iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** IV **Month of publication:** April 2020

DOI: http://doi.org/10.22214/ijraset.2020.4087

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: 7.429
Volume 8 Issue IV Apr 2020- Available at www.ijraset.com

Convergent Dispersal: Toward Storage-Efficient Security in a Cloud-of-Clouds

C. Vijayalakshmi[1], Masimukku Sai Swetha[2], Meenakshi. K N[3], Tanari Priyanka[4]
[1]*Associate Professor,* [2, 3, 4]*UG Students, Panimalar Engineering College*

Abstract: ***In the existing system, if the owner wants to share the data from one user to another user there are chances for some security issues to be present. The data which is being transferred from user to user can be hacked. To overcome the security issues, we propose a system where the data transformation is done with high security. If the uploaded data is stored directly then there are chances for data leak. We provide a solution where the uploaded data is getting split into four parts and each key will be generated for the four parts while storing it in the database and it will be encrypted. If the user wants the file access which is uploaded by the owner then the user can send the request. After sending the request, it will be forwarded to the admin. After receiving the request from user, the admin will accept the request. After user login, the user will receive the four keys for the single file. Type the key in the key box mentioned there by hearing the key through audio and then the user can read the file that is being encrypted.***

I. INTRODUCTION

Network security is protection of the access to files and directories in a computer network against hacking, misuse and unauthorized changes to the system. An example of network security is an anti virus system. A good network security system helps business reduce the risk of falling victim of data theft and sabotage. Network security helps protect your workstations from harmful spyware. It also ensures that shared data is kept secure. The purpose of security is to keep you, your family, and your properties safe from burglaries, theft and other crimes. On the other hand, the prominent visibility of security guards in gated communities deters criminals and thieves.

Network security consists of the policies and practices adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security starts with authentication, commonly with a username and a password.

Since this requires just one detail authenticating the user name i.e., the password this is sometimes termed one-factor authentication. With two-factor authentication, something the user 'has' is also used (e.g., a security token or an ATM card, or a mobile phone); and with three-factor authentication, something the user is also used (e.g., a fingerprint or retinal scan).

II. PROBLEM DEFINITION

This is a single-server scheme for secure cross-user deduplication with client-side encrypted data. The scheme allows a client uploading an existing file to securely obtain the encryption key that was used by the client who has previously uploaded that file. Clients who care about privacy prefer to have their data encrypted on the client-side using secure encryption schemes. Data deduplication enables data storage systems to find and remove duplication within data without compromising its availability. The goal of data deduplication is to store more data in less space by storing and maintaining files (blocks in fine-grained deduplication manner) into a single copy, where the redundant copies of data are replaced by a reference to this copy. It means that data deduplication storage system could reduce the storage size of u clients, who share the same data copy m, from O ($u \cdot |m|$) to O ($u + |m|$) if some implementation-dependent constants are hidden.

Also, clients do not need to upload their data to the cloud storage server when there has been one copy stored, which will not only greatly reduce the communication cost of clients and cloud server, but also save the network bandwidth. Since the data from different clients is encrypted with different secret keys, it is difficult to conduct cipher text data deduplication among clients. Storage has become an indispensable part for various applications in nowadays network, which store a large amount of data and provide the partial data needed.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue IV Apr 2020- Available at www.ijraset.com

A. Related Work

In 2017 Hui Cui, Robert H. Deng ,Yingjiu Li[2] proposed the Attribute-based encryption (ABE) that has been widely used in cloud computing where a data provider outsources his/her encrypted data to a cloud service provider, and can share the data with users possessing specific credentials (or attributes).

The authors Zahra Pooranian, Kang-Cheng Chen in 2018[3] introduced Client-side data deduplication enables cloud storage services (e.g., Dropbox) to achieve both storage and bandwidth savings, resulting in reduced operating cost and high level of user satisfaction. However, the deduplication checks (i.e., the corresponding essential message exchange) create a side channel, exposing the privacy of file existence status to the attacker.

Recently, Halevi et al. (CCS'11) proposed a cryptographic primitive called proofs of ownership (PoW) to enhance security of client-side deduplication in cloud storage. In a proof of ownership scheme, any owner of the same file F can prove to the cloud storage that he/she owns file F in a robust an efficient way, in the bounded leakage setting where a certain amount of efficiently-extractable information about file F is leaked. To achieve high storage saving the authors Hyungjune Shin , Dongyoung Koo , Youngjoo Shin in 2018[1], introduced data deduplication techniques are in cloud storage services, which remove redundant data and keeps only a single copy of them.

III. SYSTEM ANALYSIS

A. Existing System

In existing framework, one of a couple of basic advancements to distributed storage administration, deduplication permits cloud servers to spare extra room by erasing excess record duplicates. The drawbacks of this existing system are it allows duplicates data and occupies the storage an also has security vulnerabilities.

B. Proposed System

In proposed framework, to upset this sort of assault we plan a safe edge deduplication conventions. In particular, we have concocted a novel cryptographic crude called "dispersed convergent encryption" (DCE) plot.The advantages of this proposed system are it cannot upload repeated file and reduces the storage space.

C. Requirement Analysis And Specification

These are the requirements for doing the project. Without using these tools and software's we can't do the project. So we have two requirements to do the project. They are Hardware Requirements and Software Requirements.

1) *Hardware Requirements:* The hardware requirements may serve as the basis for a contract for the implementation of the system and should therefore be a complete and consistent specification of the whole system. They are used by software engineers as the starting point for the system design. It shows what the system does and not how it should be implemented.

a) Processor: PENTIUM IV 2.6GHz, IntelCore2 Duo.
b) Ram : 4GB DD RAM
c) Monitor : 15" COLOR
d) Hard Disk : 40 GB

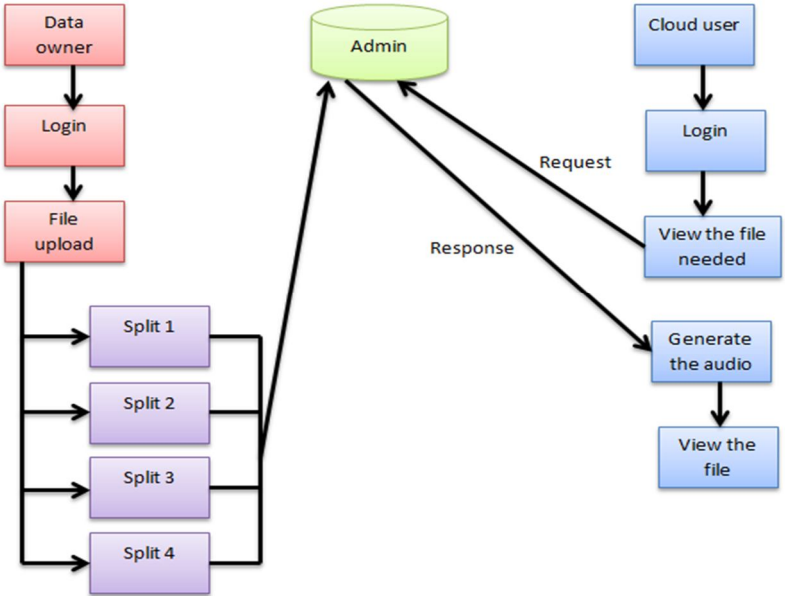
2) *Software Requirements:* The software requirements document is the specification of the system. It should include both a definition and a specification of requirements. It is a set of what the system should do rather than how it should do it. The software requirements provide a basis for creating the software requirements specification. It is useful in estimating cost, planning team activities, performing tasks and tracking the teams and tracking the team's progress throughout the development activity.

a) FRONT END J2EE (JSP,SERVLETS)JAVASCRIPT
b) BACK END : MY SQL 5.5
c) OPERATING SYSTEM: Windows 07
d) IDE : Eclipse

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue IV Apr 2020- Available at www.ijraset.com

IV. SYSTEM ARCHITECTURE

A. *Architecture Overview*



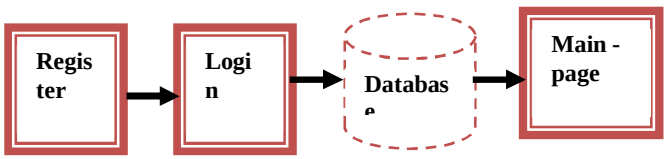
System architecture is the conceptual model that defines the structure, behavior, and more views of a system. An architecture description is a formal description and representation of a system, organized in a way that supports reasoning about the structures and behaviors of the system. A system architecture can consist of system components and the sub-systems developed, that will work together to implement the overall system. There have been efforts to formalize languages to describe system architecture; collectively these are called architecture description languages.

B. *Module Design*

Specification

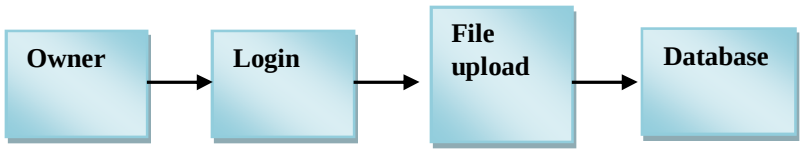
a) User interface design
b) File upload and getting split into four parts
c) Request a file that user needs
d) Response to the user with key
e) Type the key by hearing the audio
f) Download the file

1) *User Interface Design:* This is the first module of our project. The important role for the user is to move login window to user window. This module has created for the security purpose. In this login page we have to enter login user id and password. It will check username and password is match or not (valid user id and valid password). If we enter any invalid username or password we can't enter into login window to user window it will shows error message. So we are preventing from unauthorized user entering into the login window to user window. It will provide a good security for our project. So server contain user id and password server also check the authentication of the user. It well improves the security and preventing from unauthorized user enters into the network. In our project we are using JSP for creating design. Here we validate the login user and server authentication.

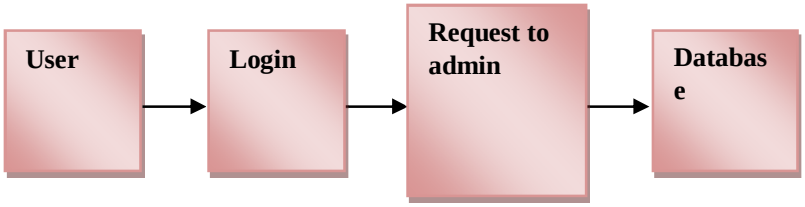


ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue IV Apr 2020- Available at www.ijraset.com

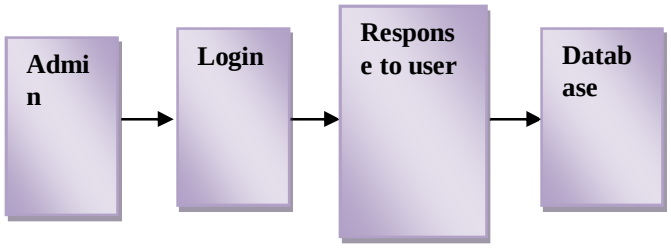
2) *File Upload And Getting Split Into Four Arts:* In this module, after login the owner will upload the file and getting split into four parts and then the file will be getting encrypted while storing in the database.



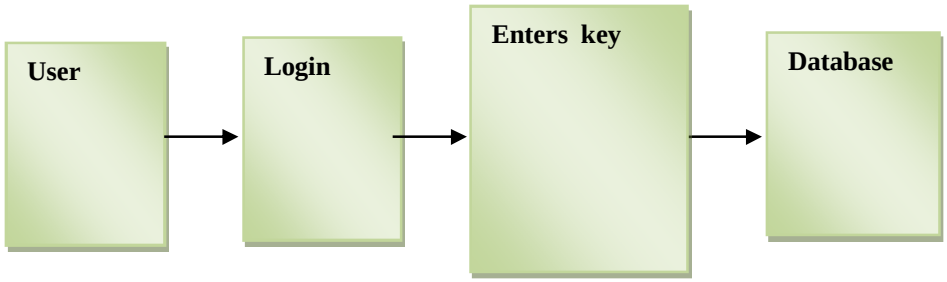
3) *Request A File That User Needs:* In this module, the user will be viewing the file which is being uploaded by the owner. If the user wants the particular file means, the user can send the request to admin for getting the file which the user needs.



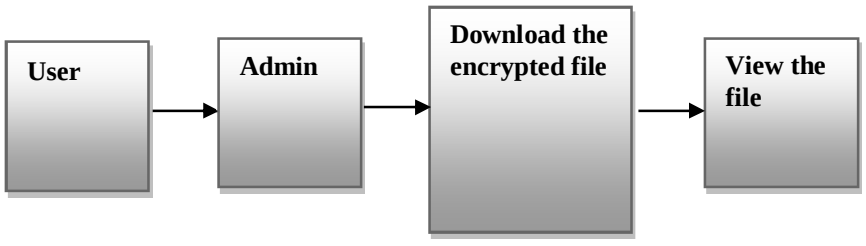
4) *Response To The User With Key:* In this module, after requesting the file to the admin, the admin will be checking that the user will be a correct user. If there is a valid user admin will send a key, else admin cannot send a key to the admin.



5) *Type The Key By Hearing The Audio***:** For valid users, user will get a key with their inbox as a audio file. User has to enter the key by hearing audio file. For security purpose admin will send a key as audio file.



6) *Download The File:* In this module, after entering the key, user will download the file. If the key matches with the file it downloads, otherwise it cannot be downloaded.



C. System Techniques

1) Technique: AES Data Integration is the combination of technical and business processes used to combine data from disparate sources into meaningful and valuable information. The process of Data Integration is about taking data from many disparate sources (such as files, various databases, mainframes etc.,) and combining that data to provide a unified view of the data for business intelligence. Data integration is needed when a business decides to implement a new application and migrate its data from the legacy systems into the new application. It becomes even critically important in cases of company mergers where two companies merge and they need to consolidate their applications. One of the most commonly known uses of data integration is building a data warehouse for an enterprise which enables a business to have a unified view of their data for analysis and business intelligence (BI) needs.

V. TESTING

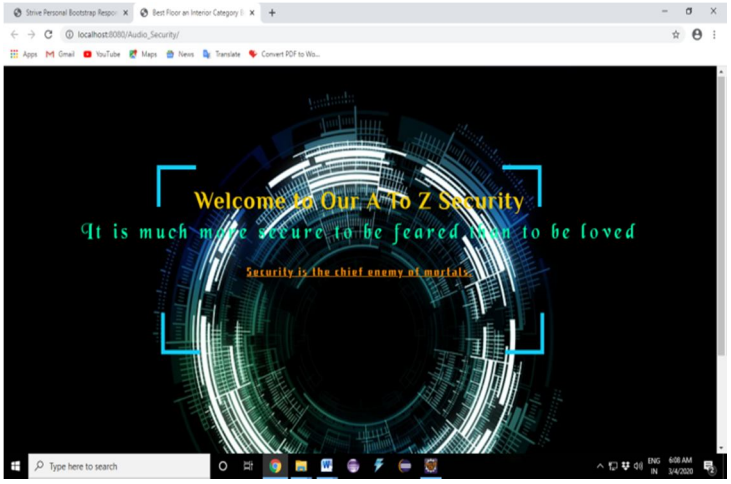
A. Software Testing

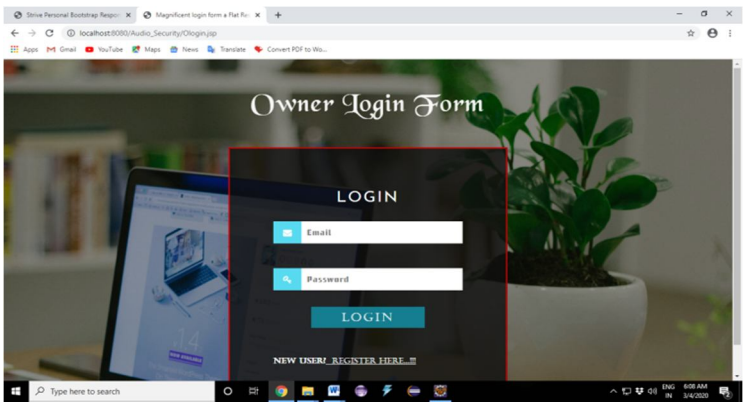
The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, sub assemblies, assemblies and/or a finished product It is the process of exercising software with the intent of ensuring that the Software system meets its requirements and user expectations and does not fail in an unacceptable manner. There are various types of test. Each test type addresses a specific testing requirement.

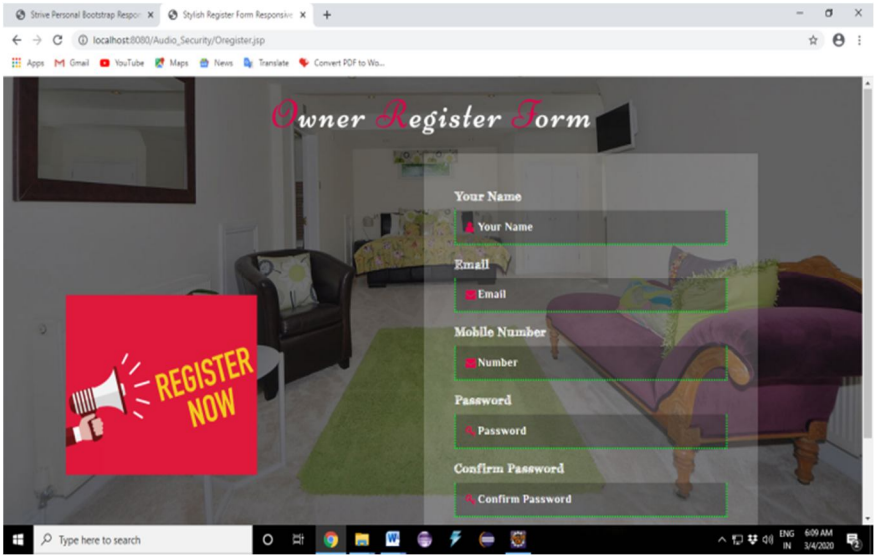
B. Developing Methodologies

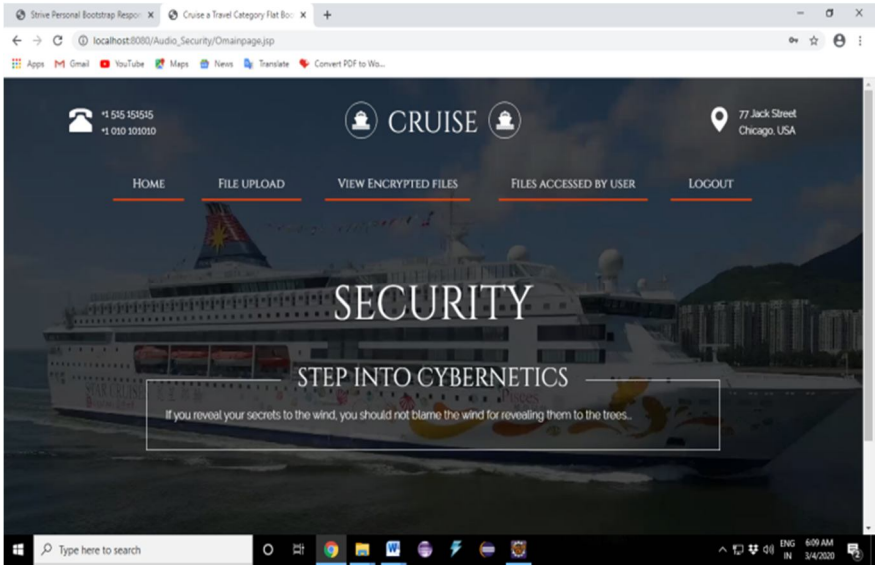
The test process is initiated by developing a comprehensive plan to test the general functionality and special features on a variety of platform combinations. Strict quality control procedures are used. The process verifies that the application meets the requirements specified in the system requirements document and is bug free. The following are the considerations used to develop the framework from developing the testing methodologies.

VI. SCREENSHOTS









VII. CONCLUSION

In this paper, we study the problem of thwarting template side-channel attack in client-side secure duplication systems on the cloud with a covert server adversary who may trigger the deduplication before the predefined threshold is reached. By introducing the k-anonymity privacy concept into our design, we have devised a novel cryptographic primitive called dispersal convergent encryption scheme which can be used to construct efficient secure deduplication protocol satisfying our requirements.

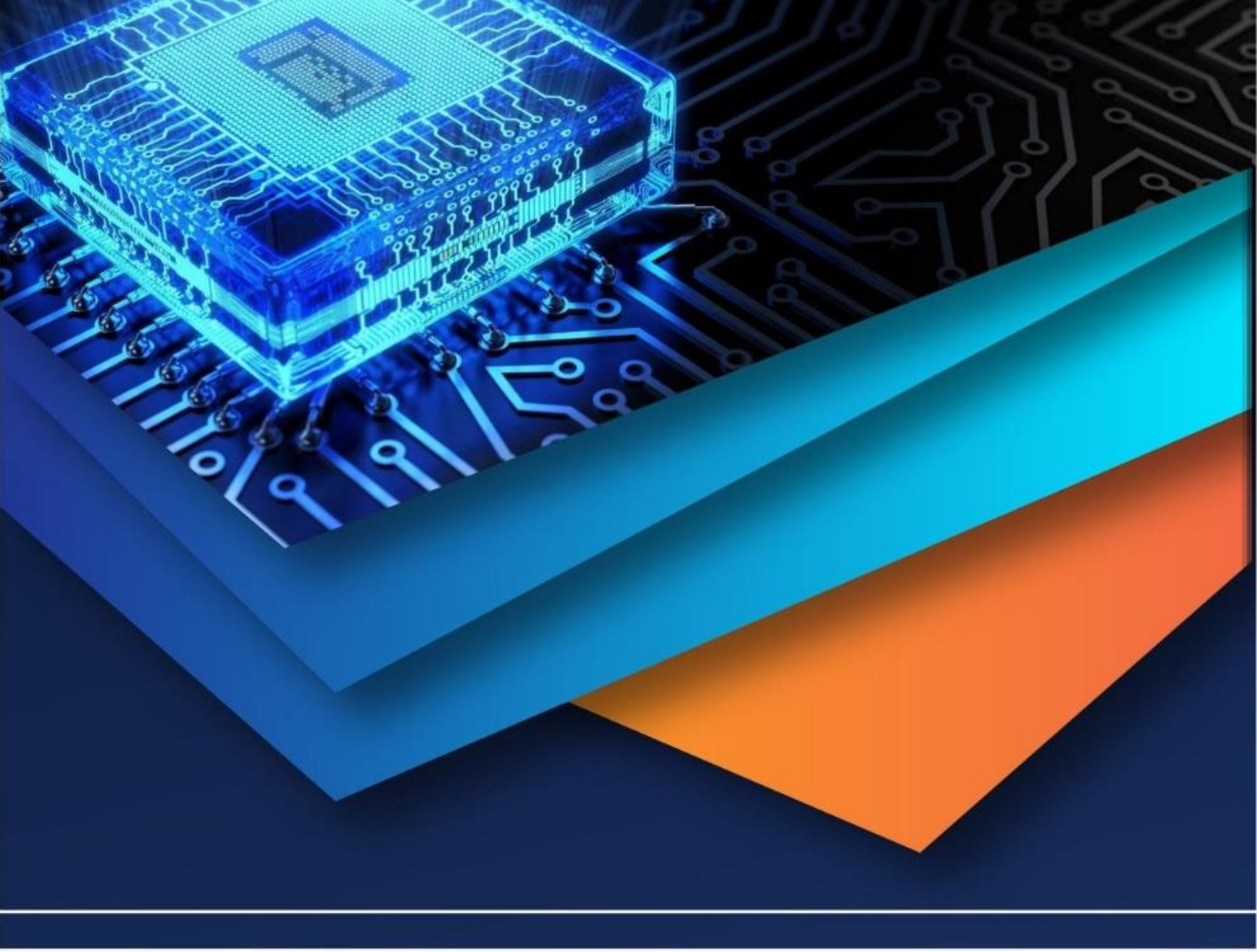
We also provide two practical constructions of DCE schemes, and theoretically prove their excellent security guarantees against three kinds of important adversaries. Experiment results show our secure deduplication protocols achieve very good performance.

VIII. FUTURE ENHANCEMENT

An accumulation is often needed to gather the partial results from these parallel executions in different servers. The runtime system captures new events and run corresponding actions to analyze the page and store more URLs into the URL set to generate new events. We propose a simple yet efficient model, called dual sentiment analysis (DSA), to address the polarity shift problem in sentiment classification. By using the property that sentiment classification has two opposite class labels (i.e., positive and negative), we first propose a data expansion technique by creating sentiment reversed reviews. The original and reversed reviews are constructed in a one-to-one correspondence.

REFERENCES

[1] M. Bellare, S. Keelveedhi, and T. Ristenpart. Messagelocked encryption and secure deduplication. In Annual International Conference on the Theory and Applications of Cryptographic Techniques, pages 296–312. Springer, 2013.
[2] J. Blasco, R. Di Pietro, A. Orfila, and A. Sorniotti. A tunable proof of ownership scheme for deduplication using bloom filters. In Communications and Network Security (CNS), 2014 IEEE Conference on, pages 481– 489. IEEE, 2014.
[3] H. Cui, R. H. Deng, Y. Li, and G. Wu. Attribute-based storage supporting secure deduplication of encrypted data in cloud. IEEE Transactions on Big Data, 2017.
[4] R. Di Pietro and A. Sorniotti. Boosting efficiency and security in proof of ownership for deduplication. In Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security, pages 81–82. ACM, 2012.
[5] J. R. Douceur, A. Adya, W. J. Bolosky, P. Simon, and M. Theimer. Reclaiming space from duplicate files in a serverless distributed file system. In Distributed Computing Systems, 2002. Proceedings. 22nd International Conference on, pages 617–624. IEEE, 2002.
[6] J. R. Douceur, W. J. Bolosky, and M. M. Theimer. Encryption systems and methods for identifying and coalescing identical objects encrypted with different keys, Jan. 3 2006. US Patent 6,983,365.
[7] S. Halevi, D. Harnik, B. Pinkas, and A. Shulman-Peleg. Proofs of ownership in remote storage systems. In Proceedings of the 18th ACM conference on Computer and communications security, pages 491–500. ACM, 2011.
[8] D. Harnik, B. Pinkas, and A. Shulman-Peleg. Side channels in cloud services: Deduplication in cloud storage. IEEE Security & Privacy, 8(6):40–47, 2010.
[9] C. Hazay and Y. Lindell. Efficient secure two-party protocols: Techniques and constructions. Springer Science & Business Media, 2010.
[10] T. Jiang, X. Chen, Q. Wu, J. Ma, W. Susilo, and W. Lou. Secure and efficient cloud data deduplication with randomized tag. IEEE Transactions on Information Forensics and Security, 12(3):532–543, 2017.
[11] S. Lee and D. Choi. Privacy-preserving cross-user sourcebased data deduplication in cloud storage. In 2012 International Conference on ICT Convergence (ICTC), pages 329–330. IEEE, 2012.
[12] J. Li, X. Chen, M. Li, J. Li, P. P. Lee, and W. Lou. Secure deduplication with efficient and reliable convergent key management. IEEE transactions on parallel and distributed systems, 25(6):1615–1625, 2014.
[13] J. Li, Y. K. Li, X. Chen, P. P. Lee, and W. Lou. A hybrid cloud approach for secure authorized deduplication. IEEE Transactions on Parallel and Distributed Systems, 26(5):1206–1216, 2015.
[14] M. Li, C. Qin, P. P. Lee, and J. Li. Convergent dispersal: Toward storage-efficient security in a cloud-of-clouds. In 6th USENIX Workshop on Hot Topics in Storage and FileSystems (HotStorage 14), 2014.
[15] J. Liu, N. Asokan, and B. Pinkas. Secure deduplication of encrypted data without additional independent servers. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, pages 874–885. ACM, 2015.
[16] M. Mulazzani, S. Schrittwieser, M. Leithner, M. Huber, and E. R. Weippl. Dark clouds on the horizon: Using cloud storage as attack vector and online slack space. In USENIX security symposium, pages 65–76. San Francisco, CA, USA, 2011.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY