INTERNATIONAL JOURNAL OF TECHNO-ENGINEERING
IJTE
ISSN: 2057-5688

EXCHANGING EXCLUSIVE INFORMATION BETWEEN DEVICES USING ONLINE STORAGE

[1]A. SATYANARAYANA, Professor

[2]TANISH SANGU [3]SARDARPALLY PRAVEEN KUMAR

[2]AKSHAYA MARAM [5]ABHIGNA BANDARI

[6]INDRASEN BURRA

1, 2, 3, 4, 5, 6 Siddhartha Institute of Technology & Sciences, Hyderabad, Telangana, India

ABSTRACT

The necessity to protect user data privacy has grown to be a key worry as data migration to the cloud continues to soar. Client-side encryption/decryption has emerged as a promising method of ensuring data security. Inconvenient data sharing using conventional encryption algorithms, low security caused by inadequate encryption techniques like low-entropy PINs, and poor usability necessitating specialized software/plugins on certain terminals are only a few of the problems that now confront existing solutions. Web Cloud is a feasible browser- side encryption solution that enables for the use of existing online services, according to the study provided here.

Web Cloud successfully addresses these issues and adds exceptional features such as powerful and immediate user revocation, fast data processing via offline encryption, and outsourced decryption. Web Cloud is based on own Cloud and contains its own Web Cryptography API enabling straightforward integration of complex cryptographic operations. Extensive testing on popular web browsers has confirmed Web Cloud's nature and effectiveness.

Web Cloud also has a focused and realistic cipher text-policy attribute-based key encapsulation method (CP-AB-KEM) method. This intrinsic feature has the potential to beuseful in a variety of applications other than Web Cloud, improving access control and security in a variety of circumstances.

1. INTRODUCTION

Client-side encryption is not supported by many cloud storage services, such as Google Drive and Dropbox. They employ TLS for data in transit, server-side encryption for files being stored, and two- factor authentication for user authentication. Users must, however, manually provide the password to each recipient over a separate secure channel and the sharing link through anotherchannel, which is cumbersome and unreliable.

An online client-side encryption tool iscalled Web Cloud. Data encryption anddecryption are done by users utilizing Webagents, such as web browsers. A safe and effective encryption method called Cipher text-Policy Attribute- Based Encryption (CP-ABE), which combines encryption with access control, is suggested. The cloud service does not manage users' private keys; instead, it acts as a storage backend. The growing dependence on cloud storage needs stringent safeguards to maintain user confidentiality and safety of data. Client- side encryption is a possible method for securing sensitive data. Current techniques, however, have hurdles due to insufficient security, difficult data transfer, and poor usability. This article offers Web Cloud, a viable browser-side encryption approach that deals with those problems while offering additional capabilities for increased cloud data security.

2. LITERATURE SURVEY

[1] According to Y. Yuan, C.-M. Cheng,
S. Kiyomoto, Y. Miyake, and T. Takagi, Lattice-based cryptography has attracted a high degree of attention in the cryptologic research community. It is expected to be inwide use in the foreseeable future once large quantum computers are in sight. In addition, JavaScript is a standard programming language for Web applications. It is now supported on a wide variety of computing platforms and devices with immense efficiency improvement in the past few years. In this paper, we present the results of our JavaScript implementation of several Lattice-based encryption schemes and show the speed performance on four common Web browsers on PC. Furthermore, we also show the performance on two smaller computing platforms, namely, tablets running the Android operating system, as well as Tessel, an embedded system equipped with an ARM Cortex-M3-grade microcontroller. Our results demonstrate that some of today's Lattice-based cryptosystems can already have efficient JavaScript implementations and hence are ready for use on a growing list of JavaScript-enabled computing platforms.

[2] According to H. Halpin, The W3C WebCryptography API is the standard API for accessing cryptographic primitives in Javascript-based environments. We describe the motivations behind the creation of the W3C Web Cryptography API and givea high-level overview with motivating use-cases while addressing objections.

[3] According to Z. Guan, Z. Cao, X. Zhao,
R. Chen, Z. Chen, and X. Nan, The growing popularity of web applicationsin the last few years has led users to give the management of their data to online application providers, which will endangerthe security and privacy of the
users. In this paper, we present WebIBC, which integrates public key cryptography into web applications without any browser plugins. The
public key of WebIBC is provided by identity based cryptography, eliminating the need of public key andcertificate online retrieval; the private key is supplied by the fragment identifier of the URL inspired by BeamAuth. The implementation and performance evaluation demonstrate that WebIBC is secure and efficient both in theory and practice.

[4] According to W. He, D. Akhawe, S. Jain, E. Shi, and D. Song, A number of recent research and industry proposals discussed using encrypted data in web applications. We first present a systematization of the design space of webapplications and highlight the advantages and limitations of current proposals. Next,we present ShadowCrypt, a previously unexplored design point that enables encrypted input/output without trusting any part ofthe web applications. ShadowCrypt allows users to transparentlyswitch to encryptedinput/output for text- based web applications. ShadowCrypt runsas a browser extension, replacing input elements in a page with secure, isolated shadow inputs and encrypted text with secure, isolated cleartext. ShadowCrypt's key innovation is the use of Shadow DOM, an upcoming primitive that allowslow-overhead isolation of DOM trees.
Evaluation results indicate that ShadowCrypt has low overhead and of practical use today. Finally, based on our experience with ShadowCrypt, we presenta study of 17 popular web applications, across different domains, and the functionality impact and security advantages of encrypting the data they handle.

3. According to N. Attrapadung, G. Hanaoka, S. Mitsunari, Y. Sakai, K. Shimizu, and T. Teruya,

We construct an efficient two-level homomorphic public- key encryption in prime-order bilinear groups. Such a scheme supports polynomially many homomorphic additions and one multiplication over encrypted data, similar to the cryptosystemof Boneh, Goh, and Nissim (BGN, presented at TCC 2005), which was constructed in composite-order bilinear groups. Prior to our work, the state-of-the- art for two-level homomorphic public-key encryption is the Freeman scheme (presented at Eurocrypt 2010), which is indeed the prime-order realization of the BGN scheme. Our proposed scheme significantly improves efficiency for almost all the aspects of the Freeman scheme, while retains the same ciphertext sizes. Our scheme is surprisingly simple asit is indeed (a concatenation of two copies of) the ElGamal encryption "in the exponent" resided in an asymmetric bilinear groups. We provide a software implementation ofour scheme in the x86 architecture. Besides this usual implementation, we alsoimplement our scheme in WebAssembly (wasm), which is a portable low-level bytecode format; this allows our scheme to be run (very fast) on any popular web browser, without any plugins required.

4. EXISTING SYSTEM

Researchers have thoroughly looked into the idea of putting cryptographic algorithms on web browsers in the body ofcurrent literature. It's noteworthy that one research focused on using Identity- Based Cryptography to improve client- side security in online applications. The researchers chose to use the Combined Public Key cryptosystem as the encryptiontechnique and gave a JavaScript implementation of their designed scheme. This choice was taken to avoid the complex calculations required by elliptic curve and bilinear pairing encryption.

4.1 Limitations of Existing Systems

The available research has looked into how cryptographic algorithms can be integrated on web browsers. However, there are a number issues with this strategy. First off, compared to other ways,it shows rather low security. It also has coarse-grained access control, which leadsto rigid and ineffective file sharing procedures. Last but not least, poor usability is a significant problem. Notably,users frequently upload files using a variety of terminals, including desktop, online, and mobile apps, whichcontributesto the usability issues in this situation.

5. PROPOSED SYSTEM

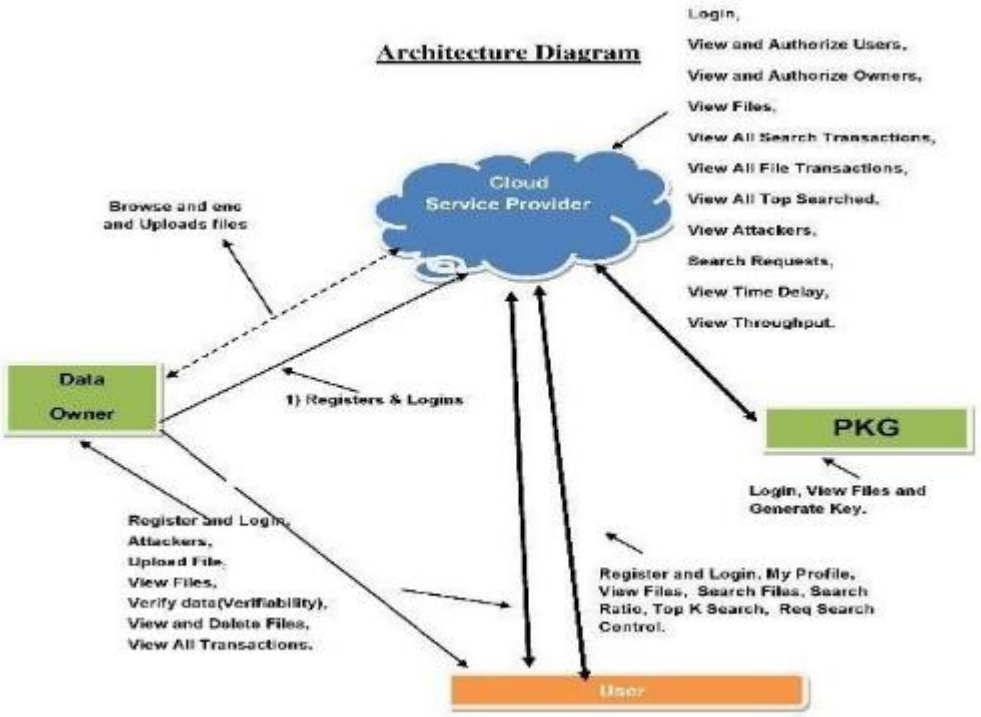
We present Web Cloud, a useful client- side encryption solution for public cloud storage that successfully fuses cutting- edge Web technologies with cryptographicmethods. It is generally

acknowledged thatattribute-based encryption (ABE) has promise for precise data access control. We provide a security model for Web Cloud that concurrently incorporates Webadversarial models and a cryptographic technique. The proposed system focuses on the development and deployment of Web Cloud, a practical and secure public cloud storage solution. With the use of web clients like web browsers, users of this cutting-edge technology may encrypt and decrypt their data using a client-side encryption strategy that is Web-based.

5.1 Advantages of Proposed System

The system guarantees data security and secrecy by using this technique. In order to increase the system's overall security and integrity, the proposed system also uses Multi-Factor Authenticated Key Exchange, which provides a further layer of protection.

6. SYSTEM ARCHITECTURE



The Attribute-Based Key EncapsulationMechanism (AB-KEM) is the target of aChosen Plaintext Attack (CPA), also known as CP-AB-KEM. The attribute- based encryption (ABE) and key encapsulation mechanism (KEM) techniques are combined in AB-KEM toencrypt data based on attributes while creating a shared secret key for decoding. In a CPA, the attacker can pick a subset

of the plaintext messages and get the matching encapsulation cipher texts to discover the secret key that was used toencrypt the communications. The secrecy of the cipher texts, which prevents an attacker from determining specific secret keys based on the ciphertexts, is a crucialcomponent of AB- KEM's security. A successful CP-AB- KEM attack would bring out a flaw in the AB-KEM scheme, allowing the attacker to distinguish between various secret key encapsulationsor identify thesecret key from certain plaintext-ciphertext combinations.

7. IMPLEMENTATION

7.1 The Data Owner

This module allows the data provider to upload encrypted data to a cloud server. The data owner encrypts the data file and then stores it on the serverfor security reasons. The owner of the data may be able to access and alter the encrypted datafile and carry out the following actions: Attackers, please sign up. See and delete files, verify data's verifiability, upload files, and see all transactions are all available.

7.2 Provider of Cloud Services

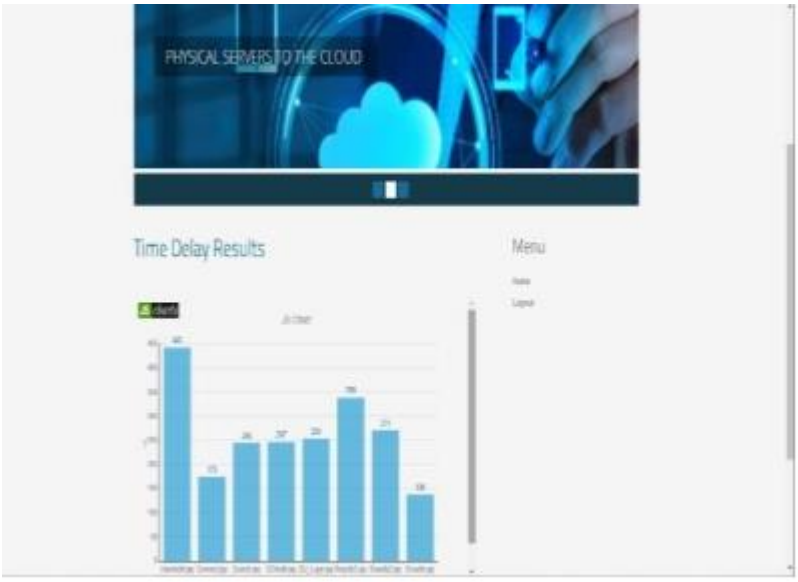
The management of the cloud server serves to offer data storage services to thedata owners. Encrypted data files are stored on the server by data ownersfor exchange with data consumers. Data consumers download encrypted data filesof interest from the server, which then decrypts them so they mayaccess the shared data files. If the end user asks file access authorization and carries out the following actions, such as logging in, viewing and authorizing users, seeing and authorizing owners, etc., the server will produce the aggregate key. Browse files, View Attackers, Top Searched, All Search Transactions, All File Transactions, All Search Requests, View Throughput and Time Delay.

7.3 End User

In this module, the user can only access the data file with the secret key. The user can search the file for a specified keyword.The data which matches for a particular keyword will be indexed in the cloud server and then response to the end user and performing the following operations Register and Login, My Profile, View Files, Search Files, Search Ratio, Top K Search, Req Search Control.

ISSN: 2057-5688

8. OUTPUT SCREENS



9. CONCLUSION

Web Cloud is a revolutionary client-side encryption system created exclusively for secured cloud storage in the online context. Users conduct all cryptographic actions in Web Cloud using only web browsers, offering a user-friendly experience. We conducted detailed performance assessments to demonstrate its utility. The outcomes illustrate the value and efficiency of our solution.

Notably, Web Cloud's architecture characteristics a specialized CP-AB-KEM scheme, presenting potential for an assortment of unique applications.

10. REFERENCES

[1] Y. Yuan, C.-M. Cheng, S. Kiyomoto, Y. Miyake, and T. Takagi, "Portable implementation of lattice-basedcryptography using javascript," International journal ofnetworking and computing,

vol. 6, no. 2, pp. 309–327, 2016.

[2] H. Halpin, "The w3c web cryptography api: motivation and overview," in Proceedings of the 23rdInternational Conference on World Wide Web. ACM, 2014, pp.959–964.

[3] Z. Guan, Z. Cao, X. Zhao, R. Chen, Z.Chen, and X. Nan, "Webibc:Identity based cryptography for client side security in web applications," in Distributed Computing Systems, 2008. ICDCS'08. The 28th International Conference on. IEEE,2008, pp. 689–696.

[4] W. He, D. Akhawe, S. Jain, E. Shi,and D. Song, "Shadowcrypt: Encrypted web applications for everyone," in Proceedings of the 2014 ACM SIGSAC Conference on Computer and

Communications Security, 2014, pp. 1028–1039.

[5] N. Attrapadung, G. Hanaoka, S.Mitsunari, Y. Sakai, K. Shimizu, and T. Teruya, "Efficient two-level homomorphic encryption in prime-order bilinear groups and a fast implementation in webassembly," in Proceedings of the 2018 on Asia Conference on Computer and Communications Security,2018, pp. 685–697.

[6] 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

[7] (2020, April) Secure file transfer — wispily. [Online]. Available: https://whisp.ly/en (2020, April) Cryptomator: Free cloudencryption for drop box And others. [Online]. Available: https://cryptomator.org/

[8] (2020, April) Whitepapers from spideroak. [Online]. Available: https://spideroak.com/whitepapers/

[9] W. Ma, J. Campbell, D. Tran, and D.Klee man, "Password entropy And password quality," in FourthInternational Conference on Network and System Security, NSS 2010,Melbourne, Victoria, Australia, September 1-3, 2010, Y. Xiang, P. Samarati, J. Hu, W. Zhou, and A. Sadeghi, Eds. IEEEComputer Society, 2010, pp. 583–587. [Online]. Available: https://doi.org/10.1109/NSS.2010.18

[10] (2020, April) Aws sdk support foramazon s3 client-side Encryption. [Online]. Available: https://docs.aws.amazon.com/General/latest/gr/aws sdkcryptography.html

[11] (2020, April) Cloud storage security -secure cloud storage from Tresorit. [Online]. Available: https://tresorit.com/security (2020, April) Mega - secure cloudstorage and communication.

[Online]. Available: https://mega.nz/

[12] E. Bocchi, I. Drago, and M. Mellia,"Personal cloud storage: Usage, Performance and impact of terminals," in 4th IEEE International Conference on Cloud Networking, Cloud Net 2015, Niagara Falls, ON, Canada, October 5-7, 2015. IEEE, 2015, pp. 106–111. [Online].

Available: https://doi.org/10.1109/CloudNet.2015.7335291

[13] "Web cryptography API," the Web Cryptography WG of the W3C, Tech. Rep., January 2017.

[Online]. Available: https://www.w3.org/TR/WebCryptoAPI/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 web assembly," in ACM SIGPLAN Notices, vol. 52, no. 6. ACM, 2017, pp. 185–200.

[14] B. Waters, "Cipher text-policy attribute-based encryption: An Expressive, efficient, and provably secure realization," in International Workshop on Public Key Cryptography. Springer, 2011, pp. 53–70.

[15] W. Zhu, J. Yu, T. Wang, P. Zhang, and W. Xie, "Efficient attribute based Encryption from r-lwe," Chin. J. Electron, vol. 23, no. 4, pp. 778–782, 2014.

[16] M. Green, S. Hohenberger, B. Waterset al., "Outsourcing the Decryption of abe cipher texts." inUSENIX Security Symposium, vol. 2011, no. 3, 2011.

[17] S. Hohenberger and B. Waters, "Online/offline attribute based Encryption," in International Workshop onPublic Key Cryptography. Springer, 2014, pp. 293– 310.

[18] R. Zhang, H. Ma, and Y. Lu, "Fine-grained access control system Based on fully outsourced attribute-basedencryption," Journal of Systems and Software, vol. 125, pp. 344–353, 2017.

[19] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data Sharing with attribute revocation," in Proceedings of the 5th ACM symposium on information, computer and communications Security, 2010, pp. 261–270.

[20] (2020, April) own cloud - the leading open source cloud Collaboration platform. [Online]. Available: https://owncloud.Org/

[21] (2020, April) Openpgp implementation for JavaScript. [Online]. Available: https://github.com/openpgpjs/openpgpjs

[22] E. Stark, M. Hamburg, and D. Boneh, "Symmetric cryptography in JavaScript," in Computer SecurityApplications Conference, 2009. ACSAC'09. Annual. IEEE, 2009, pp. 373– 381.