iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 4 **Issue:** X **Month of publication:** October 2016

DOI:

www.ijraset.com

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

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

A Trusted Framework for Authentication and Security for Business Applications in Cloud

Marina. Naveena[1], B.Veerendra[2]
[1]PG Scholar, [2]Assistant Professor,
Department of CSE, Kakinada Institute of Technology & Science, Divili (Tirupathi), India

Abstract: ***Cloud stands for Common Location independent Online Utility on Demand services (or) Communities Libraries Online Union Database which is abbreviated from AT&T (American Telephone & Telegraph) corporation. Now a day's cloud computing is one of the prominent technology to provide wide variety of services such as Software-as-a-Service, Infrastructure-as-a-Service, Platform-as-a-Service, Data-as-a-Service and Voice-as-a-Service etc. Cloud computing is a new innovated technology which provides various capabilities to the users on demand basis. In cloud computing data storage is one of the popular services which stores data at remote servers and reduces storage cost at client side. Apart from the benefits cloud also lagging in providing authentication, security, integrity, availability to the user's data due to data is not under control of end user. In this paper, proposed an efficient multifactor authentication algorithm for authentication and set of encryption algorithms for secure storage of data in the cloud. The encrypted algorithms are chosen by the end user for encrypting the data and provided comparison of encryption algorithms according to time factor***
Keyword: cloud, Multifactor Authentication, Encryption, Integrity, Availability, Security, Time factor.

I. INTRODUCTION

Cloud computing [1] offers an important service data storage as a service. The main benefit of using cloud computing is to reduce the installation cost of hardware, software applications, complex computations at client side. All the cloud services are maintained by the cloud providers at remote centers and services are provided to the end users with a simple web browser through the internet connection. Using cloud computing small industries are getting more beneficial to their companies. Cloud computing provides more benefits to the users but still users have some consideration and worrying about their data which is stored at cloud because whatever data is stored at cloud not under control of users .All the security mechanisms are provided by the cloud providers only. The security of the data which is stored at cloud is maintained by the cloud provider or cloud user is based on the type of application choose by the user. Different Companies providing cloud services like Amazon, Google, Azure cloud etc. The main requirement of providing security to the cloud data is done by providing proper authentication , confidentiality and integrity[2] .Whenever cloud users believes all these services are maintained by the cloud provider then successfully uploads their data in to cloud. In this paper, proposed an efficient multifactor authentication mechanism .Once authentication is successful completed then encrypts the files by the user then uploads data in to cloud. Encrypting of file is required because cloud provider also not a trusted entity. Cryptography [3] is the art of providing security to the data through encryption, authentication mechanism. Data security is a service which provides accessing of the data is possible only authorized users in secure way. Authentication of users in cloud is possible by various authentication algorithms like DSA, ELGAMAL etc and confidentiality of the data is possible by using encryption algorithms. Encryption is the mechanism which converts plain text in to cipher text and decryption is the process which converts cipher text in to plaintext. Encryption algorithms are divided in to symmetric and Asymmetric encryption algorithms. In symmetric only one key is used in both encryption and decryption and in Asymmetric two keys are used .The work in this paper is divided in two stages. 1) Multi factor Authentication 2) Encryption. Multifactor authentication is done by considering multiple factors like user name, password, and color value. Encryption is the process of converting the plain text in to cipher text and vice versa. In this followed AES, Blowfish, DES, recursive key generation encryption algorithms for storing sensitive information in cloud.

The Paper is organized as follows. Section II Related work describes proposed Multi Factor Authentication. Section, III Proposed Algorithm IV presents experimental results. Finally, Section V presents conclusion.

II. RELATED WORK

MazharAli [4] proposed security in cloud computing: opportunities and challenges. In this, discussed the main services of cloud like

infrastructure as a service, software as a service and platform as a service. The author also identified the various security challenges occurred at cloud computing.

GurpreetSinghetal [4] proposed A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security. In this they discussed the procedure of various encryption algorithms like DES, AES, RSA etc.

Encryption [2] is process which converts plain text in to cipher text base on key value. At the receiver side the cipher text is decrypted in to plain text by using the same key value.

A. DES

DES is a symmetric encryption algorithm with 56 bit key size. The process of DES is based on the festal structure .The DES is based on the set of substitutions and permutations. According to surrey DES having some weak keys. Next replacement is triple DES which DES is executed three times with multiple keys which improves the key length.

B. AES

AES is a symmetric block cipher algorithm which takes the key size as 128 bit or 192 or 256 bit. Based on the key size the number of rounds also varied . Most cloud provider's uses AES -128 encryption algorithm for storing sensitive data in encrypted form in to cloud. From the AES provides better security with good resistance

C. BLOWFISH

Blow fish is a symmetric encryption algorithm which is divided in to two parts.1.Key expansion and 2.Data Expansion. The Blowfish uses large number of sub keys and these keys are precompiled before data encryption. The data encryption which converts plain text in to cipher text with function which iterates 16 times. Blow fish design supports fast, simple compact execution

D. Recursive Key Geneartion

Srikanth swamy [5] proposed recursive key generation process in this the key generation process is unique .For each character, the key values is double recursively. This procedure is simple and executed easily in any platform.

III. PROPOSED ALGORTIH

The proposed scheme provides multi factor authentication and encrypting user data with different algorithms according to user choice.

A. MULTI FACTOR AUTHENTICATION

Authentication is a mechanism which verifies users are authorized or not to access the resources. The basic authentication mechanism is login and password. It is two factor authentication mechanisim.In our proposed system, we consider multiple factors for authentication username, password and color value for authenticating user. The authentication process is done in two phases.1.registration phase and2.login phase. In registration the user is registered with business server by providing the personal details, username, password, color .Once the registration completed login to the application by entering valid login details. The password and color information is stored in the database in hash format. Here, MD5 hash function is applied to convert password and color information into hash format which 32 digit.MD5 is a hash function which converts variable length text in to fixed 128 bit value. The proposed method provides strong security with the help of color variable. Color is a value which is having the key space of [255,255,255] of RGB values.

Generally user credentials are stored in cloud server and authentication is also done by cloud the server. In our frame work, the user credentials are stored in business server in hash format and encrypted format for some sensitive values and verification is done by cloud server without storing credentials at cloud server. Assume that business server is protected in a high secure way by the organisation. The major components included in this framework is Authentication server, Preserving Privacy .To describe our approach, first user registered with business server by providing personal details, colour information generated by the client side .Once registration is successfully completed the password along color value is stored in hash format. Here colour is considered as secret key.

To describe our approach, we defined some terminologies for registered values and login input values.

A. Registered password is pwd, and password provided at login time pwd*.

Volume 4 Issue X, October 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

B. User selected color at registration time is color_value

C. Password and color information is stored in the database in MD5 hash format.

MD5 is hash algorithm which converts any arbitrary text in to 128 bit value. The objective of hashing algorithms is to provide integrity for data. The hashing algorithms having one important property, i.e. getting original information from the hash value is not possible. In our algorithm we have stored the password in hash format by using MD5 because even the data is hacked by the intruder it is impossible to recover the original data.

IV. EXPERIMENTAL RESULTS

We implemented our results in Net beans IDE, using java awt, javax.swings, crypto api.java.crypto is an api which provides different classes for implementing encryption and hashing algorithms. The evaluated results are shown below.

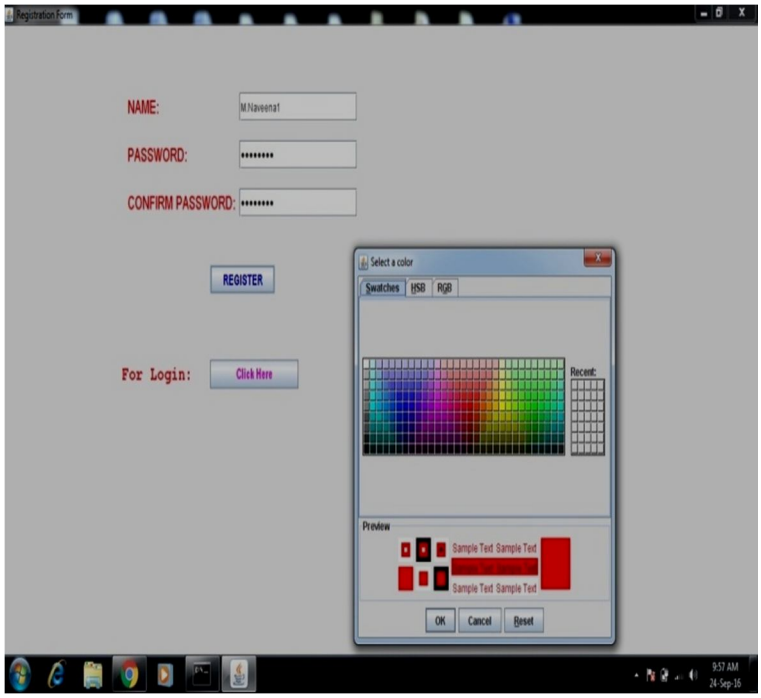


Fig 1: Registration Page

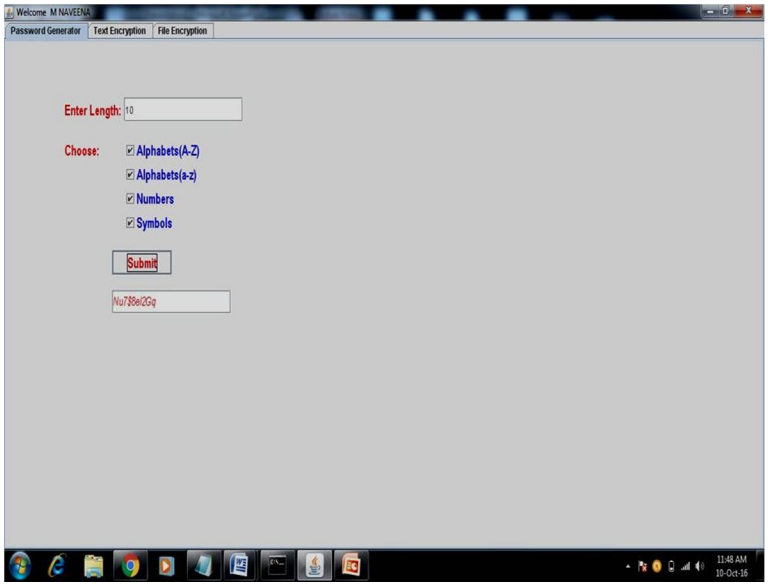


Fig 2: Random password generator

Volume 4 Issue X, October 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

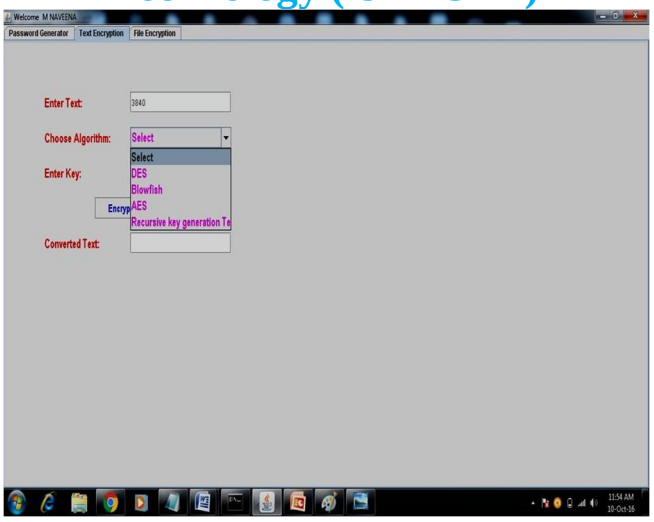


Fig: 3Text Encryption process

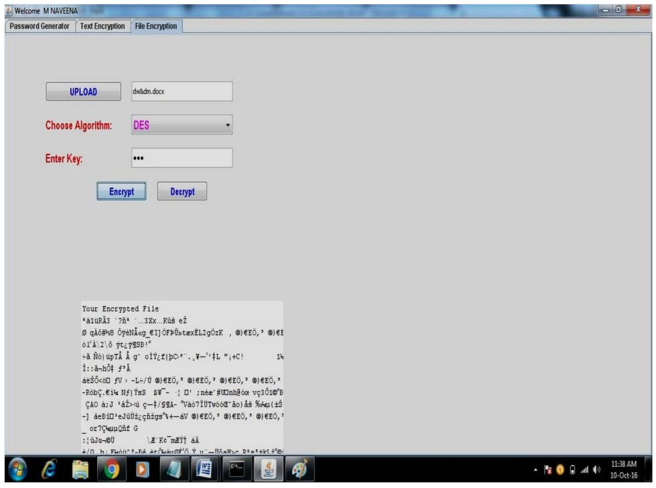


Fig: 4 Uploading File Encryption process

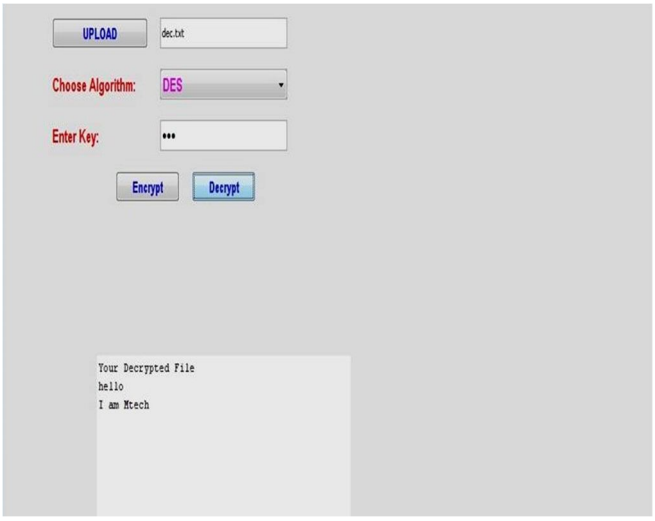


Fig: 5 Decryption process

V. CONCLUSION

In this paper, we implemented multifactor authentication with less computation by considering id, password and color values as

multifactor's which provides strong security compare to traditional authentication. We also implemented multiple encryption algorithms for encrypting messages and files. The choice of encryption algorithm is done by the user .We also created a simple password generator with random class. All these services provide better security to the data which is stored in the cloud. The evaluated results show our frame work is combination of multiple services.

REFERENCES

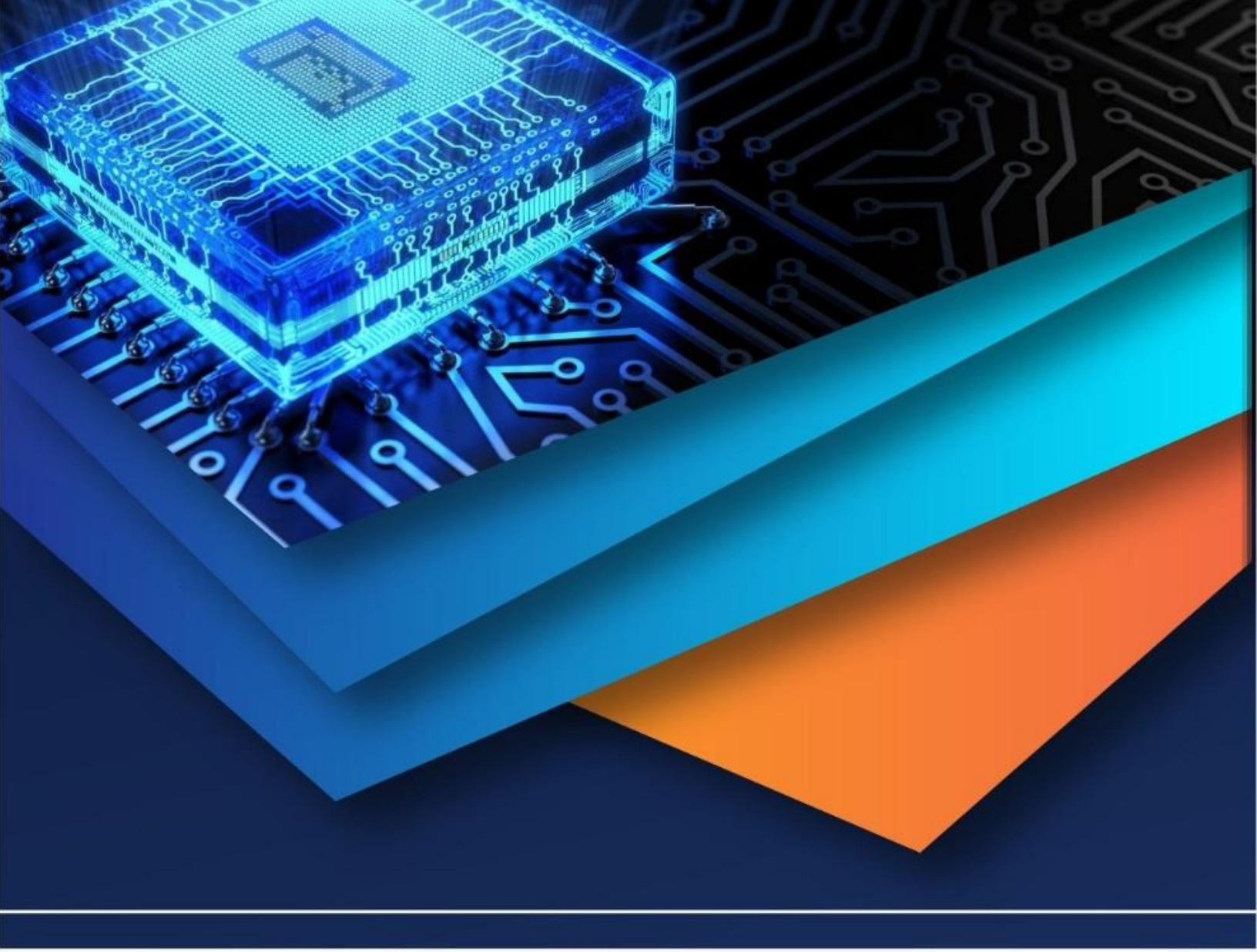
[1] Mazhar Ali , Samee U. Khan a, Athanasios V. VasilakosP. Security in cloud computing: Opportunities and challenges Information Sciences.
[2] Chang Liu ∗, Chi Yang, Xuyun Zhang, Jinjun Chen External integrity verification for outsourced big data in cloud and IOT: A big picture Future Generation Computer Systems
[3] Gurpreet Singh,Supriya A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security International Journal of Computer Applications (0975 – 8887) Volume 67– No.19, April 2013
[4] S.G.Srikantaswamy, H.D.Phaneendra.: A Cryptosystem Design with Recursive Key Generation Techniques: Procedia Engineering, International Conference on Communication Technology and System Design 2011.
[5] Cryptography and network security by William stallings
[6] Kevin hamlen,murat kantarcioglu,latifur khan,bhavani thuraisingham. Security Issues for Cloud Computing. International Journal of Information Security and Privacy, 4(2), 39-51, April-June 2010 39
[7] Er.Ashima Pansotra,Er.simar Preet singh" Cloud Security Algorithms" International Journal of Security and Its Applications Vol.9,No.10(2015),pp.353-360 http://dx.doi.org/10.14257/ijsia.2015.9.10.32
[8] Jawahar Thakur, Nagesh Kumar, AES, DES, .Blowfish: Symmetric key algorithm Simulation based performance analysis", ,International Journal of Emerging Technology and Advanced Engineering ,Volume 1, Issue 2, pp 6-12, ISSN 2250-2459, December 2011.
[9] Jing-Jang Hwang and Hung-Kai Chuang, Yi-Chang Hsu and ChienHsing Wu, "A Business Model for Cloud Computing Based on a Separate Encryption and Decryption Service", IEEE Conference on Information Science and Applications (ICISA), April 2011.

AUTHOR'S BIOGRAPHIES

Miss. M.Naveena is a student of Kakinada Institute of Technology & Science, Divili (Tirupathi). Presently she is pursuing M.Tech [CSE] from this college, she is received B.Tech degree from Kakinada Institute of Technology & Science, Divili (Tirupathi), Affiliated to JNTU Kakinada University in the year 2014. Her area of interest includes Cloud Computing, Web Technologies, Cryptography and Network Security, current trends and technologies in Computer Science.

Mr. B.Veerendra is received B.Tech, CSE from Abdul Kalam Institute of Technological Sciences, JNTUH, Hyderabad and M.Tech, CSE from Kakinada Institute of Technology & Science, Divili (Tirupathi), Affiliated to JNTU Kakinada University, and working as Assistant Professor in Kakinada Institute of Technology & Science, Divili (Tirupathi), Andhra Pradesh, India. His area of Interest includes Cloud Computing, Data Warehousing and Data Mining, Cryptography and network security etc.

.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY