Ricardo Borges Almeida

Avaliação de Estratégias de Segurança Adaptativa para a Internet das Coisas

Trabalho Individual apresentado ao Programa de Pós-Graduação em Computação da Universidade Federal de Pelotas, como requisito parcial à obtenção do título de Doutor em Ciência da Computação

Orientador: Profª. Drª. Ana Marilza Pernas
Coorientadoraes: Prof. Dr. Adenauer Corrêa Yamin
Sr. Lucas Medeiros Donato

Pelotas, 2018

RESUMO

ALMEIDA, Ricardo Borges. **Avaliação de Estratégias de Segurança Adaptativa para a Internet das Coisas**. 2018. 48 f. Trabalho Individual (Doutorado em Ciência da Computação) – Programa de Pós-Graduação em Computação, Centro de Desenvolvimento Tecnológico, Universidade Federal de Pelotas, Pelotas, 2018.

Uma materialização da Computação Ubíqua que vem ganhando destaque é a Internet das Coisas (IoT), a qual consiste de um ecossistema que combina redes de sensores com e 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 potencializaram enquanto características necessárias e viabilizadoras para IoT. Promover a segurança com mecanismos pré-definidos e estáticos sobre este ambiente dinâmico e heterogêneo não se mostra mais uma abordagem oportuna. Por isso, são necessárias soluções para segurança auto-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; e (iii) desenvolver uma análise crítica sobre os trabalhos identificados em um esforço para elencar as lacunas existentes nesta área.

Palavras-Chave: internet das coisas; segurança adaptativa; ciência de contexto

ABSTRACT

ALMEIDA, Ricardo Borges. **Assessment of Adaptive Security Strategies for the Internet of Things**. 2018. 48 f. Trabalho Individual (Doutorado em Ciência da Computação) – Programa de Pós-Graduação em Computação, Centro de Desenvolvimento Tecnológico, Universidade Federal de Pelotas, Pelotas, 2018.

One of Ubiquitous Computing most prominent materializations is the Internet of Things (IoT), which consists of an ecosystem that combines wireless and wired 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 challenging task. Therefore, solutions for self-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; and (iii) develop a critical analysis of the work identified in an effort to fill the gaps in this area.

Keywords: internet of things; adaptive security; context awareness

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ARM	*Adaptive Risk Management*
CERP-IoT	*Cluster of European Research Projects on the Internet of Thing*
HP	*Hewlett-Packard*
IBM	*International Business Machines*
IDS	*Intrusion Detection System*
IoT	Internet das Coisas
IP	*Internet Protocol*
ISMS	*Information Security Management System*
ISRM	*Information Security Risk Management*
MAPE-K	*Monitor-Analyze-Plan-Execute plus Knowledge*
OWASP	*Open Web Application Security Project*
PDCA	*Plan-Do-Check-Act*
QoS	*Quality of Service*
RBAC	*Role-Based Access Control*
RFID	*Radio Frequency Identification*
UbiComp	*Ubiquitous Computing*
WAF	*Web Application Firewall*

SUMÁRIO

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 em que se busca, acessa e compartilha as informações, tornando o ambiente mais interativo, adaptável e informativo (TWENEBOAH-KODUAH; SKOUBY; TADAYONI, 2017). 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 são 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 gerenciamento inteligente de produtos (ASHTON, 2009). 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.

Esta proliferação de dispositivos conectados criou uma nova lacuna na segurança tradicional. O crescimento da IoT impulsionado pelas demandas do mercado inspirou novas tecnologias e protocolos, no entanto, os fabricantes tem concebido produtos mais rapidamente do que a segurança pode ser inserida desde o início deste processo (KLIARSKY; LEUNE, 2017). 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 das preocupações de segurança (SICARI et al., 2015).

As ameaças e vulnerabilidades associadas à IoT são proporcionais as superfícies

de ataque (KLIARSKY; LEUNE, 2017). 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. O relatório destaca 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 (HP, 2015; OWASP, 2018). Estas são algumas preocupações graves, especialmente para os serviços de saúde apoiados na IoT, onde o tipo de informação tratada 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 sensores 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 (AMAN; SNEKKENES, 2015).

Promover a segurança com mecanismos pré-definidos e estáticos sobre este ambiente dinâmico e heterogêneo não se mostra mais uma abordagem oportuna. Por isso, são necessárias soluções para segurança auto-adaptativa (EVESTI; TUTKIMUSKESKUS, 2013). Esses sistemas auto-adaptativos podem ser estáticos ou dinâmicos em termos de quando a adaptação ocorre. Neste segundo caso, o processo é apoiado por um clico de *feedback* que permite que os sistemas tomem suas próprias decisões de adaptação sem intervenção humana (LAMPRECHT, 2012). Desta forma, uma vez que este texto tem interesse particular na adaptação dinâmica, em tempo de execução, o termo adaptação será usado como sinônimo para auto-adaptação.

A segurança adaptativa, visa selecionar automaticamente mecanismos de segurança e seus parâmetros em tempo de execução para preservar o nível de segurança requerido em um ambiente em mudança (EVESTI; TUTKIMUSKESKUS, 2013). Isso é buscado por meio do monitorando de atributos e ações que afetam a segurança atual e a desejada. Quando uma diferença entre a segurança atual e a necessária é identificada, os mecanismos de segurança são modificados. Nesta pesquisa, o foco está na adaptação baseada em arquitetura, onde o sistema considera o próprio modelo em

conjunto com o seu ambiente, e se adapta quando necessário de acordo com alguns objetivos de adaptação.

A adaptação, ou comportamento autonômico é considerado um desafio importante da IoT (AMAN, 2016; ALABA et al., 2017; PANETTA, 2017). Esse desafio está relacionado à capacidade de dispositivos e aplicações adaptarem seu comportamento como resposta às mudanças em seu ambiente de operação. Desta forma, a segurança adaptativa decorre do fato que os sistemas enfrentam ambientes e situações distintas durante sua operação que requerem diferentes objetivos de segurança. Ou seja, em algumas situações, a integridade é um objetivo de segurança essencial, mas em outras a autenticação tem maior prioridade. Adicionalmente, a criticidade da informação varia entre as situações, em alguns casos a aplicação pode operar com dados de acesso público, em outros, com dados sensíveis como informações sobre a saúde de pacientes. Portanto, o nível de segurança requerido varia de uma situação para outra. Essas variações e o dinamismo do ambiente são desafiadores para desenvolvedores de software pois eles não podem antecipar todas as possíveis mudanças e situações em tempo de projeto. Consequentemente, uma aplicação deve adaptar a segurança com base nas situações em mudança (EVESTI; TUTKIMUSKESKUS, 2013).

Com isso, a ciência de contexto torna-se um conceito chave para fornecer segurança adaptativa, ou seja, o sistema deve selecionar entre as características e pilares da segurança (confidencialidade, integridade e disponibilidade) mais adequados de acordo com as informações de contexto relevantes para a situação corrente, promovendo 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.

1.1 Motivações

Os serviços na IoT devem se adaptar adequadamente a diferentes situações com base nos contextos que às compõem. Uma série de esforços de pesquisa para a construção de serviços adaptativos foram realizados nos últimos anos. No entanto, ainda não é possível alcançar uma compreensão global de como desenvolver serviços adaptativos considerando o nível de flexibilidade exigido pelos cenários IoT. Além disso, muitas das abordagens propostas para segurança adaptativa foram concebidas para serem aplicadas em um único e específico campo de aplicação (MIORANDI et al., 2012).

A segurança adaptativa possui múltiplas dimensões, logo, se faz necessário entender os desafios pertinentes à este panorama para que assim seja possível identificar as necessidades específicas e atuais decorrentes da IoT. Por exemplo, é possível

adaptar modelos de segurança convencionais existentes, assim como adaptar as mudanças de contexto pré-planejadas de segurança. Ainda existe a possibilidade dos sistemas da IoT serem projetados para adaptarem-se de maneira nativa. Estes sistemas precisam se adaptar à reconfiguração e manutenção ativa dos dispositivos da IoT e de seus sistemas tanto pelos usuários quanto por agentes artificiais.

Os desafios na segurança adaptativa consideram que o algoritmo deve responder às mudanças no sistema dinamicamente e as atividades do algoritmo devem ter desvios mínimos do modo normal de operação do sistema, abordando a reconfiguração funcional, a arquitetura como um todo e o tratamento de conflitos. Outros desafios para a implementação de algoritmos adaptativos são a complexidade da definição correta de metas e restrições, a necessidade de monitoramento contínuo do sistema e do ambiente, e o tempo de reação mínimo para a efetivação da adaptação.

Observa-se também que os riscos de segurança ficam intensificados devido à natureza heterogênea e a forma invisível de como ocorre a comunicação na IoT (LANGHEINRICH, 2010). Percebe-se que também o rápido desenvolvimento e a inserção da IoT na vida cotidiana resultou em um crescimento natural em tamanho, complexidade e distribuição das infraestruturas de rede, implicando em limitações nas soluções de segurança quanto a desempenho, escalabilidade e flexibilidade (ONWUBIKO, 2012; LIU; LIJUAN, 2008; GHORBANI; LU; TAVALLAEE, 2010; HU et al., 2014). A utilização total deste volume de dados de contexto 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 analisador (LI et al., 2015). Este cenário vem sendo percebido nas organizações de acordo com um estudo realizado pela SANS, onde 45% dos 507 entrevistados citaram a falta de visibilidade sobre os eventos de segurança como um dos principais impedimentos para uma eficaz resposta a incidentes (TORRES; WILLIAMS, 2015).

Em (WEYNS et al., 2012), é realizado um estudo sobre os desafios no campo dos sistemas auto-adaptativos, onde os autores reconhecem que a aplicação de auto-adaptação para gerenciar atributos de qualidade, como segurança, é um tópico importante para futuras pesquisas. Consequentemente, as abordagens de adaptação de segurança existentes não oferecem um meio completo para produzir software com capacidades de segurança adaptativa. Adicionalmente, após a revisão literária realizada, foi possível perceber que as abordagens existentes não são genéricas, geralmente elas se concentram em objetivos de segurança específicos, como autenticação, verificação e controle de acesso. Não obstante, Yuan et al. (2012) destaca que a maioria das abordagens existentes se concentra na parte de monitoramento do clico de adaptação. Os autores observam também que em termos arquiteturais os trabalhos existentes possuem lacunas a serem consideradas.

Este panorama encaminha a necessidade de pesquisa adicional para identificação das principais lacunas existentes no estado da arte em segurança adaptativa para IoT, avaliando também a sustentabilidade das abordagens existentes.

1.2 Objetivos

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; e (iii) desenvolver uma análise crítica sobre os trabalhos identificados em um esforço para elencar as lacunas existentes nesta área.

1.3 Estrutura do Texto

Este trabalho foi organizado em 4 capítulos. Neste primeiro capítulo foi apresentada uma breve introdução ao tema do trabalho, suas motivações e objetivos. Na sequência, são discutidos os conceitos em torno da segurança adaptativa para IoT. O capítulo 3 apresenta o estado da arte. Por fim, o capítulo 4 discute as considerações finais sobre este trabalho.

2 SEGURANÇA ADAPTATIVA PARA A INTERNET DAS COISAS

Para fornecer uma visão coerente sobre segurança adaptativa para IoT primeiramente é abordado neste capítulo a IoT, incluindo suas características e desafios para segurança. Na sequência são apresentados os conceitos em torno da segurança adaptativa. Finalmente, discuti-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, popularmente conhecida como 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 (GIUSTO et al., 2010). Semanticamente, a IoT pode ser percebida como uma combinação de dois conceitos, ou seja, 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 a definição de “coisas” adotada-se neste texto a elaborada pelo *Cluster of European Research Projects on the Internet of Thing* (CERP-IoT), o 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 (SUNDMAEKER et al., 2010).

A IoT, ao menos na teoria, visa tornar o cotidiano das pessoas mais simples, prática e produtiva, 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 a visão da IoT. Para exemplificar alguns dos dispositivos associados à esta afirmação é possível citar os relógios inteligentes, carros, cafeteiras, geladeiras, robôs aspiradores, entre outros. Este ambiente permite uma integração dos objetos físicos, móveis e de sensoriamento na infraestrutura tradicional, criando assim, novas oportunidades de negócio. A eHealth (uso de tecnologia da informação para saúde), edifícios inteligentes, redes inteligentes e sensores de meio ambiente são alguns exemplos de serviços e aplicações habilitadas pela IoT em diferentes campos (AMAN, 2016).

Para fornecer suporte a este ambiente dinâmico, considerando o escopo deste trabalho, em especial a necessidade de segurança em torno da IoT, os seguintes recursos devem ser almejados (MIORANDI et al., 2012):

- Heterogeneidade de dispositivos: a IoT é caracterizada por uma considerável heterogeneidade de dispositivos, os quais apresentam capacidades diferentes dos pontos de vista computacional e de comunicação. O gerenciamento dessa heterogeneidade deve ser suportado em 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.

- Escalabilidade: a medida 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 pelas 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 implica na necessidade que os dispositivos (ou parte 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 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, como a visibilidade global, o gerenciamento autônomo em tempo real, a regularização, a padronização, a interoperabilidade dos sistemas, o consumo de recursos, a distribuição, o suporte à QoS, a privacidade dos dados e a segurança (WEBER, 2010; MIORANDI et al., 2012). Algumas dessas preocupações, como as questões de QoS e os consumos de recursos, são, em última instância, um problema de segurança, pois influenciam ou são influenciados direta ou indiretamente.

Assim, pode-se estabelecer que a segurança é um dos problemas críticos que precisam ser adequadamente abordados (MIORANDI et al., 2012; ROMAN; ZHOU; LOPEZ, 2013; SICARI et al., 2015). Fornecer segurança na IoT é uma tarefa desafiadora, 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 impulsiona 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 Segurança Adaptativa

A adaptação consiste na capacidade de um sistema monitorar e regular de forma autônoma seu comportamento de acordo com as situações de interesse ou alterações sob observação. Esta característica 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 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 (AMAN; SNEK-

KENES, 2015).

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. Uma arquitetura de segurança adaptativa é uma estrutura útil para auxiliar as organizações a classificar a segurança existente e os potenciais investimentos para garantir uma abordagem equilibrada (MEULEN, 2017).

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 (PANETTA, 2017). 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 (PANETTA, 2018).

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 do que tange a segurança da informação (LANGHEINRICH, 2010). 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 (YANG et al., 2012; ZHAO; GE, 2013; ALABA et al., 2017). 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 (LAMPRECHT, 2012; AMAN; SNEKKENES, 2015). Uma abordagem promissora para segurança adaptativa considerando os ambientes da IoT é o emprego de um clico de *feedback*. Um clico de *feedback* (vide 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 finalmente 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.

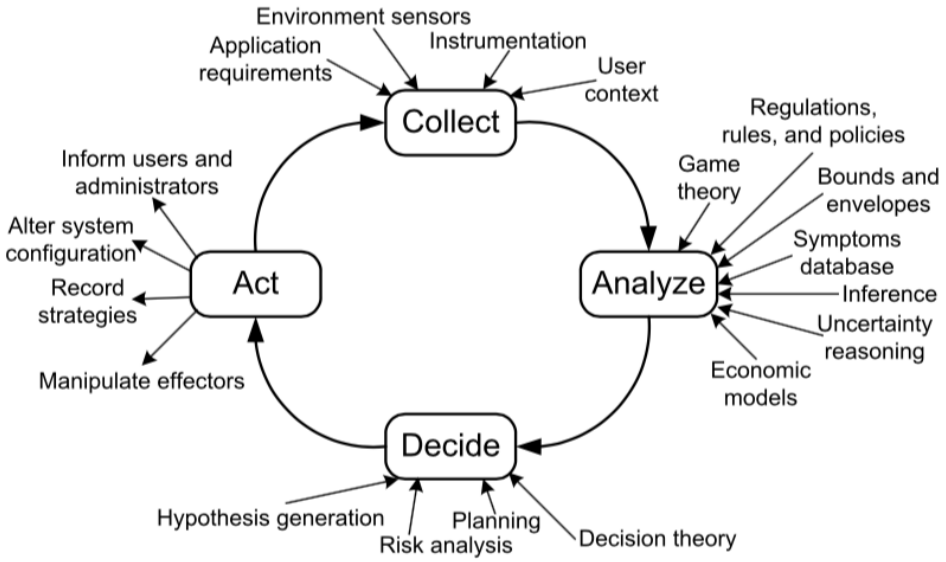

Figura 1 – Ciclo de *feedback* genérico (DOBSON et al., 2006)

Um exemplo da aplicação do clico de *feedback* é discutido em (BRUN et al., 2009). Os autores consideram que para manter os serviços Web em funcionamento durante um longo período de tempo requer a coleta de informações que reflitam o estado atual do sistema, analisando essas informações para diagnosticar problemas de desempenho ou para detectar falhas, decidindo como resolver o problema (por exemplo, via balanceamento dinâmico de carga ou corrigindo falhas), e agindo 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 questões levantas em (BRUN et al., 2009; 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 exem-

plo, usando modelos, teorias e regras). Algumas das questões aplicáveis aqui são: Como o estado atual do sistema é inferido? Qual a quantidade/tempo de situações passadas podem ser necessárias 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 clicos de *feedback* e em um único clico 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 clicos 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 clico de *feedback* ilustrado na Figura 1, muitas vezes referido como o clico de controle autonômico, enfatiza as atividades que realizam feedback. Embora este modelo forneça um ponto de partida sobre os clicos de feedback, ele não detalha o fluxo de dados e o controle em torno do clico (DOBSON et al., 2006). Ainda que esses clicos 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 (LAMPRECHT, 2012).

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 clico de controle em conjunto com o componente Conhecimento que fornece as informações necessárias para realizar a adaptação (AMAN; SNEKKENES, 2015). O componente Monitor coleta os dados apropriados dos recursos gerenciados por meio dos sensores. Os dados são correlacionados, filtrados e/ou

agregados e o sintoma descoberto é passado para o componente Analisar. Sintomas e outros dados também podem ser armazenados em uma base de conhecimento compartilhada. O analisador determina se uma mudança precisa ser feita com base no conhecimento compartilhado (potencialmente uma política) e nos sintomas. Caso pertinente, uma solicitação de mudança no ambiente é passada para o componente Planejar. O planejador gera os comandos ou fluxos de trabalho necessários na forma de um plano de alteração que é passado para o componente Executar. O executor aplica o plano de mudança no recurso de gerenciamento usando os atuadores. Caso necessário, a base de conhecimento pode ser atualizada, fornecendo dados do impacto da adaptação para serem aplicados como feedback para o próximo clico (LAMPRECHT, 2012).

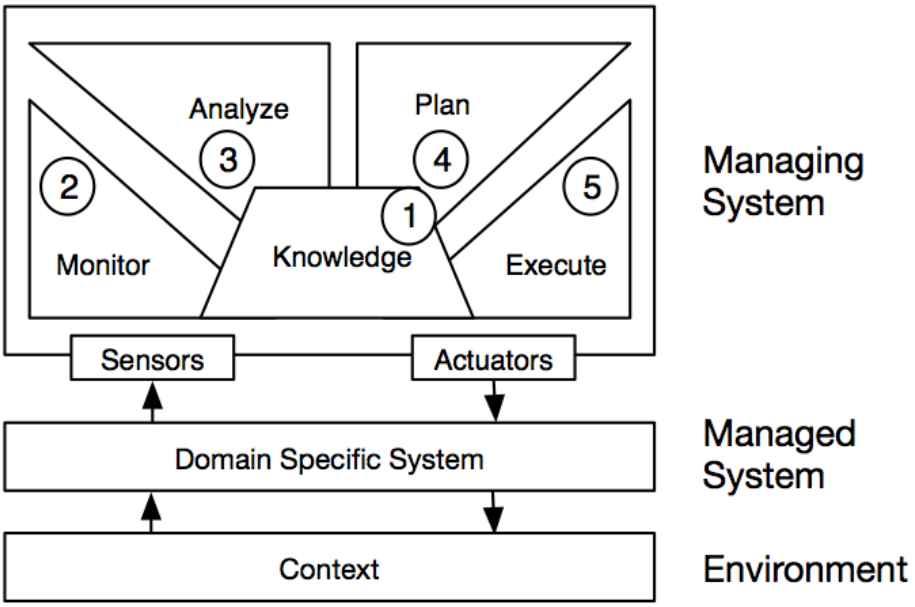

Figura 2 – MAPE-K - Modelo para sistema adaptativos (IGLESIA; WEYNS, 2015)

De acordo com a IBM, um sistema autonômico deve ter os seguintes auto-atributos (KEPHART; CHESS, 2003; IGLESIA; WEYNS, 2015):

- 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 controlar

os recursos e os parâmetros de segurança para melhorar o desempenho e a eficiência, consequentemente aprimorando a qualidade dos serviços (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 confiabilidade do sistema.

- Autoproteção (*self-protection*): este atributo envolve dois aspectos: a defesa contra ataques e antecipação de ataques. A defesa deve ser realizada com o objetivo de protejer 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 autoconsciência (*self-awareness*) e a ciência de contexto (*context awareness*). A autoconsciência é a capacidade do sistema em conhecer seu próprio estado, seus componentes, capacidades, limites, recursos e comportamento. Já a ciência do contexto, consiste do conhecimento sobre o ambiente operacional ao qual o sistema está inserido.

2.3 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 (BRÉZILLON, 1999; LI et al., 2015).

Existem seis questões básicas que podem ser realizadas para facilitar a compreensão do contexto, elas são conhecidas como 5W+1H (VIEIRA et al., 2004). 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 (BRÉZILLON; ARAUJO, 2005). 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 (DEY, 2001).

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

No que tange a segurança adaptativa, caso os contextos relevantes para a identificação das situações a serem avaliadas não sejam adequadamente levadas 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 outras 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 é especialmente crítica nos cenários da IoT, em particular na adaptação, pois esta consiste de uma comunicação máquina para máquina, a priori sem a inteligência (envolvimento direto) dos humanos. Caso sejam levados em consideração contextos irrelevantes, incorretos ou insuficientes, a adaptação pode não ser eficiente (AMAN; SNEKKENES, 2015).

2.4 Considerações sobre o Capítulo

Inicialmente neste capítulo foi apresentada a definição de IoT, sendo destacado que a segurança adaptativa é considerado um desfio importante e atual. Posteriormente a segurança adaptativa foi discutida, sendo exposto que o uso de um clico 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.

3 ESTADO DA ARTE

Neste capítulo será apresentado o estado da arte das pesquisas que tem como tema processamento de eventos complexos e internet das coisas. Na seção seguinte será apresentado o protocolo seguido para a execução do mapeamento sistemático assim como todos os passos executados que levaram a escolha dos trabalhos de interesse. Por fim será apresentado uma discussão sobre as soluções abordadas nos trabalhos de interesse selecionados.

3.1 Mapeamento Sistemático da Literatura

O mapeamento sistemático abordado neste capítulo é baseada na metodologia proposta por Petersen et al. (2008), onde seguindo a série de passos proposto, torna o estudo realizado, possível de ser replicado por outros pesquisadores (PETERSEN et al., 2008). A partir desta metodologia, podemos citar cinco etapas das quais serão seguidas por este mapeamento:

1. Definição das questões de pesquisa;
2. Execução da pesquisa para identificação de estudos primários realizados;
3. Triagem inicial empregando critérios de inclusão e exclusão considerando o resumo dos artigos;
4. Triagem final considerando as seções de introdução, concepção do projeto e conclusão;
5. Extração dos dados e mapeamento.

Para a consulta dos trabalhos relacionados primeiramente foi definido um conjunto de palavras como candidatas a palavras chave para a String de busca, dentre estas podemos citar: *internet of things*, *distributed* e *complex event processing*. A Partir da definição destas como palavras chave, foi possível elaborar a String de busca usada para executar as consultas sobre as bases da: ACM Digital Library, IEEE Explore,

ScienceDirect, Springer, Web of Science e Scopus; e assim obter-se os trabalhos relacionados com o tema de pesquisa, as strings de consulta podem ser vistas na figura 3 incluindo a qual respectiva base estas foram executadas.

Base de Dados	String de Busca
ACM Digital Library	recordAbstract:(distributed AND ("internet of things" OR iot) AND ("event stream processing" OR "event processing" OR "complex event processing"))
Demais Bases	distributed AND ("internet of things" OR iot) AND ("event stream processing" OR "event processing" OR "complex event processing")

Figura 3 – Strings de buscas usadas.

Após a execução desta consulta preliminar, que entende-se como a etapa de levantamento dos estudos primários relevantes, foi identificado 647 trabalhos de interesse onde este valor compreende-se da soma dos resultados obtidos em todas as bases de consulta.

Todas as buscas foram realizadas sobre os metadados dos artigos(titulo, resumo e palavras chave), porem, como a base de dados Springer não oferecia suporte a este tipo de consulta, este problema foi contornado da seguinte forma: primeiramente foi feito a exportação do resultado preliminar da busca na base para o formato CSV(o único suportado) resultando em 472 artigos, após isto fez-se uso da ferramenta CSV2Bib[1] para converter o arquivo CSV para bib com o intuito de importar o resultado, para a ferramenta Zotero[2], que permitiu a execução da String de busca sobre os metadados dos 472 artigos encontrados preliminarmente, resultando em 6 documentos de interesse, a figura 5 apresenta um gráfico de barras contendo o numero de artigos encontrados pela String de busca em cada uma das bases, já o gráfico 4 apresenta o percentual de publicações que cada uma das bases contribuiu para o montante final.

O gráfico 6 apresenta o numero de publicações de interesse encontradas e cada uma das bases, o eixo X apresenta o ano do qual os artigos foram publicados e o eixo Y apresenta o numero total de publicações em relação ao ano, ainda podemos ressaltar que para a representação do gráfico foram removidos todas as publicações duplicadas. Podemos perceber pelo figura que a partir do ano de 2015 á um considerável aumento no numero de publicações, e ainda um grande pico no ano de 2017, demonstrando assim pontos de interesses neste período de publicações.

[1] `https://github.com/jacksonpradolima/csv2bib`
[2] `http://lapes.dc.ufscar.br/tools/start_tool`

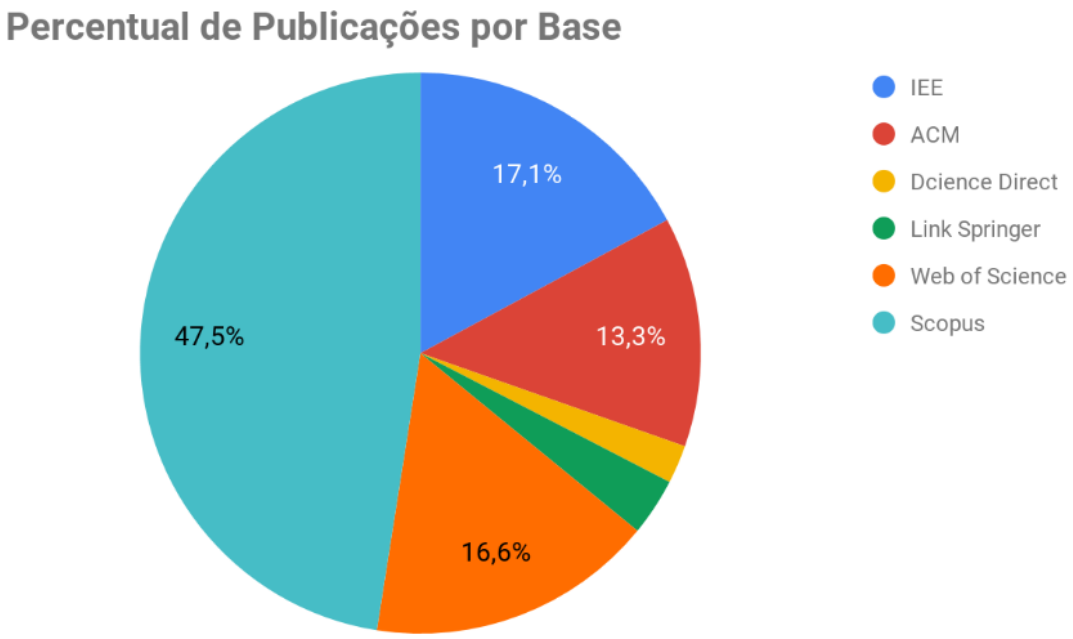

Figura 4 – Percentual de publicações encontradas por base.

3.1.1 Critérios de Inclusão e Exclusão

Após a seleção inicial realizada sobre as bases de dados, executou-se a triagem inicial sobre o resumo dos artigos, aplicando os seguintes critérios de inclusão e exclusão conforme a ordem apresentada abaixo:

- (E) Foi publicado antes de 2015;
- (E) Não é um artigo Full paper;
- (E) Não esta em Inglês ou Português;
- (E) Indisponibilidade de acesso ao artigo completo;
- (E) Artigos que não apresentam avaliação da proposta;
- (I) Explora conceitos de segurança;
- (I) Explora conceitos de computação Ubiqua;
- (E) O artigo não possui nenhum dos critérios de inclusão.

Para auxiliar na aplicação dos critérios de inclusão e exclusão foi feita a importação dos resultados preliminares das buscas na ferramenta Start[3], para isso usou-se os arquivos .bib exportados pelas ferramentas das bases de busca, com exceção apenas da Spriger, onde usou-se o arquivo .bib exportado pelo Zootero, que foi gerado apos

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

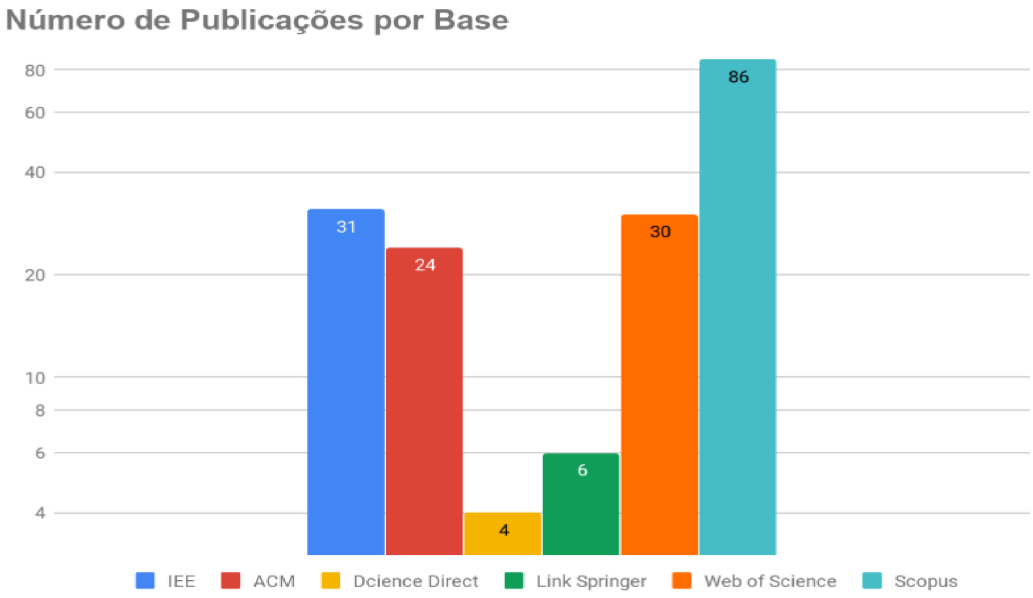

Figura 5 – Número de publicações encontradas por base.

a execução da consulta sobre os metadados, aplicada sobre o resultado preliminar da base.

Os critérios de exclusão foram aplicados seguindo a seguinte ordem e etapas:

- **Remoção de Trabalhos Duplicados -** Muitos dos trabalhos retornados pela String de busca estavam indexados em ambas as bases de consulta, tornando necessário a execução de uma etapa de remoção dos mesmos, resultando em 74 trabalhos duplicados removidos.

- **Filtro por Data -** O intervalo de interesse para a aplicação do filtro foi adotado baseado no numero de publicações por ano, após o levantamento dos trabalhos de interesse, identificou-se o ano de 2015, como sendo o ano em que o numero de publicações aumenta considerável mente, continuando a ascender até o pico máximo no ano de 2017, como pode ser visto na figura 6. Assim optou-se por eliminar todas as publicações que fossem anteriores ao ano de 2015 eliminando desta forma 26 artigos.

- **Artigos Full Paper -** Com o intuito de remover artigos que apresentem apenas resumos superficiais sobre os trabalhos, ou que não tenham apelo cientifico, optou-se por remover artigos que não sejam Full Paper (livro ou capítulo de livro, introdução de anais, entre outros), onde foram removidos 9 trabalhos.

- **Filtro por Idioma -** Como as pesquisas foram realizadas sobre varias bases de dados onde muitas destas indexam trabalhos em vários idiomas, optou-se por usar um filtro por idiomas para remover qualquer trabalho que não esteja em

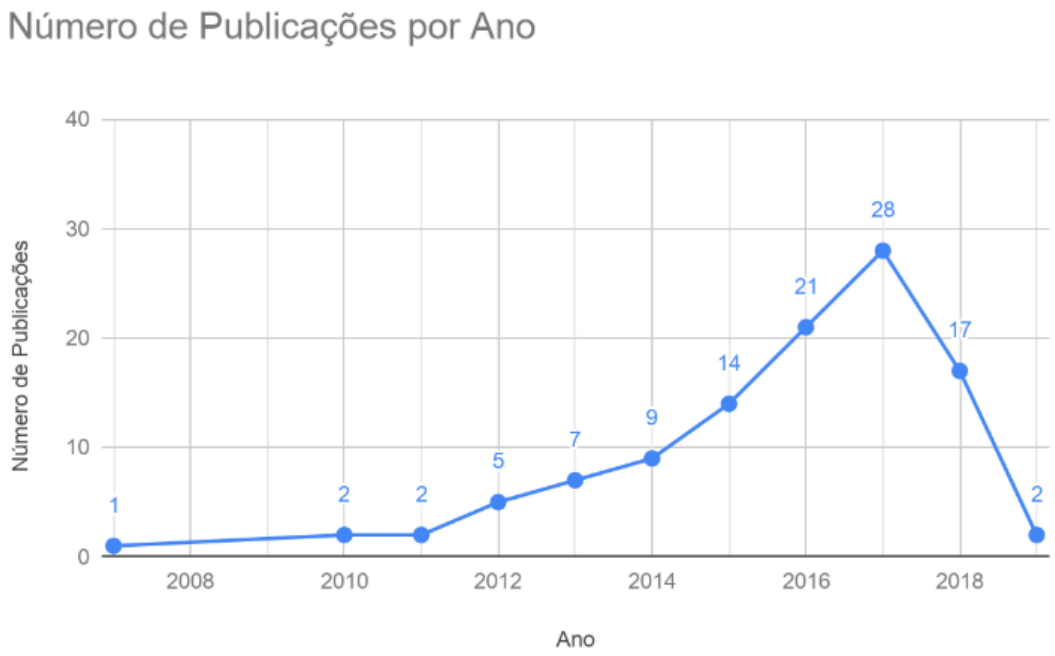

Figura 6 – Quantidade de publicações de interesse por ano.

Português ou Inglês(idiomas de total domínio do autor) removendo desta forma 1 artigo.

- **Indisponibilidade do Artigo completo -** Dado que alguns dos estudos de interesse selecionados apresentaram apenas seus resumos e introdução disponíveis não oferecendo a opção de obter-se o trabalho completo, optou-se por remover estes do pesquisa, excluindo desta forma 3 trabalhos.
- **Avaliação da Proposta -** Foram removidos todos os artigos que não executaram algum tipo de teste ou estudo de caso das soluções propostas por seus trabalhos, excluindo assim 17 artigos.
- **Sem Nenhum Critério de Inclusão -** Todos trabalhos que não se enquadraram em nenhum dos critério de inclusão foram removidos, excluindo desta forma 28 trabalhos da pesquisa.

Após execução da triagem inicial dos trabalhos, aplicando os critérios de inclusão e exclusão sobre o resumo dos artigos, selecionou-se 24 documentos de interesse, o fluxo da aplicação dos critérios de exclusão pode ser visto na figura 7 assim como o numero total de trabalhos removidos por cada um dos critérios de aplicação.

A execução da 4 etapa do mapeamento, que consiste da triagem final dos trabalhos de interesse, selecionou dez dos 24 artigos para analise completa de seu conteúdo e da extração das informações destes. O critério para a seleção dos dez trabalhos consistiu, se estes exploravam conceitos de segurança da informação ou ainda se

estes apresentavam o uso de conceitos de computação Ubiqua de interesse para o autor deste documento.

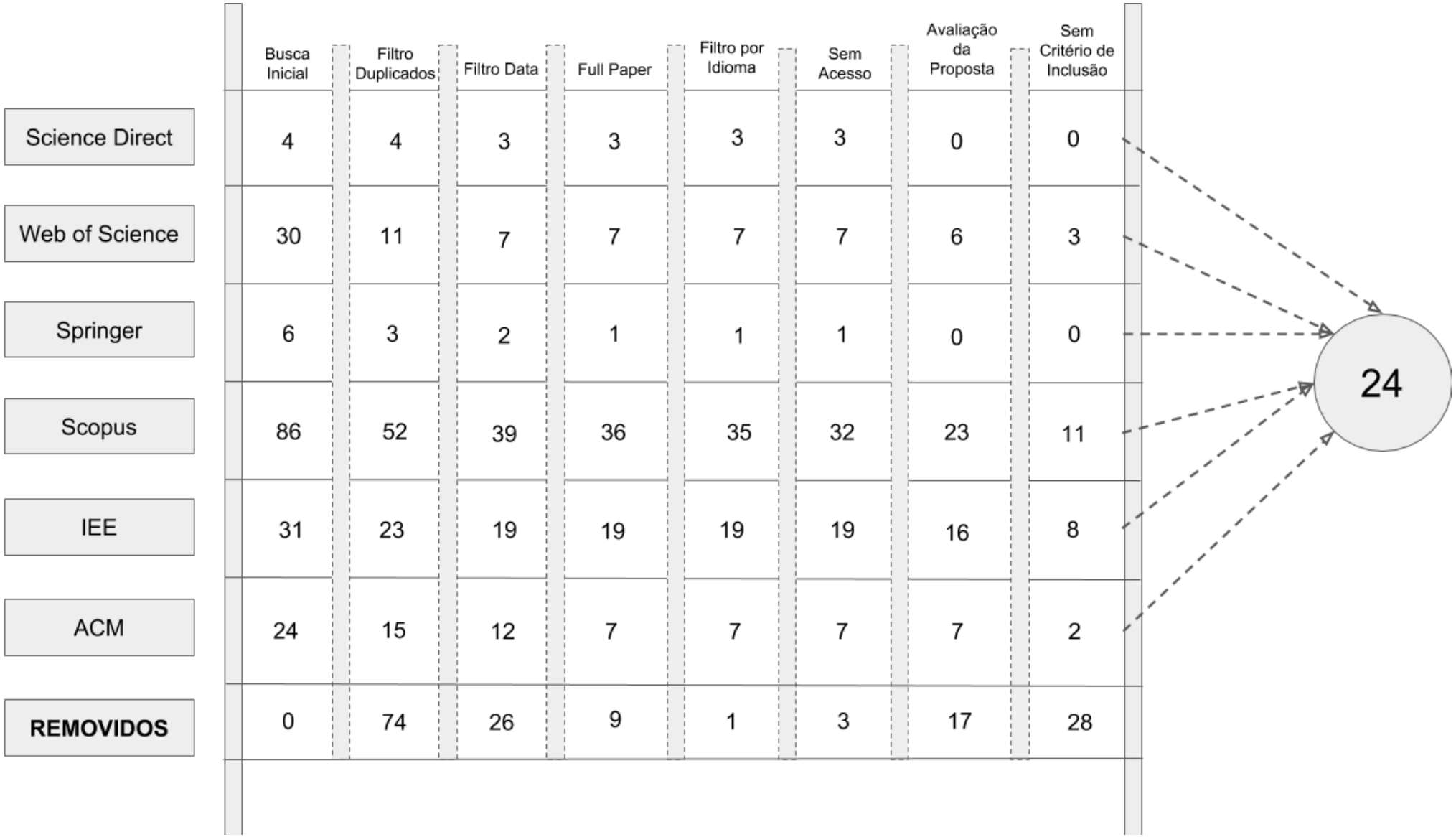

Figura 7 – Fluxo de remoção.

3.2 Trabalhos Relacionados

Com a execução do mapeamento sistemático da literatura foram selecionados dez trabalhos de interesse, os quais serão apresentados nas subseções a seguir, onde serão abordados os seguintes tópicos de interesse: motivação e justificativa do trabalho, a solução apresentada, avaliação e Resultados da Proposta.

3.2.1 Towards a Generalized Approach for Deep Neural Network based Event Processing for the Internet of Multimedia Things

- **Motivação e Justificativa do Trabalho:** O uso de dispositivos IoT multimídia tem aumentado consideravelmente (uso de câmeras para monitorar o trafego de uma cidade por exemplo), desta forma os tipos dos eventos criados na IoT estão também mudando, onde estes eventos multimédia geram dados não estruturados, gerando uma procura crescente na utilização eficiente do processamento de fluxos de eventos multimídia. No entanto, os mecanismos de processamento de eventos atuais têm suporte limitado ou inexistente para tipos de evento não estruturados.

- **Solução Apresentada:** É proposto um sistema genérico para manipular eventos da Internet das Coisas Multimídia (IoMT) como um tipo de evento nativo em ferramentas de processamento de eventos com alta eficiência. O sistema proposto estende as linguagens de processamento de eventos com a introdução de operadores para análise multimídia de eventos não estruturados (eventos multimídia) e aproveita um combinador de eventos baseado em rede neural convolucional profunda para processamento de eventos de imagem, para extrair recursos.

- **Avaliação e Resultados da Proposta:** O sistema desenvolvido foi otimizado usando uma abordagem de seleção de classificador baseada em restrições de assinatura. Os resultados obtidos mostram que a ferramenta atinge uma taxa de transferência média de 110 quadros/segundo com uma precisão aproximada de 66,34% em eventos do mundo real de várias aplicações de cidades inteligentes. Foi apresentado ainda um teste de desempenho com o aumento do numero de classes por classificador, onde os resultados obtidos mostram uma taxa de transferência estável para um classificador de uma classe, porem com o aumento do numero de classes a taxa de transferência cai continuamente.

3.2.2 A Web-based Approach using Reactive Programming for Complex Event Processing in Internet of Things Applications

- **Motivação e Justificativa do Trabalho:** Nos últimos anos a Internet das coisas (IoT) tem crescido substancialmente, aumentando progressivamente o numero de dispositivos conectados a rede, estima-se que em poucos anos cada um dos

objetos de uso comum irá conter sensores para coletar e/ou fornecer algum tipo informação ou serviço para seus usuários, se conectando na Internet e gerando cada vez mais uma enorme quantidade de dados para serem trafegados pela rede. Esse crescente aumento no numero de dispositivos e consequentemente a grande expansão no volume de dados, gera a necessidade que seja desenvolvida uma abordagem simples para que se possa lidar com esta nova grande avalanche de dados.

- **Solução Apresentada:** Foi proposto a combinação de duas abordagens distintas para a solução do problema citado: a CEP(*Complex Event Processing*) e WoT (*Web of Things*) com o uso de Ferramentas gráficas que exploram programação de fluxo (Mashups). Também utilizou-se Programação Reativa para o desenvolvimento dos operadores CEP que foram fornecidos como uma extensão da plataforma WoT Node-RED, onde foram implementado três dos programas Coral8 amplamente referenciados para sistemas CEP.

- **Avaliação e Resultados da Proposta:** Para a avaliação da proposta do trabalho, um cenário de caso de uso é apresentado onde para este proposito usou-se o simulador node-red-node-pi-sense-hatsimulator, desenvolvido pela equipe Node-RED que tem como objetivo reproduzir uma placa real Raspberry PI a qual incorpora alguns sensores e atuadores como LEDs, temperatura, pressão barométrica e sensores de umidade, entre outros, os quais foram usados para a simulação dos CEP da proposta. Com o desenvolvimento deste trabalho os autores citaram duas como as principais contribuições da pesquisa: (1) uma abordagem visual para construir consultas CEP para aplicativos de Internet e (2) o uso de Programação Reativa para detectar e acionar o CEP.

3.2.3 Semantic IoT Middleware-enabled Mobile Complex Event Processing for Integrated Pest Management

- **Motivação e Justificativa do Trabalho:** Existem diversos desafios na agricultura moderna que são tipicamente encontrados no domínio dos Sistemas Ciber-Físicos (CPSs), dentre estes podemos citar: conhecimento e deficiência de infraestrutura, informações incompletas, fontes limitadas de informação, perturbações externas (clima), autoridade de controle limitada (fertilizantes não podem fazer uma planta crescer arbitrariamente rápido). O gerenciamento agrícola moderno depende de muitas metodologias diferentes de sensoriamento para fornecer informações precisas sobre a cultura, o clima e as condições ambientais. Graças a miniaturização, da grande evolução e da difusão de sensores e recursos computacionais de baixo custo, tornou-se possível o desenvolvimento de dispositivos que produzem dados e que interagem entre sí, produzindo assim

uma rede de "coisas", gerando dados, processos e serviços interconectados. Desta forma os CPSs estão transformando a indústria agrícola.

- **Solução Apresentada:** O trabalho propõe uma infraestrutura inteligente projetada para processar fontes de dados heterogêneas, como dados de sensores, dados meteorológicos e conhecimento agrícola coletado em uma ontologia, possibilitando uma comunicação mais suave e homogênea entre os dispositivos de uma infraestrutura dinâmica, configurável e extensível. A solução desenvolvida é baseada em processamento de eventos complexos (CEP) com o uso da ferramenta Esper, onde um modulo é executada parcialmente em dispositivos móveis através da introdução do DeviceHive, um *middleware* da Internet das Coisas (IoT), ainda fez-se uso de uma linguagem de programação com suporte a mecanismos de reflexão, os quais servem como uma interface entre os componentes da IoT e o conhecimento ontológico. Segundo os autores a solução visa tornar-se um instrumento utilizado para conscientizar sobre o uso dos tratamentos agrícolas, onde o agricultor pode (i) ter acesso a todas as informações relacionadas ao domínio de interesse no momento necessário, (ii) criar um plano de defesa personalizado, (iii) receber alertas de mudanças nas condições climáticas e (iv) receber notificações e recomendações sobre seus planos de tratamento.

- **Avaliação e Resultados da Proposta:** Para a validação da proposta desenvolvida foi apresentado uma instanciação de um cenário real, projetando também uma Ontologia OWL 2 que codifica o conhecimento sobre aspectos relacionados à prática de Manejo Integrado de Pragas. Também os autores executaram um primeiro conjunto de experimentos para validar a abordagem de fornecer a ferramenta para uma empresa e testar componentes individuais. Por fim os autores citaram como principais contribuições do trabalho: (i) a possibilidade de usar o motor CEP em tempo de execução do sistema, o que permite o monitoramento orientado a eventos e notificações de atualização, e (ii) sistema de modelagem com ontologias compreensíveis homem-máquina, que garante uma reconfiguração mais fácil a ferramenta.

3.2.4 Predictive Analytics for Complex IoT Data Streams

- **Motivação e Justificativa do Trabalho:** Os CEP são capazes de fornecer soluções escaláveis e distribuídas para lidar com fluxos de dados complexos em tempo real, no entanto, os CEPs não possuem a capacidade de realizar predições assim como muitas das técnicas de aprendizado de máquina e análise estatística de dados. A grande parte dos aplicativos CEP disponíveis na literatura destina-se apenas a fornecer soluções reativas ao correlacionar fluxos de dados usando regras predefinidas, não explorando dados históricos devido a sua me-

mória limitada. Existem diversos casos em que a predição de um evento futuro é muito mais útil que apenas a detecção do mesmo, por exemplo, seria muito mais útil a predição de um congestionamento em uma auto estrada do que sua detecção, já que caso conseguíssemos prever tal evento com certa antecedência, poderíamos informar os administradores de trafego para que assim estes possam tomar as medidas preventivas de modo a evitar o congestionamento. Podemos citar ainda diversos outros casos onde a predição de eventos futuros podem trazer diversos ganhos como a previsão de desastres naturais e doenças epidêmicas.

- **Solução Apresentada:** Neste trabalho foi proposto uma arquitetura pró-ativa capaz de explorar dados históricos usando técnicas de aprendizado de máquina em conjunto com processamento de eventos complexos, de forma a combinar o poder do processamento de dados em tempo real do CEP com a capacidade de predição de eventos das técnicas de ML. Foi apresentado um algoritmo de predição adaptativo chamado de AMWR (*Adaptive Moving Window Regression*) para dados dinâmicos de IoT, capaz de realizar predições precisas quase que em tempo real, e ainda sendo capaz de trabalhar em conjunto com o CEP. Para a execução da proposta foram utilizados: Node-RED para fornecer o Front-End da arquitetura, o Apache Kafka como Broker de mensagens e por ultimo, a implementação foi elaborada em Python com o módulo de aprendizagem de máquina scikit-learn.

- **Avaliação e Resultados da Proposta:** Para avaliação da proposta foi elaborado um caso de uso do mundo real onde dados de trafego de sistemas de transportes inteligentes foram usados para os testes, onde o algoritmo de predição foi capaz de atingir uma precisão de 96%, demonstrando assim a sua viabilidade de uso, já que com predições corretas sobre o trafego, como as que foram apresentadas nos testes, permitem que os administradores do sistema gerenciem o tráfego de uma maneira melhor, tomando decisões para evitar situações indesejadas, como congestionamentos por exemplo. Os autores do artigo citam como principais contribuições do trabalho: A implementação de uma arquitetura genérica baseada em componentes de código aberto para combinar ML com CEP, a fim de prever eventos complexos para aplicativos proativos de IoT; O desenvolvimento de um algoritmo de predição adaptativo para fluxos de dados dinâmicos de IoT que foi implementado em um caso de uso real do ITS atingindo uma precisão de até 96%. também foi proposto um novo método para encontrar tamanho ótimo para janela de treinamento, explorando componentes espectrais de dados de séries temporais; A modelagem do erro introduzido pelo algoritmo de previsão usando uma distribuição paramétrica e a derivação em expressões para o

erro global do sistema, à medida que o erro se propaga através do CEP.

3.2.5 DRESS: A Rule Engine on Spark for Event Stream Processing

- **Motivação e Justificativa do Trabalho:** Nos últimos anos o numero de dispositivo conectados a rede vem aumentando, com esse crescimento, a quantidade de fluxos de dados, aumenta simultaneamente, gerando a necessidade de sistemas capazes de reagir automaticamente a determinados eventos desencadeados por estes fluxos de dados. Tais sistemas se baseiam em um conjunto de regras pre definidas, onde através da análise dos fluxos de informações, executam determinadas ações que satisfação a alguma das regras deste conjunto. Nas últimas três décadas, sistemas como estes têm sido amplamente empregados em empresas, governos e organizações. Porem com o aumento crescente no tamanho dos fluxos de dados, como o grande numero de fluxos produzidos por eventos de dispositivos da Internet of Things (IoT), fazem com que os atuais sistemas baseados em regras enfrentem sérios desafios em termos de velocidade, escalabilidade e tolerância a falhas.

- **Solução Apresentada:** O artigo apresenta a proposta de adaptar sistemas baseados em regras para trabalhar em conjunto com o Spark Streaming visando desta forma melhorar seu desempenho. Foi apresentado uma Transformação do algoritmo Rete, que está por trás de muitos dos *Rule based systems* (RBSs) atuais, esta transformação faz com que o algorítimo funcione como um mecanismo de regras no ambiente do Spark. Também foi introduzido juntamente com um novo sistema de mensagens baseado em Kafka o DRESS (*Distributed Rule Engine no Spark Streaming*) onde foi demonstrado uma forma automatizada de transformar regras escritas no estilo do Apache Drools para serem executadas no DRESS, tornando fácil para os atuais usuários do Drools mover seus sistemas para o DRESS sem esforço, este método de transformação de regras é baseada em técnicas MDA e na biblioteca de usuários SiTra.

- **Avaliação e Resultados da Proposta:** O sistema proposto foi avaliado com a ajuda de um estudo de caso, onde foi simulado um sistema bancário para a execução dos testes. Os autores usaram o DRESS para transformar as regras CEP definidas para o ambiente de estuo, em código Scala e assim executá-lo no Spark Streaming, um gerador de dados foi criado com o intuito de produzir informação aleatoriamente para a simulação do ambiente bancário, incluindo fluxos de caixa, contas e períodos contábeis com um parâmetro de escala. Durante os testes o DRESS demonstrou uma melhora significativa de desempenho e escalabilidade se em comparação ao Drools, demonstrando ser capaz de lidar com grandes volumes de dados, em contra partida, o Drools não demonstrou esta

mesma capacidade. Além da alta capacidade de processamento, o DRESS se demonstrou mais flexível em termos de gerenciamento de memória, mesmo nos testes executados em uma única máquina, este pode processar um conjuntos de dados maiores que o Drools e em menos tempo. Assim os autores destacam que com os dados coletados pelo estudo de caso, se pode demonstrar que o DRESS tem potencial para resolver muitos dos problemas de processamento de grande fluxo de dados presentes nas RBSs.

3.2.6 TrustCEP: Adopting a Trust-Based Approach for Distributed Complex Event Processing

- **Motivação e Justificativa do Trabalho:** O avanço da Internet das Coisas(IoT), com o uso de sensores modernos e dispositivos moveis capazes de capturar grandes quantidades de informações, estimulou o desenvolvimento de aplicativos aptos a trabalhar com essa nova grande avalanche de informações. Uma técnica eficaz que surgiu com o objetivo de extrair informações contextuais de alto nível deste grande fluxo de dados foi o CEP(*Complex Event Processing*), facilitando a analise de dados em tempo real provenientes de fontes heterogêneas e distribuídas. Considerando que o contexto dos usuários pode ser de informações sensíveis, a preservação da privacidade destes dados é critica, tendo em vista que o processamento do contexto do usuário pode ocorrer em vários dispositivos (possivelmente maliciosos), especialmente em cenários colaborativos. Os trabalhos atuais sobre processamento de eventos complexos geralmente negligenciam o nível de privacidade dos dados do contexto de seus usuários onde estes são processados e diferentes dispositivos, muitas vezes com níveis de segurança desconhecidos.

- **Solução Apresentada:** Para solucionar o problema de controle de privacidade, os autores propõem uma abordagem baseada em confiança, onde usam esta métrica de confiança definida para o posicionamento e a execução de operadores CEP em ambientes distribuídos, atribuindo o processamento de dados sensíveis para dispositivos que tenham um nível de confiança mais alto. Para a definição deste valor, a ferramenta pode usar o histórico de interação entre os dispositivos, ou ainda usar uma funcionalidade de recomendações de confiança, a qual faz uma verificação de similaridade baseada em cosseno, evitando assim ataques de collusion e on-off. Como as fontes de informações em um ambiente IoT são decentralizadas o modelo do sistema construído escolhido pelos autores foi entorno de uma rede device to device(D2D).

- **Avaliação e Resultados da Proposta:** Para a validação da proposta, um sistema CEP foi desenvolvido de forma distribuída baseado em SmartPhones, o

qual da a possibilidade dos usuários se comunicarem com o uso do Bluetooth e processar gráficos de maneira distribuída, esta ferramenta foi chamada de Trust-CEP a qual foi usado para avaliar a abordagem. Para medir as relações de confiança, foi gerado um histórico de interações entre usuários em canais síncronos e assíncronos, os quais representam aspectos comportamentais da confiança dos usuários. Como métricas de comparação foram usado o consumo médio de energia e a troca de dados na rede, onde os autores observaram que com a implementação da proposta os SmartPhones usados para os testes apresentaram um leve aumento de 2-6% no consumo de energia, se comparado a abordagens quem não levam em consideração a privacidade dos dados, em contra partida o modelo proposto se mostra robusto contra ataques collusion e on-off. Os autores citam como principais contribuições de seu trabalho: o desenvolvimento de um modelo de gestão de confiança (descentralizada) para adaptar a disseminação de eventos e a colocação de operadores para o CEP distribuído; Foi introduzido um modelo de gestão de confiança baseado nas relações do usuário e no histórico de interação de comunicação; Foi apresentado um esquema de recomendação de confiança robusto usando a medida de similaridade de cosseno.

3.2.7 Anaysis of Controller Based IEEE 802.11 System with Similarity Measure Clustering

- **Motivação e Justificativa do Trabalho:** A eficiência de um sistema WiFi que contenha dezenas de estações em uma área física pequena, em suma, é dada pela capacidade do sistema de alocar de forma ótima canais de rede para estas estações de forma a evitar conflitos de frequências ns rede ao máximo. Com a evolução dos dispositivos moveis, com alta capacidade de trafego de dados, sua grade popularização e seu uso acentuado em locais densamente povoados como por exemplo o uso de smartphones em grandes edifícios, se faz necessário o desenvolvimento ferramentas inteligentes capazes de oferecer bons níveis de QoS aos usuários. Para a configuração dos canais em um modo de operação normal uma rede WiFi usa o algoritmo de gerenciamento de recursos de rádio (RRM) onde este é executado periodicamente. Sendo definido vários valores de configurações nos pontos de acesso para iniciar tarefas de gerenciamento adicionais no controlador entre os períodos, as quais podem ser enxergadas como eventos complexos. Devido à complexidade, esses parâmetros para os valores do algoritmo RRM são normalmente fornecidos como valores padrões. Existindo uma falta significativa de experiências práticas sobre os operadores de serviço WiFi em busca dos valores ideais.

- **Solução Apresentada:** Como proposta do trabalho os autores levantam as seguintes questões de: Qual é o nível real de desempenho de um determinado

sistema WiFi configurado com o controlador? Quão sensato é este algoritmo RRM para futuros ataques de inundação nos canais de rádio em um AP ou terminal móvel? Com o intuito de responder a estas questões levantadas, os autores propõe a execução de uma análise profunda deste sistema onde estes usam uma abordagem de análise estatística baseada em mecanismos de agrupamento de comportamento e detecção de mudanças, fazendo a analise das informações coletadas para assim chegar a uma conclusão final. Alem disso os autores também propõem um novo método de clustering baseado em medidas de similaridade e aplicado nas redes Wifi IEEE 802.11.

- **Avaliação e Resultados da Proposta:** Para a validação da proposta do trabalho, foram executadas as medições do sistema WiFi na rede de informática da Universidade de Debrecen, os autores também ressaltam que as medições das duas tecnologias WiFi relativas as bandas de 2,4 GHz e 5 GHz foram analisadas separadamente. Após a execução dos testes sobre as redes wifi da universidade, os autores concluem que o método de clustering baseado em comportamento proposto, é capaz de avaliar o desempenho do algoritmo de gerenciamento de recursos de rádio do controlador WiFi de forma eficiente, sendo capaz de informar os valores reais de desempenho que os AP produzem com a configuração do algoritmo padrão e gerar os valores ótimos mais adequados para aquela rede.

3.2.8 Parallel big data processing system for security monitoring in Internet of Things networks*

- **Motivação e Justificativa do Trabalho:** Atualmente as redes de Internet das Coisas (IoT) tem se popularizado em diversas áreas, assim como a sua popularização, a preocupação com a segurança dessas redes tem aumentado, levando ao interesse do desenvolvimento de sistemas de segurança sofisticados para a proteção destas redes, os quais são necessários ja que o uso de sistemas de proteção tradicionais são de difícil ou impossível aplicação devido às peculiaridades para a construção e operação de redes IoT. Podemos citar como fatores complicantes na implementação de sistemas de segurança nas redes IoT como: a necessidade de analisar grandes quantidades de dados em tempo real com o menor custo computacional possível, grande numero de fontes de dados heterogêneos, computação limitada e recursos de energia limitado. Outro fator que destaca a importância de sistemas de segurança para redes IoT é a grande variedade de ataques cibernéticos existentes e a gravidade de suas consequências. Sistemas de informações de segurança e gerenciamento de eventos (SIEM) tem a capacidade de monitorar a segurança de redes por meio da coleta de dados sobre: eventos de interesse de dispositivos remotos, sensores de informação e

seu processamento preliminar. Porem redes IoT possuem um grande número de tipos de fontes de dados, o que pode tornar extremamente complexo o monitoramento da segurança de rede devido a alta intensidade de fluxos de eventos, levando a necessidade do desenvolvimento de sistemas de segurança com capacidade de processamento de Big Data.

- **Solução Apresentada:** Levando em consideração as limitações citadas para o desenvolvimento de sistemas de segurança para redes IoT, o trabalho propõe uma nova arquitetura de segurança para redes IoT baseada em um sistema de processamento paralelo distribuído de Big Data. A ferramenta de processamento de dados paralelo desenvolvido tem as seguintes características: devido ao uso da tecnologia CEP (Processamento de Eventos Complexos), o sistema implementa funções básicas de pré-processamento em tempo real, as quais são: normalização de dados, filtragem de dados, agregação de dados e correlação de dados; Os resultados do processamento preliminar dos dados são fornecidos pela representação visual do sistema; A ferramenta é configurado para operar sob condições de limitações computacionais, inerentes aos elementos de rede da IoT. Para o desenvolvimento do sistema de processamento paralelo de dados de segurança, foi usado como base a ferramenta de código aberto Hadoop em conjunto com o ambiente de processamento de dados distribuído Apache Spark. A arquitetura do sistema também inclui componentes responsáveis pela coleta, armazenamento, agregação, normalização, análise e visualização de dados onde: a Agregação dos dados, normalização, análise e visualização são realizadas "on-the-fly"; Os dados são armazenados em um sistema de arquivos distribuídos do HDFS, proporcionando um aumenta da confiabilidade do armazenamento e da velocidade com que as solicitações de dados são processadas.

- **Avaliação e Resultados da Proposta:** Para avaliação da proposta do artigo os fluxos de dados usados para os testes foram obtidos combinando fluxos de ventos de segurança em um fragmento da rede IoT com fluxos representados em um banco de dados externo de tráfego em uma rede real de computadores. A avaliação aplicada mostrou que mesmo em um ambiente IoT com recursos computacionais limitados quando o sistema executa com o Hadoop, a ferramenta desenvolvida apresenta um desempenho razoavelmente alto, excedendo significativamente as implementações conhecidas, porem quando este é executado no Apache Spark a ferramenta mostrou um aumento de desempenho de cerca de dez vezes, se o ambiente tiver uma quantidade de memoria RAM suficiente. Como principais contribuições do trabalho os autores citam: A execução de um comparativo de desempenho das plataformas Hadoop e Spark implementadas em uma sistema de segurança de redes aplicado a IoT, O desenvolvimento de

uma arquitetura destinada ao processamento paralelo e ao monitoramento de redes IoT.

3.3 Discussão dos Trabalhos Relacionados

Conforme destacado na introdução deste trabalho, de acordo com a literatura (em especial alguns "*surveys*"), inclusive com os trabalhos identificados no estado da arte, os seguintes aspectos foram identificados como problemas relacionados as pesquisas em arquiteturas/modelos de segurança adaptativa:

1. se concentram em apenas um serviço/objetivo de segurança, como a autenticação (AMAN; SNEKKENES, 2014), (ELKHODARY; WHITTLE, 2007);
2. as abordagens existentes não definem todo o ciclo de adaptação MAPE (YUAN; MALEK, 2012).
3. fornecem uma arquitetura genérica sem detalhar os métodos usados em cada componente (AMAN; SNEKKENES, 2014), (YUAN; MALEK, 2012);
4. a falta de detalhes nas arquiteturas genéricas dificulta a reutilização e extensibilidade das abordagens propostas (YUAN; MALEK, 2012);

No que diz respeito ao primeiro e segundo problemas elencados, o mapeamento sistemático buscou filtrar esta questão, sendo selecionados apenas artigos onde as arquiteturas/modelos concebidos podem ser aplicados em diferentes objetivos de segurança e que contemplam o ciclo MAPE por inteiro. Já quanto ao terceiro e quarto tópicos levantados, é possível observar que o primeiro trabalho apresentado neste capítulo (ABIE; BALASINGHAM, 2012) - o qual é concebido por uma das referências na área (Abie Habtamu) - possui tal limitação, a qual é tratada apenas em alguns dos demais trabalhos.

Tendo estas observações em vista, a tabela 1 busca apresentar algumas das características consideradas para comparação entre os trabalhados identificados como estado da arte em segurança adaptativa para IoT. O sinal de hífen ("-") na tabela representa a falta de informações ou limitação por parte do trabalho quanto a referida característica. A seguir é apresentada uma breve descrição das características selecionadas:

- coleta: uma dos desafios na IoT diz respeito a coleta de eventos de dispositivos com recursos limitados, logo, esta característica busca identificar se são destacados no trabalho os detalhes para coleta dos eventos;
- normalização: uma vez que o foco é na IoT, a heterogeneidade e a consequente diversidade no formato dos eventos produzidos deve ser tratada, sendo assim,

este tópico identifica se a proposta detalha a estratégia utilizada para normalização;

- correlação: estratégia utilizada para correlação dos diferentes contextos identificados para identificação de situações de interesse;
- armazenamento: determina a tecnologia de armazenamento do conhecimento empregada, sendo relevante por fatores de expressividade, escalabilidade e usabilidade;
- implementação: visa caracterizar o nível de detalhamento do protótipo desenvolvido para validação do trabalho, podendo ser “Não”, “Parcial” e “Sim”;
- extensibilidade: representa a possibilidade de extensão da arquitetura/modelo proposto;
- reusabilidade: busca evidenciar se o trabalho descreve detalhes suficientes que permitem o reuso da proposta, sendo passível de replicação dos testes realizados;
- maturidade: descreve o nível de maturidade da abordagem em função da validação desenvolvida e da comunidade em torno das tecnologias empregadas;
- cenário: caracteriza a área de estudo do cenário de avaliação;
- escalabilidade: procura identificar limitações ou competências quanto a escalabilidade da proposta uma vez que na IoT o volume de dados tratados em função da quantidade de dispositivos adquirindo contextos é um desafio a ser considerado.

Em (EVESTI; SUOMALAINEN; OVASKA, 2013), exceto no que tange o emprego da ontologia, os detalhes de implementação identificados por este autor são considerados superficiais e as tecnologias adotadas (como por exemplo, Qt C++) são fortemente dependentes da plataforma empregada. Também não são descritos de forma clara as tecnologias envolvidas para coleta e normalização de eventos. Com isso, apesar do autor Antti Evesti ressaltar a sua abordagem como extensível e reutilizável, para o autor deste trabalho, esta afirmação pode ser aplicada apenas no que tange a ontologia, porém não no seu trabalho de maneira geral.

De forma geral, o quesito maturidade, a maior parte dos trabalhos apresentou cenários para validação da proposta, porém, as tecnologias envolvidas possuem restrição quanto à sua adoção pela comunidade, em especial pela utilização de ontologias, que apesar de ser um tópico importante de pesquisa em desafios de segurança da informação, não é possível afirmar que a sua adoção vem sendo praticada na área.

Tabela 1 – Tabela comparativa entre os trabalhos identificados como estado da arte em segurança adaptativa

	(ABIE; BALASINGHAM, 2012)	(EVESTI; SUOMALAINEN; OVASKA, 2013)	(AMAN; SNEKKENES, 2014)	(RAMOS; BERNABE; SKARMETA, 2015)	(MOZZAQUATRO et al., 2016)	(EL-MALIKI; SEIGNE, 2016)
Coleta	-	-	Sim	Sim	-	-
Normalização	-	-	Expressão Regular	SensorML	-	-
Correlação	Teoria dos Jogos	Regras próprias	XML	CEP	SPARQL	-
Adaptação	-	Ontologia	Ontologia	-	Ontologia	-
Conhecimento	-	OWL	OWL	-	OWL	-
Implementação	-	Parcial	Sim	-	Parcial	Sim
Extensibilidade	-	Parcial	Sim	-	Parcial	-
Reusabilidade	-	Parcial	Sim	-	Parcial	-
Maturidade	-	Validação, Comunidade	Validação, Comunidade	-	Validação	Validação
Cenário	-	Espaços Inteligentes	eHealth	IoT – Autenticação	Metalurgia	IoT
Escalabilidade	-	-	-	-	-	-

Percebe-se também que a adoção de ontologias por parte dos trabalhos (EVESTI; SUOMALAINEN; OVASKA, 2013), (AMAN; SNEKKENES, 2014) e (MOZZAQUATRO et al., 2016) implica em dificuldades de escalabilidade, sendo em geral uma problemática levantada como limitações em seus trabalhos ou teses derivadas. Além disso, em (AMAN; SNEKKENES, 2014), a tecnologia OSSIM empregada é reconhecida por possuir problemas de estabilidade e escalabilidade (ROCHFORD; KAVANAGH, 2015), (SHANKAR, 2014).

O trabalho (RAMOS; BERNABE; SKARMETA, 2015), por sua vez, apresenta um modelo genérico, sem detalhar os modelos e tecnologias empregadas. Assim assim, ele destaca alguns dos protocolos geralmente envolvidos para coleta de eventos na IoT, como o *Constrained Application Protocol* (CoAP), *Extensible Messaging and Presence Protocol* (XMPP) ou *Message Queue Telemetry Transport* (MQTT).

El-Maliki apresenta em sua tese (EL MALIKI, 2014) uma série de testes e simulações realizadas para validação, avaliando em especial a latência decorrente do uso da criptografia e o consumo de energia, os quais evidenciam estratégias de implementação em diferentes cenários da IoT. Apesar disso, o protótipo é fortemente associado ao estudo de caso, não sendo uma abordagem voltada para eventos, consequentemente não possuindo detalhes sobre a coleta de eventos, sua normalização, correlação, armazenamento, bem como estratégia empregada na adaptação. Além disso, não é

uma característica a possibilidade de extensão e reuso da proposta.

3.4 Considerações do Capítulo

Este capítulo apresentou os trabalhos identificados como estado da arte em arquiteturas ou *frameworks* genéricos de segurança adaptativa para IoT. O processo para esta análise seguiu o mapeamento sistemático da literatura. Os trabalhos foram descritos em termos do modelo proposto, buscando detalhar as estratégias de concepção e prototipação. Finalmente, foi realizada uma comparação entre os mesmos seguindo características consideradas oportunas considerando as críticas e desafios identificados durante esta revisão.

4 CONSIDERAÇÕES FINAIS

O presente trabalho buscou apresentar uma revisão conceitual sobre segurança adaptativa 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 arquiteturas para segurança adaptativa que promovam a adaptação dinâmica dos mecanismos de segurança de forma que as mudanças aplicadas não prejudiquem a eficiência, flexibilidade, confiabilidade e segurança dos ambientes da IoT. Tendo em vista a natureza ubíqua, 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.

Para a concepção dessas arquiteturas foi apresentado o ciclo de *feedback* MAPE-K, o qual consiste de um método formal que estabelece as etapas a serem executadas para a adaptação. É importante salientar que para implementar cada umas destas etapas algumas questões devem ser respondidas. Além disso, um sistema adaptativo deve contemplar auto-atributos como: autoconfiguração, auto-otimização, autocura e autoproteção. Não obstante, pesquisas vem sendo desenvolvidas nessa área indicando a ciência de contexto como outro atributo a ser explorado.

Desta forma, a segurança adaptativa baseada em contexto envolve a coleta de informações contextuais tanto do sistema como do meio ambiente, medindo o nível de segurança e as métricas, realizando o processamento dessas informações coletadas e respondendo às mudanças (i) ajustando parâmetros internos, como esquemas de criptografia, protocolos de segurança, políticas de segurança, algoritmos, diferentes mecanismos de autenticação e autorização, alterando a QoS e automatizando a reconfiguração dos mecanismos de proteção e/ou (ii) fazendo mudanças dinâmicas na estrutura do sistema de segurança (ABIE; BALASINGHAM, 2012).

Atualmente, existem várias abordagens para segurança adaptativa (ELKHODARY; WHITTLE, 2007; YUAN; MALEK, 2012). No entanto, conforme ressaltado no capítulo sobre o estado da arte, as abordagens existentes se concentram em objetivos de

segurança específicos. Percebe-se também a falta no tratamento total do ciclo de *feedback*, ou seja, as abordagens não definem todo o ciclo MAPE. Além disso, Yuan et al. observa que as arquiteturas genéricas não detalham os métodos usados em cada componente, o que dificulta a reutilização e extensibilidade das abordagens propostas. Com o mapeamento sistemático realizado 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.

REFERÊNCIAS

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

ALABA, F. A.; OTHMAN, M.; HASHEM, I. A. T.; ALOTAIBI, F. Internet of Things security: A survey. **Journal of Network and Computer Applications**, [S.l.], v.88, p.10 – 28, 2017.

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

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

AMAN, W.; SNEKKENES, E. EDAS: An Evaluation Prototype for Autonomic Event-Driven Adaptive Security in the Internet of Things. **Future Internet**, [S.l.], v.7, n.3, p.225–256, 2015.

ASHTON, K. That 'Internet of Things' Thing. **RFID Journal**, [S.l.], June 2009.

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.

BRÉZILLON, P. Context in problem solving: a survey. **Knowl. Eng. Rev.**, New York, NY, USA, v.14, n.1, p.47–80, May 1999.

BRÉZILLON, P.; ARAUJO, R. M. Reinforcing Shared Context to Improve Collaboration. **Revue d Intelligence Artificielle**, [S.l.], v.19, n.3, p.537–556, 2005.

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.

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

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.

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

ELKHODARY, A.; WHITTLE, J. A Survey of Approaches to Adaptive Application Security. In: INTERNATIONAL WORKSHOP ON SOFTWARE ENGINEERING FOR ADAPTIVE AND SELF-MANAGING SYSTEMS, 2007., 2007, Washington, DC, USA. **Proceedings...** IEEE Computer Society, 2007. p.16–. (SEAMS '07).

EVESTI, A.; OVASKA, E. Comparison of adaptive information security approaches. **ISRN Artificial Intelligence**, [S.l.], v.2013, 2013.

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

EVESTI, A.; TUTKIMUSKESKUS, V. teknillinen. **Adaptive Security in Smart Spaces**. [S.l.]: VTT, 2013. (VTT science).

GHORBANI, A.; LU, W.; TAVALLAEE, M. **Network Intrusion Detection and Prevention**: Concepts and Techniques. [S.l.]: Springer, 2010. (Advances in Information Security).

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

HEIMERL, J.-L. Effective Security Requires Context. Disponível em: <http://www.securityweek.com/effective-security-requires-context>, acesso em: 29 jan 2018.

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.

HU, W. et al. Online Adaboost-Based Parameterized Methods for Dynamic Distributed Network Intrusion Detection. **Cybernetics, IEEE Transactions on**, [S.l.], v.44, n.1, p.66–82, Jan 2014.

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

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.

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

LAMPRECHT, C. J. **Adaptive Security**. 2012. Tese (Doutorado em Ciência da Computação) — Newcastle University. School of Computing Science.

LANGHEINRICH, M. **Privacy in Ubiquitous Computing**. [S.l.]: J. Krumm, ed., CRC Press, 2010. 95-160p.

LI, X.; ECKERT, M.; MARTINEZ, J.-F.; RUBIO, G. Context Aware Middleware Architectures: Survey and Challenges. **Sensors**, [S.l.], v.15, n.8, p.20570, 2015.

LIU, J.; LIJUAN, L. A Distributed Intrusion Detection System Based on Agents. In: COMPUTATIONAL INTELLIGENCE AND INDUSTRIAL APPLICATION, 2008. PACIIA '08. PACIFIC-ASIA WORKSHOP ON, 2008. **Anais...** [S.l.: s.n.], 2008. v.1, p.553–557.

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.

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

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

ONWUBIKO, C. **Situational Awareness in Computer Network Defense**: Principles, Methods and Applications: Principles, Methods and Applications. [S.l.]: Information Science Reference, 2012.

OWASP. Disponível em: <https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project>, OWASP Internet of Things Project. Acesso em janeiro de 2018.

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.

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.

PETERSEN, K.; FELDT, R.; MUJTABA, S.; MATTSSON, M. Systematic Mapping Studies in Software Engineering. In: INTERNATIONAL CONFERENCE ON EVALUATION AND ASSESSMENT IN SOFTWARE ENGINEERING, 12., 2008, Swindon, UK. **Proceedings...** BCS Learning & Development Ltd., 2008. p.68–77. (EASE'08).

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

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

ROMAN, R.; ZHOU, J.; LOPEZ, J. On the features and challenges of security and privacy in distributed internet of things. **Computer Networks**, [S.l.], v.57, n.10, p.2266 – 2279, 2013. Towards a Science of Cyber Security Security and Identity Architecture for the Future Internet.

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

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

SUNDMAEKER, H. et al. **Vision and Challenges for Realising the Internet of Things**. [S.l.]: Publications Office of the European Union, 2010.

TORRES, A.; WILLIAMS, J. Maturing and Specializing: Incident Response Capabilities Needed. **SANS Institute. SANS Analyst Program**, [S.l.], 2015.

TWENEBOAH-KODUAH, S.; SKOUBY, K. E.; TADAYONI, R. Cyber Security Threats to IoT Applications and Service Domains. **Wireless Personal Communications**, [S.l.], v.95, n.1, p.169–185, Jul 2017.

VIEIRA, V.; MANGAN, M.; WERNER, C.; MATTOSO, M. Ariane: An Awareness Mechanism for Shared Databases. In: **Groupware**: Design, Implementation, and Use. [S.l.]: Springer Berlin Heidelberg, 2004. p.92–104. (Lecture Notes in Computer Science, v.3198).

WEBER, R. H. Internet of Things – New security and privacy challenges. **Computer Law and Security Review**, [S.l.], v.26, n.1, p.23 – 30, 2010.

WEISER, M. The Computer for the 21st Century. **Scientific American**, [S.l.], v.265, n.3, p.66–75, January 1991.

WEYNS, D.; IFTIKHAR, M. U.; MALEK, S.; ANDERSSON, J. Claims and Supporting Evidence for Self-adaptive Systems: A Literature Study. In: INTERNATIONAL SYMPOSIUM ON SOFTWARE ENGINEERING FOR ADAPTIVE AND SELF-MANAGING SYSTEMS, 7., 2012, Piscataway, NJ, USA. **Proceedings...** IEEE Press, 2012. p.89–98. (SEAMS '12).

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.

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.l.: s.n.], 2012. p.109–118.

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.l.: s.n.], 2013. p.663–667.