JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

One Time Print: A Tool to Corrupt Files

[1]Meghali Kalyankar, [2]Arya Gaikwad, [3]Siddhant Mavani, [4]Krish Shah, [5]Sameer Shah

[1]Project Mentor SAKEC, [2, 3, 4, 5]Engineering Student
[1, 2, 3, 4, 5]Department of Cyber Security
[1, 2, 3, 4, 5]Shah & Anchor Kutchhi Engineering College, Mumbai, India

Abstract : The rise of digitalization has led to increased concerns about data security and privacy, prompting the exploration of innovative solutions such as self-deleting PDF applications. This report delves into the concept, development, and implications of creating a tool that enables the automatic deletion of PDF files after a single use, aiming to safeguard confidential information. The necessity for such a tool stems from the challenges of controlling the dissemination of sensitive data once shared in digital formats, highlighting the risks of unauthorized access and information leakage. While this technology offers enhanced security and control over sensitive information, its implementation necessitates a comprehensive understanding of the technical, practical, and ethical considerations involved. The report assesses the potential benefits and limitations of self-deleting PDFs, emphasizing the importance of respecting user privacy and addressing vulnerabilities. Additionally, it references relevant studies, emphasizing the significance of addressing JavaScript malware in PDFs, secure PDF merging, and enhanced PDF reader capabilities. Furthermore, the report touches upon the critical challenges and innovative solutions in data storage, integrity verification, metadata management, software vulnerability detection, and machine learning, demonstrating a concerted effort to improve data-centric technologies. Finally, the report discusses the design considerations and security measures for a printing website, highlighting the importance of data protection and compliance with privacy regulations. The proposed One Time Print (OTP) approach is emphasized for its prioritization of user privacy and minimized data storage requirements, positioning it as a viable solution for ensuring secure and efficient digital document printing.

IndexTerms **– Meta-data, Hex-data, Cryptography, Bash Files, Batch Files, Malware, PDF, Windows Defender.**

I. INTRODUCTION

A self-deleting PDF application may become one of the viable ways to ensure confidentiality by making such documents secure and inaccessible after their use. This is a form of software that will erase the pdf file after being opened/viewed only once so as to prevent illegal accesses and copying. The report examines if it is possible develop such a tool and its associated issues surrounding the development itself.

However, the concept of self-deleting files raises some important technical, practical and ethical concerns. This report analyzes the creation, usage and even challenges associated with such a device, including possible applications, limitations and security vulnerabilities.

1.1 Need of the project

This leads to the conceptualization of a delete-a-pdf-after use tool from a PC. There results into the need for an automatic PDF deletion software, which is a response to the current concerns of data security and privacy as we advance towards the age of digitization. PDF files are commonly used for exchanging highly private and secret material—both on enterprises' premises, universities, colleges, or in our everyday lives. Given that a PDF is difficult to stop after distribution into an external environment its exposure to multiple openings and storage areas cannot be controlled. The absence of control may result to a leakage of data or unlawful diffusion and exposure of private information. These issues are resolved through the self-deleting PDF tool, which can allow the user to view the information just once and eliminate the likelihood for unwanted exposure and possible information leakage. Even though it might not be ideal for all situations, it represents a move forward towards more secure documents, with greater control over confidential details in the digital world. The self-deleting PDF tool has its usefulness but at the same time, it's also imperative to think about the possible downfalls of this utility. listade. Though it is possible for an individual to design new ways of getting around such devices, or that there are possible user privacy and data management issues. This tool must be fully comprehended concerning its possible effects while ensuring users' right and privacy perception.

1.2. Motivation behind our project

Developing a new instrument whose purpose would be to erase a single-use pdf out of the computer is based upon the increasing attention paid to confidentiality of information and data safety. The threats that come along with an increased dependency on electronic or digital documents include information leaking, losing access to files and theft. The document format of PDF is pervasive and used for sharing secret documents in private and business settings. However, managing this distribution and access once a PDF is shared becomes hard. Such a tool has aimed at providing individuals and organizations with precise control on their digital property. In addition, this enables the sender to determine whether the recipient will view the document just once and therefore cuts down the chance of leakages or re-forwarding of the data. It caters to the recent demands of strengthened data security and privacy amid a growing culture of document sharing with minimal security measures.

1.3. Conclusion

In conclusion, the concept of a self-deleting PDF application presents a promising solution to the persistent challenges of data security and privacy in an increasingly digitalized world. By addressing the need for greater control over confidential information, this tool represents a significant step forward in the protection of sensitive data shared across various platforms. Its potential to limit unauthorized access and prevent data leakage is particularly valuable in contexts where the dissemination of sensitive information must be closely monitored. However, the development and implementation of such a tool must be approached with careful consideration of the technical, practical, and ethical implications involved. While the tool demonstrates a proactive approach to enhancing document security, it remains essential to anticipate and address potential vulnerabilities and user privacy concerns, ensuring that the rights and perceptions of users are respected throughout its deployment. Moreover, continual assessment and adaptation will be necessary to maintain the effectiveness and reliability of the tool in the face of evolving digital threats and user behaviors.

II. Review of Literature

2.1 Reference papers

[1] In this paper “Is eval () Evil : A study of JavaScript in PDF malware”, we understand that client-side attacks, particularly through third-party software like Adobe's Acrobat Reader, have gained prominence. The study focuses on the distinct nature of JavaScript within malicious PDFs compared to non-malicious ones. Analyzing samples from VirusTotal Intelligence, the research highlights significant disparities in keyword distribution, revealing that malware JavaScript utilizes unique obfuscation techniques and triggers code generation not present in normal files. Notably, the absence of keywords associated with standard PDF automation tasks further differentiates malicious JavaScript. This empirical evidence supports existing inferences on detecting malicious JavaScript in PDFs and offers valuable insights for developing a classifier based on keyword distributions.

[2] In this paper “SecureCMerge: Secure PDF Merging over Untrusted Servers”, we learned that the common practice of merging PDF files through online tools and cloud services can compromise the confidentiality of sensitive data. To address this, the authors introduce SecureCMerge, a secure method for merging PDF files via free online merge sites. Their approach involves encrypting the content of PDF files using Shamir's Secret Sharing (SSS) scheme before uploading them to the merge server. Highlighting the merge homomorphic nature of the SSS scheme, the method ensures information-theoretic security. Experimental results indicate that SecureCMerge achieves secure PDF merging with an acceptable computation time and size overhead.

[3] In this paper “A PDF reader based on SM2 algorithm”, we understood that electronic signatures are crucial for securing electronic documents, with PDF readers serving as effective carriers for such signatures. However, many existing PDF readers lack support for national cryptography algorithm libraries, relying instead on popular SHA and RSA algorithms. To address this gap, the authors developed a PDF reader using PKI/CA systems, PDF document parsing technology, and C# technology, enabling support for national cryptography algorithms. Leveraging ActiveX control and USBKey technologies, the reader successfully facilitates various signature and verification operations, both online and offline. Additionally, the system allows customization of signature and verification processes, enhancing its versatility.

[4] This paper “Breaking the Specification: PDF Certification”, highlights the significance of certification signatures in PDFs, enabling complex workflows with specific document alterations without compromising the signature. It introduces two new attack classes, Evil Annotation, and Sneaky Signature attacks, exploiting PDF specification flaws. These attacks allow for unauthorized modifications to certified documents without detection in various PDF viewer applications. The study emphasizes the need for improved security measures, proposing specific countermeasures and enhancements to the current PDF specification to mitigate these vulnerabilities.

[5] In this paper “HEX-BLOOM: An Efficient Method for Authenticity and Integrity Verification in Privacy-preserving Computing”, the limitations of the computationally expensive Merkle tree in verifying data integrity and authenticity in various applications are highlighted. The proposed alternative, HEX-BLOOM, employs a combination of hash, Exclusive-OR, and Bloom Filter, eliminating the dependency on network latency for data block verification. HEX-BLOOM utilizes an approximation model, Bloom Filter, and a deterministic model for final verification, showcasing superior performance compared to the conventional Merkle tree in terms of computational cost and network traffic reduction.

2.2 Keywords

- Hex-data
- Meta-data
- Windows Defender
- Batch Files
- Bash Files
- PDF
- Malware

III. Comparative Analysis

3.1 Overview

The overabundance of small files in HDFS/MapReduce for large-scale data analytics is a significant challenge. A mechanism is proposed to efficiently store small files in HDFS and improve metadata space utilization. The compression method 'harballing' provided by Hadoop is used to better utilize HDFS. New job functionality is introduced for in-job archival of directories and files, allowing MapReduce programs to complete without being killed by JobTracker due to quota policies. The Robust Integrity Verification Algorithm (RIVA) is proposed to strengthen the integrity of file transfers by forcing checksum computation tasks to read files directly from disk. A blockchain-based ledger architecture is presented to store the checksum of frequently accessed scientific

datasets, minimizing performance overhead. A file system metadata accelerator (FSMAC) is proposed to optimize metadata access by efficiently exploiting the advantages of Nonvolatile Memory (NVM).
Efficient metadata management is crucial for system performance in large distributed storage systems. Two common techniques, directory subtree partitioning and pure hashing, suffer from bottlenecks at high concurrent access rates. A new approach called lazy hybrid (LH) metadata management combines the best aspects of these two approaches while avoiding their shortcomings. A method to detect, assess, and mitigate OSS vulnerabilities is proposed, which is code-centric and uses static and dynamic analysis to determine the reachability of vulnerable libraries. Vulas, a tool implementing this code-centric approach, has been recommended by SAP for Java software scanning. Machine Learning models require vast amounts of data for accurate training, but the excessive computational overhead of the security protocol makes it impractical.

3.2 Conclusion

In conclusion, the diverse array of research contributions discussed in the analysis sheds light on various critical challenges and innovative solutions within the domain of data storage, integrity verification, metadata management, software vulnerability detection, metadata standards, and machine learning. The proposed mechanisms and algorithms demonstrate a concerted effort to enhance the efficiency, security, and resilience of large-scale data analytics, file system performance, and collaborative learning processes, addressing issues such as overabundant small files, data corruption, performance overhead, and integration constraints. These solutions, including RIVA for end-to-end integrity verification, the blockchain-based ledger architecture for checksum storage, FSMAC for file system metadata acceleration, LH metadata management, Vulas for OSS vulnerability detection, and the incorporation of Secret Sharing in FTL, collectively represent a significant stride in advancing data-centric technologies while ensuring robust security measures, optimized performance, and streamlined collaboration among diverse stakeholders. Continued research and implementation of these advancements are vital for fostering sustainable and secure data-driven ecosystems, promoting knowledge sharing, and nurturing a more interconnected and efficient technological landscape.

IV. RESEARCH SUMMARY

4.1 Overview

The website's security measures include data privacy, code vulnerabilities, file compatibility, print options, confirmation and logging, and secure file deletion mechanisms. It should also assess user experience, including ease of use, speed and efficiency, notifications, and maintenance.
The website should be well-documented and modular, with easy-to-update backend code. It should also handle updates and patches for security and functionality improvements. Scalability should be considered, considering the website's architecture and performance under heavy load.
Compliance with data protection and privacy regulations is crucial, especially if handling sensitive or personal data. Cost and resource requirements should be considered, including hosting, storage, and potential licensing fees for third-party components. User support and documentation should be available to assist users with troubleshooting and printing issues.
User feedback and reviews should be sought to gauge user satisfaction and identify potential issues or shortcomings. Overall, the website should be secure, user-friendly, and efficient, with a focus on user satisfaction and compliance with regulations.
A normal printing website is a service that allows users to order and print physical copies of digital files, such as documents, photos, or artwork. However, it can raise privacy and security concerns, especially if sensitive information is involved. One Time Print (OTP) websites prioritize user privacy and data security by immediately deleting files after printing, minimizing the risk of data exposure or unauthorized access.
Normal printing websites store files for a certain period, which can lead to potential risks if the website is compromised or files are accessed without authorization. On the other hand, OTP files are not stored beyond the immediate printing process, minimizing the risk of data exposure or unauthorized access.
Users may find it convenient to have their files stored for reordering or reference, but OTP may require re-uploading for additional copies or changes to the printed material. Storing files can consume server resources and require data management practices, increasing operational costs.
One Time Print (OTP) reduces the need for file storage and management, making it cost-effective. Legal and compliance considerations may be necessary for OTP, but it aligns more easily with data protection and privacy regulations since files are not retained.

4.2 Conclusion

In conclusion, the comprehensive research overview delves into the intricacies of designing and implementing a secure, user-friendly, and compliant printing website, highlighting key considerations encompassing security measures, user experience, maintenance, scalability, and resource management. Emphasizing the significance of data protection and privacy regulations, the summary underscores the critical need for robust security protocols, immediate file deletion mechanisms, and adherence to privacy standards to mitigate potential risks associated with unauthorized access and data exposure. While acknowledging the potential trade-offs in user convenience and operational costs, the One Time Print (OTP) approach emerges as a compelling solution that prioritizes user privacy and minimizes data storage and management overhead. By prioritizing security, user satisfaction, and regulatory compliance, the proposed OTP model presents a promising avenue for addressing the privacy and security concerns associated with traditional printing websites, ultimately paving the way for a more secure and streamlined user experience in the digital realm.

V. PROJECT SUMMARY

5.1 Overview

The ongoing endeavor to develop an application for the automatic deletion of PDF files marks a significant step in the realm of digital document security. At its core, this project aims to address the pressing concerns surrounding data confidentiality, privacy, and secure information management. Through a systematic approach that integrates comprehensive research, rigorous testing, and meticulous development, the project endeavors to provide a robust and user-friendly solution for managing sensitive digital content.

The initial phase of the project emphasizes an in-depth analysis of the technological, ethical, and legal dimensions associated with the implementation of the self-deleting PDF application. Extensive research efforts are directed towards identifying potential challenges and opportunities, thereby laying the groundwork for the subsequent stages of development and testing. By delving into the intricate details of user interface design and file accessibility, the project team strives to create an intuitive and user-friendly platform that fosters a seamless and secure user experience.

Furthermore, the research team places a significant emphasis on evaluating the potential safety implications and privacy concerns that may arise with the deployment of such an innovative application. The ethical implications of the technology are carefully scrutinized to ensure that the project adheres to established industry standards and best practices. By fostering a culture of responsible data management and user privacy, the project seeks to instill confidence among users regarding the secure handling of their confidential documents.

As the project progresses into the developmental and testing phases, meticulous attention is devoted to refining the application's features and functionalities. Through a comprehensive testing protocol that incorporates user feedback and real-world simulations, the team endeavors to optimize the application's performance and user experience. The ultimate goal is to deliver a reliable, efficient, and user-friendly application that not only meets the stringent requirements of data security but also aligns with the evolving needs of a digital-savvy user base.

In conclusion, the project's comprehensive approach to addressing the complex challenges of digital document security reflects a commitment to excellence and innovation in the field. By leveraging cutting-edge technologies and ethical best practices, the project aims to establish a new standard for secure document management, ultimately empowering users with a reliable and intuitive solution for safeguarding their sensitive digital content.

5.2 Conclusion

In conclusion, the project's comprehensive focus on developing an automatic PDF deletion application underscores a commitment to advancing the field of digital document security. By meticulously navigating the intricate landscape of technological, ethical, and legal considerations, the project team demonstrates a dedicated approach to fostering a secure and user-friendly environment for managing confidential digital content. Through a systematic integration of robust research, thoughtful development, and rigorous testing, the project endeavors to instill confidence among users by providing an intuitive and reliable solution for safeguarding sensitive documents. By prioritizing user privacy, data security, and ethical data management practices, the project seeks to set a new benchmark in the realm of secure document handling, catering to the evolving needs of a technologically adept user base. With a relentless commitment to excellence and innovation, the project aspires to establish itself as a pioneering force in the domain of digital document security, thereby contributing to a more secure and trustworthy digital ecosystem.

VI. CONCLUSION

The development of a self-deleting PDF application represents a significant stride towards ensuring enhanced document security and privacy in the digital realm. Through a comprehensive analysis of the technical, practical, and ethical considerations, it becomes apparent that this innovative solution addresses critical concerns related to data confidentiality, unauthorized access, and information leakage.

The notion of a self-deleting PDF application introduces a sophisticated yet intuitive approach to safeguarding sensitive information, particularly in contexts where sharing confidential documents is commonplace. By enabling users to exert greater control over document accessibility and preventing unauthorized dissemination, this tool serves as a proactive measure against potential data breaches and privacy infringements.

Despite the potential benefits offered by this technology, it is crucial to acknowledge the associated challenges and ethical implications. Issues such as user privacy concerns, potential workarounds, and data management intricacies must be carefully examined to ensure the responsible and ethical deployment of this application.

As the project progresses from the research phase towards development and testing, it is imperative to maintain a steadfast focus on user-centric design principles and rigorous testing protocols. This approach will facilitate the creation of a robust, user-friendly application that not only aligns with the evolving landscape of data security but also fosters a culture of responsible information management and privacy protection.

In sum, the self-deleting PDF application represents a proactive step towards establishing a secure digital environment, empowering individuals and organizations to exercise greater control over the confidentiality and integrity of their sensitive documents. The successful implementation of this project stands to redefine the standards of data security and privacy in an increasingly digital world.

VII. ACKNOWLEDGMENT

We have great pleasure in presenting the project on “One Time Print: A tool to Corrupt Files”. We take this opportunity to express our sincere thanks to our Guide, Ms. Meghali Kalyankar, the faculty in the Department of Cyber Security in Shah and Anchor Kutchhi Engineering College for guiding us and suggesting regarding the line of work. We would like to express our gratitude towards their constant encouragement, support and guidance throughout the progress.

Also, we would like to thank our Principal Dr. Bhavesh Patel and Head of Cyber Security Department Dr. Nilakshi Jain, for their help, support & guidance for this project.

We are also thankful to all Faculty members of our department for help and guidance during completion of our project

.

REFERENCES

[1] Y. Kulkarni and A. Gorkar, "Intensive Image Malware Analysis and Least Significant Bit Matching Steganalysis," 2020 IEEE International Conference on Big Data (Big Data), Atlanta, GA, USA, 2020, pp. 2309-2317, doi: 10.1109/BigData50022.2020.9377974.

[2] R. Patgiri and M. D. Borah, "HEX-BLOOM: An Efficient Method for Authenticity and Integrity Verification in Privacy-preserving Computing," 2022 IEEE International Performance, Computing, and Communications Conference (IPCCC), Austin, TX, USA, 2022, pp. 397-403, doi: 10.1109/IPCCC55026.2022.9894352

[3] Rismayani and C. Susanto, "Using AES and DES Cryptography for System Development File Submission Security Mobile-Based," 2020 8th International Conference on Cyber and IT Service Management (CITSM), Pangkal, Indonesia, 2020, pp. 1-7, doi: 10.1109/CITSM50537.2020.9268805.

[4] J. J. Lee, J. H. Kim, J. B. Park and J. W. Jeon, "Analysis of Combination HEX and Minimal HEX Reprogramming Methods Using UDS Protocol," 2023 International Technical Conference on Circuits/Systems, Computers, and Communications (ITC-CSCC), Jeju, Korea, Republic of, 2023, pp. 1-6, doi: 10.1109/ITC-CSCC58803.2023.10212492.

[5] S. C. Nayak, V. Tiwari and B. K. Samanthula, "Review of Ransomware Attacks and a Data Recovery Framework using Autopsy Digital Forensics Platform," 2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 2023, pp. 0605-0611, doi: 10.1109/CCWC57344.2023.10099169.

[6] I. M. A. D. S. Atmaja, I. N. G. A. Astawa, N. W. Wisswani, I. M. R. A. Nugroho, P. W. Sunu and I. K. Wiratama, "Document Encryption Through Asymmetric RSA Cryptography," 2020 International Conference on Applied Science and Technology (iCAST), Padang, Indonesia, 2020, pp. 46-49, doi: 10.1109/iCAST51016.2020.9557723.

[7] N. Sharma, P. Singh and P. K. Atrey, "SecureCMerge: Secure PDF Merging over Untrusted Servers," 2018 IEEE Conference on Multimedia Information Processing and Retrieval (MIPR), Miami, FL, USA, 2018, pp. 402-407, doi: 10.1109/MIPR.2018.00087.

[8] S. Rohlmann, V. Mladenov, C. Mainka and J. Schwenk, "Breaking the Specification: PDF Certification," 2021 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 2021, pp. 1485-1501, doi: 10.1109/SP40001.2021.00110.

[9] A. Lemay and S. P. Leblanc, "Is eval () Evil : A study of JavaScript in PDF malware," 2018 13th International Conference on Malicious and Unwanted Software (MALWARE), Nantucket, MA, USA, 2018, pp. 1-10, doi: 10.1109/MALWARE.2018.8659374.

[10] O. P. Samantray, S. N. Tripathy and S. K. Das, "Notice of Violation of IEEE Publication Principles: A study to Understand Malware Behavior through Malware Analysis," 2019 IEEE International Conference on System, Computation, Automation and Networking (ICSCAN), Pondicherry, India, 2019, pp. 1-5, doi: 10.1109/ICSCAN.2019.8878680.

[11] M. A. Ayub and A. Sirai, "Similarity Analysis of Ransomware based on Portable Executable (PE) File Metadata," 2021 IEEE Symposium Series on Computational Intelligence (SSCI), Orlando, FL, USA, 2021, pp. 1-6, doi: 10.1109/SSCI50451.2021.9660019.

[12] M. O. F. Rokon, P. Yan, R. Islam and M. Faloutsos, "Repo2Vec: A Comprehensive Embedding Approach for Determining Repository Similarity," 2021 IEEE International Conference on Software Maintenance and Evolution (ICSME), Luxembourg, 2021, pp. 355-365, doi: 10.1109/ICSME52107.2021.00038.

[13] A. Corum, D. Jenkins and J. Zheng, "Robust PDF Malware Detection with Image Visualization and Processing Techniques," 2019 2nd International Conference on Data Intelligence and Security (ICDIS), South Padre Island, TX, USA, 2019, pp. 108-114, doi: 10.1109/ICDIS.2019.00024.

[14] I. Baptista, S. Shiaeles and N. Kolokotronis, "A Novel Malware Detection System Based on Machine Learning and Binary Visualization," 2019 IEEE International Conference on Communications Workshops (ICC Workshops), Shanghai, China, 2019, pp. 1-6, doi: 10.1109/ICCW.2019.8757060.

[15] T. M. Mohammed, L. Nataraj, S. Chikkagoudar, S. Chandrasekaran and B. S. Manjunath, "HAPSSA: Holistic Approach to PDF malware detection using Signal and Statistical Analysis," MILCOM 2021 - 2021 IEEE Military Communications Conference (MILCOM), San Diego, CA, USA, 2021, pp. 709-714, doi: 10.1109/MILCOM52596.2021.9653097.

[16] Ö. A. Aslan and R. Samet, "A Comprehensive Review on Malware Detection Approaches," in IEEE Access, vol. 8, pp. 6249-6271, 2020, doi: 10.1109/ACCESS.2019.2963724.

[17] X. Xing, X. Jin, H. Elahi, H. Jiang and G. Wang, "A Malware Detection Approach Using Autoencoder in Deep Learning," in IEEE Access, vol. 10, pp. 25696-25706, 2022, doi: 10.1109/ACCESS.2022.3155695.

[18] R. Kumar, K. Sethi, N. Prajapati, R. R. Rout and P. Bera, "Machine Learning based Malware Detection in Cloud Environment using Clustering Approach," 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kharagpur, India, 2020, pp. 1-7, doi: 10.1109/ICCCNT49239.2020.9225627.

[19] P. Anantharaman, R. Lathrop, R. Shapiro and M. E. Locasto, "PolyDoc: Surveying PDF Files from the PolySwarm network," 2023 IEEE Security and Privacy Workshops (SPW), San Francisco, CA, USA, 2023, pp. 117-134, doi: 10.1109/SPW59333.2023.00017.

[20] O. Suciu, S. E. Coull and J. Johns, "Exploring Adversarial Examples in Malware Detection," 2019 IEEE Security and Privacy Workshops (SPW), San Francisco, CA, USA, 2019, pp. 8-14, doi: 10.1109/SPW.2019.00015.

[21] A. Alhussen and E. Arslan, "RIVAChain: Blockchain-based Integrity Verification for File Transfers," 2020 IEEE International Conference on Big Data (Big Data), Atlanta, GA, USA, 2020, pp. 3255-3261, doi: 10.1109/BigData50022.2020.9378235.

[22] B. Charyyev, A. Alhussen, H. Sapkota, E. Pouyoul, M. H. Gunes and E. Arslan, "Towards Securing Data Transfers Against Silent Data Corruption," 2019 19th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID), Larnaca, Cyprus, 2019, pp. 262-271, doi: 10.1109/CCGRID.2019.00040.

[23] B. Charyyev and E. Arslan, "RIVA: Robust Integrity Verification Algorithm for High-Speed File Transfers," in IEEE Transactions on Parallel and Distributed Systems, vol. 31, no. 6, pp. 1387-1399, 1 June 2020, doi: 10.1109/TPDS.2020.2966616.

[24] S. Sharma, C. Xing, Y. Liu and Y. Kang, "Secure and Efficient Federated Transfer Learning," 2019 IEEE International Conference on Big Data (Big Data), Los Angeles, CA, USA, 2019, pp. 2569-2576, doi: 10.1109/BigData47090.2019.9006280.