Revista Científica UNAR (ISSN 1982-4920), Araras (SP), v.24, n.2, p.01-11, 2023.
DOI: 10.18762/1982-4920.20230013

Comparação entre a Arquitetura Serverless e a Arquitetura Tradicional

Igor L. S.da Silva Moreira, Vinicius P. Ferreira Barreto, Wdson de Oliveira

Resumo

Nas últimas décadas, a arquitetura serverless tem ganhado destaque como uma alternativa inovadora às abordagens tradicionais de desenvolvimento de software, especialmente no contexto de computação em nuvem. Este estudo aborda a transição da arquitetura tradicional, baseada em servidores físicos ou virtuais, para a arquitetura serverless, onde aplicativos são executados em serviços gerenciados por provedores de nuvem. A principal vantagem da arquitetura serverless reside na sua capacidade de proporcionar escalabilidade automática, reduzindo custos e simplificando o gerenciamento de recursos. Além disso, a segurança da informação é analisada em profundidade, destacando como a adoção da arquitetura serverless pode aprimorar a proteção dos dados, uma vez que a responsabilidade pela segurança recai sobre os provedores de nuvem. O estudo também enfatiza a importância de uma análise detalhada das implicações de segurança, escalabilidade e custos ao decidir entre essas arquiteturas. A plataforma AWS é utilizada como referência. Em um ambiente empresarial cada vez mais centrado na nuvem, compreender as nuances das arquiteturas serverless e tradicionais é crucial para a tomada de decisões informadas sobre a segurança da informação e eficiência dos recursos de TI.

Palavras-chave: Arquitetura Serverless, Arquitetura Tradicional, Segurança da Informação, AWS, Escalabilidade, Custos.

Abstract

In recent years, serverless architecture has emerged as an innovative alternative to traditional software architectures, particularly in the realm of cloud computing. This study explores the transition from traditional architecture, relying on physical or virtual servers, to serverless architecture, where applications run on managed services provided by cloud providers. The primary advantage of serverless architecture lies in its ability to provide automatic scalability, reducing costs, and simplifying resource management. Furthermore, this study delves into information security, highlighting how the adoption of serverless architecture can enhance data protection, as security responsibilities shift to cloud providers. The study also underscores the importance of a detailed analysis of security, scalability, and costs when deciding between these architectures. The AWS platform is used as a reference point. In an increasingly cloud-centric corporate environment, understanding the nuances of serverless and traditional architectures is crucial for making informed decisions regarding information security and IT resource efficiency.

Keywords: Serverless Architecture, Traditional Architecture, Information Security, AWS, Scalability, Costs.

1 Introdução

Nos últimos anos, a arquitetura serverless emergiu como uma alternativa inovadora para as arquiteturas tradicionais de software. A arquitetura tradicional de software é baseada em servidores físicos ou virtuais, onde os aplicativos são executados em instâncias de servidores dedicados. Nessa abordagem, os servidores precisam estar em funcionamento continuamente, mesmo quando não estão sendo utilizados, o que pode levar a custos desnecessários.

Por outro lado, na arquitetura serverless, os aplicativos são executados em serviços em nuvem gerenciados por provedores de nuvem, como a Amazon Web Services, Microsoft Azure e Google Cloud Platform. O termo "serverless" pode levar a um entendimento equivocado, já que os aplicativos ainda precisam ser executados em servidores, mas o gerenciamento desses servidores é realizado pelo provedor de nuvem, eliminando a necessidade de gerenciamento e manutenção dos servidores pelos desenvolvedores.

Essa abordagem também oferece escalabilidade automática, em que os recursos são alocados dinamicamente para atender à demanda do aplicativo. Quando há um pico de tráfego, os recursos são aumentados automaticamente para atender à demanda, e quando a demanda diminui, os recursos são reduzidos para economizar custos. Isso torna a arquitetura serverless muito mais flexível do que a arquitetura tradicional.

Além disso, a arquitetura serverless também pode oferecer uma abordagem mais segura para a segurança da informação. Com a arquitetura tradicional, os desenvolvedores precisam gerenciar a segurança dos servidores, o que pode ser uma tarefa desafiadora. Por outro lado, com a arquitetura serverless, a segurança é gerenciada pelo provedor de nuvem, que possui recursos especializados e equipe dedicada para garantir a segurança da plataforma.

No entanto, como com qualquer tecnologia, há vantagens e desvantagens em ambas as abordagens, e a decisão de escolher uma ou outra deve levar em consideração as necessidades específicas de cada aplicativo. Este projeto tem como objetivo analisar essas diferenças com mais detalhes, oferecendo uma comparação detalhada entre a arquitetura serverless e a arquitetura tradicional, incluindo as diferenças em termos de escalabilidade, custos e gerenciamento de recursos, inclusive explorando como a arquitetura serverless pode ser usada para melhorar a segurança da informação.

A segurança da informação é uma preocupação constante em projetos de software e a arquitetura serverless pode oferecer benefícios significativos nessa área. Com a arquitetura serverless, a segurança é gerenciada pelo provedor de nuvem, o que elimina a necessidade de gerenciamento e manutenção dos servidores pelos desenvolvedores. Além disso, os provedores de nuvem geralmente oferecem recursos de segurança robustos, como proteção contra ataques DDoS (Distributed Denial of Service ou Negação Distribuída de Serviço), criptografia de dados e monitoramento constante de segurança.

A AWS, provedora de serviços em nuvem líder no mercado, tem investido em

soluções e ferramentas de segurança para arquiteturas serverless, incluindo a proteção contra-ataques DDoS e a criptografia de dados. Além disso, a arquitetura serverless oferece a possibilidade de executar funções apenas quando necessário, minimizando a superfície de ataque e reduzindo o tempo de exposição a possíveis ameaças.

Ainda assim, é fundamental avaliar as implicações de segurança da informação na adoção de arquiteturas serverless em comparação com arquiteturas tradicionais. Para isso, é necessário realizar uma comparação detalhada entre as duas arquiteturas, com foco em segurança da informação. Essa comparação incluirá a análise das diferenças em termos de escalabilidade, custos e gerenciamento de recursos.

Diante disso, a problemática deste projeto consiste em analisar e comparar a segurança da informação nas arquiteturas serverless e tradicionais, com foco na plataforma AWS. O objetivo é entender as diferenças entre as arquiteturas e como a adoção de arquiteturas serverless pode contribuir para a melhoria da segurança da informação em relação às arquiteturas tradicionais.

Com a crescente adoção de tecnologias baseadas em nuvem, a segurança da informação tornou-se uma das principais preocupações das empresas. A arquitetura serverless tem sido apresentada como uma alternativa para melhorar a segurança em ambientes de Tecnologia da Informação (TI), pois é capaz de isolar as funções executadas, reduzindo a superfície de ataque e fornecendo um ambiente mais seguro para a execução de código. Além disso, a arquitetura serverless pode ser facilmente integrada com serviços de segurança de nuvem, como firewalls e serviços de autenticação, fornecendo uma camada adicional de segurança para a aplicação.

No entanto, ainda há uma falta de compreensão sobre como a arquitetura serverless pode melhorar a segurança da informação em comparação com a arquitetura tradicional. Este projeto justifica-se pela necessidade de avaliar as diferenças entre as duas arquiteturas em termos de segurança da informação, a fim de fornecer insights para a tomada de decisões em relação à escolha da arquitetura mais adequada para ambientes corporativos que lidam com informações críticas.

Este trabalho teve como objetivo principal a realização de uma comparação detalhada entre a arquitetura serverless e a arquitetura tradicional, com foco na segurança da informação. Dessa forma, busca-se avaliar como cada uma dessas arquiteturas pode contribuir para a melhoria da segurança dos sistemas de informação, especialmente em ambientes corporativos, onde a proteção dos dados é essencial.

Outro objetivo deste trabalho é analisar as diferenças em termos de escalabilidade, custos e gerenciamento de recursos entre as duas arquiteturas. Com base nessa análise, será possível identificar as principais vantagens e desvantagens de cada uma delas, e avaliar em que medida a adoção da arquitetura serverless pode trazer benefícios para a segurança da informação, sem comprometer a eficiência e a economia de recursos.

Por fim, este trabalho pretende contribuir para o avanço do conhecimento sobre as arquiteturas serverless e tradicional, em especial no que se refere à sua relação com a segurança da informação. Espera-se que os resultados obtidos possam ser úteis para profissionais da área de tecnologia da informação, gestores de empresas e pesquisadores interessados em aprimorar a segurança dos sistemas de informação em seus respectivos contextos.

2 Referencial Teórico

Este projeto é composto por três seções principais, que apresentam uma discussão sobre segurança da informação e as arquiteturas tradicionais e *serverless*, além de uma análise comparativa das duas arquiteturas em termos de segurança.

Na primeira seção, foram abordados os fundamentos da segurança da informação, incluindo a importância de se ter um sistema de computação seguro e confiável. Segundo (MATTORD & WHITMAN, 2018, p. 130),a segurança da informação envolve a proteção dos ativos de informação contra ameaças, como ataques DDoS e invasões de rede. Uma arquitetura segura é essencial para mitigar essas ameaças.

A segunda seção discute os conceitos fundamentais das arquiteturas tradicionais e serverless, incluindo suas principais características e funcionalidades. Foram apresentados exemplos de casos de uso em ambas as arquiteturas e as diferenças em termos de escalabilidade, custos e gerenciamento de recursos.

Por fim, a terceira seção apresenta uma análise comparativa das duas arquiteturas em termos de segurança da informação. Foram discutidos os recursos de segurança disponíveis em cada uma das arquiteturas, incluindo proteção contra-ataques DDoS e criptografia de dados. De acordo com (HOFFMAN, SCARFONE, & SOUPPAYA, 2011, p. 16), “A arquitetura serverless pode oferecer benefícios em termos de segurança devido ao modelo de execução por demanda e menor superfície de ataque”. No entanto, também existem desafios relacionados à confiança e à dependência de provedores de serviços.

A análise comparativa foi feita com base em informações e dados coletados em pesquisas anteriores sobre as duas arquiteturas, bem como nas próprias experiências do autor.

2.1 Fundamentos da Segurança da Informação

A segurança da informação é um elemento crucial em qualquer sistema de computação, uma vez que dados sensíveis e confidenciais estão armazenados e processados nesses sistemas. É essencial garantir que esses dados estejam protegidos contra ameaças, tais como invasões de rede e ataques DDoS, que podem resultar em vazamento de informações, perda de dados e danos à reputação da organização.

Podemos definir a segurança da informação como o processo de proteger a informação de divulgação não autorizada, uso indevido, alteração ou descrição, seja em formato eletrônico ou físico (MATTORD & WHITMAN, 2021). Nesse contexto, a

implementação de uma arquitetura segura é fundamental para prevenir e mitigar essas ameaças.

Uma das principais formas de prevenção de tais ameaças é através de uma arquitetura segura e confiável. A arquitetura segura é a estrutura subjacente que dá suporte à segurança de um sistema de computação e inclui políticas, procedimentos e mecanismos de segurança.

A implementação de uma arquitetura segura envolve a adoção de diversas medidas de segurança. Segundo (BROWM & STALLINGS, 2017), essas medidas podem incluir a utilização de firewalls, sistemas de detecção de intrusão, sistemas de criptografia, controle de acesso, entre outros.

Além disso, é importante garantir que os funcionários que acessam o sistema estejam cientes da importância da segurança da informação e saibam como agir em caso de incidentes. Conforme ressaltado por (MATTORD & WHITMAN, 2021, p. 76), "a conscientização dos usuários é uma das defesas mais importantes para garantir a segurança da informação".

Dentre as ameaças à segurança da informação, os ataques DDoS são um dos mais comuns. Um ataque DDoS ocorre quando um grande número de sistemas de computadores distribuídos é usado para inundar um alvo específico com um grande volume de tráfego. Para prevenir esses tipos de ataques, é necessário implementar medidas de proteção, tais como sistemas de mitigação de DDoS e redes de distribuição de conteúdo.

Outra ameaça comum à segurança da informação é a invasão de rede, que envolve um atacante que acessa a rede de computadores da organização sem autorização. Conforme mencionado por (MATTORD & WHITMAN, 2021, p. 98), "Os ataques de invasão de rede podem ser lançados de dentro ou de fora da organização". Para prevenir esse tipo de ameaça, são necessárias medidas de proteção, tais como firewalls, sistemas de autenticação e autorização, e sistemas de detecção de intrusão.

Em resumo, a segurança da informação é um elemento crucial em qualquer sistema de computação. Para garantir a proteção contra ameaças, é necessário implementar uma arquitetura segura e confiável, além de garantir a conscientização dos usuários do sistema e a implementação de medidas de proteção contra ameaças comuns, como ataques DDoS e invasões de rede.

2.2 Fundamentos da Arquitetura Tradicional

A arquitetura tradicional é caracterizada por ter um servidor central que gerencia e coordena todas as atividades do sistema. Esse servidor é responsável por receber as solicitações dos clientes e processá-las, retornando as respostas correspondentes. Além disso, a arquitetura tradicional é baseada em uma comunicação síncrona, ou seja, o cliente deve esperar pela resposta do servidor antes de continuar sua execução. (SOMMERVILLE, 2011)

De acordo com (NAKAGAWA, 2006) uma arquitetura de software tem sido

largamente reconhecida na literatura como um dos principais habilitadores em proporcionar ganhos efetivos em agilidade e eficiência na manutenção e evolução dos sistemas.

Essa arquitetura se baseia na necessidade da configuração de escalabilidade de mais máquinas quando haver mais acessos, configuração de segurança e proteção conta invasões e ataques de DDoS, o que em muitos casos há a necessidade de uma ou mais pessoas envolvidas apenas para gerir e cuidar desses processos; com isso dependendo da demanda e do uso pode-se haver problemas envolvendo desempenho e instabilidade.

De acordo com a pesquisa realizada, a configuração de segurança é uma das principais preocupações em arquiteturas de software, especialmente em relação à proteção contra invasões e ataques cibernéticos. Uma arquitetura flexível de segurança para compartilhamento de contexto em Internet das Coisas, por exemplo, é uma solução que pode ser aplicada em diferentes contextos para garantir a segurança dos dados e informações (MARTINS JÚNIOR, 2022, p. 54). Além disso, a migração de sistemas monolíticos para microsserviços pode ser uma alternativa para garantir a segurança e proteção contra invasões, uma vez que permite menos pontos de falhas e tentativas de invasões. (OLIVEIRA PAULA, 2022, p. 40)

Outra questão importante é a escalabilidade, que pode ser alcançada por meio da configuração de mais máquinas quando houver mais acessos. No entanto, é importante considerar que a escalabilidade pode levar a problemas de desempenho e instabilidade, especialmente em sistemas com alta carga de trabalho. Por isso, é fundamental avaliar cuidadosamente a demanda e o uso do sistema antes de configurar a escalabilidade

Por fim, a proteção contra-ataques de DDoS é outra preocupação importante em arquiteturas de software. “Uma arquitetura de desenvolvimento adaptada contra ataques cibernéticos, por exemplo, é uma solução que pode ser aplicada nas demais arquiteturas para garantir a proteção contra-ataques de DDoS”. (POUW, 1999, p. 21)

2.3 Fundamentos da Arquitetura Serverless

A arquitetura de sistemas de computação desempenha um papel fundamental na determinação do desempenho, escalabilidade e eficiência das aplicações. Entre as abordagens arquiteturais, a serverless, também conhecida como sem servidor, emerge como uma revolução na computação em nuvem. Nesse modelo, a infraestrutura é fornecida pelo provedor de serviços em nuvem, permitindo que os desenvolvedores se concentrem exclusivamente na lógica da aplicação.

Conforme (CHATLEY & GOJKO, 2017, p. 1) destacam em seu artigo, "Em uma arquitetura tradicional, a aplicação é executada em um único servidor físico ou virtual". Nessa configuração, a aplicação é dividida em módulos, cada um executado em um servidor separado. No entanto, essa abordagem pode apresentar desafios significativos em termos de gerenciamento de recursos e escalabilidade.

As arquiteturas serverless são projetadas para superar esses desafios de maneira elegante. Nesse modelo, a infraestrutura é gerenciada pelo provedor de serviços em nuvem, e a aplicação é executada em uma rede de servidores distribuídos. O provedor de serviços em nuvem lida com a escalabilidade de forma automática, ajustando dinamicamente os recursos disponíveis de acordo com a demanda da aplicação.

Uma das características mais notáveis das arquiteturas serverless é a facilidade de escalabilidade. Em um ambiente serverless, a aplicação pode escalar horizontalmente de maneira automática, adicionando novas instâncias em resposta ao aumento da carga de trabalho. Isso não apenas otimiza a utilização de recursos, mas também evita problemas de desempenho em momentos de tráfego intenso.

Além disso, as arquiteturas serverless são reconhecidas por sua alta disponibilidade e tolerância a falhas. Os provedores de serviços em nuvem distribuem a carga de trabalho em diversos servidores, garantindo que a aplicação continue funcionando mesmo em caso de falha de um servidor. Isso é particularmente crucial em aplicações críticas, onde a disponibilidade contínua é essencial.

2.4 Análise comparativa entre a arquitetura tradicional e arquitetura serverless

A arquitetura tradicional apresenta limitações significativas quando se trata de segurança e eficiência. A abordagem tradicional é centralizada, com um servidor principal que gerencia todas as operações, o que pode resultar em pontos únicos de falha e desafios na escalabilidade. A configuração e manutenção de medidas de segurança, como firewalls e sistemas de detecção de intrusão, podem ser complexas e dispendiosas. A infraestrutura centralizada, incluindo servidores e hardware, pode gerar custos significativos de manutenção e operação.

Por outro lado, a arquitetura serverless surge como a escolha superior em diversas frentes, especialmente em segurança da informação (RAWAT & REDDY, 2017). Na arquitetura serverless, os recursos são alocados apenas quando necessários, reduzindo drasticamente a superfície de ataque, uma vez que os servidores não ficam permanentemente expostos à internet. As funções serverless são independentes e executadas em servidores distribuídos, o que significa que a falha de um servidor não afeta a aplicação como um todo, aumentando a tolerância a falhas e garantindo a continuidade do serviço. A escalabilidade é uma característica intrínseca da arquitetura serverless, e a infraestrutura se adapta automaticamente às flutuações na carga de trabalho, melhorando o desempenho e a disponibilidade. A alocação de recursos apenas durante a execução de funções resulta em custos mais baixos, já que não há necessidade de manter servidores ociosos.

Além das vantagens de segurança, a arquitetura serverless também oferece eficiência operacional (RAWAT & REDDY, 2017). A gestão de recursos é tratada pelo provedor de serviços em nuvem, reduzindo a complexidade operacional para as equipes de TI. A escalabilidade automática elimina a necessidade de planejamento detalhado e configuração manual, economizando tempo e recursos.

Desenvolvedores podem se concentrar exclusivamente na lógica da aplicação, sem se preocupar com a infraestrutura subjacente (RAWAT & REDDY, 2017).

Em resumo, a análise comparativa deixa claro que a arquitetura serverless é a escolha superior em termos de segurança da informação e eficiência operacional. Sua natureza sob demanda, tolerância a falhas aprimorada, escalabilidade automática e redução de custos fazem dela a opção preferida para ambientes seguros e eficientes nas aplicações modernas (RAWAT & REDDY, 2017). Embora a arquitetura tradicional ainda tenha seu lugar em cenários específicos, a arquitetura serverless está na vanguarda da inovação tecnológica e da segurança da informação.

3 Metodologia

Para atingir os objetivos propostos, foi realizada uma pesquisa bibliográfica com base em artigos, livros, relatórios técnicos e documentação oficial fornecida pela AWS. A pesquisa foi realizada em fontes confiáveis e relevantes, visando obter informações precisas e atualizadas sobre as arquiteturas tradicional e *serverless*, bem como sobre as práticas de segurança relacionadas a cada uma delas.

Foi feita uma análise comparativa entre as duas arquiteturas, abordando as diferenças em termos de escalabilidade, custos e gerenciamento de recursos, com foco principal na segurança da informação. Para isso, foram utilizados critérios pré-definidos, como a confidencialidade, integridade e disponibilidade dos dados.

Além disso, foram analisadas as práticas de segurança específicas da arquitetura *serverless*, como a proteção contra-ataques DDoS e a criptografia de dados, a fim de avaliar como essa arquitetura pode melhorar a segurança da informação em comparação com a arquitetura tradicional.

Foi utilizada uma abordagem metodológica qualitativa, que permitirá a análise crítica e a interpretação dos dados coletados, a fim de atingir os objetivos propostos.

4 Resultado e discussão

A pesquisa e análise comparativa entre as arquiteturas tradicional e serverless revela diferenças significativas em termos de segurança da informação e eficiência operacional. Na arquitetura tradicional, a centralização das operações em um servidor único apresenta desafios, como pontos únicos de falha e configuração complexa de segurança. Além disso, ataques DDoS representam ameaças importantes.

Por outro lado, a arquitetura serverless melhora a segurança ao alocar recursos apenas quando necessários, reduzindo a superfície de ataque. Sua execução em servidores distribuídos aumenta a tolerância a falhas, garantindo a continuidade do serviço. Provedores de serviços em nuvem, como a AWS, oferecem recursos de segurança robustos, incluindo proteção contra ataques DDoS e criptografia de dados.

Em termos de eficiência operacional, a arquitetura tradicional requer

configuração manual e planejamento detalhado, gerando custos significativos. A arquitetura serverless simplifica a gestão de recursos, escalabilidade automática e permite que os desenvolvedores se concentrem apenas na lógica da aplicação, economizando tempo e recursos.

Concluindo, a arquitetura serverless destaca-se como uma escolha preferida para ambientes seguros e eficientes, embora a arquitetura tradicional possa ser relevante em cenários específicos. Essa análise destaca a importância da segurança da informação e eficiência operacional na tomada de decisões relacionadas à arquitetura de sistemas de computação.

5 Considerações finais

A análise das arquiteturas tradicional e serverless no contexto da segurança da informação e eficiência operacional revela a importância de escolher a abordagem adequada para cada aplicativo e organização. A arquitetura serverless se destaca por oferecer uma série de benefícios, como redução da superfície de ataque, escalabilidade automática e custos mais baixos, devido à alocação de recursos apenas quando necessários. Além disso, provedores de serviços em nuvem oferecem recursos de segurança robustos.

Por outro lado, a arquitetura tradicional ainda pode ser relevante em cenários específicos, mas apresenta desafios, como configuração manual complexa, pontos únicos de falha e custos de manutenção elevados.

É fundamental reconhecer que a segurança da informação é uma prioridade inquestionável em qualquer ambiente de computação, e a escolha da arquitetura deve levar em conta as necessidades específicas de cada aplicativo e organização. Em última análise, a pesquisa destaca a importância de uma abordagem proativa para garantir a segurança da informação e a eficiência operacional na arquitetura de desenvolvimento.

REFERÊNCIAS

BROWM, L., & STALLINGS, W. (2017). *Computer Security: Principles and Practice 4th Edition.* Pearson.

CHATLEY, R., & GOJKO, A. (2017). Serverless Computing: Economic and Architectural Impact. *Proceedings of the 2017 11th Joint Meeting on Foundations of Software Engineering*, 884-889. Acesso em 23 de Setembro de 2023, disponível em Site da Imperial College London: https://www.doc.ic.ac.uk/~rbc/papers/fse-serverless-17.pdf

HOFFMAN, P., SCARFONE, K., & SOUPPAYA, M. (2011). Guide to security for full virtualization. *NIST Special Publications*.

MARTINS JÚNIOR, F. C. (2022). *Uma arquitetura flexível de segurança para compartilhamento de contexto em Internet das Coisas.* Fortaleza: Universidade Federal do Ceará.

MATTORD, H., & WHITMAN, M. (2018). *Management of Information Security.* Cengage Learning.

MATTORD, H., & WHITMAN, M. (2021). *Principles of Information Security 7th Edition.* Principles of Information Security 7th Edition.

NAKAGAWA, E. Y. (2006). *Uma contribuição ao Projeto Arquitetal de Ambientes de Engenharia de Software.* São Carlos: Universidade de São Paulo - USP.

OLIVEIRA PAULA, A. (2022). *Uma arquitetura de automação adaptada para Smart Grids contra ataques cibernéticos.* Brasília: Faculdade de Tecnologia, Universidade de Brasília.

POUW, K. D. (1999). *Segurança na arquitetura TCP/IP: de firewalls a canais seguros.* Campinas: Instituto de Computação, Universidade Estadual de Campinas.

RAWAT, D., & REDDY, R. (2017). Software Defined Networking Architecture, Security and Energy Efficiency: A Survey. *IEEE Communications Surveys & Tutorials - Volume 19*, 325 - 346.

SOMMERVILLE, I. (2011). *Engenharia de Software; 9ª edição.* Pearson Universidades.