UNIVERSIDADE FEDERAL DO PARÁ
INSTITUTO DE CIÊNCIAS EXATAS E NATURAIS
FACULDADE DE COMPUTAÇÃO
CURSO DE BACHARELADO EM CIÊNCIA DA COMPUTAÇÃO

RAÍSSA LORENA SILVA DA SILVA

UM ESTUDO SOBRE AMBIENTE IOT E SEUS ASPECTOS DE SEGURANÇA

Belém
2017

UNIVERSIDADE FEDERAL DO PARÁ
INSTITUTO DE CIÊNCIAS EXATAS E NATURAIS
FACULDADE DE COMPUTAÇÃO
CURSO DE BACHARELADO EM CIÊNCIA DA COMPUTAÇÃO

RAÍSSA LORENA SILVA DA SILVA

UM ESTUDO SOBRE AMBIENTE IOT E SEUS ASPECTOS DE SEGURANÇA

Trabalho de Conclusão de Curso apresentado para obtenção do grau de Bacharel em Ciência da Computação.

Orientador: Prof. Dr. Roberto Samarone dos Santos Araújo

Belém
2017

Raíssa Lorena Silva da Silva
Um Estudo Sobre Ambiente IoT e Seus Aspectos de Segurança/ Raíssa Lorena Silva da Silva. – Belém, 2017.
66 p. : il. (algumas color.) ; 30 cm.

Orientador: Prof. Dr. Roberto Samarone dos Santos Araújo

Monografia – Universidade Federal do Pará
Instituto de Ciências Exatas e Naturais
Curso de Bacharelado em Ciência da Computação, 2017.

1. Segurança em IoT. 2. Criptografia ABE. 3. Internet das Coisas. 4. Confidencialidade em IoT. 5. Sigilo em IoT. I. Título.

RAÍSSA LORENA SILVA DA SILVA

UM ESTUDO SOBRE AMBIENTE IOT E SEUS ASPECTOS DE SEGURANÇA

Trabalho de Conclusão de Curso apresentado para obtenção do grau de Bacharel em Ciência da Computação.

Data da Defesa: 17 de abril de 2017
Conceito: Bom

Banca Examinadora

Prof. Dr. Roberto Samarone dos Santos Araújo
Faculdade de Computação - UFPA
Orientador

Prof. Dr. Denis Lima do Rosário
Faculdade de Computação - UFPA
Membro da Banca

Prof. Dr. Nelson Cruz Sampaio Neto
Faculdade de Computação - UFPA
Membro da Banca

Belém
2017

Dedico este trabalho à Deus e a minha família.

AGRADECIMENTOS

Agradeço primeiramente à Deus, por ter sido a minha base de tudo na vida, a quem sempre recorri nas horas mais difíceis e sempre me ouviu.

Agradeço a minha amada família, por sempre estarem ao meu lado e mostrarem a importância dos estudos, por me oferecer toda a ajuda possível para que eu alcançasse meus objetivos.

Agradeço ao meu namorado, Fábio Miranda, por ter me dado todo o apoio durante o desenvolvimento deste trabalho e por ter me ajudado imensamente.

Agradeço aos meus amigos, Hugo Lima, Tiago David e Wendel Renan, os quais tiveram grande importância para o desenvolvimento deste trabalho e sempre tirarem minhas dúvidas, mesmo quando eram dúvidas deles.

Agradeço ao meu amado amigo, Luiz Danin, por me acompanhar deste os tempos do CEFET, a quem tive o prazer de conhecer juntamente quando conheci o mundo da computação, a quem sempre foi o mais próximo de mim, mesmo quando esteve longe. Sou muito grata por todos esses anos de amizade.

Agradeço aos amigos que adquiri durantes esses anos de curso, Leonardo Formento, Janynne Palheta, Brunelli Miranda, Roberto Junior, Angelo Oliveira, Nicoli Souza, Renato Oliveira e Anderson Furtado. Aos que esqueci, mas que sempre estiveram comigo durante esses anos na UFPA, sou profudamente grata.

Agradeço aos meus queridos professores, por terem me ensinado, terem tido paciência e dedicação para compartilhar seus conhecimentos durantes esses anos de curso. Em especial, agradeço à Prof[a]. Regiane Kawasaki, Prof. Benedito Ferreira e Prof[a] Marcelle Mota.

Por último, mas não menos importante, agradeço ao meu querido orientado, Prof. Roberto Samarone. Sou grata pela paciência e dedicação para me instruir, por saber me cobrar nas horas certas, por me guiar quando eu não sabia o que fazer e por ser um dos professores que me são fonte de inspiração para prosseguir nessa área.

“A mente que se abre a uma nova ideia
jamais voltará ao seu tamanho original.”
(Albert Einstein)

RESUMO

A Internet das Coisas (IoT) é um novo conceito tecnológico que permite a adaptação de dispositivos do cotidiano para transmitirem informações à Internet. Ou seja, é uma arquitetura de Internet capaz de conectar diversos dispositivos inteligentes, proporcionando a integração do mundo físico ao digital. Os dispositivos IoT são capazes de executar tarefas e utilizar a Internet para envio ou consumo de informações, podendo ou não necessitar da intervenção humana. A Internet é um ambiente hostil, durante o tráfego das informações, dados podem ser capturados e/ou alterados, provocando o comprometimento das informações e a privacidade dos usuários. Neste contexto, este trabalho tem como objetivo apresentar um estudo sobre a segurança em ambientes IoT, visando principalmente o sigilo das informações.

Palavras-chave: Internet das coisas. segurança em IoT. confidencialidade em IoT. sigilo em IoT

ABSTRACT

The Internet of Things (IoT) is a new technological concept that allows the adaptation of everyday devices to transmit information to the Internet. That is, it is an Internet architecture capable of connecting several intelligent devices, providing the integration of both physical and digital world. IoT devices are able to perform tasks and use the Internet for sending or consuming information that may or may not need human intervention. The Internet is a hostile environment during the traffic of information; data can be captured and / or altered compromising information and privacy of users. In this context, this work aims to present a study on the security in IoT environments, aiming mainly at the secrecy of information.

Keywords: Internet of things. Security of IoT. Confidentiality of IoT. Secrecy of IoT .

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

ABAC	Attribute-Based Access Control
ABE	Attribute-Based Encryption
AES	Advanced Encryption Standard
CP-ABE	Ciphertext-Policy Attribute-Based Encryption
CRC	Cyclic Redundancy Check
ECC	Elliptic Curve Cryptography
EMEA	Europe, the Middle East and Africa
DTLS	Datagram Transport Layer Security
IoT	Internet of Things
KP-ABE	Key Policy Attribute Based Encryption
NIST	National Institute of Standards and Technology
RBAC	Role-based Access Control
RFID	Radio Frequency Identification
SOA	Service Oriented Architecture
SSO	Single Sign-On

SUMÁRIO

1 INTRODUÇÃO

O aperfeiçoamento dos computadores para compartilhamento de informações ampliou o seu uso em diversos setores. Essa onda de aperfeiçoamento promoveu o desenvolvimento de novas tecnologias, as quais continuaram a crescer ao longo dos anos e foram se expandindo em vários aspectos da vida cotidiana. Nos dias atuais, estamos cercados de tecnologias, objetos como telefones, carros e televisores são capazes de se conectar a Internet para realizar tarefas ou trocar informações. Essa rede de objetos inteligentes que se conectam a Internet é conhecida como Internet das Coisas (IoT).

A IoT é uma infraestrutura para realizar a integração de objetos físicos e virtuais, por meio de tecnologias de comunicação e de captura de dados. Com a IoT, não são apenas pessoas e recursos que estão conectados, tudo pode está conectado a uma rede. Objetos, pessoas e até animais, poderão estar conectados e gerando ou capturando informações, e todas essas informações podem se relacionar através da adoção de computação em nuvem no ambiente IoT.

A inserção da IoT no cotidiano muda a forma como as tarefas são executadas. Tarefas que antes consumiam muito tempo para serem exercidas, com a adoção dispositivos da IoT, podem ser realizadas de forma mais ágil e eficiente. Por exemplo, na coleta de informações para registro de pacientes em um hospital: ao utilizar um dispositivo que contenha o histórico clínico conectado ao paciente, as coletas de informações para a criação de um prontuário passam a ser mais dinâmicas.

Além de tornar a realização de tarefas mais rápidas, ou até mesmo automatizá-las, outra vantagem da IoT é fazer os dispositivos se ajustarem a predileções ou necessidades do usuário ou ambiente. Por exemplo, ao utilizar dispositivos IoT, um médico pode otimizar sua rotina ao monitorar um paciente a distância e verificar o andamento dos tratamentos recomendados e sua eficácia de forma mais segura. Da mesma forma, o paciente poderá tirar dúvidas, realizar exames, notificar o médico sobre qualquer alteração clínica em tempo real sem que precise sair de sua casa.

Apesar de seus inúmeros benefícios, a IoT possui necessidades que dificultam sua implantação. Entre essas necessidades, estão questões relacionadas à segurança e privacidade dos usuários e dispositivos. Os dados utilizados em ambiente IoT devem ser seguros, protegendo e assegurando a confidencialidade das informações. Caso contrário, haverá vulnerabilidades e sistemas críticos ficarão sujeitos a ataques. Dentro deste contexto, este trabalho realiza um estudo sobre os aspectos de segurança em ambiente IoT, apresentando trabalhos e medidas adotadas atualmente para garantir a segurança em IoT e propondo um esquema teórico para distribuição de chaves em ambientes IoT.

1.1 Objetivos

Este trabalho tem como objetivo geral a elaboração de um esquema teórico para distribuição de chaves em ambiente IoT, considerando principalmente o sigilo das informações. Para alcançar o objetivo geral, foram determinados os seguintes objetivos específicos:

- Identificar o quadro atual de segurança em IoT;
- Estudar arquiteturas IoT relevantes;
- Comparar a segurança nas arquiteturas estudadas;
- Elaborar um esquema teórico para distribuição de chaves em ambiente IoT.

1.2 Motivação

O cenário atual da IoT apresenta um forte crescimento. Gartner (2016) realizou uma pesquisa sobre IoT em 18 setores de negócios na América do Norte, EMEA, Ásia / Pacífico e América Latina. Nesta pesquisa, 29% das empresas estão usando IoT, 14% está planejando implementar nos próximos 12 meses, 21% deseja implementar em 2016. Em outras palavras, o número de organizações que adotam IoT vai crescer 50% em 2016, atingindo 43% das organizações em geral. Este crescimento da implantação da IoT acarreta no crescimento de troca de informações entre dispositivos e/ou usuários, o que torna relevante a necessidade de meios para garantir a segurança e privacidade.

Para Borgohain, Kumar e Sanyal (2015), apesar do grande potencial da IoT, toda a infraestrutura de comunicação da IoT é falho do ponto de vista da segurança e é suscetível a perda de privacidade para os usuários finais. Sendo assim, há a necessidade de garantir que somente os dispositivos autorizados tenham acesso a dados e recursos aos quais são permitidos, bem como fornecer dados consistentes. Desta forma, este trabalho foi motivado a elaborar um esquema teórico para distribuição de chaves em ambientes IoT, promovendo o sigilo das informações trocadas neste ambiente.

Outra motivação para o desenvolvimento do esquema proposto, foi a escassez de pesquisas que não sofram influência de tecnologias utilizadas por determinadas empresas ou plataformas específicas ou características da região de pesquisa, por exemplo, dificuldades na infraestrutura. Essas interferências dificultam a implantação de soluções em maior escala, requerendo uma solução adaptável a diferentes cenários (WEBER, 2010).

A partir disso, o trabalho propõe um esquema que seja utlizados em ambientes IoT de forma a considerar a variação de participantes e ambientes, e o baixo poder de processamento computacional encontrados nestes ambientes.

1.3 Metodologia

Para a realização deste trabalho, foi realizado inicialmente uma revisão da literatura, identificando trabalhos relevantes sobre IoT. Após isso, foram identificados os desafios que ainda são persistentes para a implantação da IoT. Entre esses desafios, estão presentes questões relacionadas à segurança e privacidade dos dispositivos e usuários. Desta forma, este trabalho teve seu foco em segurança da informação.

Dentro deste contexto, foi estudado sobre os mecanismos de segurança utilizados atualmente em IoT, os quais foram destacadas técnicas de autenticação, controle de acesso, confidencialidade e integridade. Cada técnica foi estudada a fim de analisar as características e identificar as vulnerabilidades.

Após realizado o estudo, foi elaborado um esquema simples de criptografia para distribuição de chaves. O esquema trata os dados trafegados de forma sigilosa, para tal, todos os dados transmitidos são criptografados. A partir da criptografia utilizada, também é abordado o tratamento de controle de acesso, no qual somente os participantes com características definidas podem ter acesso aos dados.

1.4 Trabalhos relacionados

Com o objetivo facilitar o entendimento e levantar os diferentes tipos de soluções sobre segurança em IoT, foram estudados três trabalhos relacionados que estão no mesmo contexto desta pesquisa. O primeiro trabalho, de Wangham, Domenech e Mello (2013), trata de autenticação e de autorização para IoT. O segundo trabalho, de Sicari et al. (2015), realiza uma análise sobre segurança, privacidade e confiança em IoT. O terceiro trabalho, de Borgohain, Kumar e Sanyal (2015), é uma pesquisa sobre a segurança em IoT.

Wangham, Domenech e Mello (2013) apresentam um trabalho sobre infraestruturas de autenticação e autorização para IoT, identificando os principais desafios e soluções de segurança. Para tal, foi realizado um estudo apresentando uma visão geral sobre IoT mostrando as tecnologias envolvidas e aplicações para IoT. Após isso, os autores apresentam questões sobre segurança, identificando requisitos e ameaças. Dentro deste contexto, é apresentada uma visão de autenticação e autorização em IoT, definindo a autenticação de usuários, a autenticação de dispositivos e os mecanismos de autorização. Após isso, os autores apresentam as infraestruturas de autenticação e autorização aplicadas à IoT, as iniciativas de gestão de identidades para IoT e os trabalhos acadêmicos que abordam autenticação ou autorização em IoT.

O trabalho de Sicari et al. (2015) apresenta os principais desafios de pesquisa e as soluções existentes no campo da segurança da IoT, identificando questões em aberto e sugerindo dicas para pesquisas futuras. Para tal, o trabalho apresenta uma análise de autenticação, confidencialidade e controle de acesso para IoT abordando os trabalhos existentes e as tecnologias utilizadas. Os

autores também analisam trabalhos sobre a privacidade em IoT, argumentando que a privacidade é apenas parcialmente resolvida e há um amplo espaço de pesquisa sobre privacidade que deve ser investigado. O termo confiança é apresentado, assumindo as suas variações de significados na literatura, e os trabalhos que se propõem a tratar de confiança em IoT. Sicari et al. (2015) também apresentam e analisam aplicações, camadas de segurança e segurança móvel para IoT.

O terceiro trabalho relacionado, de Ahlmeyer e Chircu (2016), é uma revisão na literatura considerando a atuação da IoT no setor empresarial e as tecnologias que mais se destacam. São analisados três desafios de segurança em Iot. O primeiro é o problema de falta de segurança para quem desenvolve e para quem utiliza dispositivos IoT. O segundo desafio é a falta de documentos técnicos que analisam as ameaças à segurança da IoT. O terceiro é a falta de leis e regulamentação para a segurança e privacidade de aplicações IoT. Após isso, os autores propõem como solução uma estrutura de segurança para IoT que contém níveis de segurança, atividades de segurança, cadeia de valores de segurança, normas de segurança e educação em segurança.

1.5 Estrutura do trabalho

Este trabalho foi dividido em 5 capítulos. Além dessa Introdução, os outros 4 capítulos são listados abaixo:

Capítulo 2 – Embasamento Teórico. Este capítulo apresenta conceitos que são abordados durante o desenvolvimento do trabalho. Apresentando assuntos que se correlacionam durante o estudo, como computação em nuvem e técnicas de segurança.

Capítulo 3 – Internet das Coisas. Este capítulo aborda IoT, identifica os cenários, aplicações, desafios e o contexto atual de segurança em IoT. Da mesma forma, apresenta três arquiteturas da IoT e seus aspectos de segurança.

Capítulo 4 – Proposta de uma esquema para distribuição de chaves em ambientes IoT. Este capítulo apresenta um esquema para compartilhamento de chaves, apresentando uma visão geral, requisitos necessários para o funcionamento do esquema, participantes, premissas, descrição do esquema, discussão sobre a segurança do esquema e uma a aplicação do esquema em uma das arquiteturas estudadas.

Capítulo 5 - Considerações Finais. Este capítulo apresenta as conclusões obtidas após o desenvolvimento do trabalho e os trabalhos futuros.

2 EMBASAMENTO TEÓRICO

Este trabalho realiza um estudo sobre a segurança em ambientes IoT, para tal, é necessário o entendimento de alguns conceitos. Desta forma, neste capítulo são apresentados características de computação em nuvem, técnicas nas quais computação em nuvem é baseada, técnicas de implantação e modelos de serviços. Da mesma forma, são apresentados conceitos de segurança como autenticação, controle de acesso, autorização e integridade.

2.1 Computação em Nuvem

Abordar temas como IoT requer a compreensão de conceitos como computação em nuvem. Segundo Botta et al. (2014), a computação em nuvem tem recursos praticamente ilimitados em termos de capacidade de armazenamento e processamento, e os problemas da IoT são pelo menos parcialmente resolvidos, tornando nuvem e IoT tecnologias complementares.

Segundo Mell e Grance (2011), do *National Institute of Standards and Technology - NIST*, a computação em nuvem é um modelo que permite acesso sob-demanda de recursos computacionais compartilhados e configuráveis (por exemplo, redes, servidores, armazenamento, aplicativos e serviços) que podem ser rapidamente provisionados e liberados com esforço de gestão mínimo ou interação do provedor de serviços.

Os recursos de computação em nuvem podem ser utilizados a qualquer hora e local com acesso a Internet, proporcionando serviços de forma global. De acordo com Kaushik e Jha (2015), a computação em nuvem permite ao usuário armazenar, compartilhar, acessar, manter e controlar dados na Internet em vez de fazê-lo em qualquer *hardware*. Para Benatallah (2011), a computação em nuvem é uma arquitetura onde computadores poderosos são substituídos por um super computador e até mesmo uma rede de supercomputadores, e os usuários estão distribuídos em várias áreas geográficas acessando pela Internet.

Os recursos utilizados em nuvem são dispostos ao usuário sob demanda. Ou seja, caso o usuário precise de mais recursos (por exemplo, mais espaço para armazenamento), o serviço de nuvem irá dispor sem que seja necessário realizar solicitações ao provedor de serviço. Esses recursos são dispostos a vários clientes para o acesso a serviços através da Internet por diferentes plataformas (por exemplo, computador, *notebook*, celular, *tablet*). Os serviços são reunidos e realocados conforme a necessidade do usuário, podendo dois usuários fazerem uso de um mesmo recurso (por exemplo, local de armazenamento de dados) sem que um tenha a consciência do outro.

A utilização de serviços sob demanda requer que recursos sejam alocados ou liberados a qualquer momento, isso proporciona elasticidade rápida sobre os serviços de nuvem. Essa elasticidade oferece ao usuário uma ideia de que os recursos são ilimitados e podem ser utilizados

a qualquer momento. Segundo Mell e Grance (2011), o uso de recursos pode ser monitorado, controlado e reportado, oferecendo transparência para o provedor e para o consumidor do serviço utilizado.

Para Benatallah (2011), a computação em nuvem está baseada em duas principais técnicas, Arquitetura Orientada a Serviços (SOA) e Virtualização. É dito que computação em nuvem é baseado em SOA por fornecer um conjunto de serviços vagamente integrado que pode ser usado em vários domínios de negócios, permitindo que os serviços sejam descobertos, compostos e executados. A virtualização permite ao usuário dispensar compra de recursos e instalações, logo que a nuvem traz os recursos para os usuários.

Técnica ou modelo de implantação em nuvem é a maneira pela qual uma nuvem é utilizada para fornecer um serviço específico. Mell e Grance (2011) definem como nuvem privada, nuvem comunitária, nuvem pública e nuvem híbrida. A nuvem privada dispõe de infraestrutura para uma única organização que pode ser utilizada por vários usuários. A nuvem comunitária dispõe de infraestrutura para uma comunidade de usuários, sendo propriedade, gerenciada e operada por uma ou mais organizações. A nuvem Pública dispõe de infraestrutura para um público em geral, sendo propriedade, gerenciada eoperada por uma empresa, organização acadêmica ou governamental. A nuvem híbrida é composta por diferentes modelos de nuvem (privada, comunitária ou pública).

Mell e Grance (2011) definem três modelos de serviço para computação em nuvem, Software como Serviço, Plataforma como Serviço e Infraestrutura como Serviço. O *Software* como Serviço (*Software as a Service - SaaS*) oferece ao usuário o uso de aplicação em nuvem, dispondo acesso somente à aplicação. A Plataforma como Serviço (textitPlatform as a Service - PaaS) dispõe ao usuário infraestrutura para implantar, configurar e desenvolver aplicações no ambiente da hospedagem. A Infraestrutura como Serviço (textitInfrastructure as a Service - IaaS) oferece recursos computacionais ao usuário permite acesso a sistemas operacionais, componentes de rede, processamento, armazenamento, implantação e desenvolvimento de aplicações.

Embora Mell e Grance (2011) apresentem somente três modelos de serviços para computação em nuvem, outro autores, por exemplo, Benatallah (2011), apresentam outros modelos tais como: Banco de Dados como Serviço; Informação como Serviço; Processo como Serviço; Integração como Serviço; Segurança como Serviço; Gerenciamento como Serviço; e Teste como Serviço.

2.2 Segurança

A tecnologia aplicada à informação cria riscos, a informação pode ser revelada, modificada, destruída ou perdida (BLAKLEY; MCDERMOTT; GEER, 2001). Segundo Anderson

(2008), a segurança é importante pois muitos sistemas de segurança têm requisitos de garantia críticos, o seu fracasso pode pôr em perigo a vida humana e o ambiente, prejudicar seriamente as grandes infraestruturas econômicas, pôr em risco a privacidade pessoal e facilitar a criminalidade.

Algumas técnicas devem ser oferecidos para garantir a segurança na comunicação entre sistemas. A seguir são apresentadas as técnicas de autenticação, controle de acesso, confidencialidade e integridade, que são abordas durante este trabalho.

2.2.1 Autenticação

A autenticação é uma forma de identificar digitalmente um usuário, devendo garantir que tanto a entidade quanto a conexão devem são legítimas. "No caso de uma mensagem, como uma advertência ou sinal de alarme, a função do serviço de autenticação é garantir ao destinatário que a mensagem é proveniente de onde ela afirma ter vindo."(STALLINGS, 2008, p. 8). A autenticação pode se dar por meios biométricos (impressão digital, padrão de retina, padrão de voz), objetos de identificação (cartão de identificação), conhecimentos do usuário (senhas, sistemas de desafio-resposta) ou até mesmo por um local específico de acesso. No decorrer deste trabalho, é abordado a técnica de autenticação através de Federação de Identidade.

Federação de Identidade

Uma federação de identidade é um serviço que oferece autenticação única (*Single Sign-On - SSO*), onde o usuário pode utilizar a identificação de um serviço em outros serviços, sem que disponibilize suas informações novamente em outros servidores. De acordo com Wangham et al. (2010, p. 5), “esta autenticação traz facilidades para os usuários, pois permite que esses passem pelo processo de autenticação uma única vez e usufruam das credenciais obtidas por todos os serviços que desejarem acessar”.

A autenticação federada consiste em permite ao usuário, ao solicitar *login* em um site, escolher um provedor de identidades que contenha seus dados. Após a autenticação do usuário, o provedor de identidade repassa o resultado dessa autenticação ao site e cria uma sessão de uso associada ao usuário.

Para Miorandi et al. (2012), identidades federadas são controladas por um grupo de organizações que colaboram com mecanismos de gestão e acesso a informações de identidade de uma determinada entidade no sistema e outros recursos através das fronteiras organizacionais, considerando usuários como entidades. O uso de identidades federadas para identificar instituições ou organizações tem sido instigado, promovendo grupos de federações. “Na literatura, constata-se um forte interesse na formação de federação de federações, chamada de confederação, para prover um gerenciamento de identidades federadas ainda mais globalizado.” (WANGHAM et al., 2010, p. 14).

2.2.2 Controle de acesso

O controle de acesso permite ao sistema definir direitos de acesso de acordo com cada indivíduo, bloqueando acessos não autorizados, garantindo que somente usuários permitidos e com determinados direitos de acesso façam uso de dados ou recursos. Anderson (2008) afirma que, o controle de acesso serve para controlar quem tem acesso (pessoas, processos, máquinas, ...) a quais recursos no sistema, quais arquivos eles podem ler, que programas eles podem executar, como eles compartilham dados com outros, e assim por diante. Neste trabalho são apresentadas as técnicas Controle de Acesso Baseado em Papéis, Controle de Acesso Baseado em Atributos e Modelo SecKit.

Controle de Acesso Baseado em Atributos (ABAC)

O Controle de Acesso Baseado em Atributos (do inglês *Attribute Based Access Control – ABAC*) é um mecanismo que identifica permissões, definindo políticas de controle de acesso com base em diferentes atributos do solicitante, meio ambiente, ou objeto de dados (HUR; NOH, 2011). O ABAC se baseia em características definidas como atributos de descrição ou de credenciamento. ABAC identifica os atributos e os usa para tomar uma decisão de autorização, por exemplo, se o usuário tem o atributo de *login*, o sistema de *login* irá liberá-lo para fazer login.

Yuan e Tong (2005) definem os atributos como atributo de sujeito, atributo de recursos e atributo de ambiente. O atributo de sujeito pertence a uma entidade, onde o atributo está associado à identidade ou a características do sujeito. O atributo de recurso pertence a um sujeito que disponibiliza um recurso. O atributo de ambiente está relacionado a características do ambiente ou contexto (por exemplo, data, hora, entre outros).

O ABAC proporciona uma flexibilidade que permite à uma grande variedade de usuários acesso a diversos objetos, sem a necessidade de especificar as relações entre cada usuário e cada objeto. O administrador ou proprietário cria as regras de controle de acesso, podendo modificar os atributos e seus valores ao longo do ciclo de vida dos usuários e objetos sem modificar a relação entre eles.

Controle de Acesso Baseado em Papéis (RBAC)

O Controle de Acesso Baseado em Papéis (do inglês *Role Based Access Control - RBAC*) é um modelo, proposto por David e Richard (1992), sendo aprimorado nos anos seguintes, foi concebido como forma de integrar os recursos que haviam em algumas aplicações específicas e consolidar um modelo de controle de acesso baseado em papéis de forma genérica.

O RBAC é um mecanismo que identifica permissões, utilizado principalmente para sistemas com vários usuários, associando direitos de usuários à papéis. Permissões são atribuídas conforme as funções desempenhadas pelo usuário dentro de uma instituição. A atribuição de permissão determinada pela função caracteriza um papel. Um usuário pode trocar de papel, bem como um papel pode ser atribuído a outro usuário, desta forma, mostrando uma maior

estabilidade no uso de papéis.

Quando um papel é criado e destinado a um usuário de acordo com suas funções e capacidades para realizar tarefas, é construído um controle de acesso não discricionário, que permite e promove a administração central de uma política de segurança específica pela instituição. As decisões de controle de acesso são freqüentemente baseadas nas funções que os usuários individuais assumem como parte de uma instituição (DAVID; RICHARD, 1992). Sandhu et al. (1996) afirmam que um papel pode representar competência para realizar tarefas específicas, atribuir autoridade e responsabilidade.

Modelo SecKit

O SecKit é um modelo que realiza técnicas de segurança, entre essas técnicas está o controle de acesso. Este modelo contém um conjunto de regras que devem ser configuradas, definindo o que é permitido dentro dessas regras. Da mesma forma, deve ser determinado quando as regras são dispensáveis. O administrador ou proprietário cria uma regra de controle de acesso para gerenciar conjunto de operações permitidas. Este modelo também pode oferecer serviços como autenticação, confidencialidade e integridade, por meio de regras definidas pelo usuário.

Para Neisse et al. (2014), SecKit integra abordagens para a política de refinamento, a tecnologia de aplicação de políticas em diferentes níveis de abstração, especificação de políticas baseadas em contexto, e gerenciamento de identidade com confiança de negociação. Segundo Neisse et al. (2015), SecKit foi desenvolvida com o objetivo final de dar ao usuário a possibilidade de conceber e aplicar um conjunto de políticas de segurança e privacidade completamente personalizadas, em outras palavras, é o usuário final que decide a troca desejável entre a divulgação de informações, privacidade e segurança.

2.2.3 Confidencialidade

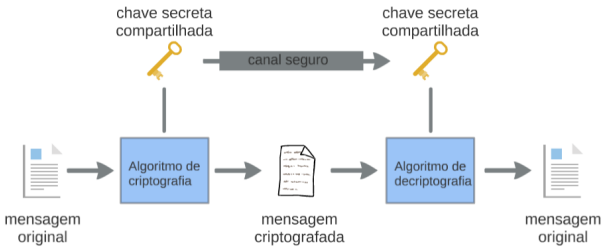
A confidencialidade, ou sigilo da informação, assegura a proteção dos dados contra ataques passivos (monitoramento de transmissões), protegendo um fluxo de mensagens ou uma mensagem completa ou partes específicas da mensagem. De acordo com Anderson (2008), a confidencialidade envolve a obrigação de proteger os informações de outra pessoa ou organização e o segredo se refere ao efeito dos mecanismos usados para limitar o acesso às informações.

As técnicas de confidencialidade devem garantir que os dados sejam protegidos. Entre essas técnicas, está o mecanismo de criptografia. A criptografia consiste em ocultar uma mensagem que é transmitida entre dois indivíduos, tornando-a ilegível através da criptografia da mensagem, somente sendo acessada por partes autorizadas por meio de uma chave. Há dois tipos de criptografias, a simétrica e a assimétrica, e ambas saão utilizadas neste trabalho.

2.2.3.1 Criptografia Simétrica

Na criptografia simétrica (ou criptografia de chave privada), a chave do remetente é igual a do destinatário, ou seja, a chave que é utilizada para criptografar é a mesma utilizada para decriptografar. Desta forma, as partes envolvidas compartilham um segredo de acesso, a chave secreta, conforme apresentado na Figura 1.

Figura 1 – Criptografia Simétrica.



Fonte: Elaborada pelo autor (2017).

Neste trabalho, é abordado a criptografia simétrica através do AES (Advanced Encryption Standard).

Advanced Encryption Standard (AES)

Advanced Encryption Standard (ou Padrão de Criptografia Avançada) ou Rijndael, proposto por Daemen e Rijmen (1999), é um algoritmo de chave simétrica que realiza cifragem em bloco. O tamanho do bloco é definido pelo tamanho de sua chave, trabalhando com chaves que podem ter tamanho de 128, 192 ou 256 bits.

O AES utiliza uma série de "rodadas"em que os bytes sofrem transformações não lineares para realizar a cifragem, porém essas transformações são reversíveis. Ou seja, a decifragem corresponde ao inverso das mesmas operações, assim, revertendo as transformações. Caso haja problemas de segurança, o número das "rodadas"de pode ser modificado como um parâmetro.

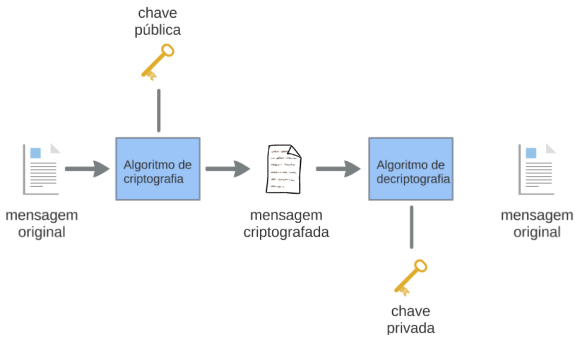
AES é considerado relativamente rápido quando comparado a outros algoritmos de criptografia simétrica, não exigindo muito poder de processamento. No entanto, ao realizar a inversão de uma "rodada", AES requer mais poder de processamento.

2.2.3.2 Criptografia Assimétrica

Na criptografia assimétrica (ou criptografia de chave pública), são utilizadas duas chaves, uma pública e uma privada. A chave pública serve para criptografar uma mensagem. Por outro lado, a chave privada serve para decriptografar a mesma mensagem, conforme apresentado na Figura 2. Vale ressaltar que, embora sejam diferentes, a chave pública e a privada estão conectadas matematicamente.

Neste trabalho, é abordado a criptografia assimétrica através da Criptografia de Curvas Elípticas e da Criptografia Baseada em Atributos.

Figura 2 – Criptografia Assimétrica.



Fonte: Elaborada pelo autor (2017).

Criptografia de Curvas Elípticas (ECC)

Proposto por Miller (1985), Criptografia de Curvas Elípticas (do inglês *Elliptic Curve Cryptography - ECC*) utiliza uma variação da criptografia assimétrica, baseada na matemática das curvas elípticas. ECC constrói protocolos de criptografia para troca de chaves usando o grupo de pontos de uma curva elíptica definida sobre um campo finito em vez do grupo multiplicativo de um campo finito.

ECC é um mecanismo de criptografia de chave pública. Cada participante na comunicação tem geralmente um par de chaves, uma chave pública e uma chave privada. As operações criptográficas estão associadas a essas chaves. Segundo Anoop (2007), alguns algoritmos de chave pública exigem que um conjunto de constantes predefinidas seja conhecido por todos os dispositivos que participam na comunicação, 'Parâmetros de domínio' no ECC é um exemplo de tais constantes.

ECC tem estabelecido como requisito mínimo de tamanho de chave 160 bits, o que correspondente a um bloco simétrico de 80 bits, trabalhando com curvas elípticas recomendadas de 5 tamanhos distintos de chave: 80, 112, 128, 192 e 256 bits.

Criptografia Baseada em Atributos (ABE)

Criptografia Baseada em Atributos (do inglês Attribute-Based Encryption - ABE) é um mecanismo de criptografia proposto por Sahai e Waters (2005) que utiliza atributos para descrever quais usuários são permitidos a decriptografar os dados, dessa forma, também exercendo uma técnica de controle de acesso. Os atributos são identificados como caracteristicas que descrevem o usuário.

Por exemplo, se uma clínica que realiza exames cardíacos envia os resultados dos exames de um paciente à um médico, os dados criptografados por ABE podem ter como atributos {"médico", "cardiologista", "hospital-x"}. Logo, somente um médico cardiologista pertencente ao hospital-x irá acessar os dados.

Segundo Bethencourt, Sahai e Waters (2007), a pessoa pode não saber a identidade

exata de todas as pessoas que devem ser capazes de acessar os dados, mas tem uma maneira de descrevê-los por meio de atributos descritivos ou credenciais. Ou seja, características como função desempenhada ou cargo dentro de uma empresa podem servir para se tornarem atributos.

Um protocolo de criptografia ABE contém quatro algoritmos, Configuração, Criptografar, Geração de Chave e Decriptografar. O algoritmo de Configuração define parâmetros para a execução da criptografia. O algoritmo Criptografar cifra uma mensagem juntamente com os atributos e parâmetros públicos. O algoritmo de Geração de Chave fornece uma chave privada. O algoritmo Decriptografar reconstrói a mensagem original.

Longo, Marcolla e Sala (2016) afirmam que há duas formas complementares de ABE que são hoje padrão: Criptografia Baseada em Atributos com Políticas nas Chaves Privadas (*Key-Policy Attribute-Based Encryption – KP-ABE*) proposta por Goyal et al. (2006); e Criptografia Baseada em Atributo com Políticas nos Textos Cifrados (*Ciphertext-Policy Attribute-Based Encryption – CP-ABE*) proposta por Bethencourt, Sahai e Waters (2007).

A criptografia CP-ABE, assim como a KP-ABE, executam quatro algoritmos, Configuração, Criptografar, Geração de Chave e Decriptografar. Ambas possuem um algoritmo chamado *Delegate*, no entanto, não é requisito obrigatório para o funcionamento das criptografias.

- Criptografia Baseada em Atributos com Políticas nas Chaves Privadas (KP-ABE)

  Em KP-ABE, cada texto cifrado possui atributos descritivos e cada chave privada possui uma estrutura de acesso que determina a qual texto cifrado é cedido o acesso. Ou seja, a estrutura de acesso é encontrada na chave privada e os atributos são encontrados nos textos cifrados, onde os atributos desempenham a função de rotular os textos cifrados.

  Uma característica de KP-ABE é não permitir que um segredo seja compartilhado, assim, garantindo que usuários não serão capazes de ter acesso à mensagem cifrada mesmo que colaborem para ter acesso ao segredo. Outra característica dessa criptografia é o mecanismo de delegação, conforme Goyal et al. (2006), isso permite que qualquer usuário que tenha uma chave para a estrutura de acesso x, poderá obter uma chave para estrutura de acesso y, se e somente se y for mais restritiva do que x.

- Criptografia Baseada em Atributo com Políticas nos Textos Cifrados (CP-ABE)

  Enquanto o trabalho de Goyal et al. (2006) propõe que a estrutura de acesso esteja na chave privada, o trabalho apresentado por Bethencourt, Sahai e Waters (2007) apresenta a estrutura de acesso no texto cifrado. As chaves privadas estão associadas aos atributos e não a estrutura de acesso.

  Bethencourt, Sahai e Waters (2007) descrevem que a chave privada do usuário é associada com um número arbitrário de atributos expressos como *strings*, quando uma mensagem é criptografada, uma estrutura de acesso é associada sobre os atributos.

Vale ressaltar que a principal diferença na execução do KP-ABE e do CP-ABE está nos algoritmos Criptografar e Geração de Chave. No esquema de KP-ABE, a estrutura de acesso está sendo integrada na Geração de Chave, no esquema CP-ABE a estrutura de acesso está no Criptografar.

2.2.4 Integridade de Dados

A integridade dos dados garante a proteção contra ataques ativos (alteração do fluxo de informações ou fluxo falso), garantindo que os dados que chegam ao destino são idênticos ao que saíram da origem. Podendo ou não ter serviços de recuperação de perda dos dados. Para Stallings (2008), a integridade de dados pode se aplicar a um fluxo de mensagens, uma única mensagem, ou campos selecionados dentro de uma mensagem, sendo a técnica mais útil e direta a proteção total do fluxo.

Verificação de Redundância Cíclica

A Verificação de Redundância Cíclica (do inglês Cyclic Redundancy Check - CRC) é um método de verificação de erros em dados que foram transmitidos ou para detectar alterações em dados de dispositivos de armazenamento. Segundo Sobolewski (2003), podem ser introduzidos erros durante a leitura, escrita ou transmissão real dos dados. Conseqüentemente, o controle de erros tornou-se parte integrante do projeto de computadores modernos e sistemas de comunicação.

Para uma verificação de redundância cíclica, um dispositivo de envio aplica um polinômio de 16 ou 32 bits a um bloco de dados a ser transmitido e acrescenta o código de redundância cíclica (CRC) resultante ao bloco. O dispositivo receptor aplica o mesmo polinômio aos dados e realiza uma comparação do seu resultado com o resultado anexado pelo remetente. Se o resultado coincidir, os dados foram recebidos com sucesso. No caso da verificação não coincidir, o remetente pode ser notificado para reenviar o bloco de dados.

Datagram Transport Layer Security

O Datagram Transport Layer Security (DTLS) é um protocolo de camada de sessão que permite que aplicativos baseados em datagramas se comuniquem de forma projetada para evitar espionagem ou alteração de mensagens. O aplicativo que utilizar DTLS não sofre com os atrasos associados aos protocolos de fluxo, mas tem de lidar com o reordenamento de pacotes, perda de datagramas e dados maiores do que o tamanho de um pacote de rede datagrama .

O DTLS é utilizado para proteger os canais de controle de transmissão para vários protocolos de transmissão (por exemplo, Protocolo de Controle de Congestionamento de Datagramas).

Da mesma forma, é adequado para proteger aplicações e serviços que são sensíveis ao atraso, tais como VOIP (voz sobre IP), VPN (rede particular virtual), videoconferência e aplicações como jogos online.

Segundo Rescorla e Modadugu (2012), a principal consideração de segurança adicional levantada pela DTLS é a de negação de serviço. DTLS inclui uma troca de *cookie* destinada a proteger contra a negação de serviço. No entanto, implementações que não usam essa troca de *cookie* ainda são vulneráveis.

2.3 Conclusão

Este capítulo apresentou conceitos sobre computação em nuvem, a qual vem ganhando destaque nos últimos anos principalmente por possuir benefícios como: a mobilidade de realizar tarefas, onde o usuário pode acessar de várias áreas geográficas com acesso a Internet; dispor de recursos que se ajustem a necessidade do usuário, pagando somente o que for utilizado, o que contribui para a redução de custo; e a facilidade de aumentar ou diminuir recursos sem que seja necessário processos demorados de atualização de componentes de máquinas físicas. Devido a esses benefícios e a facilidade de uso, a computação em nuvem se tornou um suporte para auxiliar na resolução de problemas encontrados em IoT, sendo citado por vários autores, logo, é fundamental que este assunto seja abordado neste trabalho.

É indispensável falar de segurança quanto tratamos sobre IoT, sendo esta uma das mais importantes questões a serem resolvidas para a implantação global da IoT. A falta de técnicas específicas para garantir a segurança e privacidade dos dispositivos e usuários ainda é notável na literatura. Desta forma, a maioria das técnicas de seguranças empregadas são variações de métodos tradicionais aplicados em redes de computadores, técnicas as quais algumas são apresentados neste trabalho.

3 INTERNET DAS COISAS

A Internet das Coisas, termo aderido do inglês Internet of Things (IoT), é uma arquitetura de Internet para dispositivos, consistindo na simplificação da troca de bens e serviços de distribuição global (WEBER, 2010). Ou seja, dispositivos podem se comunicar a outros dispositivos, podendo ou não haver intervenção humana, para solicitar e/ou oferecer serviços em qualquer parte do mundo.

Com IoT, o uso de dispositivos inteligentes torna a troca de bens e serviços mais ágil e eficiente. A computação em nuvem pode fornecer infraestrutura virtual para integrar dispositivos de monitoramento, dispositivos de armazenamento, ferramentas, plataformas de visualização e entrega de clientes (TIWARI; SINGH, 2017).

Este capítulo apresenta um estudo sobre IoT, detalhando características da IoT e abordando seus aspectos de segurança. Dessa forma, está dividido em quatro seções. A primeira seção apresenta os cenários, aplicações e desafios. A seção seguinte apresenta três arquiteturas da IoT. A seção 3 apresenta técnicas de segurança utilizadas em IoT. A última seção aborda a segurança nas arquiteturas descritas.

3.1 Cenário, Aplicações e Desafios

A IoT possibilita que o ambiente possa se comunicar por meio de mecanismos como o uso de sensores, cartões inteligentes e etiquetas de Identificação de Rádio Frequência (RFID - Radio Frequency Identification). Isto é, dispositivos inteligentes podem capturar ou produzir informações sobre um determinado ambiente. Dentre deste contexto, são apresentados a seguir os cenários, as aplicações e os desafios atuais da IoT.

3.1.1 Cenário

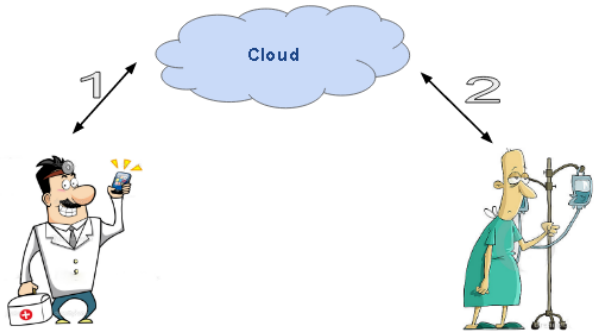
A IoT proporciona variados cenários de atuação, seja de dispositivos para dispositivos ou dispositivos para aplicação. Por exemplo, a utilização de sensores para regular temperaturas de ambientes, veículos inteligentes que reconhecem seus condutores, dispositivos médicos que enviam prontuários do paciente em tempo real, entre outros cenários.

Em um cenário geral da IoT, é possível encontrar os seguintes componentes: um dispositivo inteligente capaz de exercer tarefas, com ou sem intervenção humana, e utiliza mecanismos de comunicação para solicitar e/ou fornecer informações; usuários e/ou serviços que utilizem as informações produzidas por dispositivos inteligente; e recursos de rede para transmitir as informações. Nesse cenário geral, esses componentes podem se relacionam da seguinte forma: um dispositivo inteligente fornece informações a um serviço em nuvem; usuários podem solicitar informações do dispositivo ao serviço em nuvem; o dispositivo também pode solicitar ao serviço

em nuvem as informações dos usuários; todas as trocas de informações fazem uso de recursos de rede.

A visão geral pode ser aplicada em um cenário mais específico. Por exemplo, é adotado um cenário de um hospital, no qual um médico deseja obter as informações atualizadas sobre o monitoramento de um paciente de qualquer lugar que ele esteja. O médico utiliza uma aplicação *App* que realiza atualizações sobre o estado do paciente por meio de um serviço em nuvem *cloud*(1). O serviço *cloud* obtém as informações para o *App* a partir do dispositivo *device* que fica monitorando o paciente(2). Este cenário é ilustrado na Figura 3, abaixo:

Figura 3 – Cenário de Internet das Coisas.



Fonte: Elaborada pelo autor (2017).

Devido a grande troca de informações, muitos dados são gerados nos cenários da IoT. A fim de simplificar, os dados podem ser classificados por dados gerados por ambiente/sistema e dados gerados por humanos. Por um lado, os dados provenientes do ambiente são produzidos por meio de dispositivos capazes de capturar informações do meio em que se situam. Por exemplo, o uso de dispositivos com sensores para detectar temperatura, luminosidade, umidade, entre outros, ou são produzidos automaticamente como dados do sistema. Por outro lado, os dados provenientes de humanos correspondem a informações que o próprio usuário fornece, como nome, localização, comentários e outros que necessitam da interação do usuário para serem produzidos. Esses dois tipos de dados interagem entre si para satisfazer as necessidades de aplicações dos usuários.

3.1.2 Aplicações

Diferentes setores estão aderindo a IoT e desenvolvendo aplicações adaptadas a essa nova tecnologia. Segundo Gubbi et al. (2013), para a IoT emergir com sucesso, o paradigma de computação precisa evoluir para conectar objetos cotidianos existentes e incorporar a inteligência em nosso ambiente. Atualmente, algumas aplicações IoT são apresentadas com termos baseados em seus cenários de atuação, por exemplo, *e-Health*, *Smart Home*, *Smart City* e *Smart Cars*.

O *E-Health* é definido como prática de cuidados de saúde suportados por dispositivos eletrônicos e de comunicação (BORIC-LUBECKE et al., 2014). Ou seja, ele envolve o uso

de tecnologias para prestação de cuidados de saúde, oferecendo suporte para tarefas como arquivamento de imagens e sistemas de comunicação, registros eletrônicos de saúde e até mesmo telemedicina. Nesse contexto, é encontrado o termo *Healthcare IoT*, que propõe o cuidado de pacientes por meio de dispositivos inteligentes.

A *Smart Home* (ou *Home Automation*) é caracterizado por Kurkinen (2016) como soluções para o controle, monitoramento e automação de funções no lar, requerendo um aplicativo de *smartphone* ou *web* como uma interface para o usuário. Por exemplo, o uso de sensores para regular a temperatura do ambiente, podendo ser ajustada pelo usuário por meio de uma aplicação, de qualquer local, desde que esteja conectado a Internet.

A *Smart City* estende a Internet para o mundo físico de uma cidade, por meio da implantação generalizada de dispositivos com sensores conectados a Internet, espacialmente distribuídos, permitindo melhorar a eficiência dos serviços da cidade (LANZA et al., 2015). O uso de dispositivos IoT pode economizar dinheiro e energia das cidades, e promover uma melhor comunicação entre os moradores e a cidade. O termo *Smart City* abrange tecnologias para se conectar com os moradores com a cidade ou tecnologias para melhorar a infraestrutura da cidade.

O *Smart Cars* aborda a inserção de dispositivos inteligentes em veículos para otimizar ou automatizar tarefas, e proporcionar maior segurança. Atualmente os carros são compostos por dispositivos inteligentes, tais como assistência inteligente ao condutor, comunicação de veículo para veículo (V2V), condução automatizada, entre outros (HUMAYED; LUO, 2015). Cada vez mais perceptíveis ao ambiente em que estão situados, os carros podem identificar a pessoa que está dirigindo ou até mesmo outros carros. Esses veículos são conectados a Internet sendo capaz de solicitar, caso necessário, serviços para problemas mecânicos ou assistência médica.

3.1.3 Desafios

A IoT traz uma grande inovação no modo de troca de bens e serviços, sendo capaz de integrar o ambiente físico ao digital através de mecanismos de comunicação como sensores, cartões inteligentes, etiqueta RFID, entre outros. No entanto, a implantação da IoT ainda enfrenta dificuldades a serem superadas. Dentre esses desafios, é dado destaque à heterogeneidade, escalabilidade, interoperabilidade e segurança e privacidade.

A heterogeneidade é uma particularidade da IoT que provém da diversidade de objetos inteligentes que fazem parte dela (por exemplo, carros, relógios, refrigeradores, e diversos outros objetos) que recorrem a interação com a Internet para fornecer ou utilizar informação objetivando satisfazer seus serviços. Os objetos da IoT podem variar quanto ao mecanismo de comunicação, e também divergem na forma de acesso à internet, seja por *Wifi*, *3g* ou *Bluetooth*. Essas variações exigem uma forma de padronização dos dispositivos ou a integração dos dados gerados.

A escalabilidade em IoT é devido ao rápido crescimento de dispositivos miniaturizados (sensores, cartões inteligentes, etc.). Assim como o número de dispositivos é crescente, os dados

produzidos por estes dispositivos crescer sem barreiras (SARKAR et al., 2014). O aumento do número de dispositivos, que consequentemente geram uma grande quantidade de dados, requer uma infraestrutura adequada para gerenciamento de informações capaz de suprir a necessidade de troca de informações a alcance global. O problema de escalabilidade deve ser resolvido para garantir que os recursos sejam distribuídos de forma eficiente.

A interoperabilidade aborda a necessidade dos dados adquirirem parâmetros adequados para trabalhar em conjunto e serem integrados para cumprir o solicitado por uma aplicação que nem sempre é a mesma de origem dos dados.

A segurança e privacidade em IoT devem ser garantidas aos seus utilizados por meio de técnicas de autenticação, confidencialidade de dados, integridade dos dados e níveis de anonimato (SICARI et al., 2014). Aplicações como *e-Health*, *Smart Home*, *Smart City*, *Smart Cars*, entre tantas outras, possuem um grande número de vetores de ataques disponíveis, podendo pôr em risco não somente a privacidade do usuário, mas comprometer sua integridade física. Por exemplo, um veículo com sistema inteligente, ao sofrer uma ataque, pode provocar um acidente. A seção seguinte apresenta mais detalhes sobre este desafio, apresentando as técnicas adotadas.

3.2 Segurança em Internet das Coisas

Uma grande rede de dispositivos interconectados irá representar novas ameaças de segurança e privacidade, e colocar esses dispositivos ao risco de *hackers* através de brechas de segurança para fazer os dispositivos trabalharem para seus benefícios pessoais (FAROOQ et al., 2015). Desta forma, são levantadas questões quanto à confiabilidade, segurança e privacidade dos dispositivos e usuários em IoT.

Os dispositivos ou "coisas" podem variar quanto às técnicas empregadas para proporcionar segurança em IoT. Sendo assim, a seguir é apresentado um estudo sobre segurança em IoT, abordando as técnicas de autenticação, controle de acesso, confidencialidade e integridade.

Autenticação em IoT

De acordo com Sicari et al. (2014), a autenticação em IoT representa a necessidade de identificar o usuário ou dispositivo que está permitido a acessar os dados por meio de algum mecanismo (mais ou menos robustos). Devido a crescente quantidade e heterogeneidade de usuários e dispositivos na IoT, é preciso controlar os dados, identificando se um determinado dado é proveniente da origem esperada, por meio da identificação do usuário ou dispositivo. Segundo Wangham, Domenech e Mello (2013) "na literatura, a autenticação em IoT deve ser tratada de forma diferente para usuários e para dispositivos".

A autenticação de dispositivos pode ser realizada de dispositivo para dispositivo ou dispositivo para aplicação. Mahalle et al. (2012) propõem uma autenticação de dispositivos para dispositivo que estejam em um mesmo domínio. A autenticação ocorre por meio de um protocolo

de desafio resposta. Cada dispositivo recebe uma chave em uma central de distribuição de chaves confiável.

A autenticação de dispositivos para aplicação pode ser realizada por identificadores integrados nos dispositivos. Segundo Miorandi et al. (2012), a solução mais adotada é o Código Eletrônico de Produto (EPC). Os identificadores EPC seriam distribuídos na Internet por uma autoridade chamada *Object Naming Service* (ONS) que seria encarregada de controlar as informações de cada código eletrônico e os distribuidores dos códigos (WEBER, 2010).

Wangham, Domenech e Mello (2013) e Domenech, Carvalho e Wangham (2015) apresentam como mais adequado para autenticação de usuários em IoT o uso de Federação de Identidades (ver seção 2.2.1).

Domenech, Boukerche e Wangham (2016) propõem uma infraestrutura que suporta autenticação de dispositivos e de usuários. A infraestrutura é composta por um sistema de gestão de identidades que é baseado em uma solução para identidade federadas, fornecendo *login* federado único para usuários e dispositivos que enfrentam diferentes mecanismos de autenticação dentro de uma infraestrutura integrada.

Deve-se ressaltar que devido ao baixo poder de processamento computacional presente em grande parte dos dispositivos IoT, a autenticação por meio de mecanismos de segurança mais robustos, como o uso de certificado digital, não é muito recomendado.

Controle de Acesso em IoT

Após um usuário ou dispositivo autenticado, o controle de acesso deve definir quais recursos que estão disponíveis através do mecanismo de autorização, consultando quais permissões o sujeito está encarregado. Para Wangham, Domenech e Mello (2013), os mecanismos de controle de acesso para autorização utilizados em IoT são modelos já conhecidos e empregados na Internet clássica. Atualmente, há mecanismos de autorização que utilizam modelos clássicos e novos modelos para IoT.

Oh e Kim (2014) propõem um mecanismo de controle de permissão de acesso que considera as características de *Web* para arquiteturas baseadas em recursos. Para aliviar a sobrecargar de solicitação de um objeto, é adicionado uma classificação adicional para grupos associado ao modelo de Controle de Acesso Baseado em Papéis - RBAC (ver seção 2.2.2). Esse modelo permite a atribuição de papéis e funções aos usuários, embora a utilização implique em atribuições estáticas, ou seja, não há prática de trocar grupos, atributos ou nível de confiança do sujeito. A dinamicidade dos usuários e dispositivos pode ser um obstáculo para o uso deste modelo na IoT.

Outra solução proposta para controle de acesso em IoT é o modelo SecKit (ver seção 2.2.1). Seckit é uma ferramenta de segurança baseada em modelos apresentada por Neisse et al. (2014). Nesta ferramenta deve ser especificado um conjunto de regras de política de au-

torização e obrigação. O conjunto de regras deve ser configurado definido quais são as regras, quando se aplicam e quando são dispensáveis. A utilização de SecKit leva em consideração a heterogeneidade da IoT, tecnologias, o grande número de dispositivos e sistemas e os diferentes tipos de usuários e papéis. SecKit demonstra flexibilidade e eficiência para suportar a especificação e avaliação das políticas de segurança especificadas usando modelos de regras (NEISSE et al., 2015). Os autores afirmam que mecanismos de controle de acesso clássicos como Modelo Baseado em Atributos - ABAC ou Modelo Baseado em Papéis - RBAC (ver seção 2.2.1) geralmente não são escaláveis para IoT;

Domenech, Carvalho e Wangham (2015) propõem um mecanismo de autorização flexível desenvolvido em XACML, que é uma linguagem de política de autorização baseada em XML. O mecanismo permite que o dispositivo solicite autorização a uma entidade AAI (Infraestrutura de Autenticação e Autorização) uma permissão para utilização de recursos. Fica a cargo da AAI decidir a autorização, o dispositivo somente realiza a decisão tomada.

Segundo Miorandi et al. (2012), a fim de evitar o acesso não autorizado, principalmente considerando o grande número de dispositivos que fazem uso de comunicações sem fio em IoT, os mecanismos de controle de acesso devem ser combinados com outras técnicas de proteção de dados.

Confidencialidade em IoT

De acordo com Miorandi et al. (2012), a confidencialidade de dados representa uma questão fundamental em cenários da IoT, permitindo somente a usuários ou objetos autorizados acessar e modificar dados. A confidencialidade deve ser capaz de garantir a privacidade das informações do usuário por meio de diferentes mecanismos. Para Farooq et al. (2015), embora a confidencialidade dos dados não se limite a criptografia, criptografar os dados, convertendo dados em forma de texto cifrado, torna difícil o acesso à usuários não autorizados. Atualmente são utilizados algoritmos de criptografia simétrica e assimétrica (ver seção 2.2.3) para garantir a confidencialidade dos dados em IoT.

Segundo Miorandi et al. (2012), as soluções clássicas para assegurar a confidencialidade dos dados não podem ser diretamente aplicadas a contextos da IoT. Isso se deve a crescente quantidade de dados gerando problemas de escalabilidade e a necessidade de controlar o acesso aos dados com mudanças em tempo de execução e fluxos de dados dinâmicos.

Kulkarni e Dixit (2014) propõem como solução um sistema que criptografa e decriptografa os dados utilizando a técnica ABE para registros pessoais de saúde, utilizando uma plataforma *e-Health* em nuvem para armazenar grandes volumes de dados. A privacidade do paciente é mantido com a ajuda de várias autoridades ABE (ver seção 2.2.3). O sistema funciona em cenários com múltiplos dados, dividindo os usuários em vários domínios de segurança que reduz muito a complexidade de gerenciamento de chaves para os proprietários e usuários. Os pacientes podem permitir o acesso para utilizadores privados, mas não é acessível para usuários

públicos.

Outra solução é apresentada por Yao, Chen e Tian (2015), que propõem um esquema que utiliza ABE baseado em Criptografia de Curvas Elípticas (ECC), considerando as vantagens de ECC combinado com a sintaxe de KP-ABE (ver seção 2.2.3), apresentando baixa sobrecarga de comunicação e baixa sobrecarga computacional. Neste esquema é considerado uma autoridade atributo central (responsável pela geração de chaves para atributos) e os usuários, sendo a mensagem criptografada por um algoritmo de segurança criptográfica simétrica. A chave de criptografia é derivado a partir de um número aleatório pela Criptografia de Curva Elíptica, podendo ser reconstituídas sob o conjunto de atributos.

Hossain e Muhammad (2016) propõem a utilização de uma criptografia com chaves secretas e chaves privadas em um sistema de monitoramento de saúde, buscando a preservação de privacidade durante coleta de dados e transmissão segura em uma arquitetura de redes móveis de saúde. A transmissão segura é obtida usando criptografia baseada em atributos, onde apenas usuários autorizados acessam os dados. Esses métodos geralmente valem a pena, no entanto, o principal problema é complexidade computacional alta.

Deve-se ressaltar que durante o estudo ficou evidente que muitos trabalhos desenvolvidos nos últimos anos apresentam esquemas que utilizem ABE em sua estrutura ou promovam o uso de ABE para prover confidencialidade em IoT. Ambrosin et al. (2016) mostram a viabilidade de adotar ABE em sistemas IoT, sugerindo que novas soluções de segurança baseadas em ABE sejam desenvolvidas, focando em melhorar a eficiência de ABE.

Integridade em IoT

De acordo com Stallings (2008, p. 9), integridade "é a garantia de que os dados recebidos estão exatamente como foram enviados por uma entidade autorizada (ou seja, não contém modificação, inserção, exclusão ou repetição)". Os dados trocados entre o usuário e IoT devem ser protegidos, pois, se a integridade dos dados for comprometida, a operação normal do sistema é interrompida e pode resultar em danos tanto financeiros quanto pessoal para o utilizador (ATAMLI; MARTIN, 2014).

Farooq et al. (2015) afirmam que para a integridade dos dados os mecanismos necessitam garantir a precisão e originalidade de dados, incluindo métodos como a soma de verificação e verificação de redundância cíclica - CRC (ver seção 2.2.4), que é um mecanismo de detecção de erro simples para parte dos dados.

3.3 Arquiteturas para Internet das Coisas

Com a advento da IoT, o grande fluxo de informações exigiu uma infraestrutura capaz de gerenciá-las. Logo foram surgindo propostas de arquiteturas para IoT, exercendo um tratamento sobre os dados provenientes de ambientes IoT. Atualmente há diversas arquiteturas IoT que

buscam formas de tratar as informações que trafegam entre dispositivos e aplicações. Segundo Botta et al. (2014), uma série de soluções recentemente propostas sugerem a utilização de arquiteturas em nuvem para permitir a descoberta, conexão e integração de sensores e atuadores, criando plataformas para aplicações de conectividade em tempo real e onipresente para cidades inteligentes.

3.3.1 Descrição das Arquiteturas

Considerando a importância das arquiteturas em IoT, são descritas a seguir três arquiteturas julgadas relevantes na literatura da IoT.

Arquitetura com Sistema de Segurança e Qualidade

A Arquitetura com Sistema de Segurança e Qualidade de Sicari et al. (2014) propõe a captura dos dados provenientes do ambiente e/ou contexto (dados gerados pelo sistema) por meio de uma interface distribuída onde cada nó é chamado de e-node. Os dados trabalhados nos e-nodes podem ser diversificados, sendo assim, esta arquitetura leva em consideração a heterogeneidade na IoT.

A Figura 4 apresenta o funcionamento da arquitetura de Sicari et al. (2014) em uma cidade com diversos dispositivos. Cada dispositivo funciona como um nó e cada nó é uma estrutura dividida em três camadas com funções específicas. As camadas são denominadas de análise, anotação de dados e integração.

Figura 4 – Sistema de Arquitetura de Segurança e Qualidade.

Fonte: Adaptada de SICARI et al., 2014, p. 6.

A camada de análise objetiva extrair informações necessárias para a camada seguinte, retirando informações como: fonte dos dados para identificar se são dados do sistema ou dados humanos; modo de comunicação para identificar como os dados são recolhidos; esquema dos dados (tipo, formato, atributos); metadados de segurança; e metadados de qualidade. Essa camada tem como vantagem analisar profundamente a qualidade dos dados levando em consideração a

reputação de origem pela soma de dois fatores, o conteúdo e o proprietário. A desvantagem é não ter uma garantia de que a reputação provém de uma fonte confiável.

Após os dados serem analisados, as informações extraídas são descritas com precisão. A camada de anotação tem como objetivo produzir um novo conjunto de metadados contendo descrição da fonte dos dados, do tipo dos dados, do conteúdo, dos metadados de segurança (valores associados à autenticação, confidencialidade, integridade e privacidade) e dos metadados de qualidade (valores associados à oportunidade, perfeição, exatidão e reputação). Os dados de saída dessa camada são as anotações dos metadados apropriados. A vantagem dessa camada é ter a capacidade de tratar a heterogeneidade dos dados. A desvantagem decorre de uma grande quantidade de dados que são produzidos.

A camada de integração faz uso das anotações da camada anterior, objetivando atender as necessidades da aplicação. Algumas solicitações de usuário requerem uso de informações provenientes de diferentes tecnologias, sendo necessário mesclar ou combinar dados. A vantagem dessa camada é poder selecionar fontes de dados (caso haja mais de uma alternativa de fonte) para integrar, considerando os melhores níveis de segurança e qualidade de dados. A integração de várias fontes pode ser desvantajoso logo que, quanto maior a quantidade de fontes a serem integradas, mais complexo será.

Arquitetura Distribuível e Escalável (DIAT)

A Arquitetura Distribuível e Escalável - DIAT (do inglês *Distributed Internet-like Architecture for Things*) de Sarkar et al. (2015), segue uma estrutura em camadas semelhantes a uma arquitetura orientada a serviços. Ela funciona com o mínimo de intervenção humana possível, para isso, os serviços são tratados de forma homogênea.

Antes dos serviços serem criados e gerenciados, eles devem ser analisados. A arquitetura de DIAT apresenta três camadas: Camada de Objeto Virtual; Camada de Composição de Objetos Virtuais; e Camada de Serviço. As três camadas da arquitetura DIAT são colocadas em uma pilha chamada IoT Daemon, juntamente as camadas é executada as políticas de segurança e privacidade pelo Gerenciamento de Segurança. Representação da arquitetura na Figura 5.

Figura 5 – Arquitetura DIAT.

Fonte: Adaptada de SARKAR et al., 2015, p.3.

A Camada de Objeto Virtual (*Virtual ObjectLayer* - VOL) é objetiva virtualizar objetos físicos e entidades, sendo capaz de representar os objetos físicos, descrevendo suas capacidades e características em uma forma virtual chamada Objeto Virtual (Virtual Object - VO). A vantagem dessa camada é combater a heterogeneidade entre os dispositivos, sistemas e redes através da abstração de objetos físicos, assim garantindo a interoperabilidade e reutilização de objetos.

Algumas tarefas necessitam da interação de diferentes objetos para cumprir metas. A Composição de Objetos Virtuais (*Composite Virtual Object* - CVO) tem como objetivo coordenar e otimizar operações entre entidade e por realizar interação entre VOs, uma CVO é formada por um ou vários VOs, ou por outras CVOs, dependendo da necessidade da tarefa a ser executada. A Camada de Composição de Objetos Virtuais (Composite Virtual ObjectLayer - CVOL) tem como vantagem forma uma CVO identificando qual o conjunto de VOs (e/ou outra CVO) mais adequado para realizar determinada tarefa.

O objetivo da Camada de Serviço (*Service Layer* - SL) é criar e gerenciar os serviços, podendo iniciar solicitações de serviços e tratar as solicitações de usuários dividindo-as em subtarefas menores. Posteriormente esta camada decide quais subtarefas são necessárias para atender um propósito.

A arquitetura DIAT propõe uma camada transversal de Gerenciamento de Segurança (Security Management - SM) com controle de uso que suporta autorização baseado em eventos e obrigações. O principal objetivo do SM é controlar o uso de dados, recursos e serviços dos objetos da IoT.

Todas as funcionalidades das camadas e do SM são referidas como uma IoT Daemon. Cada objeto com poder de processamento e memória gera seu próprio IoT Daemon. Em caso de dispositivos embarcados que não possuem capacidade para suportar uma IoT Daemon completa, é executado uma IoT Daemon com conjuntos limitados de funções.

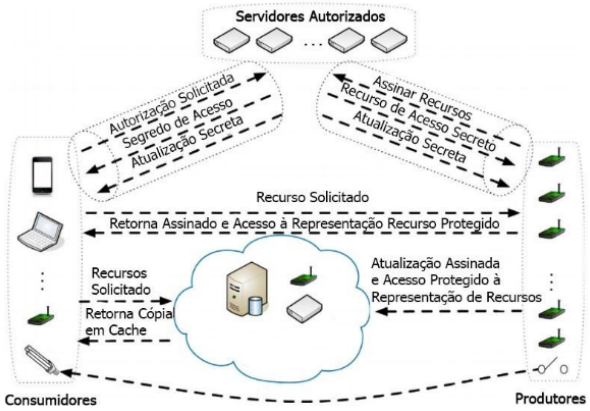
Arquitetura de Segurança de Objetos (OSCAR)

A Arquitetura de Segurança de Objetos (do inglês *Object Security Architecture* - OSCAR) é uma arquitetura proposta por Vučinić et al. (2014), baseada em uma arquitetura de segurança produtor-consumidor. O principal objetivo dessa arquitetura é minimizar o número de *frames*/pacotes enviados ou recebidos para diminuir o consumo de energia, para tal, faz uso de chaves públicas criptografadas. Seus principais componentes são:

- Os Produtores capazes de fornecer dados em forma de recursos assinados e criptografados;
- Os Consumidores que solicitam recursos;
- Os Servidores de Autorização que armazenam os certificados de produtores recebem assinaturas de produtores de recursos gerados e disponibilizam segredos de acesso;
- Os Servidores Proxy que oferecem serviço de *cache* entre Produtores e Consumidores.

A Figura 6 apresenta os componentes da arquitetura OSCAR.

Figura 6 – Componentes da arquitetura OSCAR.

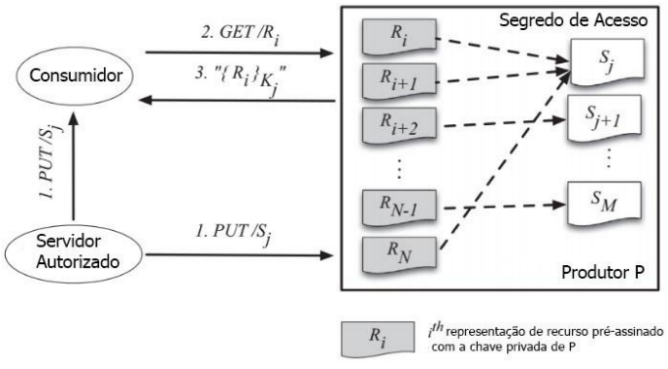


Fonte: Adaptado de VUCINIC et al., 2014, p. 6.

Para o funcionamento seguro da arquitetura OSCAR, Vučinić et al. (2014) assumiram que devem ser emitidos certificados válidos para os Produtores e Consumidores por meio de uma Autoridade Certificadora. Um Produtor poderá usar sua chave pública para assinar seus recursos, assim como os recursos comuns podem ter seus identificadores públicos compartilhados.

A Figura 7 apresenta os princípios de acesso a recursos da arquitetura OSCAR por meio da visão do Produtor P. Onde P gerencia um conjunto de recursos identificado por R_i e um conjunto de segredos de acesso identificado por S_j obtido de um Servidor de Autorização. O segredo de acesso S_j define um conjunto de direitos de acesso que possibilita diferentes níveis de autorização.

Figura 7 – Representação dos recursos de acesso do Produtor



Fonte: Adaptado de VUCINIC et al., 2014, p. 6.

3.4 A Segurança nas Arquiteturas

As arquiteturas descritas na seção anterior apresentam técnicas para prover segurança e privacidade em IoT. Desta forma, está seção apresenta a seguir os aspectos de segurança das

arquiteturas estudadas.

Arquitetura com Sistema de Segurança e Qualidade

Segundo Sicari et al. (2014), na fase de análise, os dados são analisados para suportar as fases seguintes. A Arquitetura com Sistema de Segurança e Qualidade encarrega de extrair os metadados de segurança na Camada de Análise, descrevendo na Camada de Anotação os esquemas de segurança encontrados e utilizando-os na Camada de Integração, caso seja solicitado pela aplicação.

Sicari et al. (2014) afirmam que a definição de um mecanismo de controle de acesso e a definição de um processo de autenticação de objeto devem ser fatores abordados na IoT. Entretanto, os dados de autenticação e autorização dos dispositivos encontrados na camada de análise somente são utilizados na camada de integração. A arquitetura de Sicari et al. (2014) não oferece um controle de acesso prévio para realizar a manipulação dos dados.

Os metadados sobre confidencialidade também são extraídos na camada de análise, sendo avaliados por meio de pontuação conforme a robustez da técnica de criptografia encontrada e do esquema de distribuição de chaves que foi utilizado.

Quanto a integridade dos dados na arquitetura, ela é atribuída por um sistema de pontuação. Cada pontuação é calculada dependendo do tipo de dados e do modo de comunicação. A adoção de pontuação para requisitos de segurança não permite ao sistema identificar com precisão os pontos fracos e pontos fortes das diferentes fontes de dados de entrada (SICARI et al., 2014).

Arquitetura DIAT

Sarkar et al. (2015) desenvolveram uma linguagem para controle de uso que suporta autorização baseada em eventos e obrigações utilizando operadores temporais. O controle de uso executa a política de segurança em todas as camadas.

O sistema de gerenciamento de segurança da arquitetura DIAT faz uma modelagem para relação de confiança e risco utilizando o modelo SecKit (NEISSE et al., 2014) (ver seção 2.2.2) para definir regras. O SecKit é formado pelo Gerenciamento de Política (PM), Repositório de Política (PR) e Ponto de Política de Decisão (PDP). O PM é responsável por recuperar as regras de política de segurança armazenados no PR e implantá-los no PDP. Por sua vez, o PDP convoca as regras de política e assina os eventos nos Pontos de Política de Aplicação (PEPs) implantados em diferentes camadas da arquitetura DIAT (SARKAR et al., 2015).

Sarkar et al. (2015) utilizam políticas de segurança para garantir o anonimato de dados, autorização, proteção de dados, consentimento, integridade, não-repúdio e confiança para atender as necessidades de um sistema da IoT. Para a definição de regras de políticas, são combinados algoritmos que podem ser configurados para decidir as prioridades.

Arquitetura OSCAR

A arquitetura OSCAR (VUČINIĆ et al., 2014) utiliza canais autenticados pelo protocolo *Datagram Transport Layer Security* - DTLS (ver seção 2.2.4. Para garantir a autenticidade e integridade dos recursos, a arquitetura aproveita as assinaturas digitais.

O produtor gerencia um conjunto de recursos e segredos de acesso por meio de um servidor de autorização, definindo um grupo de direitos de acesso que permitem diferentes níveis de autorização.

Em nível de confidencialidade, o produtor disponibiliza os recursos assinados e criptografados. É gerada uma chave de criptografia simétrica 2.2.3) para criptografar uma representação do recurso. Somente o consumidor que tem direito de acesso pode decriptografar.

Quadro comparativo

A partir do estudo dos aspectos de segurança das arquiteturas apresentadas, no Quadro 1 abaixo, é retratado um breve comparativo entre as arquiteturas e suas técnicas de segurança. Para tal, foi adotado as técnicas de segurança de autenticação, controle de acesso, confidencialidade e integridade como parâmetros de comparação.

Quadro 1 – Comparação entre as arquiteturas

	Arquitetura com Sistema de Segurança e Qualidade	Arquitetura Distribuível e Escalável (DIAT)	Arquitetura de Segurança de Objetos (OSCAR)
Autenticação	Utiliza os dados de autenticação que são extraídos dos metadados.	Utiliza o modelo SecKit para autenticação.	Utiliza certificados digitais.
Controle de Acesso	Utiliza os dados de autorização que são extraídos dos metadados.	Utiliza o modelo SecKit para controle de acesso.	Utiliza segredos de acesso de um servidor de autorização.
Confidencialidade	Utiliza pontuação pela robustez da técnica de criptografia e do esquema de distribuição de chaves.	Utiliza o modelo SecKit para proteção dos dados.	Utiliza chave privada e criptografia dos recursos.
Integridade dos Dados	Utiliza pontuação com base em algoritmos que dependem do tipo de dados e do modo de comunicação.	Utiliza o modelo SecKit para integridade dos dados.	Não apresenta.

3.5 Conclusão

Neste capítulo foram apresentados aspectos da IoT, levando em consideração as principais caracteristicas, como cenários, aplicações e desafios. Também foi abordado sobre as medidas de segurança atualmente adotadas para prover privacidade e segurança dos dispositivos e usuários IoT. Para tal, foi realizado um estudo sobre as técnicas de autenticação, controle de acesso, confidencialidade e integridade. Outro aspecto importante da IoT apresentado é o funcionamento de três arquitetura e como as técnicas de segurança abordadas atuam sobre elas.

A segurança em IoT tem sido o foco de muitas pesquisas durantes os últimos anos. A busca por soluções para garantir a segurança e privacidade de dispositivos e usuários IoT tem gerado grandes discussões para pôr em prática um modelo que possa se enquadrar em diferentes cenários, a fim de implantar IoT de forma global.

4 UM ESQUEMA PARA DISTRIBUIÇÃO DE CHAVES EM AMBIENTES IOT

Como apresentado no Capítulo 3, os dispositivos no ambiente da IoT realizam comunicação entre si ou com seus usuários (por exemplo, aplicações de rastreamento de automóveis). Isso ocorre através de uma rede local que interliga esses dispositivos ou através da Internet. Essa comunicação, em princípio, é realizada sem nenhum tratamento relativo ao sigilo da informação. Dessa forma, os dados que trafegam nesse ambiente podem ser facilmente obtidos ou modificados por terceiros não autorizados. Em um ambiente hospitalar, por exemplo, onde é realizada a coleta de dados dos pacientes por dispositivos IoT, um agente malicioso poderia facilmente ter acesso a rede dos dispositivos e obter informações sigilosas sobre os pacientes.

De forma a tratar o problema do sigilo no ambiente IoT, este capítulo apresenta um esquema teórico que emprega ABE para distribuir chaves e assim obter sigilo no ambiente IoT. O capítulo está organizado da seguinte forma: na seção 4.1 é apresentada uma ideia geral do esquema proposto; em seguida, a Seção 4.2 apresenta um conjunto de requisitos necessários ao esquema; após, na Seção 4.3 são apresentadas as entidades participantes; a Seção 4.4 introduz as premissas do esquema; na Seção 4.5, é apresentado a descrição do esquema; a Seção 4.6 aborda uma breve discussão sobre a segurança do esquema; por último, na Seção 4.7, é apresentado o emprego do esquema em uma arquitetura IoT.

4.1 Visão Geral

O esquema proposto considera que dispositivos IoT precisam se comunicar, enviando dados de forma segura e sigilosa. Para tal, os dados devem ser criptografados na origem antes de serem enviados ao destino. Assim, cada dispositivo que participa da comunicação deverá possuir uma chave para acessar os dados criptografados. Essas chaves devem ser provenientes de uma fonte confiável e que reconhece os dispositivos participantes.

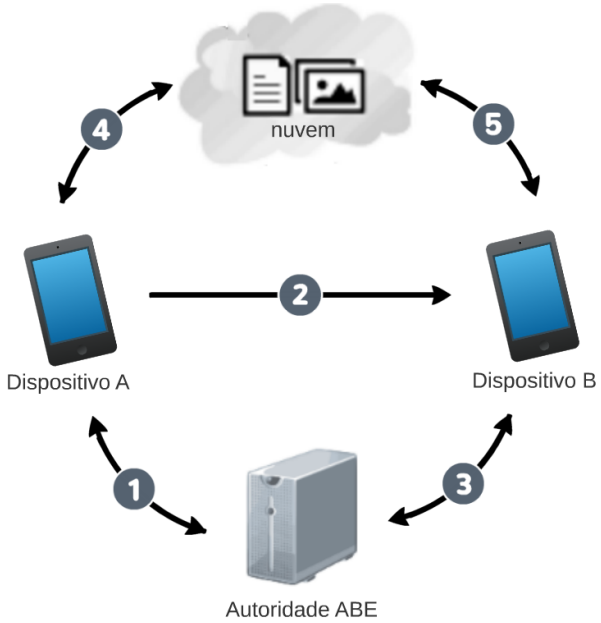
As entidades que participam do esquema são uma autoridade ABE e os dispositivos da reda IoT. A autoridade ABE é encarregada por gerar pares de chaves ABE para os dispositivos que irão se comunicar. As chaves são geradas de acordo com os atributos de cada dispositivo. Por exemplo, em um ambiente hospitalar, os dispositivos pertencentes a ala do hospital que trata de diabéticos possuem o atributo *diabeticos*. Ao gerar um texto criptografado utilizando uma chave pública, a chave é correspondente ao atributo utilizado. Assim, somente os dispositivos que possuem esse atributo poderão decriptografar o texto criptografado. Os dispositivos IoT podem se comunicam utilizando as chaves geradas pela autoridade ABE.

Os dispositivos que possuam os mesmos atributos podem compartilhar chaves secretas. Essas chaves são então utilizadas para comunicação segura entre dispositivos. Mais especificamente, o esquema utiliza PK-ABE (ver seção 2.2.3.2) para distribuir chaves secretas entre

dispositivos que possuam os mesmos atributos. Após obterem essas chaves, os dispositivos podem se comunicar utilizando criptografia simétrica.

O esquema requer primeiramente a geração das chaves ABE para os dispositivos. Como resultado, uma chave pública ABE é gerada e cada dispositivo possuirá uma chave privada ABE capaz de decriptografar os textos criptografados com atributos específicos. Após isso, cada dispositivo está apto a se comunicar de forma sigilosa com outros dispositivos ou usuários que possuam os mesmos atributos. Antes de enviar um dado a um dispositivo, este dado é primeiramente criptografado. Para isso, o dispositivo origem primeiramente obtém a chave pública ABE. Após isso, ele gera uma chave simétrica e secreta de sessão, e criptografa essa chave com a chave pública ABE. O texto cifrado resultante é enviado ao dispositivo destino. Ao receber o texto cifrado, o dispositivo destino o decriptografa com sua chave ABE e obtém a chave secreta de sessão. A partir desse momento, qualquer dado enviado entre esses dispositivos é criptografado com a chave de sessão utilizando criptografia simétrica (ver seção 2.2.3.1).

Figura 8 – Visão Geral .



Fonte: Elaborada pelo autor (2017)

A visão geral do esquema é apresentada na Figura 8. O dispositivo *A* obtém uma chave pública ABE da autoridade (etapa 1). Após isso, o dispositivo *A* gera uma chave simétrica e secreta, e criptografa essa chave com a chave pública ABE. Em seguida, o dispositivo *A* envia o texto criptografado para o dispositivo *B* (etapa 2). Após isso, o dispositivo *B* obtém uma chave ABE (etapa 3) da autoridade, decriptografa o texto cifrado e obtém a chave secreta. Ao concluir esse processo, os dados enviados entre A e B (etapa 4 e 5) serão criptografados com por meio de criptografia simétrica utilizando a chave de sessão.

4.2 Requisitos

O esquema proposto apresenta requisitos que são condições básicas para o funcionamento dessa estrutura. A partir da visão geral apresentada anteriormente, foi definido um conjunto de requisitos necessários. Esses requisitos são apresentados a seguir:

- Autenticação de dispositivos e usuários. Para que um dispositivo possa se comunicar com um usuário, ou com outro dispositivo, deve ser realizado um procedimento de autenticação que torne válida a sua identidade. O esquema requer que os usuários participantes tenham realizado um processo de autenticação prévia e esta autenticação deve ser reconhecida pela autoridade ABE. Após a autenticação, a autoridade ABE será capaz de determinar um conjunto de atributos para a construir a estrutura de acesso, correspondentes com os atributos identificados no processo de autenticação.
- Dispositivos com poder de processamento computacional relevativamente alto. Os dispositivos devem possuir processamento computacional para executar tarefas como criptografar e decriptografar os dados. Alguns dispositivos IoT (por exemplo, dispositivos que utilizam etiquetas RFID), não retém tal poder de processamento computacional, no entanto, podem utilizar dispositivos auxiliares de armazenamento de dados que assegurem a capacidade para criptografar e decriptografar os dados.
- Criptografia simétrica. Um dos componentes criptográficos do esquema é a criptografia simétrica que deve ser aplicada diretamente sobre os dados transmitidos em IoT. Neste esquema, não é especificado nenhum algoritmo de criptografia simétrica que deva ser utilizada. No entanto, considera-se o uso de algoritmos seguros, como o AES, para realizar a criptografia diretamente sobre os dados IoT.
- Criptografia KP-ABE. Outro componente criptográfico do esquema é a criptografia assimétrica ABE. Em específico, deve ser utilizado a Criptografia Baseada em Atributos com Políticas nas Chaves Privadas (PK-ABE) para criptografar chaves simétricas.

4.3 Participantes

Para que haja o estabelecimento das partes atuantes neste esquema, foram identificados os participantes. Eles são: dispositivos IoT (*Device*) ou usuários ($User$); autoridade ABE (A_{Att}) e serviço em nuvem ($Cloud$) .

Device é caracterizado como um dispositivo inteligente, que necessita ou não de intervenção humana para executar suas tarefas, realizando comunicação com outro dispositivo ou aplicação. Este dispositivo IoT deve conter mecanismo de comunicação com a Internet, seja diretamente (por exemplo, sensores que possuem comunicação via WiFi) ou indiretamente (por exemplo, dispositivo auxiliar).

User é identificado como um usuário que utiliza aplicações que necessitam de dados gerados por dispositivos IoT. *User* pode fornecer dados a *Device* para realizar uma tarefa.

A_{Att} é uma autoridade de fonte confiável capaz de reconhecer *Device* e *User*. Esta autoridade é responsável por emitir os conjuntos de atributos utilizados nas estruturas de acesso. A_{Att} também é responsável por gerar as chaves de criptografia e decriptografia ABE.

Cloud atua como um mecanismo de interação entre dispositivos ou entre dispositivo e usuário. *Cloud* pode solicitar informações de *Device* e *User*. Da mesma forma, *Cloud* pode fornecer informações caso *Device* e *User* não estejam disponíveis.

4.4 Premissas

É apresentado um conjunto de informações essenciais que servem de base para o esquema proposto. Estas informações são denominadas de premissas do esquema. As premissas devem ser verdadeiras para que o funcionamento do esquema seja considerado válido.

A primeira premissa corresponde aos recursos de redes utilizados para realizar a comunicação entre os participantes. É admitido que os recursos estão disponíveis sempre que necessários e não há falhas durante a comunicação. Da mesma forma, todos os canais de comunicação são seguros e autenticados.

A utilização de criptografia recorrente durante a transmissão dos dados é outra premissa deste esquema. Ou seja, todos os dados são criptografados antes de serem enviados. Deste modo, a criptografia KP-ABE está disponível sempre que solicitada pelos participantes. Da mesma forma, a criptografia simétrica está disponível.

É assumido como premissa que os participantes *Device* e *User* obtém as chaves ABE correspondentes aos seus atributos. Ou seja, a autoridade A_{Att} gera as chaves ABE sempre relacionando os atributos às características dos participantes, sendo esses participantes reconhecidos pela autoridade A_{Att}.

Como última premissa, a autoridade A_{Att} é reconhecida como uma fonte confiável para distribuir chaves e A_{Att} está disponível para gerar as chaves ABE para *Device* e *User* sempre que solicitada.

4.5 Descrição do Esquema

O esquema proposto objetiva distribuir chaves para prover o sigilo dos dados em ambientes IoT. Para isso, é utilizada uma criptografia simétrica diretamente sobre os dados IoT e a criptografia PK-ABE para proteger a chave da criptografia simétrica. Desta forma, é realizada uma combinação dos recursos de KP-ABE e criptografia simétrica para proteção e recuperação de dados IoT. O esquema proposto contém três etapas, Configuração, Criptografia e Decriptografia,

descritas a seguir.

4.5.1 Etapa de Configuração

Esta etapa exerce o estabelecimento das chaves ABE utilizadas no esquema proposto para realizar criptografia e decriptografia dos dados. A etapa de configuração tem como entrada um conjunto de atributos S e uma estrutura de controle de acesso T. A autoridade A_{Att} determina S correspondendo aos atributos do participante, *Device* ou $User$, para construir a estrutura de controle de acesso T. Em seguida, é executado o algoritmo de configuração ABE que determina um conjunto de parâmetros para gerar a chave mestre MK_{ABE} e a chave pública PK_{ABE}. A autoridade A_{Att} é a responsável por gerar MK_{ABE} e PK_{ABE}.

- **Geração da Chave Privada ABE**

  Para gerar uma chave privada correspondente a chave pública PK_{ABE}, é obtido como entrada a estrutura de controle de acesso T, a chave mestre MK_{ABE} e a chave pública PK_{ABE}. A partir disso, é gerada uma chave privada ABE que contém a estrutura de acesso T. Como saída, teremos a chave privada SK_{ABE_T}.

Como saída da etapa de configuração, são obtidas a chave mestre MK_{ABE}, a chave pública PK_{ABE} e a chave privada SK_{ABE_T}.

4.5.2 Etapa de Criptografia

Nesta etapa é realizado o estabelecimento da chave simétrica e é realizada a criptografia dos dados. Para tal, esta etapa tem como entrada uma mensagem m que corresponde à dados provenientes do participante, o conjunto de atributos S e a chave pública PK_{ABE}. É executado o algoritmo de criptografia simétrica e é gerada uma chave simétrica e secreta de sessão K. A mensagem m é cifrada com criptografia simétrica utilizando a chave K, resultando em um texto cifrado C.

Após isso, a chave K é criptografada por ABE utilizando a chave PK_{ABE} e rotulada com o conjunto de atributos S. Desta criptografia, é produzido o texto cifrado $C_{ABE}K_S$. Como saída desta etapa, é obtido os textos cifrados C e $C_{ABE}K_S$. Esta etapa pode ser acompanhada no Algoritmo 1 mostrado abaixo.

Algoritmo 1: Criptografando a mensagem m.

1 $C \leftarrow E(m,K)$

2 $C_{ABE}K_S \leftarrow E_{ABE}(K,PK,S)$

4.5.3 Etapa de Decriptografia

Para recuperar a mensagem m, a etapa de Decriptografia tem como entrada os textos cifrados C e $C_{ABE}K_S$, e a chave privada SK_{ABE_T}. É decriptografado por ABE o texto cifrado $C_{ABE}K_S$ utilizando a chave privada SK_{ABE_T}. Caso a estrutura de acesso T contida em SK_{ABE_T} seja satisfeita, é recuperada a chave simétrica K.

Após a chave K obtida, é decriptografado o texto cifrado C utilizando a chave simétrica K e recuperando a mensagem m. Como saída dessa etapa, teremos a chave simétrica K e a mensagem m. A seguir, o Algoritmo 2 descreve essa etapa.

Algoritmo 2: Decriptografando a mensagem m.

1 $K \leftarrow D_{ABE}(C_{ABE}K_S, SK_{ABE_T})$
2 $m \leftarrow D(C,K)$

Após os participantes obterem a chave K, qualquer dado enviado entre eles é criptografado somente com a chave de sessão K utilizando criptografia simétrica.

4.6 Discussão Sobre a Segurança do Esquema

O objetivo deste esquema é distribuir chaves para proporcionar o sigilo dos dados no ambiente da IoT e assim garantir a confidencialidade. Desta forma, nesta seção é apresentada uma discussão sobre a segurança do esquema.

O emprego de ABE no esquema requer que os participantes possuam atributos que lhe dão acesso a determinados dados, desta forma, ABE também pode exercer a função de controle de acesso aos dados. Por exemplo, um sensor X pode possuir atributos como {“id do usuário”, “função”, “número de série”, "data de fabricação"}, somente terá acesso aos dados os participantes que corresponderem a esses atributos. Quanto maior o número de atributos, maior será a especificação do controle de acesso aos dados. Vale ressaltar que o uso de ABE não dispensa que outras técnicas de controle de acesso possam ser utilizadas em conjunto.

A autoridade de atributos garante que os participantes envolvidos já possuem uma autenticação prévia antes de trocarem dados. Desta forma, é proporcionando uma garantia de reconhecimentos entre os participantes.

O esquema considera que um terceiro não autorizado (t) não pode quebrar a privacidade do usuário acessando os dados criptografados m. Para decriptografar m, t primeiramente precisa ter acesso a chave privada SK_ABE concedidada pela autoridade de atributos. Desde que t não possua os atributos rotulados no texto criptografado por ABE, ele não poderá ter a chave SK_ABE. Consequentemente, t não obterá a chave de sessão para decriptografar m.

A desvantagem deste esquema é a necessidade de poder de processamento computacional relativamente alto para executar o esquema apresentado. O participante deve ter poder computa-

cional para criptografar e/ou decriptografar dados. Quanto maior a quantidade de atributos, é necessário mais recursos para a execução do esquema. Segundo Wang et al. (2014), a maioria dos casos de aplicações IoT, em cada instância de criptografia de dados, o número de atributos envolvidos não deve exceder a 30.

O esquema proposto não trata de atributos revogados. Ao criptografar dados por KP-ABE, a estrutura de acesso T é compatível ao atributos rotulados no texto criptografado. Se um participante tiver um ou mais atributos revogados durante o processo, ele deve requerir novos atributos. Desta forma, deve ser gerado uma nova chave ABE, assim como uma nova estrututa T compatível.

4.7 Empregando o esquema em uma Arquitetura IoT

Para exemplificar o uso do esquema, foi utilizada a arquitetura OSCAR apresentada na Seção 3.3, por apresentar uma estrutura semelhante ao funcionamento do esquema. A semelhança se deve ao fato da arquitetura OSCAR possuir componentes que podem desempenhar as tarefas apresentadas no esquema proposto. Para melhor compreensão é necessário relembrar quatro componentes importantes dessa arquitetura: o Produtor que fornece recursos; o Consumidor que solicita recursos; o Servidor de Autorização que fornece certificados e fornece segredos de acesso; e o Servidor Proxy que fornece cópias de recursos caso o produtor esteja indisponível.

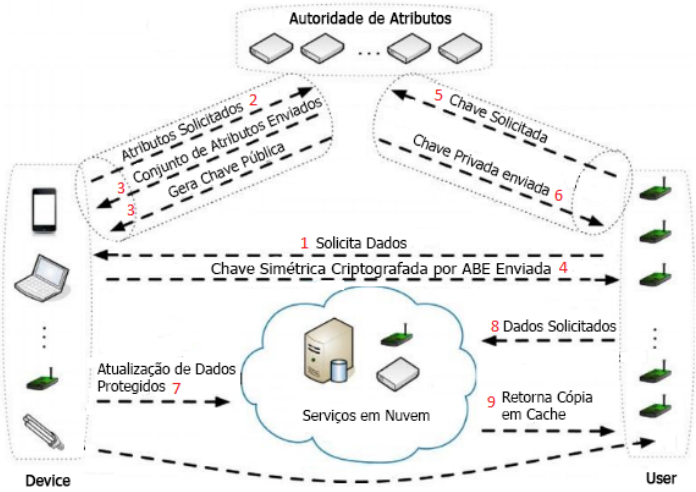
Ao adotar os componentes para exercer as tarefas do esquema proposto, teremos:

- O Produtor e o Consumidor podem ser identificados como os participantes *Device* ou $User$, fornecendo ou utilizando recursos;
- O Servidor de Autorização pode ser reconhecido como a autoridade de atributos A_{Att}, determinando os atributos e disponibilizando as chaves para criptografia e decriptografia;
- O Servidor Proxy pode ser reconhecido como serviços em nuvem.

Vale ressaltar que o propósito não é substituir as funções da arquitetura OSCAR, mas mostrar que o esquema funcionaria neste ambiente. Desta forma, teremos a seguinte modificação na arquitetura, identificado por 9 etapas, conforme Figura 9.

Na Figura 9, é adotado que os participantes *Device* e $User$ desejam trocar informações. $User$ solicita os dados de *Device* (etapa 1). *Device*, por sua vez, solicita à autoridade A_{Att} os atributos correspondentes à $User$ (etapa 2). Então, A_{Att} gera um conjunto de atributos e uma chave pública (etapa 3). Após isso, *Device* executa o ABE e criptografa a chave simétrica e o texto criptografado é rotulado com os atributos. Em seguida, os dados são enviados (etapa 4). Então, $User$ solicita uma chave de decriptografia ABE para A_{Att} (etapa 5). Por sua vez, A_{Att} envia uma chave para $User$ (etapa 6). Se $User$ possuir os atributos, os dados poderão ser decriptografados e a chave simétrica será recuperada.

Figura 9 – Componentes da arquitetura OSCAR modificados.



Fonte: Modificado de VUCINIC et al., 2015, p. 6.

O dispositivo *Device* fornece atualizações dos seus dados protegidos ao serviço em nuvem (etapa 7). *User* pode solicitar ao serviço em nuvem os dados de *Device*, caso ele esteja indisponível (etapa 8). A nuvem poderá disponibilizar a cópia em *cache* (etapa 9). Como *User* já possui a chave de sessão, ele terá acesso aos dados cifrados por criptografia simétrica.

É assumido que os participantes *Device* e *User* têm atributos válidos identificados previamente pela autoridade de atributos A_{Att}. Os participantes obtém suas chaves ABE para decriptografar suas chaves de sessão. As chaves ABE são utilizadas por todos que possuírem os atributos de acesso. Por exemplo, se for rotulado no texto criptografado o atribulo "x", todos os participantes que tiverem esse atributo poderão obter a chave ABE, e consequentemente, obter a chave de sessão.

4.8 Conclusão

O capítulo apresentou uma proposta de esquema para distribuição de chaves em ambientes IoT. Para tal, foi sugerido a utilização de Criptografia Baseada em Atributos com Políticas na Chave Privada combinado com criptografia simétrica. Desta forma, os dados são transmitido de forma sigilosa e a privacidade do usuário é garantida.

O esquema considerou a utilização de KP-ABE no esquema por ser mais eficiente do que CP-ABE quando executado em ambiente IoT, levando em conta tempo de execução, sobrecarga de dados e de rede, consumo de energia, bem como uso de CPU e memória, conforme apresentado em Wang et al. (2014).

A utilização de criptografia simétrica para realizar a criptografia de sessão, deve se ao fato de que a execução de uma criptografia simétrica é relativamente mais rápida do que a execução

de ABE. No entanto, ABE é considerado mais seguro. Devido a isto, há a necessidade de proteger a chave da criptografia simétrica com ABE. A não especificação de uma criptografia simétrica para o esquema considera que diferentes cenários podem requerer diferentes criptografias de sessão.

5 CONSIDERAÇÕES FINAIS

A procura por processos de otimização ou automatização de tarefas do cotidiano gera o desenvolvimento de novas tecnologias e dispositivos para IoT. Devido às limitações dos dispositivos IoT, é necessário a elaboração de técnicas que promovam o sigilo das informações.

Neste contexto, a fim de contornar os desafios encontrados na implantação da IoT, este trabalho foi desenvolvido abordando o problema de segurança quanto as técnicas de confidencialidade na IoT. Foi realizado um estudo sobre as técnicas de seguranças utilizadas em IoT, visando principalmente as técnicas de confidencialidade propostas atualmente na literatura da IoT.

Este trabalho considera as diferentes características de dispositivos IoT para garantir que haja o sigilo dos dados transmitidos. Desta forma, foi desenvolvido um esquema de distribuição de chaves, no qual é combinado o uso de criptografia simétrica e Criptografia Baseada em Atributos com Políticas nas Chaves Privadas. No esquema proposto, os dispositivos ou usuários podem se comunicar de forma sigilosa, assegurando que os dados são protegidos. É realizada uma comunicação restrita a participantes autorizados. Para tal, uma autoridade garante a autenticação dos participantes antes da comunicação.

O que se pôde concluir quanto a utilização do esquema proposto neste trabalho foi que:

- O esquema considera o baixo poder de processamento computacional presente em dispositivos IoT;
- Os dados são transmitidos de forma sigilosa utilizando o esquema de distribuição de chaves;
- O esquema funciona tanto horizontalmente (dispositivo para dispositivo) quanto verticalmente (dispositivo para aplicação);
- O esquema pode ser aplicado teoricamente em uma arquitetura IoT, como mostrado na Seção 4.7.

5.1 Trabalhos Futuros

Como trabalhos futuros, é pretendido continuar o desenvolvimento do esquema analisando criptografias simétricas que apresentem melhor desempenho para serem executadas em IoT. Também é pretendido realizar a implementação do esquema. Desta forma, poderá ser testada a viabilidade da proposta e identificar novas considerações. Será verificado as limitações presentes nos cenários (por exemplo, mecanismos que possam interferir de alguma forma no funcionamento do esquema) e será analisado os dispositivos e usuários com condições restritas.

Para o desenvolvimento deste trabalho, foi considerado ambientes que não possuam especificações de funcionamento da transmissão dos dados (por exemplo, não é empregada nenhuma plataforma). Acredita-se que ao realizar uma análise mais específica nos cenários, o esquema possa ser conciliado a uma estrutura.

Além disso, é pretendido fazer uma análise sobre o impacto do esquema criptográfico proposto sobre a transmissão dos dados em IoT e discorrer sobre as considerações positivas e negativas desses impactos.

REFERÊNCIAS

AHLMEYER, M.; CHIRCU, A. M. Securing the internet of things: A review. **Issues in Information Systems**, v. 17, n. 4, 2016.

AMBROSIN, M. et al. On the feasibility of attribute-based encryption on internet of things devices. **IEEE Micro**, IEEE, v. 36, n. 6, p. 25–35, 2016.

ANDERSON, R. **Security engineering**. [S.l.]: John Wiley & Sons, 2008.

ANOOP, M. Elliptic curve cryptography. **An Implementation Guide**, 2007.

ATAMLI, A. W.; MARTIN, A. Threat-based security analysis for the internet of things. In: IEEE. **Secure Internet of Things (SIoT), 2014 International Workshop on**. [S.l.], 2014. p. 35–43.

BENATALLAH, B. **Cloud computing: methodology, systems, and applications**. [S.l.]: CRC Press, 2011.

BETHENCOURT, J.; SAHAI, A.; WATERS, B. Ciphertext-policy attribute-based encryption. In: IEEE. **2007 IEEE symposium on security and privacy (SP'07)**. [S.l.], 2007. p. 321–334.

BLAKLEY, B.; MCDERMOTT, E.; GEER, D. Information security is information risk management. In: ACM. **Proceedings of the 2001 workshop on New security paradigms**. [S.l.], 2001. p. 97–104.

BORGOHAIN, T.; KUMAR, U.; SANYAL, S. Survey of security and privacy issues of internet of things. **arXiv preprint arXiv:1501.02211**, 2015.

BORIC-LUBECKE, O. et al. E-healthcare: Remote monitoring, privacy, and security. In: IEEE. **2014 IEEE MTT-S International Microwave Symposium (IMS2014)**. [S.l.], 2014. p. 1–3.

BOTTA, A. et al. On the integration of cloud computing and internet of things. In: IEEE. **Future Internet of Things and Cloud (FiCloud), 2014 International Conference on**. [S.l.], 2014. p. 23–30.

DAEMEN, J.; RIJMEN, V. Aes proposal: Rijndael. 1999.

DAVID, F.; RICHARD, K. Role-based access controls. In: BALTIMORE, MARYLAND: NIST-NCSC. **Proceedings of 15th NIST-NCSC National Computer Security Conference**. [S.l.], 1992. v. 563.

DOMENECH, M. C.; BOUKERCHE, A.; WANGHAM, M. S. An authentication and authorization infrastructure for the web of things. In: ACM. **Proceedings of the 12th ACM Symposium on QoS and Security for Wireless and Mobile Networks**. [S.l.], 2016. p. 39–46.

DOMENECH, M. C.; CARVALHO, G. M. de; WANGHAM, M. S. Um provedor de identidades para autenticação de dispositivos e de usuários baseado no padrão saml. **Anais do Computer on the Beach**, p. 522–524, 2015.

FAROOQ, M. et al. A critical analysis on the security concerns of internet of things (iot). **International Journal of Computer Applications**, Foundation of Computer Science, v. 111, n. 7, 2015.

GARTNER. **Gartner Survey Shows That 43 Percent of Organizations Are Using or Plan to Implement the Internet of Things in 2016**. 2016. Comunicado de Imprensa. Disponível em: <http://www.gartner.com/newsroom/id/3236718>. Acesso em: 09 out 2016.

GOYAL, V. et al. Attribute-based encryption for fine-grained access control of encrypted data. In: ACM. **Proceedings of the 13th ACM conference on Computer and communications security**. [S.l.], 2006. p. 89–98.

GUBBI, J. et al. Internet of things (iot): A vision, architectural elements, and future directions. **Future Generation Computer Systems**, Elsevier, v. 29, n. 7, p. 1645–1660, 2013.

HOSSAIN, M. S.; MUHAMMAD, G. Cloud-assisted industrial internet of things (iiot)–enabled framework for health monitoring. **Computer Networks**, Elsevier, v. 101, p. 192–202, 2016.

HUMAYED, A.; LUO, B. Cyber-physical security for smart cars: taxonomy of vulnerabilities, threats, and attacks. In: ACM. **Proceedings of the ACM/IEEE Sixth International Conference on Cyber-Physical Systems**. [S.l.], 2015. p. 252–253.

HUR, J.; NOH, D. K. Attribute-based access control with efficient revocation in data outsourcing systems. **IEEE Transactions on Parallel and Distributed Systems**, IEEE, v. 22, n. 7, p. 1214–1221, 2011.

KAUSHIK, A. B. Y.; JHA, C. K. A comparison of heuristics algorithm for load balancing in cloud environment. **International Journal of Scientific and Engineering Research**, IJSER, v. 6, n. 9, p. 1208–1213, 2015.

KULKARNI, K.; DIXIT, A. M. **Privacy Preserving System Using Attribute Based Encryption for e-health Cloud**. [S.l.]: IJSR, 2014.

KURKINEN, L. **Smart Homes and Home Automation**. 2016.

LANZA, J. et al. Large-scale mobile sensing enabled internet-of-things testbed for smart city services. **International Journal of Distributed Sensor Networks**, Taylor & Francis, Inc., v. 2015, p. 157, 2015.

LONGO, R.; MARCOLLA, C.; SALA, M. **Collaborative Multi-Authority KP-ABE for Shorter Keys and Parameters**. [S.l.], 2016.

MAHALLE, P. N. et al. Identity establishment and capability based access control (iecac) scheme for internet of things. In: IEEE. **Wireless Personal Multimedia Communications (WPMC), 2012 15th International Symposium on**. [S.l.], 2012. p. 187–191.

MELL, P.; GRANCE, T. The nist definition of cloud computing. Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology Gaithersburg, 2011.

MILLER, V. S. Use of elliptic curves in cryptography. In: SPRINGER. **Conference on the Theory and Application of Cryptographic Techniques**. [S.l.], 1985. p. 417–426.

MIORANDI, D. et al. Internet of things: Vision, applications and research challenges. **Ad Hoc Networks**, Elsevier, v. 10, n. 7, p. 1497–1516, 2012.

NEISSE, R. et al. A model-based security toolkit for the internet of things. In: IEEE. **Availability, Reliability and Security (ARES), 2014 Ninth International Conference on**. [S.l.], 2014. p. 78–87.

NEISSE, R. et al. Seckit: a model-based security toolkit for the internet of things. **Computers & Security**, Elsevier, v. 54, p. 60–76, 2015.

OH, S. W.; KIM, H. S. Decentralized access permission control using resource-oriented architecture for the web of things. In: IEEE. **16th International Conference on Advanced Communication Technology**. [S.l.], 2014. p. 749–753.

RESCORLA, E.; MODADUGU, N. Datagram transport layer security version 1.2. 2012.

SAHAI, A.; WATERS, B. Fuzzy identity-based encryption. In: SPRINGER. **Annual International Conference on the Theory and Applications of Cryptographic Techniques**. [S.l.], 2005. p. 457–473.

SANDHU, R. S. et al. Role-based access control models yz. **IEEE computer**, v. 29, n. 2, p. 38–47, 1996.

SARKAR, C. et al. A scalable distributed architecture towards unifying iot applications. In: IEEE. **Internet of Things (WF-IoT), 2014 IEEE World Forum on**. [S.l.], 2014. p. 508–513.

SARKAR, C. et al. Diat: A scalable distributed architecture for iot. **IEEE Internet of Things Journal**, IEEE, v. 2, n. 3, p. 230–239, 2015.

SICARI, S. et al. A security-and quality-aware system architecture for internet of things. **Information Systems Frontiers**, Springer, p. 1–13, 2014.

SICARI, S. et al. Security, privacy and trust in internet of things: The road ahead. **Computer Networks**, Elsevier, v. 76, p. 146–164, 2015.

SOBOLEWSKI, J. S. Cyclic redundancy check. John Wiley and Sons Ltd., 2003.

STALLINGS, W. **Criptografia e segurança de redes 4ª ed**. [S.l.]: São Paulo: Pearson Prentice Hall, 2008.

TIWARI, V. K.; SINGH, V. Study of internet of things (iot): A vision, architectural elements, and future directions. **International Journal of Advanced Research in Computer Science**, v. 7, n. 7, 2017.

VUČINIĆ, M. et al. Oscar: Object security architecture for the internet of things. In: IEEE. **World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2014 IEEE 15th International Symposium on a**. [S.l.], 2014. p. 1–10.

WANG, X. et al. Performance evaluation of attribute-based encryption: Toward data privacy in the iot. In: IEEE. **2014 IEEE International Conference on Communications (ICC)**. [S.l.], 2014. p. 725–730.

WANGHAM, M. S.; DOMENECH, M. C.; MELLO, E. R. de. Infraestrutura de autenticaçao e de autorizaçao para internet das coisas. **Minicursos do XIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais—SBSeg**, 2013.

WANGHAM, M. S. et al. Gerenciamento de identidades federadas. **Minicurso-SBSeg 2010-Fortaleza-CE**, 2010.

WEBER, R. H. Internet of things–new security and privacy challenges. **Computer Law & Security Review**, Elsevier, v. 26, n. 1, p. 23–30, 2010.

YAO, X.; CHEN, Z.; TIAN, Y. A lightweight attribute-based encryption scheme for the internet of things. **Future Generation Computer Systems**, Elsevier, v. 49, p. 104–112, 2015.

YUAN, E.; TONG, J. Attributed based access control (abac) for web services. In: IEEE. **IEEE International Conference on Web Services (ICWS'05)**. [S.l.], 2005.