iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** VI **Month of publication:** June 2023

DOI: https://doi.org/10.22214/ijraset.2023.54446

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VI Jun 2023- Available at www.ijraset.com

Client-Side Encryption Based Secure Data Sharing Schemes for Cloud Platforms

B. Rama Murthi[1], A.V.N. Sai Akshay[2], N. Divya Sruthi[3]
[1, 2]*UG Scholar, Department of CSE, Geethanjali Institute of Science & Technology, Nellore, A.P*
[3]*Assistant Professor, Department of CSE, Geethanjali Institute of Science & Technology, Nellore, A.P*

Abstract: ***With more and more data moving to the cloud, privacy of user data have raised great concerns. Client-side encryption/decryption seems to be an attractive solution to protect data security, however, the existing solutions encountered three major challenges: low security due to encryption with low-entropy PIN, inconvenient data sharing with traditional encryption algorithms, and poor usability with dedicated software/plugins that require certain types of terminals. This work designs and implements Web Cloud, a practical browser-side encryption solution, leveraging modern Web technologies. It solves all the above three problems while achieves several additional remarkable features: robust and immediate user revocation, fast data processing with offline encryption and outsourced decryption. Notably, our solution works on any device equipped with a Web user agent, including Web browsers, mobile and PC applications. We implement Web Cloud based on own Cloud for basic file management utility, and utilize Web Assembly and Web Cryptography API for complex cryptographic operations integration. Finally, comprehensive experiments are conducted with many well-known browsers, Android and PC applications, which indicates that WebCloud is cross-platform and efficient. As an interesting by-product, the design of Web Cloud naturally embodies a dedicated and practical ciphertext- policy attribute-based key encapsulation mechanism (CP-AB-KEM) scheme, which can be useful in other applications.***

Keywords: AWS, WEBCLOUD, CPABE, Cryptography, ciphertext

I. INTRODUCTION

Public cloud storage service becomes increasingly popular due to cost reduction and good data usability for users. This trend has prompted users and corporations to store (unencrypted) data on public cloud, and share their cloud data with others. Using a cloud for high-value data requires the user to trust the server to protect the data from unauthorized disclosures. This trust is often misplaced, because there are many ways in which confidential data leakage may happen, e.g. these data breaches reported. To counteract data leakage, one of the most promising approaches is client-side encryption/decryption. Concretely, client-side encryption allows senders to encrypt data before transmitting it to clouds, and decrypt the data after downloading from clouds. In this way, clouds only obtain encrypted data, thus making server-side data exposure more difficult or impossible. At the same time, as a crucial functionality of cloud storage, flexible file sharing with multiple users or a group of users must be fully supported. However, existing client-side encryption solutions suffer from more or less disadvantages in terms of security, efficiency and usability. Known Client-Side Encryption Solutions. We review existing solutions and point out their limitations. Many cloud storage providers, including Google Drive and Drop box, do not provide support for client- side encryption. They adopt server-side encryption for files stored, TLS for data at transit, and two- factor authentication for user authentication. Apple I Cloud supports end-to end encryption for sensitive information, e.g., I Cloud Keychain, Wi-Fi passwords. For other data uploaded to I Cloud, only server encryption is adopted. Some products use symmetric encryption (typically AES) to encrypt users' data and then upload cipher texts to clouds. However, in these schemes, the cryptographic keys are derived from a password/ passphrase or even a 4-digit PIN. Relying on such low entropy is considered unsafe . Worse still, most password-based solutions only deal with the case of single-user file encryption and decryption, and do not provide any file sharing mechanism. Notably, allows users to generate a share link for each password-protected file. However, users must manually send the share link through one channel, and password to all receivers through another secure channel, which is inconvenient and brittle.

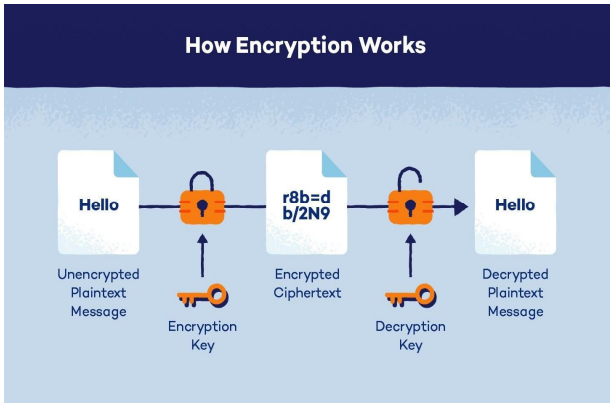
II. LITERATURE SURVEY

Many cloud storage providers, including Google Drive and Drop box, do not provide support for client- side encryption. They adopt server-side encryption for files stored, TLS for data at transit, and two- factor authentication for user authentication. Apple I Cloud supports end-to end encryption for sensitive information, e.g., I Cloud Keychain, Wi-Fi passwords. For other data uploaded to I Cloud, only server encryption is adopted.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VI Jun 2023- Available at www.ijraset.com

A. Password-Based Solutions

Some products use symmetric encryption (typically AES) to encrypt users' data and then upload ciphertexts to clouds. However, in these schemes, the cryptographic keys are derived from a password/ passphrase or even a 4-digit PIN. Relying on such low entropy is considered unsafe . Worse still, most password-based solutions only deal with
the case of single-user file encryption and decryption, and do not provide any file sharing mechanism. Notably, allows users to generate a share link for each password-protected file.
However, users must manually send the share link through one channel, and password to all receivers through another secure channel, which is inconvenient and brittle.



B. Hybrid Encryption Scheme

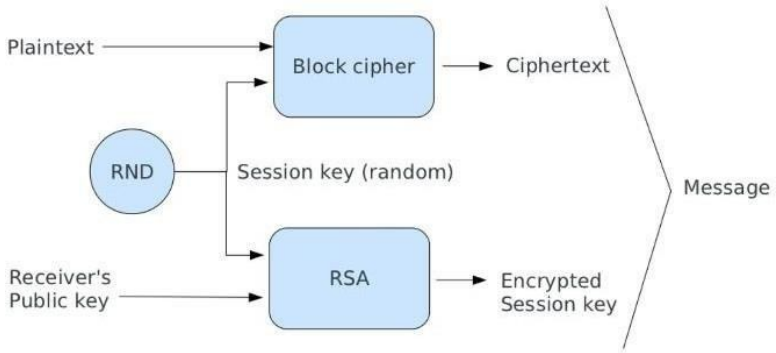
The cloud adopts a key encapsulation mechanism (KEM) and a data encapsulation mechanism (DEM), so called the KEM-DEM setting. Many public cloud service providers, including Amazon , Tresor it and Mega , adopt the RSA-AES paradigm. Users generate RSA key pairs and apply for certificates from the providers, who build and maintain a Public Key Infrastructures (PKI). Users encrypt data under fresh sampled AES keys, which are further encrypted under all recipients' RSA public keys.
This file sharing mechanism is inflexible and inefficient. A sender needs to obtain and specify the public keys of all receivers during encryption. Even worse, the size of the cipher text and encryption workload are proportional to the number of recipients, resulting in greater bandwidth and storage costs and more user expenditure.

C. Limitations of the Existing Solutions

Three drawbacks exist in above-mentioned solutions:

1) Comparatively poor security,
2) Coarse-grained access control, inflexible and inefficient file sharing, and
3) Poor usability.

The first two are easy to see and we now elaborate the usability issue. Typically, users use different terminals to upload files, including desktop, Web and mobile applications. However, almost all the existing solutions require additional software or plugins, thus limiting users' devices and platforms. When switching to a new device, users need to repeat the boring installation process, whichgreatly increases users' burden thus decreases usability.



ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VI Jun 2023- Available at www.ijraset.com

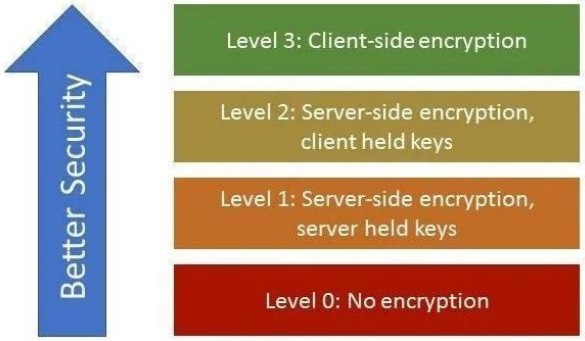
III.METHODOLOGY

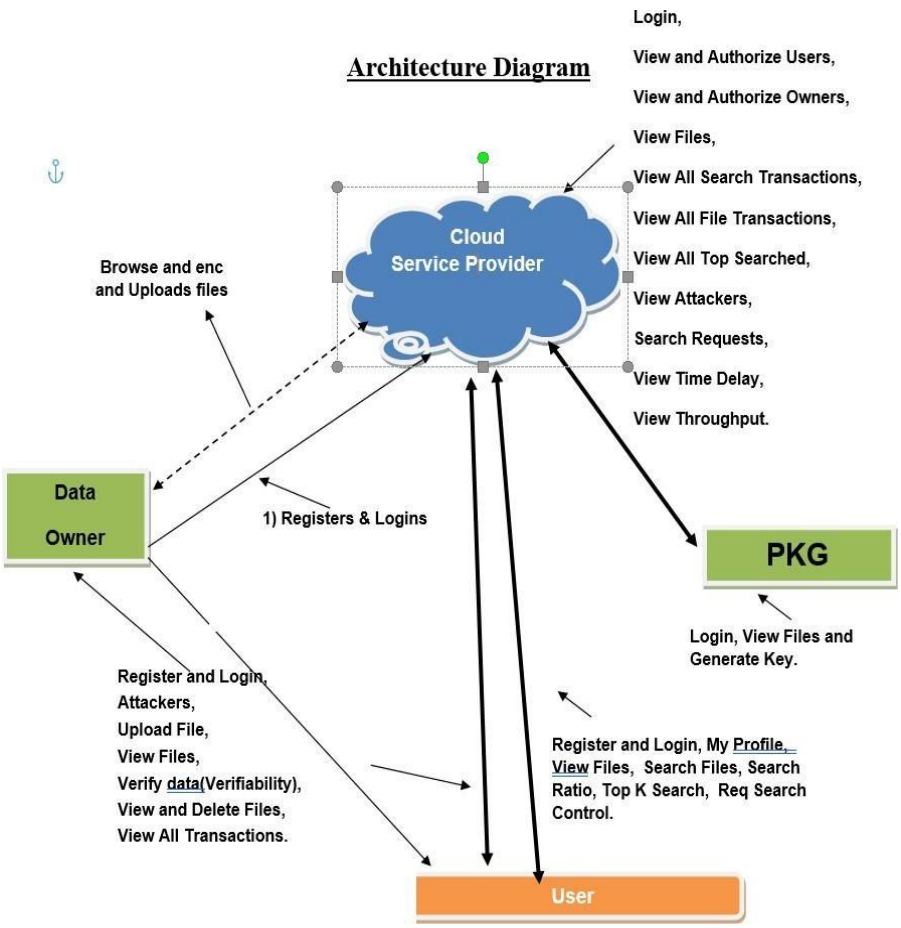
A. Client Side Encryption

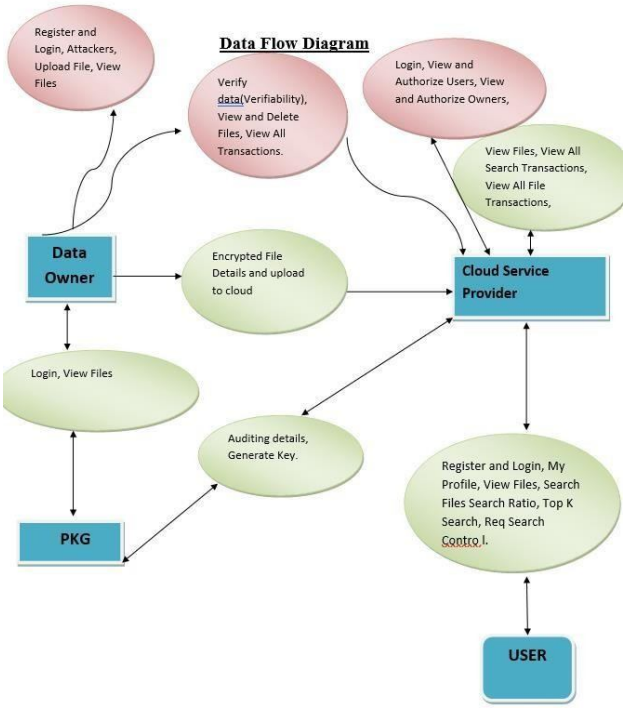
Client-side encryption is not about transport encryption. The point of client-side encryption is not whether an eavesdropper can capture your communication on the way to a server. Rather it's about encrypting data without involving another party (i.e. the service provider, "the server") in the process.

Client-side encryption just means that the server doesn't encrypt the data which it's storing for a user by itself, but leaves the encryption to the client, giving the client full control over the process. This way the service provider is proving that they can't access the plaintext because they never handled the encryption keys in the first place. In theory, this means you don't need to trust the service provider to handle your data confidentially. (In practice, you'd have to verify that the provided client application actually implements CSE as promised by the provider.)

Whether the client-side-encrypted data is transferred securely (over an encrypted channel between you and the server) is a separate issue.

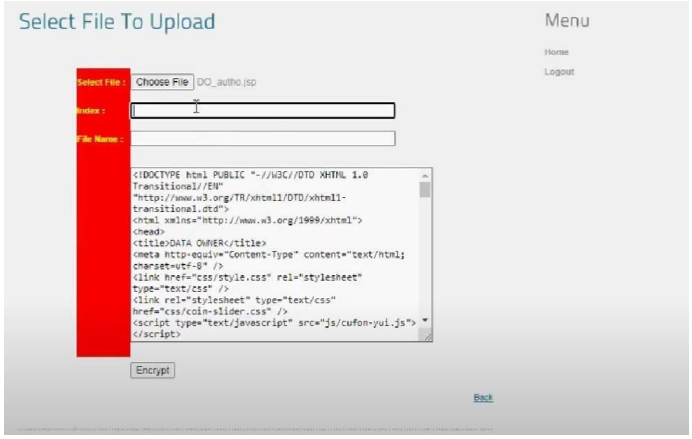


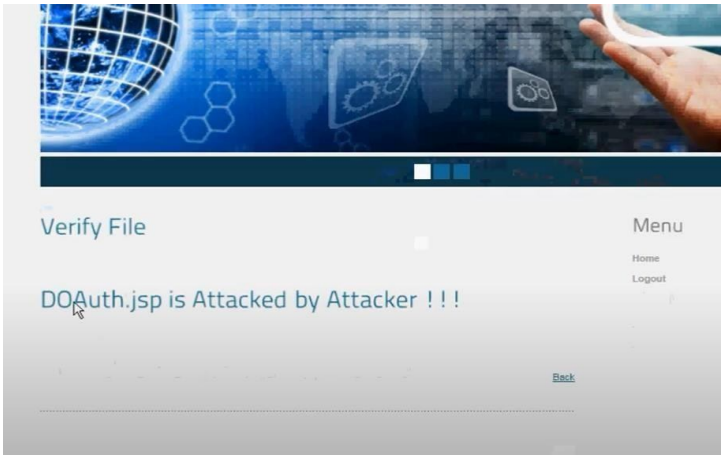




IV. TESTING & RESULTS

The screenshot of the proposed system is as shown in the figure. The front end for the system was designed using Streamlet package.





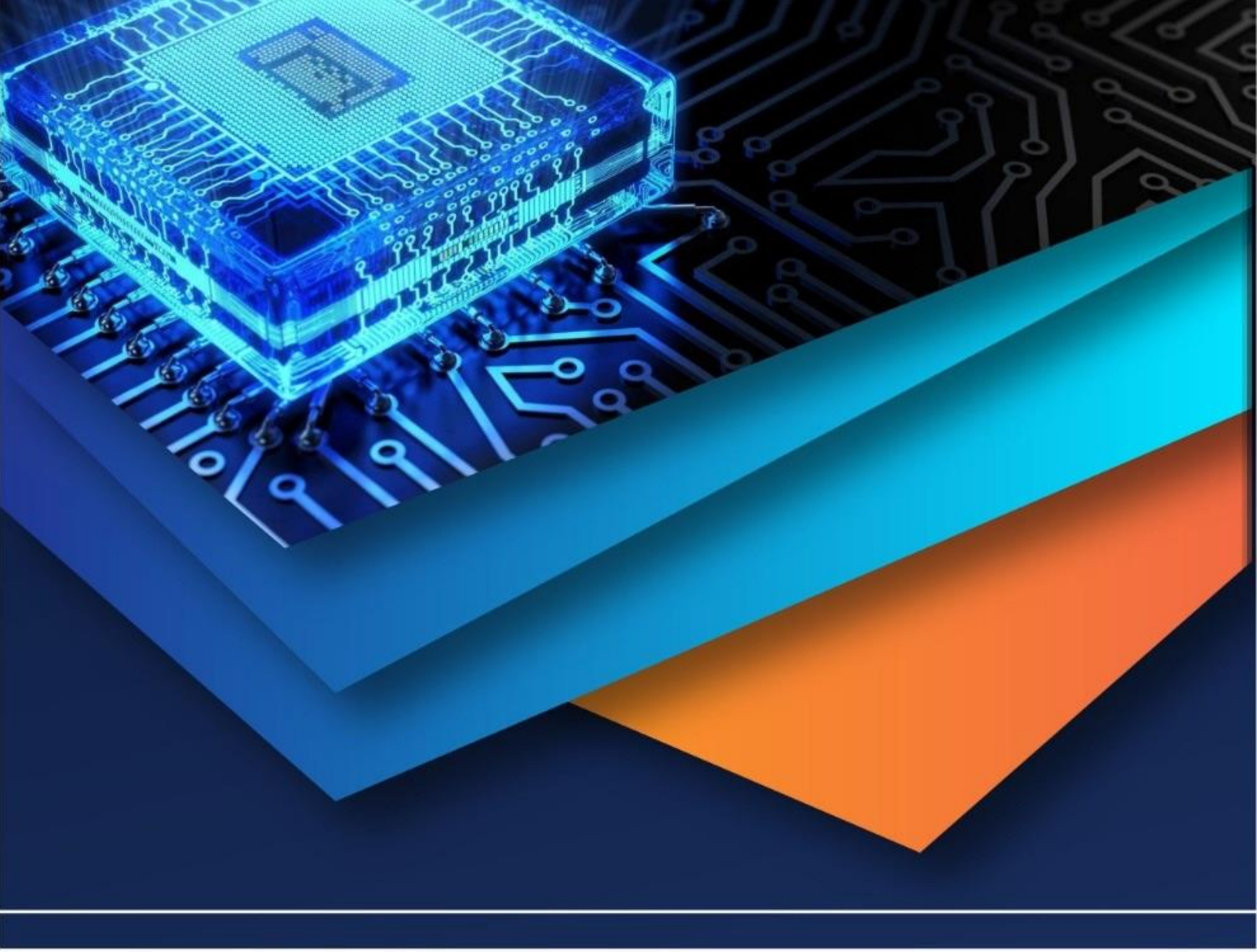
The system was tested by creating an AWS EC2 Instance in cloud and tested by creating several users. The system performed as per the requirements.

V. CONCLUSIONS

We propose Web Cloud, a practical client-side encryption solution for public cloud storage in the Web setting, where users do cryptography with only browsers. We analyze the security of Web Cloud and implement Web Cloud based on own Cloud and conduct a comprehensive performance evaluation. The experimental results show that our solution is practical. As an interesting by-product, the design of Web- Cloud naturally embodies a dedicated CP-AB-KEM scheme, which is useful in many other applications. After the continues trials and training of the system, we have succeeded to detect and predict the two major things such as helmet detection and license plate recognition with high accuracy of 88% by using CNN with YOLO V8 Algorithm. But there is a scope to acquire 100% of accuracy by using the upcoming and latest technologies developed with Deep Learning, Machine Learning, and Image Processing. We hope for the best and 100% of accuracy to detect helmet and license plate for saving lives. Web cloud storage has become an essential part of our digital lives, allowing us to store and share data with ease. However, as the amount of data we store and share increases, so does the need forenhanced security and improved collaboration across platforms.

REFERENCES

[1] "Vulnearability and threat in 2018," Skybox Security, Tech. Rep., 2018. [Online]. Available: https://lp.skyboxsecurity.com/ WICD-2018-02-Report-Vulnerability-Threat-18 Asset.html
[2] D. Lewis, "icloud data breach: Hacking and celebrity photos," Duo Security, Tech. Rep., September 2014. [Online]. Available: https://www.forbes.com/sites/davelewis/2014/09/ 02/icloud-data-breach-hacking-and-nude-celebrity-photos
[3] T. Hunt, "Hacked dropbox login data of 68 million users is now for sale on the dark web," Tech. Rep., September 2016. [Online]. Available: https://www.troyhunt.com/the-dropbox-hack-is-real/
[4] "Amazon data leak," ElevenPaths, Tech. Rep., November 2018. [Online]. Available: https://www.elevenpaths.com/ amazon-data-leak/index.html
[5] K. Korosec, "Data breach exposes trade secrets of carmakers gm, ford, tesla, toyota," TechCrunch, Tech. Rep., July
[6] 2018. [Online]. Available: https://techcrunch.com/2018/07/20/ data-breach-level-one-automakers/
[7] M. Grant, "$93m class-action lawsuit filed against city of calgary for privacy breach," Tech. Rep., October 2017. [Online]. Available: http://www.cbc.ca/news/canada/calgary/city-calgary-class-action-93-million-privacy-breach-1.4321257(2020, April) Secure file transfer — whisply. [Online]. Available: https://whisp.ly/en
[8] (2020, April) Whitepapers from spideroak. [Online]. Available: https://spideroak.com/whitepapers/
[9] W. Ma, J. Campbell, D. Tran, and D. Kleeman, "Password entropy and password quality," in Fourth International Conference on
[10] Network and System Security, NSS 2010, Melbourne, Victoria, Australia, September 1-3, 2010, Y. Xiang, P. Samarati, J. Hu,
[11] W. Zhou, and A. Sadeghi, Eds. IEEE Computer Society, 2010, pp. 583–587. [Online]. Available: https://doi.org/10.1109/NSS.2010. 18 (2020, April)
[12] Aws sdk support for amazon s3 client-side encryption. [Online]. Available: https://docs.aws.amazon.com/ general/latest/gr/aws sdk cryptography.html (2020, April)
[13] Cloud storage security - secure cloud storage from tresorit. [Online]. Available: https://tresorit.com/security (2020, April)
[14] Mega - secure cloud storage and communication. [Online]. Available: https://mega.nz/
[15] E. Bocchi, I. Drago, and M. Mellia, "Personal cloud storage: Usage, performance and impact of terminals," in 4th IEEE International Conference on Cloud Networking, CloudNet 2015, Niagara Falls, ON, Canada, October 5-7, 2015. IEEE, 2015, pp. 106–111. [Online]. Available: https://doi.org/10.1109/CloudNet.2015.7335291
[16] "Web cryptography api," the Web Cryptography WG of the W3C, Tech. Rep., January 2017. [Online]. Available: https://www.w3.org/TR/WebCryptoAPI/
[17] A. Haas, A. Rossberg, D. L. Schuff, B. L. Titzer, M. Holman, D. Gohman, L. Wagner, A. Zakai, and J. Bastien, "Bringing the web up to speed with webassembly," in ACM SIGPLAN Notices.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY