DLPS baseado em Deep Learning: Nova Abordagem para Detecção de Exfiltração em HDFS

James de Castro Martins[1], **Li Weigang**[1], **Luís Paulo Faina Garcia**[1], **Gabriel Alves Castro**[1]

[1]Universidade de Brasília (UnB)
Campus Darcy Ribeiro – 70910-900 – Asa Brasília – DF – Brazil . Asa Norte, Brasília, DF

[2]Departamento de Ciência da Computação
– Brasília, DF – Brazil

james76cm@gmail.com, weigang@unb.br, luis.garcia@unb.br

gabriel_alvesozorio@hotmail.com

Abstract. *This article describes cybersecurity applied to Social Media with an emphasis on using Hadoop Distributed File System (HDFS) for storing and processing large volumes of data. The objective was to develop a DLPS framework based on Machine Learning (ML) that improves the accuracy in identifying data leaks in HDFS structures. Thus, the main categories of cyber security approaches were identified, within the scope of HDFS, in comparison with MITRE ATT&CK Framework. Research gaps have been identified in works involving DLPS and Machine Learning, offering the need to develop correlated solutions. A Deep Learning based framework applied to Hadoop metadata and logs is proposed as a solution to improve exfiltration detection.*

Resumo. *Este artigo descreve segurança cibernética aplicada a Mídias Sociais com ênfase no uso de HDFS para armazenamento e processamento de grandes volumes de dados. O objetivo foi desenvolver um framework de DLPS baseado em ML que melhore a precisão na identificação de vazamento de dados em estruturas de HDFS. Assim, identificou-se as principais categorias de abordagens em segurança cibernética, no âmbito de HDFS, em comparação com Framework MITRE ATT&CK. Lacunas de pesquisas foram identificadas, em trabalhos realizados envolvendo DLPS e Machine Learning, oferecendo a necessidade do desenvolvimento de soluções correlacionadas. Um framework baseado em Deep Learning aplicado aos metadados e logs do Hadoop é proposto como solução para melhorar a detecção de exfiltração.*

1. Introdução

Mídias Sociais [Hudson 2020] atualmente ocupam uma parcela considerável das iterações computacionais com a internet. Empresas como Facebook, Instagram, dentre outras, oferecem à sociedade, como um todo, inúmeras possibilidades de relacionamento interpessoal, entre pessoas e empresas, além da vasta possibilidade de entretenimento [Li et al. 2021].

Para garantir a eficiência e a eficácia no uso dessas aplicações, as empresas fazem uso de recursos computacionais presentes em *Cloud Computing*. [Coulouris et al. 2005] define o termo como uma visão de computação utilitária. Uma nuvem é definida como um

conjunto de aplicativos baseados na Internet, armazenamento e serviços de computação suficientes para dar suporte às necessidades da maioria dos usuários, permitindo-lhes dispensar em grande parte ou totalmente o armazenamento de dados local e software de aplicativo. Sobre esta última característica, Sistemas de Arquivos Distribuídos normalmente, dentre outras funcionalidades, são utilizados para o gerenciamento e processamento desta grande massa de dados.

Nesse sentido, o ecossistema Hadoop é uma das soluções mais utilizadas pelas grandes empresas fornecedoras de *Cloud Computing*, sendo popularmente conhecido e usado pelas seguintes razões: poder de computação, tolerância a falhas, flexibilidade, escalabilidade e baixo custo. Entretanto, em contraponto ao incremento funcional e de usabilidade da solução, questões relacionadas com a segurança cibernética vêm sido negligenciadas e tratadas sem a devida importância, principalmente quanto ao HDFS, um dos principais componentes do ecossistema Hadoop [Saraladevi et al. 2015], [Suganya and Selvamuthukumaran 2018] e [Bhathal and Singh 2019].

Ao se estudar e pesquisar sobre segurança cibernética em HDFS, mesmo que a exfiltração de dados seja um preocupação constante e estudos indiquem a eficácia no uso de *Machine Learning* (ML) para a identificação desta ameaça [Sabir et al. 2020], ainda não existem estudos que tenham comprovado a eficácia de *Data Leakage Protection System* (DLPS) envolvendo a aplicação de ML para identificar vazamentos de dados em HDFS, principalmente quando o *hacker* se utiliza da própria estrutura para auferir sucesso em seu ataque cibernético.

Desta forma, dada a importância da estrutura de *Cloud Computing* para as Mídias Sociais e, neste contexto, a necessidade de mais pesquisas e estudos sobre segurança cibernética aplicada a HDFS, principalmente pela necessidade na utilização de DLPS neste contexto, este trabalho de pesquisa objetiva **desenvolver um framework de DLPS baseado em ML que melhore a precisão na identificação de vazamento de dados em estruturas de HDFS**.

2. Contextualização

Nesta seção, apresentam-se as principais categorias envolvendo segurança cibernética e, ao final, uma comparação com o Framework MITRE ATT&CK [MITRE 2021].

O Hadoop Distributed File System (HDFS) é um sistema de código aberto, desenvolvido pela comunidade APACHE e integra o ecossistema Hadoop. Foi desenhado para ser executado em hardwares de baixo custo. Sua arquitetura foi pensada para ser simples, registrando de maneira distribuída e com resistência às possíveis perdas de dados. [ApacheFoundation 2019b].

A arquitetura é baseada em um modelo mestre-escravo, sendo dividida entre duas abstrações: *Name Nodes*, os quais são responsáveis por toda a gestão dos metadados e operações do HDFS e os *Data Nodes*, os quais são responsáveis por registrar os pedaços de dados. Como uma estratégia de performance, o HDFS leva a computação para onde os dados estão, evitando transferências de dados desnecessárias na rede e agilizando os processos computacionais. Além disso, o cliente após receber o direcionamento do *NameNode*, se conecta diretamente aos *DataNodes* para a realização de operações de consulta/inserção.

2.1. Segurança em HDFS

Nesta seção, apresentam-se considerações sobre segurança cibernética em HDFS, as principais questões sobre segurança cibernética envolvendo este sistema e, ao final, uma comparação destas questões com o framework MITRE ATT&CK.

Segundo [Choudhary et al. 2017], o ecossistema Hadoop pelo grande conjunto de dados armazenados e processados, possui como um dos principais desafios a segurança cibernética. Neste contexto, alguns pesquisadores identificaram o HDFS como a estrutura mais sensível do ecossistema Hadoop [Suganya and Selvamuthukumaran 2018] e dividiram segurança cibernética aplicada a HDFS em quatro categorias: criptografia, autenticação, autorização e auditoria [Chu 2020].

Criptografia é basicamente utilizada com a finalidade de proteger dados armazenados, visando a proteção contra ataques cibernéticos que venham a promover algum vazamento de dados ou exfiltração. Neste sentido, [Lin et al. 2012] propuseram e implementaram duas integrações, HDFS-RSA e HDFS-Pairing, como extensões do HDFS. Os experimentos foram conduzidos para demonstrar a sobrecarga de desempenho do HDFS-RSA e do HDFS-Pairing, fornecendo alternativas para se alcançar melhor confidencialidade dos dados e [Tondon and Khurana 2017] exploraram a criptografia apresentando uma técnica que detecta ataques cibernéticos nos *Data Nodes*, com base no método de AES-MR (*Advanced Encryption Standard using Map Reduce*) com processamento distribuído, analisando o trabalho do HDFS, sendo o foco auxiliar contra ataques de negação de serviço para um único *DataNode*.

Já ***Autenticação*** está intimamente ligada a questão de quem está autorizado a acessar ou não a arquitetura do HDFS. Neste contexto, alguns trabalhos colaboraram com o fortalecimento e proteção contra acessos indevidos. A solução mais popular para autenticação em HDFS foi desenvolvida pelo MIT - Kérberos [Sharma and Navdeti 2014] e [Bhathal and Singh 2019]. O protocolo Kerberos fornece comunicação segura por meio de criptografia de chave secreta; [Thuraisingham et al. 2010] trouxeram outra abordagem. A proposta foi, em um ambiente de nuvem privada, os dados seriam persistidos em uma estrutura HDFS e, sobre este, criou-se uma camada a mais de segurança utilizando Hive e a aplicação de linguagem SQL para realização das operações e, finalmente, [Sadasivam et al. 2012] sugerem o uso das propriedades fundamentais de um triângulo e servidores duais para melhorar o nível de segurança dos *clusters*. A senha fornecida pelo usuário é interpretada e alienada em mais de uma unidade utilizando o servidor de autenticação, sendo armazenada em vários servidores *backend* junto com o nome de usuário correspondente.

A ***Autorização*** diz respeito às políticas de segurança aplicadas ao processo de autenticação e de acesso à arquitetura. Conforme [Cloudera 2020], a ferramenta mais popular para controle de autorização é o Apache Sentry. [Sharma and Navdeti 2014] e [Bhathal and Singh 2019] acrescentam que a ferramenta Apache Ranger [ApacheFoundation 2019a] também colabora com esta categoria por centralizar a administração de segurança, fornecendo autorização padronizada e refinada, métodos de autorização e suporte para a auditoria de ações administrativas relacionadas ao acesso do usuário em todos os componentes do Hadoop.

E, finalmente, a ***Auditoria*** diz respeito a análise dos dados com a finalidade de

identificar atividades maliciosas. Neste sentido, algumas soluções tratam da auditoria interna no HDFS. O algoritmo *Bull Eye*, segundo [Saraladevi et al. 2015], é capaz de fornecer segurança para os dados nó a nó no HDFS. O algoritmo concentra-se apenas em dados confidenciais, realizando a varredura dos dados antes que eles sejam armazenados em blocos pelo *DataNode*. [Fu et al. 2017] trataram de ataques hackers com foco em exfiltração de dados e propuseram um framework em forense que possui um método de coleta de dados sob demanda e um método de análise automática para ataques de vazamento de dados em HDFS. Neste contexto, ocorre a coleta de dados e ao final da aplicação da arquitetura, oferecem-se evidências que podem ser usadas para localizar invasores e reconstruir cenários de ataque. Entretando, conforme [Chu 2020], o trabalho conjunto de duas soluções, algoritmo *Bull Eye* e *Name Node Approach*, trariam melhores condições para análise e o monitoramento interno dos dados.

2.2. Comparação com o Framework MITRE ATT&CK

Após a apresentação de trabalhos relacionados às principais categorias de abordagens em segurança cibernética com ênfase na arquitetura HDFS, [Saraladevi et al. 2015] e [Chu 2020], esta subseção apresentará uma análise, à luz do Framework MITRE ATT&CK [MITRE 2021], com vistas a identificar como cada categoria apresentada anteriormente corresponderia com cada etapa no passo a passo de um ataque cibernético. Conforme [Al-Shaer et al. 2020], o framework MITRE oferece um vasto repositório sobre as principais Táticas, Técnicas e Procedimentos (TTP) presentes em um ataque hacker.

Seguindo o *Framework Enterprise Mitre*, escolhido devido a similaridade com o ambiente de estudo desta pesquisa, as seguintes etapas são apresentadas:

- **Reconhecimento**: o adversário tenta reunir informações que possam utilizar para planejar operações futuras;
- **Desenvolvimento de Recursos**: tentativa de implementar recursos que possam ser utilizados para apoiar o ataque;
- **Acesso Inicial**: tentativa de invasão de rede ou sistema;
- **Execução**: tentativa de executar código malicioso;
- **Persistência**: tentativa de permanência da sua posição dentro da rede atacada;
- **Escalação de Privilégios**: obtenção de permissões de nível superior;
- **Evasão de Defesa**: O adversário está tentando evitar ser detectado;
- **Acesso a Credenciais**: roubo de nomes e senhas de contas;
- **Descoberta**: atividade de reconhecimento e descoberta no ambiente atacado;
- **Movimento Lateral**: o atacante está tentando se movimentar dentro da rede ou sistema atacado;
- **Coleção**: tentativa de reunir dados de interesse para seu objetivo;
- **Comando e Controle (C²)**: o adversário está tentando se comunicar com sistemas comprometidos para controlá-los;
- **Exfiltração**: atividade de roubo, vazamento e exfiltração de dados;
- **Impacto**: tentativa de manipulação, interrompimento ou destruição de sistemas e dados.

A Tabela 1 apresenta a relação entre cada categoria de abordagem de segurança cibernética no contexto de HDFS em comparação com o framework MITRE ATT&CK. A proposta é identificar, pela comparação, quais outras novas abordagens ou quais abordagens poderiam ser aprimoradas, levando-se em consideração a sequência de um ataque hacker demonstrado no MITRE ATT&CK.

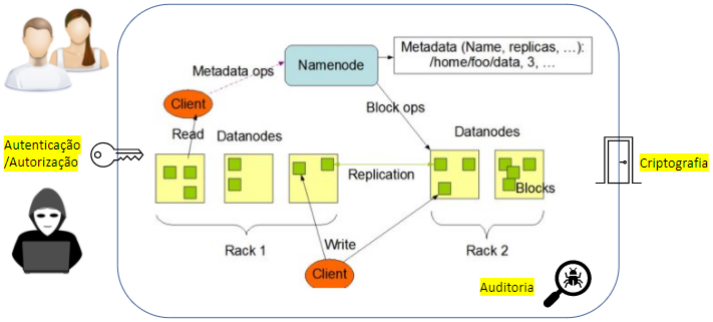


Figura 1. Arquitetura HDFS integrada às categorias de segurança cibernética aplicadas. Fonte: adaptada de [ApacheFoundation 2019b]

Após analisar os dados apresentados na Tabela 1, percebe-se que as atuais abordagens em segurança cibernética apresentadas no contexto de HDFS não são suficientes, levando-se em consideração à arquitetura de ataque cibernético apresentada no *Framework* MITRE ATT&CK. Das 14 etapas apresentadas no framework MITRE, nove, em torno de 64%, estão relacionadas com a categoria auditoria: execução, persistência, escalação de privilégios, evasão de defesa, descoberta, movimento lateral, coleção, C² e impacto. Ainda que os trabalhos de [Saraladevi et al. 2015], [Fu et al. 2017] e [Chu 2020], de alguma forma, possam oferecer opções para a defesa contra essas etapas de um ataque, pela heterogeneidade presente em cada etapa do framework, existe a necessidade de mais estudos dedicados a cada uma dessas etapas.

Todas as categorias de segurança em HDFS revelam uma preocupação com um ataque externo. Tanto a criptografia, proteção no dado; como autenticação e autorização, atenção com quem pode acessar e o que deve ser acessado e, finalmente, como a auditoria, analise dos *logs* e dados para identificação de ataque cibernéticos se mostram atentas ao ataque vindo de fora, mas a questão do próprio atacante se beneficiar de todas essas categorias não é estudada e explorada. A figura 1 apresenta as categorias de segurança na arquitetura HDFS.

Especificamente, para a exfiltração de dados, ainda que exista uma área da defesa que trata especificamente desse ataque, *Data Leakage Protection System* (DLPS) [Alneyadi et al. 2016] e [Nayak and Ojha 2020] ainda não foram identificados estudos que implementassem DLPS no interior do HDFS, principalmente no contexto da categoria auditoria.

3. Trabalhos Realizados

Segundo [Alneyadi et al. 2016], *Data Leakage Protection System* (DLPS) são mecanismos dedicados à detecção e prevenção de vazamento de dados confidenciais. DLPS possuem a capacidade de analisar conteúdo dos dados e seus metadados em três possibilidades de estado do dado: em trânsito, em uso e em repouso.

Atualmente, a aplicação de ML, mais especificamente *Deep Learning* (DL) vém se mostrado eficiente e eficaz na detecção de vazamento de dados pela identificação de características intrínsecas à massa de dados.

Nesse sentido, [Sabir et al. 2020] classifica o emprego de ML em duas abordagens: orientada a dados ou orientada a comportamento. Cada uma com suas subcategorias:a primeira apresenta (a) inspeção de contexto, (b) inspeção de distribuição e (c) inspeção de direta e a segunda já apresenta as seguintes abordagens: (a) baseada em eventos, (b) baseada em Fluxos, (c) baseadas no uso de recursos, (d) baseada em propagação e (e) abordagem híbrida.

Assim, dadas as característica de cada subcategoria supracitada e a natureza da exfiltração de dados presente na estrutura HDFS, os seguintes trabalhos, envolvendo a aplicação de ML em DLPS, foram selecionados:

[Shrestha et al. 2015], para resolver o problema de detecção de comunicação secreta por meio de canais laterais dentro de recursos de rede, propôs uma estrutura de ML para detecção confiável de canais de temporização ocultos. As impressões digitais estatísticas do tráfego foram extraídas e utilizadas como pontos de recursos para treinar o algoritmo *Support Vector Machine* (SVM) e assim, o algoritmo classificaria o tráfego investigado em secreto ou aberto.

[Altay et al. 2019] trataram do problema de vazamento de dados, via páginas maliciosas, que são detectadas por métodos que utilizam *blacklists*. Para isto, propuseram um método sensível a contexto e baseado em densidade de palavras-chaves para classificação de páginas maliciosas utilizando ML supervisionado, *Support Vector Machine* (SVM), *Maximum Entropy* (MaxEnt) e *Extreme Learning Machine* (ELM).

Similar a [Altay et al. 2019], [Mokbal et al. 2019] procuraram resolver a questão da atual falta de segurança presente nos aplicativos de web dinâmicos, quando no processo de manipulação e interação de recursos entre clientes e servidores. Esta pesquisa propôs um esquema de detecção baseado em Redes Neurais Artificiais, onde seus principais pilares foram a qualidade dos dados coletados, vetores de recursos e a caracterização genuina do fenômeno anômalo *Cross Site Script* (XSS), ataque cibernético direcionado a aplicativos web.

Já, [Fang et al. 2019] propuseram um framework, denominado THEMIS, para classificação de e-mails baseado em um modelo aprimorado de Redes Neurais Convolucionais Recorrentes com vetores de vários níveis utilizando cabeçalhos de e-mail, corpo do e-mail, o nível de caractere e o nível da palavra. Este trabalho buscou mitigar o problema de *phishing*, que vem a cada dia aperfeiçoando suas técnicas de ataque.

Da mesma forma, [Huang et al. 2019] também ofereceram soluções para *phishing*, mas, diferente dos autores anteriores, o foco de pesquisa foram páginas web e não e-mail. A proposta dos autores foi um método, denominado PhishingNet, baseado em DL para detecção de URL de *phishing*, que consiste em um módulo CNN e um módulo RNN baseado em atenção hierárquica. Algoritmos CNN foram adotados para a extração de representações de recursos espaciais em nível de caracteres de URL.

Ataques de injeção SQL são uma das principais maneiras de exfiltração de dados em páginas web, que utilizam Banco de Dados (BD). Atualmente, devido ao fraco desempenho em tempo real da análise do conteúdo do tráfego e a alta taxa de falsos positivos na detecção, as soluções atuais tornaram-se pouco confiáveis. Assim, [Zhang et al. 2019] propuseram um método de detecção de injeção de SQL analisando a rede de tráfego, precisamente, por meio da solicitação de alguns recursos para detecção de injeção de SQL

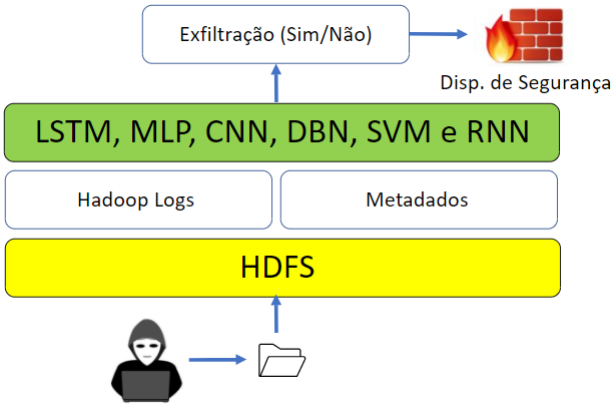


Figura 2. Framework para aplicação de DLPS baseado em DL para detecção de exfiltração. Fonte: autor

e para isso os seguintes algoritmos de DL foram utilizados: LSTM, MLP, CNN e DBN, sendo este último o que obteve o melhor desempenho.

[Kar et al. 2016] ofereceram uma proposta diferente de [Zhang et al. 2019]. Os autores apresentaram uma abordagem para detectar ataques de injeção de SQL modelando consultas SQL, como um grafo de *tokens*, usando a centralidade de nós para treinar um classificador SVM. As consultas SQL foram normalizadas em sequência de *tokens*, preservando a composição estrutural e capturou-se a interação entre os *tokens* na forma de um grafo.

[Liu et al. 2019] propuseram uma solução para o problema da ameaça interna, i.e., usuários legítimos que exfiltram dados sensíveis de suas organizações. Neste artigo, foi proposto uma abordagem de detecção de ameaças internas, que aplica um *autoencoder* para facilitar o aprendizado de recursos extraídos usando o Word2vec, modelo de vários tipos de logs de segurança. A abordagem proposta compreendeu a extração automatizada de recursos usando Word2vec e detecção de ameaças internas usando um codificador automático.

E, finalmente, [Singh et al. 2019] também abordaram a questão da ameaça interna, como propuseram [Liu et al. 2019], entretanto estes autores ofereceram uma proposta que consiste em um LSTM modificado como LSTM de vários estados, sendo semelhante ao Processamento de Linguagem Natural (PLN) para aprender a linguagem de comportamento do usuário.

4. Framework para Detecção de Exfiltração em HDFS baseado em DLPS

Apoiado pela metodologia CRISP-DM, o Framework proposto é apresentado na Figura 2.

Da análise dos trabalhos relacionados com o uso de ML em DLPS para detecção de exfiltração de dados, pode-se perceber que ainda não existem trabalhos que identifiquem o uso do HDFS em proveito de uma ação hacker, apesar da existência desta lacuna de estudo, conforme apresentada na subseção ”Segurança em HDFS”.

Ainda assim, os trabalhos de [Liu et al. 2019] e [Singh et al. 2019] apresentaram abordagens relacionadas a ameças internas e em comparação com este framework, a

diferença existe na origem do emissor, pois nesta pesquisa, aborda-se a ação de malware de exfiltração e não a ação de usuários mal intencionados. Entretanto, a pesquisa de [Singh et al. 2019] apresenta o uso de dados em claro, sendo esta possibilidade descartada neste framework, pois o conteúdo interno é criptografado, restando apenas a possibilidade de análise de metadados.

A análise de metadados, ainda que em ameças diferentes, é apresentada nos trabalhos de [Shrestha et al. 2015], [Fang et al. 2019], [Huang et al. 2019] e [Zhang et al. 2019], condição que apoia a estratégia de uso dos mesmos algoritmos de DL, no caso, LSTM, MLP, CNN, DBN, SVM e RNN. Além da técnica de *autoencoder* apresentada por [Liu et al. 2019].

Dessa forma, de forma resumida, os dados e logs são coletados e armazenados, seguindo a proposta de [Fu et al. 2017]. Após esta etapa, o dado deverá ser pré-processado e tratado, conforme metodologia CRISP-DM, para em seguida serem processados pelos algoritmos de DL identificados. Assim, um modelo será treinado e testado para, ao final, classificar o conjunto de dados como uma exfiltração ou não.

5. Conclusão e Trabalhos Futuros

HDFS vem sendo largamente utilizado pela principais empresas de Midia Social (Facebook, Instagran, dentre outras) e questões envolvendo segurança cibernética são relevantes para sua disponibilidade. Assim, este trabalho de pesquisa objetivou explorar o tema *security* em HDFS e propor solução para eventuais lacunas ao tema.

Conforme [Chu 2020], existem quatro categorias de abordagens em segurança cibernética aplicada ao ambiente HDFS: criptografia, autenticação, autorização e auditoria. Trabalhos realizados envolvendo as quatro categorias foram pesquisados para que se pudesse compreender, à luz do *Framework* MITRE ATT&CK, a existência de lacunas de pesquisa ao tema.

Dessa maneira, percebe-se que as atuais abordagens em segurança cibernética no contexto de HDFS ainda são insuficientes, pesquisas envolvendo a aplicação da categoria auditoria em cada etapa do *framework* MITRE são necessárias, sendo uma perspectiva inovadora o estudo do ambiente onde o hacker utiliza a própria estrutura a seu favor e, finalmente, com ênfase em exfiltração de dados, a aplicação do conceito de DLPS é recomendada.

Nesse contexto, desenvolveu-se um Framework para aplicação de DLPS baseado em DL para a detectação de exfiltração em uma estrutura HDFS utilizada em um ataque hacker.

Para trabalhos futuros, propõe-se a aplicação do framework proposto para a identificação de qual estrutura de DL é mais eficaz e computacionalmente utilizável.

Referências

Al-Shaer, R., Spring, J. M., and Christou, E. (2020). Learning the associations of mitre att & ck adversarial techniques. In *2020 IEEE Conference on Communications and Network Security (CNS)*, pages 1–9. IEEE.

Alneyadi, S., Sithirasenan, E., and Muthukkumarasamy, V. (2016). A survey on data leakage prevention systems. *Journal of Network and Computer Applications*, 62:137–152.

Altay, B., Dokeroglu, T., and Cosar, A. (2019). Context-sensitive and keyword density-based supervised machine learning techniques for malicious webpage detection. *Soft Computing*, 23(12):4177–4191.

ApacheFoundation (2019a). The apache software foundation. Disponível em: ¡https://ranger.apache.org/¿.Acesso em: 14 abr. 2021.

ApacheFoundation (2019b). Hdfs architecture guide. Disponível em: ¡https://hadoop.apache.org/docs/r1.2.1/hdfs$_d esign.html File + Deletes + and + Undeletes > .Acessoem : 14abr.2021$.

Bhathal, G. S. and Singh, A. (2019). Big data: Hadoop framework vulnerabilities, security issues and attacks. *Array*, 1:100002.

Choudhary, M., Yadav, A. S., Yadav, D. K., and Pawar, V. (2017). A review on hadoop security issues.

Chu, K. (2020). Apache hadoop: A review on security issues and solutions for hdfs: A deep dive into the security issues occur in hdfs structure, and the available technologies to protect it. Disponível em: ¡https://medium.com/swlh/apache-hadoop-a-review-on-security-issues-and-solutions-for-hdfs-5ba06861b7cd¿.Acesso em: 13 abr. 2021.

Cloudera (2020). Authentication. Disponível em: ¡https://docs.cloudera.com/documentation/enterprise/latest/topics/¿.Acesso em: 14 abr. 2021.

Coulouris, G. F., Dollimore, J., and Kindberg, T. (2005). *Distributed systems: concepts and design*. pearson education.

Fang, Y., Zhang, C., Huang, C., Liu, L., and Yang, Y. (2019). Phishing email detection using improved rcnn model with multilevel vectors and attention mechanism. *IEEE Access*, 7:56329–56340.

Fu, X., Gao, Y., Luo, B., Du, X., and Guizani, M. (2017). Security threats to hadoop: data leakage attacks and investigation. *IEEE Network*, 31(2):67–71.

Huang, Y., Yang, Q., Qin, J., and Wen, W. (2019). Phishing url detection via cnn and attention-based hierarchical rnn. In *2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, pages 112–119. IEEE.

Hudson, M. (2020). What is social media? Disponível em: ¡https://www.thebalancesmb.com/what-is-social-media-2890301¿.Acesso em: 12 abr. 2021.

Kar, D., Panigrahi, S., and Sundararajan, S. (2016). Sqligot: Detecting sql injection attacks using graph of tokens and svm. *Computers & Security*, 60:206–225.

Li, Y., Shi, S., Wu, Y., and Chen, Y. (2021). A review of enterprise social media: visualization of landscape and evolution. *Internet Research*.

Lin, H.-Y., Shen, S.-T., Tzeng, W.-G., and Lin, B.-S. P. (2012). Toward data confidentiality via integrating hybrid encryption schemes and hadoop distributed file system. In *2012 IEEE 26th International Conference on Advanced Information Networking and Applications*, pages 740–747. IEEE.

Liu, L., Chen, C., Zhang, J., De Vel, O., and Xiang, Y. (2019). Unsupervised insider detection through neural feature learning and model optimisation. In *International Conference on Network and System Security*, pages 18–36. Springer.

MITRE (2021). Enterprise matrix. Disponível em: ¡https://attack.mitre.org/matrices/enterprise/¿.Acesso em: 14 abr. 2021.

Mokbal, F. M. M., Dan, W., Imran, A., Jiuchuan, L., Akhtar, F., and Xiaoxi, W. (2019). Mlpxss: an integrated xss-based attack detection scheme in web applications using multilayer perceptron technique. *IEEE Access*, 7:100567–100580.

Nayak, S. K. and Ojha, A. C. (2020). Data leakage detection and prevention: Review and research directions. *Machine Learning and Information Processing*, pages 203–212.

Sabir, B., Ullah, F., Babar, M. A., and Gaire, R. (2020). Machine learning for detecting data exfiltration. *arXiv preprint arXiv:2012.09344*.

Sadasivam, G. S., Kumari, K. A., and Rubika, S. (2012). A novel authentication service for hadoop in cloud environment. In *2012 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM)*, pages 1–6. IEEE.

Saraladevi, B., Pazhaniraja, N., Paul, P. V., Basha, M. S., and Dhavachelvan, P. (2015). Big data and hadoop-a study in security perspective. *Procedia computer science*, 50:596–601.

Sharma, P. P. and Navdeti, C. P. (2014). Securing big data hadoop: a review of security issues, threats and solution. *Int. J. Comput. Sci. Inf. Technol*, 5(2):2126–2131.

Shrestha, P. L., Hempel, M., Rezaei, F., and Sharif, H. (2015). A support vector machine-based framework for detection of covert timing channels. *IEEE Transactions on Dependable and Secure Computing*, 13(2):274–283.

Singh, M., Mehtre, B. M., and Sangeetha, S. (2019). User behavior profiling using ensemble approach for insider threat detection. In *2019 IEEE 5th International Conference on Identity, Security, and Behavior Analysis (ISBA)*, pages 1–8. IEEE.

Suganya, S. and Selvamuthukumaran, S. (2018). Hadoop distributed file system security-a review. In *2018 International Conference on Current Trends towards Converging Technologies (ICCTCT)*, pages 1–5. IEEE.

Thuraisingham, B., Khadilkar, V., Gupta, A., Kantarcioglu, M., and Khan, L. (2010). Secure data storage and retrieval in the cloud. In *6th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom 2010)*, pages 1–8. IEEE.

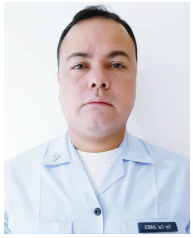
Tondon, D. and Khurana, M. (2017). Security of big data in hadoop using aes-mr with auditing. In *International Journal of Advanced Research in Computer Science and Software Engineering*.

Zhang, H., Zhao, B., Yuan, H., Zhao, J., Yan, X., and Li, F. (2019). Sql injection detection based on deep belief network. In *Proceedings of the 3rd International Conference on Computer Science and Application Engineering*, pages 1–6.

Tabela 1. Relação entre categorias de segurança cibernética em HDFS e o framework Mitre ATT&CK

MITRE ATT&CK	CATEGORIAS SEGURANÇA HDFS	JUSTIFICATIVA	TRABALHOS RELACIONADOS
Reconhecimento	Nil	Nil	Nil
Desenvolvimento de Recursos	Nil	Nil	Nil
Acesso Inicial	Autenticação, Autorização	Essas categorias dificultam o acesso inicial do atacante.	[Thuraisingham et al. 2010], [Sadasivam et al. 2012], [Sharma and Navdeti 2014], [Bhathal and Singh 2019], [Cloudera 2020b], [ApacheFoundation 2019]
Execução	Auditoria	A execução de códigos maliciosos no interior pode ser observado por meio do monitoramento de logs.	[Fu et al. 2017]
Persistência	Auditoria	A persistência é uma ação hacker que ocorre após um ataque de sucesso. Uma vez que o atacante já está dentro da rede, suas atividades poderiam ser monitoradas.	[Fu et al. 2017]
Escalação de Privilégios	Auditoria	A obtenção de privilégios internos a rede ou sistema requerem atividades internas que poderiam ser observadas pelo monitoramento do sistema.	[Saraladevi et al. 2015], [Fu et al. 2017] e [Chu 2020]
Evasão de Defesa	Auditoria	A eficácia na evasão contra contra atividades de defesa, como: antivirus, sistemas de detecção de intrusão, dentre outros, depende de que nenhuma atividade interna maliciosa seja detectada.	[Saraladevi et al. 2015], [Fu et al. 2017] e [Chu 2020]
Acesso a Credenciais	Criptografia, Autenticação e Autorização	A tentativa de roubo de credenciais poderia ser evitada por uma política robusta de acesso, I.e., autorização ou por mecanismos de acesso eficazes. Em caso de roubo, a criptografia dificultaria o roubo de credenciais.	[Thuraisingham et al. 2010], [Sadasivam et al. 2012], [Lin et al. 2012] [Sharma and Navdeti 2014], [Tondon and Khurana 2017] , [Bhathal and Singh 2019],[Cloudera 2020b], [ApacheFoundation 2019]
Descoberta	Auditoria	A identificação, por parte do atacante de informação internas ao sistema ou rede invadidos promovem a produção de logs ou a possibilidade de detecção, via análise dos dados.	[Saraladevi et al. 2015], [Fu et al. 2017] e [Chu 2020]
Movimento Lateral	Auditoria	Idem justificativa anterior.	[Saraladevi et al. 2015], [Fu et al. 2017] e [Chu 2020]
Coleção	Auditoria	Idem justificativa anterior.	[Saraladevi et al. 2015], [Fu et al. 2017] e [Chu 2020]
Comando e Controle (C^2)	Auditoria	A atividade de C^2 passa necessariamente pela atividade de entrada e saida de dados, assim paciveis de serem monitorados.	[Saraladevi et al. 2015], [Fu et al. 2017] e [Chu 2020]
Exfiltração	Criptografia e Auditoria	O vazamento de dados ou exfiltração são dificultados, se os dados estiverem criptografados e evitados, caso ocorra uma atividade de monitoria eficiente e e eficaz.	[Saraladevi et al. 2015], [Fu et al. 2017] e [Chu 2020]
Impacto	Auditoria	A proposta desta etapa do ataque cibernético é a manipulação, o interrompimento ou a destruição de sistemas e dados, assim, um monitoramento eficaz poderia evitar tais ocorrências.	[Saraladevi et al. 2015], [Fu et al. 2017] e [Chu 2020]

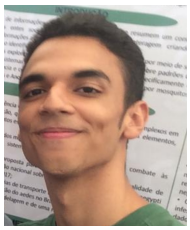
Autores



James de Castro Martins possui graduação em Ciências Aeronáuticas pela Academia da Força Aérea (AFA) (1997 - 2000). Mestrado em Engenharia Eletrônica e Computação pelo Instituto Tecnológico de Aeronáutica (ITA) (2016 - 2017). Doutorando pela Universidade de Brasília (UNB) (2019 -). Tem experiência na área de Análise de Sistemas, com ênfase em Algoritmos Orientados a Objetos. Experiência operacional na área de Defesa Cibernética com foco em Gestão e Análise de Incidentes Cibernéticos, Threat Hunting e identificação de Advanced Persistent Threat (APT). cv_link: http://lattes.cnpq.br/6130298560737616

Li Weigang é professor, coordenador do TransLab e titular do Departamento de Ciência da Computação da Universidade de Brasília (UnB), Brasil. Ele recebeu grau de Ph.D. pelo Instituto de Tecnologia da Aeronáutica (ITA), Brasil, em 1994. É bolsista (PQ) do Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) e membro sênior do IEEE. Coordenou diversos projetos de pesquisa da CAPES, CNPq, FINEP, FAPESP, FAPDF e os projetos de cooperação da indústria com a Atech e Boeing Company. Foi co-presidente do BraSNAM 2014, 2015 e atuou em programas e comitês científicos em várias conferências e periódicos internacionais. Ele propôs o mecanismo "Once Learning" para o Parallel Self-organization Map (PSOM) em 1998 como sua principal contribuição científica. O Prof. Li aconselhou cerca de 100 alunos, incluindo alunos de doutorado. Seus interesses de pesquisa incluem inteligência artificial com ênfase em aprendizado de máquina, análise de dados, redes sociais e modelagem computacional em gerenciamento de tráfego aéreo. cv_link: http://lattes.cnpq.br/4218593188956443

Luís Paulo Faina Garcia possui graduação em Engenharia de Computação (2010) e doutorado em Ciências da Computação (2016) pela Universidade de São Paulo. Em 2017 teve a tese classificada entre as melhores pela Sociedade Brasileira de Computação (SBC) e recebeu o prêmio CAPES de melhor tese em Ciência da Computação do país. Atualmente é Professor Adjunto A no Departamento de Ciência da Computação (CIC) da Universidade de Brasília (UnB), em Brasília - Distrito Federal. Tem experiência na área de Ciência da Computação principalmente nos temas relacionados a Mineração de Dados e Aprendizado de Máquina, atuando nas seguintes linhas de pesquisa: detecção de ruídos, meta-aprendizado e fluxo contínuo de dados. cv_link: http://lattes.cnpq.br/1607852138156562



Gabriel Alves Castro é graduando na Universidade de Brasília em Ciência da Computação e Engenharia da Computação (2017-presente), com ênfase em Ciência de dados e inteligência artificial. Completou projeto de iniciação científica, na área de Análise de redes sociais e complexas aplicada ao âmbito da saúde, no contexto das vigilâncias epidemiológica e entomológica brasileiras. Possui interesse nas áreas de computação teórica relacionada à lógica, representação do conhecimento, abstrações, renomeamento de funções, e inteligência artificial sendo que completou um projeto de iniciação científica em cálculo lambda. Fundador e pesquisador com foco em deep learning e sistemas autônomos, neurologia e análise do comportamento na start-up ainda não formalizada Panaceia Inteligente, aonde trabalha atualmente em conjunto com o EsSalud - Peru em uma solução multidisciplinar para o rastreamento de contatos digital. Pesquisa inteligência artificial aplicada à cibersegurança junto ao departamento de ciência da computação da Universidade de Brasília. cv_link: http://lattes.cnpq.br/9518234894816462.

Agradecimentos

O Workshop Brasileiro de Análise de Redes Sociais e Mineração (BraSNAM) chegou em sua 10ª edição em 2022. Nos últimos anos, este evento teve um número expressivo de publicações, um grande público e se tornou um importante fórum de discussão e troca de conhecimento no Brasil nesta área. Obrigado pelo convite especial da comissão organizadora do BraSNAM 2021.