iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** V **Month of publication:** May 2018

DOI: http://doi.org/10.22214/ijraset.2018.5151

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: 6.887
Volume 6 Issue V, May 2018- Available at www.ijraset.com

Security of User Credential on Cloud Computing

Deepak Soni[1], B V Parveen[2], Atul Katiyar[3], Dr. Ashish Chopra[4], Deepika Saxena[5]
[4,5]*Asst. Professor,* [1, 2, 3, 4, 5]*Dept. of Computer Application, National Institute of Technology, Kurukshetra, Haryana, India*

Abstract: ***This survey paper is about security of the information in cloud computing which is the thought realized to cure the Daily Computing Problems. Cloud computing is on a very basic level virtual pool of benefits and it gives these resources for customers by methods for web. It offers an extent of organizations for end customers; among which there's capacity as an organization. As of late, Storage in Cloud picked up ubiquity among the two organizations and private clients. Nevertheless, information protection, security, unwavering quality and interoperability issues still must be enough settled. There ought to be essential, secure, and insurance protecting designing for inter cloud data sharing. Security of information can be offered by methods for cryptography. Many such algorithms of cryptography are discussed which can convert the plain text into cipher text before storing it onto to the cloud, so that the data can be secured.***
Keywords: Cloud Computing, Data security, Plain text, Cipher text, Encryption, Decryption.

I. INTRODUCTION

There is no such thing as “THE CLOUD”, it’s just somebody else’s computer. Distributed computing is otherwise called on-request registering and it is a kind of online handling, where shared resources and information are given to PCs and diverse devices on-request.

Distributed computing is basically planned to give the most extraordinary breaking point from minimum assets. The end customer has the base hardware need yet uses the most extraordinary limit of preparing.

Recently service of cloud computing that is storage as a service (STAAS) has become popular about providing services to both private users and public users. STAAS is a Cloud model in which a special organization rents space in its storage framework to people or organizations.

The data stored on the cloud can be exploited by the service provider or other unauthorised person thus data stored on the cloud is sensitive and needs a security. This weakness has motivated us to find some solution that will enable the user to secure their data on the cloud.

There are various research challenges in cloud computing such as mobility, interoperability, storage access, security, cost, energy efficiency etc. But security is one of the major obstacle which limits the spread of cloud computing.

This archive speaks to as takes after: right off the bat it gives the definition and attributes of distributed computing. Besides, it portrays administrations of distributed computing and their advances identified with this idea. Thirdly, it depicts the diverse kinds of cloud and their qualities. Fourthly, it portrays the distinctive sort of encryption calculations which can be utilized as a part of securing that information on the cloud.

A. About Cloud Computing

Cloud computing is a model for empowering helpful, on-request organize access to a common pool of configurable processing resources(example systems, servers, stockpiling, applications and administrations) that can be quickly provisioned and discharged with insignificant administration exertion.

Cloud computing generally referred to as the delivery of demands. It is a kind of computing in which computing resources that is everything from applications to data centres are asked over the internet on a pay for use basis.

B. Characteristics

1) *On demand Service:* A consumer without requiring a interaction with each service provider can provision computer capabilities, such as server time and network storage.
2) *Broad Network Access:* Abilities are accessible over the network and got to through standard components that promote use by different thin or thick client stages (e.g., cell phones, tablets, laptops and workstations).
3) *Resource Pooling:* The supplier's figuring resources are pooled to serve various buyers utilizing a multi-inhabitant display, with different physical and virtual assets powerfully relegated and reassigned according to consumer demand. Examples of resources include storage, processing, memory, and network bandwidth.

4) *Rapid Elasticity:* Capabilities can be flexibly provisioned and released, sometimes consequently, proportional quickly outward and inner comparative with request.

C. Services of Cloud Computing

1) *Software as a Service (SAAS):* This service explains that the user doesn't really have to worry about any particular software installation; it means the client can use desired software without installing it on its own system. This layer includes applications that run off the cloud. They are paid for on a per-use basis, anytime anywhere basis. These applications are available on demand to web.
2) *Storage as a Service (STAAS):* It is a service which provides cyber storage or online remote storage, which is independent of client system and its platform. It felicitates cloud applications to a scale beyond their limited servers. There are two types of remote storage
3) *Object Storage:* This is a kind of storage where client only can store data like docs, pdf, text, movies etc
4) *Block Storage:* Type of storage which provides raw storage over network. This is the method where we can share real block storage over network using real time operating system.
5) *Infrastructure as a service (IAAS):* It provides virtualized computing resources over the internet. It is a service model that delivers computer infrastructure on an outsourced premise to help enterprise operations. In this model, a third party provider hosts hardware, software, servers, storage and other infrastructure components on behalf of its users. IaaS suppliers likewise have client, applications and handle tasks including system maintenance, backup and resiliency planning.
6) *Platform as a service (PaaS):* It is a model in which service provider provides or delivers hardware and software tools, which are needed by the user for any software development over the internet.
   It is service where in integrated environment for development is provided. Example: service for java or service for c language is configured accordingly like the required software's and editor is installed and is made available to user.

D. Applicatons of Cloud Computing

There are a few applications of cloud computing as follows:

1) Cloud computing provides dependable and secure data storage centre.
2) Cloud computing can realize data sharing between different equipments.
3) The cloud provides nearly infinite possibility for users to use the internet.
4) Cloud computing does not need high quality equipment for the user and it is easy to use.

II. RELATED WORK

Security of storage in cloud computing is the objective of several issues.

Zaid kartit et. al. [1], it is proposed for Applying Encryption Algorithm to Enhance Data Security in Cloud Storage. basic, secure, and protection saving design for bury Cloud information sharing. This engineering depends on an encryption/decoding calculation which means to ensure the information put away in the cloud from the unapproved get to. There are two sections in there calculation. The first is the record transfer part in which, the calculation scrambles Clair content with AES Algorithm. In second part which is called record download this calculation got additionally two stages. In the primary stage, the calculation decodes AES key utilizing RSA Algorithm. In the second stage, it unscrambles figure content utilizing AES key recovered from the server. Their calculation is intense in light of the fact that the uprightness and classification of the information transferred by the client is guaranteed doubly once by utilizing AES calculation and again the AES key is scrambled utilizing RSA calculation. The AES calculation is more secure and less helpless to cryptanalysis. AES has 128 piece square size which makes it less open to attacks.AES is speedier in both equipment and programming and afterward promote that AES key is scrambled utilizing RSA calculation is essentially an uneven encryption/unscrambling calculation. Open key disseminated to all through which one can encode the message and private key which is utilized for unscrambling is kept mystery and isn't shared to everybody. It in light of exponentiation in a limited field over whole numbers modulo a prime numbers. In this calculation, Only the approved client can get to the information. Regardless of whether a gatecrasher (unapproved client) gets the information unintentionally or purposefully, he can't decode it and requirements two keys originating from two unique areas.

Suruchee V.Nandgaonkar et. al. [2] gave "A Comprehensive Study on Cloud Computing" which describes that cloud computing is becoming an increasingly popular enterprise in which computing resources are made available on-demand. It defines the architecture that is all the services of the cloud." They have defined cloud computing and have described that cloud computing is

becoming one next IT industry Buzz. The unique value proposition of cloud computing creates new opportunities to align IT and business goals. Cloud computing use the internet technologies for delivery of IT-Enabled capabilities 'as a service' to any needed users i.e. through cloud computing we can access anything that we want from anywhere to any computer without worrying about anything like about their storage, cost, management and so on. In this paper they provide a comprehensive study on the motivation factors of adopting cloud computing, review the several cloud deployment and service models. It also explore certain benefits of cloud computing over traditional IT service environment-including scalability, flexibility, reduced capital and higher resource utilization are considered as adoption reasons for cloud computing environment. They also include security, privacy, and internet dependency and availability as avoidance issues. The later includes vertical scalability as technical challenge in cloud environment. They have explained the cloud Architecture, cloud service models (IaaS,PaaS,SaaS). They have compared these different cloud service models. They have explained the motivating factors and challenges related to cloud computing. They have explained that Cloud computing have several benefits over traditional (non- cloud) environment and have capability to handle most sudden, temporary peaks in application demand on cloud infrastructures.

K.Prasanthi et. al. [3] they gave "the cutting edge symbol of juleus ceaser" by presenting a prime whole number , its crude roots and the generators. What's more, the movements of characters will shift as indicated by it. Caesar utilized a move of 3 to decide the figure content. Ci=(Mi + 3) mod 26 .In the proposed calculation the movements change, as indicated by decision of the prime whole number, its crude root and the generators. From that arbitrarily chose prime no. All the crude underlying foundations of that number are created and from those roots one irregular root is chosen and its generators are registered. They have characterized a table which demonstrates discrete logarithm of a no to the base of haphazardly picked crude root, they will locate the key 'k'. As per this the estimations of the movements are differed. This was the over all procedure of encryption. In the unscrambling procedure Mi= (Ci-Ki) mod26. Here Ki is the k which was ascertained previously. They have ended up being more grounded by clarifying that If the message is longer, say of 500 or 900 characters, at that point picked a prime esteem will resemble 503 or 907 or above. So relying on the length of the message a suitable prime esteem can be picked. From there on it is a significant errand to decide all their crude roots or base esteems, and register their generators. Deciding the prime factor and the crude root utilized for deciding the discrete logarithm esteems is extremely troublesome. The interceptor needs to experiment with all the prime elements, and afterward work with their discrete logarithm esteems. The quality of this proposed calculation is in picking the prime factor and its significant crude root.

Aditi Saraswat et. al. [4] they have proposed "an extended hybridization of vigenere and ceaser cipher techniques for secure communication". They have proposed a algorithm which combines vigenere and ceaser cipher encryption techniques for encryption and decryption. The algorithm uses a modified vigenere table with alphanumeric cross section. Here the alphabets (A-Z) ranges from values 0-25 and the digits (0-9) ranges from 26-35 are appended after the alphabets. The first row represents the key character and the first column represents the plaintext character. For Encryption the intersection of key character and plain text character gives an intersection character in which 3 is added to get the cipher character. They have been able to include digits in the plaintext which will reduce the length of the plain text and the key used. Another advantage is that the complexity of the encrypting process will also increase as the possible number of replacement for each alphabet or digit will also increase by ten. This paper incorporates the various cipher techniques available. It majorly focuses on the poly alphabetic cipher techniques and the vigenere table. In this paper they have extended the vigenere table by including the digits in the table so that numerical data can also be encrypted using the new proposed table. It also reduces the size of the plaintext, in case numbers are present in the plain text and also make cryptanalysis a difficult task. The proposed algorithm fails for the special characters in the Modified Vigenere table as the table only contains alphanumeric key and text axis. Because of this the cryptanalysis process will become easier. Since simple Caesar cipher is used it will be easier to analyze the code.

Zhibin Chen et. Al. [5] proposed a report in which they have defined cloud computing and have described all the service models of cloud computing further they have described all the deployment models of cloud computing that is public cloud, private cloud ,hybrid cloud, community cloud. They have explained issues related to cloud computing which are security of data in the cloud, Privacy of users data which is sometimes compromised in cloud computing because the user's personal data is scattered in various data centres. Reliability The cloud servers also experience downtimes and slowdowns there is no reliability, Legal issues, Compliance, Freedom etc. They have concluded the paper by describing that Cloud computing brings us the approximately infinite computing capability, good scalability, service on-demand and so on, also challenges at security, privacy, legal issues and so on and they have focused on defining that beside the fact that the coming cloud computing is becoming a great era, there are still existing issues related cloud computing which are serious issues and they are required to be solved.

Anuradha Thilakarathne et. Al. [6] describes "different existing security threats and attacks on cloud like VM escaping and VM monitoring, Zombies in the cloud, Flooding attacks etc. "They have addressed the security issues associated in cloud data storage and have explored many of them such as security, privacy, reliability, legal issues, open standards, compliance, freedom and long term viability." They have defined different security issues, the different existing security threats and attacks. They have explained Cloud Security has inevitably become a significant business differentiator. There are certain things which in cloud we need to focus on which have explained above. In conclusion to this there should be security to the data which is stored in the cloud. There are certain encryption algorithms which can be used to encrypt that data to secure it by malicious attacks. Techniques of encryption are further presented in modified forms."

III. COMPARATIVE STUDY

S.NO	Title	Year	Comparison
1	Applying Encryption Algorithm to Enhance Data Security in Cloud Storage	2015	It depends on an encryption/decoding algo which intends to ensure the information put away in the cloud from the unapproved get to. To improve security; AES key will be increpted using RSA calculation and will be put away in understudy server.
2	A Comprehensive Study on Cloud Computing	2014	cloud computing is becoming an increasingly popular enterprise in which computing resources are made available on-demand.
3	A Modern Avatar of Julius Ceasar and Vigenere Cipher	2013	The advanced symbol of juleus ceaser" by presenting a prime whole number , its crude roots and the generators.
4	Security Challenges Of Cloud Computing	2014	They have addressed the security issues associated in cloud data storage and have explored many of them such as security, privacy, reliability, legal issues, open standards, compliance, freedom and long term viability." They have defined different security issues , the different existing security threats and attacks
5	Cloud Computing Research and Security Issues	2010	They have defined distributed computing and have described all the administration models of distributed computing further they have portrayed all the organization models of distributed computing. They have disclosed issues related to cloud computing.
6	An Extended Hybridization of Vigenere and Caesar Cipher Techniques for Secure Communication.	2016	Includes 0 to 9 digits in vigenere table and called it modified vigenere table, to make the encryption process more complex.

IV. PROPOSED WORK

As cloud computing provides storage to the user and that storage is available to the user and the to the provider the privacy of the users data is compromised. For this data security is very important . until now we have discussed all the issued related to cloud computing and the techniques by which integrity and consistency of the data can be maintained. Our main focus is to provide security to the data and encrypt the txt file(plain text) before storing it onto the cloud which is called file uploading. For data decryption the file should be downloaded. In Zaid kartit et. al. [8], they have explained the issue related to cloud computing and

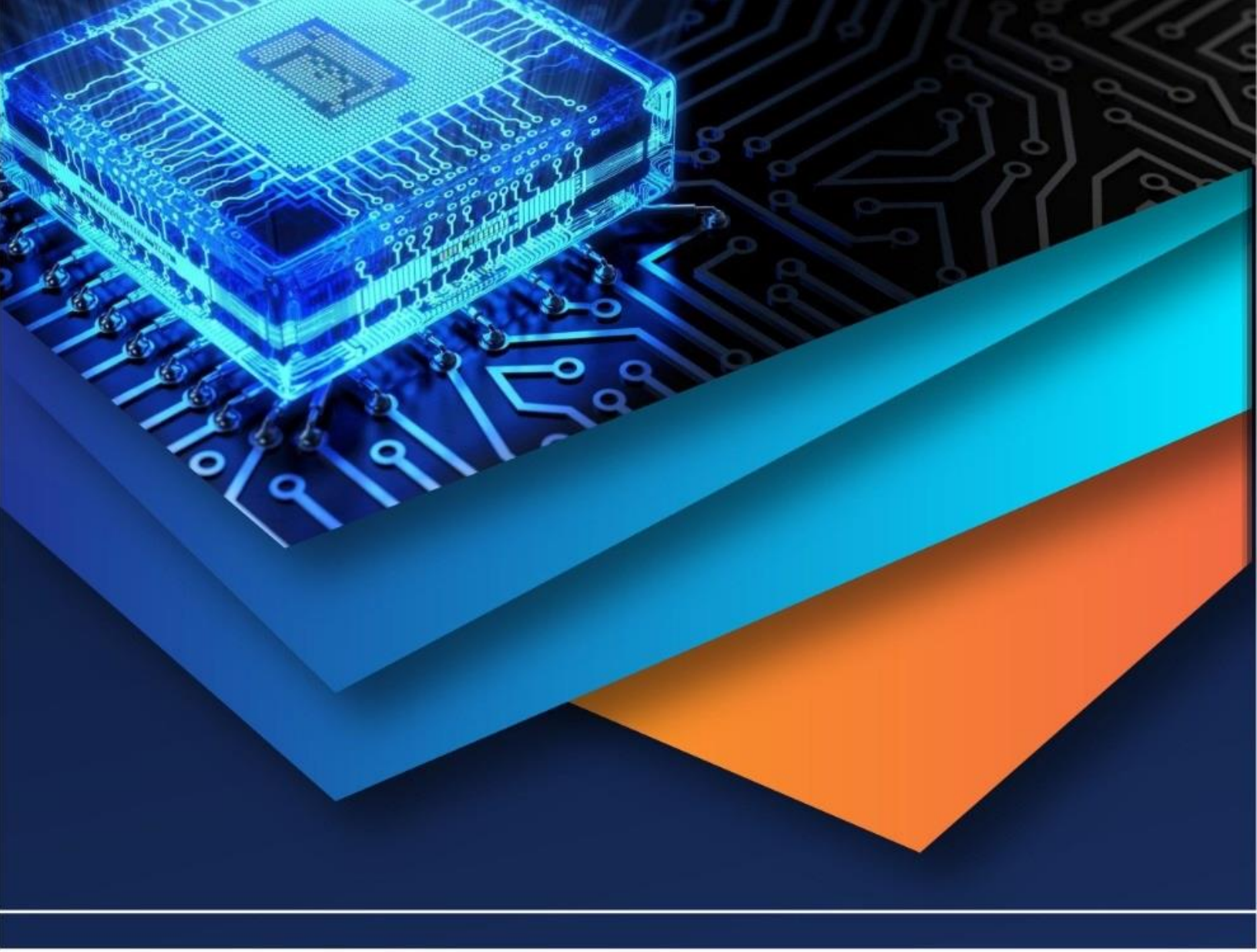
have proposed that security to the data should be provided before storing the data in the cloud. For this they have used AES algorithm for plain text encryption and then encrypted that AES key using RSA algorithm till now this is a secured technique. But we are proposing a more secure technique which will be a combination of RSA and ElipticCurve,. Strength of ElipticCurve is its non-determinism encrypting the same plain text multiple times will result in different cipher texts. It will make the encryption process more secure.

V. CONCLUSION

After studying all the reviews paper published by the authors from different perspective we found that security is a major issue in the network. However, many algorithms has been defined for maintaining the data security up to some extent, in all algorithms there are some transparencies issues which result in the breach of the network security. Here we survey various types of security technique that could be possible to use in prevention technique.

REFRENCES

[1] Zaid KARTIT, "Applying Encryption Algorithm to Enhance Data Security in Cloud Storage" Advance online publication: 17 November 201
[2] Suruchee V.Nandgaonkar et al, "A Comprehensive Study on Cloud Computing " International Journal of Computer Science And Mobile Computing, Vol.3 Issue.4, April- 2014, pg. 733-73
[3] K.Prasanthi, "A Modern Avatar of Julius Ceasar and Vigenere Cipher" IEEE International Conference on Computational Intelligence and Computing Research 201
[4] Aditi Saraswat, Chahat Khatri, Sudhakar, Prateek Thakral and Prantik Biswas, 'An Extended Hybridization of Vigener andcaeser cipher techniques for secure communication', Elsevier Procedia Computer Science 92, 355-360, 201
[5] Zhibin Chen, Jianfeng Yang "Cloud Computing Research and Security Issues" 978-1-4244-5392-4/10/$26.00 ©2010 IEE
[6] Anuradha Thilakarathne, Janaka I Wijayanayake,"Security Challenges Of Cloud Computing", International Journal scientific & technology research volume 3, issue 11, November 2014 ISSN 2277-8616



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY