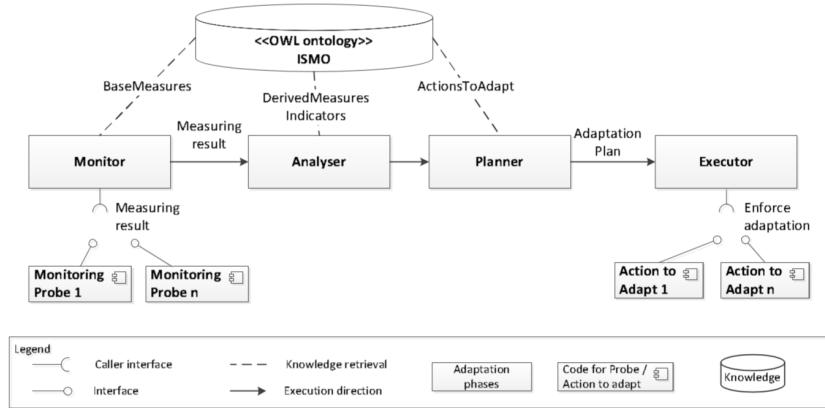


Figura 7 – Estrutura da arquitetura de adaptação

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 8 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.

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.

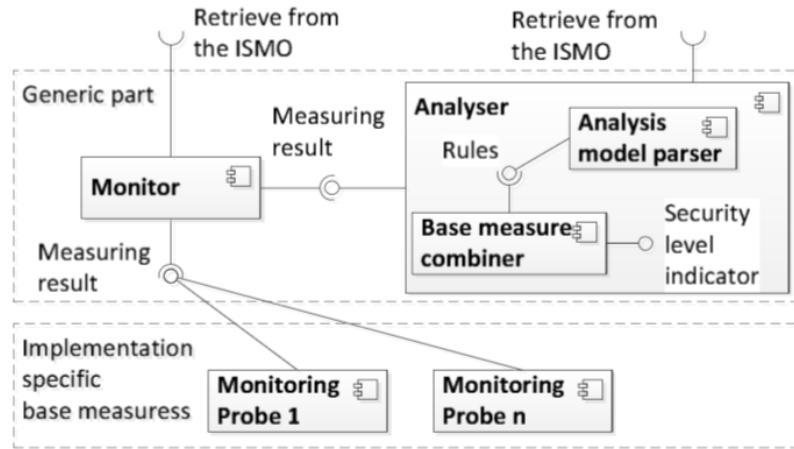


Figura 8 – Partes genéricas e específicas da implementação do monitoramento do nível de segurança

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 9.

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 armazenamento ou processamento.

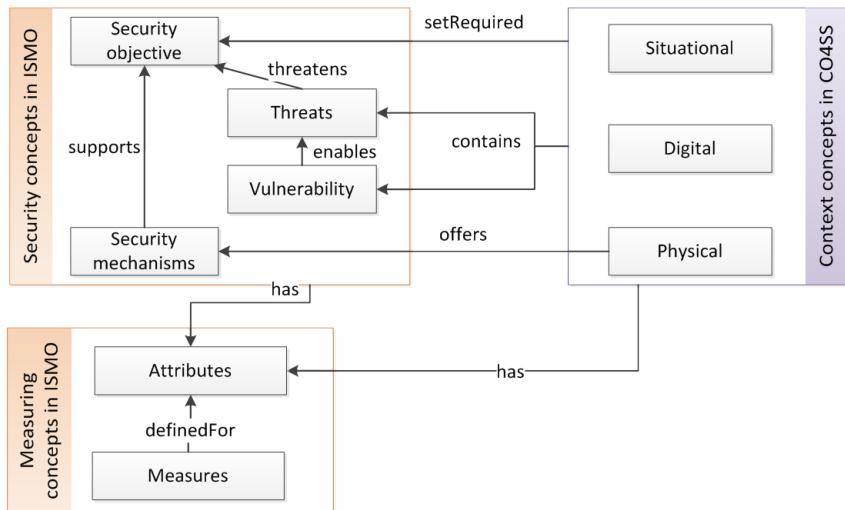


Figura 9 – Dependências entre ontologias de segurança e de contexto

3.2.3 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 10 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.

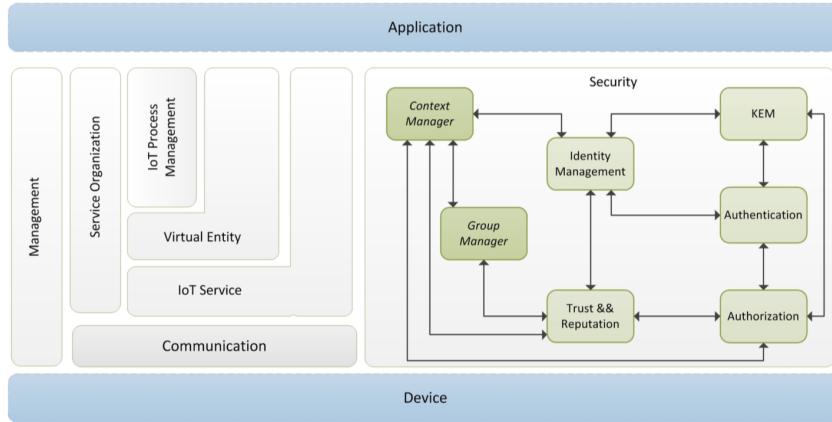


Figura 10 – Framework de segurança cliente de contexto para IoT

Além disso, são propostos diferentes estágios para o ciclo de vida do gerenciamento de contexto (incluindo aquisição, modelagem, organização, raciocínio, combinação e inferência de informações contextuais), bem como um conjunto de diretrizes sobre implicações de segurança durante estes estágios.

A Figura 11 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)

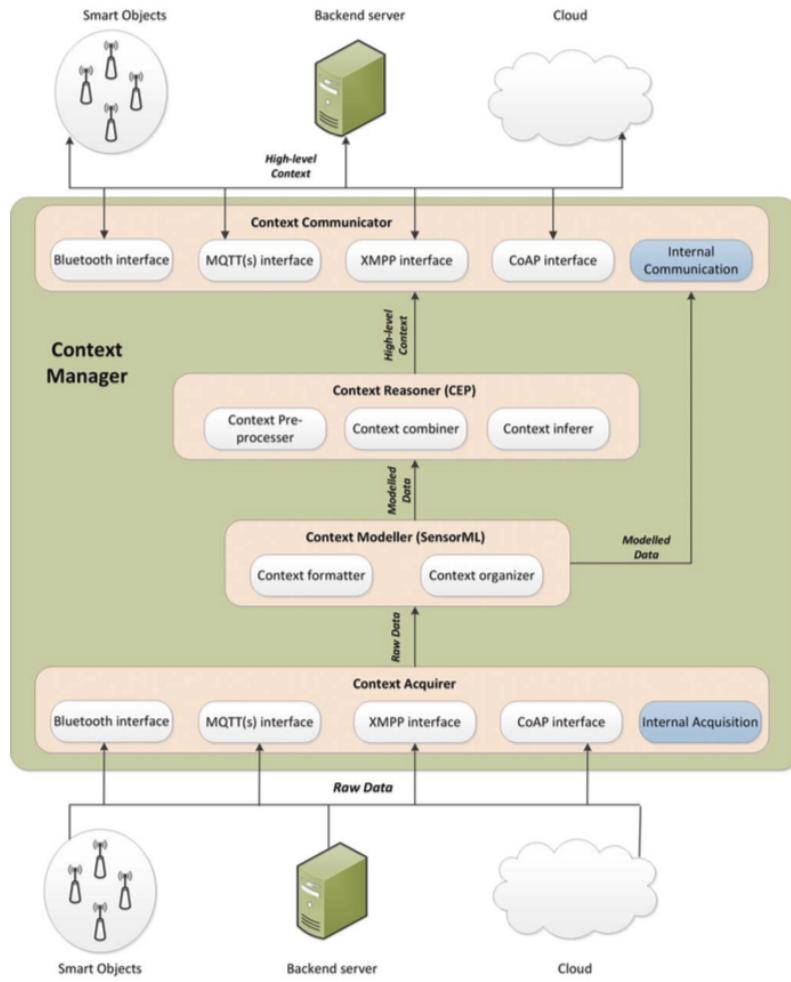


Figura 11 – Visão geral do Gerenciador de Contexto

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 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) (68) (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 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 res-

ponsável 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-processor* 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 contextual 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, agrregar 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 (69), 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 12, 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.

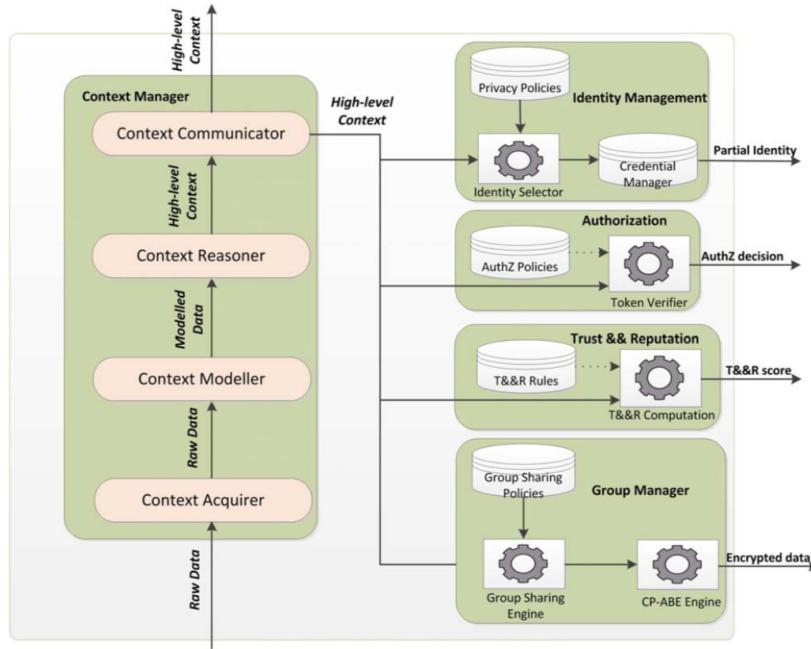


Figura 12 – Interações do *framework* para mecanismos de segurança adaptativa cientes de contexto

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, leves e adaptativos em diferentes cenários.

3.2.4 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) (6). 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 círculo 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 13, a qual inclui três principais componentes *Monitor*, *Analyzer* e *Adaptor*.

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 pla-

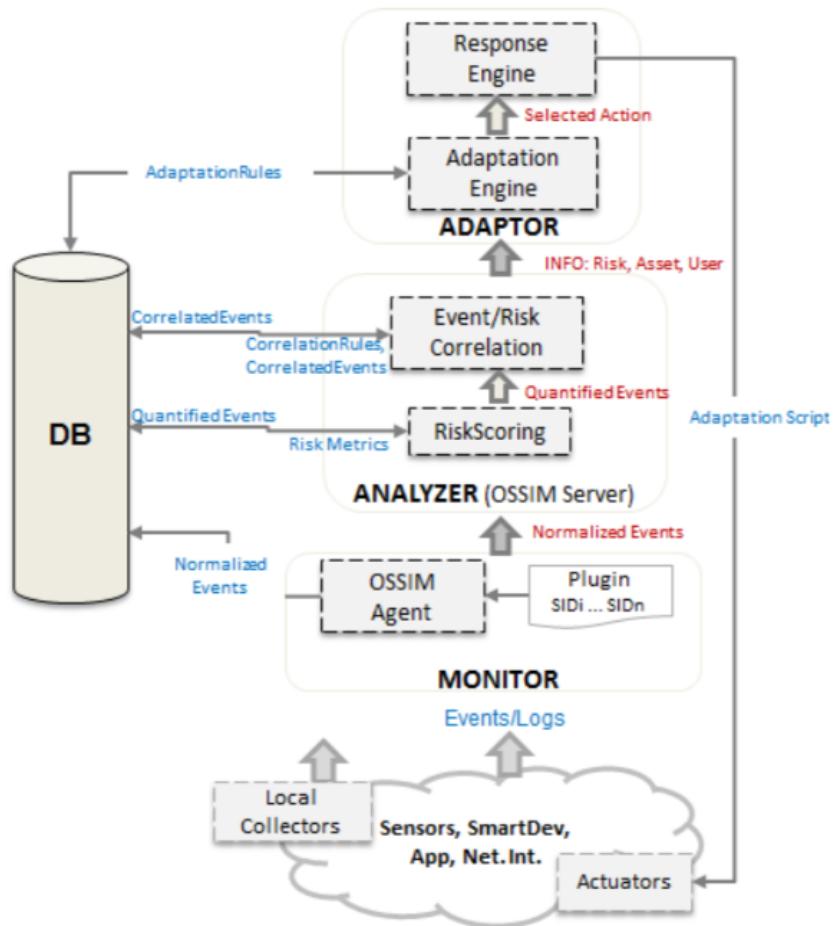


Figura 13 – EDAS - modelo de referência

taforma. 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:

$$Risk(X) = (Priority \times AssetValue \times Reliability)/25$$

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 14.

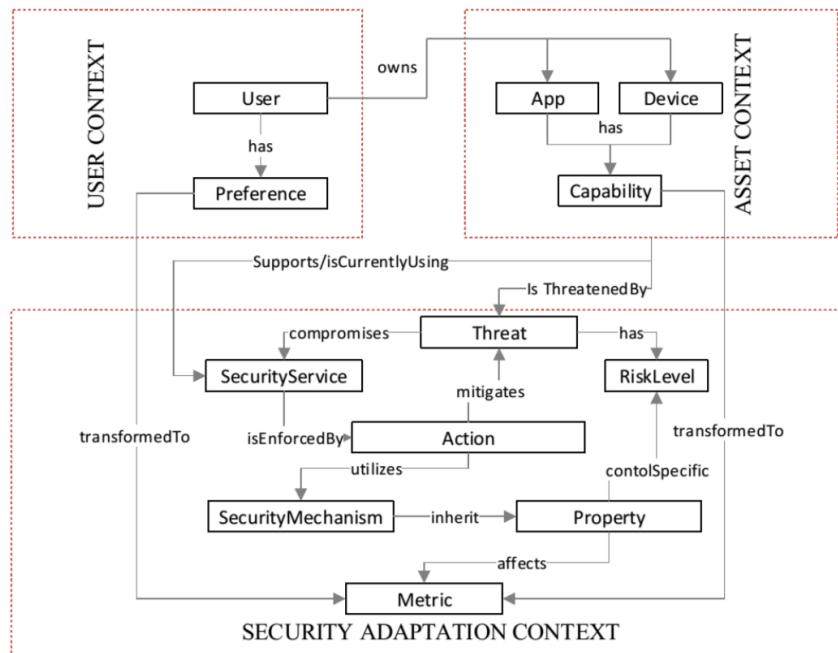


Figura 14 – EDAS - ontologia para segurança adaptativa

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 15. 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 adap-

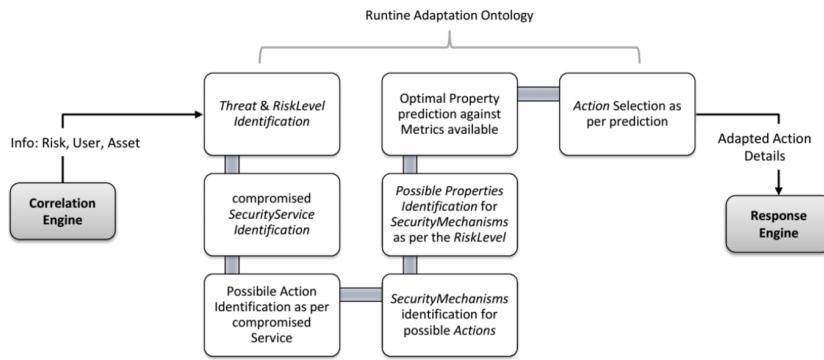


Figura 15 – EDAS - processo de segurança adaptativa

tada) para um usuário específico. As métricas refletem parâmetros, como usabilidade, confiabilidade, custo do serviço, entre outros, que podem ser influenciados negativamente ou positivamente 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 (76; 82). 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 Mozzaquato et al. (2017), ao referenciar o EDAS, os autores destacam que o modelo não considera possíveis vulnerabilidades que possam impedir eventuais ameaças no ambiente.

3.2.5 Efficient Security Adaptation Framework for Internet of Things

O artigo (30) apresenta um *framework* genérico denominado *Security Adaptation Reference Monitor* (SARM) que emprega o paradigma autônomo, sendo desenvolvido especialmente para ambientes suportados por redes sem fio altamente dinâmi-

cas. 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 16 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.

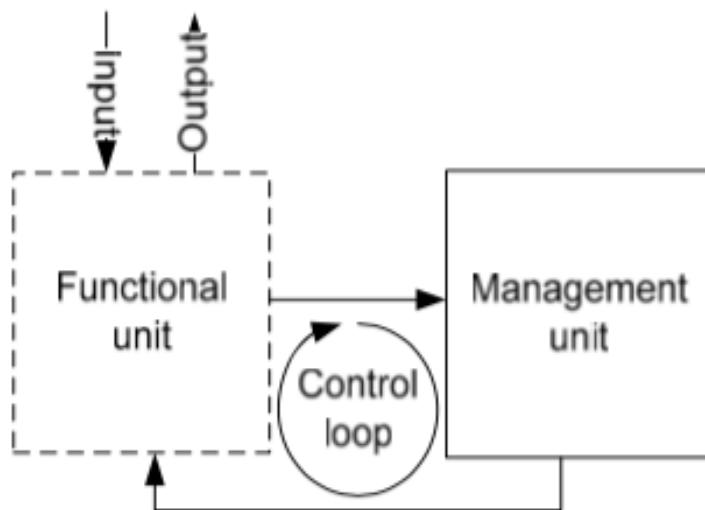


Figura 16 – SARM - descrição do sistema autônomo

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 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 17. 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, foram 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 mo-

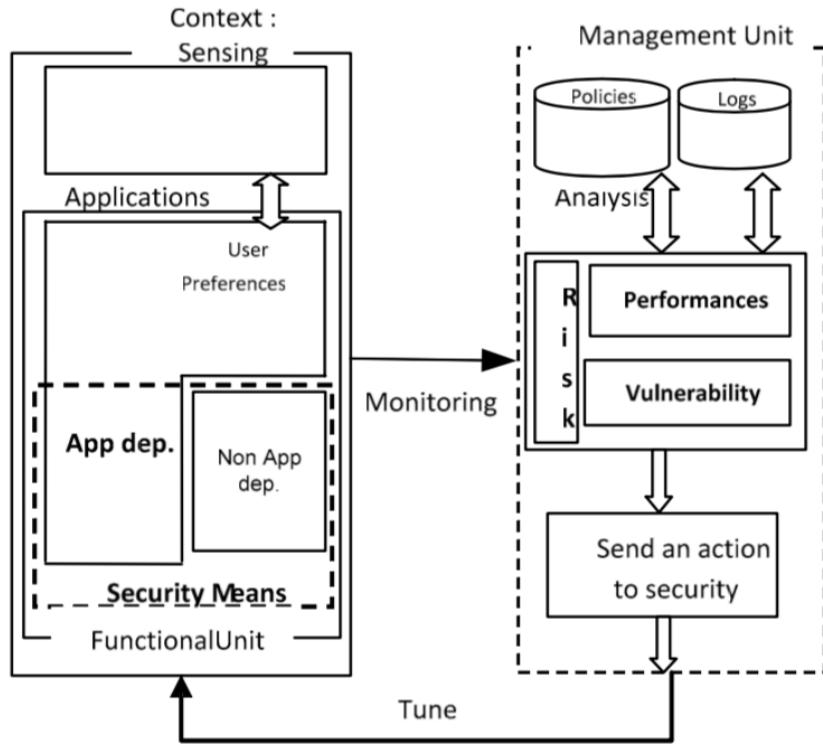


Figura 17 – SARM - fundamentos do *framework* genérico para segurança adaptativa

dulares 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 melhorar 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.

3.2.6 An Ontology-based Cybersecurity Framework for the Internet of Things

O trabalho de Mozzaquattro et al. (2016) propõe uma arquitetura para *framework* de segurança adaptativa (vide Figura 18) 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 Mozzaquattro 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.

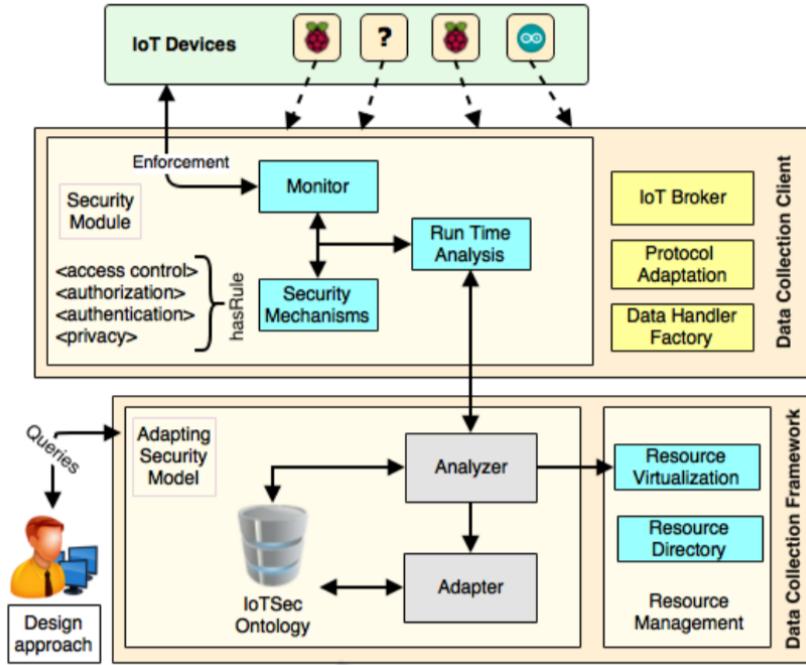


Figura 18 – Uma arquitetura para *framework* de segurança adaptativa baseada em ontologia integrada com a plataforma C2NET.

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 apresentada na Figura 19, 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 implementado no âmbito do projeto *Cloud Collaborative Manufacturing Networks* (C2NET⁵) para verificar a adequação da aplicação do *framework* considerando algumas questões de cibersegurança.

A plataforma colaborativa C2NET tem como base a computação na nuvem per-

⁵<http://c2net-project.eu/>

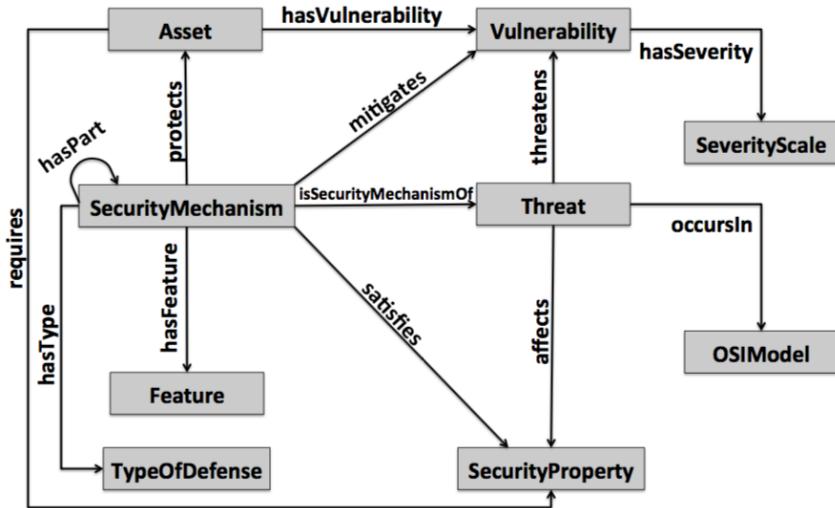


Figura 19 – Ontologia de referência para segurança na IoT (65)

mitindo 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 validação da proposta dois cenários foram desenvolvidos sobre o setor metalmúrgico 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 (65; 66; 64) proporem a concepção de um *framework* 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 Mozzaquattro 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.

3.2.7 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. 20. 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.

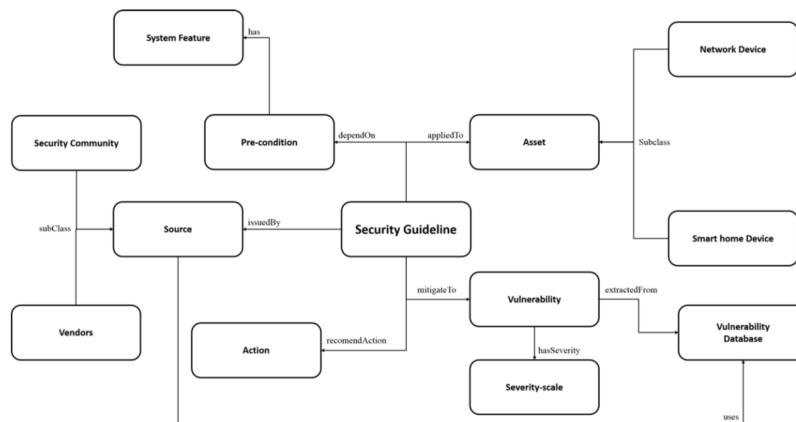


Figura 20 – Modelo abstrato de diretrizes de segurança (51)

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; semiautomático; 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.

3.3 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 principal 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);
- 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;

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

- 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 da IoT, seja automático ou semiautomático, nenhum dos trabalhos contempla de maneira

Tabela 7 – Tabela comparativa

	ABIE, 2012	EVESTI, 2014	RAMOS, 2015	AMAN, 2016	EL- MALIKI, 2016	MOZZA- QUATRO, 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

satisfatória esta propriedade. Ou seja, apesar dos trabalhos possuírem como objetivo o fornecimento de segurança adaptativa, parte deles suporta este requisito de forma limitada, por meio de scripts personalizados como em Aman (2016) ou de códigos desenvolvidos especificamente para a avaliação (30; 64).

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 escolha entre as diferentes opções de adaptação, a maior parte dos trabalhos tem empregado ontologias, a qual já é utilizada para 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 (21; 64). 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. Também observa-se a necessidade de propostas que contemplam a distribuição e escalabilidade dos *frameworks*, possibilitando as suas aplicações 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, os impactos destas informações necessitam 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.

3.4 Considerações sobre o Capítulo

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 (39; 89; 55). 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.

4 AS-PROCBE: SEGURANÇA ADAPTATIVA BASEADA EM ENRIQUECIMENTO PROGRESSIVO DE CONTEXTO

Considerando os objetivos elencados, um modelo arquitetural para segurança adaptativa ciente de contexto foi concebido visando oferecer recursos oportunos no emprego dos diferentes cenários da IoT.

O esforço de concepção do modelo considerou as premissas do *Execution Environment for Highly Distributed Applications - Situational Awareness* (EXEHDA-SA), propondo uma continuidade da pesquisa discutida em Almeida et al. (2019), com o intuito de melhor atender os requisitos da IoT no que tange a contextualização para segurança adaptativa. Desta forma, na seção seguinte são descritas as características do EXEHDA-SA relevantes para a compreensão da abordagem desenvolvida nesta tese, para posteriormente descrever o modelo concebido.

4.1 Escopo do Trabalho: EXEHDA-SA

A adoção do EXEHDA-SA visa apoiar o atendimento de alguns requisitos chaves para a IoT como escalabilidade, modularidade, extensibilidade e interoperabilidade. Além disso, a sua utilização é motivada por seu modelo arquitetural flexível e extensível, além de apresentar uma estratégia de prototipação viável para processamento de eventos nos ambientes da IoT. Outros aspectos que influenciaram esta decisão incluem:

- o EXEHDA-SA foi proposto com base no *middleware* EXEHDA, o qual é direcionado às aplicações distribuídas, móveis e cientes de contexto, e tem como objetivo criar e gerenciar um ambiente ubíquo formado por células de execução distribuídas e promover a computação sobre esse ambiente heterogêneo;
- o modelo propõe a coleta de eventos de dispositivos heterogêneos, e discute funcionalidades para normalização, contextualização, processamento de eventos, atuação e armazenamento, o que se alinha com as etapas MAPE do ciclo de *feedback*;

- emprego dos conceitos de ciência de situação, tendo como base o modelo de Endsley (31; 32), o qual está diretamente associado com a demanda de contextualização dos eventos de segurança, e pode ser identificado pela nomenclatura dos módulos do EXEHDA-SA, bem como por seus respectivos propósitos.

O EXEHDA-SA é formado por três componentes:

- o Collector (vide Figura 21), que atua na borda da arquitetura, sendo principalmente responsável por coletar eventos do ambiente ubíquo, podendo adicionalmente, realizar o processamento de eventos para detecção de situações de interesse, e inclusive realizar a respectiva atuação;

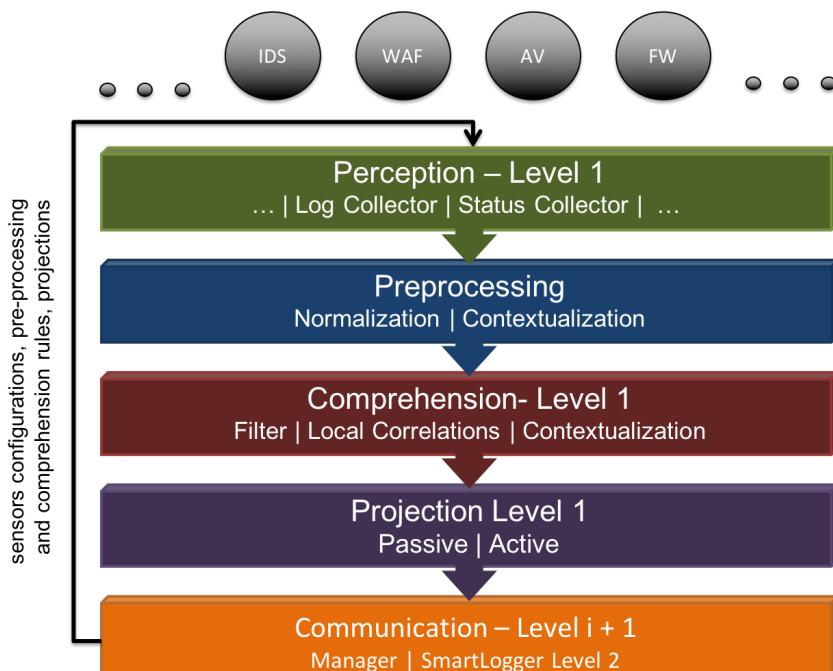


Figura 21 – Componente projetado para o EXEHDA-SA Collector

- o SmartLogger, o qual foi projetado para ser implantado em um dispositivo dedicado visando o recebimento de eventos e situações de diferentes Collectors e SmartLoggers sob sua gerência, oferecendo assim recursos de pré-processamento, correlação e atuação, bem como um repositório de armazenamento (conforme observa-se na Figura 22); ao possibilitar o envio e recebimento de eventos e situações de SmartLoggers para SmartLoggers, o EXEHDA-SA estabeleceu um modelo arquitetural multinível, preservando a organização celular proposta originalmente pelo *middleware* EXEHDA - observada na Figura 23 - e consequentemente garantindo a autonomia de cada célula, seja ela representada fisicamente por diferentes instituições parceiras, filiais, unidades, segmentos de rede, entre outras (conforme Figura 22). Ou seja, o fluxo de comunicação do EXEHDA-SA visa estabelecer diferentes níveis dentro de uma hierarquia,

onde cada nível representa os aspectos de ciência de situação de um escopo específico. Esses níveis são criados alocando diferentes SmartLoggers que lidam com a autonomia de cada célula.

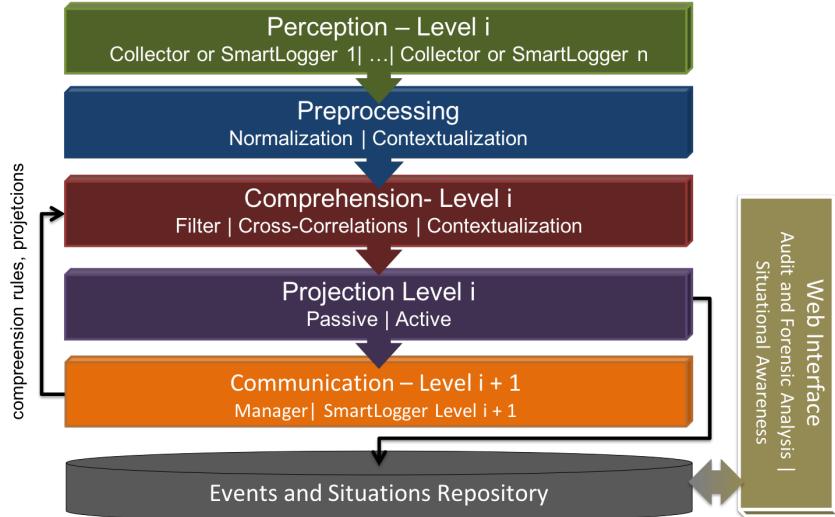


Figura 22 – Componente projetado para o EXEHDA-SA SmartLogger

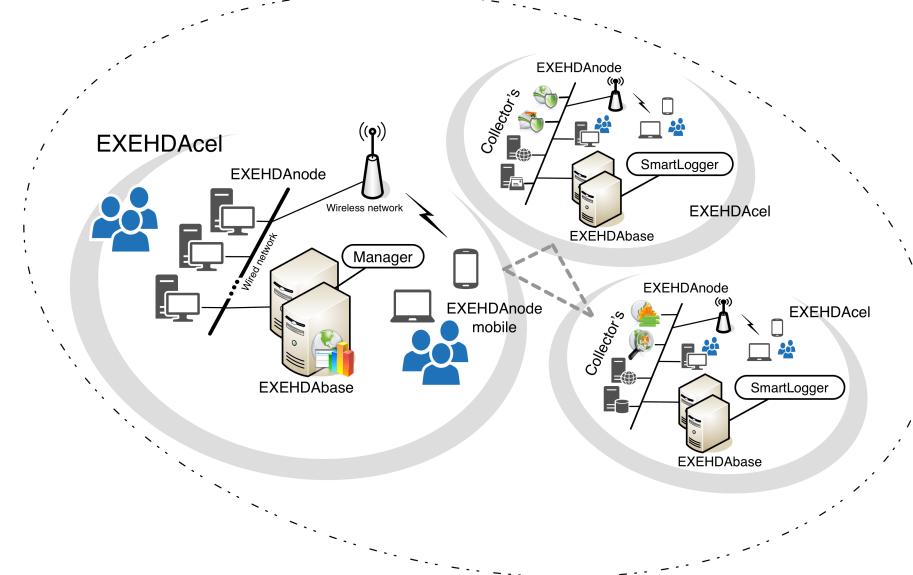


Figura 23 – Componentes do EXEHDA-SA mapeados sobre o ambiente ubíquo

- o Manager, ilustrado na Figura 24, foi concebido para receber eventos de diferentes Collectors e SmartLoggers, sendo o último ponto de contato para agrupamento da visão geral sobre todos os dispositivos sob coordenação da instância de implantação do EXEHDA-SA.

O principal aspecto a ser observado é que o projeto inicialmente proposto em Almeida (2016), previa a contextualização como uma funcionalidade provida no módulo

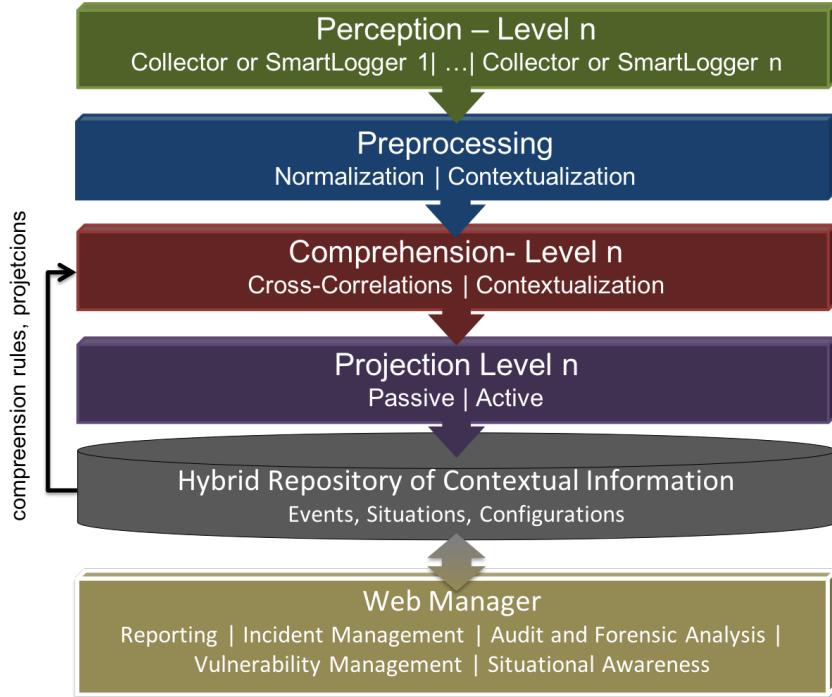


Figura 24 – Componente projetado para o EXEHDA-SA Manager

de pré-processamento, o qual era previsto apenas no componente Collector. No entanto, com a evolução da pesquisa e a concepção do EXEHDA-SA, conforme pode ser observado nas diferentes Figuras apresentadas para cada componente, a contextualização passou a integrar também o módulo de compreensão. Além disso, o EXEHDA-SA provê os módulos de pré-processamento tanto no Collector, como no SmartLogger e Manager.

4.2 Proposta Concebida

Para concepção do modelo foram utilizados diagramas de componentes elaborados em uma linguagem denominada *Technical Architecture Modeling* (TAM), a qual trata-se de diagramas baseados na *Unified Modeling Language* (UML) (80). Em especial, destaca-se o uso do elemento agente, o qual consiste de um elemento ativo capaz de executar alguma ação, podendo conter agentes, unidades de armazenamento, subsistemas, componentes e classes. A sua utilização foi definida pois este elemento permite a especificação de múltiplos agentes, escalonando/sobrepondo os elementos na imagem ou mostrando três pontos entre elementos do mesmo tipo. Seguindo o princípio de modularidade da engenharia de software (13) e visando padronizar a nomenclatura utilizada, os agentes definidos na TAM serão denominados de módulos neste texto.

A elaboração desta tese pode ser subdividida em três principais proposições:

- a principal, que apresenta o diferencial deste trabalho por meio da distribuição

da contextualização de forma transversal no ciclo MAPE-K, conforme disposto na Figura 25, bem como a adaptação do modelo de Endsley ilustrada na Figura 26;

- a consequente concepção de um modelo arquitetural com base em um conjunto de módulos propostos tendo como referência o EXEHDA-SA, e;
- a decorrente adaptação do modelo arquitetural do EXEHDA-SA, realizando tanto a especialização do módulo de projeção, bem como a simplificação dos diferentes componentes para uma única abstração.

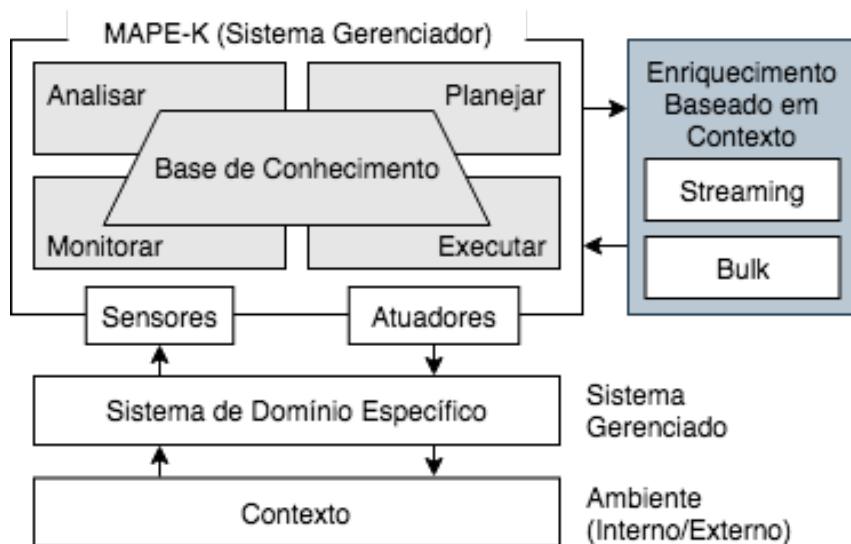


Figura 25 – Adaptação Concebida do Ciclo de *feedback* MAPE-K com Enriquecimento Baseado em Contexto

Finalmente, destaca-se na figura o módulo Enriquecimento Baseado em Contexto, o qual representa uma extensão do modelo MAPE-K apresentado pela IBM, uma vez que este apresentava o contexto apenas como uma base de informações proveniente do ambiente monitorado. Com o modelo proposto, a aquisição de informações contextuais é enfatizada em um esforço de tornar o contexto o principal componente de segurança para direcionar o comportamento de dispositivos IoT. Sendo assim, a proposta permite que dados de contexto sejam coletados tanto do próprio ambiente como de diferentes fontes, bem como nas diferentes etapas do ciclo, considerando o momento mais adequado no fluxo de tratamento dos eventos.

A Figura 25 destaca a adaptação do ciclo de *feedback* MAPE-K proposto pela IBM, anteriormente apresentado na Figura 2. Neste novo modelo concebido, é realizada a adição de um componente denominado “Enriquecimento Baseado em Contexto” que visa a contextualização dos eventos coletados pelos sensores de forma onipresente nos demais componentes.

Com o modelo proposto, a aquisição de informações contextuais é enfatizada em um esforço de tornar o contexto o principal componente de segurança para direcionar o comportamento de dispositivos IoT. Sendo assim, a proposta permite que dados de contexto sejam coletados tanto do próprio ambiente como de diferentes fontes externas, bem como nas diferentes etapas do ciclo, considerando o momento mais adequado para cada cenário no fluxo de tratamento dos eventos. Esta proposta parte da premissa que, por um lado, sabe-se que o enriquecimento é crucial para a priorização de incidentes e demais investigações, mas por outro, quando a contextualização é realizada em excesso pode poluir o ambiente dificultando a análise dos dados, além de exigir recursos de processamento, rede e armazenamento, podendo inclusive, prejudicar o desempenho de sistemas em produção como bases de dados, serviços de diretórios, entre outros serviços.

Sendo assim, este componente foi concebido com duas classificações de estratégias para o enriquecimento dos eventos:

- enriquecimento baseado em fluxo, ou *streaming enrichment*: projetado para contemplar as rápidas mudanças no ambiente, ou seja, informações dinâmicas. Por exemplo, à medida que os usuários conectam e desconectam de diferentes ativos e se autenticam para navegação web, é possível relacionar estes eventos associando através do endereço IP, todos os acessos web registrados inicialmente apenas com este IP do dispositivo junto aos dados do usuário utilizados para autenticação (por exemplo, CPF) registrados em um diferente fluxo de eventos.
- o enriquecimento baseado em lotes, ou *bulk enrichment*: visa dar suporte à coleta de informações em lote, geralmente envolvendo dados estáticos dispostos em alguma base de dados. Por exemplo, considerando o mesmo cenário anterior, seria possível ainda, adicionar a criticidade do ativo utilizado para o acesso buscando este dado de uma solução de inventário, e buscar a partir do CPF usado para autenticação, qual o nome do usuário e o seu nível de acesso em uma tecnologia de gestão de identidades para posterior análise.

Uma vez que o EXEHDA-SA foi proposto tendo como referência o modelo de Endsley de ciência de situação, também foi realizada a adaptação deste modelo para adequação à idealização de contextualização proposta nesta tese. Visando evidenciar a proposição de uma contextualização transversal, a Figura 26, apresenta a adaptação realizada no modelo, similar ao proposto para o ciclo MAPE-K, onde observa-se a interação dos demais componentes do modelo com o componente proposto.

Partindo da adaptação do modelo MAPE-K proposto, do modelo arquitetural do EXEHDA-SA e da necessidade de formalização da sua organização modular para adequação à um ciclo de *feedback*, a Figura 27 ilustra o mapeamento dos módulos

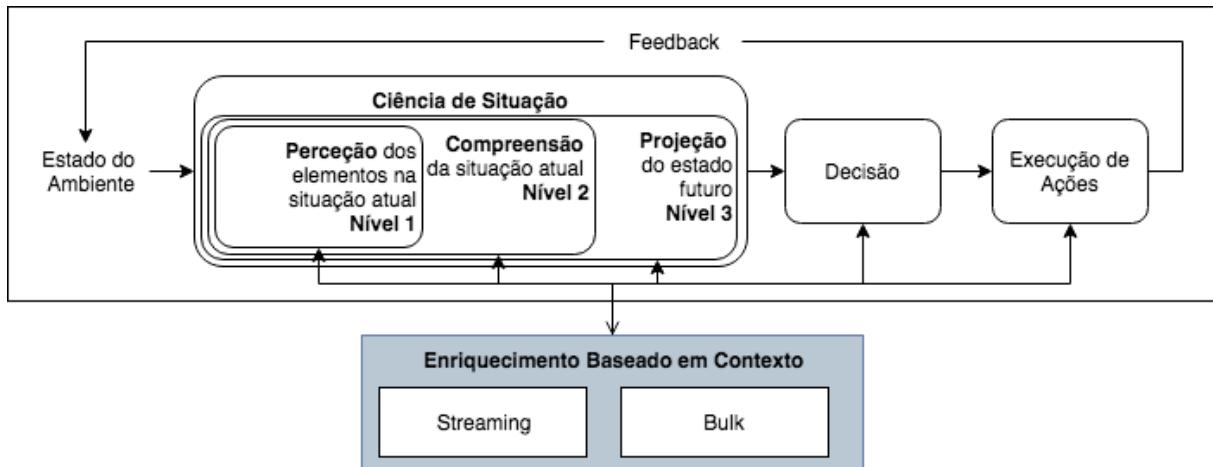


Figura 26 – Adaptação Concebida do Modelo de Endsley de Ciência de Situação com Enriquecimento Baseado em Contexto

projetados no MAPE-K sob o EXEHDA-SA. Nela, fica evidenciada a associação entre os conceitos de ciência de situação e as etapas propostas pela IBM no MAPE-K.

Observa-se na figura que a base de conhecimento é mapeada para o “Repositório Híbrido de Informações Contextuais”, o qual foi proposto e amplamente discutido em Machado et al. (2017). O módulo “Percepção”, por meio dos seus diferentes submódulos (*Log Collector*, *Status Collector*, entre outros), possibilita o atendimento das atividades propostas tanto para o componente “Sensores” quanto para o “Monitorar”. Já as atividades do componente “Analizar” do ciclo são realizadas pelos módulos de “Compreensão” e “Projeção”. O componente “Planejar” é mapeado para o módulo “Decisão”. Por sua vez, o módulo “Execução de Ações” representa os componentes “Executar” e “Atuadores” do ciclo MAPE-K. Os módulos “Execução de Ações” e “Decisão” não foram propostos inicialmente no EXEHDA-SA, porém serão descritos a seguir no modelo arquitetural concebido nesta tese.

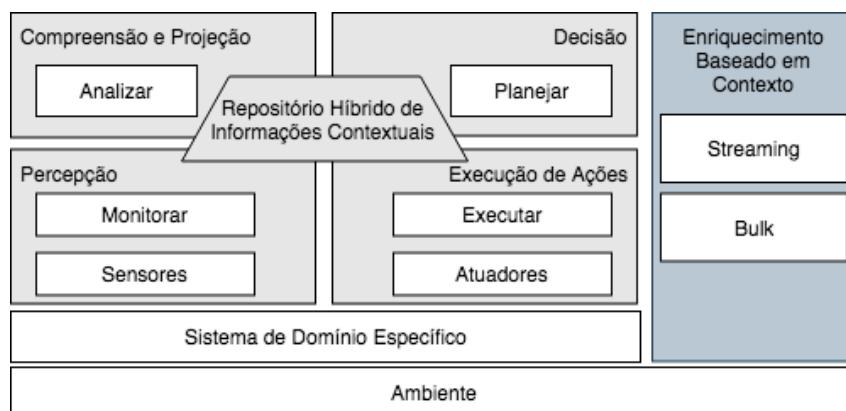


Figura 27 – Mapeamento do modelo MAPE-K proposto sob o EXEHDA-SA

Tendo discutido a adaptação dos modelos MAPE-K e de Endsley, e ilustrado o mapeamento do MAPE-K sob o EXEHDA-SA, a seguir será apresentada a concepção

do modelo arquitetural em uma estratégia modular. A Figura 28 apresenta uma visão geral dos módulos propostos no modelo arquitetural para segurança adaptativa cliente de contexto para a IoT denominado *Adaptive Security through PROgressive Context-Based Enrichment* (AS-ProCBE). Na figura, é possível verificar inicialmente o módulo de enriquecimento baseado em contexto, o qual se destaca perante os trabalhos relacionados e evidencia a principal modificação do EXEHDA-SA, o que será discutido em detalhes na sequência.

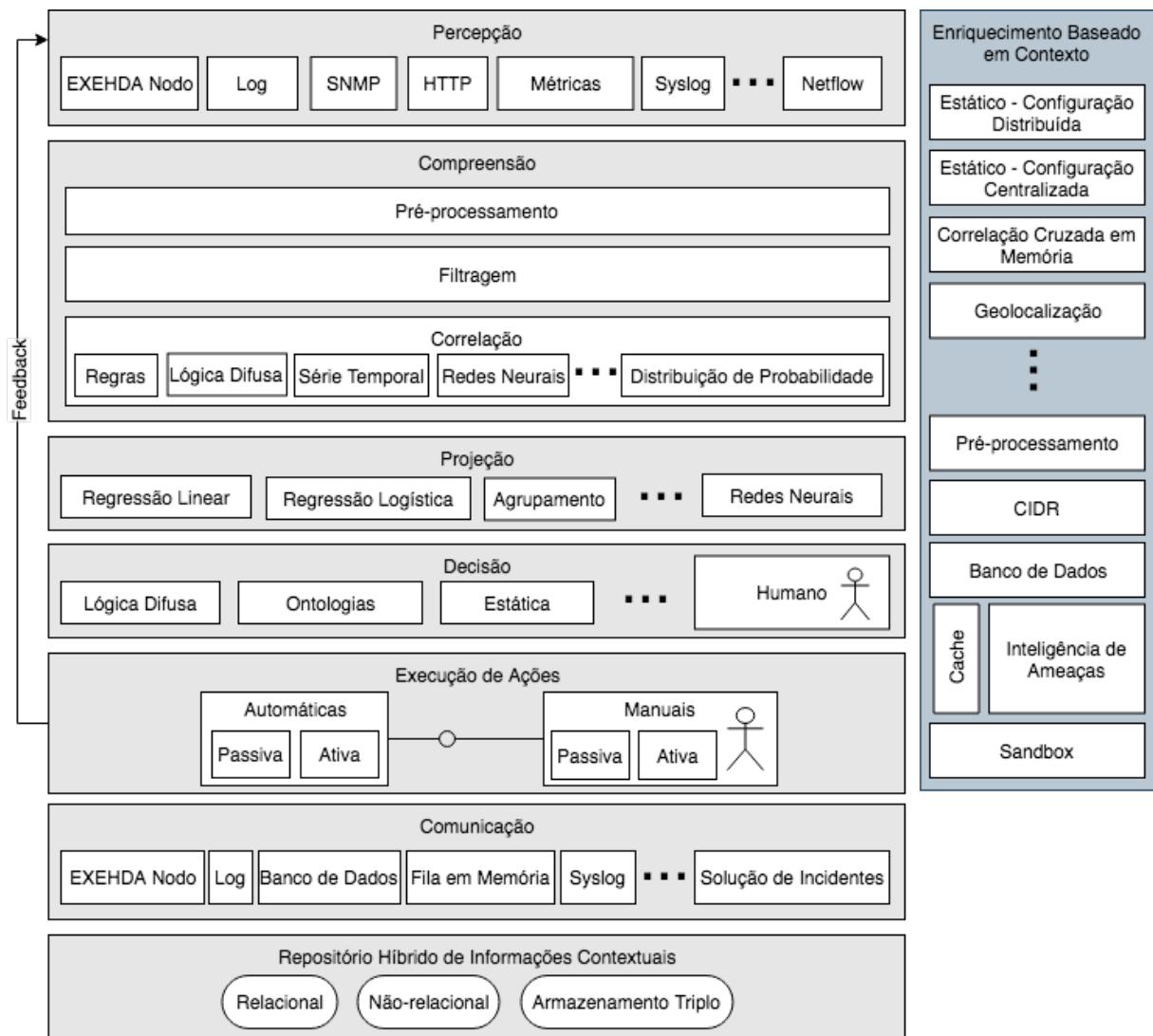


Figura 28 – Visão geral dos módulos do modelo arquitetural para segurança adaptativa cliente de contexto

Diferentemente do EXEHDA-SA, a organização arquitetural do modelo foi concebida em um único componente, o qual pode assumir os diferentes propósitos do Collector, SmartLooger e Manager, uma vez que ele foi proposto para ser modular, podendo os diferentes módulos e sub-módulos serem ativados de acordo com o perfil operacional desejado. Ou seja, uma vantagem da arquitetura modular proposta é que os módulos são implantados apenas quando necessário, o que é oportuno para dis-

positivos com restrições de hardware, como os que compõem a IoT.

Destaca-se também que cada módulo projetado neste componente é extensível e permite a alocação de seus módulos e sub-módulos em diferentes dispositivos. Além disso, a Figura 28 ilustra a adição de novos módulos que visam dividir, e especializar as ações anteriormente de responsabilidade exclusiva do módulo de projeção.

A seguir é apresentada uma discussão de cada módulo proposto no modelo arquitetural projetado.

4.2.1 Enriquecimento Baseado em Contexto

Este módulo foi proposto visando a aquisição dinâmica de informações contextuais a partir de fontes heterogêneas e distribuídas. A sua concepção tem como intuito viabilizar uma contextualização no momento oportuno, minimizando impactos, como o aumento desnecessário no tráfego da rede, e possibilitando uma contextualização distribuída na arquitetura, evitando assim limites impostos por soluções de inteligência de ameaças, ou ainda, preservando a privacidade dos dados em cenários como empresas com organização hierárquica. Além disso, com esta proposta pretende-se prevenir o excesso de informações contextuais irrelevantes, que por sua vez impactam negativamente no volume de informações processadas e armazenadas.

A dinamicidade da contextualização do AS-ProCBE disposta neste módulo comprehende que informações contextuais sejam adquiridas com base nas informações dos próprios eventos. Estas informações podem ser baseadas em dados do próprio evento coletado pelo módulo “Percepção”, bem como por dados já derivados de etapas prévias de contextualização. Por exemplo, tendo como referência eventos de tráfego web de clientes internos à infraestrutura, é possível na etapa de percepção adicionar informações sobre a localização do usuário com base no endereço IP de origem do acesso, e em caso de atividade suspeita identificada na etapa de compreensão, mais precisamente pelo módulo de correlação, seria oportuno adicionar informações de geolocalização, e de inteligência de ameaças (por exemplo, identificar se a URL acessada está em alguma *blacklist*). Ainda considerando este cenário, seria viável e interessante, na etapa de decisão, coletar de uma base de dados de usuários, o e-mail do usuário em questão para notificá-lo sobre a atividade identificada.

Desta forma, destaca-se a existência de duas estratégias de contextualização no AS-ProCBE:

- a contextualização pré-definida: corresponde a adição de informações contextuais de forma estática e pré-definida, por exemplo, todo evento coletado de determinado arquivo de log pode receber a informação contextual relativa a sua prioridade. Esta contextualização está fortemente associada ao módulo “Percepção” discutido na sequência.

- a contextualização dependente de contexto: prevista neste módulo, comprehende informações contextuais adicionadas tendo como referência os dados dos eventos, por exemplo, com base na criticidade do ativo, na prioridade do evento e na severidade de uma regra, é possível calcular o risco seguindo a indicação (5), com base na expressão:

$$\text{risco} = |(\text{criticidade} * \text{severidade} * \text{prioridade})/25|$$

Este módulo pode ser consultado por qualquer um dos demais módulos e submódulos, permitindo uma contextualização pervasiva no modelo arquitetural. Visando os objetivos mencionados, alguns submódulos foram propostos desde sua concepção:

- Pré-processamento: este submódulo, assim como o proposto no módulo de compreensão, desempenha a normalização dos dados recebidos, convertendo-os de diferentes formatos para um padrão dentro do modelo arquitetural por meio da separação dos eventos em campos, os quais serão adicionados aos eventos ou situações. Esta funcionalidade viabiliza a contextualização a partir de fontes heterogêneas, independentemente dos formatos retornados. Com isso, é possível por exemplo, coletar informações contextuais por meio de requisições web em sites da darknet, ou até mesmo em sites com publicação anônima, geralmente utilizados para divulgação de dados vazados como o <https://pastebin.com>, ou de desfiguração de sites, como o <https://zone-h.org>.
- Cache: promove o armazenamento de informações contextuais tanto em memória quanto em disco, especialmente aquelas coletadas de fontes externas e que podem ser requisitadas várias vezes, as quais podem possuir um tempo de resposta para coleta substancial. Um exemplo para o seu uso seria a verificação de determinado domínio em alguma *blacklist*, como por exemplo a <https://www.dnsbl.info>.
- Estático - Configuração Distribuída: consiste de informações adicionais de forma fixa e distribuída em cada sensor configurado, podendo consistir por exemplo, da especificação de tipo do evento coletado, da prioridade do mesmo, ou ainda da criticidade do ativo monitorado, estando mais direcionado a interação com o módulo de percepção.
- Estático - Configuração Centralizada: consiste da adição de informações semelhantes ao anterior, porém propondo uma configuração centralizada, especialmente direcionado a atender solicitações dos submódulos de pré-processamento ou correlação do módulo de Compreensão, ou ainda, do módulo de execução de ações.

- Geolocalização: adiciona informações sobre a localização geográfica dos endereços IP.
- CIDR: verifica se endereços IP em eventos podem pertencer a uma lista de faixas de rede. Vários endereços podem ser verificados em várias faixas de redes, e em caso de sucesso, informações podem ser adicionados ao evento, como por exemplo, um nome representativo de qual sub-rede o endereço pertence, o que pode auxiliar tanto na definição de onde atuar na infraestrutura de rede, como na localização física de dispositivos.
- Contextualização Cruzada em Memória: consiste da capacidade de armazenar dados em memória provenientes de diferentes fontes de eventos, para posteriormente utilizá-los para contextualização. Um possível exemplo é o armazenamento das informações de autenticação (data, endereço IP e usuário) para posteriormente cruzá-los tendo como referência o IP, com os dados de navegação web.
- Banco de Dados: consiste de um conector para coleta de dados contextuais de diferentes banco de dados, incluindo o repositório híbrido proposto, além de bases externas, por exemplo, de soluções de análise de vulnerabilidades.
- Inteligência de Ameaças: este submódulo permite a coleta de informações sobre endereços IP, nomes de domínio, endereços de e-mail, nomes, páginas da Web, listas negras de spam, metadados de arquivos e serviços como SHODAN (<https://www.shodan.io>), HaveIBeenPwned? (<https://haveibeenpwned.com>), entre outros.
- Sandbox: executáveis novos e suspeitos descobertos por diferentes soluções de segurança e possivelmente correlacionados no módulo de compreensão podem ser encaminhados para soluções de sandbox para serem examinados na busca por indicadores de risco para análise de comportamento potencialmente malicioso.

Apesar da relevância dos submódulos projetados, novamente destaca-se em especial a possibilidade de extensibilidade deste módulo que possibilita a integração com diferentes soluções de segurança, as quais podem fornecer informações contextuais relevantes para a segurança adaptativa.

4.2.2 Percepção

O módulo de Percepção é responsável por interagir com o ambiente monitorado para coleta dos eventos de segurança. Este módulo representa a primeira etapa da ciência de situação. Ele foi proposto para ser composto por vários submódulos, os

quais podem ser ativados de acordo com as necessidades. Além disso, destaca-se principalmente, que esta estratégia permite que novos submódulos sejam desenvolvidos, provendo extensibilidade e consequentemente suporte a heterogeneidade. Esta propriedade é oportuna, especialmente na IoT, uma vez que os provedores muitas vezes não seguem os protocolos padrões já estabelecidos.

Uma importante característica deste módulo é a possibilidade de operar tanto no dispositivo alvo da coleta, como de forma remota, recebendo ou coletando eventos por meio de diferentes protocolos, como o Syslog e o SNMP. A primeira opção permite que sejam coletados um maior número de dados do dispositivo. Por outro lado, a coleta remota permitirá a coleta de eventos nos quais a implementação deste módulo não é possível ou desejável, devido a limitações de hardware, consumo de energia, entre outras razões.

Considerando o escopo desta pesquisa e a área de segurança da informação, os submódulos “Log”, “SNMP”, “Syslog” e “Métricas” foram herdados do EXEHDA-SA. Além destes, outros submódulos, como o “HTTP” e o “Netflow” foram propostos.

No entanto, como principal diferença para o EXEHDA-SA, destaca-se o submódulo “EXEHDA Nodo”, o qual viabiliza o recebimento de eventos de outras instâncias do componente de software proposto, criando assim uma arquitetura hierárquica multinível. Com isto, o modelo proposto mantém a hierarquia que era anteriormente fornecida pelo componente SmartLogger. Esta estratégia flexibiliza a implantação do componente proposto por possibilitar o recebimento de eventos de outros nodos, seja por limitações de recursos computacionais ou por questões de privacidade dos dados e hierarquia da instituição.

O módulo de Percepção fornece uma capacidade similar a de filtragem, a qual permite a especificação de que apenas um subconjunto dos campos dos eventos de um sensor monitorado serão encaminhados para os próximos módulos. É possível também especificar que apenas determinados eventos registrados por um sensor serão coletados ou excluídos. Com o custo de aplicar alguma expressão regular, ela pode remover possíveis sobrecargas causadas pelo processamento, transmissão e armazenamento de eventos e campos indesejados.

4.2.3 Compreensão

A concepção do módulo de Compreensão foi proposta por meio da especificação de 3 submódulos: pré-processamento; filtragem; e correlação. Este módulo realiza a síntese e integração dos elementos desconexos identificados no nível de percepção por intermédio de diferentes estratégias, tais como, baseadas em conhecimento e em anomalias. Este nível requer a integração dessas informações para entender como isso vai impactar a segurança do ambiente computacional.

O primeiro submódulo consiste principalmente da capacidade de normalização dos

eventos recebidos, convertendo-os de diferentes formatos para um padrão dentro do modelo arquitetural por meio da separação dos eventos em campos. Esse recurso, além de permitir que as próximas etapas sejam realizadas com base nos campos criados, possibilita que o usuário realize consultas em eventos coletados de fontes variadas, independentemente do formato original. O submódulo de filtragem, possui funcionalidades equivalentes as providas na etapa de percepção - habilitando a eliminação ou seleção de eventos ou campos de eventos de acordo com a necessidade - porém, centralizando o gerenciamento das configurações, uma vez que pode tratar eventos de diferentes sensores e dispositivos.

Finalmente, o submódulo de correlação desempenha uma das principais tarefas deste módulo, realizando a união e processamento dos eventos recebidos na tentativa de identificar situações de interesse. Isso é realizado com o suporte de diferentes algoritmos, bem como dos conceitos de *Complex Event Processing* (CEP), que abordam o problema de corresponder um fluxo de eventos recebidos a um padrão quase em tempo real de forma assíncrona (33).

Seguindo as mesmas estratégias do módulo de Percepção, este também é projetado para ser modular e extensível. Essas características são propostas considerando que para cada tipo de evento podem existir diferentes estratégias de processamento, por exemplo, para análise de tráfego de rede pode ser interessante usar um algoritmo de árvores de decisão, enquanto, para eventos de log, uma abordagem baseada em regras pode ser mais oportuna. Além disso, cada tipo de evento pode ser processado em sua infraestrutura dedicada, evitando a sobrecarga com o processamento no dispositivo que gerou os eventos e permitindo uma melhor distribuição da arquitetura projetada. É possível também realizar a composição de diferentes algoritmos realizando a combinação de diferentes estratégias de processamento, executando uma abordagem híbrida.

4.2.4 Projeção

O módulo de Projeção, mantendo o alinhamento com os conceitos de ciência de situação, tem como objetivo o emprego de algoritmos que possibilitem projetar os eventos coletados adiante no tempo para determinar como isso afetará os estados futuros do ambiente operacional. Em outras palavras, ele fornece a capacidade de projetar as ações futuras dos elementos no ambiente.

É importante destacar que para atingir os objetivos propostos neste módulo, é necessário que os módulos de Percepção e Compreensão, os quais fornecem o conhecimento do estado e da dinâmica dos elementos e a identificação da situação destes, estejam habilitados em algum nível inferior do modelo arquitetural, independentemente da hierarquia do nodo.

No que tange a segurança da informação, possíveis projeções envolvem a iden-

tificação de futuros ataques cibernéticos, ou de futuras fases de um ataque em andamento. De acordo com a sofisticação dos ataques, eles podem decorrer por um longo período de tempo e envolver múltiplas atividades, como de reconhecimento, exploração e ofuscação para atingir o seu objetivo, seja de espionagem cibernética, sabotagem, entre outros. A antecipação de futuras ações de ataque é geralmente derivada das atividades maliciosas identificadas a partir da coleta (módulo de Percepção) e correlação (módulo de Compreensão) de eventos. A projeção em segurança inclui também, a possibilidade de projetar o impacto de atividades mal-intencionadas percebidas, em outros nodos através da rede, ou projetar possíveis caminhos para ataques futuros.

Tais projeções podem ser realizadas de diferentes formas, incluindo a análise de possíveis caminhos de ataque com base em vulnerabilidades da rede e do sistema, conhecimento dos padrões de comportamento dos invasores, aprendizado contínuo ou novos padrões e a capacidade de analisar e identificar as ameaças através das estratégias de ofuscação dos atacantes. Para atingir tais objetivos, entende-se que é oportuna a utilização de diferentes algoritmos, como regressão linear e logística, clusterização, redes neurais, entre outros métodos estatísticos e provenientes da inteligência artificial. Assim como no submódulo de correlação, é prevista a possibilidade de uma abordagem híbrida usufruindo-se de diferentes algoritmos aplicados em sequência.

4.2.5 Tomada de Decisão

O modelo de Endsley destaca como os conceitos de ciência de situação oferecem a base para a tomada de decisão e ações subsequentes na operação de sistemas complexos e dinâmicos. Ou seja, embora empregando exclusivamente as etapas de percepção, compreensão e projeção não possa garantir uma tomada de decisão bem-sucedida, estes submódulos suportam as informações de entrada necessárias sobre os quais as decisões são baseadas.

Sendo assim, este módulo visa selecionar uma ação de mitigação a partir de um conjunto de ações de maneira que sua utilidade, em termos de usabilidade, QoS e segurança, seja máxima entre as ações possíveis conforme os requisitos de cada situação. Para atingir este objetivo, foram propostos diferentes algoritmos, incluindo submódulos para tomada de decisão estática, onde não há incerteza ou diferentes opções de atuação, bem como estratégias automatizadas como o uso de ontologias para inferências e lógica difusa para lidar com a incerteza, e inclusive a possibilidade de interação com analistas usufruindo do raciocínio e conhecimento do mesmo. Naturalmente, assim como nos demais módulos, este também permite a extensibilidade para adoção de novos algoritmos, possibilitando o uso das diferentes opções de acordo com o tipo da situação em análise.

4.2.6 Execução de Ações

O objetivo deste módulo é evitar ocorrências de situações indesejadas anteriormente identificadas durante as etapas de compreensão e projeção. Este módulo é personalizável e extensível, fornecendo os meios para interação com a infraestrutura heterogênea da IoT.

Dois submódulos foram propostos para prover os objetivos elencados. O primeiro, ações automatizadas, foi concebido visando a execução de tarefas (comandos, scripts, códigos, coleta de contexto, entre outras) sem a interação com o analista de segurança. Já o segundo, foi projetado para possibilitar a interação do analista, seja para confirmação prévia de tarefas a serem executadas, para inclusão de contexto adicional, entre outras atividades que exijam o raciocínio humano. Com isso, destaca-se que estes submódulos podem se comunicar, propondo uma execução de ações que estabeleça um fluxo para o tratamento da situação identificada, onde sempre que possível, será exigido o mínimo de interação com o analista.

Para cada um dos submódulos, existem duas categorias possíveis de ações que podem ser configuradas:

- Passiva: são ações que não realizam modificações na infraestrutura computacional. Por exemplo, envio de alertas por e-mail, Serviço de Mensagens Curtas, do inglês *Short Message Service* (SMS), ou entrando em contato por meio de um canal que implementa mensagens confiáveis, abrir um ticket em um sistema externo, entre outros. Essa categoria de ação também permite a adição de informações contextuais, como indicadores de comprometimento. Nesse módulo específico, a contextualização é adequada para adicionar informações contextuais para situações detectadas, enquanto no módulo Compreensão a contextualização é usada como um subsídio para a detecção de novas situações.
- Ativa: esta categoria promove a interação com o ambiente distribuído sob gerência, causando a adaptação da infraestrutura. Um exemplo é a execução de comandos que podem atuar para alterar regras de firewall. Além disso, este módulo oferece a possibilidade de atuação distribuída, permitindo realizar operações remotas quando necessário.

Após a atuação, os dados sobre as situações identificadas são encaminhados para o módulo de comunicação, o qual poderá encaminhar para um novo nodo de processamento ou de armazenamento. Além disso, as situações, junto aos resultados das ações executadas são repassados a etapa de percepção, estabelecendo assim o ciclo de *feedback*.

4.2.7 Comunicação

Este módulo tem como finalidade, permitir a comunicação dos diferentes módulos por meio do oferecimento de suporte a diferentes protocolos. Ele viabiliza a comunicação entre diferentes tecnologias, como por exemplo, enviando eventos ou alertas associados a situações para soluções de monitoramento, de tratamento de incidentes de segurança e para servidores de logs externos via protocolo Syslog. Três dos submódulos projetados para comunicação devem ser destacados: o comunicador com banco de dados; o comunicador com fila de mensagens; e o comunicador com outros nodos EXEHDA.

O primeiro provê suporte aos protocolos empregados nos diferentes modelos de bancos de dados disponibilizados no repositório, permitindo assim o armazenamento dos eventos brutos e normalizados, bem como das situações identificadas e possibilitando a interação das ontologias com o armazenamento de triplas. O segundo fornece a capacidade de interação com sistemas de fila de mensagens, seja em memória ou em disco, o que é oportuno tanto para comunicação entre os módulos ou submódulos, como para possibilitar falhas nas transferências dos dados ou quedas de comunicação sem perda de dados.

Finalmente, o submódulo EXEHDA Nodo, permite a comunicação de um nodo com o módulo de Percepção do outro, formando assim uma arquitetura hierárquica multi-nível. Desta forma, no início da operação do nodo, ele solicita ao Gerente (nodo do último nível) uma lista de componentes de nível superior que ele pode usar para encaminhar eventos e situações. Com a lista configurada com mais de um componente de nível superior para enviar eventos, existem duas opções mutuamente exclusivas: (i) balanceamento de carga da saída entre os componentes de nível superior, ou; (ii) fornecer “failover” no caso de um componente de nível superior se tornar inacessível. O módulo irá armazenar os dados que precisa encaminhar quando a comunicação com componentes de nível superior falhar.

O módulo de comunicação também solicita do último nível as configurações para sua operação, incluindo sensores (logs, métricas, entre outros) a serem monitorados, e parâmetros para os demais módulos, como regras de pré-processamento e de compreensão, algoritmos para projeções e tomada de decisões, os fluxo de trabalho para atuações a serem executados.

Destaca-se por fim que, tendo em vista a possibilidade de tratamento de um elevado volume de eventos, estes podem ser compactados em diferentes níveis de compactação antes de serem encaminhados, oportuno nos casos em que os recursos da rede são escassos. Aumentar o nível de compactação reduzirá o uso da rede ao custo de aumentar o processamento.

4.2.8 Repositório Híbrido de Informações Contextuais

Visando oferecer os benefícios e minimizar as desvantagens dos diferentes modelos de banco de dados, bem como prover suporte ao uso de ontologias - a estratégia mais utilizada para implementação de bases de conhecimento no modelo MAPE-K - foi adotado nesta proposta o Repositório Híbrido de Informações Contextuais (59). Este repositório é composto de três modelos de armazenamento apresentando uma abordagem híbrida. Ele pode ser formado por vários dispositivos com hardware independente dos outros módulos, beneficiando-se de estratégias de redundância, distribuição e balanceamento de carga. Os modelos considerados são descritos abaixo:

- modelo não relacional, mais precisamente, a adoção da categoria orientado a documentos é proposta com a premissa de suportar o grande volume de dados, a variedade de formatos e a velocidade do seu tratamento, sendo direcionado ao armazenamento dos eventos brutos e normalizados, e das situações identificadas, bem como de informações contextuais. A utilização deste submódulo em nodos de diferentes níveis na arquitetura faz com que o armazenamento de eventos e situações se torne distribuído e multinível. Os eventos que não precisam ser encaminhados para o nível superior da arquitetura podem residir nas instâncias do nodo de níveis intermediários, permitindo a redução dos custos de transmissão e processamento. Há também a possibilidade de atender as restrições hierárquicas impostas ao ambiente por estratégias de negócio;
- modelo relacional, o qual é aplicado para armazenar informações como os parâmetros de configuração para a operação do modelo arquitetural, incluindo as fontes de eventos a serem coletadas, as regras de pré-processamento, as situações a serem identificadas, respectivas atuações no ambiente, entre outros;
- modelo de triplas, sendo proposto para dar suporte ao uso de ontologia.

4.3 Considerações sobre o Capítulo

+

Tabela 8 – Tabela comparativa com o PROCEN-AS

	ABIE, 2012	EVESTI, 2014	RAMOS, 2015	AMAN, 2016	EL-MALIKI, 2016	MOZZA- QUATRO, 2018	KHAN, 2018	PROCEN- AS
R1	Não	Limitada	Sim	Sim	Não	Sim	-	Sim
R2	MAPE	MAPE-K	-	MAPE-K	MAPE	MAPE-K	K	MAPE-K
R3	Não	Não	Não	Limitada	Limitada	Limitada	Prevista	Sim
R4	Não	Não	Não	Fórmula	-	Não	Não	Sim
R5	-	Conjuntos Fuzzy	-	Ontologia	-	Ontologia	Ontologia	RHIC
R6	eHealth	Ambientes Inteligentes	Não	eHealth	Redes de Sensores sem Fio	Indústria Metalúrgica	Não	Segurança
R7	Não	Não	-	Não	Não	-	-	Sim
R8	Não	Não	-	Sim	Não	-	-	Sim
R9	Usuário, QoS e Segurança	Segurança	Segurança	Usuário, QoS e Segurança	Usuário, QoS e Segurança	Segurança	Segurança	Independente
AQ	4	8	5	10	7	7	5	10

5 MÉTODO DE AVALIAÇÃO

5.1 Objetivos da Avaliação

5.2 Tecnologias Utilizadas

O núcleo do protótipo concebido foi baseado na solução Elastic Stack¹, incluindo o Elasticsearch, Logstash e Kibana, em conjunto com a plataforma Beats (Filebeat, Metricbeat e Packetbeat). Para a correlação baseada em regras, foi adotado especialmente o CorReactive², junto ao Redis e scripts personalizados. A figura 29 apresenta o mapeamento das tecnologias para cada módulo proposto, observando a existência de variações dependendo do cenário e do perfil do AS-ProCBE ao qual os módulos estão associados. Essas tecnologias foram escolhidas considerando opções *Free and Open Source Software* (FOSS) existentes, como o *Open Source SIEM* (OSSIM) da AlienVault e o SIEMONster³, e as boas práticas em segurança de infraestrutura computacional, bem como o alinhamento com os recursos do AS-ProCBE.

A plataforma Beats é responsável pela coleta dos eventos, representando parcialmente as funcionalidades projetadas no módulo de percepção quando o AS-ProCBE é implantado com o perfil Collector. Ele oferece a possibilidade de filtragem e compactação de eventos, além de comunicação criptografada, *failover* e balanceamento de carga. Filebeat abrange o submódulo “Log File”, Metricbeat o “Device Metrics” e Packetbeat pode ser usado para coleta de tráfego de rede e é uma possível extensão deste módulo. Outras extensões são desenvolvidas pela comunidade de usuários para a plataforma⁴. Essa plataforma se comunica através do protocolo Beats, que implementa o congestionamento de eventos e o controle de fluxo, características provenientes do EXEHDA-SA igualmente oportunas para o AS-ProCBE.

As funcionalidades fornecidas pelo Logstash oferecem suporte ao AS-ProCBE por sua flexibilidade no tratamento de eventos, incluindo o recebimento por meio de dife-

¹<https://www.elastic.co/products>

²<https://sourceforge.net/p/correactive/wiki/FAQ/>

³<http://siemonster.com>

⁴<https://www.elastic.co/guide/en/beats/libbeat/current/community-beats.html>



imagens/prototype-technologies.pdf

Figura 29 – Organização das tecnologias mapeadas para a abordagem modular do AS-ProCBE

rentes protocolos e o processamento destes eventos, até o envio para outras tecnologias. Como ele pode consumir eventos de várias fontes, este software é incorporado no módulo de percepção, podendo ser empregado nos diferentes perfis (Collector, SmartLogger e Manager). Pode ser uma alternativa ao Filebeat com a desvantagem de exigir Java para execução, requisitos de processamento mais altos, maior memória e configurações mais complexas. O módulo de pré-processamento também é formado pelo Logstash para normalização e contextualização de eventos por meio de filtros⁵ com opções para personalização para o ambiente desejado. Vários formatos de saída fornecidos pelo Logstash atendem aos requisitos do módulo de comunicação.

No módulo de compreensão, o Logstash encaminha eventos para o Redis. O CorReactive é responsável por buscar e executar a correlação baseada em regras nesses eventos. Os incidentes detectados podem ser contextualizados usando a anotação “@Enrichment”. Além disso, o CorReactive realiza adaptações dinâmicas com base em regras definidas que compõem tanto o módulo de decisão quanto o de execução

⁵<https://www.elastic.co/guide/en/logstash/current/filter-plugins.html>

de ações. Embora não seja validado nos estudos de caso descritos aqui, o uso do processamento híbrido é viável através da adoção do Redis (23; 3), já que outra tecnologia de processamento de eventos pode buscar do Redis as saídas da correlação do CorReactive e processá-las novamente utilizando outra técnica.

O Elasticsearch é um mecanismo de pesquisa distribuído orientado a documentos, sendo responsável pelo armazenamento de eventos e incidentes detectados no repositório HRCI. Por ser um mecanismo de pesquisa distribuído, o Elasticsearch oferece escalabilidade, resiliência, replicação e indexação de documentos para uma pesquisa textual mais rápida, útil em muitos casos, como em investigações forenses e análise de incidentes.

Finalmente, o Kibana representa parcialmente as funcionalidades fornecidas para interação entre os analistas de segurança e o repositório. Ele permite a visualização gráfica e textual do estado atual e passado do ambiente monitorado, fornecendo uma visão geral sobre a segurança da infraestrutura.

5.3 Descrição do Ambiente de Avaliação

Os estudos de caso desenvolvidos foram inspirados em uma infraestrutura de computação distribuída existente responsável por oferecer suporte a um número crescente de usuários e dispositivos da IoT. O ambiente é composto por 20 edifícios geograficamente dispersos e suportado por dois data centers, chamados InfraA e InfraB, que dependem da Internet para sua intercomunicação.

Considerando as tecnologias descritas na seção anterior, bem como os objetivos elencados, um hardware dedicado foi alocado para implantação do AS-ProCBE empregando um perfil de SmartLogger em cada uma das duas infraestruturas mencionadas anteriormente (InfraA e InfraB). Outro nodo com o perfil Manager foi implantado na InfraA para permitir que a equipe de segurança alocada fisicamente neste data center interaja com o componente independentemente da comunicação na Internet. Finalmente, foram implantados os componentes com perfil de Collector em cada dispositivo monitorado, incluindo alguns servidores de aplicações web, servidores de proxy web, entre outros. A figura 30 apresenta uma visão geral do ambiente descrito.

5.4 Cenários

A seguir serão descritos os diferentes cenários elaborados junto as métricas coletadas por meio das tecnologias adotadas para prototipação. Diferentes cenários foram projetados considerando alguns dos principais ataques realizados atualmente.

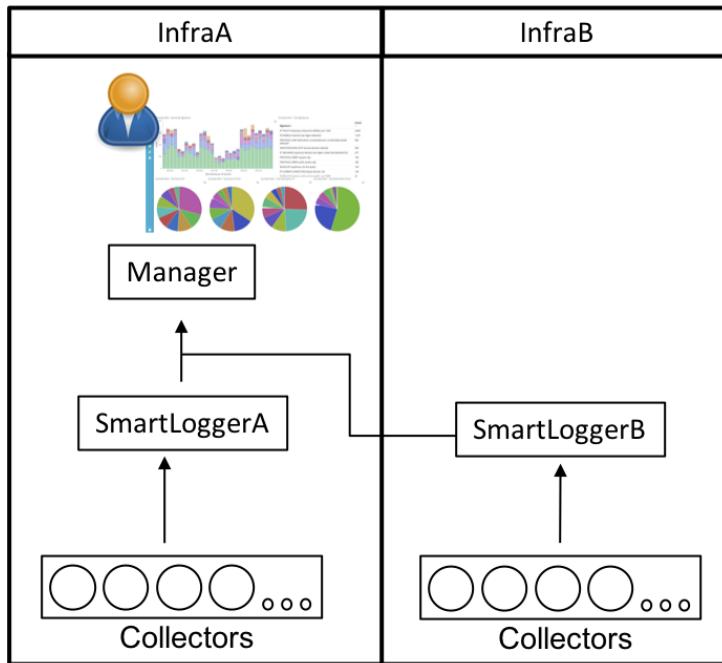


Figura 30 – Visão geral do ambiente de avaliação

5.4.1 Ataque de Injeção de Comandos

Injeção de comandos é uma forma de ataque em que comandos específicos do sistema operacional são injetados para execução por meio de um aplicativo vulnerável. Depois que os invasores encontram a vulnerabilidade em um aplicativo, geralmente eles utilizam algum comando para carregar para o dispositivo comprometido um *shell script* personalizado que será responsável por permitir acesso adicional e direto ao sistema, bem como executar os comandos desejados. Na maioria dos casos, páginas PHP dedicadas à obtenção de acesso ao shell são enviadas para o dispositivo depois que a vulnerabilidade é explorada. Tendo obtido acesso ao shell, o invasor pode monitorar todos os processos para encontrar vetores de ataque adicionais.

O cenário deste caso foi baseado em uma incidente real, onde inicialmente uma vulnerabilidade em um servidor web com a aplicação Wordpress (WP) foi explorada. Através da vulnerabilidade, os atacantes inseriram e executaram scripts no diretório /tmp, visto que este possuía permissões de escrita e execução para todos os usuários, inclusive para o www-data (usuário que o servidor web Apache estava executando). Dentre outras atividades, os scripts realizaram varreduras de portas e vulnerabilidades na rede, além de inúmeras requisições web que passaram pelo servidor de proxy web.

Visando a simulação deste cenário e a reprodução do ambiente, dois servidores foram alocados na InfraB, um para representar a instalação do WP e outro para o proxy web, ambos com o AS-ProCBE no perfil Collector implantado. Estes, encaminham os eventos monitorados para o SmartLoggerB, conforme previamente ilustrado na Figura 30.

Cada Collector foi implantado apenas com o módulo de percepção ativo explorando o Filebeat, realizando o monitoramento dos logs oportunos para o caso. Para o servidor proxy, destaca-se a coleta dos eventos registrados em /var/log/squid/access.log, enquanto que para o servidor WP foram coletados os eventos em /var/log/apache2/. No que tange a contextualização, foi realizada a adição do campo “tipo do evento”, visto que o mesmo foi necessário para a divisão dos eventos em diferentes tópicos no Kafka. Também foi adicionado o campo referente a criticidade do ativo, visto que ele será utilizado posteriormente para o cálculo do risco das situações identificadas.

O SmartLoggerB no submódulo de pré-processamento, empregado pelo logstash, foi configurado para realizar a conversão de determinados campos dos logs do squid para inteiro, e converter o tempo de resposta de milissegundos (padrão registrado no log) para segundos (padrão facilmente tratado pelo kibana). Nesta etapa, também é adicionado o campo de prioridade dos eventos. Com base no endereço IP de origem do acesso dos logs do proxy squid, foi configurado plugin CIDR para adicionar a zona/prédio/unidade de origem do acesso, oportuno para visualizar nos gráficos do kibana os locais de maior tráfego. Neste caso, como a origem do acesso tratava-se de um dispositivo na DMZ, a execução do plugin aggregate (que será explorado no cenário seguinte) não foi empregada.

Na sequência, o módulo de correlação foi configurado com a regra disposta na Figura ??, a qual visa identificar a existência de um número elevado de requisições ao serviço de proxy em um intervalo curto de tempo. Caso isto ocorra para uma máquina da DMZ, o motor de correlação empregado pelo CorReactive passará para a etapa de decisão, realizando a busca no dados de inventário do dispositivo, identificando a criticidade do ativo para então realizar o cálculo do risco (risco = ...). Este enriquecimento de dados foi possibilitado pelo CorReactive por meio da anotação @Enrich utilizando o tipo “window”, e pelo armazenamento destes dados em memória utilizando a anotação @Persist.

Finalmente, no módulo de atuação, devido a contextualização identificar o dispositivo como pertencente a DMZ, um comando de bloqueio das requisições de saída e entrada a partir deste endereço IP é realizado no firewall da DMZ. Além disso, é realizada uma busca no HRCI por eventos com o mesmo endereço IP do servidor WP para verificar a possibilidade de acesso à outros servidor bem como movimentos laterais. Em um esforço de coletar algumas evidências, antes do bloqueio no firewall também foram coletados os processos em execução e as conexões estabelecidas no dispositivo comprometido. Também é verificada a possibilidade das URLs requisitadas estarem em bases de inteligência de ameaças.

5.4.2 Download de Arquivo Suspeito

Este cenário foi inspirado no *Webcast* promovido pelo Instituto SANS intitulado “New SIEM Poster - Architecture, Enrichment, and More”⁶. O mesmo apresenta como estudo de caso dois alertas, um primeiro de atividade considerada normal, e o segundo como suspeita. Para chegar nesta conclusão é enfatizado a importância do enriquecimento dos eventos com informações contextuais.

O ambiente de avaliação foi projetado por meio do uso de um servidor de autenticação para navegação web, um servidor de proxy que registra as requisições web das estações, um servidor de *Network Intrusion Detection System* (NIDS) e uma estação Windows. Estes dispositivos foram alocados na InfraA e o restante do ambiente segue a descrição da Figura 30, com destaque para o SmartLoggerA que será detalhado na sequência.

A implantação do AS-ProCBE nos dispositivos mencionados acima, com exceção do SmartLoggerA, segue o perfil operacional de um Collector, conforme ilustrado na Figura 31.

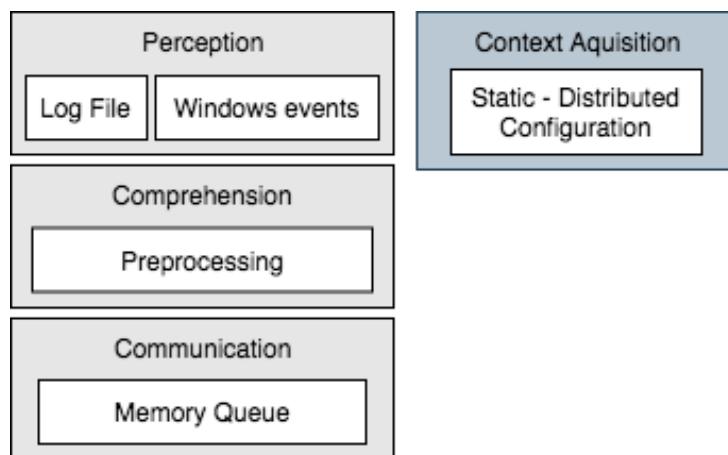


Figura 31 – Abstração da implantação do AS-ProCBE com perfil de Collector

Tanto o servidor de proxy web quanto o servidor de autenticação utilizam o módulo de percepção para realizar a coleta dos principais eventos para este cenário por meio do sub-módulo “Log File”. No proxy web é realizado o monitoramento dos arquivos onde todos os eventos relativos aos acessos das estações são registrados, mais especificamente o /var/log/squid/access.log. Já para a autenticação, são monitorados os eventos com sucesso, sendo principalmente registrados em /var/log/portal/auth.log os campos referentes à data, endereço IP da estação, Cadastro de Pessoa Física (CPF) e informações do navegador utilizado.

Quanto a contextualização, destaca-se a utilização do sub-módulo de contexto estático via configuração distribuída, o qual é responsável pela adição do campo “type”

⁶<https://www.sans.org/webcasts/learn-about-siem-poster-architecture-enrichment-111740>

que representa o tipo do evento coletado, sendo geralmente empregado ao menos um tipo diferente por arquivo ou fonte de eventos monitorado. Para estes dispositivos, o módulo de compreensão não foi utilizado, sendo os eventos encaminhados diretamente para o módulo de comunicação, que envia os dados para uma fila em memória (sub-módulo “Memory Queue”). Neste momento, o campo “type” é utilizado para determinar a fila em que os eventos coletados serão armazenados para posterior consumo.

O AS-ProCBE no servidor de NIDS também foi configurado com perfil operacional de Collector utilizando para percepção o “Log File” para realizar a coleta dos eventos registrados em /var/log/suricata/eve.json. A aquisição de contexto, além de realizar a adição do campo “type”, também identifica o valor de severidade registrada nos alertas do Suricata e cria um campo específico que será utilizado para cálculo do risco posteriormente. Neste caso, observa-se que os eventos gerados pelo suricata foram configurados para serem gerados no formato *JavaScript Object Notation* (JSON). Desta forma, se fez oportuno empregar o módulo de compreensão para realizar o pré-processamento e decodificar o JSON no próprio dispositivo. Apesar de a decodificação deste formato no Collector possuir baixo impacto quanto ao consumo de recursos, isto foi realizado pois o volume de eventos geralmente registrados em NIDS é consideravelmente alto, logo, a tarefa de divisão dos eventos em campos realizada pelo pré-processamento local desonera o SmartLogger que será responsável por outras atividades. Finalmente, os eventos são encaminhados para o módulo de comunicação realizar o envio dos eventos para a fila em memória.

Na estação Windows foi realizada a instalação do Sysmon, bem como do Winlogbeat, responsável pela implementação do submódulo “Windows events”. Como contextualização, é realizada a adição do campo “type” com o valor fixo “winevents”. O AS-ProCBE para este dispositivo também emprega o pré-processamento local dos eventos realizando transformações dos campos para seguir os padrões estabelecidos pelo *Elastic Common Schema* (ECS⁷), além de enviar os dados para a fila em memória, via módulo de comunicação, já no formato JSON.

Todos os eventos enviados para as diferentes filas mapeadas pelo campo “type” são armazenados e consumidos pelo SmartLoggerA no módulo de percepção. Para cada tipo diferente, um fluxo de tratamento é realizado. A figura 32 ilustra os módulos do AS-ProCBE utilizados para implantação do SmartLoggerA.

Iniciando pelos logs registrados no portal de autenticação, a primeira etapa realizada é a normalização dos eventos pelo submódulo de pré-processamento. Na sequência, o submódulo de aquisição de contexto “UserAgent” identifica os detalhes do sistema operacional e navegador web utilizados com base no campo “agent”, criando novos campos para estes dados. Os eventos são então encaminhados para o

⁷<https://www.elastic.co/guide/en/ecs/1.2/ecs-reference.html>

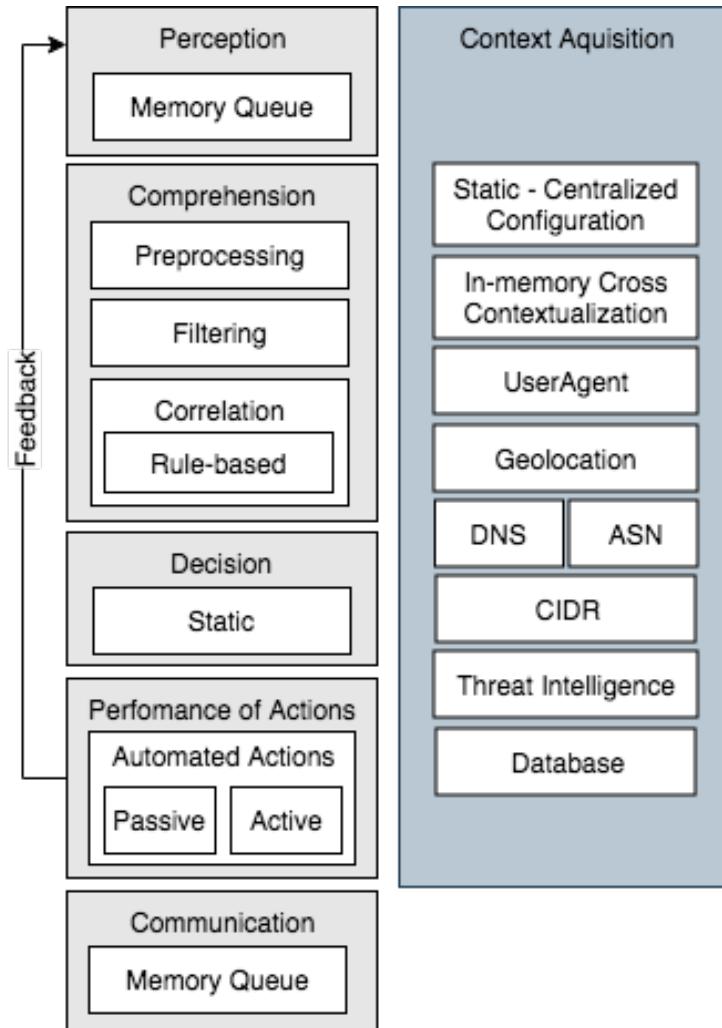


Figura 32 – Abstração da implantação do AS-ProCBE com perfil de SmartLogger

“In-memory Cross Contextualization”, o qual armazena em memória um mapeamento entre o endereço IP atribuído ao dispositivo do usuário e o CPF utilizado para autenticação. Os eventos também são encaminhados para correlação e para o módulo de comunicação. Este último enviará os eventos já normalizados e contextualizados para a fila em memória.

Os logs produzidos pelo suricata já são recebidos pelo módulo de compreensão normalizados. Sendo assim, ele inicia o enriquecimento dos eventos com informações contextuais. Primeiramente é aplicada a correlação cruzada em memória, onde o endereço IP registrado em log é confrontado com os dados previamente coletados da autenticação na busca pelo campo CPF, ou seja, ocorre a associação entre os alertas do NIDS ao usuário. Na sequência, é aplicado o submódulo CIDR aos campos de endereço IP de origem e de destino da requisição. Desta forma é identificado o fluxo do acesso, seja tráfego de saída ou de entrada, e isto é armazenado no campo “traffic_flow”. Além disso, para o endereço da rede interna, campos que descriminam o valor do ativo (“asset_value”), o campus onde o mesmo está alocado (“campus”), e

a identificação da faixa de rede (“netname”) são adicionados.

A partir deste momento, com base no campo “traffic_flow”, os submódulos para contextualizações referentes a geolocalização, ao *Autonomous System Number* (ASN) e ao *Domain Name System* (DNS) são aplicados para o campo do endereço IP externo. A Figura 33 apresenta um exemplo de evento com os novos campos adicionados associados à estes submódulos. Apesar de neste momento ser possível visualizar um comportamento incomum, uma vez que o ASN indica a entidade como sendo da Amazon e o DNS apresenta o domínio “trackmypackage-com.biz”, ainda assim é possível adicionar contexto para reforçar esta suspeita.



Figura 33 – Evento após a contextualização por DNS, ASN e geolocalização

Nesta etapa é aplicada uma das principais contextualizações por meio do submódulo de inteligência de ameaças. Para este caso, serão aplicados os Indicadores de Comprometimento, do inglês Indicators Of Compromise (IOC), o que ocorre confrontando as URLs, endereços IPs, domínios e hashes com diferentes bases. Para este estudo, tanto o endereço IP externo quanto o domínio foram aplicados, apresentando como resultado a adição dos campos no evento conforme apresentado na Figura 34.

Percebesse a partir dos novos campos que, tanto o endereço IP quanto a URL, foram identificadas em bases de inteligência de ameaças. Este evento é encaminhado para o módulo de correlação que detecta a situação de interesse visto a existência dos campos associados aos IOC (regra disponibilizada na Figura 35). Como contextualização configurada nesta etapa, os dados referentes ao nome do usuário e e-mail são adicionados ao evento para subsidiar a etapa de execução de ações.



Figura 34 – Evento do NIDS após a contextualização por IOC



Figura 35 – Regra de correlação e contextualização para evento com IOC

Na sequência, o módulo de decisão foi configurado para executar uma sequência estática de tarefas. Desta forma, o módulo de execução de ações realiza o envio de e-mail ao usuário, utilizando as informações contextuais sobre o endereço de e-mail e nome para personalizar a mensagem. Além disso, foi configurado a coleta

de dados sobre o inventário do dispositivo, incluindo local físico de alocação, unidade organizacional e responsável, os quais podem ser úteis para determinar ações futuras, como direcionar programas de conscientização em segurança da informação.

Ainda no módulo de atuação, de forma hipotética, uma vez que o nível de confiança do alerta é razoável em decorrência da identificação do endereço IP e do domínio como IOC, seria possível realizar uma adaptação no ambiente pela configuração de VLAN para colocar em quarentena o dispositivo. Para o ambiente de avaliação foi realizada a adaptação por meio de um regra no *firewall* bloqueando o tráfego. Por fim, os dados referentes ao nome do processo que originou a requisição e o nome do arquivo baixado - dados previamente coletados pelo Sysmon - são adicionados ao evento para auxiliar na compreensão do incidente.

Todos os eventos coletados junto as informações contextuais foram encaminhados ao módulo de comunicação e posteriormente consumidos e processados pelo Manager da InfraA.

5.5 Considerações sobre o Capítulo

6 CONSIDERAÇÕES FINAIS

O presente trabalho buscou apresentar uma revisão conceitual sobre segurança adaptativa ciente de contexto para IoT. No decorrer da revisão foi possível perceber os diferentes desafios existentes na IoT que potencializam a segurança da informação enquanto estratégia para viabilização dos inúmeros benefícios decorrentes deste paradigma.

Com isso, foi encaminhada a necessidade de modelos para segurança adaptativa que promovam a adaptação dos mecanismos de segurança de forma que as mudanças aplicadas não prejudiquem a eficiência, a flexibilidade, a confiabilidade e a segurança dos ambientes da IoT. Tendo em vista a natureza pervasiva, distribuída e dinâmica da IoT, as informações contextuais devem ser um dos principais componentes para conduzir o comportamento dos dispositivos, a fim de tornar as decisões de segurança adequadas ao ambiente.

Além disso, com a revisão sistemática da literatura realizada neste trabalho, foi possível identificar que atualmente existem várias abordagens para segurança adaptativa. No entanto, muitas delas se concentram em objetivos de segurança específicos (39; 89; 55). Percebe-se também a falta no tratamento completo do ciclo de *feedback*, ou seja, as abordagens não definem todo o ciclo MAPE-K. Além disso, as arquiteturas genéricas analisadas não detalham os métodos usados em cada componente, o que dificulta a reutilização e a extensibilidade das abordagens propostas. Com a revisão sistemática realizada neste trabalho, foi possível identificar que apesar dos avanços nas pesquisas em segurança adaptativa em diferentes frentes, os desafios mencionados continuam em aberto, existindo ainda poucas abordagens genéricas que detalhem a sua concepção, prototipação e estratégias de avaliação.

6.1 Contribuições

Nessa seção são apresentadas as principais contribuições esperadas com a concepção e o desenvolvimento da proposta apresentada.

6.1.1 Com Relação ao Estado da Arte

Considerando os desafios da IoT, bem como as limitações dos projetos identificados como estado da arte, no Capítulo 4 foi apresentada a proposta concebida, a qual possui como diferencial, o seu módulo de aquisição de informações contextuais. Este módulo destaca-se por possibilitar uma contextualização dos eventos utilizando fontes heterogêneas de contexto, bem como por sua integração com o modelo arquitetural como um todo, fornecendo assim a aquisição de contexto no momento oportuno, permitindo aos analistas analisarem criticamente o ambiente e definirem quando e como ocorrerá a contextualização considerando desafios como volume do tráfego da rede, capacidades de processamento e memória, escalabilidade, entre outros.

Mostrando o alinhamento da proposta com os objetivos elencados, bem como com o tratamento de algumas das limitações destacadas nos trabalhos selecionados, outros aspectos importantes a serem destacados da proposta são:

- (i) atendimento de todas as etapas do ciclo de *feedback* MAPE-K, o qual é evidenciado especialmente pelo mapeamento do modelo arquitetural proposto sobre o ciclo (vide Figura ??);
- (ii) a flexibilidade é provida, tanto pela possibilidade de implantar a arquitetura de diferentes formas, visto que os módulos podem ser habilitados conforme a necessidade, bem como pela extensibilidade do modelo;
- (iii) coleta de informações contextuais a partir de fontes heterogêneas, o que é proposto pela concepção de um módulo exclusivamente com esta finalidade, e reforçado em específico pelo submódulo de normalização que possibilita que os diferentes formatos de contextos adquiridos sejam convertidos para um formato padrão dentro do modelo proposto;
- (iv) distribuição da contextualização nos diferentes módulos, funcionalidade que é fornecida pela capacidade de interação dos diferentes módulos com o de aquisição de informações contextuais a qualquer momento;
- (v) e finalmente, a última característica elencada é apoiada no EXEHDA-SA, modelo arquitetural no qual esta proposta foi baseada, e que caracteriza-se por uma estratégia de prototipação que permite a replicação de seus cenários de avaliação, o que será constantemente buscado na continuidade desta pesquisa, mantendo um alinhamento entre os modelos.

6.1.2 Com Relação à Divulgação de Resultados Parciais

Durante o desenvolvimento deste trabalho foram publicados alguns artigos em periódicos e anais de congresso, dos quais são destacados os seguintes:

- ALMEIDA, R. B.; MACHADO, R. S.; YAMIN, A. C.; PERNAS, A. M. Revisão Sistemática sobre Segurança Adaptativa Ciente de Contexto para a Internet das Coisas In: **Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos, 2019, Gramado/RS.** - Este trabalho teve como objetivos apresentar os conceitos sobre segurança adaptativa ciente de contexto para IoT, e especialmente, realizar uma revisão sistemática da literatura buscando identificar o estado da arte, para na sequência, desenvolver uma análise crítica sobre os trabalhos identificados, em um esforço para elencar oportunidades de pesquisa.
- ALMEIDA, R. B.; JUNES, V.R.C; MACHADO, R. S.; ROSA, D. Y. L.; DONATO, L. M.; YAMIN, A. C.; PERNAS, A. M. A distributed event-driven architectural model based on situational awareness applied on internet of things. **Information and Software Technology, 2019.** - Tendo em vista que os ambientes da IoT são compostos de inúmeros dispositivos heterogêneos capazes de gerar uma quantidade significativa de eventos, é necessário integrar, processar e reagir a eventos em tempo de execução. Com isto, este artigo teve como objetivo a concepção de um modelo arquitetura baseado nos conceitos de ciência de situação para suportar as crescentes demandas de escalabilidade, flexibilidade, autonomia e heterogeneidade no processamento de eventos de IoT. Dentre as funcionalidades oferecidas pelo modelo, destaca-se a coleta de eventos de dispositivos da IoT, o processamento híbrido e recursos de reação customizados e dinâmicos. As contribuições foram evidenciadas por meio de experimentos realizados em um protótipo implementado utilizando tecnologias consolidadas de código aberto e livre. Os experimentos são baseados em cinco estudos de caso, onde cada um avalia um cenário para demandas da IoT. Por meio desses estudos de caso que foram propostos na área de segurança da informação, foi possível demonstrar a viabilidade do modelo para implantação em ambientes de produção da IoT. Além disso, o modelo é capaz de operar em diferentes cenários devido à modularidade de cada componente e sua consequente extensibilidade.
- ALMEIDA, R. B.; JUNES, V.R.C; MACHADO, R. S.; ROSA, D. Y. L.; YAMIN, A. C.; DONATO, L. M.; PERNAS, A. M. A hierarchical architectural model for network security exploring situational awareness In: the 34th ACM/SIGAPP Symposium, 2019, Limassol. **Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing - SAC '19.** New York: ACM Press, 2019. - Neste artigo é proposto um modelo arquitetural que tem como principal motivação o fato de que muitas vezes, as organizações utilizam tecnologias de segurança de propósitos específicos, o que implica na falta de uma visão holística sobre os eventos de segurança. Desta forma, o modelo é inspirado em sistemas SIEM e nos conceitos de ciência de situação, sendo composto por três componentes modulares

que se comunicam promovendo uma arquitetura hierárquica multinível. O modelo oferece recursos como coleta de eventos, processamento híbrido e utiliza uma abordagem híbrida de armazenamento de dados contextuais. Com o propósito de avaliar o modelo, quatro estudos de caso foram desenvolvidos para validar a visão holística dos eventos de segurança, bem como as características de flexibilidade, autonomia, escalabilidade e suporte à heterogeneidade.

- ALMEIDA, R. B.; MACHADO, R. S. ; ROSA, D. Y. L.; PERNAS, A. M. ; YAMIN, A. C. . Hybrid approach to provide situational awareness for information security in computational environments. In: **Conferência Latino-americana de Informática, 2018, São Paulo**. SLMDI - Simpósio Latino-Americano de Gerenciamento de Dados e Informação, 2018. - Este artigo apresenta uma abordagem para fornecer ciência de situação para segurança em ambientes computacionais, produzindo uma visão holística sobre os eventos. A abordagem explora diferentes recursos desde a aquisição dos eventos, um processamento híbrido, uma estratégia para armazenamento de dados híbrida e a atuação resultante. A abordagem proposta foi avaliada por meio de um protótipo, o qual foi aplicado em três casos de uso, mostrando-se estável e flexível na provisão de aspectos de segurança em ambientes computacionais.

6.2 Cronograma de Atividades

Para a continuidade do desenvolvimento desta pesquisa, está prevista a realização de uma série de atividades, as quais são enumeradas a seguir. A Tabela 9 apresenta as atividades em uma perspectiva temporal, incluindo as que já foram realizadas, as que estão em andamento, e as que serão desenvolvidas até a conclusão da tese.

1. estudar e sistematizar os principais temas relacionados à tese;
2. realizar a revisão sistemática da literatura;
3. determinar qual frente de pesquisa será considerada;
4. considerando o desafio escolhido, estudar as possíveis estratégias a serem consideradas;
5. realizar a concepção de uma estratégia para o desafio;
6. definir os cenários de uso, prototipar e avaliar os resultados alcançados;
7. reavaliar os trabalhos relacionados comparando-os com a pesquisa desenvolvida;
8. elaborar artigos sobre o tema da tese;

9. escrita da tese;

10. defesa da tese.

Tabela 9 – Cronograma de atividades

REFERÊNCIAS

- [1] 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).
- [2] ABIE, H. et al. Self-Healing and Secure Adaptive Messaging Middleware for Business Critical Systems. **International Journal on Advances in Security**, [S.I.], v.3, 2010.
- [3] ABUGHOFA, T.; ZULKERNINE, F. Towards online graph processing with spark streaming. In: IEEE INTERNATIONAL CONFERENCE ON BIG DATA (BIG DATA), 2017., 2017. **Anais...** [S.I.: s.n.], 2017. p.2787–2794.
- [4] ALABA, F. A.; OTHMAN, M.; HASHEM, I. A. T.; ALOTAIBI, F. Internet of Things security: A survey. **Journal of Network and Computer Applications**, [S.I.], v.88, p.10 – 28, 2017.
- [5] ALIENVAULT. **AlienVault Unified Security Management™ Solution - Complete. Simple. Affordable - Correlation Reference Guide**. [S.I.]: AlienVault, 2015.
- [6] ALIENVAULT. OSSIM: The Open Source SIEM | AlienVault. Disponível em: <<https://www.alienvault.com/products/ossim>>, acesso em: 11 feb 2018.
- [7] ALMEIDA, R. **EXEHDA-USM**: uma arquitetura hierárquica multinível ciente de situação aplicada a segurança da informação. 2016. Dissertação (Mestrado em Ciência da Computação) — Universidade Federal de Pelotas - UFPel, Pelotas, RS.
- [8] ALMEIDA, R. B. et al. A distributed event-driven architectural model based on situational awareness applied on internet of things. **Information and Software Technology**, [S.I.], v.111, p.144 – 158, 2019.

- [9] AMAN, W. **Adaptive Security in the Internet of Things**. 2016. Tese (Doutorado em Ciéncia da Computação) — Norwegian University of Science and Technology, Trondheim, Norway.
- [10] 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.I.], p.7–15, 2014. cited By 6.
- [11] AMAN, W.; SNEKKENES, E. EDAS: An Evaluation Prototype for Autonomic Event-Driven Adaptive Security in the Internet of Things. **Future Internet**, [S.I.], v.7, n.3, p.225–256, 2015.
- [12] ASHTON, K. That 'Internet of Things' Thing. **RFID Journal**, [S.I.], June 2009.
- [13] BASS, L.; CLEMENTS, P.; KAZMAN, R. **Software Architecture in Practice**. 3.ed. [S.I.]: Addison-Wesley Professional, 2012.
- [14] BATES, J. **John Bates of Progress explains how complex event processing works and how it can simplify the use of algorithms for finding and capturing trading opportunities**. [S.I.]: Fix Global Trading, 2012.
- [15] 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.
- [16] 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.
- [17] BOUZEGHOUB, A.; DO, K. N.; LECOCQ, C. A Situation-Based Delivery of Learning Resources in Pervasive Learning. In: LECTURE NOTES IN COMPUTER SCIENCE, SPRINGER- VERLAG, BERLIN, HEIDELBERG, 2007. **Anais...** [S.I.: s.n.], 2007.
- [18] BRÉZILLON, P. Context in problem solving: a survey. **Knowl. Eng. Rev.**, New York, NY, USA, v.14, n.1, p.47–80, May 1999.
- [19] BRÉZILLON, P.; ARAUJO, R. M. Reinforcing Shared Context to Improve Collaboration. **Revue d Intelligence Artificielle**, [S.I.], v.19, n.3, p.537–556, 2005.
- [20] BRUN, Y. et al. Software Engineering for Self-Adaptive Systems. In: CHENG, B. H. et al. (Ed.). **Software Engineering for Self-Adaptive Systems**. Berlin, Heidelberg: Springer-Verlag, 2009. p.48–70.

- [21] 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.I.: s.n.], 2016. p.384–393.
- [22] CERT.BR. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil - FAQ: Perguntas Frequentes ao CERT.br. Disponível em: <<http://www.cert.br/docs/certbr-faq.html#6>>, acesso em: 18 nov 2015.
- [23] CHINTAPALLI, S. et al. Benchmarking Streaming Computation Engines: Storm, Flink and Spark Streaming. In: IEEE INTERNATIONAL PARALLEL AND DISTRIBUTED PROCESSING SYMPOSIUM WORKSHOPS (IPDPSW), 2016., 2016. **Anais...** [S.I.: s.n.], 2016. p.1789–1792.
- [24] CHUVAKIN, A.; SCHMIDT, K.; PHILLIPS, C. **Logging and Log Management:** The Authoritative Guide to Dealing with Syslog, Audit Logs, Events, Alerts and other IT ‘Noise’. [S.I.]: Elsevier Science, 2012.
- [25] CLEMENTE, R. G. **UMA ARQUITETURA PARA PROCESSAMENTO DE EVENTOS DE LOG EM TEMPO REAL.** 2008. Mestrado em Informática — Pontifícia Universidade Católica do Rio de Janeiro - PUC-RIO.
- [26] DEY, A. K. Understanding and Using Context. **Personal and Ubiquitous Computing**, [S.I.], v.5, p.4–7, 2001.
- [27] 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.
- [28] DOBSON, S. et al. A Survey of Autonomic Communications. **ACM Trans. Auton. Adapt. Syst.**, New York, NY, USA, v.1, n.2, p.223–259, Dec. 2006.
- [29] EL MALIKI, T. **Security adaptation in highly dynamic wireless networks.** 2014. Tese (Doutorado em Ciência da Computação) — Université de Genève.
- [30] 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.I.: s.n.], 2016. p.206–211.
- [31] ENDSLEY, M. R. Design and Evaluation for Situation Awareness Enhancement. **Proceedings of the Human Factors Society Annual Meeting**, [S.I.], v.32, n.2, p.97–101, 1988.

- [32] ENDSLEY, M. R. **Designing for Situation Awareness**: An Approach to User-Centered Design, Second Edition. 2nd.ed. Boca Raton, FL, USA: CRC Press, Inc., 2011.
- [33] ETZION, O.; NIBLETT, P. **Event Processing in Action**. 1st.ed. Greenwich, CT, USA: Manning Publications Co., 2010.
- [34] EVESTI, A. **Adaptive Security in Smart Spaces**. 2014. Tese (Doutorado em Ciência da Computação) — University of Oulu.
- [35] EVESTI, A.; FRANTTI, T. Situational Awareness for security adaptation in Industrial Control Systems. In: SEVENTH INTERNATIONAL CONFERENCE ON UBIQUITOUS AND FUTURE NETWORKS, 2015., 2015. **Anais...** [S.I.: s.n.], 2015. p.1–6.
- [36] EVESTI, A.; OVASKA, E. Comparison of adaptive information security approaches. **ISRN Artificial Intelligence**, [S.I.], v.2013, 2013.
- [37] EVESTI, A.; SUOMALAINEN, J.; OVASKA, E. Architecture and Knowledge-Driven Self-Adaptive Security in Smart Space. **Computers**, [S.I.], v.2, n.1, p.34–66, 2013.
- [38] EVESTI, A.; TUTKIMUSKESKUS, V. teknillinen. **Adaptive Security in Smart Spaces**. [S.I.]: VTT, 2013. (VTT science).
- [39] 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.I.], 2016. cited By 0.
- [40] FINK, A. **Conducting Research Literature Reviews**: From the Internet to Paper. [S.I.]: SAGE Publications, 2010.
- [41] GANEK, A. G.; CORBI, T. A. The dawning of the autonomic computing era. **IBM Systems Journal**, [S.I.], v.42, n.1, p.5–18, 2003.
- [42] GHORBANI, A.; LU, W.; TAVALLAEE, M. **Network Intrusion Detection and Prevention**: Concepts and Techniques. [S.I.]: Springer, 2010. (Advances in Information Security).
- [43] GIUSTO, D.; IERA, A.; MORABITO, G.; ATZORI, L. **The Internet of Things**: 20th Tyrrhenian Workshop on Digital Communications. [S.I.]: Springer New York, 2010.
- [44] 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.

- [45] HEIMERL, J.-L. Effective Security Requires Context. Disponível em: <<http://www.securityweek.com/effective-security-requires-context>>, acesso em: 29 jan 2018.
- [46] HOSSEINZADEH, S. et al. Diversification and obfuscation techniques for software security: A systematic literature review. **Information and Software Technology**, ELSEVIER, 2018.
- [47] HP. Disponível em: <<http://files.asset.microfocus.com/4aa5-4759/en/4aa5-4759.pdf>>, Hewlett Packard Enterprise - Internet of things research study. Acesso em janeiro de 2018.
- [48] HU, W. et al. Online Adaboost-Based Parameterized Methods for Dynamic Distributed Network Intrusion Detection. **Cybernetics, IEEE Transactions on**, [S.I.], v.44, n.1, p.66–82, Jan 2014.
- [49] IGLESIAS, 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.
- [50] KEPHART, J. O.; CHESS, D. M. The Vision of Autonomic Computing. **Computer**, Los Alamitos, CA, USA, v.36, n.1, p.41–50, Jan. 2003.
- [51] 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.I.], v.2018-January, p.35–40, 2018. cited By 0.
- [52] KLIARSKY, A.; LEUNE, K. Detecting Attacks Against The Internet of Things. **SANS Institute. InfoSec Reading Room**, [S.I.], 2017.
- [53] LAMPRECHT, C. J. **Adaptive Security**. 2012. Tese (Doutorado em Ciência da Computação) — Newcastle University. School of Computing Science.
- [54] LANGHEINRICH, M. **Privacy in Ubiquitous Computing**. [S.I.]: J. Krumm, ed., CRC Press, 2010. 95-160p.
- [55] LE, A.; MAPLE, C.; WATSON, T. A profile-driven dynamic risk assessment framework for connected and autonomous vehicles. **IET Conference Publications**, [S.I.], v.2018, n.CP740, 2018. cited By 0.
- [56] LI, X.; ECKERT, M.; MARTINEZ, J.-F.; RUBIO, G. Context Aware Middleware Architectures: Survey and Challenges. **Sensors**, [S.I.], v.15, n.8, p.20570, 2015.

- [57] LIU, J.; LIJUAN, L. A Distributed Intrusion Detection System Based on Agents. In: COMPUTATIONAL INTELLIGENCE AND INDUSTRIAL APPLICATION, 2008. PACIAA '08. PACIFIC-ASIA WORKSHOP ON, 2008. *Anais...* [S.I.: s.n.], 2008. v.1, p.553–557.
- [58] LOVINS, J. B. Development of a stemming algorithm. **Mechanical Translation and Computational Linguistics**, [S.I.], v.11, p.22–31, 1968.
- [59] MACHADO, R. S. et al. EXEHDA-HM: A compositional approach to explore contextual information on hybrid models. **Future Generation Computer Systems**, [S.I.], v.73, p.1 – 12, 2017.
- [60] MEULEN, R. van der. Disponível em: <<https://www.gartner.com/smarterwithgartner/build-adaptive-security-architecture-into-your-organization/>>, Gartner - Build Adaptive Security Architecture Into Your Organization. Acesso em janeiro de 2018.
- [61] MIORANDI, D.; SICARI, S.; PELLEGRINI, F. D.; CHLAMTAC, I. Internet of things: Vision, applications and research challenges. **Ad Hoc Networks**, [S.I.], v.10, n.7, p.1497 – 1516, 2012.
- [62] MITRE. Common Event Expression: Architecture Overview. **The CEE Editorial Board**, [S.I.], 2010.
- [MOTTA; OLIVEIRA] TRAVASSOS(2019)MOTTA; OLIVEIRA]; TRAVASSOS]MOTTA2019231 MOTTA, R. C.; OLIVEIRA], K. M. [de; TRAVASSOS, G. H. A conceptual perspective on interoperability in context-aware software systems. **Information and Software Technology**, [S.I.], v.114, p.231 – 257, 2019.
- [64] MOZZAQUATRO, B. A. et al. An Ontology-Based Cybersecurity Framework for the Internet of Things. **Sensors**, [S.I.], v.18, n.9, 2018.
- [65] 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.I.: s.n.], 2015. p.1–6.
- [66] 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.I.: s.n.], 2016. p.779–788.

- [67] MOZZAQUATRO, B.; AGOSTINHO, C.; MELO, R.; JARDIM-GONCALVES, R. A model-driven adaptive approach for IoT security. **Communications in Computer and Information Science**, [S.I.], v.692, p.194–215, 2017.
- [68] OCG. Open Geospatial Consortium. Sensor Model Language (SensorML). Disponível em: <<http://www.opengeospatial.org/standards/sensorml>>, acesso em: 12 feb 2018.
- [69] O.M.A. **NGSI Context Management**. [S.I.]: Open Mobile Alliance, 2012.
- [70] ONWUBIKO, C. **Situational Awareness in Computer Network Defense**: Principles, Methods and Applications: Principles, Methods and Applications. [S.I.]: Information Science Reference, 2012.
- [71] OWASP. Disponível em: <https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project>, OWASP Internet of Things Project. Acesso em janeiro de 2018.
- [72] PANETTA, K. Disponível em: <<https://www.gartner.com/smarterwithgartner/gartners-top-10-technology-trends-2017/>>, Gartner - Top 10 Strategic Technology Trends for 2017. Acesso em janeiro de 2018.
- [73] PANETTA, K. Disponível em: <<https://www.gartner.com/smarterwithgartner/gartner-top-10-strategic-technology-trends-for-2018/>>, Gartner - Top 10 Strategic Technology Trends for 2018. Acesso em janeiro de 2018.
- [74] PERERA, C.; ZASLAVSKY, A.; CHRISTEN, P.; GEORGAKOPOULOS, D. Context Aware Computing for The Internet of Things: A Survey. **IEEE Communications Surveys Tutorials**, [S.I.], v.16, n.1, p.414–454, First 2014.
- [75] 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.
- [76] ROCHFORD, O.; KAVANAGH, K. M. **Magic Quadrant for Security Information and Event Management**. [S.I.]: Gartner Group, 2015.
- [77] ROMAN, R.; ZHOU, J.; LOPEZ, J. On the features and challenges of security and privacy in distributed internet of things. **Computer Networks**, [S.I.], v.57, n.10, p.2266 – 2279, 2013. Towards a Science of Cyber Security Security and Identity Architecture for the Future Internet.
- [78] ROUSE, M. What is wildcard character?. Disponível em: <<https://whatis.techtarget.com/definition/wildcard-character>>, acesso em: 28 abr 2020.

- [79] SAHU, C. G.; ADANE, D. S. A Survey on Context-Aware Middleware. **International Journal of Advanced Research in Computer and Communication Engineering**, USA, v.4, n.5, p.650–656, May 2015.
- [80] SAP. STANDARDIZED Technical Architecture Modeling. Disponível em: <http://www.fmc-modeling.org/download/fmc-and-tam/SAP-TAM_Standard.pdf>, acesso em dezembro 2018.
- [81] SCHMERKEN, I. **Deciphering the Myths Around Complex Event Processing**. [S.I.]: Wall Street and Technology, 2008.
- [82] SHANKAR, V. Clash of the titans - Arcsight vs QRadar. Disponível em: <<http://infosecnirvana.com/clash-titans-arcsight-vs-qradar/>>, acesso em: 04 fev 2018.
- [83] SICARI, S.; RIZZARDI, A.; GRIECO, L.; COEN-PORISINI, A. Security, privacy and trust in Internet of Things: The road ahead. **Computer Networks**, [S.I.], v.76, p.146 – 164, 2015.
- [84] SUNDMAEKER, H. et al. **Vision and Challenges for Realising the Internet of Things**. [S.I.]: Publications Office of the European Union, 2010.
- [85] TORRES, A.; WILLIAMS, J. Maturing and Specializing: Incident Response Capabilities Needed. **SANS Institute. SANS Analyst Program**, [S.I.], 2015.
- [86] TWENEBOAH-KODUAH, S.; SKOUBY, K. E.; TADAYONI, R. Cyber Security Threats to IoT Applications and Service Domains. **Wireless Personal Communications**, [S.I.], v.95, n.1, p.169–185, Jul 2017.
- [87] VERIZON. Data Breach Investigations Report. **Verizon Enterprise Solutions**, [S.I.], 2013.
- [88] VIEIRA, V.; MANGAN, M.; WERNER, C.; MATTOSO, M. Ariane: An Awareness Mechanism for Shared Databases. In: **Groupware: Design, Implementation, and Use**. [S.I.]: Springer Berlin Heidelberg, 2004. p.92–104. (Lecture Notes in Computer Science, v.3198).
- [89] 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.I.: s.n.], 2017. p.17–24.
- [90] WEBER, R. H. Internet of Things – New security and privacy challenges. **Computer Law and Security Review**, [S.I.], v.26, n.1, p.23 – 30, 2010.

- [91] WEISER, M. The Computer for the 21st Century. **Scientific American**, [S.I.], v.265, n.3, p.66–75, January 1991.
- [92] WENDT, E.; JORGE, H. **Crimes Cibernéticos**: Ameaças e procedimentos de investigação. [S.I.]: Brasport, 2013.
- [93] WINDER, D. How to define a security incident. Disponível em: <<http://www.itpro.co.uk/security/20852/how-define-security-incident>>, acesso em: 17 nov 2015.
- [94] YANG, X.; LI, Z.; GENG, Z.; ZHANG, H. A Multi-layer Security Model for Internet of Things. In: INTERNET OF THINGS, 2012, Berlin, Heidelberg. **Anais...** Springer Berlin Heidelberg, 2012. p.388–393.
- [95] YUAN, E.; MALEK, S. A taxonomy and survey of self-protecting software systems. In: INTERNATIONAL SYMPOSIUM ON SOFTWARE ENGINEERING FOR ADAPTIVE AND SELF-MANAGING SYSTEMS (SEAMS), 2012., 2012. **Anais...** [S.I.: s.n.], 2012. p.109–118.
- [96] ZHAO, K.; GE, L. A Survey on the Internet of Things Security. In: NINTH INTERNATIONAL CONFERENCE ON COMPUTATIONAL INTELLIGENCE AND SECURITY, 2013., 2013. **Anais...** [S.I.: s.n.], 2013. p.663–667.

Apêndices

APÊNDICE A – Um Apêndice

Anexos

ANEXO A – Um Anexo

ANEXO B – Outro Anexo