iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** VI **Month of publication:** June 2019

DOI: http://doi.org/10.22214/ijraset.2019.6272

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: 7.177
Volume 7 Issue VI, June 2019- Available at www.ijraset.com

AES (Advanced Encryption Standard) Based Cryptography for Data Security in Cloud Environment

Aastha Tiwari[1], M. V. Padmavati[2], Monika Arya[3]
[1, 2, 3]*Dept. of CSE, Bhilai Institute of Technology, Durg, Chhattisgarh*

Abstract*: With the growing rate of cloud computing and Information sharing, there is a growth in users and security breach into the system and data. Cryptography based on identity has allowed us to define an innovative solution to ensure the confidentiality of data stored on remote servers. This paper presents, data security technique based on AES (Advanced Encryption Standard) cryptography approach for secure data sharing among users of the cloud. Our approach is to provide secure data before storing on the cloud using the AES algorithm. Using this approach only authorized users of the application can access the available resources and facilities. In this research proposed a new algorithm called DSICE (Data Security in Cloud using Encryption), which encrypt the file using secure key, uploaded by the user at the cloud end and DSICD (Data Security in Cloud using Decryption), which decrypt the file data using secure key from the cloud at the other end. The application has been implemented through a multi-tier web application based on Java technology, Apache Server and Mysql database. Security of data can be reached using AES cryptography and the overall system has been tested using the JMeter application and the comparative study was taken into account between localhost and cloud.

Keywords*: Web Application, Data Security, AES (Advanced Encryption Standard) cryptography, Multi-tier WebApp, JMeter.

I. INTRODUCTION

A new way of service is offered by cloud computing. In this service, available resources are arranged in such a way that they fulfill users demands using the internet based on the features offered by cloud computing. The process which is being discussed in this paper is by Storing data into the cloud that reduces the burden of users [1] and brings them the convenience of access; which has become one of the greatest advantages [2]. Overall enthusiasm for distributed storage benefits mostly exudes from business associations and government offices looking for stronger and savvy frameworks. That is, the advantages of cloud reception are truly unmistakable in another period of responsiveness, viability and proficiency in Information Technology administration conveyance. Thus, there is never again a need to spend a lot of capital on purchasing costly application programming or complex equipment that they may never require again. These efficient advantages present the primary basic inspirations for cloud selection as they help endeavors lessening the Capital Expenditure (CapEx), saved to purchase fixed resources and the Operational Expenditure (OpEx) which is a continuous expense for running an item, business, or a framework. For instance, corporate associations and seaward re-appropriating include comparative trust and administrative issues. Essentially, open source software empowers IT, divisions, to rapidly construct and send applications, however at the expense of control and administration. Also, virtual machine assaults and Web administration vulnerabilities existed some time before distributed computing wound up in vogue. Therefore, the assorted variety of the administrations conveyed through cloud frameworks expands their powerlessness to security occurrences and assaults. In this way, these provoke should be tended to as for security and protection in a cloud setting. Circulated registering security is a quickly making association that gives a basic number of well-defined functionalities from standard IT security. These breakers shielding basic data from robbery, information spillage, and cancellation. One of the upsides of cloud associations is that you can work at scale and still stay secure. It takes after how you at present direct security, yet now you have better philosophies for passing on security designs that region new areas of concern. Cloud security does not change the framework on the best way to deal with oversee security from avoiding to the operator and restorative activities. Regardless, it does at any rate engage you to play out these exercises in an inexorably dexterous way. Your information is secured inside server farms and where two or three nations foresee that information ought to be verified in their nation, picking a supplier that has assorted server develops over the world can accomplish this. Information collecting from time to time combines certain consistence basics, particularly while verifying charge card numbers or success data. Many cloud suppliers offer free distant study reports to endorse that their inside methodology exists and are reasonable in dealing with the security inside their working environments where you store your information.

A. Cloud Storage Basics

Cloud clients are raised to a dimension of deliberation that shrouds the subtleties of equipment or programming foundations, sent for supporting escalated calculation and information stockpiling. From this definition, three principle key focuses must be considered. To begin with, NIST plots the improvement of advances that help an inescapable, all-inclusive and proper new plan of action. Second, it includes the significance of the system get to procedures to shared assets that guarantee a liquid communication between the cloud suppliers and their customers. Third, this definition centers around the related valuing model of cloud which enables clients to pay just for devoured assets.

To all the more likely comprehend the center ideas and advances in the cloud, we extricate from the NIST definition record five characteristics. These properties portray a cloud-based framework as a general model giving metered on interest administrations to his customers. These attributes are exhibited as pursues:

1) *On-Request self-Administration:* Cloud clients may get additional assets, for example, the use of capacity limits and processing exhibitions, with no human intercession.
2) *Broad System Get to:* The huge assortment of heterogeneous gadgets, for example, cell phones, PCs, tablets, and all hand-held and static types of gear must almost certainly access to cloud benefits through standard instruments.
3) *Shared Assets*: Based on a multi-occupant model, cloud assets are shared among a few clients.
4) *Elasticity:* Along with self-provisioning assets, the cloud is portrayed with the real ability to proficiently find and discharge assets. This property exhibits an adaptability of more prominent assets.
5) *Metered Administration*: This property alludes to the plan of action received by cloud-based administrations, where clients pay on a utilization premise, empowering real cost decreases.

Expanding upon equipment offices, these administration models are offered in different structures:

a) *Infrastructure as a Service (IaaS):* In this administration model, assets are overseen totaled and conveyed to clients as capacity limits (e.g., Amazon Simple Storage Service (S3) [Ama]), organize mediums, or registering abilities (e.g., Amazon Elastic Compute Cloud (EC2) [Inc08]). Clients would then be able to run any working frameworks and programming that best meet their prerequisites. Simply, they can't oversee or control the fundamental cloud foundation.
b) *Platform as a Service (PaaS):* This administration model gives an advancement domain or stage, on which clients execute their applications. That is, clients can modify applications that objective a particular stage, with the devices offered by their Cloud Service Provider (CSP).
c) *Software as a Service (SaaS):* In this model, the cloud supplier offers programming applications as an administrator. For example, rather than purchasing and introducing programming on individual frameworks, customers utilize the proposed applications, in a compensation for every utilization premise. Access to these applications can be performed from different gadgets through either a custom interface or a program interface.

B. Cloud Security And Privacy Challenges

Protection is one more basic worry with respect to cloud situations, because of the way that customers' information lives among remote dispersed servers, kept up by possibly untrusted cloud suppliers.

Similarly, as with any remote stockpiling framework, there are main security properties that are very prescribed in distributed storage, specifically, classification, trustworthiness and freshness. These properties guarantee that customer information is secure and can't be changed by unapproved clients. Besides, the information should be ensured when moved and put away in distributed storage servers. Accordingly, specialist co-ops need to guarantee fine-grained access, information accessibility claims, and successful information and procedure separation which remain a noteworthy issue in cloud frameworks. We have likewise to underline the significance of the guideline and the enactment consistency, when laying out the distinctive security necessities. That is, when put away, information might be transmitted through various cloud structures, and afterward, they may fall under various administrative consistence limitations which can offer ascent to Service Level Agreement (SLA) or security infringement.

Then again Data security, protection and trust in the cloud become urgent issues. To begin with, storing the information into the cloud expands the danger of information spillage and unapproved get to. Second, Cloud server farms are turning into the objectives of assaults and interruptions, which challenge cloud information security. Third, information the executive's tasks, for example, information stockpiling, reinforcement, relocation, erase, update, search, inquiry and access in the cloud may not be completely trusted by its proprietors. To conquer the above hindrances cloud information security, Privacy and trust are for sure turning into a key innovation in the achievement of distributed computing [3].

C. Cryptography

The concept of Cryptography (CoC) is widely applied to ensure trust, privacy and data security in cloud computing. But the problem is that the existing systems are inadequate and not up to the mark. Storing encrypted data in the cloud makes it hard to perform, but the risk of privacy leakage is greatly reduced [4, 5, 6]. The Key management for access over cloud and revocation introduces complex computation and communication costs. In addition, operations such as fusion, aggregation, and mining on encrypted data are still impractical to be deployed due to high computational complexity and inefficiency.

Cryptography in cloud computing promises many novel solutions and at the same time, many challenges are yet to be overcome. This paper proposes one of the methods to secure data using symmetric key cryptography.

Given below are some possible solutions, which will help to overcome the challenges:

1) Improving data confidentiality in cloud storage environments while enhancing dynamic sharing between cloud users.
2) Provide cloud storage environments for data integrity verification like security level, public verifiability, and performance.
3) Implementing the proposed techniques using standards and widely deployed schemes, and validating their visibility and impact on real hardware.

D. AES Cryptography

The Advanced Encryption Standard (AES) is a formal encryption technique grasped by the National Institute of Benchmarks and Technology of the US Government, and is recognized the world over [7].

In 1997 the National Institute of Standards and Innovation (NIST), a piece of the US government, started a method to perceive an exchange for the Data Encryption Standard (DES). It was generally seen that DES was not checking because of advances in PC dealing with power. The target of NIST was to portray an exchange for DES that could be used for non-military information security applications by US government workplaces. Clearly, it was seen that business and other non-government customers would advantage from made by NIST and that the work would be ordinarily held onto as a business standard.

AES encryption uses alone key as a bit of the encryption procedure. The key can be 128 bits (16 bytes), 192 bits (24 bytes), or 256 bits (32 bytes) in length. The term 128-piece encryption shows to the use of a 128-piece encryption key. With AES both the encryption and the unscrambling are performed using a comparable key. This is known as asymmetric encryption estimation. Encryption computations that use two various keys, an open and a private key, are called disproportionate encryption figuring.

There are different systems for using keys with the AES encryption procedure. These different procedures are characterized by "strategies for action". NIST portrays different techniques for action for AES which include:

1) Electronic codebook (ECB)
2) Cipher square securing (CBC)
3) Counter (CTR)
4) Cipher analysis (CFB)
5) Output analysis (OFB)
6) Galois Counter Mode (GCM)

Each mode uses AES in a substitute way. Cloud and VMware customers benefit from the various operational and cost efficiencies given by these stages. Regardless, affiliations need to pick encryption courses of action inside these phases that rely upon industry measures. While rising encryption advancements are open, it is basic to simply use courses of action that have encountered NIST endorsement and rely upon measures, for instance, AES.

II. LITERATURE SURVEY

In this paper, Heroku is executed as a cloud stage, after which AES is actualized for information security in Heroku. Heroku depends on an oversaw compartment framework, with incorporated information administrations and a ground-breaking biological system, for sending and running current applications. One fundamental issue in distributed computing is information security, which is taken care of utilizing cryptography techniques. A conceivable technique to encode information is Advanced Encryption Standard (AES). The exhibition assessment demonstrates that AES cryptography can be utilized for information security [8]. The execution for sending Heroku as a cloud stage comprises of a few stages. Site conveying AES as security calculation is actualized as an application to information security [9, 10, 11]. The execution assessment demonstrates that AES cryptography can be utilized for information security. Postpone count of information encryption demonstrates that the bigger the size of information builds the information defer the time for encryption of information. The approach pursued is, to gather asset/information, store information in the cloud pursued by information preparing by offering access to bring the asset to client IP, checking programmer's data and

administrator reacting by limiting separate IP. The limited IP client can never get to the assets any longer [14, 15, 16]. Huge information security in the cloud, brings about following unapproved clients (programmers) who attempt to get to the assets. The administrator has an exceptional benefit to hinder the programmer's machine by crippling the IP address of the individual machine [12, 13]. A cryptography approach, by which the cloud administration administrators can't legitimately achieve halfway information [17, 18, 19] is being utilized. The proposed methodology isolates the record and independently stores the information in the dispersed cloud servers. An elective methodology is intended to decide if the information parcels need a split to abbreviate the task time. The proposed plan is entitled Security-Aware Efficient Distributed Storage (SA-EDS) model, which is for the most part bolstered by our proposed calculations, including Alternative Data Distribution (AD2) Algorithm, Secure, Efficient Data Distributions (SED2) Algorithm, and Efficient Data Conflation (EDCon) Algorithm. A tale approach entitled as Security-Aware Efficient Distributed Storage (SA-EDS) model is additionally been examinations. In this model, the frameworks are utilized as the proposed calculations, including Alternative Data Distribution (AD2), Secure, Efficient Data Distributions (SED2) and Efficient Data Conflation (EDCon) calculations [20]. Their test assessments demonstrated that our proposed plan could successfully protect real dangers from the cloud side [21]. A proposed framework that actualizes the trust the board framework for distributed computing, that guarantees secure information access through a reliable cloud specialist organization. Here, the trust assessment strategy is proposed in which the weighted trust factor is determined thinking about various properties. The trust factor encourages clients to distinguish reliable cloud specialist co-ops through which they can utilize cloud administrations [22, 23]. This work incorporates information to the executives in cloud servers with security and protection [24]. It likewise incorporates the execution of the two servers, first, the essential server offers the administrations for applications, and second, the optional server is implemented to expend the essential server's administrations in a verifying way [25]. To save the information in system and capacity, the cryptographic framework is likewise proposed. Notwithstanding that this strategy gives a weighted trust assessment to getting to and putting away information on the server.

III. PROBLEM IDENTIFICATION

Cloud information stockpiling administrations bring many testing configuration issues, impressively because of the loss of physical control. These difficulties affect the information security and execution of cloud frameworks. This is to a great extent because of the way that clients redistribute their information on remote servers, which are controlled and overseen by conceivable untrusted Cloud Service Providers (CSPs). It has ordinarily concurred that information encryption at the customer side is a decent choice to moderate such worries of information classification. In this manner, the customer safeguards the decoding keys far from the cloud supplier. In any case, this methodology offers to ascend to a few key administration concerns, for example, putting away and keeping up keys accessibility at the customer side. Furthermore, classification conservation turns out to be progressively entangled with adaptable information sharing among a gathering of clients. To begin with, it requires a productive sharing of decoding keys between various approved clients. The test is to characterize a smooth gathering disavowal which does not require refreshing the mystery keys of the rest of the clients. Along these lines, the multifaceted nature of key administration is limited.

Second, get to control arrangements ought to be adaptable and recognizable among clients with various benefits to get to the information. That is, information might be shared by various clients or gatherings, and clients may have a place with a few gatherings. On the opposite side, information trustworthiness is considered as a pertinent worry, in cloud situations. That is, the obligation of safely overseeing re-appropriated information is part of various capacity limits. Such appropriation gives strength against equipment. In any case, to lessen working expenses and spare stockpiling limits, untrustworthy suppliers may purposefully slight these replication techniques, bringing about unrecoverable information mistakes or even information misfortunes. Notwithstanding when cloud suppliers execute a deficiency tolerant approach, customers have no specialized methods for confirming that their documents are not defenseless, for example, to drive crashes. There may be the usage of remote information checking at the three after dimensions:

1) *Between a Customer and a CSP:* A cloud client ought to have a productive method to perform periodical remote trustworthiness confirmations, without keeping the information locally. Furthermore, the customer ought to likewise identify SLA infringement, for the capacity strategy. This present client's worry is amplified by his obliged stockpiling and calculation abilities and the enormous size of redistributed information.
2) *Within a CSP:* It is significant for a cloud supplier to check the uprightness of information squares put away over various capacity hubs, to alleviate Byzantine disappointments and drive-crashes.
3) *Between two CSPs:* For the situation of the haze of cloud situations, where information is partitioned on various cloud foundations. Accordingly, a CSP, through its cloud entryway, ought to intermittently confirm the credibility of information squares facilitated by another cloud stage.

These security concerns are much progressively significant, as the European guidelines will be increasingly extreme and resolute, including further disparagements to successfully ensure individual information which is re-appropriated on remote servers. The EU General Data Protection Regulation (GDPR) is required to be passed for the current year and produces results at the start of 2015. The US Sky high Networks Company overviewed more than 7000 cloud administrations and demonstrate that solitary 1 of every 100 cloud suppliers satisfies all the security necessities plot by the new European guideline. In that capacity, cloud suppliers will have genuine work to guarantee consistency with these new criticisms.

IV. METHODOLOGY

It is an effective and flexible distributed scheme with explicit dynamic data support to ensure the correctness of users' data in the cloud. We rely on erasure correcting codes in the file distribution, preparation to provide redundancies and guarantee the data dependability. This construction drastically reduces the communication and storage overhead as compared to the traditional replication-based file distribution techniques. By utilizing the homomorphism token with distributed verification of erasure-coded data, our scheme achieves the storage correctness insurance as well as data error localization: whenever data corruption has been detected during the storage correctness verification, our scheme can almost guarantee the simultaneous localization of data errors, i.e., the identification of the misbehaving server(s).

There are two different algorithms proposed, one for uploading a secure file using secure key management and the other end downloading that secure file from the server using the secure key.

The first part is uploading a data file using an algorithm called DSIC Encryption (Data Security in Cloud using Encryption) algorithm, in which specific users can upload files in the cloud for file sharing that is encrypted By AES algorithm. Encryption and Decryption have done through AES before saving of actual file stored in Server Side.

A. Data Security Model

File owner who wants to share a file to any other cloud user has to initiate the process in the application. The first owner must authenticate from a web application, a separate session is managed by the server to each user who logged-in. The owner has to upload a file which he or she wants to share must provide a secure key of 16 char. Before uploading of a file to cloud the file is encrypted and stored in a server. At the other end who wants the file must provide key to decrypt the file from the server. After uploading only 3 times a user can download the file. After three successful attempts the file itself is deleted from the server shown in figure 1 and after the encryption and decryption algorithm is written step by step.

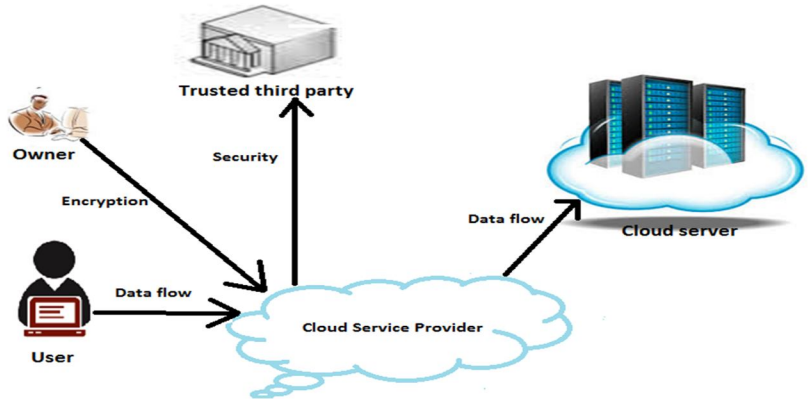


Figure 1. Our Research Data Security Model

B. The Steps of Algorithm for DSIC Encryption

1) *Step 1:* Client Authentication from the Server Side and Backend Database (MYSQL).
2) *Step 2:* Session and State Maintenance of Client.
3) *Step 3:* Initiate File Sharing from the client Side (Done through Java Server Page) with Servlet (Server Side Program).
4) *Step 4:* File is uploaded through Servlet and JSP (Java Server Page) with proper authentication of file and file type.
5) *Step 5:* Encrypted Data is stored in the form of Binary Large Object with the proper key and properly maintain with another attribute.
6) *Step 6:* A limited number of download is permitted during secure file sharing done through server side.
7) *Step 7:* End (Secured Data Sharing have been Done).

The Second Part is downloading a file using DSIC Decryption (Data Security in Cloud using Decryption)

C. The Steps of Algorithm for DSIC Decryption

1) *Step 1:* Client Authentication from the Server Side and Backend Database (MYSQL).
2) *Step 2:* Session and State Maintenance of Client.
3) *Step 3:* Initiate File Downloading from the client Side (Done through Java Server Page with Servlet (Server Side Program).
4) *Step 4:* File is downloaded through Servlet and JSP with proper 16 characters key.
5) *Step 5:* Decrypted Data is stored in an original format form the Binary Large Object with the proper key and properly maintain with another attribute.
6) *Step 6:* Limited number of download is permitted during secure file sharing done through server side.
7) *Step 7:* End (Secured Data Sharing have been Done).

V. IMPLEMENTATION AND RESULT

The implementation part of our Research has been done through Java Technology (JDK 1.8, Servlet 3.3 and JSP), MYSQL 5.5 for database, Apache Tomcat 7 a server and JMeter 3.0 as a performance test. The Snapshots of our research implementation is below...

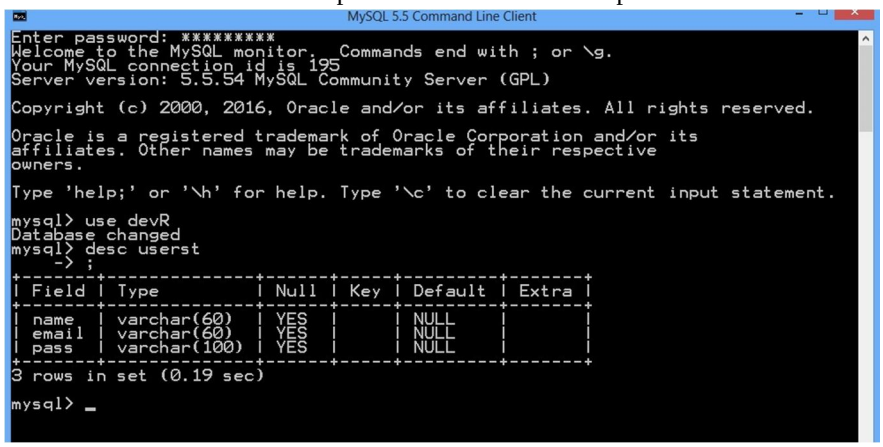


Figure 2. Web application data table userst

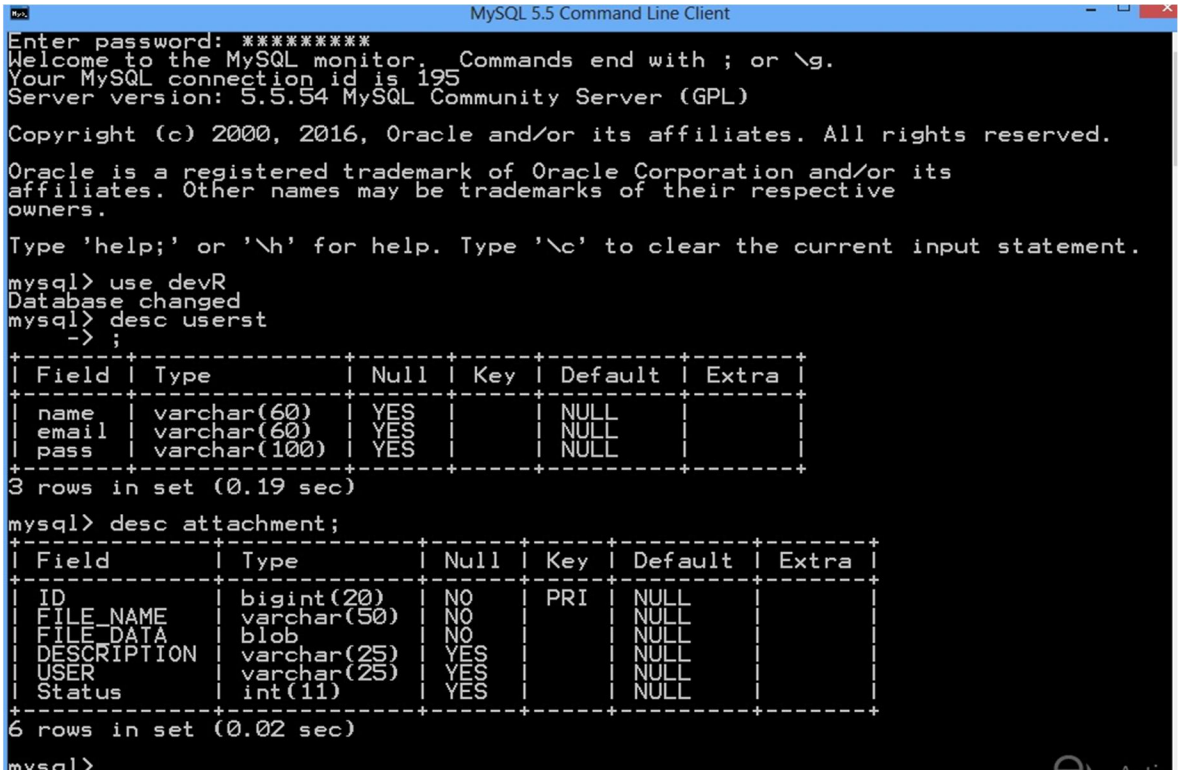


Figure 3. Web application data table Attachment

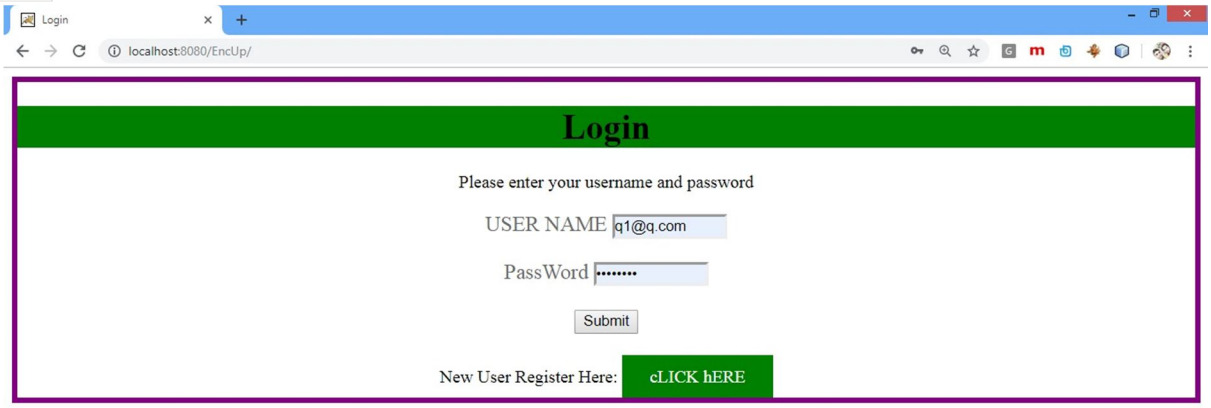


Figure 4. Home Page for user authentication

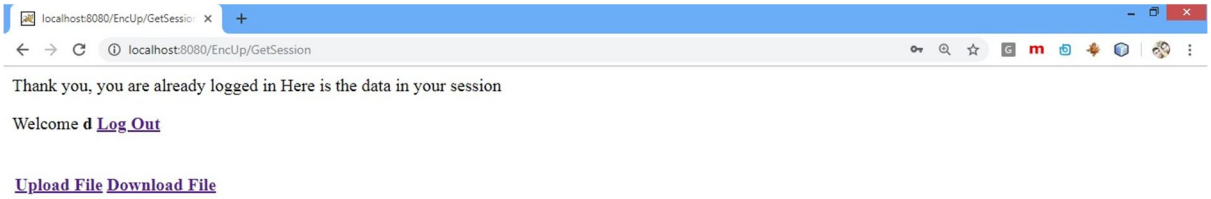


Figure 5. After successfully user authentication

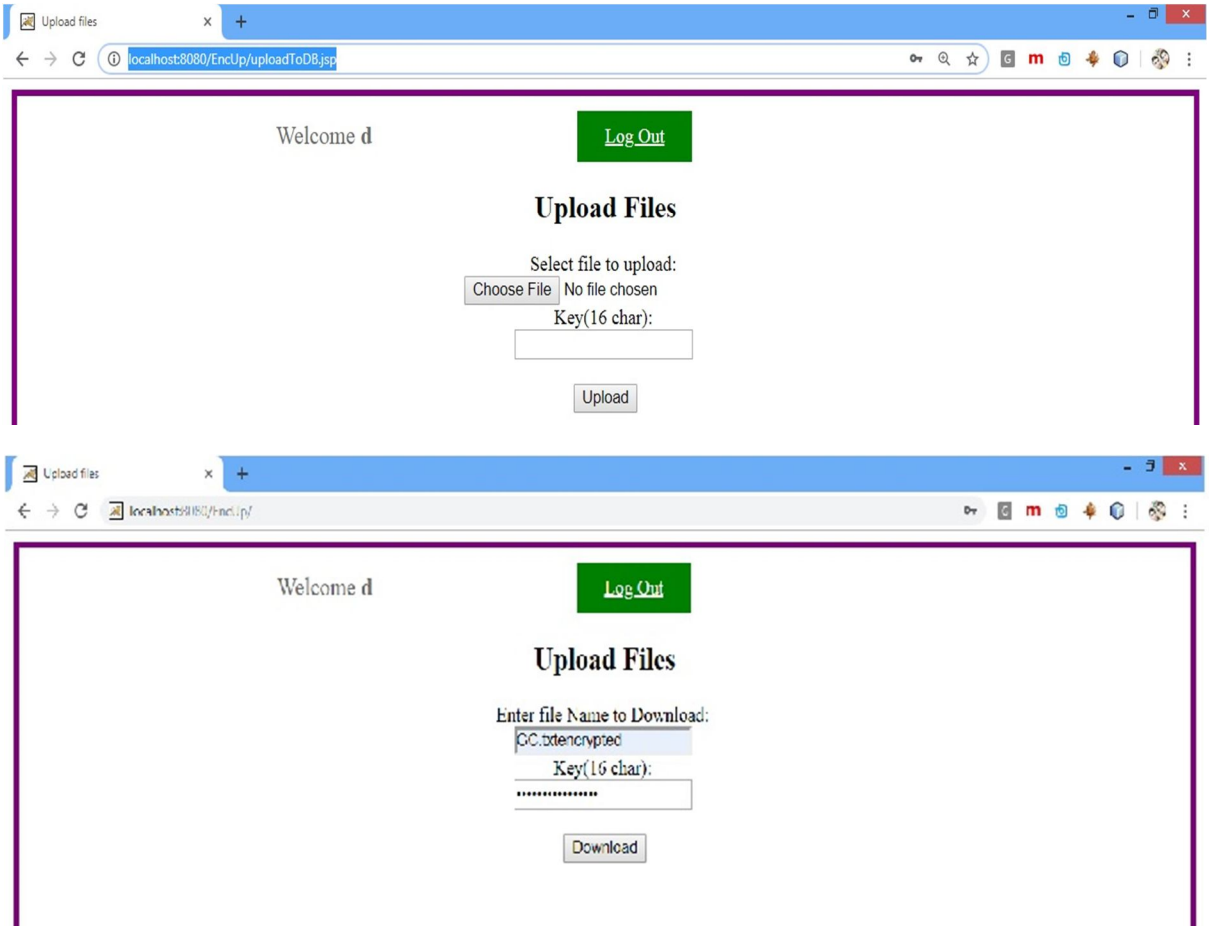


Figure 6. Uploading File page with 16 char key

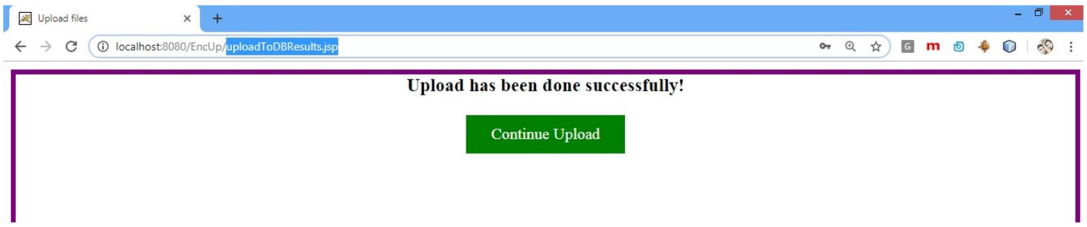


Figure 7. Successfully uploading of file

Figure 8. File Data is stored in an encrypted format

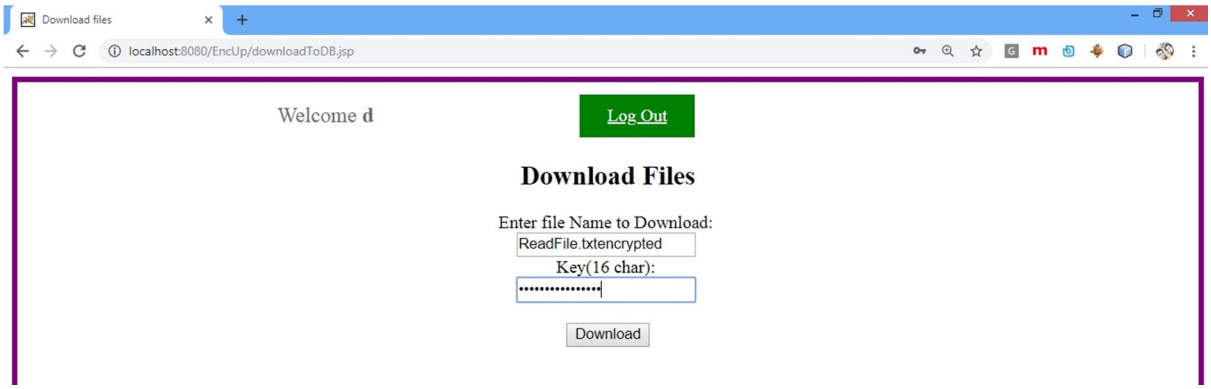


Figure 9. Downloading of File using 16 char key

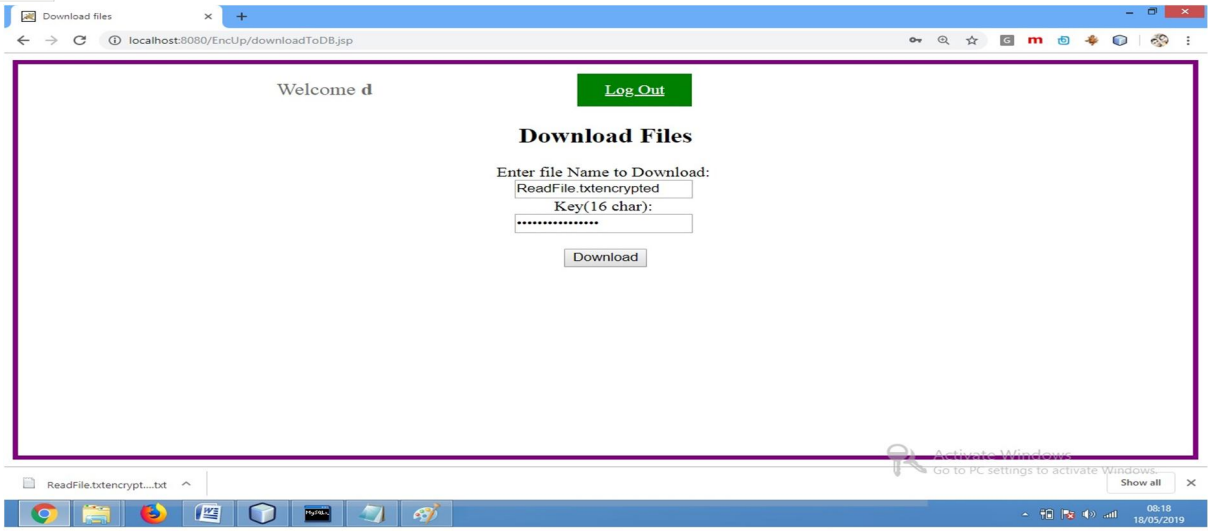


Figure 10. Downloaded File

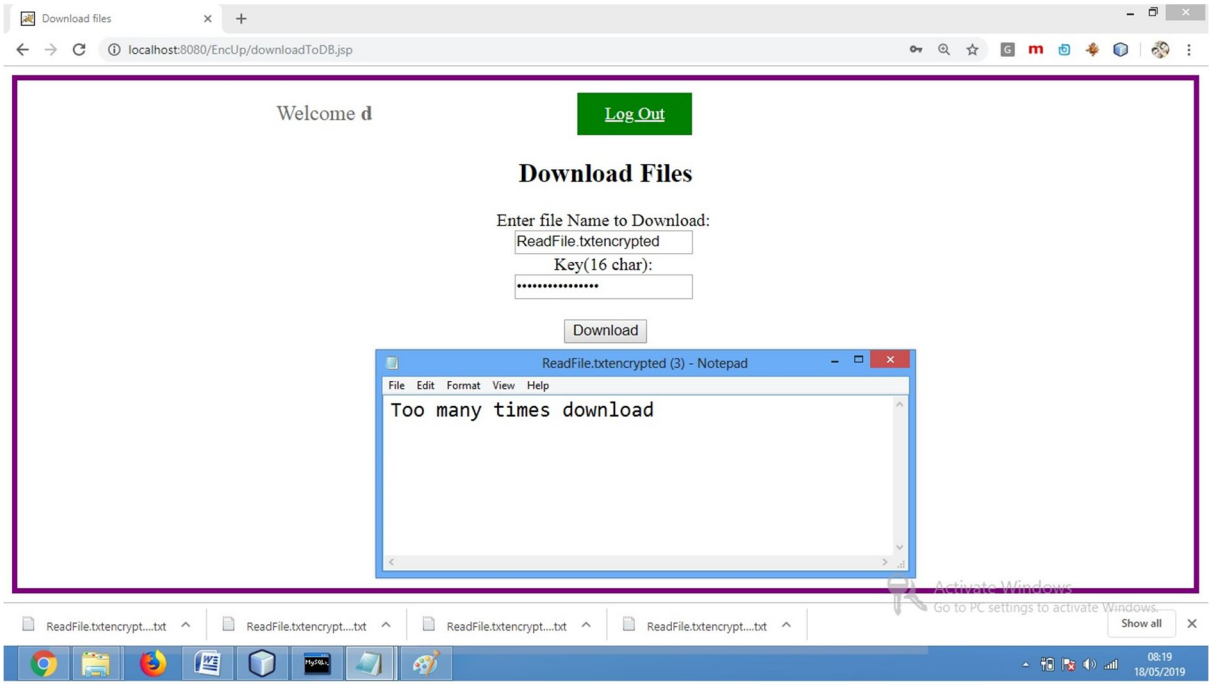


Figure 11. Error Message after limited times of downloading

In addition to testing and evaluating whether the data is secured, we also evaluate the delay calculation using Apache JMeter 3.3. In the localhost cloud environment with a 50 number of users, the data traffic will become high, which will have an impact on the system. In a real environment, many factors could cause delay, e.g. the size of the uploaded file, the network speeds, etc., which will cause delays and congestion.

When the file is uploaded, it is initially split into different blocks before encryption. The size of each block depends on the file size. Delay metric is calculated as the sum of delay during the block-wise upload to a different location in the cloud [8].

Delay=T_s-T_b ---------- (1)

T_s: Time after a successful load

T_b: Time before load

Delay calculation is done by recording the encryption time for files with a size of 3000 KB, 5000 KB, 7000 KB, 10000 KB, and 15000 KB. The delay calculation is shown in below Figure 12.

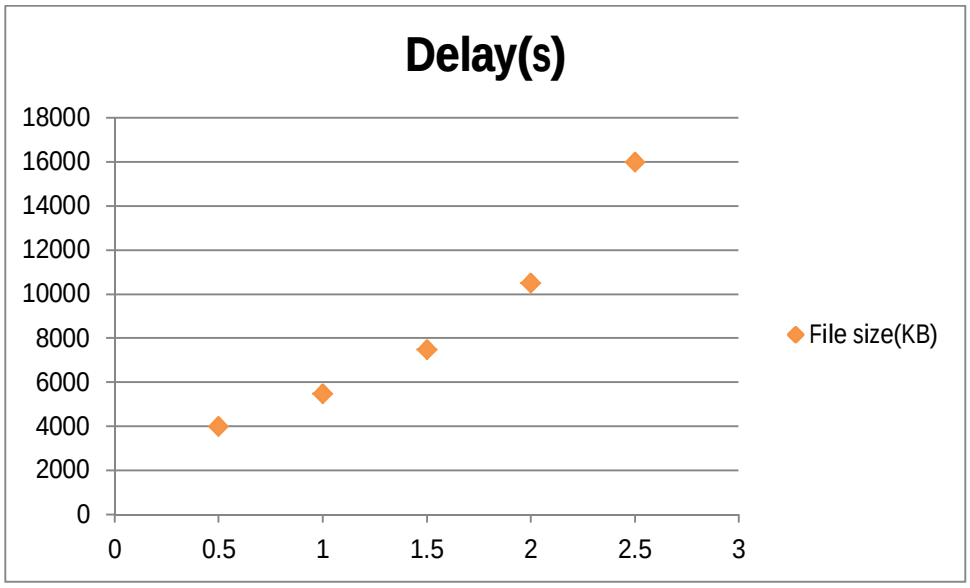


Figure 12. Delay calculation

The larger numbers of file sizes indicate increased delay due to the time when more data encrypt generate. The Delay Comparison of previous methodology [8] and our research shows the significant differences in the delay that indicate our research is better than the previous solution.

VI. CONCLUSION AND FUTURE WORK

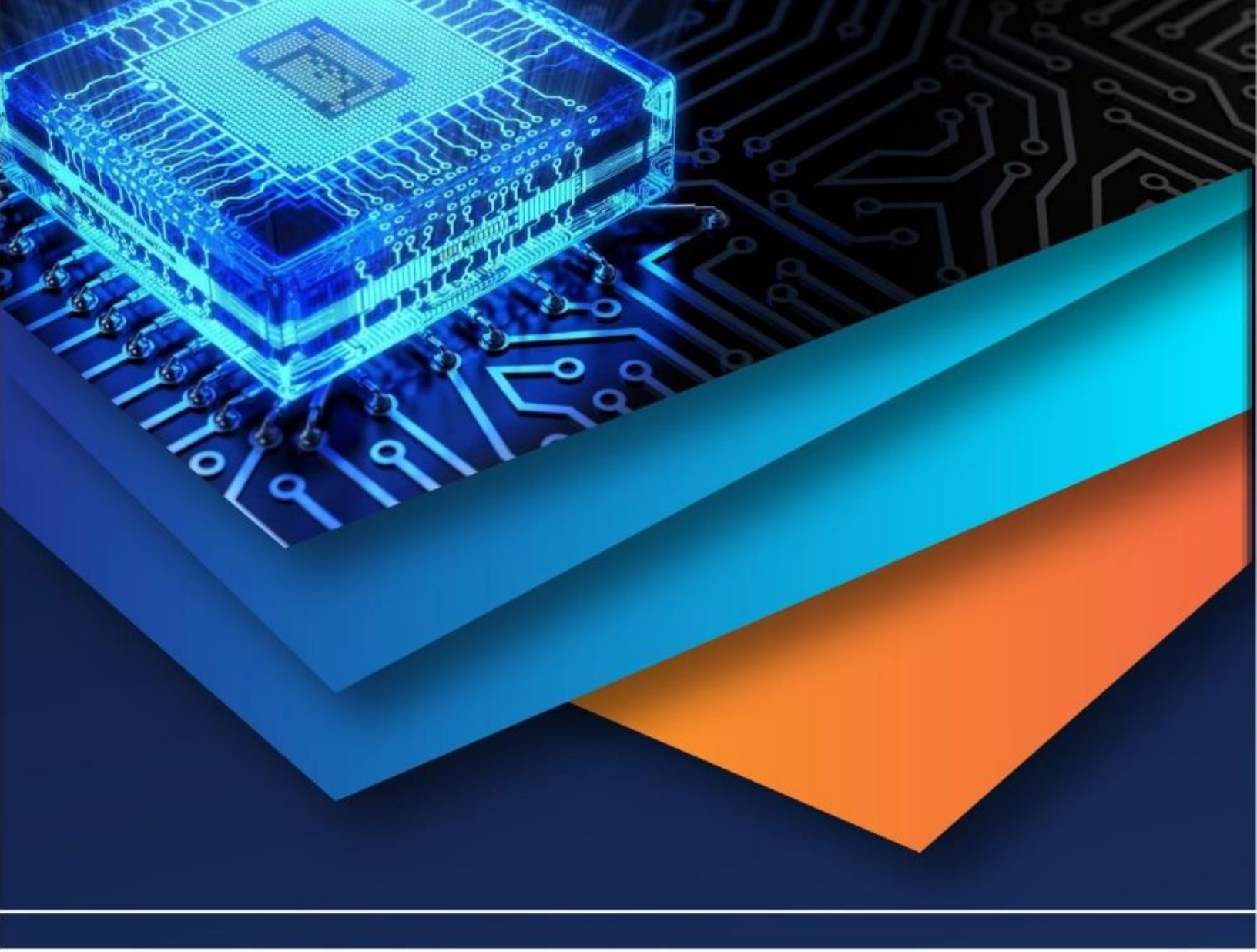
The rise in demand for secure storage services correlates with the specificities of cryptography based on identity has allowed us to define an innovative solution to ensure the confidentiality of data stored on remote servers.

We have completed all the objectives with a given period. The outcome of the objective is to make sure that the system allows only valid users to access the functionality of approaches, maintain better level security using cryptography algorithm and the outcome of the application is measured in the JMeter Application software and implementation of the application is done in the real cloud. So as of now, this research satisfies all the objective and user implemented web application can ensure the secured file sharing. In the future, there is a scope of trust management service to ensure the uses of the cloud.

REFERENCES

[1] Aastha Tiwari, M. V. Padmavati, Monika Arya, "Data Security in Cloud using Cryptographic Approach", IJMTE Spl.2019. Page No: 1143-1156, DOI: 16.10089.V9I3.19.27678.
[2] S. Zarandioon, D. Yao, and V. Ganapathy, " K2c: Cryptographic cloud storage with lazy revocation and anonymous access", In Secure Comm., volume 96, pages 59–76. Springer, 2011.
[3] K. Zunnurhain, "Fapa: a model to prevent flooding attacks in clouds", In Proceedings of the 50th Annual Southeast Regional Conference, ACM-SE '12 pages 395–396, New York, NY, USA, 2012. ACM.
[4] J. Xu and E. Chang, "Towards efficient proofs of irretrievability", In Proceedings of the 7th ACM Symposium on Information, Computer, and Communications Security, ASIACCS '12, New York, NY, USA, 2012.
[5] C. Wang, Q. Wang, K. Ren, and W. Lou., "Privacy-preserving public auditing for data storage security in cloud computing", In Proceedings of the 29th Conference on Information Communications, INFOCOM'10, pages 525–533, Piscataway, NJ, USA, 2010. IEEE Press.
[6] Wang, Q., Wang, C., Li, J., Ren, K., & Lou, W. (2009, September), "Enabling public verifiability and data dynamics for storage security in cloud computing", In European symposium on research in computer security (pp. 355-370), Springer, Berlin, Heidelberg.
[7] Van Dijk, M., Juels, A., Oprea, A., Rivest, R. L., Stefanov, E., & Triandopoulos, N. (2012, October). "Hourglass schemes: how to prove that cloud files are encrypted", In Proceedings of the 2012 ACM conference on Computer and communications security (pp. 265-280), ACM.
[8] Lee, B. H., Dewi, E. K., & Wajdi, M. F. (2018, April). "Data security in cloud computing using AES under HEROKU cloud", in 2018 27th Wireless and Optical Communication Conference (WOCC) (pp. 1-5), IEEE.
[9] Smart, N. P., & Vercauteren, F. (2010, May). "Fully homomorphic encryption with a relatively small key and ciphertext sizes", In International Workshop on Public Key Cryptography (pp. 420-443). Springer, Berlin, Heidelberg.
[10] Van Dijk, M., Gentry, C., Halevi, S., & Vaikuntanathan, V. (2010, May), "Fully homomorphic encryption over the integers", In Annual International Conference on the Theory and Applications of Cryptographic Techniques (pp. 24-43). Springer, Berlin, Heidelberg.
[11] Lalitha, V. P., Sagar, M. Y., Sharanappa, S., Hanji, S., & Swarup, R. (2017, August), "Data security in cloud", In 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS) (pp. 3604-3608), IEEE.

[12] Ristenpart, T., Tromer, E., Shacham, H., & Savage, S. (2009, November). Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. In Proceedings of the 16th ACM conference on Computer and communications security (pp. 199-212), ACM.
[13] Mallaiah, K., & Ramachandram, S. (2014), Applicability of homomorphic encryption and CryptDB in social and business applications: Securing data stored on the third party servers while processing through applications. International Journal of Computer Applications, 100(1).
[14] Koblitz, N. (1987). Elliptic curve cryptosystems. Mathematics of computation, 48(177), 203-209.
[15] Kaaniche, N., & Laurent, M. (2014, March), "A secure client-side reduplication scheme in cloud storage environments". In 2014 6th International Conference on New Technologies, Mobility and Security (NTMS) (pp. 1-7), IEEE.
[16] Li, Y., Gai, K., Qiu, L., Qiu, M., & Zhao, H. (2017), "Intelligent cryptography approach for secure distributed big data storage in cloud computing", Information Sciences, 387, 103-115.
[17] Kaaniche, N., Laurent, M., & El Barbori, M. (2014, August). Cloudasec:" A novel public-key based framework to handle data sharing security in clouds". In 2014 11th International Conference on Security and Cryptography (SECRYPT) (pp. 1-14), IEEE.
[18] Juels, A., & Kaliski Jr, B. S. (2007, October). PORs: Proofs of retrievability for large files. In Proceedings of the 14th ACM conference on Computer and communications security (pp. 584-597) Acm.
[19] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker. Cipher text-policy attribute-based threshold decryption with flexible delegation and revocation of user attributes (extended version), April 2009
[20] Harbajanka, S., & Saxena, P. (2016, March). Survey paper on trust management and security issues in cloud computing. In Colossal Data Analysis and Networking (CDAN), Symposium on (pp. 1-3), IEEE.DOI: http://dx.doi.org/10.1145/2909067.2909068
[21] D. Johnson, D. Molnar, D. Xiaodong Song, and D. Wagner. Homomorphic signature schemes. In CT-RSA, pages 244–262, 2002.[KBL13] N. Kaaniche, A. Boudguiga, and M. Laurent. ID based cryptography for cloud data storage. In 2013 IEEE Sixth International Conference on Cloud Computing, Santa Clara, CA, USA, June 28 - July 3, 2013, pages 375–382, 2013.
[22] Krzywiecki, Ł., & Kutyłowski, M. (2012, November). Proof of possession for cloud storage via Lagrangian interpolation techniques. In International Conference on Network and System Security (pp. 305-319). Springer, Berlin, Heidelberg.
[23] S. Kamara and K. Lauter. Cryptographic cloud storage. In Proceedings of the 14th international conference on financial cryptography and data security, FC'10, Berlin, Heidelberg, 2010. Springer-Verlag
[24] Lee, C. C., Chung, P. S., & Hwang, M. S. (2013), " A Survey on Attribute-based Encryption Schemes of Access Control in Cloud Environment", IJ Network Security, 15(4), 231-240.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY