iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** IV **Month of publication:** April 2022

DOI: https://doi.org/10.22214/ijraset.2022.41631

www.ijraset.com

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

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue IV Apr 2022- Available at www.ijraset.com

Secure File Storage on Cloud Computing Using Cryptographic Algorithm

Shreya Sambhaji Ranadive[1], Harshada Sanjay Sawant[2], Jayesh Ekanath Pinjarkar[3]
[1, 2, 3]*Department of Computer Engineering, University of Mumbai, Shivajirao S. Jondhale College of Engineering, Dombivli (East), Maharashtra*

Abstract: ***Cloud computing is one among today's hottest research areas thanks to its ability to scale back costs related to computing while increasing scalability and adaptability for computing services. Cloud computing is Internet based computing thanks to shared resources, software and knowledge are provided to consumers on demand dynamically. Cloud computing is one among the fastest growing technology of the IT trade for business. Since cloud computing share disseminated resources via the network in the open environment, hence it makes security problems vital for us to develop the cloud computing applications. Cloud computing security has become the leading explanation for hampering its development. Cloud computing security has become a hot topic in industry and academic research. This system will explore data security of cloud in cloud computing by creating unique key and encryption by using that key.***
Keywords: cloud computing, cloud security, data security, encryption, elliptic curve cryptography, AES.

I. INTRODUCTION

The demand of internet for wireless communication is rising day by day and therefore there's a need of security to guard similar communication by druggies on unsecure wireless channels. Data transferred over the communication channels is susceptible to attacks because of sensitive information it contain.

To defend the data from external trouble the conception of Cryptography is surfaced. Cryptography is defined as " An art of writing a secret law" Methodology of writing similar law is cipher where a normal textbook is converted into cipher textbook which is generally called Encryption whereas the rear practice of converting a cipher textbook into normal textbook is known as Decryption.

Cryptography can be distributed as classical and ultramodern, classical cryptography ways were used to Antipode wiretapping and communication interception problems whereas the ultramodern cryptography ways are more secure and useful for high speed dispatches. The plain textbook will be accepted as input and cipher after encryption will be the affair. Using key, stoner can decide the original plain textbook after decryption

To crack the translated lines, a stoner needs an encryption key. While it's possible to crack translated information, utmost hackers do not have access to the quantum of computer processing power they would need to decrypt information. Authentication processes, which bear creating a stoner name and word. The customer lists the people who are authorized to pierce information stored on the pall system.

II. LITERATURE REVIEW

This section will have the sight of all research work done in field of Advance encryption algorithm. In the past years lot of research has been wiped out the area of cryptography, various cryptography techniques are evaluated on the idea of various parameters. In [5] a comparative analysis is performed between various symmetric techniques and at the top it's concluded that AES requires medium memory size as compared to other symmetric techniques and the strength of the algorithm in perspective of security is excellent. Also from [6] AES consumes less time for encryption than RSA. AES algorithm gives better security than RSA and DSA because it requires less time for encryption and decryption [7]. With the same key length if we compare, 3DES is far slower than AES almost 3 times and AES with respect to key length if we compare with RSA is much faster than RSA about hundred times [8]. For cloud security AES is considered as best cryptography technique [9], with respect to security having diverse key sizes of 128, 192 and 256 bit.Also it provides shield adjacent to different attacks such as differential attack, recovery attack, key attack and square attack. In [3] we can see on accumulating additional rounds (Nr) 16 to AES more computational time is required to interrupt the security of algorithm hence enhancing system data. In [10] a comparison study is done for AES which concludes that for fewer memory requirement AES is better. For the same file size it requires 10.2 MB and DES requires 43.3MB, also the simulation time of DES is bigger than AES.

In [11] a hybrid approach is employed combining the AES and RSA for improved security where data is encrypted by AES and key management is performed by RSA. For securing the Bluetooth transmissions a hybrid approach is employed in [12]where AES keys are encrypted by RSA and this approach takes the benefits of both AES and RSA thus highly secure. For the transmission of digital motion images AES is employed with DES which will provide better security as AES cannot withstand algebraic attacks [13]. In [14] encryption is done by AES first, then DES is employed for encryption after encrypting with AES and DES, data is encrypted with combined approach AES and DES which gave complex results or cipher code that's difficult to break. AES has been used with various algorithms before like RSA, DSA, Blowfish and lots of more. In this paper we are going to analyze the performance of AES combining this algorithm with Elliptic curve cryptography (ECC). User will input the text files, then the performance are going to be analyzed on the idea of varied parameters like time, storage, avalanche effect and correlation.

III. DESIGN

A. Step 1: Software Concept

The first step is to identify a need for the new system. This will include determining whether a business problem or opportunity exists, conducting a feasibility study to work out if the proposed solution is cost effective, and developing a project plan.

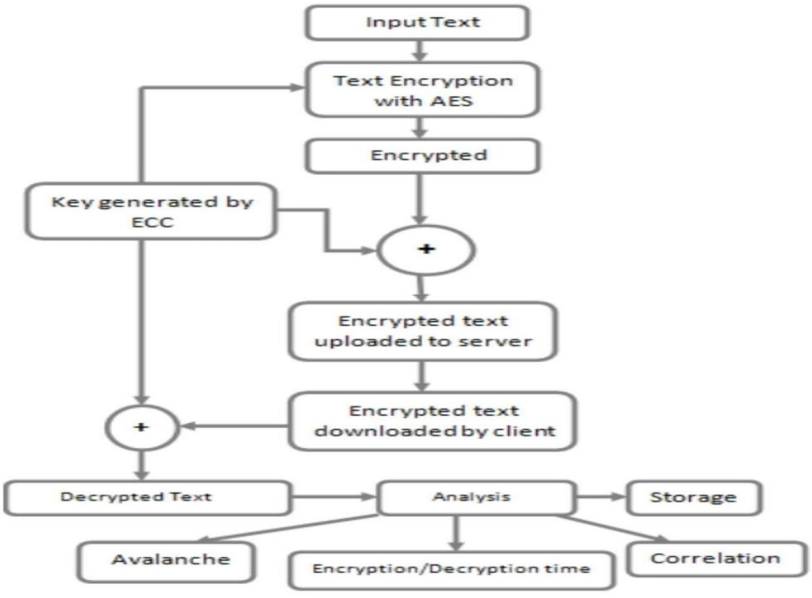
This process may involve end users who come up with a thought for improving their work. Ideally, the process occurs in tandem with a review of the organization's strategic plan to make sure that it's getting used to assist the organization achieve its strategic objectives. Management may have to approve concept ideas before any money is budgeted for its development.

B. Step 2: Requirements Analysis

Requirements analysis is that the process of analyzing the knowledge needs of the end users, the organizational environment, and any system presently getting used , developing the functional requirements of a system which will meet the requirements of the users. Also, the wants should be recorded during a document, email, interface storyboard, executable prototype, or some other form. The requirements documentation should be mentioned throughout the remainder of the system development process to make sure the developing project aligns with user needs and requirements. Professionals must involve end users during this process to make sure that the new system will function adequately and meets their needs and expectations.

C. Step 3: Architectural Design

After the wants are determined, the required specifications for the hardware, software, people, and data resources, and therefore the information products which will satisfy the functional requirements of the proposed system can be determined. The design will function a blueprint for the system and helps detect problems before these errors or problems are built into the final system. Professionals create the system design, but must review their work with the users to make sure the design meets users' needs.



D. Step 4: Coding and Debugging

Coding and debugging is the act of creating the final system. This step is done by software developer.

E. Step 5: System Testing

The system must be tested to guage its actual functionality in reference to expected or intended functionality. Some other issues to think about during this stage would be converting old data into the new system and training employees to use the new system. End users are going to be key in determining whether the developed system meets the intended requirements, and therefore the extent to which the system is really used.

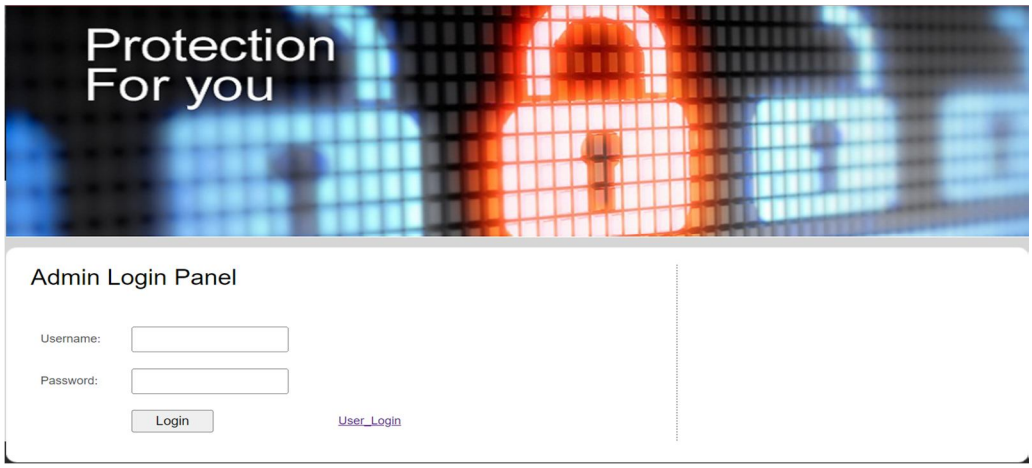
F. Step 6: Maintenance

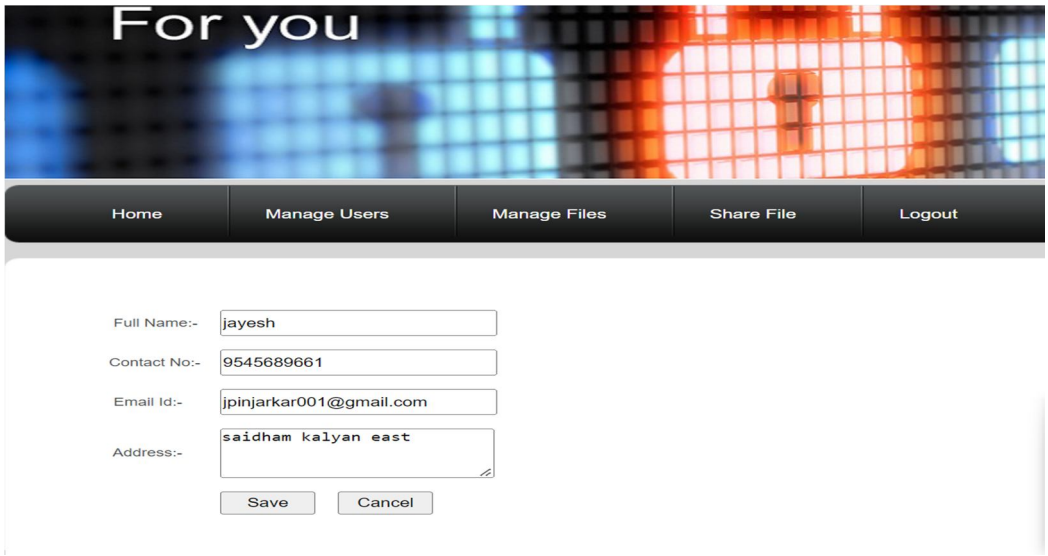
Inevitably the system will need maintenance. Software will definitely undergo change once it is delivered to the customer. There are many reasons for the change. Change could happen because of some unexpected input values into the system. In addition, the changes in the system could directly affect the software operations. The software should be developed to accommodate changes that would happen during the post implementation period.

IV. RESULTS

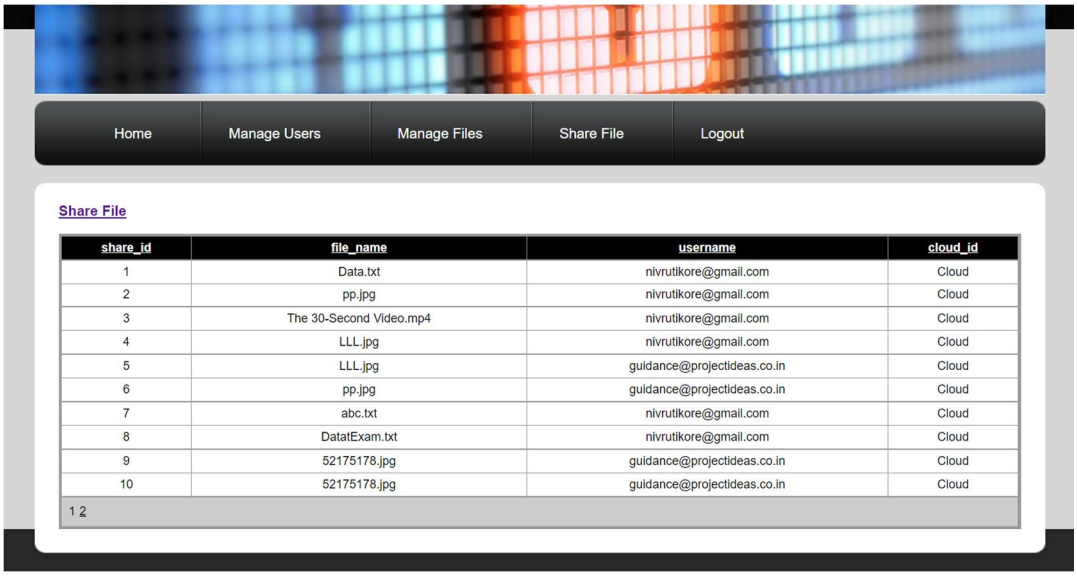
A. Put Screenshots Of Output

1) Admin Login and Sharing Files with User

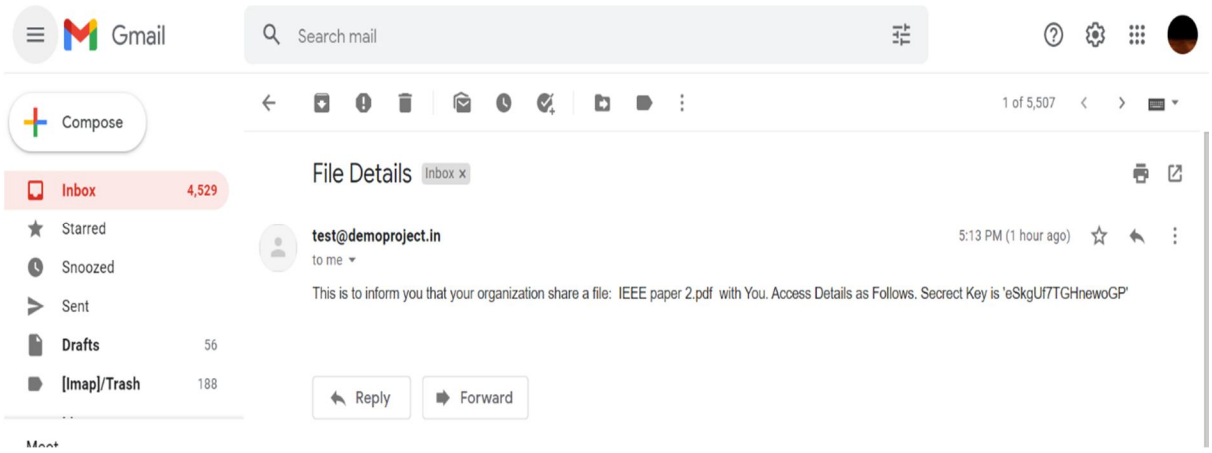


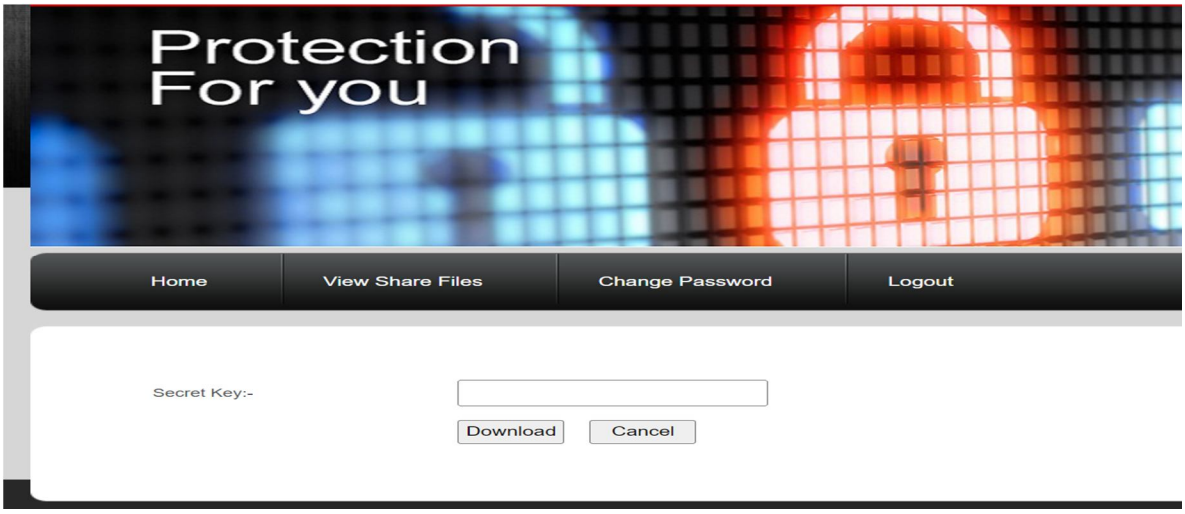


2) Share Files Window



3) User Panel: Secret Key Details





V. CONCLUSION

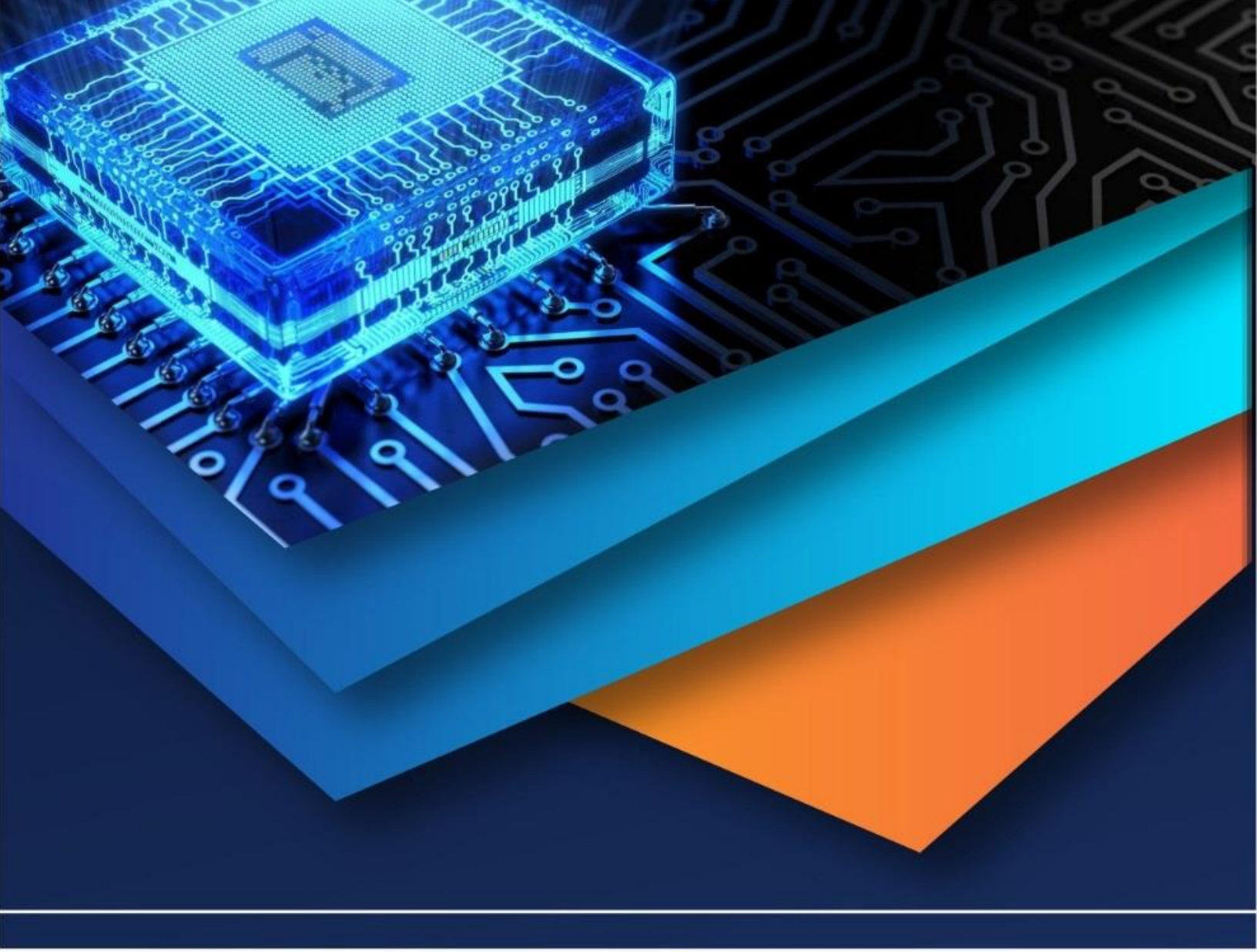
The main aim of the system is to securely store and retrieve data on the cloud that is only controlled by the owner of the data. Cloud storage issues of data security are solved using cryptography. Data security is achieved by using AES and ECC Algorithms. Users are most concerned about data security, so virtualization security and data security are the main problem of the cloud computing security. We concern here data security with Elliptic curve cryptography to provide confidentiality and authentication of data between clouds. The input text file is transformed into encrypted form using AES encryption but the key is generated through ECC (Elliptic curve cryptography). Client will use that key to decrypt the text file which is uploaded to the server in encrypted form to get the original text file. At last analysis of AES encryption with ECC is done on the basis of different parameters like storage requirement, encryption time, decryption time, effect and correlation. Obtained results illustrate that the impact of this hybrid approach is significant and better than other algorithms.

VI. ACKNOWLEDGEMENT

This project work has been most practical and exciting part of my learning experience, which would be assets for future career. No system is created entirely by an individual. Many people have helped to create this system and each of their contribution has been valuable. Proper organization of concept and analysis of the system is due to knee interest and helping hand of my teacher and colleagues. We would like to take this opportunity to thank all of them from the bottom of our hearts. Our deepest gratitude to our guide Prof. Manisha Sonawane, without whose counseling this project wouldn't have been as focused and sound. She showed a keen interest in checking the minute details of the project work and giving valuable suggestions. With technical knowledge there was a need of understanding and moral guidance which was also provided by him. Then Dr. Uttara. Gogate , our H.O.D. under whose direction we could study the project thoroughly. The Honorable Principal, Dr. P.R Rodge who has always encouraged the work of the students and made sure that all necessary resources were available to us. The Professors of our department played an important role in the study by clearing all the doubts that arises. An important piece of the success of this project we owe to the college Head Librarian who helped us sort through the required books. Lastly to all the fellow group members who have worked very hard for the completion, of this project. Also thank you to every individual who has , in some way or another contributed to this project research.

REFERENCES

[1] V.S. Mahalle , A. K. Shahade, "Enhancing the Data Security in Cloud by Implementing Hybrid (Rsa & Aes) Encryption Algorithm", IEEE , INPAC,Oct .2014.
[2] Abu Marjan, Palash Uddin, "Developing Efficient Solution to Information Hiding through text steganography along with cryptography", IEEE, IFOST , October 2014.
[3] P. S. Bhendwade and R. T. Patil, "Steganographic Secure Data Communication" ,IEEE, International Conference on Communication and Signal Processing, April2014.
[4] Tingyuan Nye and Tang Zhang "An investigation of DES and Blowfish encryption algorithm", in Proc. IEEE Region 10 Conference, Jan. 2009.
[5] Achill Buhl, "Rising Security Challenges in Cloud Computing", in Proc. of World Congress on Information and correspondence Technologies , Dec. 2011.
[6] Dr. S.H Patil and Rohini Khalkar, "Data Security Technique In Cloud Storage", International Journal of Computer Engineering and Technology, vol.4,Issue. 2, June 2013.
[7] M. Nagle, D. Nilesh, "The New Cryptography Algorithm with High Throughput", IEEE, ICCCI, January 2014.
[8] Wikipedia: Free Online Encyclopedia; Author – Volunteers around the world and the Wikimedia Foundation; Website Link: https://www.wikipedia.org/
[9] All You Need to Know About Encryption Algorithm : Types and Examples; Author – Noel Cata; Website Link: https://tallyfy.com/encryption/
[10] Microsoft azure cloud: https://azure.microsoft.com/en-in/account



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY