IoT: conceitos de segurança de dados e criptografia

Gabriel Brogno Alcantara Pauferro[1]
Seila Vasti Faria de Paiva[2]
Nayari Marie Lessa[3]

Resumo: O presente artigo trata de conceitos de Internet das Coisas (IoT), um paradigma computacional que conecta objetos do cotidiano entre si e através da internet. Seu objetivo é otimizar atividades e processos em diversos aspectos da vida humana através do compartilhamento de dados. Devido a sua popularização através de objetos inteligentes e aplicações contemporâneas, observa-se um crescimento exponencial dessa filosofia tecnológica envolvendo o uso e manipulação de dados sensíveis ao usuário. Com isso, torna-se evidente a necessidade de se revisar alguns protocolos de segurança da informação que envolvem estas aplicações, ou seja, encriptação de dados. Será dado um enfoque na questão da segurança da informação dessas aplicações, com especificidade à criptografia das informações sensíveis. Serão conceituados quatro procedimentos de cifragem de informações sensíveis mais utilizados em segurança de dados: RSA, ECC, AES e SHA, com exemplificações simples de uso em uma infraestrutura IoT.

Palavras-chave: Algoritmos; Criptografia; Internet das coisas (IoT); Segurança de dados.

Abstract: This article concerns the concepts of Internet of Things (IoT), a computational paradigm, which connects everyday objects between themselves through the internet. IoT' main focus is to optimize humankind's everyday activities and workflow processes throughout data sharing. Due to smart objects and contemporary applications' popularity, it can be observed an exponential growth in its technological philosophy that uses and manipulates sensible data to the user. With that, it becomes evident, review some of the data security protocols that surround these applications, specifically about sensible data cryptography. Then, four of the most used sensible data safety encryption procedures: RSA, ECC, AES and SHA shall be conceptualized with simple exemplification inside an IoT infrastructure.

Keywords: Algorithms; Encryption; Internet of things (IoT); Data security.

Introdução

O conceito de Internet das Coisas (IoT) foi criado em 1999 pelo pesquisador britânico Kevin Ashton. Este paradigma tecnológico computacional interliga aparelhos de uso cotidiano

[1] Discente do curso de Tecnologia em Análise e Desenvolvimento de Sistemas do Instituto Federal de São Paulo (IFSP), Câmpus Salto, gabriel.brogno@aluno.ifsp.edu.br
[2] Docente do curso de Bacharelado em Ciência da Computação do Instituto Federal de São Paulo (IFSP), Câmpus Salto, svfpaiva@ifsp.edu.br
[3] Técnica de Laboratório do Instituto Federal de São Paulo (IFSP), Câmpus Salto, nayari@ifsp.edu.br

Submetido: 12/06/2020 Publicado: 03/11/2020

com capacidade de processamento computacional embarcado conectando-os através da Internet. Segundo Leite *et al.* (2017), a Internet das Coisas pode ser considerada como uma nova onda tecnológica que criou uma fronteira de conexão do mundo com pessoas, computadores, dispositivos (objetos/coisas), ambientes e objetos virtuais, capazes de se conectarem e interagirem entre si.

Segundo Al-Fuqaha *et al.* (2015), o conceito geral da Internet das Coisas é aquele que transforma objetos tradicionais em inteligentes, fazendo com que os objetos físicos vejam, ouçam, tomem decisões, executem tarefas, "conversem", compartilhem informações e coordenem decisões. A figura 1 mostra o conceito geral da IoT, onde objetos inteligentes que atuam em um particular conjunto de problemas em aplicações específicas de domínio, constituem o que chamamos de mercados verticais. As plataformas de serviços de computação e análises não endereçadas à solução de problemas específicos, serviços independentes de domínio, constituem os chamados mercados horizontais.

Figura 1: Conceito geral da IoT

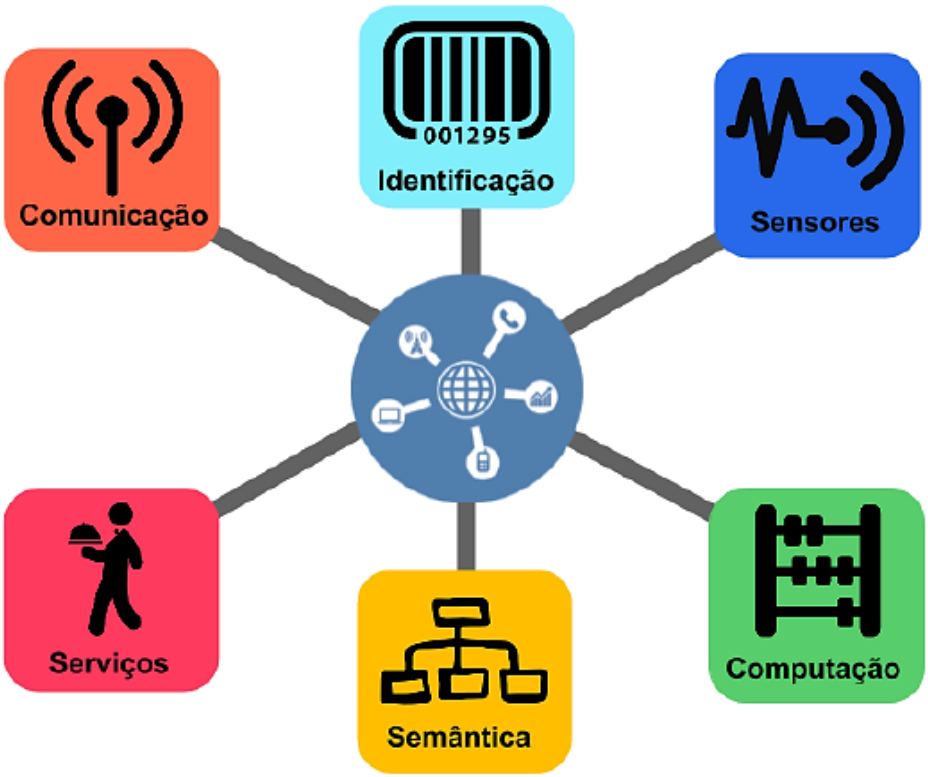
Fonte: AL-FUQAHA *et al.*, 2015 (adaptado pelos autores)

Em outras palavras, cada aplicativo específico interage com serviços independentes e enquanto isso os sensores e atuadores se comunicam diretamente entre si em cada domínio. Espera-se que a IoT permita o desenvolvimento de aplicações que possam contribuir para a vida doméstica e para o crescimento da economia mundial. Como exemplo, uma residência inteligente permitirá que seus moradores abram suas garagens ao chegarem em casa, prepare seu café, liguem e escolham a temperatura do ar-condicionado, ligue ou desligue a TV e outros aparelhos através de seu aparelho celular.

As aplicações de IoT não exigem mais do que uma configuração única, que pode ser realizada através de uma interface gráfica, para que haja interação entre seus componentes e os seres humanos. Elas possuem como característica um escopo de interação mínimo ou quase inexistente. No entanto, elas são de grande alcance. (HENRIQUES; VENEKAR, 2017).

Esse paradigma tecnológico utiliza seis componentes em sua fundamentação, os quais combinam tecnologias diversas que se complementam permitindo a interação. Santos *et al.* (2016), nomeia estes componentes como blocos básicos de construção da IoT, como podemos ver na figura 2:

Figura 2: Blocos básicos de construção da IoT



Fonte: SANTOS *et al.*, 2016

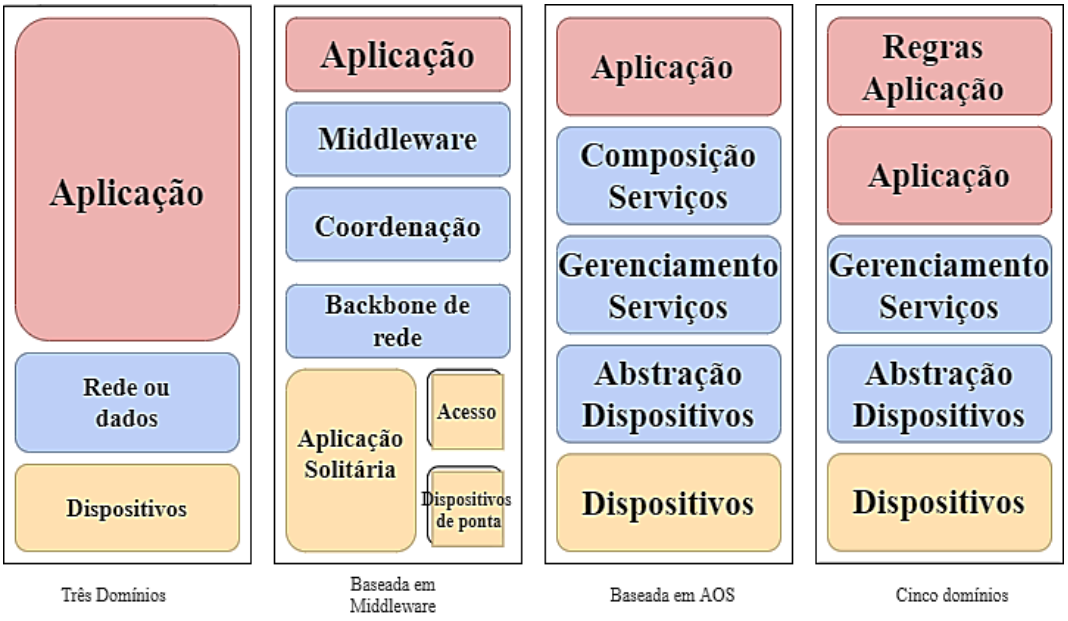
Se faz necessário definir os componentes fundamentais de uma aplicação IoT, ou seja, os blocos básicos de construção da IoT, conforme Santos *et al.* (2016):

1. Identificação: métodos ou componentes de hardware que identificam de maneira única determinado objeto. Exemplos: identificação por radiofrequência ou RFID, endereço MAC ou controle de acesso de mídia e endereçamento IP.
2. Sensores: coletores de dados que estejam orientados ao contexto da necessidade da aplicação instalada naquele ambiente. Exemplos: sensores de iluminação, termômetros e oxímetros.
3. Comunicação: métodos, protocolos e tecnologia de rede que permitem a interatividade entre os componentes e usuários finais daquela implementação com a internet para a utilização de serviços contextualizados à aplicação. Exemplos: modems, gateways, 3G, 4G, WAN, LAN.
4. Computação: a capacidade de processamento utilizada em todos os níveis e atividades em aplicações IoT. Exemplos: serviços de processamento em nuvem, redes neurais e processadores embarcados.
5. Serviços: destacamos algumas classes de serviços que a IoT pode prover:
   a. De identificação;
   b. De agregação de dados;
   c. De colaboração e inteligência;
   d. De ubiquidade.
6. Semântica: habilidade que essa aplicação tem em transformar os dados gerados em informações e contextualizá-las em conhecimento compreensível conforme as necessidades estabelecidas no escopo do sistema, para o uso de outras máquinas ou seres humanos de maneira mais eficiente. Exemplo: Relatórios, Storytelling.

Diferentes arquiteturas de IoT vem sendo propostas por diferentes pesquisadores que incorporam os componentes básicos dos sistemas de IoT em diferentes áreas de aplicações, dos quais podemos citar as arquiteturas baseadas em três e cinco domínios, baseada em Middleware e baseada em AOS, como mostra a figura 3:

- A arquitetura de três domínios agrupa a camada de baixo nível ou camada de Dispositivos (sensores e comunicação), a camada de Rede ou Dados (identificação e computação) e a camada de alto nível ou camada de Aplicação, a semântica;
- A arquitetura de cinco domínios incorpora a camada de Abstração de Dispositivos (transferência de dados dos dispositivos), camada de Gerenciamento de Serviços (processamento de dados) e camada de Regras de Aplicação (modelamento de dados de interface, monitoramento e gerenciamento das quatro camadas inferiores);
- Baseada em Middleware: provém serviços que facilitam e coordenam aspectos de processamento cooperativo entre diferentes sistemas e está entre a camada de aplicação e de operação do sistema;
- Baseada em AOS (arquitetura orientada a serviço): é uma abordagem utilizada para criar uma arquitetura baseada no uso de sistemas de serviços.

Figura 3: Arquiteturas de IoT (AL-FUQAHA et al., 2015)



Fonte: AL-FUQAHA *et al.*, 2015

Singh e Singh (2015) definem em seu artigo, uma espécie de benefício e componente da utilização de implementações IoT: a conservação de recursos. A capacidade de saber monitorar o desperdício de recursos com ambiente, com energia elétrica ou capacidade hídrica em torneiras ou sistemas de irrigação é considerado um componente muito importante no escopo de se implantar uma solução IoT.

Podemos então, classificar o restante dos benefícios de se integrar uma solução IoT no objetivo de compreender melhor o que esse paradigma pode realizar:

A. Interconectividade: a capacidade de objetos se reconhecerem através da conexão para realizarem uma tarefa com um propósito em comum;
B. Heterogeneidade: a funcionalidade e comunicação entre dispositivos de diferentes hardwares e softwares em uma mesma rede;
C. Dinamismo: o ato de reconhecer e agir com os mais diferentes estados de dispositivos, seja uma alteração em seu comportamento, localização ou velocidade de acesso;
D. Escalabilidade: a habilidade daquela aplicação funcionar e gerenciar com os mesmos índices de desempenho, considerando um crescimento no número de objetos;
E. Inteligência: o ato de fornecer serviços relacionados adequados e otimizados para o contexto da aplicação;
F. Serviços relacionados: serviços (geralmente encontrados em uma nuvem de processamento) realizados através de atuadores (máquinas autônomas) que otimizem

as diversas situações e atividades relacionadas ao contexto de aplicação. Exemplo: em uma casa inteligente, os sensores daquele local recebem uma mensagem avisando que seu dono chegará no intervalo de quinze minutos. Com essa informação, um serviço é disparado e de acordo com as preferências do proprietário da casa, o ambiente pode ter a temperatura, iluminação e som ajustados conforme as instruções;

G. Velocidade: A habilidade que o sistema possui em tomar decisões em tempo real ou em um intervalo de tempo hábil;

H. Segurança: métodos e sistemas que garantam a segurança do usuário durante o uso da implementação.

Assim como em aplicações tradicionais para a internet, as aplicações em IoT envolvem a utilização de dados e informações confidenciais e sensíveis de usuários ou de qualquer máquina que esteja aplicada àquele contexto. Com isso, percebe-se a importância de se garantir a segurança da informação em quaisquer aplicações que envolvam dados pessoais e/ou dados de empresas.

A segurança da informação (SI) pode ser definida como um conjunto de ações para permitir proteção aos dados ou a um grupo de dados, protegendo o valor destas informações para uma organização ou para um indivíduo específico. Estas ações devem ser desenvolvidas com o objetivo de garantir que os princípios básicos da SI sejam atingidos, os quais são: confidencialidade, integridade, disponibilidade e autenticidade. (SÊMOLA, 2014)

Segundo uma lista feita pelo OWASP (*Open Web Applications Security Project* – Projeto Aberto de Segurança de Aplicações Web) – IoT Project (2018), existem dez grandes vulnerabilidades recorrentes em tecnologias de IoT, os quais são: senhas, serviços de redes inseguros, interfaces comprometedoras, falta de mecanismos de atualização seguros, uso de componentes datados ou inseguros, proteção insegura de dados, transferência insegura de dados, falta de gerenciamento de dispositivos, configurações padrões inseguras e falta de proteção física dos dispositivos.

Logo, com a popularização de objetos e aplicações desse paradigma nos mais diferentes escopos da atividade humana na última década, torna-se necessário revisar os procedimentos de segurança associados ao uso dessas implementações, visto que os recursos e mecanismos de IoT não podem ser protegidos por protocolos de segurança da internet convencional, que foi desenvolvida para computadores de mesa e laptops, mas a aplicação de mecanismos de segurança devem ser aplicados em todos os domínios da IoT.

Sklavos e Zaharakis (2016) definiram que aparelhos inteligentes ou objetos com sistemas embarcados disponíveis no mercado também são vulneráveis a *malwares* tradicionais devido à falta de sistemas de segurança e o fato da limitação do poder de processamento de tais aparelhos.

Assim como qualquer sistema está sujeito a falhas na comunicação, Carracedo *et al.* (2018), apontaram que a IoT ganhou notoriedade por ter pontos de ataque ou origens de ataque e que para evitar esse tipo de problema é necessário reforçar componentes físicos e virtuais para promover os princípios da segurança das aplicações, principalmente nas características de criptografia das informações gerenciadas pelos softwares ainda nos dispositivos e no contexto em que estão inseridos.

Segundo Sicari *et al.* (2015), é necessário que sejam propostos modelos válidos de segurança da informação para que os usuários de aplicações de IoT possam ter confiança em utilizar tais tecnologias. Na figura 4 são listados os principais problemas de segurança nas aplicações de IoT, quais são: autenticação, confidencialidade, controle de acesso, privacidade, confiança, aplicação de políticas, *middlewares* seguros e segurança em dispositivos móveis.

Figura 4: Principais problemas de segurança na IoT

Fonte: SICARI *et al.*, 2015

Neste contexto, vamos definir a criptografia, que é a ferramenta mais importante para a segurança da informação. Vale ressaltar que a confidencialidade e a integridade das informações podem ser alcançadas por meio da criptografia. Embora foram mencionados todos os problemas de segurança na IoT, este artigo tratará apenas da confidencialidade e integridade, através de exemplos de criptografia das informações sensíveis.

A palavra criptografia vem do grego *kryptós* (esconder) e *grápho* (escrita) e ao contrário do que parece é uma ciência muito antiga e foi amplamente utilizada pelos militares, em tempos de guerra, para evitar que pessoas não autorizadas descobrissem suas estratégias de combate e defesa.

Criptografia é o conjunto de métodos para codificar a escrita utilizando uma chave de acesso, transformando-a em um texto incompreensível, chamado de texto-cifra, para garantir a segurança do canal de comunicação e de seu conteúdo. Faz parte de uma área mais extensa conhecida como criptologia. Esse campo de estudo evoluiu para a utilização de conceitos matemáticos como métodos de embaralhamento. (TALBOT; WELSH, 2006)

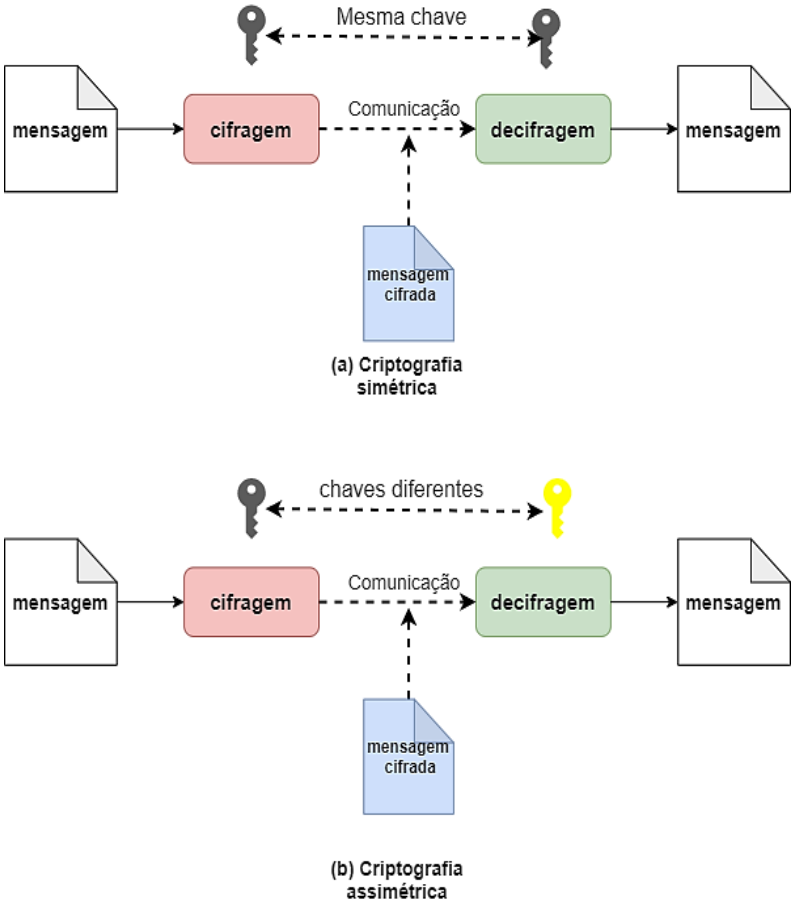
Material e Métodos

Neste trabalho foram estudados métodos de criptografia das informações sensíveis e nesta seção serão conceituados os procedimentos de cifragem de informações sensíveis mais utilizados em segurança de dados, quais são: RSA, ECC, AES e SHA, com exemplificações simples de uso em uma infraestrutura IoT.

O princípio criptográfico é bastante simples: um emissor deseja enviar uma mensagem a um destinatário de maneira segura. Utilizando um método secreto, referido como **chave**, ele embaralha a informação de sua mensagem, transformando-a em um **texto cifrado** e a envia utilizando o canal de comunicação que desejado. O seu receptor, recebe a mensagem. A partir daí, diverge-se o tipo de encriptação baseado na chave que ele possui. Se a chave que é usada para decriptar o texto-cifra em informação compreensível for a mesma que o emissor usou, esse sistema é conhecido como **simétrico**.

Caso contrário, se a chave utilizada para decifrar o texto é diferente da chave usada pelo emissário da mensagem, esse sistema é conhecido como **assimétrico**, o qual é classificado através do tipo de chave utilizada: **privada ou pública**. Chaves públicas são chaves conhecidas por todos os envolvidos naquela comunicação, já as chaves privadas têm o seu segredo restrito ao receptor da mensagem (TALBOT; WELSH, 2006, adaptado). A figura 5 ilustra o mecanismo da criptografia simétrica e assimétrica.

Figura 5: Diagrama de tipos de criptografias



Fonte: MACORATTI, 2016

No contexto da IoT, um sensor após uma varredura, recolhe os dados que ele inferiu, junto com outros dados que sejam úteis para os demais objetos e em sua unidade de processamento, utilizando uma chave, criptografa a mensagem produzida e a manda pela rede da aplicação. Em outro ponto dessa rede, o processo computacional do servidor pega essa cifra e utilizando do mesmo ou um método próprio decripta essa informação e a utiliza para a tomada de decisões ou despacho de serviços.

Métodos e protocolos criptográficos já vem sendo utilizados há décadas na informática e tecnologia de informação para assegurar que informações sensíveis não caiam na mão de indivíduos com más intenções ou sem a devida autorização para visualização daqueles dados (CARRACEDO *et al.;* 2018). Embora, com o avançar do estudo da área da Criptologia, novas implementações e ferramentas foram descobertas, utilizando conhecimento de outras áreas da ciência, como a mecânica quântica para a geração de chaves, conhecido como método quântico. No entanto, outros meios de criptografar foram criados e adotados através da anexação de bibliotecas em códigos e o uso de funções *hash* na área da ciência da computação.

Através de uma coletânea de artigos científicos, foram analisadas quatro técnicas de criptografia de dados. Os critérios de escolha foram o frequente uso destes algoritmos por pesquisadores da área e sua complexidade em implementação. No entanto é necessário reforçar que os objetos de estudo não são os métodos mais recentes de criptografia, mas são arcabouços nas tecnologias implementadas e pesquisadas atualmente para IoT.

Métodos Assimétricos:

A. RSA (Rivest–Shamir–Adleman): O método mais difundido de aplicação criptográfica em aplicações. Seu algoritmo baseia-se na geração de chaves públicas da fatoração de dois números primos (IRELAND, 2012) com o tamanho máximo de 4 kB. Devido sua natureza, a geração de chaves para criptografar a mensagem pode ser utilizada como um método de assinatura digital.

B. ECC (Curva de Crescimento Elíptico): Segundo Carracedo *et al*. (2018), é um tipo de criptografia que se baseia a geração de chaves públicas na estrutura algébrica de curvas elípticas em planos finitos. ECC acaba gerando chaves menores do que os demais métodos assimétricos.

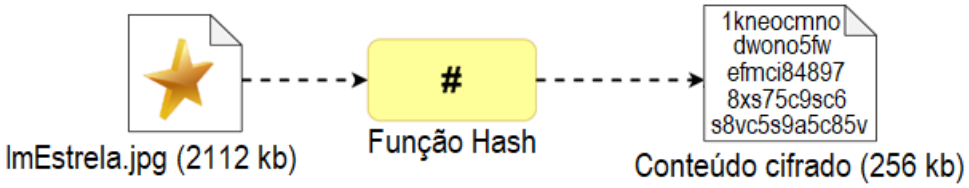
Método Simétrico:

AES (Advanced Encryption Standard): Cifra que utiliza de permutação e combinação de blocos de bits através de chaves públicas de tamanhos variados. É um subconjunto de outra cifra, Rijndael, um amálgama entre os sobrenomes dos criadores (Rijmen e Daemen) e seu desempenho, segundo os criadores, é rápido em softwares e hardwares.

Métodos Quânticos ou pós-quânticos:

SHA (Secure Hash Algorithms): Uma família de algoritmos de cifragem e decifragem que utilizam de funções hash, que são funções que mapeiam dados de tamanho arbitrários para um tamanho fixo, na geração e análise de textos cifrados, conforme ilustra a figura 6.

Figura 6: Diagrama de uma Função Hash



Fonte: ROSENBAUM, 2017

Resultados e Discussão

Os métodos criptográficos em aplicações IoT devem ser pensados conforme a arquitetura utilizada e qual é o seu objetivo dentro daquele processo. Além disso, devem ser adaptados às diferentes circunstâncias em que a solução foi implantada. Métodos que garantem a segurança de uma assinatura digital, como RSA, podem ser utilizados em instrumentos que necessitem de unicidade, como sensores e/ou identificadores de baixo consumo energético, como as etiquetas RFID. (AL-FUQAHA *et at.*, 2015)

Na área de serviços, por envolverem softwares e hardwares com maior poder computacional e decisões a serem tomadas, gerando uma maior quantidade de dados para serem sincronizados, métodos como ECC ou AES podem gerar economia de recursos (SINGH; SINGH, 2015), aumentando o rendimento através da melhor integração de software-hardware e garantir uma diminuição na latência na parte de comunicação, aumentando a velocidade de acesso em uma banda de internet limitada.

Também, a utilização de algum método de SHA pode assegurar que o conhecimento gerado e acessado pelos usuários da aplicação através dos serviços e interfaces disponíveis em navegadores, aplicativos para *smartphones e tablets* esteja de acordo com as normas e padrões de segurança utilizados em aplicações mais tradicionais. Segundo recomendação do *National Institute of Standards and Technology* (2015) aplicações federais americanas devem utilizar subfamílias do SHA mais especificamente, SHA-2 e SHA-3, para garantir a segurança de dados, prática que foi adotada depois por empresas como Google, em 2017. (PROTALINSKI, 2016)

Singh e Singh (2015) define que soluções IoT devem ser pensadas como soluções de baixo consumo a fim de sua continuidade de uso e popularização. No entanto, soluções criptográficas mais tradicionais não são adequadas para o baixo nível de uma aplicação IoT, pois não respeitam as capacidades de hardware e software de aparelhos. Uma solução foi proposta para esse tipo de problema: a “criptografia leve”.

Sugerida por Dhanda *et al.* (2020), a “criptografia leve” enfatiza sua utilização em dispositivos que não possuem alta capacidade de processamento e armazenamento, ainda levando em consideração os aspectos que a implementação IoT precisa alcançar para ser uma solução bem-sucedida.

Conclusão

Foram apresentados de maneira simples e abrangente conceitos, teorias e breves exemplos de aplicações do paradigma tecnológico conhecido como Internet das Coisas (IoT) e foram mencionados conceitos de segurança da informação e a utilização de criptografia de acordo com a necessidade estrutural nessas aplicações.

IoT é um paradigma computacional recente, vasto em oportunidades econômicas, capacidade de melhorar a qualidade de vida humana, mas essas possibilidades são dependentes do quão seguro uma implementação IoT pode ser, para isso é necessário conhecer suas limitações, arquiteturas e melhores protocolos de segurança, com o objetivo de gerar confiança e privacidade para seus usuários.

Referências

AL-FUQAHA, A. *et al.* **Internet of Things:** A Survey on Enabling Technologies, Protocols and Applications. IEEE Communications Surveys & Tutorials, [*s. l.*], v. 17, ed. 4, p. 2347-2376, 15 jun. 2015. DOI 10.1109/COMST.2015.2444095. Disponível em: <https://ieeexplore.ieee.org/document/7123563>. Acesso em: 3 de jun. de 2020.

CARRACEDO, J.M. *et al.* Cryptography for Security in IoT. 2018. **Fifth International Conference on Internet of Things**: Systems, Management and Security (IoTSMS), [*s. l.*], p. 23-30, 2018. DOI 10.1109/IoTSMS.2018.8554634. Disponível em: <https://ieeexplore.ieee.org/ document/8554634>. Acesso em: 3 de jun. de 2020.

DHANDA, S.S.; SINGH, B.; JINDAL, P. **Lightweight Cryptography:** A Solution to Secure IoT. Wirelles Pers Commun 112, 1947-1980. Disponível em: <https://doi.org/10.1007/s11277-020-07134-3>. Acesso em: 11 de jun. de 2020.

HENRIQUES, M.S.; VERNEKAR, N.K. **Using Symmetric and Asymmetric Cryptography to Secure Communication between Devices in IoT.** IoT and Application (ICIOT), International Conference on, [*s. l.*], 2017. DOI 10.1109/ICIOTA.2017.8073643. Disponível em: <https://ieeexplore.ieee.org/document/8073643>. Acesso em: 3 de jun. de 2020.

IRELAND, D. RSA Algorithm. In: DI MANAGEMENT (Austrália). **RSA Algorithm**. [*s. l.*], 2012. Disponível em: <https://www.di-mgt.com.au/rsa_alg.html>. Acesso em: 4 de jun. de 2020.

LEITE, J.R.E.; MARTINS, P.S.; URSINI, E. **A Internet das Coisas (IoT):** Tecnologias e Aplicações. In: BRAZILIAN TECHNOLOGY SYMPOSIUM, 2017, Campinas - São Paulo. Proceedings [...]. [*s. l.: s. n.*], 2017. DOI ISSN 2447-8326. Disponível em: <http://lcv.fee.unicamp.br/images/BTSym-17/Papers/76926.pdf>. Acesso em: 2 de jun. de 2020.

MACORATTI, J.C. **Net_cripto31.png.** 2016. 1 imagem png. Disponível em: <http://www.macoratti.net/16/09/net_cripto31.png>. Acesso em: 9 de jun. de 2020.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (EUA). **NIST Policy on Hash Functions.** In: NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (EUA). Hash Functions. [*s. l.*], 15 ago. 2015. Disponível em: <https://csrc.nist.gov/Projects/Hash-Functions/NIST-Policy-on-Hash-Functions>. Acesso em: 9 de jun. de 2020.

OPEN WEB APPLICATIONS SECURITY PROJECT. **OWASP Internet of Things Project.** In: OWASP wiki. OWASP Internet of Things (IoT) Project. [*s. l.*], 2018. Disponível em: <https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project>. Acesso em: 1 de jun. de 2020.

PROTALINSKI, E. **Google will drop SHA-1 encryption from Chrome by January 1, 2017.** In: PROTALINSKI, Emil. Google will drop SHA-1 encryption from Chrome by January 1, 2017. Venturebeat, 18 dez. 2015. Disponível em: <https://venturebeat.com/2015/12/18/google-will-drop-sha-1-encryption-from-chrome-by-january-1-2017/>. Acesso em: 9 de jun. de 2020.

SANTOS, B.P. *et al.* **Internet das Coisas:** da Teoria à Prática. [*s. l.: s. n.*], 2016. Disponível em: <https://homepages.dcc.ufmg.br/~mmvieira/cc/papers/internet-das-coisas.pdf>. Acesso em: 1 de jun. de 2020.

SÊMOLA, M. **Gestão da segurança da informação:** uma visão executiva. 2. ed. Rio de Janeiro: Elsevier, 2014. 171 p. ISBN 9788535271782.

SICARI, S. *et al.* **Security, privacy and trust in Internet of Things:** The road ahead. Elsevier, Itália, 2015. DOI 76. 10.1016/j.comnet.2014.11.008. Disponível em: <https://www.researchgate.net/publication/270107935_Security_privacy_and_trust_in_Internet_of_Things_The_road_ahead>. Acesso em: 2 de jun. de 2020.

SINGH, S.; SINGH, N. **Internet of Things (IoT):** Security Challenges, Business Opportunities & Reference Architecture for E-commerce. 2015 International Conference on Green Computing and Internet of Things (ICGCIoT), 2015. DOI 10.1109/ICGCIoT.2015.7380718. Disponível em: <https://ieeexplore.ieee.org/document/7380718>. Acesso em: 3 de jun. de 2020.

SKLAVOS, N.; ZAHARAKIS, I.D. **Cryptography and Security in Internet of Things (IoTs):** Models, Schemes, and Implementations. 2016 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS), 4 jun. 2020. DOI 10.1109/NTMS.2016.7792443. Disponível em: <https://ieeexplore.ieee.org/document/7792443>. Acesso em: 4 de jun. de 2020.

ROSENBAUM, K. **Cat picture.** 26 jun. 2017. 1 desenho. Disponível em: <https://freecontent.manning.com/cryptographic-hashes-and-bitcoin/>. Acesso em: 10 de jun. de 2020.

TALBOT, J; WELSH, D. **Basics of cryptography:** A basic scenario: cryptosystems. In: TALBOT, John; WELSH, Dominic. Complexity and Cryptography an Introduction. 1. ed. Estados Unidos: Cambridge University Press, 2006. cap. 1, p. 3-7. ISBN 0-511-14070-3. E-book.