UNIVERSIDADE FEDERAL DA FRONTEIRA SUL
CAMPUS DE CHAPECÓ
CURSO DE CIÊNCIA DA COMPUTAÇÃO

JOVANI DE SOUZA

SEGURANÇA E PRIVACIDADE NA INTERNET DAS COISAS:
ESTUDO DE CASO COM A *KAA IOT PLATFORM*

CHAPECÓ
2019

JOVANI DE SOUZA

SEGURANÇA E PRIVACIDADE NA INTERNET DAS COISAS:
ESTUDO DE CASO COM A *KAA IOT PLATFORM*

Trabalho de conclusão de curso apresentado como requisito para obtenção do grau de Bacharel em Ciência da Computação da Universidade Federal da Fronteira Sul.
Orientador: Prof. Dr. Marco Aurélio Spohn

CHAPECÓ
2019

Souza, Jovani de

Segurança e privacidade na internet das coisas: Estudo de caso com a *Kaa IoT Platform* / Jovani de Souza. – 2019.
51 f.: il.

Orientador: Prof. Dr. Marco Aurélio Spohn.
Trabalho de conclusão de curso (graduação) – Universidade Federal da Fronteira Sul, curso de Ciência da Computação, Chapecó, SC, 2019.

1. Internet das Coisas. 2. Segurança. 3. Privacidade. 4. *Kaa IoT Platform*. I. Spohn, Prof. Dr. Marco Aurélio, orientador. II. Universidade Federal da Fronteira Sul. III. Título.

E-mail: jovanidesouza@estudante.uffs.edu.br

JOVANI DE SOUZA

SEGURANÇA E PRIVACIDADE NA INTERNET DAS COISAS:
ESTUDO DE CASO COM A *KAA IOT PLATFORM*

Trabalho de conclusão de curso apresentado como requisito para obtenção do grau de Bacharel em Ciência da Computação da Universidade Federal da Fronteira Sul.

Orientador: Prof. Dr. Marco Aurélio Spohn

Este trabalho de conclusão de curso foi defendido e aprovado pela banca avaliadora em: 11/12/2019.

BANCA AVALIADORA

Prof. Dr. Marco Aurélio Spohn – UFFS

Prof. Dr. Emilio Wuerges – UFFS

Prof. Me. Adriano Sanick Padilha – UFFS

AGRADECIMENTOS

Gostaria, inicialmente, de agradecer a minha família por sempre oferecer condições e oportunidades para que eu me dedicasse aos estudos. Quero especialmente dedicar este trabalho a minha mãe por sempre ter colocado a educação dos seus filhos em primeiro lugar, por sempre ter me incentivado nas minhas conquistas e ser compreensiva nas minhas falhas; sem o exemplo, o amor e o carinho dela eu não teria me tornado a pessoa que sou hoje. Também gostaria de agradecer a todos os professores que tive na universidade, por terem contribuído com a minha formação pessoal e profissional, em particular ao meu orientador, o professor Marco Aurélio Spohn, por todas os ensinamentos, orientações e conversas que tivemos nos últimos anos. Quero também dedicar essa conquista a todos os colegas da graduação que fizeram com que essa jornada fosse muito mais leve e divertida. Por fim, gostaria de agradecer a minha namorada Gabriele, por estar sempre ao meu lado em todos os momentos difíceis, por me ajudar com a revisão deste trabalho, por dividir comigo as alegrias e também as angústias da graduação e por todo amor e companheirismo de sempre.

RESUMO

Esta pesquisa tem como objetivo principal analisar as soluções de segurança e de privacidade implementadas pela plataforma de Internet das Coisas, denominada *Kaa IoT Platform*, por meio de um estudo de caso. A Internet das Coisas (IoT), objetivando ambientes inteligentes e interativos, estabelece que milhares de dispositivos de uso comum sejam conectados a algum tipo de rede e, assim, possam atuar sob controle ou de forma autônoma para melhorar a vida dos seus usuários gerando, coletando e processando dados em tempo real. O grande volume de dispositivos que podem ser conectados, somados ao barateamento nos custos de fabricação de pequenos *Hardwares* e a alta diversidade de tecnologias de redes sem fio, são fatores que fazem com que a IoT tenha grande relevância no mundo globalizado e, consequentemente, em pesquisas acadêmicas. As plataformas, enquanto *Softwares Middlewares*, surgem no intuito de padronizar e acelerar o desenvolvimento da área. Nesse cenário, esse estudo se torna relevante, pois para que o desenvolvimento da área possa acontecer, é fundamental que essas ferramentas sejam testadas e avaliadas positivamente. Tenciona-se, além disso, problematizar a importância da privacidade dos dados pessoais no paradigma da Internet das Coisas, demonstrando sua implícita inferência na adesão do usuário a essas novas tecnologias. Diante desse contexto, formulou-se a hipótese de que a plataforma *Kaa IoT Platform* seja uma ferramenta válida para o desenvolvimento de aplicações para a Internet das Coisas.

Palavras-chave: Internet das Coisas. Segurança. Privacidade. *Kaa IoT Platform*.

ABSTRACT

This research aims to analyze the security and privacy solutions implemented by the Internet of Things platform, named Kaa IoT Platform, through a case study. The Internet of Things (IoT), projecting intelligent and interactive environments, establishes that thousands of common devices are connected to networks and then can act under control or autonomously to improve the lives of the users, generating, collecting and processing data in real time. The large volume of devices that can be connected, allies of the low cost to manufacturing small Hardwares and the high diversity of wireless networking technologies, make IoT very important in the modern world and in academic researchs. Platforms as Middlewares, arise in order to standardize and accelerate the development of the IoT. In this scenario, this study becomes relevant to contribute to the development of the area, testing and evaluating these development tools. It is also intended to question the importance of privacy on personal data in the paradigm of the Internet of Things, demonstrating its implicit inference in user adherence to these new technologies. Given this context, it was hypothesized that the Kaa IoT Platform is a valid tool for the development of IoT applications.

Keywords: Internet of Things. Security. Privacy. *Kaa IoT Platform*.

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

AAA Autenticação, Autorização e Auditoria

AES *Advanced Encryption Standard*

API *Application Programming Interface*

AWS *Amazon Web Services*

CID Confidencialidade, Integridade e Disponibilidade

DDoS *Distributed Denial of Service*

DTLS *Datagram Transport Layer Security*

IOT *Internet of Things* (Internet das Coisas)

IP *Internet Protocol*

KPC *Kaa Protocol Communication*

LoRa *Long Range Network*

LPWAN *Low Power Wide Area Network*

M2M *Machine-to-Machine*

MQTT *Message Queuig Telemetry Transport*

NFC *Near Field Communication*

NoSQL *Not only Structured Query Language*

OTA *Over-The-Air-Updates*

PaaS *Plataform as a Service*

RAID *Redundant Array of Inexpensive Disks*

RSA *Rivest-Shamir-Adleman*

SDK *Software Development Kit*

SQL *Structured Query Language*

SSL *Secure Sockets Layer*

TCP *Transmission Control Protocol*

TLS *Transport Layer Security*

SUMÁRIO

1 INTRODUÇÃO

A Internet das Coisas, mais conhecida como IoT (*Internet of Things*) é considerada por muitos especialistas da área como a nova era da internet. É o nome dado ao paradigma que objetiva criar uma rede de dispositivos inteligentes, operando sistemas inteligentes. Este é um paradigma em pleno desenvolvimento que promete mudar drasticamente a forma como as pessoas utilizam seus dispositivos eletrônicos. A Cisco[1], uma das pioneiras e maiores empresas de redes e internet do mundo, considera que a IoT é a primeira grande evolução da internet como se conhece na contemporaneidade (EVANS, 2011).

A ideia básica de IoT é conectar à internet objetos comuns do dia a dia, chamados ao decorrer dessa pesquisa como "Coisas", como acessórios e eletrodomésticos, os quais passarão a trabalhar coletando dados e atuando sobre outros dispositivos. Desse modo, o principal objetivo dela é fazer com que essas Coisas sejam melhor utilizadas, gerando dados de interesse do usuário, podendo ser controladas remotamente e também atuando de forma completamente autônoma. Em outras palavras, o grande intuito da Internet das Coisas é melhorar a qualidade de vida dos seus usuários, utilizando para isso objetos conectados e inteligentes.

Esse ecossistema digital idealizado pela IoT oferece aplicações para as mais diversas áreas de negócios, do comércio, da agricultura e da indústria, fazendo com que as tecnologias desenvolvidas para a IoT influenciem na vida de todas as pessoas, direta ou indiretamente. O ambiente iminente da IoT, portanto, precisa que as tecnologias existentes sejam adaptadas para dar suporte ao aumento massivo de conexões que serão necessárias. Também é necessário que a IoT gerencie o grande volume de dados gerados por esses dispositivos. Com isso, é natural que muitos desafios precisarão ser superados para que a IoT possa alcançar seu potencial máximo.

Outro fator que gera preocupação com relação à popularização da Internet das Coisas é a questão da segurança e da privacidade dos dados gerados por esses dispositivos. Considera-se que cada novo dispositivo conectado à internet seja visto como uma nova porta de entrada para os sistemas e para a rede em si. A segurança desses dispositivos torna-se, então, uma das principais questões a serem melhoradas pela IoT, visto que esse aumento no número de dispositivos implica em um maior risco desses sistemas ficarem vulneráveis. Ademais, a capacidade de coleta de dados, adicionada a produtos comuns precisa ser supervisionada para que esses dispositivos não sejam usados para obter informações pessoais e privadas dos usuários.

Nesse sentido, visando facilitar a resolução de problemas e acelerar o desenvolvimento de novas aplicações para a Internet das Coisas surgem no mercado a ideia de *PaaS (Platform as a Service)* ou plataformas como serviço, dedicadas à Internet das Coisas. Uma plataforma de IoT é um *Software Middleware* que atua como uma ponte entre os usuários e suas Coisas. Além disso, possibilita a programação e o gerenciamento completo dos dispositivos a ela conectados. Sobretudo, permite a inserção de novos recursos para o ambiente da IoT, como técnicas de segurança para os dispositivos e de privacidade para os dados coletados.

[1] Disponível em: <https://www.cisco.com>. Acesso em: 15 set. 2019.

Diante disso, essa pesquisa objetiva fazer uma avaliação conceitual sobre as características da plataforma de Internet das Coisas, *Kaa IoT Platform*, focando especificamente nas funcionalidades de segurança da informação e de privacidade de dados que são implementadas pela plataforma. Pretende-se, assim, identificar as melhores práticas, as possíveis melhorias e os problemas que existem na versão *Open Source* da plataforma, contribuindo com a literatura e com o desenvolvimento da área da Internet das Coisas.

Para iniciar o desenvolvimento da pesquisa, foram buscados na literatura conceitos relacionados à Internet das Coisas, plataformas de IoT, segurança da informação e privacidade de dados, visando estabelecer um aporte teórico que estruturasse a pesquisa. Em seguida, no desenvolvimento da análise, os conceitos teóricos obtidos serão reutilizados para fundamentar a avaliação das técnicas de segurança e de privacidade que compõem um conjunto maior de funcionalidades disponíveis com a *Kaa IoT Platform*.

1.1 OBJETIVOS

1.1.1 Objetivo Geral

Avaliar conceitualmente as configurações de segurança e de privacidade implementadas pela plataforma de Internet das Coisas *Kaa IoT platform* em sua versão 0.10.0 que pertence a primeira geração *Kaa IoT Open Source*.

1.1.2 Objetivos Específicos

- Verificar se as primitivas usadas na plataforma possibilitam a escalabilidade das soluções de segurança e privacidade para múltiplos dispositivos.
- Certificar a veracidade das informações contidas na documentação oficial da plataforma.
- Catalogar as vantagens e as limitações das técnicas de privacidade que são utilizadas na construção da plataforma.

1.2 JUSTIFICATIVA E ESTRUTURA DO TRABALHO

A segurança da informação e a privacidade de dados são conceitos que ganharam grande destaque nos últimos anos, assim como o aumento na quantidade de dados pessoais que trafegam na internet. Considera-se que um grande volume de dados ocasiona um aumento na relevância do estudo da privacidade, pois entende-se que esses dados contêm muitas informações e, com isso, existe a necessidade de mantê-las seguras e privadas.

Considerando que a IoT prevê um grande aumento no número de dispositivos conectados à internet e, por consequência, um aumento no número de dados gerados por esses dispositivos,

se faz necessário pensar em resolver os impasses que permeiam o avanço da área. Com isso, pensar em modelos de desenvolvimento que certifiquem a segurança e a privacidade é algo que deve acontecer naturalmente nos próximos anos. Com o objetivo de contribuir para o avanço tecnológico da IoT, esta pesquisa propõe estudar, testar e avaliar conceitualmente uma plataforma de IoT sob a perspectiva da privacidade dos dados gerados pelas Coisas que a ela serão conectadas.

Esta pesquisa foi realizada por meio de um estudo de caso, baseado na plataforma de Internet das Coisas *Kaa IoT platform*, delimitando-se em sua versão gratuita *Kaa IoT Open Source* 0.10.0. O trabalho está dividido em 7 capítulos e neste primeiro objetiva-se introduzir a ideia da pesquisa, bem como especificar os objetivos esperados. O capítulo 2 é o início do referencial teórico do trabalho, no qual é descrito o conceito de Internet das Coisas, suas ambições, problemas e desafios.

No capítulo 3 é descrito o conceito e as aplicações das plataformas de Internet das Coisas e, especificamente, será apresentada a estrutura da plataforma utilizada na pesquisa a *Kaa IoT platform*. No capítulo 4, apresenta-se a revisão da literatura sobre segurança da informação e sobre privacidade de dados, esclarecendo suas necessidades e desenvolvimento nos últimos anos. O capítulo 5, por sua vez, tem como foco evidenciar a aplicação dos conceitos de segurança da informação e de privacidade de dados na Internet das Coisas, problematizando os requisitos da IoT e apontando os principais desafios da privacidade na área.

Além do exposto, o capítulo 6 é dedicado ao detalhamento da avaliação conceitual realizada, descrevendo assim os cenários de avaliação, as métricas e a metodologia utilizada na pesquisa, bem como os resultados obtidos durante o processo. Por fim, o capítulo 7 apresenta as considerações finais do projeto, buscando esclarecer a necessidade desse estudo e promover a ambição de continuidade da pesquisa.

2 INTERNET DAS COISAS

A Internet das Coisas, ou IoT (*Internet of Things*), é um conceito com crescente popularidade atualmente no século XXI. Ela propõe que objetos simples do dia a dia, chamados de "Coisas", como por exemplo eletrodomésticos, câmeras e acessórios (*wearables*) e, até mesmo, coisas mais complexas como carros, casas e empresas estejam conectados à internet e sejam identificados unicamente para coletar, processar e compartilhar dados. Dessa forma, a IoT almeja melhorar diversos cenários, como no comércio, na agricultura, nas cidades e na indústria, além de influenciar diretamente na qualidade de vida dos seus usuários quando aplicada no meio residencial (ATZORI; IERA; MORABITO, 2010).

2.1 UMA VISÃO GERAL SOBRE A INTERNET DAS COISAS

A IoT promete revolucionar a forma como as pessoas utilizam seus dispositivos eletrônicos, gerando grandes investimentos em produção e pesquisa nos próximos anos. A criação do termo é atribuída ao pesquisador britânico Kevin Ashton[1] que mencionou o conceito pela primeira vez no ano de 1999. Mesmo se passando 20 anos desde tal feito a ideia de IoT ainda está em seus primeiros estágios de desenvolvimento. A grande inovação oferecida por ela é referente à utilização da internet e de recursos computacionais que são, na sua maioria, exclusivos para a utilização humana e que destacam o indivíduo como o único fornecedor de informações. Já na IoT os computadores e dispositivos passam a serem vistos como entidades ativas e, assim, passam também a operar como usuários da internet.

O intuito de conectar esses objetos comuns à internet é fazer com que a sua utilização seja melhor aproveitada, oferecendo novas formas de uso para objetos conhecidos e, também, criando novos dispositivos inteligentes destinados a diversas novas funcionalidades. Nesse sentido, a ideia é que os objetos "conversem"entre si por meio da internet para realizar tarefas de forma autônoma e que também ofereçam controle e acesso remoto para seus proprietários. Isso ocorre no intuito de que eles possam coletar dados à distância além de controlar e gerenciar seus dispositivos remotamente.

Nos dias atuais, a internet se tornou um serviço básico, se expandindo para todo o mundo globalizado e alcançando usuários de várias esferas econômicas da sociedade. Sendo assim, o surgimento dos computadores pessoais e das redes móveis fez com que a internet passasse a ser um recurso indispensável em qualquer sistema computacional. Ela está presente no meio científico, educacional, industrial, empresarial e em quase todos os meios de produção, comunicação, negócios e finanças. Toda essa gama de utilidades, aliada a alta eficiência na velocidade de comunicação que a rede oferece, fazem com que, sem dúvidas, a internet seja considerada uma das maiores invenções das últimas décadas.

[1] Artigo publicado na data de 22 de junho em 2009, no qual o autor cita o acontecimento: <Disponível em: https://www.rfidjournal.com/articles/view?4986> Acesso em: 15 set. 2019.

Desde a sua criação, a internet tem se tornado cada vez mais presente e indispensável na sociedade. O que no início foi projetado para ser um meio de comunicação de longo alcance tornou-se na realidade uma ferramenta que interconecta diversos paradigmas como a Web, a *Cloud computing*, a *Fog computing*, a *Big Data* e a IoT por meio de um ecossistema digital de computadores e dispositivos eletrônicos. Afirma-se que a IoT, por sua vez, pode ser vista como uma evolução da internet como se conhece, visto que com ela o número de dispositivos conectados à internet aumenta drasticamente. Além disso, computadores e "Coisas" deixam de ser apenas terminais de uso e passam a ser também independentes, interagindo com outros dispositivos por meio de tecnologias M2M (*Machine-to-Machine*).

Em suma, a Internet das Coisas se caracteriza como uma rede de objetos conectados entre si e com a internet. Esses objetos inteligentes se fazem úteis por gerarem grandes quantidades de dados e, consequentemente, pela aplicação obtida com a utilização desses dados. Nesse contexto, eletrodomésticos, acessórios, câmeras, carros e uma infinidade de outras Coisas que estarão conectados à rede serão equipadas com microprocessadores, sensores e atuadores e vão estar, a todo momento, coletando dados e executando aplicações. Todas essas características abrem diversas possibilidades para o desenvolvimento de novas tecnologias que serão inseridas na nossa sociedade em um futuro próximo (RAJ; RAMAN, 2017).

2.2 APLICAÇÕES E FATORES ALIADOS DA ÁREA

Diante do exposto até então identifica-se que a Internet das Coisas é um conceito de tecnologia aplicável para incontáveis propósitos. Quando utilizada no meio doméstico, por exemplo, ela permite elevar o conceito de automação residencial a um nível muito maior de sofisticação. Eletrodomésticos comuns podem passar a gerenciar o seu próprio consumo de energia e, respondendo a sensores, podem atuar sobre outros dispositivos. Ademais, a própria casa pode se adaptar às grandezas externas, como luz, temperatura e umidade. A título de exemplificação, já é possível encontrar no mercado, à venda, refrigeradores que fazem o controle dos alimentos nela armazenados e geram, em tempo real, uma lista de compras para repor o seu estoque e, em seguida, enviam esses dados para o celular do proprietário que fica sabendo quais itens precisam ser adquiridos antes de chegar em casa.

Na indústria, a IoT oferece soluções completas para todos os níveis de produção. Ela permite que máquinas se comuniquem e possam aumentar sua produtividade, expandir a segurança dos processos de fabricação de um produto e diminuir os desperdícios de matéria prima. Na agricultura, oferece soluções de controle em tempo real para as condições da colheita de grãos, permitindo que sensores identifiquem melhores situações de plantio ao cruzar dados de temperatura, umidade e de condições do solo. De igual forma, possibilita que exista um melhor controle de qualidade na produção e no transporte de produtos perecíveis. Além do que foi destacado, tanto na indústria como na agricultura a IoT facilita a utilização de dispositivos para realizar tarefas de risco e, com isso, diminuindo a incidência de acidentes de trabalho.

Por conta dessas características, a IoT também proporciona a utilização de dispositivos conectados em setores como comércio e logística em que permite expandir ainda mais o impacto já causado pelo uso da internet nesses segmentos. Com isso, o rastreamento de compras *online* pode ser muito mais preciso do que é atualmente por meio de sensores que podem indicar a exata localização em que o produto comprado se encontra. Também é aplicável ao monitoramento de cargas frágeis, sendo necessário que determinadas condições específicas de transporte sejam atendidas. Para que isso seja possível, utiliza-se sensores de precisão que são embarcados nos veículos e que informam todos esses dados instantaneamente.

Ainda explorando as inúmeras possibilidades, a IoT também é uma das precursoras do paradigma de cidades inteligentes (*Smart cities*). Esse termo está relacionado com o ato de construir cidades totalmente conectadas e equipadas com sensores e atuadores, melhorando diversos cenários, como a segurança pública, a mobilidade urbana e o consumo inteligente de água e energia. Essa tecnologia também se expande aos veículos que circulam nas cidades inteligentes, fazendo com que esses possam enviar e receber informações de outros veículos e dispositivos para determinar melhores rotas a seguir e também identificar locais para estacionamento e pontos de congestionamento no trânsito.

Todo o conceito de Internet das Coisas é aplicável e fortemente sustentável pelas tecnologias móveis e vestíveis (*wearebles*). Portanto, grande parte das aplicações obtidas com ela é destinada aos dispositivos que estarão próximos das pessoas. Com isso, celulares, relógios, pulseiras e demais acessórios estarão realizando tarefas como controlar a atividade física e os sinais vitais do usuário, realizar transações financeiras com NFC (*Near Field Communication*) e contratar serviços sem crédito antecipado, como passagens de transporte público e estacionamento em parquímetros digitais.

Com esse amplo leque de possibilidades, essa interconexão digital com os objetos estimula o desenvolvimento de outras áreas paralelas e, consequentemente, contribui para o desenvolvimento de novas tecnologias. A IoT, nessa perspectiva, almeja a expansão da internet, descentralizando ainda mais o processamento e o local de armazenamento de dados gerados por computadores e dispositivos. Nesse sentido, conceitos como Computação em Névoa (*Fog Computing*) e Computação de Borda (*Edge Computing*) começam a ganhar mais espaço e popularidade, sobrepondo assim a hegemonia da Computação em Nuvem (*Cloud Computing).*

Vale destacar que diversos fatores são grandes coniventes da IoT, dentre eles pode-se citar a ampliação da cobertura mundial da internet que fez com que cada vez mais houvessem dispositivos conectados à rede. A grande diversidade de conexões também exerce um papel importante, fazendo com que computadores e dispositivos possuam diferentes tipos de conexões para diversos propósitos. Isto é, existem tecnologias de conexão que se encaixam melhor em cenários específicos e fazem com que a IoT seja democrática para desenvolvimento de novas aplicações, podendo utilizar todas essas variedades de tecnologias.

Outro fator de grande relevância nesse desenvolvimento acelerado tem relação com o barateamento no custo de dispositivos de *Hardware* em geral, pois tornou-se simples e econômico

adicionar mais tecnologia em produtos comuns. A construção de circuitos eletrônicos cada vez menores e mais potentes permitiu que atualmente os fabricantes possam projetar e elaborar seus produtos tradicionais, porém já com algum microcomputador embarcado sem um grande custo de produção e, em decorrência disso, com um valor de mercado mais acessível.

Desse modo, a IoT tenciona criar um ecossistema digital, inteligente e interconectado capaz de trabalhar sem interoperabilidade e de forma fluída e escalável. Para isso, o paradigma precisa que diversas tecnologias ainda sejam melhoradas e adaptadas para suportar esse ambiente e, além disso, precisa que as pessoas se sintam seguras a respeito dos efeitos causados pela introdução dessa ideia ao seu cotidiano. Acima de tudo, as possibilidades para a IoT são diversas e supõe-se que o avanço acelerado da área deve acontecer naturalmente nos próximos anos.

2.3 PROBLEMAS E IMPASSES ENFRENTADOS PELA IOT

Em contrapartida ao que concerne os diversos fatores aliados da área, a IoT tem seu desenvolvimento prejudicado por alguns aspectos e aponta alguns problemas e dificuldades. Tratando-se de tecnologia, em um cenário com múltiplos dispositivos conectados à rede, alguns pontos precisam ser seriamente pensados, como por exemplo a quantidade de dados gerados. As soluções de tratamento de dados que existem nos dias atuais ainda não estão prontas para receber, tratar e armazenar esse grande volume oriundos de tantas fontes diferentes. Portanto, cabe a IoT buscar soluções que trabalhem em paralelo a fim de tratar essa diversidade de Coisas que futuramente estarão conectadas à internet. Nessa linha de pensamento, a *Big Data* é uma grande área da computação que se propõe a estudar formas de solucionar esse tipo de problema. Acredita-se que é nessa área que os pesquisadores possivelmente encontrarão as melhores alternativas e soluções para o grande número de dados gerados pela IoT.

Ademais, outra circunstância que atrasa o desenvolvimento da IoT é em relação à infraestrutura da rede atual, pois apesar de existirem diferentes tecnologias de conexão elas ainda são limitadas. Mesmo utilizando conceitos de redes privadas e virtualização de endereços, os protocolos de rede, que são utilizados nos dias atuais, não são preparados para suportar tantos dispositivos. O protocolo IP (*Internet Protocol*) que oferece um rótulo numérico usado como endereço de rede para dispositivos se comunicarem, na sua versão 4 (Ipv4) utilizada predominantemente hoje na internet, utiliza 32 bits para endereçamento e dispõe de aproximadamente 4,29 bilhões de endereços únicos. Mesmo assim já é algo limitado em seu estado atual e, portanto, não será suficiente para suprir toda a demanda requerida que, conforme a Cisco, será de 50 bilhões de dispositivos conectados até o ano de 2020. Nesse sentido, a migração para uma versão mais robusta como a versão 6 (Ipv6), que utiliza 128 bits para endereçamento, é algo que necessita acontecer para que toda essa demanda seja satisfeita (EVANS, 2011).

As tecnologias de conexão usadas hoje em dia precisarão suportar não apenas uma grande largura de banda mas, principalmente, um grande número de dispositivos conectados

simultaneamente. Isso significa que é preciso manter o funcionamento completo da conexão do dispositivo sem nenhuma interrupção e também é preciso que essas tecnologias de conexão sejam escaláveis para mais dispositivos. Com base nisso, novas tecnologias LPWAN (*Low Power Wide Area Network*) como a LoRa (*Long Range Network*) e também o 5G são ferramentas que se pressupõe que irão contribuir muito com a solução dos problemas de conectividade da IoT.

O ambiente de IoT é considerado como um ambiente heterogêneo, isso quer dizer que todos os elementos de *Hardware* e *Software* contidos nele são diferentes entre si. Isso ocorre dado que os dispositivos possuem variados tipos de conexão e, principalmente, devido ao poder computacional diversificado que existe em um mesmo conjunto de dispositivos. Um relógio inteligente, por exemplo, não necessita ter o mesmo poder computacional de um servidor de dados, uma vez que com pouco recurso ele consegue fazer suas tarefas de forma eficaz e enviar seus dados para um servidor mais robusto que poderá então processar os dados recebidos e devolver uma resposta ao dispositivo.

Diante desse contexto, essa diversidade de componentes faz com que as resoluções de problemas também sejam mais trabalhosas. A IoT precisa de soluções que interconectem múltiplas tecnologias de forma eficiente, que considere essa diversidade e que se adapte para evitar gargalos no sistema. É necessário que todas as Coisas que integram um ambiente de IoT possam receber atualizações constantes de *Firmware* e, em particular, de segurança para garantir que esses dispositivos continuem funcionando e que não sejam alvo de ataques de terceiros. Vale sublinhar que esses ataques almejam obter dados privados dos usuários ou simplesmente interromper o funcionamento do sistema, assim como acontece em qualquer sistema computacional conectado à internet.

A falta de padronização de uma arquitetura de referência para o desenvolvimento de produtos de IoT é outro fator que acaba afetando negativamente o desenvolvimento da área. Por ser uma área ainda muito nova não existe um padrão a ser seguido e nem requisitos delimitados para a sua infraestrutura. A definição de um padrão de desenvolvimento obtido com uma arquitetura de referência é algo que está sendo considerado para contribuir com a solução dos problemas acima citados, principalmente os relacionados à diversidade de tecnologias, volume de dados, baixo poder computacional e segurança e privacidade dos dispositivos que integram esse ambiente.

De forma geral, a IoT necessita que as tecnologias sejam adaptadas para um cenário com bilhões de dispositivos. No próximo capítulo será elaborada uma discussão sobre plataformas de Internet das Coisas e a importância destas para a resolução dos problemas mencionados. Ademais, os problemas de segurança e de privacidade para dispositivos de Internet das Coisas também terão uma descrição detalhada em seus respectivos capítulos.

3 PLATAFORMAS DE INTERNET DAS COISAS

A Internet das Coisas, como já exemplificado no decorrer deste estudo, objetiva construir um ambiente altamente heterogêneo. Isso significa que os componentes que integram esse meio são diversificados entre si. Esses elementos podem ser identificados como *Hardwares*, *Softwares*, paradigmas, tecnologias de comunicação e demais ferramentas que possam afetar ou serem afetados pela IoT. Com isso, todas as aplicações e as soluções de problemas precisam ser adaptadas para sustentar essa diversidade. Portanto, este capítulo tem a intenção de descrever as entidades que integram o ambiente de IoT e, a partir disso, apresentar as plataformas de Internet das Coisas como uma ferramenta completa para o gerenciamento dessas entidades.

A ideia básica que faz com que a IoT seja possível é a de que qualquer coisa possa ser conectada à internet. Portanto, essa capacidade de transformar objetos comuns em objetos inteligentes, bem como a possibilidade de criação de novos objetos que possam se conectar uns com os outros, é o que faz com que toda o conceito de Internet das Coisas venha se desenvolvendo atualmente. Nesse sentido, o *Hardware* tem uma função fundamental no desenvolvimento da área, pois se aplica diretamente na construção física dos objetos e necessita que o ecossistema de IoT suporte a sua alta diversidade de dispositivos. Além dos modelos de computadores já conhecidos, outros modelos de menor porte, principalmente sistemas embarcados, farão parte do ambiente de IoT e, por isso, ela precisa oferecer compatibilidade para todas as arquiteturas de *Hardware* para que elas possam ser integralizadas ao paradigma.

Diante das discussões traçadas sobre a IoT, cabe ressaltar que ela foi criada pela união de diversos fatores ao passo que ela vem estimulando o desenvolvimento das tecnologias existentes e a criação de novos conceitos tecnológicos. Em decorrência disso, ela também precisa dar suporte aos paradigmas que fizeram ela se tornar uma realidade, como a *Cloud Computing*, a *Fog Computing*, a *Web* semântica e a *Big Data*. Nesse sentido, dar suporte aos paradigmas significa integrar todos os serviços e, primordialmente, contribuir com as soluções dos problemas que já são encontrados nos demais conceitos. Um exemplo simples é com a *Cloud Computing* (que oferece serviços hospedados na Internet) para que seja possível para a IoT continuar utilizando esses serviços em nuvem e desenvolver suas aplicações. É preciso que a IoT contribua com a solução dos problemas encontrados nesse paradigma citado, como o alto consumo de largura de banda, comum nesse tipo de cenário e que deve aumentar com o amadurecimento da IoT.

Visando contribuir com a solução dos problemas que atrasam o desenvolvimento da IoT, facilitando e centralizando o desenvolvimento de aplicações, surgem nesse contexto as plataformas de Internet das Coisas que são um tipo de *PaaS (platform as a service)*. Estas são *Softwares Middlewares* caracterizados por operarem como uma ponte entre usuário e aplicação ou então entre aplicações. De modo geral, uma plataforma é definida como um conjunto de *Softwares* que podem ser instanciados em uma rede local ou na internet e, além disso, podem ser executados de forma centralizada ou completamente distribuída, permitindo, assim, fazer um gerenciamento completo dos dispositivos de IoT que estão conectados à plataforma.

Esse gerenciamento é composto por diversas funcionalidades que variam de acordo com a versão da plataforma, mas, em geral, uma plataforma de Internet das Coisas oferece serviços de coleta de dados, autenticação, configurações, atuação sobre os dispositivos e também a implementação de protocolos de segurança e técnicas de privacidade. A grande vantagem em optar por uma plataforma de IoT é que com elas o processo de desenvolvimento torna-se simplificado. De certo modo, uma plataforma de IoT padroniza o ambiente, ou seja, todas as aplicações precisam estar de acordo com as características técnicas da plataforma.

Uma plataforma de IoT, além de segurança, precisa oferecer alguns serviços mínimos, como interoperabilidade, tratamento de grande volume de dados, descoberta e gerenciamento de coisas e tudo isso com uma interface gráfica de alto nível. As plataformas também são relevantes em IoT por permitirem que esses serviços sejam implementados de forma adaptável e escalável. Elas viabilizam que dispositivos que utilizam diferentes tipos de conexões possam se comunicar utilizando o servidor. Além disso, podem funcionar diferentes protocolos de comunicação e de segurança em uma mesma plataforma, criando desse modo diferentes níveis de privacidade e segurança que podem ser escolhidos de acordo com a capacidade e necessidade do dispositivo conectado (PIRES et al., 2015).

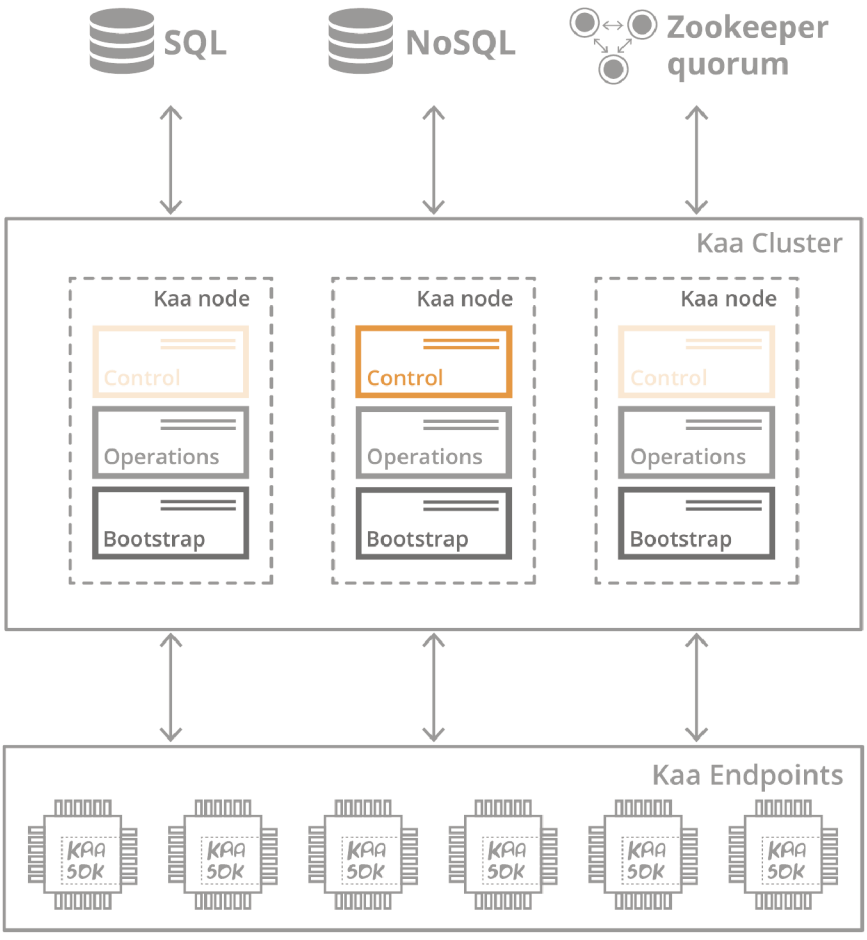
3.1 *KAA IOT PLATFORM*

A *Kaa IoT Platform*, também conhecida como *Kaa Project*, é uma plataforma de Internet das Coisas desenvolvida pela *CyberVision, Inc.* com o propósito de facilitar o desenvolvimento de produtos de IoT, oferecendo diversas soluções para que a prototipagem e os processos de implementação desses produtos sejam mais rápidos e seguros. Atualmente, a plataforma pode ser encontrada em duas gerações: a *Kaa IoT Open Source* que é a geração pioneira, totalmente gratuita e de código aberto que se encontra na versão 0.10.0; e, também, a *Kaa IoT Enterprise* que é a geração mais completa e atual, disponibilizada pela *KaaIoT Technologies, LLC.* como um *SaaS* (*Software* como serviço) pago, de código parcialmente aberto e que atualmente está na versão 1.0.0 (KAA IOT TECHNOLOGIES, 2019).

Esta pesquisa, visando cumprir os objetivos propostos, delimitou-se em estudar e analisar a primeira geração da plataforma, a *Kaa IoT Open Source* que, inicialmente, no desenvolvimento do projeto era a única disponibilizada pela desenvolvedora até então. Ainda assim, essa plataforma foi a escolhida para a pesquisa por ser totalmente de código livre, ter compatibilidade com diversas tecnologias conhecidas e por possuir os requisitos mínimos para desenvolvimento que foram elaborados durante o texto. Ademais, ela proporciona um grande número de possíveis aplicações e, esse cenário, necessita de boas técnicas de segurança e de privacidade aliados de protocolos leves e dinâmicos para poder oferecer seus serviços seguros e com qualidade. Diante disso, é esperado que as características técnicas da plataforma, que serão detalhadas em seguida, sejam testadas, analisadas e validadas de acordo com as bases teóricas obtidas na literatura.

A plataforma *Kaa IoT Open Source* é disponibilizada através da licença *Apache* 2.0[1] e é uma plataforma com uma boa flexibilidade para uso de tecnologias, oferecendo soluções para múltiplos propósitos. Dentre as principais características da plataforma podem ser listadas: a coleta de dados, o registro de Coisas, a criação de grupos para as Coisas, as notificações e os eventos usados para fazer as Coisas interagirem com o ambiente. A seguir, será feito uma descrição da arquitetura dessa versão da plataforma, esboçada na Figura 1, indicando os principais elementos que compõem a plataforma, além de evidenciar a sua compatibilidade com *Softwares*, serviços e *Hardwares*.

Figura 1 – Arquitetura da *Kaa IoT Platform*



Fonte: CyberVision, Inc. (2019).

Como brevemente mencionado, a *Kaa IoT Open Source* pode ser instanciada em modo *Single node*, ou seja, em um único servidor, replicando assim um cenário já convencional estabelecido pela *Cloud Computing*. Ela também pode ser expandida e alocada em modo *cluster* com múltiplos nodos e com cada um rodando uma própria instância da plataforma. O modo *cluster* é o mais indicado para aplicações com um maior porte que possuam uma maior

[1] Licença de *Software* livre permissiva que não possui livre direito de cópia - *copyleft*.

demanda de carga de dados e de tratamento de requisições, pois esse modo possibilita uma maior disponibilidade dos serviços e maior tolerância às falhas por não possuir um único ponto de falha como no modo *Single node*.

A *Kaa IoT Open Source* é dividida em três partes principais: o *Kaa Server*, o *Kaa endpoint SDK* e o *Kaa Extensions*. O *Kaa Server* representa os serviços de *beck-end* essenciais da plataforma, como gerenciamento de usuários, dados e aplicações. Já o *Kaa endpoint SDK* é a parte da plataforma responsável pelas Coisas, ou seja, trata-se de uma biblioteca para o desenvolvimento de aplicações que pode ser gerada para as linguagens C, C++, Objective-C e Java. A terceira parte da plataforma é a *Kaa Extensions* que são módulos que oferecem funcionalidades extras, visando ampliar as capacidades de comunicação entre o *Kaa server* e o *Kaa endpoint SDK*.

Cada nodo *Kaa* executa uma combinação de serviços internos já configurados, sendo eles: o *Control service*, o *Operation service* e o *Bootstrap service*. O *Control service* é o principal serviço executado pela *Kaa*. Esse serviço controla os dados gerais da plataforma, processa as chamadas de API da Web e de outros serviços externos. Também é responsável por fazer a comunicação com os outros serviços da plataforma, além de manter uma lista em tempo real da disponibilidade dos serviços que estão ativos naquele momento. Ainda, o *Control service* executa a API *Web* que fornece uma interface gráfica para o usuário gerenciar as contas, os acessos e as Coisas, tudo pelo navegador da *Web*. Em modo *cluster*, o *Control service* opera com alta disponibilidade e, em caso de falha no serviço em um nodo, as instâncias que estão ociosas ou executando nos outros nodos assumem a demanda de controle do nodo que teve a falha, utilizando o *Apache Zookeeper* para determinar as corretas atribuições.

O *Operation service* consegue se comunicar com múltiplos *endpoints* simultaneamente e é a aplicação que processa as requisições feitas pelas Coisas e responde a essas requisições com os dados necessários. O *Bootstrap service* é outra aplicação implementada na *Kaa IoT Platform* e trata-se de uma aplicação utilizada para enviar dados específicos para as Coisas, como configurações de outras aplicações por exemplo. O *Bootstrap service* é usado para enviar aos *endpoints* informações e parâmetros para a conexão deles com o *Operation service*. Esses parâmetros podem incluir endereços de IP, portas de conexão e também credenciais de segurança para garantir que apenas Coisas autorizadas façam requisições para o *Operation service*. Além do *Apache Zookeeper*, a plataforma também oferece integração com diversos serviços de terceiros, principalmente com bancos de dados SQL e NoSQL que são utilizados para armazenar os mais variados tipos de dados coletados e gerados pela plataforma.

De modo geral, a *Kaa IoT Platform* tem uma grande quantidade de possíveis aplicações. Ela também possui suporte para uma significativa variedade de sistemas, como *Windows, Linux, Android* e *iOS*. Além disso, oferece compatibilidade com diversos *Hadwares* de prototipagem, como *Arduino, Raspberry Pi*, ESP8266, entre outros. E, apesar de possuir algumas limitações como suporte a poucas linguagens de programação, é possível desenvolver uma grande variedade de aplicações para IoT utilizando os diversos recursos da plataforma.

4 SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE DE DADOS

Como descrito nos capítulos acima a IoT ainda precisa solucionar diversos problemas para se tornar uma realidade em um futuro próximo. Entre os problemas encontrados, as soluções para alguns necessitam de novas tecnologias que sustentem a demanda da Internet das Coisas e alguns apenas precisam que as tecnologias já existentes sejam adaptadas para o cenário da IoT. Em relação aos problemas com a segurança das informações e com a privacidade dos dados na IoT considera-se que muito do que já existe pode ser utilizado nesse novo paradigma. Diante disso, este capítulo em questão tenciona trazer da literatura os principais conceitos e ideias sobre segurança da informação e sobre privacidade de dados para que esses conceitos possam, posteriormente, serem comparados com o ambiente da Internet das Coisas.

4.1 SEGURANÇA DA INFORMAÇÃO

A segurança da informação é a área que estuda os mecanismos de proteção de um conjunto de informações. Na computação, a segurança da informação é responsável pela proteção de um sistema computacional, sendo ela necessária para que se possa preservar o valor que as informações geradas por dispositivos têm para seus proprietários. Significa, portanto, proteger computadores, dispositivos, dados e todas as coisas que fazem parte da rede de alguma forma. Sobretudo ela não é restrita ao meio eletrônico, isso quer dizer que ela também abrange os componentes físicos e humanos que fazem parte da criação, do transporte e da interpretação de informações no meio eletrônico (SILVA; STEIN, 2007).

Ao longo dos anos, a segurança da informação foi ganhando cada vez mais espaço e importância para ser estudada, posto que devido às inovações tecnológicas em crescimento tornou-se fundamental a prática da preservação da integridade das informações que circundam o meio digital. Ademais, ela pode ser vista como um conjunto de práticas que objetivam evitar que informações sejam acessadas ou alteradas por pessoas não autorizadas, bem como evitar que exista negação de serviço para as pessoas que são autorizadas a acessar essas informações (BROSTOFF, 2004).

Para garantir que esses requisitos sejam preservados, a segurança da informação é comumente fundamentada na tríade CID (Confidencialidade, Integridade e Disponibilidade). Esses princípios, apesar de não serem os únicos existentes na área da segurança, são os mais lembrados pela literatura, uma vez que abrangem a maioria dos problemas enfrentados durante os processos de proteção de dados e de dispositivos. Esses pilares da segurança são considerados requisitos fundamentais para o desenvolvimento de novas tecnologias, especialmente nas aplicações de Internet das Coisas (RAJ; RAMAN, 2017). Na sequência, serão apresentadas as primitivas que compõem a tríade CID.

4.1.1 Confidencialidade

A confidencialidade é a primitiva da segurança da informação que estipula princípios para que as informações só possam ser compreendidas por pessoas autorizadas a isso. Portanto, significa que ela tem o objetivo de manter as informações confidenciais ao máximo possível. Para garantir que o princípio da confidencialidade seja mantido mesmo quando as informações de um sistema sejam expostas de alguma forma, é preciso que medidas adicionais sejam aplicadas para que essas informações não possam ser lidas e interpretadas por terceiros. A fim de que isso seja possível, a criptografia tem sido desde os primórdios da área a técnica mais utilizada para esse fim.

A criptografia é uma técnica milenar que foi adaptada para o mundo moderno das informações digitais. Ela é utilizada para manter uma comunicação segura entre seus participantes, impedindo que terceiros mal-intencionados possam acessar o valor da informação, mesmo que tenham acesso a ela no meio físico ou digital. Seu funcionamento é baseado em aplicar uma cifra sobre a informação original antes de enviar ao destinatário, fazendo com que ela fique em um estado criptografado. Com isso, apenas os conhecedores da cifra poderão usá-la para decifrar a informação para seu estado original. Atualmente, existem variados modelos para criptografar uma informação, um deles é a criptografia simétrica que utiliza a mesma chave para cifrar e para decifrar a informação. Já a criptografia assimétrica utiliza um par de chaves no processo: uma pública para encriptar e uma privada para decriptar.

Na Ciência da Computação, a criptografia é utilizada para diversas aplicações com algoritmos criptográficos que podem ter variadas complexidades e finalidades. No decorrer dos anos, esses algoritmos foram sendo aperfeiçoados para serem cada vez mais difíceis de serem quebrados e serem fáceis para implementação. Os algoritmos mais complexos, nos dias atuais, precisariam de centenas de anos para serem decifrados por força bruta. Isso, no entanto, não significa que os algoritmos de criptografia atuais sejam perfeitos e livres de falhas, principalmente quando se considera o fator humano envolvido na utilização e na manutenção dessas técnicas (SILVA; STEIN, 2007).

4.1.2 Integridade

O princípio da integridade estipula que as informações armazenadas ou transferidas sejam sempre mantidas no seu formato original. Esse princípio tem se mostrado bastante crítico hoje em dia, em particular com o crescente aumento na prática da adulteração de informações utilizadas para a propagação de notícias falsas, conhecidas como *fake news*. Essa primitiva, portanto, tem a função de se preocupar com as alterações indevidas que uma informação possa sofrer ao ser armazenada ou ao ser enviada para um destinatário. Em outras palavras, manter o princípio da integridade é manter a consistência e a veracidade dos dados em todo o seu ciclo de vida.

Esse princípio requer artifícios extras de redundância de dados, como por exemplo a utilização de *Log* que funciona como um registro completo de todas as manipulações que foram feitas nos dados. Assim, é possível identificar se algum dado do sistema foi manipulado ou, ainda, se algum dado foi adicionado ou removido do sistema. Considerando um caso em que a integridade dos dados seja completamente comprometida, é importante que o sistema possa se recuperar para uma versão estável e consistente de si mesmo, ou seja, realizar um *Backup* dos seus dados íntegros.

Para manter a integridade dos dados garantida é preciso que os sistemas computacionais em geral possuam níveis de segurança em todos os processos que manipulem algum tipo de dado ou metadado. Isso infere que a segurança necessita estar presente desde a camada de armazenamento de um sistema, *i.e*, no seu banco de dados até na sua propriedade de conectividade (que também realiza o processo de autenticação das permissões para manipulação dos dados). Igualmente, precisa estar presente na sua propriedade de transporte que é responsável pela transferência dos dados em si.

4.1.3 Disponibilidade

A disponibilidade é o princípio que estabelece que a informação estará disponível sempre que necessário. O objetivo desse princípio é evitar falhas na obtenção ou na disponibilização de uma informação. Para isso, essa primitiva se estende a diversas partes de um sistema computacional como o *Software*, a rede e o *Hardware*. Nesse sentido, é importante que os sistemas possuam funcionalidades de redundância de dados, como RAID (*Redundant Array of Inexpensive Disks*) e *Backups*. Também é importante que a rede suporte a demanda de usuários do sistema para que todos possam obter as informações que quiserem a todo momento.

Ademais, garantir o princípio da disponibilidade em um sistema computacional é permitir que os usuários autorizados possam acessar seus dados sempre que for preciso, além de tentar impedir que a disposição desses dados seja negada devido à ação de terceiros. Inclui-se no princípio da disponibilidade garantir que possíveis falhas de segurança sejam usadas para afetar o funcionamento de um serviço hospedado na internet, assim como acontece nos ataques de negação de serviço DoS (Denial of Service).

Fundamentando-se nessas primitivas, a segurança da informação tornou-se indispensável em todos os computadores, *smartphones*, aplicações e sistemas, principalmente por conta do aumento da preocupação com a gestão do risco de vulnerabilidades desses sistemas. É possível identificar que a forte presença de dispositivos eletrônicos no cotidiano das pessoas abriu novas possibilidades de crimes cibernéticos como fraudes e apropriação indevida de informações. E, diante disso, é essencial que todos esses dispositivos utilizem de técnicas de segurança em sua construção básica (CABRAL; CAPRINO, 2015).

4.2 PRIVACIDADE

A privacidade pode ser definida como um dos objetivos finais da segurança da informação. Essa prática se baseia fortemente no princípio da confidencialidade dos dados. Em linhas gerais, trata-se de um direito pessoal e universal que se manifesta como: a garantia de confidencialidade de informações particulares e pessoais, também como a liberdade de anonimato na utilização de serviços e, por fim, a limitação da disponibilidade de informações particulares em geral. Na computação, a privacidade é um dos pontos mais críticos relacionados ao desenvolvimento de novas tecnologias. A cada novo paradigma que possa surgir é essencial que se pense em como isso afetará o componente humano e, consequentemente, a segurança e a privacidade dos usuários dessa nova tecnologia (BORGES, 2016).

O desenvolvimento de novas tecnologias paralelas à internet também fez aumentar a preocupação com a privacidade dos seus usuários. O direito à privacidade que é estabelecido no artigo 12 da Declaração dos Direitos Humanos[1], de 1948, é um direito que precisa ser preservado no mundo digital. Tendo como base o exposto sobre o grande volume de dados acessíveis na internet, é fundamental que a privacidade dos dados seja um objetivo constante para empresas e usuários, visto que a violação da privacidade em um ambiente tão amplo como a internet pode acarretar em consequências irreparáveis, podendo afetar inclusive o exercício da democracia (BORGES, 2016).

A onipresença da internet no mundo globalizado é um dos grandes pilares que sustentam a preocupação com a privacidade dos dados pessoais, pois decorrente da sua grande acessibilidade e popularidade ela passou a ser também um risco para a segurança dos seus usuários e dos próprios computadores. Por conta disso, é preciso que sejam buscadas soluções para manter sempre em segurança as informações pessoais e particulares dos indivíduos que utilizam a rede. Ademais, o crescente número de sistemas e aplicações que utilizam dados privados dos seus usuários é algo que precisa ser monitorado para que nenhuma violação no direito à privacidade do usuário aconteça.

Um dos padrões de regras para segurança da informação dedicado a garantia da privacidade dos dados é conhecido como AAA (Autenticação, Autorização e Auditoria). A autenticação é o mecanismo que objetiva validar as credenciais de acesso que um usuário ou dispositivo tem em uma aplicação. O exemplo mais simples dessa utilização é o *Login* e senha que atualmente são requeridos em praticamente todo serviço na internet. A autorização, por sua vez, se preocupa com quais procedimentos dentro de uma aplicação podem ser acessados por um usuário ou dispositivo que já passou pelo processo de autenticação, ou seja, verifica para quais funcionalidades do sistema o usuário está autorizado a acessar. Por fim, a auditoria é uma atividade periódica que é usada para verificar o andamento dos processos anteriores, como verificar tentativas fracassadas de *Login* ou tentativa de acessos às funcionalidades não permitidas (RAJ; RAMAN, 2017).

[1] Disponível em: <https://nacoesunidas.org/artigo-12-direito-a-privacidade/>. Acesso em: 20 out. 2019.

Baseando-se no problema da segurança da informação na internet, diversas técnicas foram criadas ao longo dos últimos anos tendo em vista melhorar a privacidade dos dados gerados por computadores. Uma das técnicas mais conhecidas no estudo da privacidade é a criptografia, já citada anteriormente, que objetiva distorcer o valor de uma informação para que ela não seja interpretada por pessoas e sistemas não autorizados. O desenvolvimento dos computadores pessoais, dos dispositivos móveis e das redes sem fio também contribuíram com a necessidade de aperfeiçoamento das técnicas de segurança e de privacidade de dados.

Nesse contexto, com o desenvolvimento de novas tecnologias e com o aumento na diversidade de dispositivos capazes de gerar ou coletar dados, é necessário que os algoritmos de criptografia sejam implementados por todos os dispositivos com essas capacidades. Atualmente, existem protocolos de criptografia que são matematicamente inquebráveis, no entanto demandam de um grande valor computacional para funcionarem corretamente. Além disso, os protocolos de comunicação utilizados por esses dispositivos estão cada vez mais sofisticados e, por consequência, também demandam de grande recurso computacional para ter o seu completo funcionamento. Sendo assim, a privacidade de dados é algo que precisa estar em evolução a todo momento para garantir que o desenvolvimento de novas tecnologias seja acompanhado de boas práticas que culminem em sistemas seguros e com dados privados.

Manter a privacidade das informações e de seus usuários deve ser sempre um objetivo para qualquer sistema computacional. A internet e seu alto poder de propagação de informações faz com que manter o sigilo das informações seja ainda mais importante. Com a instalação do paradigma da Internet das Coisas em um futuro próximo, essa questão passa então a ser uma prioridade para o desenvolvimento da área. A IoT requer que as soluções de segurança e de privacidade que já existem em sistemas convencionais sejam inclusivas com as novas demandas que surgirão com o amadurecimento da área. O principal desafio, então, é pensar em como o aumento no número de dispositivos capazes de coletar dados irá afetar a privacidade dos seus usuários e, portanto, encontrar soluções para isso é algo que precisa acontecer concomitantemente com o desenvolvimento dos dispositivos e *Softwares* de IoT (SANTOS; SALES, 2015).

5 SEGURANÇA E PRIVACIDADE PARA INTERNET DAS COISAS

Este capítulo almeja finalizar o aporte teórico que vem sendo estabelecido até então. Desse modo, serão retomados alguns pontos críticos relacionados ao desenvolvimento da Internet das Coisas, principalmente sobre a segurança da informação e a privacidade dos dados nesse paradigma. Como brevemente mencionado no decorrer do texto, a IoT demanda que muitas tecnologias utilizadas atualmente sejam melhoradas ou adaptadas para serem completamente integralizadas ao seu ambiente. Em decorrência disso, é necessário elencar as entidades tecnológicas existentes na área da segurança e da privacidade para que seja viável estudar formas de adaptá-las ao paradigma da Internet das Coisas.

Um dos principais desafios para a segurança da informação na Internet das Coisas é se adaptar a alta diversidade de elementos de *Hardware* e de *Software* que integram esse ambiente. Para melhorar a segurança nesse ponto é preciso que as aplicações sejam desenvolvidas com suporte nativo a uma grande variedade de protocolos de segurança e de conexão. Isso é necessário para que todos os elementos do paradigma sejam atendidos devidamente. Também é importante que a segurança da informação e privacidade dos dados sejam objetivos constantes, sendo construídos com boas práticas de desenvolvimento e com a devida gestão de risco (CABRAL; CAPRINO, 2015).

Para além disso, a segurança da informação na Internet das Coisas é um conceito que se mantém praticamente idêntico da sua concepção original na computação. De fato, ela é um tema que precisa ser melhor elaborado para que esse novo paradigma possa se desenvolver de forma estável, escalável e consistente. Por conseguinte, é preciso pensar em segurança da informação como um processo contínuo, dividido em pequenas etapas e visando criar uma rede mundial de Internet das Coisas que ofereça condições de oferecer segurança aos dispositivos e privacidade para os usuários (CABRAL; CAPRINO, 2015).

Diante disso, é essencial entender que a IoT possui requerimentos específicos para desenvolver suas aplicações. Na questão da segurança, evidencia-se que a IoT produz um ambiente com um número muito maior de dispositivos ativos, ou seja, de elementos que podem ser afetados em caso de uma má gestão da segurança. A partir do grande número de dispositivos coletando dados, a manutenção da privacidade deles na Internet das Coisas é algo que deve ser prioridade, visto que a exposição dos dados pessoais afeta diretamente os direitos humanos (BORGES, 2016).

No cenário iminente da IoT, os problemas com a segurança de todas as Coisas conectadas à internet são inevitáveis. Em decorrência disso, é preciso que os dispositivos e sistemas para a IoT sejam projetados e desenvolvidos seguindo técnicas de segurança e de privacidade e é preciso que os usuários sejam devidamente instruídos a utilizar equipamentos compatíveis com os princípios básicos da segurança. Ademais, é fundamental que esses dispositivos possam receber constantes atualizações de segurança com o objetivo de sobrepor possíveis vulnerabilidades em seus sistemas (OLIVEIRA NETO, 2015).

Como indicado anteriormente, a Internet das Coisas precisa desenvolver suas aplicações pensando na segurança da informação como um processo contínuo, estabelecendo, então, uma arquitetura de segurança definida em camadas. Essas camadas acompanham as entidades que integram o ambiente da Internet das Coisas e são definidas como: a segurança física dos objetos, da rede, da *Cloud Computing* e da *Fog Computing*, do banco de dados, do *Gateway* e do próprio dispositivo final, isto é, a Coisa. Com procedimentos de segurança aplicados em todas essas camadas, a IoT estabelece um nível de segurança muito maior para suas aplicações.

Para poder se comunicar, computadores e dispositivos eletrônicos em geral utilizam protocolos e, na computação, estes são definidos como regras sintáticas e semânticas que determinam uma linguagem para comunicações entre máquinas. Sendo assim, os protocolos são de extrema importância para a comunicação, transferência de dados e segurança para computadores. Na Internet das Coisas, os protocolos são ainda mais utilizados por conta da demanda de comunicação instantânea que existe no paradigma e, como esperado, os protocolos já conhecidos não se mostraram capazes de acompanhar as necessidades da IoT.

Com isso, a Internet das Coisas vem promovendo o desenvolvimento de novos protocolos dedicados exclusivamente para dispositivos pequenos e portáteis, como o MQTT (*Message Queuing Telemetry Transport*) que é um protocolo de comunicação para pequenos dispositivos e que foi otimizado para redes TCP/IP. Outra tecnologia inovadora desencadeada pela IoT é a LoRa que utiliza o protocolo *LoRaWAN* e é usada para comunicação de longas distâncias para mensagens que demandam uma baixa largura de banda. Esses novos protocolos e tecnologias de conexão são fundamentais para que seja possível conectar bilhões de dispositivos de forma escalável.

Retomando as reflexões traçadas no capítulo 2, um dos avanços que deve acontecer com o amadurecimento da IoT é a predominante utilização do protocolo IPv6, o qual permite a indexação de muito mais endereços que o padrão atual IPv4. Derivado do protocolo IP, o IPsec (*Internet Protocol Security*) é um protocolo de segurança que funciona diretamente na camada de rede e é composto por funcionalidades específicas para a transmissão segura de informações via protocolo IP. A sua utilização já é possível com o IPv4, entretanto ele é uma funcionalidade padrão do IPv6. A IoT também se aproveita dos protocolos de segurança já estabelecidos e utilizados atualmente na internet, como o SSL (*Secure Sockets Layer*) e o mais atual TLS (*Transport Layer Security*) que podem ser encontrados nos mais diversos tipos de serviços *on-line* (ATZORI; IERA; MORABITO, 2010).

Além do apresentado sobre segurança nos meios de comunicação, é fundamental que haja a preocupação com a segurança das *Clouds* e *Fogs*. Essas arquiteturas são essenciais para o funcionamento dos dispositivos de IoT, pois são responsáveis por realizar a interconexão desses objetos. Com isso, fazem a coleta primária de dados dos dispositivos, interpretam requisições e, com elas, disparam ações para outros dispositivos que a elas estejam conectados. A segurança nessas arquiteturas pode ser feita com o uso de *Softwares* que administrem as conexões e façam o processo de autenticação dos usuários e Coisas que se conectam até elas.

No que se refere ao armazenamento dos dados gerados pela IoT é de extrema importância que sejam projetados mecanismos de segurança para serem aplicados aos bancos de dados. O grande volume de dados gerados pela IoT implica na utilização do conceito de *Big Data* que, por sua vez, é definida pelos 3Vs (Volume, Variedade e Velocidade). Ou seja, dispositivos de Internet das Coisas geram um grande volume de dados com uma grande variedade ente si (uma vez que são oriundos de diversas fontes) e precisam ser coletados, processados e armazenados com alta velocidade. Em vista disso, a IoT está integrando soluções de segurança para trabalhar em conjunto com a *Big data* e, assim, fazer com que a persistência dos dados da IoT aconteça de forma segura. Sobretudo, os mecanismos de segurança para dados são aplicados sobre os próprios bancos de dados, principalmente dos NoSQL que são os mais indicados para dados diversos como os da IoT (RAJ; RAMAN, 2017).

Do ponto de vista da privacidade, os dados armazenados da IoT sempre serão entidades que precisam ser protegidos. A partir disso, é necessário que existam camadas extras de proteção para essas informações. Além da segurança aplicada aos bancos de dados, a utilização de criptografia aplicada aos dados armazenados é a opção mais viável e funcional. Entretanto, devido à diversidade de dispositivos e à variedade de poder computacional disponível neles, é interessante utilizar variados tipos de algoritmos de criptografia, tencionando atender um maior número de dispositivos e, além disso, criar múltiplas camadas de criptografia em um mesmo ambiente de Internet das Coisas.

Outro fator de relevância para a segurança na Internet das Coisas está relacionado com o "sequestro"de computadores e dispositivos eletrônicos em geral. Trata-se da técnica utilizada por invasores que por meio de *Softwares* maliciosos (vírus) ganham acesso a um dispositivo e passam então a controlar esse objeto remotamente. No cenário da IoT, com bilhões de dispositivos alvos, essa preocupação é evidente, pois esses dispositivos sequestrados podem ser usados para realizar ataques de DDoS (*Distributed Denial of Service*) em massa, objetivando com esses ataques interromper a funcionalidade de serviços de servidores em qualquer lugar do mundo. Esse tipo de ataque fere diretamente o princípio da disponibilidade na segurança da informação e pode ser potencialmente ampliado com a eminente disseminação da IoT (RAJ; RAMAN, 2017).

Os dispositivos eletrônicos atuais, que já são amplamente utilizados na internet como os computadores e dispositivos móveis, também precisam melhorar suas técnicas segurança da informação para serem utilizados plenamente na Internet das Coisas. Em particular, os dispositivos móveis pessoais como os *Smartphones*, que por possuírem uma alta capacidade de conectividade, armazenamento e de interação humano-computador, serão utilizados na Internet das Coisas como controladores gerais de outros dispositivos, além de serem usados para coletar, processar e visualizar dados em tempo real. Dessa maneira, é importante manter os seus sistemas operacionais seguros e seus aplicativos com constantes atualizações de segurança e de privacidade para garantir que esses dispositivos não forneçam informações indevidas para pessoas não autorizadas.

De modo geral, os dispositivos que integrarão o ambiente da Internet das Coisas devem seguir uma série de procedimentos para garantir que a segurança e a privacidade sejam preservadas. Alguns desses procedimentos são: *Security boot* que consistem em realizar uma verificação interna de segurança sempre que o dispositivo de IoT é inicializado; *Authentication for netwaorks* que são realizados quando a Coisa se conecta a um tipo de rede; e, também, *Device upgrades* que consistem em manter atualizações de segurança e de privacidade com uma determinada frequência, para que as vulnerabilidades sejam sempre corrigidas (RAJ; RAMAN, 2017).

Finalizando a abstração teórica referente à segurança da informação e à privacidade de dados na Internet das Coisas, ressalta-se, ainda, que a Ciência da Computação, sempre buscando inovações tecnológicas, almeja contribuir com o desenvolvimento da área da IoT, pesquisando novas formas de fazer com que esse paradigma seja construído com boas práticas de usabilidade e que seja escalável para bilhões de dispositivos. Para garantir que os dados pessoais dos usuários não sejam usados de forma indevida ou sem autorização dos mesmos, evidencia-se que a segurança e a privacidade precisam ser consideradas importantes desde os primeiros processos de planejamento e de prototipagem das novas aplicações para a Internet das Coisas.

6 AVALIAÇÃO DA PLATAFORMA

De acordo com o referencial teórico que foi estabelecido previamente sobre IoT, plataformas de Internet das Coisas, segurança da informação e privacidade de dados este capítulo tem o propósito de descrever a avaliação conceitual realizada na *Kaa IoT Platform* pelos pontos de vista da segurança e, principalmente, da privacidade dos dados gerenciados pela plataforma. Diante disso, a metodologia utilizada na pesquisa e os procedimentos de avaliação realizados serão aqui descritos em tópicos, não obedecendo necessariamente uma ordem cronológica.

6.1 METODOLOGIA

Nesta seção será apresentada a metodologia utilizada durante a pesquisa. Pretende-se aqui esboçar as etapas de avaliação que foram desenvolvidas para analisar a plataforma de Internet das Coisas *Kaa IoT Open Source* e, a partir disso, validar os objetivos propostos. Ademais, a descrição da metodologia também servirá para demostrar a limitação dos objetos de pesquisa que foram utilizados nas análises.

Em um primeiro momento, foi realizada uma comparação entre as gerações da *Kaa IoT Platform* verificando as particularidades da *Kaa IoT Open Source* com relação à *Kaa IoT Enterprise* para obter uma visão geral sobre as funcionalidades disponíveis na versão gratuita. Assim, utilizando a literatura e a documentação fornecida pela própria desenvolvedora foi possível validar os recursos e funcionalidades de segurança e de privacidade disponíveis na *Kaa IoT Open Source*.

Na sequência, o segundo cenário de avaliação foi idealizado sobre o *Kaa Sandbox* que é uma versão pré-configurada da *Kaa IoT Platform*. No *Kaa Sandbox* se fez possível verificar as configurações gerais de segurança disponibilizadas pela interface gráfica da plataforma. Também foi possível elencar os recursos de segurança e de privacidade presentes na plataforma que podem impactar diretamente na construção de aplicações de IoT mais seguras.

Por fim, no terceiro cenário de avaliação foi analisado uma das principais funcionalidades da plataforma: a coleta de dados (*Data Collection*). Essa funcionalidade infere diretamente no tema da pesquisa e, através disso, objetivou-se verificar as particularidades da mesma de acordo com três perspectivas diferentes. Na primeira foi utilizada a documentação oficial da plataforma para descrever e avaliar com a literatura as características da funcionalidade. Após isso, foi realizado uma avaliação a nível de aplicação verificando os dados que uma aplicação hipotética coleta. E, por fim, foram analisados via código fonte quais dados do usuário são realmente coletados pela plataforma para que fosse finalizada a validação de todos os cenários descritos.

6.2 *KAA IOT OPEN SOURCE* X *KAA IOT ENTERPRISE*

Durante a fase inicial do desenvolvimento do projeto de pesquisa cogitou-se uma possível comparação da *Kaa IoT Platform* com outra plataforma de Internet das Coisas já reconhecida na área. Entretanto, visando delimitar os estudos apenas na *Kaa IoT Platform*, optou-se por brevemente comparar a versão analisada com a *Kaa IoT Enterprise* com a intenção de especificar as funcionalidades únicas da versão gratuita e problematizar o funcionamento desses recursos. Na Figura 2, abaixo apresentada, estão listadas as funcionalidades de ambas as versões da plataforma e, na sequência, será realizada a avaliação pontual de algumas delas.

Figura 2 – Comparativo entre as gerações da plataforma

FEATURE	KAA 0.X OPEN-SOURCE	KAA ENTERPRISE
Architecture	Monolithic	Microservices
Connectivity protocol	Proprietary	Open, standards-based
Gateway connectivity model	One connection per device	Single, multiplexed connection
Communication security	RSA+AES	(D)TLS
SDK	Required	Optional
Device credential management	No	Yes
Device metadata	Structured	Structured or unstructured
Device filtering / grouping	Yes	Yes
Data collection	Single data type, structured only	Unlimited data types, isolated flows, structured or unstructured
Configuration management	Structured only	Structured or unstructured
Data processing and analytics	3-rd party integrations	Built-in or 3-rd party integrations
Data visualization	3-rd party integrations	Built-in customizable dashboards or 3-rd party integrations
Device notifications	Yes	No, superseded by commands
Command execution	No	Yes
Over-the-air updates	No	Yes
Multiple applications	Yes	Yes
Application versioning	Yes	Yes
Technology stack	Mainly Java	Polylingual
Scalability, elasticity, self-healing	Manual	Automated container orchestration
Server configuration	Non-portable, stored in DB	Portable declarative blueprint

Fonte: Kaa IoT Technologies (2019).

6.2.1 Arquitetura da plataforma

A *Kaa IoT Open Source* e a *Kaa IoT Enterprise* possuem modelos de arquitetura de *Software* distintos entre si. A versão que está sendo analisada possui uma arquitetura mais tradicional, conhecida como monolítica. Enquanto isso, a *Kaa IoT Enterprise* tem um modelo de arquitetura mais moderno que é baseado em microsserviços.

O modelo monolítico caracteriza-se por concentrar a maior parte das funcionalidades em um único programa. Com isso, apresenta-se como um modelo fácil de se trabalhar, pois todos elementos de *Software* desse modelo são integralizados. Porém, possui diversas limitações quando é preciso escalar as soluções desse *Software* para múltiplas instâncias e, também, quando é necessário integralizar novas funcionalidades nesse sistema, dado que obriga essas novas aplicações a seguirem o padrão do modelo por completo.

Já o modelo de arquitetura baseado em microsserviços, que é utilizado na versão paga da plataforma, é visto como um modelo mais atual porque considera cada serviço ou funcionalidade do *Software* como sendo um pequeno programa que é independente do restante do sistema. Esse modelo possui vantagens em relação ao monolítico por permitir a alteração e a inclusão de novas funcionalidades ao sistema sem precisar parar qualquer funcionalidade que esteja sendo executada. Ademais, pelo ponto de vista da segurança, uma arquitetura baseada em microsserviços permite o isolamento de partes críticas dos sistemas, além de possibilitar uma maior frequência de atualizações de segurança para o sistema como um todo.

6.2.2 Protocolos de comunicação

A *Kaa IoT Open Source* utiliza em sua configuração original dois protocolos dedicados a transferência de dados, listados na Figura 3. Como trata-se de uma versão *Open Source*, ou seja gratuita e livre para desenvolvimento, a ideia é que se possa implementar outros protocolos e novas abordagens para transferência de dados com a plataforma.

Figura 3 – Protocolos de comunicação da plataforma

Transport name	Default bootstrap port	Default operations port	Supported services	Based on
HTTP	9889	9999	All	HTTP 1.1
Kaa TCP	9888	9997	All	TCP

Fonte: CyberVision, Inc. (2019).

O protocolo predominantemente utilizado para transferir dados dos *endpoints* é o HTTP (*Hypertext Transfer Protocol*) e na sua implementação para a plataforma é baseado no HTTP 1.1 que é uma versão consistente e muito utilizada na internet em um modo geral. A *Kaa IoT Open Source* também suporta a utilização do protocolo KaaTCP (exceto para o serviço de *Bootstrap*) que é uma implementação proprietária baseada nos protocolos TCP e MQTT.

Na versão *Enterprise* a plataforma disponibiliza mais opções de protocolos prontos justamente por ser uma versão comercial do *Software*. Todavia, o principal protocolo utilizado é o KPC (*Kaa Protocol Communication*) que é um protocolo aberto evoluído do KaaTCP desenvolvido especialmente para a plataforma, priorizando a comunicação entre máquinas com base no protocolo MQTT.

6.2.3 Protocolos de segurança

Em relação aos recursos de segurança utilizados nos processos de comunicação a *Kaa IoT Open Source* utiliza dois algoritmos de criptografia por padrão: o RSA (Rivest-Shamir-Adleman) e o AES (Advanced Encryption Standard). Esses algoritmos são usados nos processos de registro de um novo *endpoint* e também nos procedimentos de transferência de dados. Assim como acontece com os protocolos de comunicação, a *Kaa IoT Open Source* permite que novas abordagens de segurança e novos algoritmos de criptografia sejam implementados nas aplicações da plataforma.

Na *Kaa IoT Enterprise* a segurança na comunicação e na transferência de dados é feita utilizando DTLS (*Datagram Transport Layer Security*) que é um protocolo que tem comunicação segura e visa suprir a alta demanda de conexões requeridas pela Internet das Coisas. Além disso, observou-se que esse protocolo oferece recursos para evitar a adulteração de mensagens e a interceptação de dados dos dispositivos, mantendo assim um nível de segurança elevado nas aplicações de IoT.

6.2.4 Credenciamento de dispositivos

Para o credenciamento de novos dispositivos na plataforma a *Kaa IoT Open Source* utiliza os serviços internos já citados: o *Bootstrap service* e o *Operation service*. Esses serviços processam as requisições feitas pelos *endpoints* e validam as credenciais desse novo dispositivo. Contudo, a versão *Open Source* não oferece um serviço de manutenção de permissões para os dispositivos conectados, ou seja, caso seja necessário remover ou adicionar algum tipo de permissão para um determinado dispositivo é preciso que ele seja removido manualmente da plataforma e, então, configurado novamente.

Já a *Kaa IoT Enterprise*, baseando-se em microsserviços, utiliza diversas APIs independentes para gerenciar os procedimentos de segurança. Cada procedimento como o registro de dispositivos, a manutenção de credenciais e a transferência de dados possuem uma API dedicada a realizar os procedimentos de segurança e de privacidade, facilitando a manutenção desses *Softwares* e aumentando o nível de segurança das aplicações.

6.2.5 Coleta de dados

A coleta de dados, como mencionado anteriormente, é a funcionalidade da plataforma que mais se encaixa no contexto dessa pesquisa, pois entende-se que a privacidade dos dispositivos está diretamente relacionada com os dados dos usuários que podem ser coletados por meio dessa funcionalidade. Sendo assim, é essencial entender os recursos de segurança utilizados pela plataforma nessa funcionalidade.

A *Kaa IoT Open Source* apenas permite a utilização de dados normalizados em sua construção, isto é, os dados que são gerados pelas Coisas e transportados pelos protocolos de comunicação são estruturados. Essa abordagem obriga a criação de um esquema para estruturar os dados que serão gerados pelo *endpoint* e, em seguida, enviados ao *Kaa Server* por meio do *Operation Service*.

Já a *Kaa IoT Enterprise* permite que sejam criados e transportados quaisquer tipos de dados, sejam eles estruturados ou não-estruturados. Essa característica é possível mais uma vez graças a arquitetura de microsserviços que permite a utilização de aplicações independentes, inclusive para tratar uma maior diversidade de dados. Ademais, a coleta de dados será analisada com mais detalhes na sequência do capítulo.

6.2.6 Over-The-Air updates (OTA)

Quando o ambiente da Internet das Coisas for uma realidade será primordial pensar em soluções para garantir a manutenção das funcionalidades das aplicações e dos dispositivos que estarão conectados à internet. Com isso, as atualizações de *Software*, principalmente de segurança, serão essenciais para manter o funcionamento dos serviços de Internet das Coisas sem interrompibilidade e com segurança.

Pensando nisso, as OTA (*Over-The-Air-Updates*) são atualizações utilizadas por sistemas distribuídos para garantir a disseminação de atualizações pelos dispositivos que integram o sistema. Na Internet das Coisas, elas podem inclusive ser repassadas entre dispositivos e, assim, os *endpoints* podem trocar atualizações de *Software* entre si, diminuindo as requisições feitas com o servidor principal.

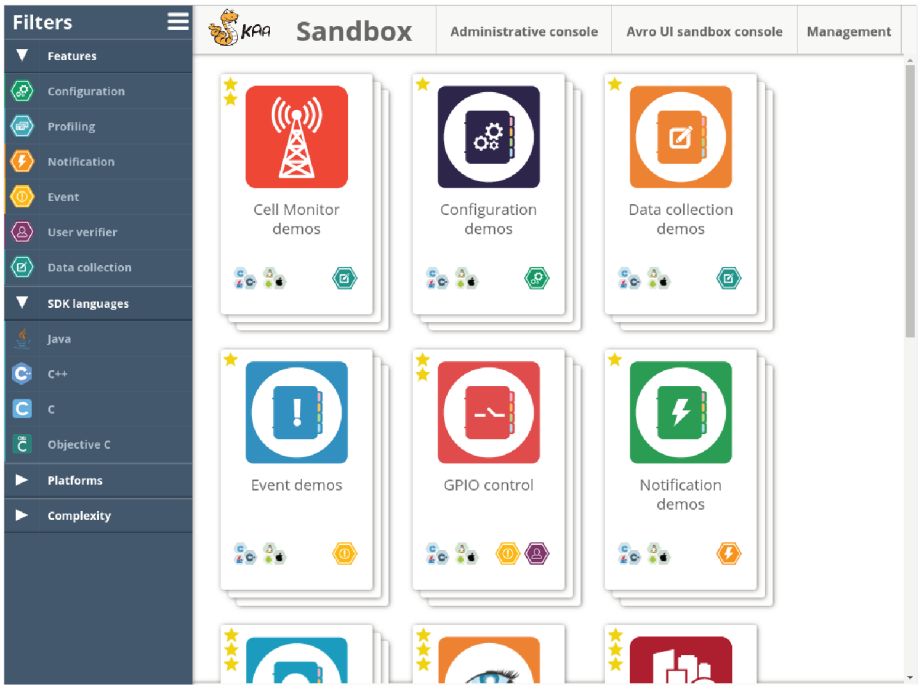
A *Kaa IoT Open Source* não suporta nativamente essa funcionalidade. Em outras palavras, para que seja utilizada é preciso fazer uma implementação da mesma na plataforma. Também não pôde ser encontrado na documentação da versão instruções referentes à implementação desse recurso. Por sua vez, a versão *Enterprise* contém suporte nativo e garante a funcionalidade desse tipo de atualização para os dispositivos finais.

6.3 *KAA SANDBOX*

Com o objetivo de facilitar o desenvolvimento de aplicações e de agilizar o *deploy* da *Kaa IoT Platform* a plataforma também é disponibilizada em um ambiente de *Sandbox*. Este, no que lhe diz respeito, é um ambiente virtualizado que contém uma instância da plataforma já pré-configurada. Com o *Kaa Sandbox* é possível isolar a execução da plataforma em uma máquina virtual facilitando o desenvolvimento e a restauração do ambiente em caso de falhas ou atualizações. Esse ambiente virtualizado é baseado em uma distribuição *Linux* e pode ser instanciado tanto localmente com o *Oracle VirtualBox* como em serviços na *Cloud* como o AWS (*Amazon Web Services*).

Após realizar a instanciação local da plataforma via *Sandbox* na *VirtualBox* é possível acessar no navegador de internet o *Administration UI*. Esse se caracteriza como um painel de administração geral da plataforma no qual pode ser configurado as permissões de usuários, os esquemas para coleta de dados, além de gerar o SDK específico para cada aplicação configurada. O *Kaa SandBox*, por padrão, fica disponível no endereço local (127.0.0.1:9080/sandbox) e oferece uma interface *Web* intuitiva que, como pode ser visto abaixo na Figura 4, permite a navegação entre os diversos menus de configurações e também conta com alguns exemplos de aplicações pré-configuradas.

Figura 4 – Página inicial do *Kaa SandBox*



Fonte: CyberVision, Inc. (2019).

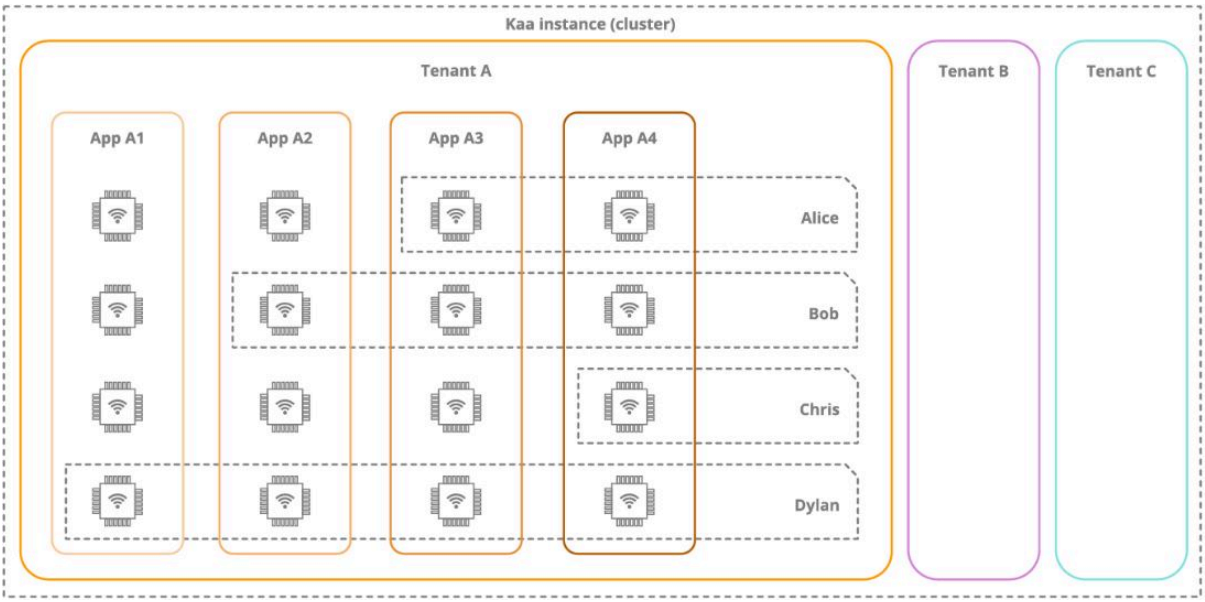
6.3.1 Sistema de autenticação e gerenciamento de permissões

A *Kaa IoT Platform* utiliza um sistema de autenticação e permissões baseados em múltiplos inquilinos (*Tenants*). Esse método possibilita classificar em níveis de permissão os usuários que utilizarão o *Software*. Por meio desse sistema é determinado uma hierarquia de quatro níveis de permissões, sendo eles: o *Kaa* administrador, o *Tenant* administrador, o *Tenant* desenvolvedor e o *Tenant* usuário.

O *Kaa* administrador tem o maior nível de permissão dentro da plataforma, dado que ele pode criar novos usuários e aplicações, além de poder remover outros usuários e permissões. O *Tenant* administrador tem permissão para gerenciar aplicações, usuários e os dispositivos conectados na plataforma. O *Tenant* desenvolvedor, por sua vez, tem permissão para gerar o SDK para aplicações e pode configurar os dispositivos da plataforma. Por último, o *Tenant* usuário representa os usuários finais da plataforma e apenas possuem permissão para acessar as aplicações.

O modelo *Multi-Tenant* tem se mostrado muito útil em plataformas como serviço, especialmente nas dedicadas à Internet das Coisas. Sua utilização tem sido recorrente, pois permite a adição de múltiplos usuários com diferentes permissões em uma mesma instância da plataforma. Nesse sentido, esse sistema garante que nenhum usuário sem a devida permissão acesse as configurações internas e de segurança da plataforma. Ademais, como pode ser visto abaixo na Figura 5, esse sistema também determina em quais aplicações os usuários da plataforma têm permissão para acesso.

Figura 5 – Sistema de permissões *Multi-Tenant* da plataforma



Fonte: CyberVision, Inc. (2019).

6.3.2 Configurações de segurança do *Administration UI*

O acesso ao *Administration UI* do *Kaa SandBox* requer autenticação de *Login* e senha do usuário. O *Kaa SandBox*, ilustrado na Figura 6, possui algumas contas padrões já configuradas e prontas para uso. As três contas já configuradas permitem o acesso às funções críticas do sistema como um todo. Nesse sentido, identifica-se que essa escolha pode acarretar em uma possível falha na segurança da plataforma. Isso ocorre visto que caso alguma dessas contas seja esquecida no sistema ou utilizada sem a devida alteração da senha padrão, usuários não autorizados podem facilmente conseguir acesso à plataforma.

Figura 6 – Contas pré-configuradas disponíveis no *Kaa SandBox*

Account type	Username	Default password
Kaa admininstrator	kaa	kaa123
Tenant admininstrator	admin	admin123
Tenant developer	devuser	devuser123

Fonte: CyberVision, Inc. (2019).

Com o acesso à conta *Kaa* administrador realizado com sucesso é possível então realizar as configurações gerais e de segurança mais importantes da plataforma. Diante disso, é essencial que a senha padrão dessa conta seja trocada no momento da primeira utilização e que a nova escolhida seja uma senha segura. Isso é necessário, uma vez que os inquilinos com acesso à conta *Kaa* administrador podem gerenciar completamente as outras contas de usuários da plataforma e configurar as aplicações que estão instanciadas na plataforma. Sobretudo, se torna possível a alteração do nome das aplicações e do endereço eletrônico para o qual elas enviam os seus dados.

Ao se acessar uma conta *Kaa* administrador, do mesmo jeito, é possível utilizar as *Outgoing mail settings* que são configurações para fazer o envio de *e-mails* para usuários e serviços externos. Com o acesso indevido a essa funcionalidade os usuários podem fazer com que a própria plataforma envie dados privados de outros usuários para entidades externas, como dados para recuperação de senhas e informações coletadas pelos dispositivos.

Perante o que foi apresentado, entende-se que a plataforma possui boas configurações de segurança em geral, como por exemplo o sistema de *Muiti-Tenant*. Entretanto, é preciso que a aplicação dessas configurações seja acompanhada de boas práticas de utilização dos usuários desse sistema para que se possa, com isso, garantir a usabilidade da plataforma como um todo e, além disso, certificar a segurança e a privacidade dos dados pessoais dos usuários.

6.4 KAA DATA COLLECTION

Após elencar as funcionalidades da *Kaa IoT Platform* que possuíam algum impacto direto na segurança e na privacidade dos usuários, optou-se por aprofundar o estudo da privacidade em uma funcionalidade específica. Assim, a funcionalidade de coleta de dados, a *Kaa Data Collection*, foi selecionada para ser detalhada por possuir implicação direta sobre os dados que transitam na plataforma. Vale destacar que caso essa funcionalidade seja mal projetada ou utilizada pode fazer com que toda a segurança da plataforma seja comprometida e com que os dados pessoais que deveriam ser privados sejam expostos para terceiros.

À vista disso, a funcionalidade de coleta de dados da plataforma será então avaliada seguindo os conceitos já estabelecidos pela literatura. Essa avaliação acontecerá sob três perspectivas diferentes em que na primeira pretende-se utilizar a documentação oficial da plataforma para descrever e avaliar os processos envolvidos na funcionalidade. Na sequência, a segunda perspectiva será sob a construção de uma aplicação hipotética utilizando o *Kaa Sandbox*. Por fim, a terceira perspectiva será a avaliação dos códigos fontes utilizados pela funcionalidade para realizar os processos de coleta de dados. Após essas análises, na seção 6.5, os resultados obtidos serão apresentados e discutidos para fim de validar os experimentos realizados na pesquisa.

6.4.1 Documentação

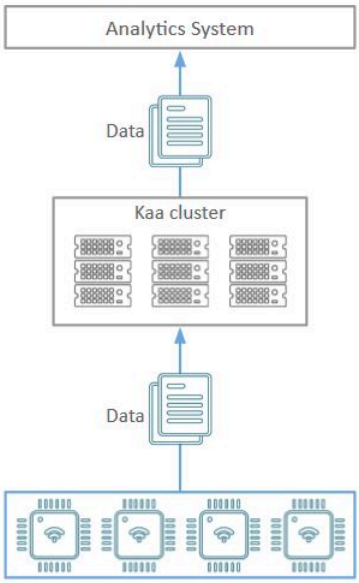
O subsistema de *Data Collection* da plataforma *Kaa* consiste em uma aplicação que coleta registros de dados (*Logs*) dos dispositivos e, a partir disso, pode armazenar esses registros em memória no próprio *endpoint* ou enviar os dados para o *Kaa Server* por meio do *Operation Service*. O *Operation Service* ao receber dados coletados dos *endpoints* pode persistir os dados no servidor utilizando um *Log Appender* (que é basicamente um banco de dados) ou ainda enviar esses registros para algum serviço de análise de dados de terceiros.

A *Kaa IoT Platform* permite a utilização de múltiplos *Log Appenders* simultaneamente e, por padrão, a plataforma possibilita utilizar o *File System Log Appender* que armazena os dados em um sistema de arquivos local no *Kaa Server*. Da mesma forma, possui suporte e integração com diversos bancos de dados como o *MongoDB*, o *Apache Cassandra*, o *Couchbase Server*, o *Apache Flume*, o *Apache Kafka* e o *Oracle NoSQL*. Isso faz com que seja possível diversificar o tratamento dos dados de acordo com a aplicação e com a necessidade do usuário.

Os dados que são coletados pela plataforma devem obrigatoriamente seguir uma estrutura que é pré-definida no momento de criação da aplicação no *Kaa SandBox*, portanto, a *Kaa IoT Open Source* só possibilita a manipulação de dados estruturados. Essa prática é adotada para garantir a compatibilidade dos dados com o sistema como um todo, posto que a arquitetura da plataforma segue um modelo monolítico e para que ela pudesse suportar uma maior diversidade de dados seria preciso que mais componentes fossem integralizados ao código fonte da plataforma.

Ademais, como pode ser visualizado na Figura 7, o *Kaa Data Collection* segue uma arquitetura que define as entidades envolvidas no processo de coleta de dados dos dispositivos finais (as Coisas). Os dados que coletados são transportados em duas etapas definidas nessa arquitetura. No primeiro caso, eles são coletados na origem (*endpoints*) e enviados ao *Operation Service* que funciona internamente no *Kaa Server* e, também são transportados quando são enviados do servidor para serviços externos utilizando os *Log Appenders*. Para fins de análise dessa pesquisa apenas a primeira situação está sendo avaliada, pois pressupõe-se que os dados que são enviados para outras aplicações pelo *Kaa Server* já foram coletados em um primeiro momento pelo *Kaa Data Collection*.

Figura 7 – Diagrama de funcionamento do *Kaa Data Collection*



Fonte: CyberVision, Inc. (2019).

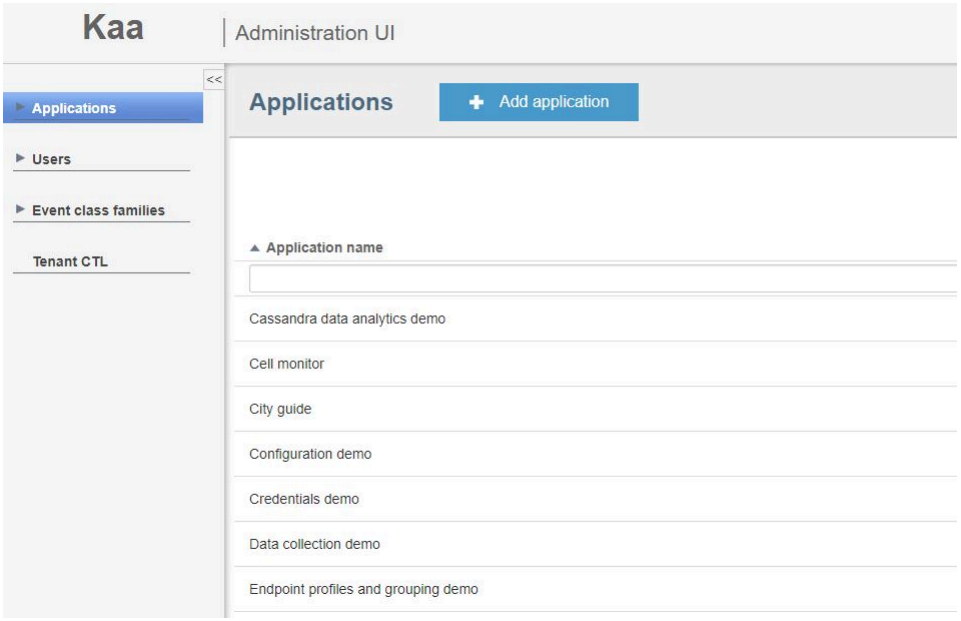
Segundo as informações contidas na documentação oficial da plataforma, o subsistema de coleta de dados da *Kaa IoT Open Source* dispõe de algumas funcionalidades estabelecidas como: a geração dos esquemas de dados diretamente no SDK do *endpoint*; a garantia de integridade dos dados e da validade das informações enviadas; a entrega eficiente dos dados para o *Operation Service*; e a persistência dos *Logs* coletados de acordo com o banco de dados escolhido pelo usuário. Também é declarado na documentação que a criação de esquemas para coleta de dados e a ativação da funcionalidade de coleta de dados em si são responsabilidades do desenvolvedor da aplicação, não sendo executado o procedimento de coleta automaticamente pela plataforma. Na sequência, será demostrado a utilização desses conceitos na criação de uma aplicação hipotética por meio do *Kaa SandBox*.

6.4.2 Aplicação

Após identificar na documentação da plataforma *Kaa* as particularidades da funcionalidade de *Data Collection* que é implementada pela *Kaa IoT Open Source*, nesta seção será descrito os procedimentos de avaliação realizados durante o processo de criação de uma aplicação hipotética de Internet das Coisas no *Administration UI*, disponível no *Kaa SandBox*. Essa avaliação objetiva listar e descrever as configurações que são disponibilizadas para o desenvolvedor no momento da criação de uma aplicação para que se possa estimar a usabilidade e a utilidade dessas configurações.

Primeiramente, na tela inicial do *Kaa SandBox* ao clicar no botão *Administration UI* o usuário é redirecionado para uma página de *Login* onde deve se identificar com uma conta já cadastrada pelo *Kaa* Administrador. Nesse caso, ao inserir as credenciais da conta padrão *"admin"* com a senha *"admin123"* é possível acessar à plataforma com as permissões de um *Tenant* administrador. Essas permissões, que já foram previamente descritas, concedem acesso às configurações que podem ser visualizadas abaixo na Figura 8.

Figura 8 – Tela de configurações do *Tenant* Administrador



Fonte: CyberVision, Inc. (2019).

Dando continuidade as discussões, ressalva-se que para iniciar a criação de uma aplicação basta o *Tenant* administrador clicar no botão *Add application*. Na tela seguinte é preciso configurar o nome da aplicação, bem como selecionar o tipo de serviço de credenciamento que será utilizado pela aplicação. Esse serviço de credenciamento oferece apenas duas opções para seleção, sendo elas a *"internal"* e a *"trustful"*. Contudo, não existem detalhes na documentação sobre a utilização desses modelos, há apenas instruções básicas indicando que deve ser usado a opção *"trustful"* para que se possa continuar as configurações da aplicação.

Após a criação da aplicação ser finalizada pelo *Tenant* administrador, é necessário fazer *Login* no *Administration UI* com uma conta de desenvolvedor para que seja possível realizar as demais configurações e programação da aplicação. O *Administration UI* permite que múltiplas contas estejam conectadas ao mesmo tempo no mesmo computador, ou seja, ao realizar o *Login* com a conta de desenvolvedor a aplicação mantém a sessão da conta de administrador que estava aberta anteriormente. Entretanto, as duas contas permanecem separadas em abas do navegador e não existem interferências das permissões de uma das contas nas ações da outra.

O *Tenant* desenvolvedor precisa em seguida configurar os esquemas de coleta de dados que serão utilizados pela aplicação. O *Kaa SandBox*, como previsto, cria uma versão inicial do esquema para facilitar o desenvolvimento. Essa versão criada pela plataforma não contém nenhum campo de dados do usuário, apenas campos com identificadores utilizados internamente pela plataforma. Com a criação de um esquema é então definido quais dados a plataforma poderá coletar da aplicação, como pode ser visto abaixo na Figura 9, o esquema padrão possui apenas campos identificadores.

Figura 9 – Esquema de coleta de dados padrão do *Kaa SandBox*

```
{
    "name":"EmptyLog",
    "namespace":"org.kaaproject.sample",
    "type":"record",
    "fields":[
    ]
}
```

Fonte: CyberVision, Inc. (2019).

Então, para finalizar a definição dos dados que serão coletados pela plataforma, se fez necessário inserir no esquema de configuração os campos identificadores dos dados. Para melhor entendimento o resultado desse processo pode ser visualizado na Figura 10.

Figura 10 – Esquema de coleta de dados com campos adicionados pelo desenvolvedor

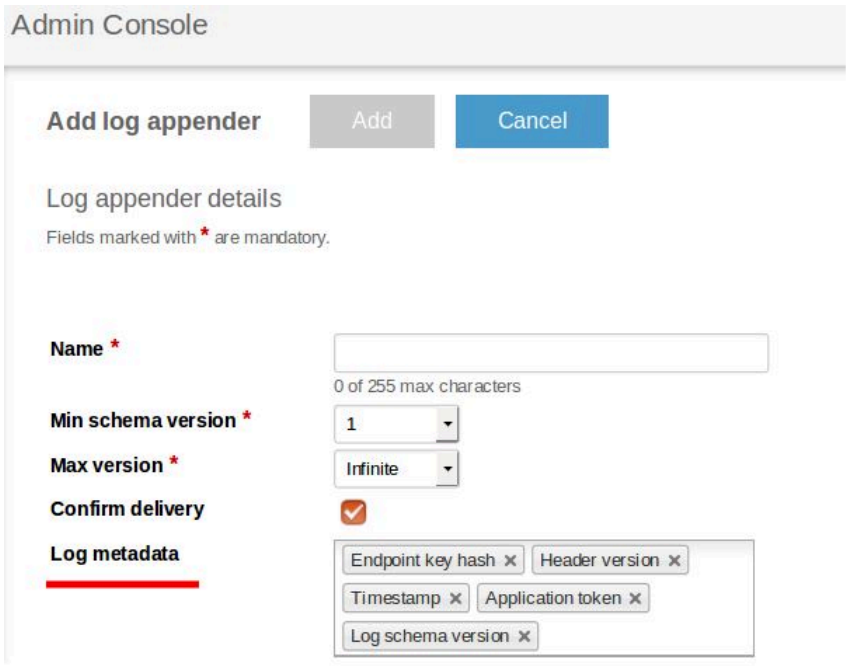
```
{
    "type":"record",
    "name":"LogData",
    "namespace":"org.kaaproject.kaa.schema.sample.logging",
    "fields":[
        {
            "name":"tag",
            "type":"string"
        },
        {
            "name":"message",
            "type":"string"
        }
    ]
}
```

Fonte: CyberVision, Inc. (2019).

Continuando o processo de configuração do *Data Collection* no *Administration UI*, o desenvolvedor precisa determinar quais serão os metadados coletados pela plataforma. Os metadados são informações sobre a aplicação e sobre os dados que foram configurados no esquema de coleta e ajudam a plataforma a identificar problemas que possam acontecer durante a coleta dos dados.

Na Figura 11 podem ser identificadas as configurações dos metadados coletados. Alguns desses que podem ser incluídos são: o *Log schema version* que controla a versão do esquema de dados que está configurado; o *Endpoint key hash* que serve como uma chave de identificação do dispositivo; o *Timestamp* o qual fornece informações sobre os tempos de coleta dos dados; e o *Aplication Token* que funciona como um identificador único da aplicação que gerou os dados coletados. Nessa tela também pode ser selecionada a opção *"Confirm delivery"* que é uma configuração utilizada quando é necessário que o servidor informe para o dispositivo a confirmação do recebimento dos dados. Essa confirmação é normalmente usada para liberar espaço de armazenamento no *endpoint*, pois após a confirmação do recebimento o dispositivo pode apagar os dados armazenados localmente sem perder dados da aplicação, visto que esses já estão salvos no *Kaa server*.

Figura 11 – Configuração dos metadados que serão coletados pelo *Log Appender*



Fonte: CyberVision, Inc. (2019).

Para finalizar a criação da aplicação de coleta de dados, é necessário que o desenvolvedor determine o *Log Appender* que receberá os dados para a plataforma. Sendo eles considerados como elementos externos, as configurações dos mesmos devem seguir os seus próprios padrões. No cenário a seguir, serão apresentadas as particularidades dos códigos utilizados pelo *Data Collection* para confirmar a veracidade das informações contidas na documentação.

6.4.3 Código

Almejando certificar a veracidade das informações contidas na documentação da plataforma e também no *Administration UI* do *Kaa SandBox*, além de finalizar os testes e as avaliações realizadas na funcionalidade de *Data Collection* da *Kaa IoT Open Source*, este tópico será usado para descrever os códigos fontes utilizados pelos *endpoints* para armazenar e enviar dados. Com essa análise espera-se confirmar que os códigos funcionam da forma como são descritos na documentação e, assim, poder assegurar o uso da *Kaa IoT Platform* como uma boa alternativa de plataforma *Open Source* para o desenvolvimento de aplicações de Internet das Coisas.

O subsistema de coleta e envio de dados da *Kaa IoT Open Source* varia de acordo com a linguagem de programação utilizada na aplicação. Como já descrito anteriormente, a plataforma suporta o desenvolvimento de aplicações com as linguagens Java, C, C++ e Objective-C. Dessa forma, como os códigos utilizados em todas as linguagens são funcionais e equivalentes, optou-se por apenas descrever os códigos escritos em Java, pois acredita-se que essa linguagem forneça suporte a um grande número de possíveis aplicações.

Internamente, o processo de coleta de dados da plataforma *Kaa* pode seguir duas abordagens: coletar e armazenar os dados ou então coletar e enviar os dados. Normalmente, uma aplicação criada só armazena dados em memória e isso faz com que dados possam ser perdidos caso aconteça algum problema com o dispositivo, como por exemplo ficar sem energia, parar de funcionar ou simplesmente ser desligado. Isto posto, em aplicações específicas pode ser necessário utilizar a primeira abordagem para persistir os dados localmente no próprio dispositivo. Nesse cenário, a *Kaa IoT Open Source* permite a integração com o *SQLite* que é uma biblioteca escrita em C que funciona como um banco de dados *SQL* leve e completo indicado para dispositivos com baixo poder computacional.

Assim como mencionado previamente, essa configuração de armazenamento de dados local só é ativada pelo desenvolvedor caso seja necessário. A plataforma *Kaa*, por padrão, não persiste nenhum tipo de dado localmente no dispositivo. Em síntese, um exemplo de código escrito em Java utilizado pela aplicação para salvar dados locais com o *SQLite* pode ser visualizado na Figura a seguir.

Figura 12 – Exemplo de persistência local de dados

```
// Default SQLite database name
String databaseName = "kaa_logs";
// Default maximum bucket size in bytes
int maxBucketSize = 16 * 1024;
// Default maximum amount of log records in a bucket
int maxRecordCount = 256;
// Setting SQLite log storage implementation
kaaClient.setLogStorage(new DesktopSQLiteDBLogStorage(databaseName, maxBucketSize, maxRecordCount));
```

```
// Setting SQLite log storage implementation
kaaClient.setLogStorage(new AndroidSQLiteDBLogStorage(/*Android context*/, "kaa_logs"/* default value */, 16 * 1024/* default value */, 256/* default valu
e */));
```

Fonte: CyberVision, Inc. (2019).

A segunda abordagem que coleta e envia os dados é utilizada com maior frequência em aplicações de Internet das Coisas. Sobretudo, é nessa configuração que é preciso que os desenvolvedores concentrem seus esforços para evitar que os dados dos usuários possam ser expostos indevidamente. Além dessa questão, como pode ser visto abaixo na Figura 13, o código em Java que coleta e envia os dados do dispositivo para o *Operation Service* na plataforma é definido como:

Figura 13 – Exemplo de código que coleta e envia dados

```
// Configure the log delivery listener
kaaClient.setLogDeliveryListener(new LogDeliveryListener() {
    @Override
    public void onLogDeliverySuccess(BucketInfo bucketInfo) { /* Called on success */ }
    @Override
    public void onLogDeliveryFailure(BucketInfo bucketInfo) { /* Called on failure */ }
    @Override
    public void onLogDeliveryTimeout(BucketInfo bucketInfo) { /* Called on timeout */ }
});
// Create a log entity according to the (org.kaaproject.sample.LogData) sample schema above
LogData logRecord = new LogData(Level.INFO, "tag", "message");
// Push the record to the collector
RecordFuture logDeliveryStatus = kaaClient.addLogRecord(logRecord);
// Get log delivery information
RecordInfo logDeliveryReport = logDeliveryStatus.get();
```

Fonte: CyberVision, Inc. (2019).

Nesse exemplo apresentado, pode ser identificado que o código utiliza os identificadores *"name"* dos campos do esquema para construir o objeto *"LogData"* que será enviado para o *Kaa Server*. Na sequência, o objeto é enviado para o *Operation Service* e então o dispositivo utiliza a função *"logDeliveryStatus"* para aguardar uma resposta do servidor. De acordo com a resposta recebida a aplicação pode reenviar os dados para garantir a persistência dos mesmos ou então limpar todos os registros locais daqueles dados, uma vez que o servidor já possui uma cópia salva com segurança.

A funcionalidade de *Data Collection* também oferece diversas estratégias para definir a frequência em que os dispositivos irão realizar o envio dos dados. A primeira opção é a função periódica, a qual faz as rotinas de coleta e envio serem chamadas várias vezes de acordo com um tempo determinado. Essa abordagem pode ser melhor compreendida na Figura 14.

Figura 14 – Função que envia os dados periodicamente

```
// Configure the strategy to upload no less than a hour worth of logs
kaaClient.setLogUploadStrategy(new PeriodicLogUploadStrategy(60, TimeUnit.MINUTES));
```

Fonte: CyberVision, Inc. (2019).

Outra abordagem que é possível ser elencada é a de contador de registros. Nessa configuração, é determinado que o envio de dados só irá acontecer quando um número específico de registros for coletado. Essa funcionalidade é muito útil para aplicações que geram dados constantes, mas que não precisam que eles estejam sempre disponíveis no *Kaa server*. Sendo assim, pode ser utilizada para enviar um, dez, cem ou mil registros de uma única vez. A função que determina essa abordagem pode ser vista abaixo na Figura 15.

Figura 15 – Função que envia os dados em grupos de registros

```
// Configure the strategy to upload logs every fifth log record added
kaaClient.setLogUploadStrategy(new RecordCountLogUploadStrategy(5));
// Configure the strategy to upload logs immediately
kaaClient.setLogUploadStrategy(new RecordCountLogUploadStrategy(1));
```

Fonte: CyberVision, Inc. (2019).

A terceira metodologia de envio de dados que pode ser utilizada com as aplicações da *Kaa IoT Platform* é a por tamanho de armazenamento. Basicamente, a função determina que a aplicação deve coletar dados até atingir um determinado tamanho em *bytes* e só então faz a aplicação enviar os dados ao servidor. Esse método faz com que o tamanho dos pacotes de dados enviados seja normalizado, ou seja, sempre do mesmo tamanho. A ilustração dessa função encontra-se na sequência.

Figura 16 – Função que envia os dados por tamanho em armazenamento

```
// Configure the strategy to upload logs every 64 KB of data collected
kaaClient.setLogUploadStrategy(new StorageSizeLogUploadStrategy(64 * 1024));
```

Fonte: CyberVision, Inc. (2019).

Além do exposto sobre as estratégias de periodicidade de envio de dados, cabe ressaltar que a plataforma também permite a utilização mesclada das três estratégias, fazendo com que se possa atender à demanda de diversas aplicações simultaneamente. Da mesma forma, permite que a aplicação se adapte as particularidades de *Hardware* dos *endpoints*. Ademais, como observado no decorrer da análise, a *Kaa IoT Platform* oferece códigos de simples implementação e que também permitem uma leitura fácil e intuitiva. Sendo assim, finaliza-se aqui as análises dos códigos que foram propostas e na seção seguinte serão apresentados os resultados obtidos através de todo o percurso analítico empreendido até então.

6.5 RESULTADOS

Baseando-se na literatura e em todas as análises realizadas no capítulo 6, objetiva-se, neste tópico, fazer a junção dos resultados obtidos e, então, perceber se os objetivos propostos no início do projeto foram alcançados. Dessa maneira, a ideia central que promoveu a execução dessa pesquisa foi a de estudar, avaliar e validar os mecanismos de segurança da informação e de privacidade de dados implementados por uma plataforma de Internet das Coisas de código livre denominada *Kaa IoT Platform*. Esse estudo se mostrou necessário devido ao eminente estabelecimento do paradigma da Internet das Coisas. Além disso, com esse estudo pretendeu-se contribuir com a solução dos problemas e impasses que acompanham o desenvolvimento da área em ascensão.

No início da avaliação, mais especificamente na seção 6.2, foi realizado uma comparação sucinta entre as gerações da *Kaa IoT Platform*, sendo elas: a *Kaa IoT Open Source*, que foi o objeto principal do estudo, e a *Kaa IoT Enterprise* que serviu para ajudar a identificar as funcionalidades da versão gratuita que foram alteradas ou melhoradas nessa versão paga. Para além disso, buscou-se listar as funcionalidades da plataforma que possuem impacto direto sobre a segurança e a privacidade para a Internet das Coisas. Com isso, identificou-se que a *Kaa IoT Open Source* é baseada na arquitetura monolítica e essa arquitetura pode ser um fator limitador quando se pensa em escalabilidade de funções e aplicações.

A arquitetura monolítica utilizada também dificulta a atualização de funcionalidades de segurança e de privacidade na plataforma, pois é necessário parar por completo o funcionamento da plataforma para que se possa realizar atualizações ou alterações no código fonte da mesma. Em relação aos protocolos de comunicação utilizados por ambas as versões, pôde ser interpretado que a versão *Open Source* da plataforma tentou utilizar uma implementação própria e fechada do protocolo *TCP*, o que foi descontinuado na versão paga. Esse ponto indica que possivelmente essa implementação não foi bem sucedida ou pelo menos não atingiu os resultados que eram esperados pelos desenvolvedores que modificaram os protocolos utilizados na versão *Enterprise* para protocolos abertos.

Na questão dos protocolos de segurança identificou-se que ambas as gerações da plataforma utilizam bons protocolos e algoritmos de criptografia. Sendo que as diferenças que existem entre elas não possuem impactos diretos na qualidade da segurança oferecida pela *Kaa IoT Open Source*. Sobre o credenciamento de novos dispositivos, a versão gratuita demonstrou não suportar o gerenciamento em tempo real dos dispositivos conectados, apenas permitindo um credenciamento inicial dos mesmos. Em relação à coleta de dados realizada pelas duas gerações, observou-se que a versão gratuita se limita aos dados estruturados, no entanto essa particularidade não afeta diretamente na segurança da plataforma. Finalizando essa primeira análise, identificou-se que a plataforma *Open Source* não dá suporte para OTA (*Over-The-Air-Updates*) que são consideradas uma tendência necessária para o futuro da Internet das Coisas, demonstrando-se, assim, como um problema.

Referente à segunda análise, objetivou-se esmiuçar o funcionamento do *Kaa SandBox* e também detalhar os sistemas de autenticação e de permissões utilizados pela *Kaa IoT Open Source*. Nessa avaliação foi possível entender que a plataforma utiliza um sistema de permissões baseado em múltiplos inquilinos (*Tenants*) e que esse modelo se mostra eficiente especialmente em plataformas de Internet das Coisas, posto que permite a coexistência de múltiplos serviços e usuários cada qual com suas devidas permissões. Contudo, é válido ressalvar que esse modelo querer atenções especiais para que não seja concedido permissões excessivas para usuários indevidos e que, igualmente, não sejam deixadas contas padrões ativas ou sem alteração de senha na plataforma.

Na última avaliação realizada foi aprofundado o estudo sobre as particularidades da funcionalidade de coleta de dados da plataforma porque essa funcionalidade implica diretamente no objeto principal da pesquisa que é a privacidade dos dados pessoais no paradigma da Internet das Coisas. Com base nisso, inicialmente, foi verificado na documentação oficial quais eram os procedimentos envolvidos no processo de coleta de dados dos *endpoints* implementados pela plataforma. Foi possível identificar via documentação que a plataforma possui uma grande variedade de integrações com bancos de dados externos, chamados nesse contexto de *Log Appenders*.

Sob uma perspectiva de aplicação, utilizando o *Kaa SandBox*, se fez viável descrever os passos que precisam ser realizados para criar uma aplicação completa de coleta de dados. Também foi possível validar o funcionamento dos esquemas de coleta de dados que funcionam na prática exatamente como descritos na documentação oficial. Além disso, ficou claro que a plataforma só coleta dados que foram previamente indicados pelo desenvolvedor no esquema de coleta. E, por fim, verificou-se que a plataforma possui uma funcionalidade que caso ativada faz com que o *endpoint* reenvie os dados coletados até receber uma confirmação de recebimento do servidor, garantido assim a persistência correta e a integridade dos dados exportados.

Na última análise realizada sob a funcionalidade de coleta de dados validou-se os códigos fontes utilizados pelos *endpoints* para enviar os dados para o *Kaa Server*. Nesse mesmo sentido, foi verificado o código usado para realizar persistência local dos dados caso necessário, utilizando para isso a biblioteca *SQLite*. Em ambos os casos foi averiguado que os códigos se comportam exatamente como descritos na documentação e no painel *Administration UI*. Também foram descritas as estratégias de periodicidade de envio de dados que podem ser utilizadas via código nas aplicações da plataforma.

Por conseguinte, percebeu-se que a plataforma de IoT *Kaa IoT Open Source* se mostrou como uma boa alternativa de *Software* livre para a prototipagem e desenvolvimento de aplicações dedicadas à Internet das Coisas. Demonstra ser uma ferramenta muito útil para pesquisas acadêmicas relacionadas à área de Internet das Coisas, podendo ser usada para a validação de outras tecnologias e paradigmas. Sob a perspectiva da segurança e da privacidade, concluiu-se que a ferramenta possui boas funcionalidades e que, assim como acontece em outros sistemas, deixa responsabilidades perigosas nas mãos de poucos usuários.

7 CONCLUSÃO

A Internet das Coisas (IoT), como evidenciado no decorrer desta pesquisa, tem se mostrado em crescente popularização no âmbito das tecnologias e, com isso, resolver os impasses que permeiam a área é um objetivo constante da Ciência da Computação. Quando se considera um cenário com bilhões de dispositivos conectados à internet e coletando dados dos usuários constantemente precisa-se pensar, primordialmente, em como a coleta desses dados está sendo administrada. Nesse sentido, por meio do desenvolvimento de novas aplicações relacionadas ao tema se faz necessário estudar e avaliar as tecnologias utilizadas nos processos de criação para validar o correto funcionamento dessas aplicações. Quando se pensa na segurança e na privacidade dos dados dos usuários, realizar essas validações mostra-se ainda mais relevante, pois esses temas se aplicam diretamente ao direito à privacidade dos usuários.

Essa pesquisa permitiu avaliar uma plataforma de Internet das Coisas, a *Kaa IoT Open Source*, pelos pontos de vista das configurações de segurança da informação e de privacidade dos dados implementadas em suas primitivas. Esses conceitos foram especialmente avaliados em cima da funcionalidade de *Data Collection* da plataforma, visto que essa funcionalidade tem inferência direta sobre a privacidade dos usuários. Com base na totalidade da avaliação realizada foi possível inferir que a plataforma possui boas tecnologias de segurança em sua construção. Apesar disso, ela depende de boas práticas da parte dos usuários desenvolvedores para que a privacidade dos dados possa ser mantida. Ademais, com esse estudo foi exequível validar a veracidade das informações contidas na documentação oficial da plataforma e, com isso, assegurar o uso da *Kaa IoT Open Source* como uma boa alternativa de plataforma de código livre para o desenvolvimento de aplicações para a Internet das Coisas.

Tencionando a possibilidade de trabalhos futuros, seria interessante fazer uma avaliação específica sobre outras funcionalidades da plataforma. Nesse contexto, também seria interessante comparar a *Kaa IoT Open Source* com outra plataforma de Internet das Coisas de código livre no intuito de elencar as funcionalidades e determinar qual delas é a mais indicada para o uso em pesquisas e no desenvolvimento de aplicações focadas em garantir a segurança e a privacidade dos dados dos usuários. Sobretudo, estudar métricas que possam ser utilizadas para validar a segurança de aplicações de Internet das Coisas também é uma possibilidade de pesquisa no futuro para avançar as pesquisas em relação à IoT e às plataformas de Internet das Coisas. Em suma, espera-se, com as análises aqui empreendidas, contribuir em novas pesquisas, principalmente, as relacionadas à segurança e privacidade na Internet das Coisas.

REFERÊNCIAS

ATZORI, L.; IERA, A.; MORABITO, G. The Internet of Things: A Survey. **Computer Networks**, Nova Iorque, v. 54, n. 15, p. 2787–2805, 2010. Disponível em: <http://dx.doi.org/10.1016/j.comnet.2010.05.010>. Acesso em: 10 mai. 2019.

BORGES, F. Introdução à Privacidade: Uma Abordagem Computacional. In: XVI Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais. Niterói: SBC, 2016. p. 1–43. Disponível em: <https://www.researchgate.net/publication/312295796_Introducao_a_Privacidade_Uma_Abordagem_Computacional>. Acesso em: 5 dez. 2018.

BROSTOFF, Alexander. **Improving password system effectiveness**. 2004. Tese (Doutorado) – Londres. Disponível em: <http://discovery.ucl.ac.uk/1445330/1/U592650%20Redacted.PDF>. Acesso em: 20 fev. 2019.

CABRAL, C.; CAPRINO, W. **Trilhas em Segurançada Informação:** Caminhos e ideias para a proteção de dados. Rio de Janeiro: Brasport, 2015. Disponível em: <https://books.google.com.br/books?id=CeInBgAAQBAJ>. Acesso em: 15 dez. 2018.

CYBERVISION, INC. **Kaa IoT Open Source**. [S.l.: s.n.], 2019. Disponível em: <https://kaaproject.github.io/kaa/docs/v0.10.0/Welcome/>. Acesso em: 10 out. 2019.

EVANS, D. **A Internet das Coisas:** Como a próxima evolução da Internet está mudando tudo. White paper: Cisco Internet Business Solutions Group (IBSG), 2011. p. 1–11. Disponível em: <https://www.cisco.com/c/dam/global/pt_br/assets/executives/pdf/internet_of_things_iot_ibsg_0411final.pdf>. Acesso em: 9 mai. 2019.

KAA IOT TECHNOLOGIES. **Kaa IoT Platform**. [S.l.: s.n.], 2019. Disponível em: <https://www.kaaproject.org/>. Acesso em: 14 out. 2019.

OLIVEIRA NETO, I. R. **Síntese de requisitos de segurança para internet das coisas baseada em modelos em tempo de execução**. 2015. Diss. (Mestrado) – Goiânia. Disponível em: <http://repositorio.bc.ufg.br/tede/handle/tede/5185>. Acesso em: 15 fev. 2019.

PIRES, P. F. et al. Plataformas para a Internet das Coisas. In: XXXIII Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos. Vitória: SBC, 2015. p. 110–169. Disponível em: <http://sbrc2015.ufes.br/wp-content/uploads/Ch3.pdf>. Acesso em: 10 fev. 2019.

RAJ, P.; RAMAN, A. C. **The Internet of Things:** Enabling Technologies, Platforms, and Use Cases. Boca Ratón: CRC Press, 2017. Disponível em: <https://books.google.com.br/books?id=cLI0DgAAQBAJ>. Acesso em: 15 set. 2019.

SANTOS, C. C.; SALES, J. D. A. O Desafio da Privacidade na Internet das Coisas. **Revista Gestão**, Recife, v. 13, p. 282–290, 2015. Disponível em: <https://periodicos.ufpe.br/revistas/gestaoorg/article/view/22115>. Acesso em: 15 fev. 2019.

SILVA, D. R. P. da; STEIN, L. M. Segurança da informação: uma reflexão sobre o componente humano. **Ciências e Cognição**, Rio de Janeiro, v. 10, p. 46–53, 2007. Disponível em: <http://www.cienciasecognicao.org/pdf/v10/m346130.pdf>. Acesso em: 10 mar. 2019.