iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** V **Month of publication:** May 2015

DOI:

www.ijraset.com

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

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Multi-Tier Authentication with DIFFIE-HELLMAN Key Exchange Using HMAC and AES Algorithm to Enhance Security in Cloud Computing

Saurin Khedia[1], Nishant Khatri[2]
[1]M.E. Scholar, Dept. of Computer Engineering, [2]Assistant Professor, Dept. of Computer Engineering,
[1,2]Sigma Institute of Engineering, Vadodara, Gujarat, India.

Abstract- Security and privacy in cloud computing is one of the most challenging ongoing research areas because data owner stores their sensitive data to remote servers which is not controlled and managed by data owners. Since cloud computing is rest on internet, various security issues like privacy, data integrity, confidentiality, authentication and trust encounter. We comprehensively survey the various existing hybrid security techniques of cloud computing and compare these combinations with their key features and drawbacks of each. With the increasing demands of a secure cloud, single security technique cannot meet the needs. One tier traditional authentication which is used in most applications relies on username and password for accessing the registered services which is not sufficient to secure from some well known attacks on the system. So we propose a mechanism for secure data transfer which ensures three way protection in terms of authenticity, confidentiality and integrity. This paper focuses on multi-tier authentication which relies on username and password as well as secure pin and one-time password (OTP) with Diffie-Hellman Key Exchange for one time key generation. The technique uses Hash Message Authentication Code (HMAC) signature for data integrity and Advanced Encryption Standard (AES) Algorithm for confidentiality.

Keywords- cloud computing, security, privacy, authentication, confidentiality, data integrity

I. INTRODUCTION

Cloud computing simply means internet computing. Cloud is a computing model that refers to both the applications derived as services over the Internet, the hardware and system software in the datacenters that provide those services. Cloud Computing is a kind of computing technique where IT services are provided by massive low-cost computing units connected by IP networks [1]. This concept also explains the applications that are broaden to be accessible through the Internet. Cloud applications use large datacenters and effective servers that host web applications and services. According to NIST, "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction [2]".

A. Motivation

According to the International Data Corporation (IDC) 2010 survey ranking of Cloud computing security challenges, "Security" ranks as the top concern among Cloud users [3]. Moving to the Cloud presents the enterprise with a number of risks which include securing critical information like the protection of intellectual property, trade secrets, personally identifiable information that could fall into the wrong hands. Making sensitive information available on the internet requires a considerable investment in security controls and monitoring of access to the contents [4].

B. Objectives

The objective is to develop an effective and secure data transfer mechanism for cloud computing system with combination of multi-tier authentication, key exchange algorithm, message integrity and encryption algorithm for confidentiality.

The outline of the paper is as follows:

1) An Overview of Related Works in Section
2) Problem Statement is discussed in Section
3) The Proposed Work is presented in Section
4) Results and Analysis is presented in Section
5) Finally, Conclusion and Future Work is mentioned in Section 6.

II. RELATED WORKS

Review of literature survey has been conducted to study the existing methods dealing with security issues on the Cloud. In this section, we will review some hybrid security techniques as below:

Satish Kumar and Anita Ganpati [3] proposes a scheme in which authentication process is carried out in two levels or two tiers. First tier uses simple username and password on a standard cloud user's interface. Second tier is use of any personal device like mobile which have a unique id and in possession of the authenticated user only. The advantage of this scheme is that it enhances the strength of authentication as if cloud server has to authenticate the standard user password and id as well as the associated device's id and password simultaneously with each other. Problem with this method is that it involves additional hardware which is costly.

V. Sulochana and R. Parimelazhagan [4] presents a puzzle based authentication scheme in which cloud user registers and solves the puzzle, puzzle solving time and sequence of image block is stored and validated by local server and the cloud user get authenticated and start accessing the cloud services. A major drawback of this method is that if attacker once identifies the stored pattern, he could easily break the security.

Prashant Rewagad and Yogita Pawar [5] proposed to make use of digital signature and Diffie Hellman key exchange blended with Advanced Encryption Standard (AES) encryption algorithm to protect confidentiality of data stored in cloud. They proposed a three way mechanism architecture which makes it tough for hackers to crack the security system, thereby protecting data stored in cloud. But this method requires many parameters which makes it heavy enough and also requires a proper key management.

Sarbjeet Singh and Maninder Singh [6] proposed a multi-authentication scheme for cloud security in which authentication process is carried out in two tiers. First tier uses general username and password. Second tier is pre-determined series of steps. The advantage of this scheme is that it does not require any additional hardware and software. So this can be used and accessed from anywhere across the globe. They concluded that the strength of any authentication technique depends upon the probability of breaking that technique.

H.A. Dinesha and V.K. Agrawal [7] presents a technique which authenticates the cloud access in multiple levels. It generates the password and concatenates the generated password at multiple levels. At each level the user has to input password to gain access. Advantage of this technique is that it uses multi-tier approach. It is quite difficult to break multilevel security as compared to single level. Disadvantage of this technique is that it uses passwords at every level but password remembrance is very hectic task for users.

Neha Tirthani and R Ganeshan [8] contemplated a design for cloud architecture which ensures secured movement of data at client and server end. It uses the non breakability of Elliptic Curve Cryptography for data encryption and Diffie Hellman key exchange mechanism for connection establishment. Problem is that it uses a traditional one tier authentication which is vulnerable to security attacks.

Eman M. Mohamed, Hatem S. Abdelkader and Sherif El-Etriby [9] propose a new data security model based on studying of cloud computing architecture. A software is implemented to select the suitable and the highest security encryption algorithm. The proposed model solves cloud user security problems, help cloud provider to select the most suitable encryption algorithm to its cloud. However, this model proves to be costly as it requires additional software.

Uma Somani, Kanika Lakhani and Manish Mundra [10] proposed a concept of digital signature with RSA algorithm, to encrypt the data while transferring it over the network. This technique include both digital signature scheme and public key cryptography to enhance the security of cloud computing and solves the dual problem of authentication and security. The strength of their work is the framework proposed to address security and privacy issue.

III. PROBLEM STATEMENT

Security in the Cloud is now the main challenge in Cloud Computing. Due to lack of understanding and proper application, there

have been lot of speculations for many organizations to use services of Cloud computing as data is stored at any physical location outside their own control. This facility has raised various security questions like privacy, confidentiality, integrity etc. and demanded a trusted environment where data confidentiality can be maintained. Thus, we need to determine the perfect blend of security using different techniques to provide the most efficient authentication, confidentiality and integrity of data over network.

IV. PROPOSED WORK

In the proposed work, the technique has been described through the proposed architecture as shown in Figure 1. A three-tier authentication scheme have been described which relies on username/password as well as Secure PIN and One-Time Password (OTP) for authentication, Diffie-Hellman Key Exchange for one time key generation, Hash Message Authentication Code (HMAC) for data integrity and Advanced Encryption Standard (AES) for confidentiality. After username/password authentication, Diffie-Hellman Key Exchange is used to generate a shared secret key which is used throughout the session for reducing the time in total. As the Man-in-the-middle attack makes the key vulnerable, the concept of Secure PIN makes the system secure. Finally, the OTP is generated by the server and sent to the registered email of the user to complete the authentication process.

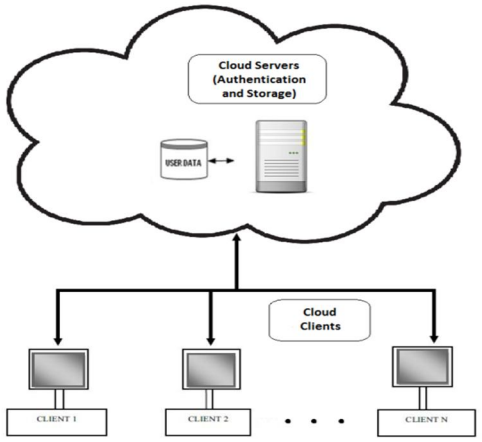


Figure 1: Proposed Architecture

After the three-tier authentication, the user performs the operation of upload/download using HMAC. It encrypts the message using a hash value and provide integrity of data in transit. The server decrypts the message to form an open link between the user and Cloud storage. Now, the user can upload/download a file from Cloud storage in an encrypted form using AES Encryption Algorithm which ensures confidentiality as well. As the Secure PIN generation and validation is managed by the server, there is no need of an additional software or hardware for key management. This results in high security which requires less space and provides fast execution.

Proposed Algorithm is shown in the execution steps as follows:

A. Login
  1) Input Credentials using Username / Password
  2) Key Exchange - Diffie Hellman
  3) Secure PIN Validation
  4) One-Time Password (OTP) via Email

B. Hash Message Authentication Code (HMAC) - SHA 256

C. Uploading / Downloading Data Encryption- AES

D. Data is stored / retrieved from Storage Server

E. Logout

V. RESULTS AND ANALYSIS

Our proposed security technique with three-tier authentication is implemented on Java platform using NetBeans IDE. It uses the Google Drive to store the user's data which is provided by Google Inc. The Google Drive works as a Cloud Storage in the Cloud application development. We have been using Gmail's SMTP Mail Server for delivering the One-Time Password (OTP) on the

Volume 3 Issue V, May 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

registered email of the user. Our application uses the HTTP request and HTTP response with port number 587 to communicate with the SMTP Mail Server of Gmail to deliver the OTP.

A. *Experimental Results*

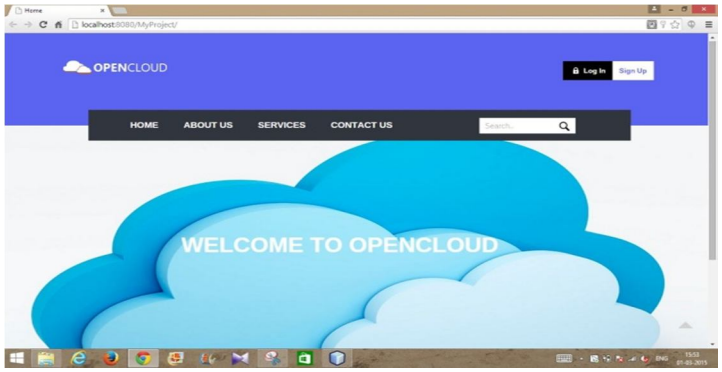


Figure 4.1: Web Application Main Page

Fig. 4.1 shows the page of the Cloud provider's website. The user goes to the URL of the site from the browser.

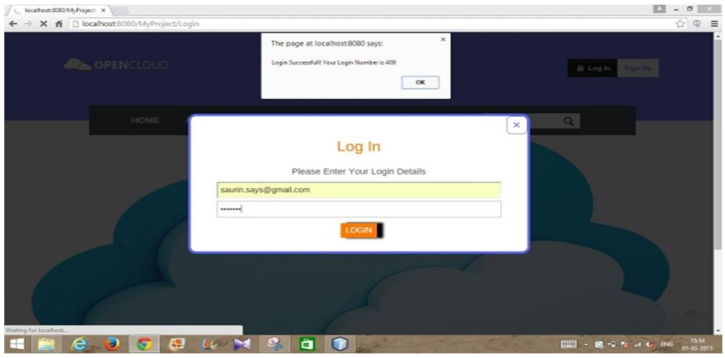


Figure 4.2: Login Credentials - First Tier of Authentication

Fig. 4.2 shows the login page of the website. The user enters his username and password as the first tier of authentication. On Successful Validation, the Cloud server generates a Login Number for the particular user and displays it on validation as shown above.

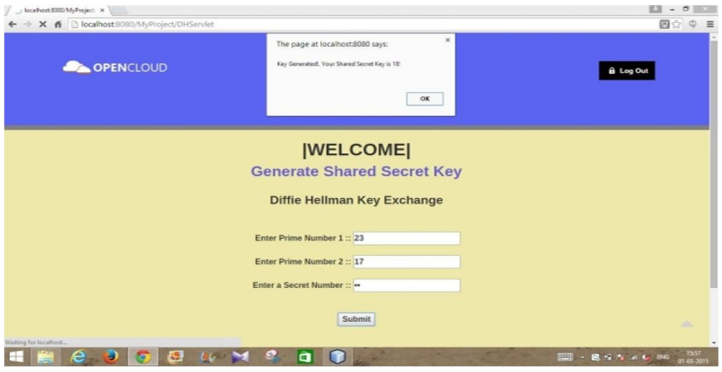


Figure 4.3: Diffie Hellman Key Exchange Process

Volume 3 Issue V, May 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Fig. 4.3 shows the Diffie Hellman Key Exchange Process which is redirected to the user after first authentication. Here, the user will choose the prime numbers and his secret number to generate the shared secret key.

Figure 4.4: Secure PIN - Second Tier of Authentication

Fig. 4.4 shows the Secure PIN page which user enters as second tier of authentication. This PIN is automatically generated by adding the shared secret key and the login number of the user which is maintained by the server. This technique is secret and only known to the user.

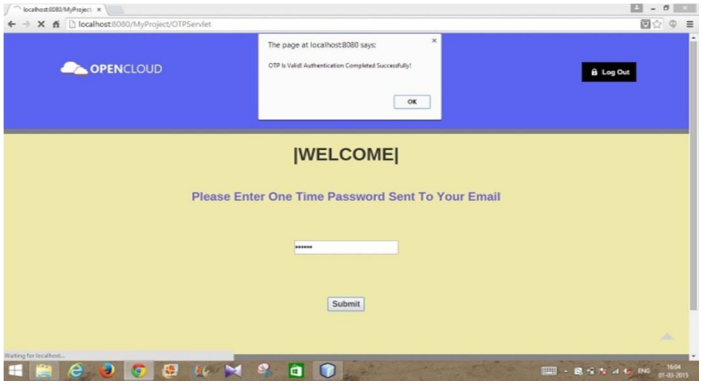


Figure 4.5: One Time Password - Third Tier of Authentication

Fig. 4.5 shows the One-Time Password page which user is redirected to as a part of third-tier authentication. After Secure PIN validation, the server generates a secret code and delivers to the registered email of the user. Finally, user enters the secret code and the authentication gets completed.

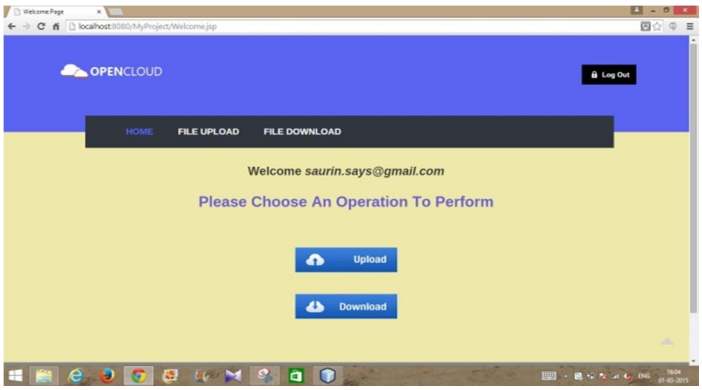


Figure 4.6: User Homepage

Fig. 4.6 shows the User Homepage after the authentication is completed. User selects an operation of upload/download. Hash Message Authentication Code (HMAC) is generated based on the operation of upload/download and the file will be transferred in encrypted form.
HMAC is used to provide data integrity so that an attacker cannot change the date in file transmission.

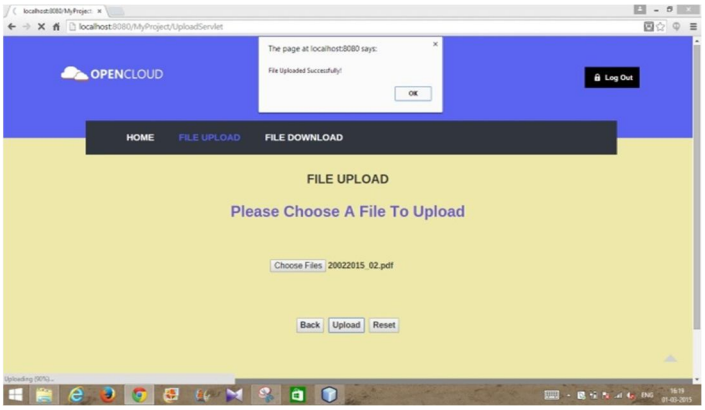


Figure 4.7: File Upload Operation

Fig. 4.7 shows the File Upload operation. User can choose any type of file which he wants to upload on the Cloud storage. The file gets uploaded in an encrypted form using Advanced Encryption Standard (AES) Algorithm.

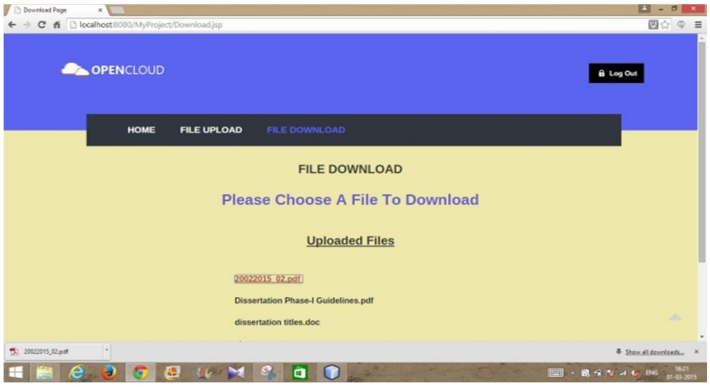


Figure 4.8: File Download Operation

Fig. 4.8 shows the File Download operation. The files which have been uploaded by the user gets enlisted on this page. User can click on the file which he wants to download.
After completing the operation of upload/download, the user can log out from the system which would terminate the connection.

B. Security Analysis

The proposed security technique uses three-tier authentication stages. First stage is used to verify using username and password, second stage authorizes the user using Secure Pin and the third and final stage authenticates the user with the One-Time Password by Email.
Let Success (S) and Failure (F) be the two possibilities of the authentication stages in the proposed security technique.
So, the possibilities of the three-tier authentication stages are SSS, FSS, SFS, SSF, FFS, SFF, FSF, FFF and N (T) = 8 for our proposed system, where T = total number of possibilities.
Now, let p = Probability of Success for accessing the system at each authentication tier. So, for breaking the whole authentication system, i.e. SSS, is denoted by P (E) where P (E) = p^3 for three-tier authentication and failure for breaking the system is 1 - P (E) = 1 - p^3.

Now, say p = 0.5, then p^2 = 0.25 and p^3 = 0.125 which means the probability of success for breaking the whole system is very less, near to zero, compared to the one-tier authentication or two-tier authentication of the existing system.

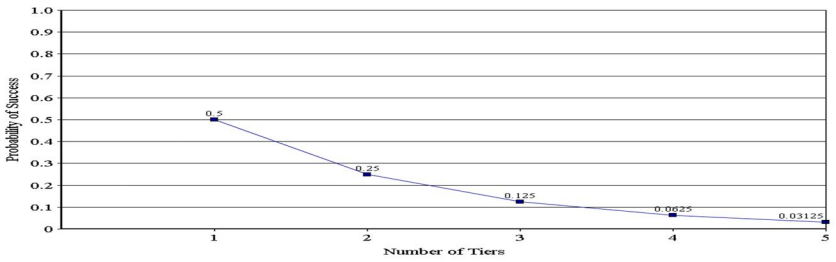


Figure 5.10: Probability of Success for Breaking the Authentication Tiers of the System

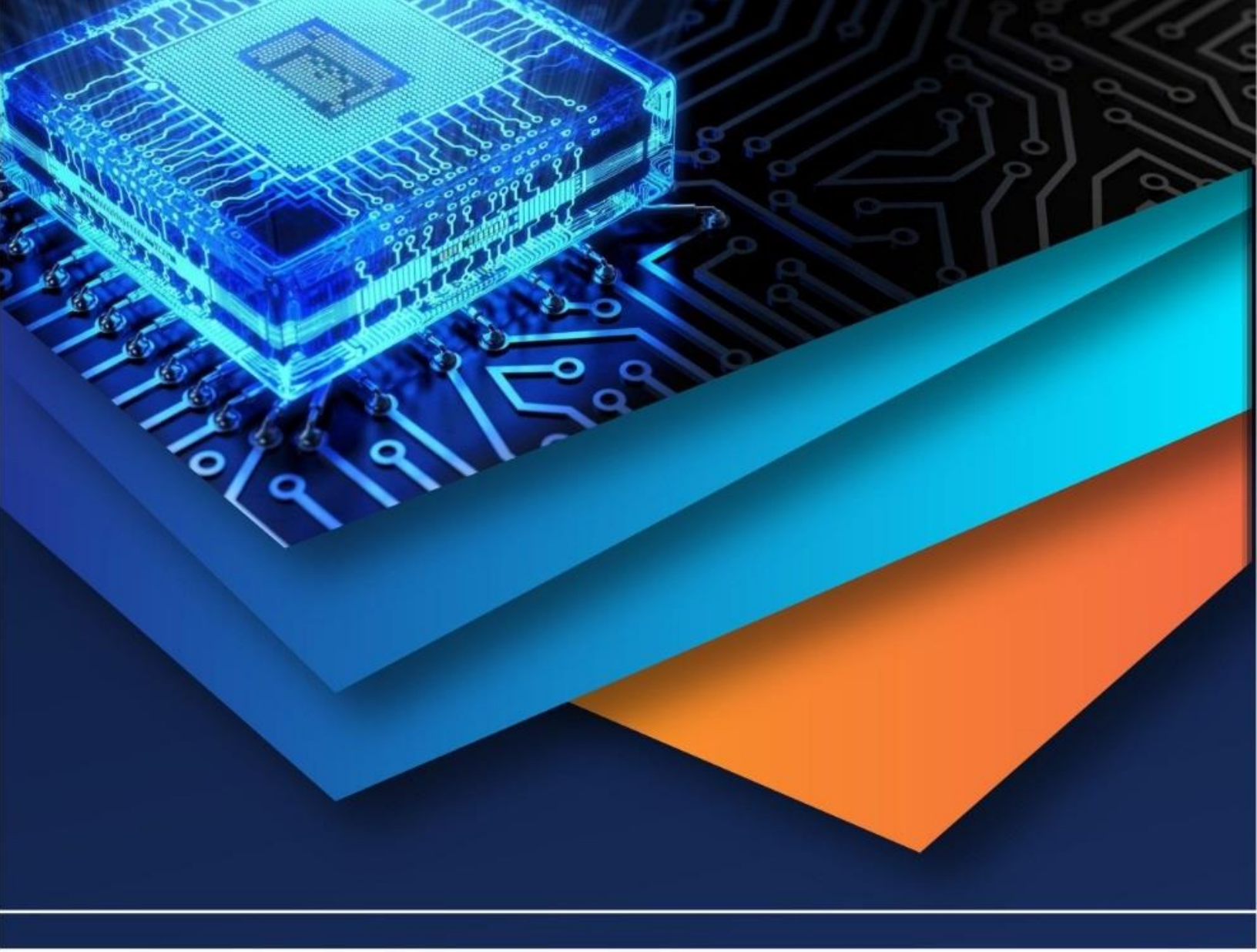
The strength of the whole three-tier authentication depends on the password chosen by the user at registration and the secure pin as well as one-time password generated by the Cloud server. It is also indirectly proportional to the probability of success for breaking the three- tier authentication of the system which means higher the strength of the system, lesser the probability of success for breaking it.

VI. CONCLUSION AND FUTURE ENHANCEMENT

In this paper, a mechanism for secure data transfer has been proposed which ensures three way protection in terms of authenticity, confidentiality and integrity. The main focus is on three-tier authentication which uses Diffie-Hellman Key Exchange algorithm for one time key generation, HMAC for data integrity and AES Encryption algorithm for confidentiality. In our proposed scheme, the core strength is in providing single sign-on access to Cloud services and the probability of success for breaking the authentication tiers of the security system which is near to zero. In Future, It is also foreseen to perform real test by deploying the system application on Amazon Cloud.

REFERENCES

[1]Ling Qian, Zhiguo Luo, Yujian Du and Leitao Guo, “Cloud Computing: An Overview”, Springer-Verlag Berlin Heidelberg CloudCom, LNCS 5931, pp. 626-631, 2009.
[2] Peter Mell and Timothy Grance, “The NIST Definition of Cloud Computing”, National Institute of Standards and Technology Special Publication 800-145, 2011.
[3] F. A. Oyegoke, "Security Challenges of Cloud Computing for Enterprise Usage and Adoption," IOSR Journal of Computer Engineering, Vol. 16, Issue 5, pp. 57-61, Oct 2014.
[4] H. Tianfield, "Security Issues in Cloud Computing," IEEE International Conference on Systems, Man and Cybernetics, pp. 1082-1089, Oct 2012.
[5] Satish Kumar and Anita Ganpati, “Multi-Authentication for Cloud Security: A Framework," International Journal of Computer Science & Engineering Technology (IJCSET), Vol. 5, Issue 4, pp. 295-303, Apr. 2014.
[6] V. Sulochana and R. Parimelazhagan, “A Puzzle Based Authentication Scheme for Cloud Computing,” International Journal of Computer Trends and Technology (IJCTT), Vol. 6, Issue 4, pp. 210-213, Dec. 2013.
[7] Prashant Rewagad and Yogita Pawar, “Use of Digital Signature with Diffie Hellman Key Exchange andAES Encryption Algorithm to Enhance Data Security in Cloud Computing,” IEEE International Conference on Communication Systems and Network Technologies (CSNT), pp. 437-439, 2013.
[8] Sarbjeet Singh and Maninder Singh, “Design and Implementation of Multi-tier Authentication Scheme in Cloud," International Journal of Computer Science Issues (IJCSI), Vol. 9, Issue 5, pp. 181-187, Sep. 2012.
[9] H.A. Dinesha and V.K. Agrawal, “Multi-level Authentication Technique for Accessing Cloud Services," IEEE International Conference on Computing, Communication and Applications (ICCCA), pp. 1-4, 2012.
[10] Neha Tirthani and R. Ganeshan, “Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography," International Association for Cryptologic Research (IACR), ePrint archive, 2014.
[11] Eman M. Mohamed, Hatem S. Abdelkader and Sherif el-etriby, “Enhanced Data Security Model for Cloud Computing,” IEEE 8th International Conference on Informatics and Systems (INFOS2012), pp. CC12-CC17, 2012.
[12] Uma Somani, Kanika Lakhani and Manish Mundra, “Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing”, IEEE 1st International Conference on Parallel, Distributed and Grid Computing (PDGC2010), pp. 211- 216, 2010.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY