

Enabling Safe and Efficient Data Sharing with Web-Based Cloud Storage

¹Bonkuri Deepak, ²Mr. D.Venkateswarlu

¹Student, Dept. of Master of Computer Applications, Amrita Sai Institute of Science and Technology, Paritala, Andhra Pradesh, 521180, India.

²Asst.Prof, Dept. of Computer Science & Engineering, Amrita Sai Institute of Science and Technology, Paritala, Andhra Pradesh, 521180, India.

ABSTRACT

As more people start moving their data to the cloud, people are starting to worry more about whether their personal information will be kept safe. Client-side encryption/decryption is often seen as a good way to keep data safe from unauthorised access. However, the current methods are not very strong, mainly because they often use weak encryption, finding it hard to share data safely, and most people don't like that they have to use separate software or special hardware to make it work. This paper describes how we built Web Cloud, a simple way to protect your data on the web using your browser, without having to use any extra apps or installation. Our approach uses up-to-date web technology to help make sharing data faster, more secure, and easier for everyone. Additionally, it adds features like being able to quickly remove someone's access, processing data quickly even when offline, and letting the encryption happen on a separate server. Importantly, Web Cloud can work with any device that uses a web browser or any similar programme, including computers, tablets, and smartphones.

Keywords: *Cloud security, client-side encryption, user data privacy, encryption algorithms, browser-based encryption, data sharing, encryption usability, offline encryption, outsourced decryption, web technologies, user revocation.*

1. INTRODUCTION

Public cloud storage services are now used by lots of people because they are cheaper and make it easier for users to access and work with their data.[1], [2]This growing trend has made people and companies more comfortable putting their unencrypted data in public clouds and letting others have access to it. However, when people put important or private data in the cloud, they need to be sure that the company running the service will keep their stuff safe and not let anyone get in without permission. Unfortunately, this trust doesn't always hold up, since data leaks can happen in a number of ways, like when there are big data breaches that make the news.[3], [4], [5]

Encrypting data at the client-side is one of the best ways to stop data leakage. By encrypting their data on their machine using client-side encryption, users ensure that cloud servers only store their data in an encrypted form.[5], [6], [7], [8] People can open the files they have downloaded and read them using the decryption key. As a result, unauthorised access to the data from the cloud provider is greatly reduced, as the information received by them is already encrypted.[3], [9]

While client-side encryption is very useful, many cloud storage providers do not provide support for it, like Google Drive and Dropbox.[5], [10] As a rule, these organisations use encryption on their servers for files at rest, secure the data sending process with TLS, and also rely on two-factor authentication for logging in.[5], [11]

For certain situations, the data of users is first protected by symmetric encryption (AES) before being saved in the cloud. But, quite often, these approaches use a password to generate the cryptographic keys needed for security, which is a risky practise. The majority of password-based tools are only meant for solo file encryption and decryption, not for allowing users to share files.[12], [13]

A more robust solution is hybrid encryption, which uses both a key wrapper (KEM) and a data wrapper (DEM) to help make the system more secure.[3], [14] This method is usually called the KEM-DEM approach. Many public cloud service providers, like Amazon, Tresorit, and Mega, use the RSA-AES method to make sure data is kept safe and encrypted.[15], [16] In this system, users make RSA key pairs and then ask the service providers for certificates, which are used to make sure messages stay safe and private.

The service providers store and look after a system called Public Key Infrastructure (PKI) so communication and encryption can work smoothly.[17]

2. LITERATURE SURVEY

Looking at ways to securely share data through different platforms, especially online cloud storage, has been a focus of interest for many researchers. Among the notable things invented are as follows:

Hohenberger, S., & Waters, B. (2014): The authors presented the idea of online/offline encryption schemes at the International Workshop on Public Key Cryptography, with a focus on improving both the speed and security of ABE methods used for storing data in cloud solutions.[19] Thanks to their method, it was possible for encryption to happen without connexion to the Internet, making distributed systems operate more effectively (Springer, 2014, pp. 293–310).[19], [20], [21]

Waters, B. (2011): Waters came up with a new and more secure way of implementing CP-ABE in his seminal paper titled “Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realisation.”[20], [21] By discussing his findings at the workshop, Sahai allowed ABE systems to be used in practise and were certified as safe for data on the cloud (Springer, 2011, pages 53 to 70).[22], [23]

Green, M., Hohenberger, S., Waters, B., et al. (2011): Researchers presented a research paper, titled “Outsourcing the Decryption of ABE Ciphertexts” at USENIX Security Symposium, which focuses on ways to decrypt ABE systems using outsourcing.[21] The paper was important for revealing how making decryption a task for external parties could make ABE possible in the large-scale cloud computing framework (USENIX, 2011).[21], [24]

3. SYSTEM STUDY

FEASIBILITY STUDY

At this point, engineers study the chosen project to find out if it can be carried out successfully. At this stage, the business draughts a proposal showing a first glimpse of the project, and its estimated costs. At the system analysis stage, a feasibility study cheques the possibilities and long-term use of the suggested system. [19] It is important that the system does not cause too many burdens on the organisation. It is necessary to fully understand the main requirements of the system in order to do feasibility analysis.[21], [23]

Usually, feasibility analysis is done by examining three key aspects.

- **ECONOMICAL FEASIBILITY**
- **TECHNICAL FEASIBILITY**
- **SOCIAL FEASIBILITY**

1. ECONOMICAL FEASIBILITY:

This step in the study assesses the technical needs involved in developing and putting the system into practise. Make sure that the system under development does not ask too much of the available tools and resources.[19] High technology requirements might make things more difficult for the clients and are therefore not advisable. The technical needs for the developed system should be marginal, so there are few or no modifications needed to use it efficiently.[19]

2. TECHNICAL FEASIBILITY:

This step in the study assesses the technical needs involved in developing and putting the system into practise.[19], [27] Make sure that the system under development does not ask too much of the available tools and resources. High technology requirements might make things more difficult for the clients and are therefore not advisable.[19], [28] The technical needs for the developed system should be marginal, so there are few or no modifications needed to use it efficiently.[19], [29]

3. SOCIAL FEASIBILITY:

The social study tries to determine if there is a chance the system will be well received by the people using it[20], [30]. Users must be taught how to properly work the system. The system should not scare users but rather be used and appreciated.[20] Promoting system usage depends a lot, on how users are familiarised with and educated about the system. When we build up

user trust and guide them to provide useful feedback, the system can better match what users need and expect, helping the system integrate and be used easily.[20], [30], [31]

4. SYSTEM ANALYSIS

4.1 Existing System

The data is organised in a CSV table, which includes information such as post text, its sentiment, and details like the topic or party involved.[28], [29], [31] It holds a lot of information that has been labelled, which forms the basis for teaching and checking the performance of sentiment classification. The annotations were created by many volunteers, leading to a wide range of opinions, but there may be some variances because people can interpret sentiment differently.

Another popular programme is Shadow Crypt, which makes it easy for users to switch to secure input and output for Web applications that handle text.[8], [10] The solution is based on a browser extension that changes regular inputs to secure, isolated shadow forms, and takes the extra step of encrypting text in isolated cleartext. Further, some of the Lattice-based encryption schemes have been implemented, and the results evidence their efficiency in popular Web browsers.[27]

Improvements have been brought by using prime-order bilinear groups and a high-performance method of homomorphic encryption.[21], [28] Web Assembly allows the solution to load quickly in any common Web browser, without requiring more plugins.[10], [15], [17]

ABE has seen major achievements and progress. At the beginning, ABE was simply fuzzy identity-based encryption until it was developed further as ABE. With ABE, a user is permitted to decrypt data only if their set of attributes matches what is specified in the policy. In Web Cloud systems, CP-ABE is commonly used so that every file is protected by an access policy stating who should be able to access (decode) that file.[20], [22]

Still, the act of pairing and exponentiation needed in ABE systems has brought about major performance problems.[17], It has been suggested that performing most of the encryption offline, without the actual attributes, can reduce the amount of work needed on each request. It has also been proposed that encryption calculations can be done offline by secure servers or smartphones owned by users, so that people with less powerful devices are able to take part.[1], [3], [11]

4.1.1 Disadvantages

Regardless of the progress, these systems face a number of issues.

1. **Relatively Weak Security:** Certain techniques used today may not provide adequate security for extremely sensitive data.[8]
2. **Coarse-Grained Access Control:** Many current systems do not allow enough flexibility in managing who gets access, which means it can be tough to design more precise policies.[31]
3. **Poor Usability:** Some problems arise when people try to access and manage their files from various devices. This creates challenges and fails to provide users with the best service.[30]

4.2 Proposed System

Web Cloud aims to solve the problems with current systems by supplying a strong and easy-to-use client-side encryption for storing files in public cloud storage. [2] It combines advanced Web tech with strong security algorithms to give users safe and convenient cloud storage, without the use of extra plugins. Some of the main aspects of **Web Cloud** are:

1. **Using Encryption for Your Files in Cloud Storage:** Client-side encryption and decryption using web agents ensure that storing information on the cloud is both efficient and safe. The solution works on most browsers, as well as on Android and PC computers.[10], [30], [19]
2. **Access Control with Attribute-Based Encryption (ABE):** Businesses can use ABE integration in the system to ensure that specific people can access different files. For CP-ABE, a policy is used within the encryption to prevent non-approved

individuals from decrypting a file. Besides, we find solutions for some of the major flaws of previous ABE approaches, such as making them costly to execute, hard to encrypt, and slow at revoking users.[31][19]

3. **Rigorous Security Analysis:** A good security model has been made, including simulation of risk from attacks on Web environments and cryptography. It ensures that both the security and key safety are reliable for the suggested CP-ABE scheme when running on the browser side.[20], [30], [31]
4. **Efficient Operations within Browsers:** The Web Cloud is setup using ownCloud and then tested for function and performance on screens including large computers and mobile devices (including Android.) It is clear from the data that Web Cloud saves time in both its encryption and decryption processes.[1], [3], [31] On the same MacBook, the process of encrypting a 1 GB file takes 3.1 seconds, while decrypting is completed in just under four seconds.[12], [14]

4.2.1 Advantages

The proposed Web Cloud system has a few benefits, including:

- **Practical and Secure Solution:** By using Web-based client-side encryption, the system makes sure users can safely encrypt and decrypt their data without the need for outside plugins or other companies.[21], [35], [20]
- **Cross-Platform Compatibility:** The solution works well in most browsers, on Android phones, and on computers, so it's easy for many different people to get into and use the system.[27], [10]
- **Enhanced Security with Multi-Factor Authentication:** We have set up a system that uses more than one way of checking identities so that we can keep your information safer and make it harder for someone to get in who shouldn't. [20], [30], [31]

5. SYSTEM DESIGN

5.1 Class Daigram

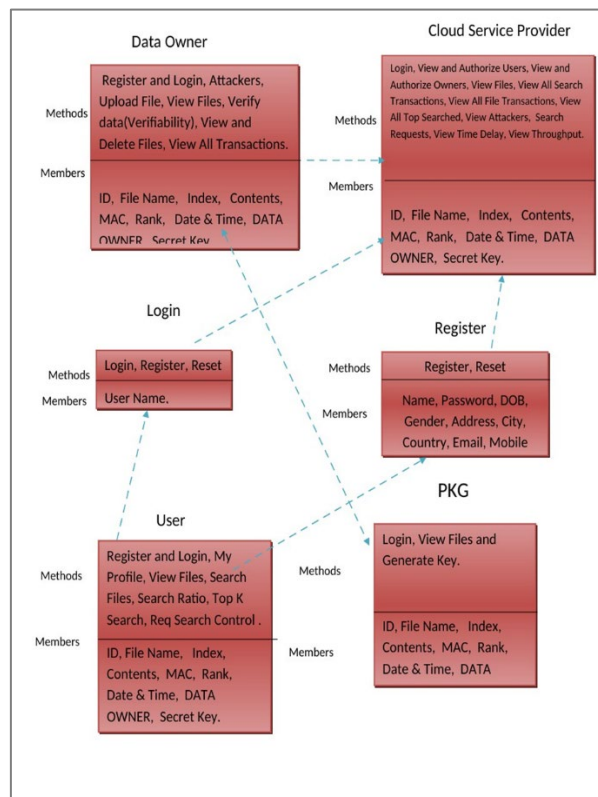


Fig 1: Class-Diagram

5.2 Data Flow Diagram

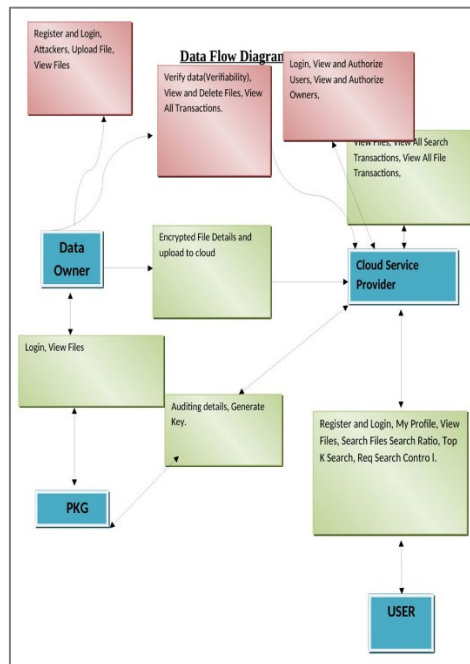


Fig 2: Data:Flow-Diagram

5.3 Flow Chart:Cloud Server

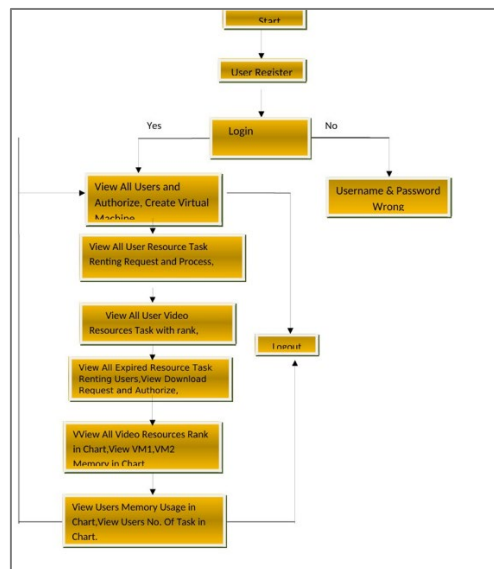


Fig 3: Flow Chart:cloud-Diagram

5.4 System Requirements

Component	Specification
Processor	Pentium – IV
RAM	4 GB (min)
Hard Disk	20 GB
Keyboard	Standard Windows Keyboard
Mouse	Two or Three Button Mouse
Monitor	SVGA

Table1: HardWare Req

Component	Specification
Operating System	Windows XP
Coding Language	Java/J2EE (JSP, Servlet)
Front End	J2EE
Back End	MySQL

Table2: SoftWare Req

6. CONCLUSION

We propose Web Cloud, which makes it easy for users to encrypt things on their own computer or phone, without having to install anything extra, for storing files using public cloud storage online. We look into the security of Web Cloud and put the system together using our own Cloud, then we cheque how well it works. The experimental results show that our solution really works well in real life. As an interesting by-product, the design of Web- Cloud naturally includes a special type of security system called a CP-AB-KEM, which is handy for other uses as well.

ACKNOWLEDGMENT

I am thankful to the Management of Amrita Sai Institute of Science and Technology for giving me an opportunity to work with his project.

I would like to the thank **Dr. M. Sasidhar**, Principal, Amrita Sai institute of science and technology, for his constant encouragement and support during the progress of this work.

I am deeply grateful to **Dr. P. Chiranjeevi**, Professor and Head of the Department, for his valuable guidance and consistent support during the course of the project.

A special note of thanks to my internal guide **Mr. D.Venkateswarlu**, for his exceptional guidance, constant motivation, and continuous encouragement, which played a crucial role in the successful completion of this project.

BONKURI DEEPAK

REFERENCES

- [1] W. You, L. Lei, B. Chen, and L. Liu, "What If Keys Are Leaked? towards Practical and Secure Re-Encryption in Deduplication-Based Cloud Storage," Information, vol. 12, no. 4, p. 142, Mar. 2021, doi: [10.3390/info12040142](https://doi.org/10.3390/info12040142).
- [2] B. K. Samanthula, G. Howser, Y. Elmehdwi, and S. Madria, "An efficient and secure data sharing framework using homomorphic encryption in the cloud," Aug. 2012, doi: [10.1145/2347673.2347681](https://doi.org/10.1145/2347673.2347681).
- [3] S. Kanatt, P. Talwar, and A. Jadhav, "Review of Secure File Storage on Cloud using Hybrid Cryptography," International Journal of Engineering Research and, no. 2, Feb. 2020, doi: [10.17577/ijertv9is020014](https://doi.org/10.17577/ijertv9is020014).
- [4] Y. Sun, J. Zhang, Y. Xiong, and G. Zhu, "Data Security and Privacy in Cloud Computing," International Journal of Distributed Sensor Networks, vol. 10, no. 7, p. 190903, Jul. 2014, doi: [10.1155/2014/190903](https://doi.org/10.1155/2014/190903).
- [5] L. Hu, Y. Huang, D. Yang, Y. Zhang, and H. Liu, "SSeCloud: Using secret sharing scheme to secure keys," in IOP

- Conference Series Earth and Environmental Science, IOP Publishing, Aug. 2017, p. 12207. doi: [10.1088/1755-1315/81/1/012207](https://doi.org/10.1088/1755-1315/81/1/012207).
- [6] “Why should you use client-side encryption for cloud storage?” Nov. 2023. Accessed: May 16, 2025. [Online]. Available: <https://www.linkedin.com/advice/0/why-should-you-use-client-side-encryption-cloud-zqabf>
- [7] “Client-side Encryption and Why Does It Matter?” Apr. 2024. Accessed: May 16, 2025. [Online]. Available: <https://www.virtu.com/blog/file-encryption/client-side>
- [8] D. Commey, S. Griffith, and J. Dzisi, “Performance comparison of 3DES, AES, Blowfish and RSA for Dataset Classification and Encryption in Cloud Data Storage,” *International Journal of Computer Applications*, vol. 177, no. 40, p. 17, Feb. 2020, doi: [10.5120/ijca2020919897](https://doi.org/10.5120/ijca2020919897).
- [9] E. Alomari and M. M. Monowar, “Towards Data Confidentiality and Portability in Cloud Storage,” in *Lecture notes in computer science*, Springer Science+Business Media, 2014, p. 38. doi: [10.1007/978-3-319-07626-3_4](https://doi.org/10.1007/978-3-319-07626-3_4).
- [10] K. Hui, “Data Encryption in the Cloud, Part 4: Comparing AWS, Azure, and Google Cloud.” Mar. 2018. Accessed: May 16, 2025. [Online]. Available: <https://medium.com/@kenhuiny/data-encryption-in-the-cloud-part-4-comparing-aws-azure-and-google-cloud-1cda50ef1606>
- [11] S. Scheffler and J. Mayer, “SoK: Content Moderation for End-to-End Encryption,” *Proceedings on Privacy Enhancing Technologies*, vol. 2023, no. 2, p. 403, Mar. 2023, doi: [10.56553/popets-2023-0060](https://doi.org/10.56553/popets-2023-0060).
- [12] H. Sadler, “Encryption-At-Rest for Web Apps with Offline Capabilities.” Sep. 2019. Accessed: May 16, 2025. [Online]. Available: https://www.linkedin.com/pulse/encryption-at-rest-web-apps-offline-capabilities-hamish-sadler?trk=pulse-article_more-articles_related-content-card
- [13] B. S. Rawal, “Proxy re-encryption architect for storing and sharing of cloud contents,” *International Journal of Parallel Emergent and Distributed Systems*, vol. 35, no. 3, p. 219, Mar. 2018, doi: [10.1080/17445760.2018.1439491](https://doi.org/10.1080/17445760.2018.1439491).
- [14] F. Weissbaum and T. Lugin, “Symmetric Cryptography,” 2023, p. 7. doi: [10.1007/978-3-031-33386-6_2](https://doi.org/10.1007/978-3-031-33386-6_2).
- [15] A. W. Dent, “A Designer’s Guide to KEMs,” *IACR Cryptology ePrint Archive*, vol. 2002, p. 174, Jan. 2002, Accessed: Jan. 2025. [Online]. Available: <https://eprint.iacr.org/2002/174.pdf>
- [16] J. Herranz, D. Hofheinz, and E. Kiltz, “Some (in)sufficient conditions for secure hybrid encryption,” *Information and Computation*, vol. 208, no. 11, p. 1243, Aug. 2010, doi: [10.1016/j.ic.2010.07.002](https://doi.org/10.1016/j.ic.2010.07.002).
- [17] S. Kumar, S. A. Rabara, and J. Martin, “MPCS,” vol. 3, p. 571, Nov. 2009, doi: [10.1145/1655925.1656029](https://doi.org/10.1145/1655925.1656029).
- [18] C. King, “Internet Electronic Mail Security,” *Information Systems Security*, vol. 7, no. 2, p. 1, Jun. 1998, doi: [10.1201/1086/43303.7.2.19980601/31043.9](https://doi.org/10.1201/1086/43303.7.2.19980601/31043.9).
- [19] S. Hohenberger and B. Waters, “Attribute-Based Encryption with Fast Decryption,” in *Lecture notes in computer science*, Springer Science+Business Media, 2013, p. 162. doi: [10.1007/978-3-642-36362-7_11](https://doi.org/10.1007/978-3-642-36362-7_11).
- [20] S. Hohenberger and B. Waters, “Online/Offline Attribute-Based Encryption,” in *Lecture notes in computer science*, Springer Science+Business Media, 2014, p. 293. doi: [10.1007/978-3-642-54631-0_17](https://doi.org/10.1007/978-3-642-54631-0_17).
- [21] M. Green, S. Hohenberger, and B. Waters, “Outsourcing the decryption of ABE ciphertexts,” p. 34, Aug. 2011.
- [22] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-Policy Attribute-Based Encryption,” in *2022 IEEE Symposium on Security and Privacy (SP)*, May 2007, p. 321. doi: [10.1109/sp.2007.11](https://doi.org/10.1109/sp.2007.11).
- [23] B. Waters, “Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization,” in *Lecture notes in computer science*, Springer Science+Business Media, 2011, p. 53. doi: [10.1007/978-3-642-19379-8_4](https://doi.org/10.1007/978-3-642-19379-8_4).
- [24] M. Green, “Secure Blind Decryption,” in *Lecture notes in computer science*, Springer Science+Business Media, 2011, p. 265. doi: [10.1007/978-3-642-19379-8_16](https://doi.org/10.1007/978-3-642-19379-8_16).
- [25] L. Shen, V. W. Y. Tam, L. Tam, and Y. Ji, “Project feasibility study: the key to successful implementation of sustainable and socially responsible construction management practice,” *Journal of Cleaner Production*, vol. 18, no. 3, p. 254, Oct. 2009, doi: [10.1016/j.jclepro.2009.10.014](https://doi.org/10.1016/j.jclepro.2009.10.014).
- [26] J. K. Ssegawa and M. Muzinda, “Feasibility Assessment Framework (FAF): A Systematic and Objective Approach for Assessing the Viability of a Project,” *Procedia Computer Science*, vol. 181, p. 377, Jan. 2021, doi: [10.1016/j.procs.2021.01.180](https://doi.org/10.1016/j.procs.2021.01.180).
- [27] A. M. O. Khairalla, X. W. Lu, and J. L. C. Ladu, “Evaluation of the Multistage Biological-Ecological Process for Removal of Organic Matter and Nutrient from the Rural Domestic Wastewater under Ambient Temperature,” *Advanced materials research*, p. 2133, Jun. 2014, doi: [10.4028/www.scientific.net/amr.955-959.2133](https://doi.org/10.4028/www.scientific.net/amr.955-959.2133).
- [28] F. Hoops and F. Matthes, “A Universal System for OpenID Connect Sign-ins with Verifiable Credentials and Cross-Device Flow,” in *2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, May 2024, p. 296. doi: [10.1109/icbc59979.2024.10634364](https://doi.org/10.1109/icbc59979.2024.10634364).
- [29] S. Strodl, F. Motlik, K. Stadler, and A. Rauber, “Personal & soho archiving,” vol. 14721, p. 115, Jun. 2008, doi: [10.1145/1378889.1378910](https://doi.org/10.1145/1378889.1378910).
- [30] B. Greenstein and B. Longstaff, “FollowMe,” p. 105, Mar. 2011, doi: [10.1145/2184489.2184511](https://doi.org/10.1145/2184489.2184511).

[31] D. Greenwood and I. Sommerville, “Expectations and Reality: Why an enterprise software system didn’t work as planned,” arXiv (Cornell University), Jan. 2011, doi: [10.48550/arxiv.1104.1370](https://doi.org/10.48550/arxiv.1104.1370).