Proteção de Dados em Dispositivos Móveis: Implementação de um Sistema de Backup Automatizado com Network Attached Storage (NAS)

Camila Lopes[1], **Euller Silva**[2], **Felipe Silva**[3], **Pedro Costa**[4], **Victor Araujo**[5]

[1]ICEI – Pontifícia Universidade Católica de Minas Gerais

Resumo. *Este artigo propõe um sistema de backup automatizado baseado em um Network Attached Storage (NAS) para dispositivos móveis, com o objetivo de proteger os dados dos usuários contra perdas decorrentes de roubo, perda ou danos aos dispositivos. A solução sincronizará arquivos tanto com um NAS local quanto com um repositório na nuvem, utilizando a mesma rede Wi-Fi residencial para simplificar o processo. A metodologia de desenvolvimento envolve planejamento, design do sistema, implementação e avaliação. As limitações incluem a simulação em um computador pessoal, que pode afetar a escalabilidade e o desempenho, e a validação em um ambiente controlado. Apesar dessas restrições, o sistema proposto visa fornecer uma solução de backup confiável e conveniente para usuários preocupados com a segurança de dados.*

Abstract. *This paper proposes an automated backup system based on a Network Attached Storage (NAS) for mobile devices, aiming to protect users' data against loss due to theft, loss, or damage to their devices. The solution will synchronize files with both a local NAS and a cloud repository, utilizing the same home Wi-Fi network to simplify the process. The development methodology involves planning, system design, implementation and evaluation. Limitations include simulation on a personal computer, which may affect scalability and performance, and validation in a controlled environment. Despite these constraints, the proposed system aims to provide a reliable and convenient backup solution for users concerned about data security.*

1. Introdução:

No contexto atual, a segurança dos dados pessoais tornou-se uma preocupação crescente, especialmente diante do aumento dos casos de roubo e perda de dispositivos móveis no Brasil. Dessa forma, perante esse cenário, surge a necessidade de oferecer soluções que garantam a proteção e a disponibilidade dos dados dos usuários. Assim, este artigo propõe a criação de um sistema de backup automatizado baseado em um NAS (Network Attached Storage), que permite aos usuários armazenar e gerenciar seus arquivos de forma segura e conveniente.

1.1. Problema Identificado:

Os usuários enfrentam o risco de perder seus dados pessoais devido a roubo, perda ou danos aos dispositivos móveis, como smartphones e tablets. Ademais, muitos não realizam backups regulares de seus arquivos, o que os expõe a perdas irreparáveis em caso de incidentes.

1.2. Hipóteses de Solução:

A solução proposta consiste na implementação de um sistema de backup automatizado que sincronize os arquivos dos dispositivos móveis dos usuários com um NAS local e um repositório na nuvem. Ao utilizar a mesma rede Wi-Fi residencial, o processo de backup será simplificado e transparente para o usuário, garantindo a proteção contínua de seus dados.

1.3. Objetivos:

- Desenvolver um sistema de backup automatizado baseado em NAS para dispositivos móveis.
- Criar um aplicativo móvel intuitivo para gerenciar o processo de backup e recuperação de arquivos.
- Garantir a segurança e a disponibilidade dos dados dos usuários, minimizando os riscos de perda ou roubo de dispositivos móveis.

1.4. Estrutura do Artigo:

1. Introdução
2. Revisão Bibliográfica
3. Metodologia de Desenvolvimento e Avaliação
4. Limitações do Trabalho
5. Desenvolvimento do Trabalho
6. Trabalhos Futuros
7. Conclusões

2. Revisão Bibliográfica:

Para embasar o desenvolvimento do sistema de backup automatizado, é fundamental revisar conceitos e tecnologias relacionadas à arquitetura de computadores, redes de computadores e sistemas operacionais.

2.1. Arquitetura de Computadores:

- Estudo das estruturas internas dos computadores, incluindo processadores, memória e rmazenamento.
- Exploração de conceitos de armazenamento de dados, como discos rígidos e dispositivos de armazenamento em rede (NAS).

2.2. Redes de Computadores:

- Compreensão dos protocolos e tecnologias de redes utilizados para comunicação entre dispositivos, como Wi-Fi.
- Exploração de conceitos de segurança de redes para garantir a proteção dos dados durante a transmissão.

2.3. Sistemas Operacionais:

- Análise das funcionalidades e requisitos dos sistemas operacionais móveis, como Android e iOS, para suportar a implementação do aplicativo de backup.
- Exploração de conceitos de gerenciamento de arquivos e permissões de acesso para garantir a integridade dos dados.

Essas referências fornecerão uma base sólida para o desenvolvimento do sistema de backup automatizado, abordando aspectos técnicos essenciais relacionados à arquitetura de computadores, redes de computadores e sistemas operacionais.

3. Metodologia de Desenvolvimento e Avaliação:

O desenvolvimento do sistema de backup automatizado será dividido em fases bem definidas, considerando um período total de três meses e duas semanas. As atividades serão distribuídas de forma a garantir o cumprimento dos objetivos do projeto dentro do prazo estabelecido. Abaixo está o cronograma proposto:

3.1. Planejamento e Definição de Requisitos (1 semana)

- Definição dos requisitos do sistema de backup automatizado.
- Especificação da arquitetura de software e hardware.
- Design da interface do aplicativo móvel.

3.2. Desenvolvimento do Sistema NAS (4 semanas)

- Implementação do sistema de backup automatizado no NAS.
- Configuração inicial do NAS para armazenamento de backups.

3.3. Desenvolvimento do Aplicativo Móvel (3 semanas)

- Desenvolvimento do aplicativo móvel para gerenciamento do backup.
- Integração das funcionalidades do aplicativo com o NAS.

3.4. Implementação Final e Integração (2 semanas)

- Integração final entre o aplicativo móvel e o NAS.
- Coleta de feedback dos usuários beta para ajustes finais.
- Preparação para a fase de implementação em ambiente de produção.

4. Limitações do Trabalho:

- **Ambiente de Simulação:** O desenvolvimento e teste do sistema de backup automatizado serão realizados em um ambiente simulado em um computador pessoal. Isso pode limitar a capacidade de reproduzir com precisão todas as condições do ambiente real, como variações de rede e configurações específicas de dispositivos móveis.
- **Hardware Limitado:** O uso de um computador pessoal para simular o ambiente do NAS pode implicar em limitações de hardware, como capacidade de armazenamento e poder computacional. Isso pode impactar no desempenho e na escalabilidade do sistema em comparação com um NAS dedicado.
- **Escopo Funcional Restrito:** Devido às restrições de hardware e ambiente de simulação, o sistema de backup automatizado pode não incluir todas as funcionalidades desejadas. Algumas características avançadas, como redundância de dados e criptografia, podem não ser implementadas devido a limitações de recursos.
- **Validação Limitada:** A validação do sistema será realizada em um ambiente controlado e simulado, o que pode não refletir totalmente o uso real em diferentes contextos e cenários de uso. Portanto, a eficácia e estabilidade do sistema podem variar em condições de produção.
- **Dependência de Software Simulado:** O uso de software simulado pode introduzir diferenças de comportamento em relação a implementações reais, o que pode afetar a precisão dos testes e a validade dos resultados obtidos durante o desenvolvimento.

- **Requisitos de Hardware e Software do Sistema:** Os requisitos de hardware e software do sistema de backup automatizado podem ser diferentes em um ambiente de produção real, o que pode exigir ajustes adicionais durante a implementação final.

Considerando essas limitações, é importante interpretar os resultados dos testes e avaliações com cautela e considerar a necessidade de adaptações durante a implementação em um ambiente de produção real.

5. Desenvolvimento do Trabalho

Este projeto foi desenvolvido seguindo o princípio de *Clean Architecture*, para garantir a separação de preocupações e a facilidade de manutenção e escalabilidade do sistema. Optamos por utilizar um monorepo para hospedar tanto o código do servidor (*server*) quanto o aplicativo móvel (*mobile*), facilitando o gerenciamento do projeto e a integração entre as partes do sistema.

5.1. Estrutura Organizacional do Monorepo

O monorepo está organizado em duas pastas principais: *apps* e *packages*. Dentro de *apps*, encontram-se os diretórios *mobile* e *server*, que contêm, respectivamente, o código fonte do aplicativo móvel e do servidor. A pasta *packages* é usada para armazenar os tipos comuns (*types*), que são compartilhados entre o servidor e o aplicativo móvel, garantindo a consistência e a correta tipagem em ambos os projetos.

5.2. Arquitetura do Servidor e Suas Camadas

A arquitetura do servidor está dividida em várias camadas, conforme os princípios de *Clean Architecture*:

- **External**: Inclui rotas, providers e serviços externos, configurados para facilitar a interação com sistemas externos e a exposição das funcionalidades do servidor.
- **Main**: Contém o servidor HTTP Express, as factories e os use-cases. Esta camada é o coração da lógica de negócio, responsável por criar e gerenciar as instâncias principais do sistema e orquestrar as operações de backup.

5.3. Aplicação de Inversão de Controle e Dependência

Utilizamos intensamente os conceitos de inversão de controle (IoC) e inversão de dependência (DI) para desacoplar o código das implementações específicas de infraestrutura. Por exemplo, os serviços de armazenamento podem ser facilmente substituídos entre o Amazon S3 e o Cloudflare R2, ou qualquer outro sistema de armazenamento, sem necessidade de alterar a camada de negócios.

5.4. Integração com Armazenamento em Nuvem

Para aumentar a segurança e a redundância dos dados, utilizamos o Cloudflare R2, que emprega a API do S3 da AWS. Isso facilita a implementação, pois a API do S3 é amplamente documentada e suportada. A integração funciona espelhando a pasta que é salva no NAS localmente para o bucket no Cloudflare R2, garantindo que os dados sejam armazenados de forma redundante e segura. Isso significa que mesmo se o NAS local falhar, os dados ainda estarão disponíveis na nuvem.

5.5. Desenvolvimento do Aplicativo com React Native e Expo

Estamos desenvolvendo o aplicativo móvel usando React Native com o Expo, que é um conjunto de ferramentas e serviços que facilita o desenvolvimento de aplicativos React Native. O Expo proporciona um ambiente de desenvolvimento mais simples e robusto, permitindo que recursos como câmeras, localização e armazenamento sejam usados com mais facilidade. Além disso, o Expo facilita a construção e a implantação do aplicativo, reduzindo a complexidade e o tempo de desenvolvimento.

5.6. Mecanismo de Seleção de Arquivos

Para permitir que os usuários selecionem os arquivos que desejam fazer backup, utilizamos a biblioteca Expo Document Picker. Esta biblioteca proporciona uma interface simples e intuitiva para selecionar arquivos no dispositivo móvel. Através dela, os usuários podem facilmente navegar pelo sistema de arquivos do dispositivo e escolher os documentos que desejam proteger, tornando o processo de backup mais acessível e conveniente.

5.7. Implementação de Login Facilitado

Para simplificar o processo de login, utilizamos o ID do dispositivo móvel que está conectado ao servidor. Isso permite uma autenticação automática e transparente, uma vez que o dispositivo esteja na mesma rede Wi-Fi. Esse método impede que terceiros não autorizados usem o sistema, pois a autenticação é baseada na rede local e no dispositivo específico, aumentando a segurança sem complicar a experiência do usuário.

5.8. Verificação de Conexão na Mesma Rede Wi-Fi

A verificação se o servidor e o cliente estão na mesma rede Wi-Fi é feita utilizando a biblioteca Axios. Através dela, realizamos uma checagem para garantir que ambos os dispositivos estejam conectados à mesma rede antes de permitir a conexão e a execução das requisições de backup. Esta medida adiciona uma camada extra de segurança, garantindo que apenas dispositivos confiáveis possam acessar o sistema de backup, protegendo os dados de acessos não autorizados.

6. Trabalhos Futuros

Para continuar aprimorando nosso sistema de backup automatizado, identificamos algumas áreas de melhoria e desenvolvimento futuro:

- **Testes Unitários e de Integração** Uma das principais prioridades para os trabalhos futuros é a implementação de testes unitários e de integração. Esses testes são essenciais para garantir que cada componente do sistema funcione corretamente de forma isolada e em conjunto com outros componentes. A inclusão desses testes ajudará a identificar e corrigir erros mais rapidamente, além de aumentar a confiabilidade e a robustez do sistema.
- **Melhoria do Front-end Através da UX** Outra área crucial de melhoria é o front-end da aplicação. Planejamos otimizar a experiência do usuário (UX) para facilitar a visualização dos dados salvos, tanto na nuvem quanto localmente no NAS (Network Attached Storage). A melhoria da interface do usuário ajudará os usuários a navegarem e gerenciarem seus backups de maneira mais intuitiva e eficiente.

- **Aprimoramento do Sistema de Login** Por fim, o sistema de login será aprimorado para aumentar a segurança e a conveniência do usuário. Estamos explorando a implementação de autenticação multifator (MFA) e outras técnicas de segurança avançadas para proteger melhor os dados dos usuários e garantir que somente usuários autorizados possam acessar o sistema.

Essas melhorias são fundamentais para garantir que nosso sistema de backup automatizado continue evoluindo e atendendo às necessidades dos usuários de maneira eficiente e segura.

7. Conclusões

Este artigo apresentou a proposta e implementação de um sistema de backup automatizado baseado em Network Attached Storage (NAS) para dispositivos móveis, visando proteger os dados dos usuários contra perdas decorrentes de roubo, perda ou danos aos dispositivos. A solução desenvolvida sincroniza arquivos tanto com um NAS local quanto com um repositório na nuvem, utilizando a mesma rede Wi-Fi residencial para simplificar o processo de backup.

Durante o desenvolvimento, adotamos a metodologia de Clean Architecture, que promove a separação clara de responsabilidades e facilita a manutenção e escalabilidade do sistema. A escolha por um monorepo para o código do servidor e do aplicativo móvel também se mostrou acertada, simplificando a gestão do projeto e melhorando a integração entre as partes.

A integração com serviços de armazenamento em nuvem, como o Cloudflare R2 utilizando a API do S3 da AWS, proporcionou uma camada adicional de segurança e redundância para os dados dos usuários. Isso garante que, mesmo em caso de falha do NAS local, os arquivos ainda estejam protegidos e acessíveis.

O desenvolvimento do aplicativo móvel com React Native e Expo permitiu uma implementação ágil e robusta das funcionalidades de seleção de arquivos e login facilitado, utilizando o ID do dispositivo móvel conectado à rede Wi-Fi como método de autenticação. A verificação de conexão na mesma rede Wi-Fi, realizada com Axios, acrescentou uma camada de segurança extra, restringindo o acesso apenas a dispositivos confiáveis na rede.

Como todo projeto, este trabalho possui limitações, como a validação em um ambiente simulado e as restrições de hardware. Esses aspectos podem influenciar na performance e na escalabilidade do sistema em um ambiente de produção real. No entanto, as melhorias planejadas, como testes unitários e de integração, melhoria da UX e aprimoramento do sistema de login, têm o potencial de mitigar essas limitações e fortalecer ainda mais a solução proposta.

Em suma, o sistema de backup automatizado desenvolvido representa um avanço significativo na proteção dos dados dos usuários de dispositivos móveis, oferecendo uma solução confiável e conveniente para aqueles que buscam garantir a segurança de suas informações pessoais. As melhorias contínuas e o aprimoramento planejado garantirão que o sistema continue atendendo às necessidades dos usuários de maneira eficaz e segura.

References

Andrew, S. T. and Herbert, B. (2015). *Modern operating systems*. Pearson Education.

Dargahi, T., Dehghantanha, A., and Conti, M. (2017). Chapter 12 - investigating storage as a service cloud platform: pcloud as a case study. In Choo, K.-K. R. and Dehghantanha, A., editors, *Contemporary Digital Forensic Investigations of Cloud and Mobile Applications*, pages 185–204. Syngress.

Drago, I., Mellia, M., Munafo, M. M., Sperotto, A., Sadre, R., and Pras, A. (2012). Inside dropbox: Understanding personal cloud storage services. *IMC '12: Proceedings of the 2012 Internet Measurement Conference*, pages 481–494.

Kurose, J. F. and Ross, K. W. (2017). *Computer networking: A top-down approach*. Pearson, 7th edition.

Miller, E. and Long, D. (2002). Strong security for Network-Attached storage. *USENIX Association*.

Peterson, L. L. and Davie, B. S. (2012). *Computer Networks: A systems approach*. Morgan Kaufmann, 5th edition.

Stallings, W., Zeno, P., and Jesshope, C. R. (2016). *Computer Organization and Architecture: Designing for performance*. Pearson Education Limited, 10 edition.