INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATION & MANAGEMENT

IJRCM

A Monthly Double-Blind Peer Reviewed (Refereed/Juried) Open Access International e-Journal - Included in the International Serial Directories

Indexed & Listed at:

Ulrich's Periodicals Directory ©, ProQuest, U.S.A., EBSCO Publishing, U.S.A., Cabell's Directories of Publishing Opportunities, U.S.A.,

Open J-Gage, India [link of the same is duly available at Inflibnet of University Grants Commission (U.G.C.)],

Index Copernicus Publishers Panel, Poland with IC Value of 5.09 & number of libraries all around the world.

Circulated all over the world & Google has verified that scholars of more than 4255 Cities in 176 countries/territories are visiting our journal on regular basis.

Ground Floor, Building No. 1041-C-1, Devi Bhawan Bazar, JAGADHRI – 135 003, Yamunanagar, Haryana, INDIA

http://ijrcm.org.in/

CONTENTS

CALL FOR MANUSCRIPTS

We invite unpublished novel, original, empirical and high quality research work pertaining to recent developments & practices in the areas of Computer Science & Applications; Commerce; Business; Finance; Marketing; Human Resource Management; General Management; Banking; Economics; Tourism Administration & Management; Education; Law; Library & Information Science; Defence & Strategic Studies; Electronic Science; Corporate Governance; Industrial Relations; and emerging paradigms in allied subjects like Accounting; Accounting Information Systems; Accounting Theory & Practice; Auditing; Behavioral Accounting; Behavioral Economics; Corporate Finance; Cost Accounting; Econometrics; Economic Development; Economic History; Financial Institutions & Markets; Financial Services; Fiscal Policy; Government & Non Profit Accounting; Industrial Organization; International Economics & Trade; International Finance; Macro Economics; Micro Economics; Rural Economics; Co-operation; Demography: Development Planning; Development Studies; Applied Economics; Development Economics; Business Economics; Monetary Policy; Public Policy Economics; Real Estate; Regional Economics; Political Science; Continuing Education; Labour Welfare; Philosophy; Psychology; Sociology; Tax Accounting; Advertising & Promotion Management; Management Information Systems (MIS); Business Law; Public Responsibility & Ethics; Communication; Direct Marketing; E-Commerce; Global Business; Health Care Administration; Labour Relations & Human Resource Management; Marketing Research; Marketing Theory & Applications; Non-Profit Organizations; Office Administration/Management; Operations Research/Statistics; Organizational Behavior & Theory; Organizational Development; Production/Operations; International Relations; Human Rights & Duties; Public Administration; Population Studies; Purchasing/Materials Management; Retailing; Sales/Selling; Services; Small Business Entrepreneurship; Strategic Management Policy; Technology/Innovation; Tourism & Hospitality; Transportation Distribution; Algorithms; Artificial Intelligence; Compilers & Translation; Computer Aided Design (CAD); Computer Aided Manufacturing; Computer Graphics; Computer Organization & Architecture; Database Structures & Systems; Discrete Structures; Internet; Management Information Systems; Modeling & Simulation; Neural Systems/Neural Networks; Numerical Analysis/Scientific Computing; Object Oriented Programming; Operating Systems; Programming Languages; Robotics; Symbolic & Formal Logic; Web Design and emerging paradigms in allied subjects.

Anybody can submit the **soft copy** of unpublished novel; original; empirical and high quality **research work/manuscript** ***anytime*** in ***M.S. Word format*** after preparing the same as per our **GUIDELINES FOR SUBMISSION**; at our email address i.e. infoijrcm@gmail.com or online by clicking the link **online submission** as given on our website (***FOR ONLINE SUBMISSION, CLICK HERE***).

GUIDELINES FOR SUBMISSION OF MANUSCRIPT

1. **COVERING LETTER FOR SUBMISSION:**

DATED: _____

THE EDITOR

IJRCM

Subject: **SUBMISSION OF MANUSCRIPT IN THE AREA OF _____.**

(e.g. Finance/Mkt./HRM/General Mgt./Engineering/Economics/Computer/IT/ Education/Psychology/Law/Math/other, please specify)

DEAR SIR/MADAM

Please find my submission of manuscript entitled '_____' for possible publication in one of your journals.

I hereby affirm that the contents of this manuscript are original. Furthermore, it has neither been published elsewhere in any language fully or partly, nor is it under review for publication elsewhere.

I affirm that all the co-authors of this manuscript have seen the submitted version of the manuscript and have agreed to their inclusion of names as co-authors.

Also, if my/our manuscript is accepted, I agree to comply with the formalities as given on the website of the journal. The Journal has discretion to publish our contribution in any of its journals.

NAME OF CORRESPONDING AUTHOR	:
Designation	:
Institution/College/University with full address & Pin Code	:
Residential address with Pin Code	:
Mobile Number (s) with country ISD code	:
Is WhatsApp or Viber active on your above noted Mobile Number (Yes/No)	:
Landline Number (s) with country ISD code	:
E-mail Address	:
Alternate E-mail Address	:
Nationality	:

NOTES:

a) The whole manuscript has to be in ***ONE MS WORD FILE*** only, which will start from the covering letter, inside the manuscript. ***pdf. version is liable to be rejected without any consideration***.

b) The sender is required to mention the following in the **SUBJECT COLUMN of the mail**:

New Manuscript for Review in the area of (e.g. Finance/Marketing/HRM/General Mgt./Engineering/Economics/Computer/IT/ Education/Psychology/Law/Math/other, please specify)

c) There is no need to give any text in the body of mail, except the cases where the author wishes to give any **specific message** w.r.t. to the manuscript.

d) The total size of the file containing the manuscript is expected to be below **1000 KB**.

e) **Abstract alone will not be considered for review** and the author is required to submit the **complete manuscript** in the first instance.

f) ***The journal gives acknowledgement w.r.t. the receipt of every email within twenty four hours*** and in case of non-receipt of acknowledgment from the journal, w.r.t. the submission of manuscript, within two days of submission, the corresponding author is required to demand for the same by sending a separate mail to the journal.

g) The author (s) name or details should not appear anywhere on the body of the manuscript, except the covering letter and the cover page of the manuscript, in the manner as mentioned in the guidelines.

2. **MANUSCRIPT TITLE: The title of the paper should be **bold typed**, **centered** and **fully capitalised**.

3. **AUTHOR NAME (S) & AFFILIATIONS: Author (s) **name**, **designation**, **affiliation** (s), **address**, **mobile/landline number** (s), and **email/alternate email address** should be given underneath the title.

4. **ACKNOWLEDGMENTS: Acknowledgements can be given to reviewers, guides, funding institutions, etc., if any.

5. **ABSTRACT: Abstract should be in **fully italicized text**, ranging between **150** to **300 words**. The abstract must be informative and explain the background, aims, methods, results & conclusion in a **SINGLE PARA**. ***Abbreviations must be mentioned in full***.

6. **KEYWORDS: Abstract must be followed by a list of keywords, subject to the maximum of **five**. These should be arranged in alphabetic order separated by commas and full stop at the end. All words of the keywords, including the first one should be in small letters, except special words e.g. name of the Countries, abbreviations.

7. **JEL CODE: Provide the appropriate Journal of Economic Literature Classification System code (s). JEL codes are available at www.aeaweb.org/econlit/jelCodes.php, however, mentioning JEL Code is not mandatory.

8. **MANUSCRIPT: Manuscript must be in ***BRITISH ENGLISH*** prepared on a standard A4 size ***PORTRAIT SETTING PAPER***. *It should be free from any errors i.e. **grammatical, spelling** or **punctuation.** It must be thoroughly edited at your end*.

9. **HEADINGS: All the headings must be bold-faced, aligned left and fully capitalised. Leave a blank line before each heading.

10. **SUB-HEADINGS: All the sub-headings must be bold-faced, aligned left and fully capitalised.

11. **MAIN TEXT**:

THE MAIN TEXT SHOULD FOLLOW THE FOLLOWING SEQUENCE:

INTRODUCTION
REVIEW OF LITERATURE
NEED/IMPORTANCE OF THE STUDY
STATEMENT OF THE PROBLEM
OBJECTIVES
HYPOTHESIS (ES)
RESEARCH METHODOLOGY
RESULTS & DISCUSSION
FINDINGS
RECOMMENDATIONS/SUGGESTIONS
CONCLUSIONS
LIMITATIONS
SCOPE FOR FURTHER RESEARCH
REFERENCES
APPENDIX/ANNEXURE

The manuscript should preferably range from ***2000 to 5000 WORDS***.

12. **FIGURES & TABLES:** These should be simple, crystal **CLEAR**, **centered**, **separately numbered** & self explained, and **titles must be above the table/figure**. **Sources of data should be mentioned below the table/figure**. *It should be ensured that the tables/figures are referred to from the main text*.

13. **EQUATIONS/FORMULAE:** These should be consecutively numbered in parenthesis, horizontally centered with equation/formulae number placed at the right. The equation editor provided with standard versions of Microsoft Word should be utilised. If any other equation editor is utilised, author must confirm that these equations may be viewed and edited in versions of Microsoft Office that does not have the editor.

14. **ACRONYMS:** These should not be used in the abstract. The use of acronyms is elsewhere is acceptable. Acronyms should be defined on its first use in each section: Reserve Bank of India (RBI). Acronyms should be redefined on first use in subsequent sections.

15. **REFERENCES:** The list of all references should be alphabetically arranged. ***The author (s) should mention only the actually utilised references in the preparation of manuscript*** and they are supposed to follow Harvard Style of Referencing. **Also check to make sure that everything that you are including in the reference section is duly cited in the paper**. The author (s) are supposed to follow the references as per the following:

- All works cited in the text (including sources for tables and figures) should be listed alphabetically.
- Use (**ed.**) for one editor, and (**ed.s)** for multiple editors.
- When listing two or more works by one author, use --- (20xx), such as after Kohl (1997), use --- (2001), etc, in chronologically ascending order.
- Indicate (opening and closing) page numbers for articles in journals and for chapters in books.
- The title of books and journals should be in italics. Double quotation marks are used for titles of journal articles, book chapters, dissertations, reports, working papers, unpublished material, etc.
- For titles in a language other than English, provide an English translation in parenthesis.
- ***Headers, footers, endnotes*** *and* ***footnotes*** *should* ***not be used*** *in the document.* However, **you can mention short notes to elucidate some specific point**, which may be placed in number orders after the references.

PLEASE USE THE FOLLOWING FOR STYLE AND PUNCTUATION IN REFERENCES:

BOOKS

- Bowersox, Donald J., Closs, David J., (1996), "Logistical Management." Tata McGraw, Hill, New Delhi.
- Hunker, H.L. and A.J. Wright (1963), "Factors of Industrial Location in Ohio" Ohio State University, Nigeria.

CONTRIBUTIONS TO BOOKS

- Sharma T., Kwatra, G. (2008) Effectiveness of Social Advertising: A Study of Selected Campaigns, Corporate Social Responsibility, Edited by David Crowther & Nicholas Capaldi, Ashgate Research Companion to Corporate Social Responsibility, Chapter 15, pp 287-303.

JOURNAL AND OTHER ARTICLES

- Schemenner, R.W., Huber, J.C. and Cook, R.L. (1987), "Geographic Differences and the Location of New Manufacturing Facilities," Journal of Urban Economics, Vol. 21, No. 1, pp. 83-104.

CONFERENCE PAPERS

- Garg, Sambhav (2011): "Business Ethics" Paper presented at the Annual International Conference for the All India Management Association, New Delhi, India, 19–23

UNPUBLISHED DISSERTATIONS

- Kumar S. (2011): "Customer Value: A Comparative Study of Rural and Urban Customers," Thesis, Kurukshetra University, Kurukshetra.

ONLINE RESOURCES

- Always indicate the date that the source was accessed, as online resources are frequently updated or removed.

WEBSITES

- Garg, Bhavet (2011): Towards a New Gas Policy, Political Weekly, Viewed on January 01, 2012 http://epw.in/user/viewabstract.jsp

DATA SECURITY AND PRIVACY PROTECTION IN CLOUD COMPUTING

ROHINI GAIKWAD
STUDENT
SHAH & ANCHOR KUTCHHI ENGINEERING COLLEGE
CHEMBUR

JALPA MEHTA
ASST. PROFESSOR
SHAH & ANCHOR KUTCHHI ENGINEERING COLLEGE
CHEMBUR

ABSTRACT

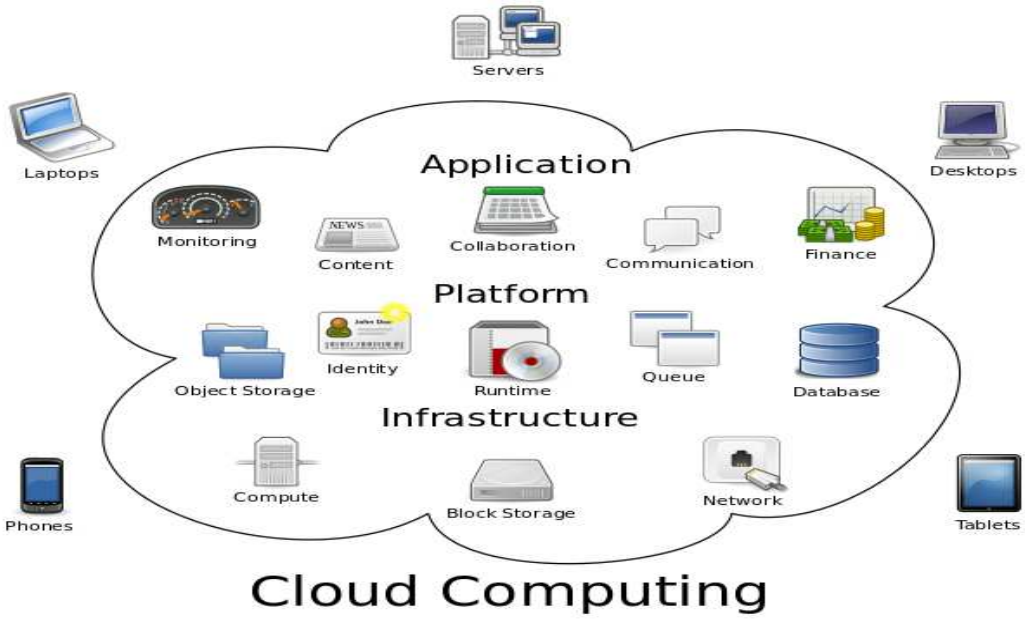
Cloud computing bears everything as a service over the web supports user demand. The benefits of cloud storage are easy access means access to your knowledge anyplace, anyhow, anytime, scalability, resilience, cost efficiency, and high reliability of the data. So each and every organization is moving its data to the cloud, means it uses the storage service provided by the cloud provider. So there is a need to protect that data against unauthorized access, modification or denial of services. Cloud refers to storing, processing and usage of data on server ports rather than local machines. Cloud reduces the load on user's machine significantly. Only thing one needs is a working data connection cloud computing system's interface software. However data handling from a distant port does raise data security concerns which cannot be compromised with. This report deals with the various encryption algorithms used to authenticate and validate the access to the cloud.

KEYWORDS
Confidentiality, Encryption Algorithm, Integrity, Privacy, Security.

1. INTRODUCTION

Cloud computing is defined as the set of resources or services offered through the internet to the users on their demand by cloud providers. It bears everything as a service over the internet based on user demand, for instance operating system, network hardware, storage, resources, and software. As each and every organization is moving its data to the cloud, means it uses the storage service provided by the cloud provider.

FIGURE 1: CLOUD COMPUTING SERVICES



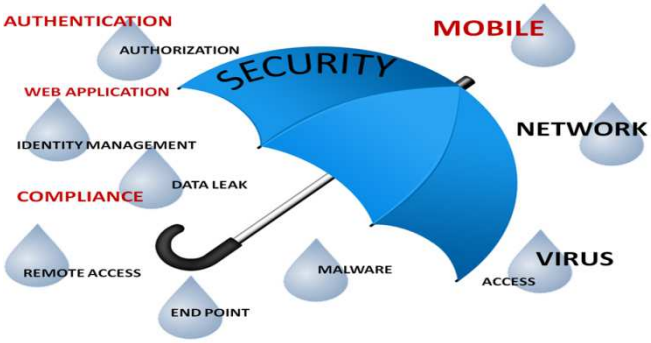
The concept of cloud computing is associated closely with Infrastructure as a Services (IaaS), Platform as a Services (PaaS), Software as a Services (SaaS) all of which means a service oriented architecture. These provide the first benefit of the cloud computing it reduce cost of hardware that cloud have been used at end user. To secure the Cloud means secure the treatments and storage “databases hosted by the Cloud provider”. Security goals of data include three points namely: Confidentiality, Integrity, and Availability (CIA). Confidentiality of data in the cloud is accomplished by Encryption/ Decryption process.

2. REVIEW OF LITERATURE

2.1 CLOUD COMPUUTING SECURITY

Cloud computing security is the set of control-based technologies and policies designed to adhere to regulatory compliance rules and protect information, data applications and infrastructure associated with cloud computing use. Because of the cloud's very nature as a shared resource, identity management, privacy and access control are of particular concern. With more organizations using cloud computing and associated cloud providers for data operations, proper security in these and other potentially vulnerable areas have become a priority for organizations contracting with a cloud computing provider.

FIGURE 2: CLOUD COMPUTING SECURITY



Cloud computing security processes should address the security controls the cloud provider will incorporate to maintain the customer's data security, privacy and compliance with necessary regulations.

2.2 GOALS OF CLOUD SECURITY

The goals of cloud security are as follows:

1. Confidentiality
2. Integrity
3. Availability

2.3 ISSUES IN CLOUD COMPUTING SECURITY

There are six types of major issues of data security in the cloud.

1. DATA AUTHENTICATION

A user may gain access within a LAN by entering a cloud identification and password, which may be affirmed by a cloud authentication mechanism. If the authentication mechanism validates the certification, the user identification and password are stored locally for subsequent authentication requests. The authentication mechanism may be applied in both domain and Workgroup LAN and may function in parallel with other users who may have a LAN or client credentials which may not be authenticated from the cloud.

2. DATA PRIVACY AND CONFIDENTIALITY

Once the clients outsource data to the cloud there should be assurance that data is accessible to only authorized users. The cloud computing service provider should make secure the customer personal data is well protected from other service provider's and user. Authentication is the best solution for data privacy because service provider must make sure who is accessing the data and who is maintaining the server; so that the customer's personal data is protected. The cloud customer must be guaranteed that data stored in the cloud will be confidential.

3. DATA INTEGRITY

Data Integrity means data is complete and consistent. The data stored in the cloud may suffer from damage during integration operations. The cloud provider must make the client aware of what particular data are outsourced to the cloud, the native and the integrity mechanisms put in place.

4. DATA LOCATION

The cloud users did not know where the data will be hosted and in fact, their users want to know the location exactly. It requires a contractual agreement between the users that data should stay in a particular location.

5. DATA AVAILABILITY

Data provided by the customer is normally stored in different servers often placing in different locations or in different clouds. Data availability becomes a major legitimate issue as the availability of corrupted and relatively difficult servers.

6. DATA STORAGE, BACKUP AND RECOVERY

The cloud users decide to move their data to the cloud provider should ensure adequate resilience storage systems. The process of recovering and backing up data is simplified. The cloud providers will store the data in several places across many independent servers.

2.4 EXISTING ENCRYPTION ALGORITHMS

1. CAESAR CIPHER

Caesar cipher is a classical substitution cipher and it is one of the simplest examples of substitution cipher. It replaces alphabet of letter in the plain text, with a letter 3 places ahead of it. For example, "HELLO" is a plain text which will be converted into "KHOOR" as cipher text. One can see that such a cipher may be difficult to break. This cipher can be broken by brute force attack because at the end there are only 25 possible available options of key.

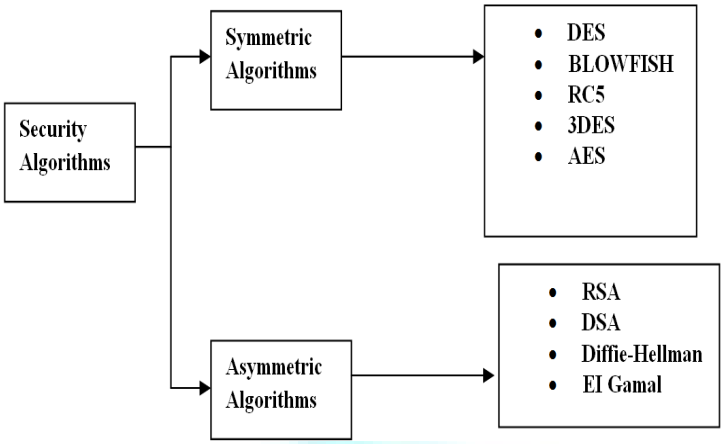
2. PLAYFAIR CIPHER

Playfair cipher which has a square matrix of 5X5 alphabetical letters arranged in an appropriate manner. The user can select a key and place it in the matrix. The remaining letters of English alphabet from the key are then one by one placed in the matrix of Playfair cipher. The plain text is broken into pairs and if a pair has same alphabet then they are separated by introducing a filler letter with "x". Otherwise if the pair is with different alphabetical letters and resides in the same row of matrix then each letter is replaced by the letter ahead of it. If the pair of letters is in same column of matrix then each letter is replaced by the letter below it, and when the pair of letters is neither in same column nor in same row then are they replaced by the letter in their row that resides at the intersection of paired letters.

2.5 MODERN ENCRYPTION

There are two main categories of encryptions used to achieve data confidentiality, integrity, availability, authentication and non-repudiation. Non-repudiation means that when something has been sent from someone, there has to be a way to track back to the sender. These are symmetric and asymmetric encryption algorithms.

FIGURE 3: SECURITY ALGORITHMS



SYMMETRIC ENCRYPTION

Symmetric-key algorithms are those algorithms which use the same key for both encryption and decryption. Hence the key is kept secret. Symmetric algorithms have the advantage of not consuming too much of computing power and it works with high speed in encryption. Symmetric-key algorithms are divided into two types: Block cipher and Stream cipher. In block cipher input is taken as a block of plaintext of fixed size depending on the type of a symmetric encryption algorithm, key of fixed size is applied on to block of plain text and then the output block of the same size as the block of plaintext is obtained. In Case of stream cipher one bit at a time is encrypted.

1. DATA ENCRYPTION STANDARD (DES)

The Data Encryption Standard (DES) is a symmetric- key block cipher published as FIPS-46 in the Federal Register in January 1977 by the National Institute of Standards and Technology (NIST). At the encryption site, DES takes a 64-bit plaintext and creates a 64-bit cipher text, at the decryption site, it takes a 64-bit cipher text and creates a 64-bit plaintext, and same 56 bit cipher key is used for both encryption and decryption. The encryption process is made of two permutations (P-boxes), which we call initial and final permutation, and sixteen Feistel rounds. Each round uses a different 48-bit round key generated from the cipher key according to a predefined algorithm.

2. BLOWFISH ALGORITHM

Blowfish is a symmetric key cryptographic algorithm. Blowfish encrypts 64 bit blocks with a variable length key of 128-448 bits. According to Schneier, Blowfish was designed with the followings objectives in mind:

- Fast- Blowfish encryption rate on 32-bit microprocessors is 26 clock cycles per byte.
- Compact- Blowfish can execute in less than 5 kb memory.
- Simple-Blowfish uses only primitive operation -s, such as addition, XOR and table look up, making its design and implementation simple.
- Secure- Blowfish has a variable key length up to maximum of 448-bit long, making it both secure and flexible.

Blowfish suits applications where the key remains constant for a long time (e.g. Communications link encryption), but not where the key changes frequently (e.g. Packet Switching).

3. ADVANCED ENCRYPTION STANDARD (AES)

Advanced Encryption Standard is a symmetric- key block cipher published as FIPS-197 in the Federal Register in December 2001 by the National Institute of Standards and Technology (NIST). AES is a non-Feistel cipher. AES encrypts data with block size of 128-bits. It uses 10, 12, or fourteen rounds. Depending on the number of rounds, the key size may be 128, 192, or 256 bits. AES operates on a 4×4 column-major order matrix of bytes, known as the state.

ASYMMETRIC ENCRYPTION

Asymmetric encryption algorithm uses two keys instead of one. One is a private key only known to the recipient of the message and the other is a public key known to everyone and can be freely distributed. Either key can be used to encrypt and decrypt the message.

1. RSA ALGORITHM

The most common Public Key algorithm is RSA, named for its inventors Rivest, Shamir, and Adleman (RSA). RSA is basically an asymmetric encryption /decryption algorithm. It is asymmetric in the sense, that here public key distributed to all through which one can encrypt the message and private key which is used for decryption is kept secret and is not shared to everyone. RSA cryptosystem realize the properties of the multiplicative Homomorphic encryption RSA uses modular exponential for encryption and decryption. RSA uses two exponents, a and b, where a is public and b is private. Let the plaintext is P and C is cipher text, then at encryption C = P^a mod n and at decryption side P = C^b mod n, n is a very large number created during key generation process.

2. ELLIPTIC CURVE CRYPTOGRAPHY (ECC)

Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. Elliptic curves are also used in several integer factorization algorithms that have applications in cryptography. The primary benefit promised by ECC is a smaller key size, reducing storage and transmission requirements, i.e. that an elliptic curve group could provide the same level of security afforded by an RSA-based system with a large modulus and correspondingly larger key – e.g., a 256-bit ECC public key should provide comparable security to a 3072-bit RSA public key . For current cryptographic purposes, an *elliptic curve* is a plane curve over a finite field (rather than the real numbers) which consists of the points satisfying the equation, y2=x3+ax+b, along with a distinguished point at infinity, denoted ∞.

3. DSA

The Digital Signature Algorithm (DSA) is a Federal Information Processing Standard for digital signatures. It was proposed by the National Institute of Standards and Technology (NIST) in August 1991 for use in their Digital Signature Standard (DSS) and adopted as FIPS 186 in 1993. Four revisions to the initial specification have been released: FIPS 186-1 in 1996, FIPS 186-2 in 2000, FIPS 186-3 in 2009, and FIPS 186-4 in 2013. With DSA, the entropy, secrecy, and uniqueness of the random signature value *k* is critical. It is so critical that violating any one of those three requirements can reveal the entire private key to an attacker. Using the same value twice (even while keeping *k* secret), using a predictable value, or leaking even a few bits of *k* in each of several signatures, is enough to break DSA.

3. REPORT ON PRESENT INVESTIGATION

3.1 CLOUD COMPUTING

Cloud Computing is the ability to access a pool of computing resources owned and maintained by a third party via the Internet. The “cloud” is composed of hardware, storage, networks, interfaces, and services that provide the means through which users can access the infrastructures, computing power, applications, and services on demand which are independent of locations. Cloud computing usually involves the transfer, storage, and processing of information on the ‘providers’ infrastructure, which is not included in the ‘customers’ control policy.

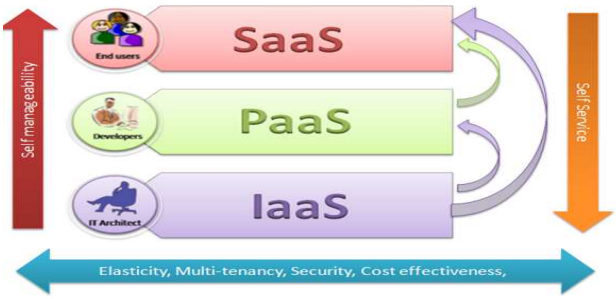
3.2 CHARACTERISTICS OF CLOUD COMPUTING

1. On demand self-services: computer services such as email, applications, network or server service can be provided without requiring human interaction with each service provider. Cloud service providers providing on demand self-services include Amazon Web Services (AWS), Microsoft, Google, IBM and Salesforce.com. New York Times and NASDAQ are examples of companies using AWS (NIST). Gartner describes this characteristic as service based.

2. Broad network access: Cloud Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms such as mobile phones, laptops and PDAs.
3. Resource pooling: The provider's computing resources are pooled together to serve multiple consumers using multiple-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. The resources include among others storage, processing, memory, network bandwidth, virtual machines and email services. The pooling together of the resource builds economies of scale.
4. Rapid elasticity: Cloud services can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.
5. Measured service: Cloud computing resource usage can be measured, controlled, and reported providing transparency for both the provider and consumer of the utilized service. Cloud computing services use a metering capability which enables to control and optimize resource use. This implies that just like air time, electricity or municipality water IT services are charged per usage metrics – pay per use.
6. Multi Tenacity: is the 6th characteristics of cloud computing advocated by the Cloud Security Alliance. It refers to the need for policy-driven enforcement, segmentation, isolation, governance, service levels, and chargeback/billing models for different consumer constituencies.

3.3 SERVICE MODELS

FIGURE 4: SERVICE MODELS



1. Infrastructure as a Service (IaaS)

Infrastructure as a Service is a provision model in which an organization outsources the equipment used to support operations, including storage, hardware, servers and networking components. The service provider owns the equipment and is responsible for housing, running and maintaining it. The client typically pays on a per-use basis.

2. Platform as a Service (PaaS)

Platform as a Service (PaaS) is a way to rent hardware, operating systems, storage and network capacity over the Internet. The service delivery model allows the customer to rent virtualized servers and associated services for running existing applications or developing and testing new ones.

Platform as a Service (PaaS) is an outgrowth of Software as a Service (SaaS), a software distribution model in which hosted software applications are made available to customers over the Internet. PaaS has several advantages for developers. With PaaS, operating system features can be changed and upgraded frequently. Geographically distributed development teams can work together on software development projects.

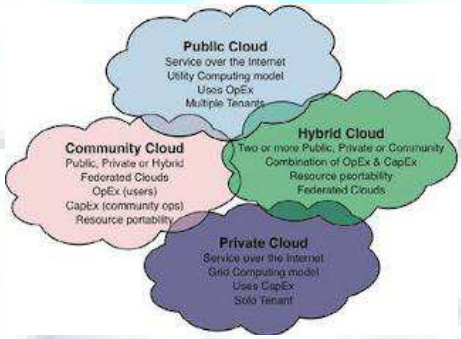
3. Software as a Service (SaaS)

Software as a Service (SaaS) is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the Internet. SaaS is becoming an increasingly prevalent delivery model as underlying technologies that support Web services and service-oriented architecture (SOA) mature and new developmental approaches, such as Ajax, become popular. Meanwhile, broadband service has become increasingly available to support user access from more areas around the world. SaaS is closely related to the ASP (application service provider) and on demand computing software delivery models. IDC identifies two slightly different delivery models for SaaS. The hosted application management (hosted AM) model is similar to ASP: a provider hosts commercially available software for customers and delivers it over the Web. In the software on demand model, the provider gives customers network-based access to a single copy of an application created specifically for SaaS distribution.

3.4 DEPLOYMENT MODELS

The four deployment models operated by cloud computing are the: Public Cloud, Private Cloud, Community Cloud, and Hybrid Cloud.

FIGURE 5: DEPLOYMENT MODELS



1. PUBLIC CLOUD

The cloud computing resource is shared exterior, someone can use it and a few payments maybe count. Public organizations assist in supplying the infrastructure to carry out the public cloud.

2. PRIVATE CLOUD

The private cloud resource is boundary to a collection of people, like a staff of a company. Infrastructure of private cloud is perfectly controlled and corporate data are completely supported by the organization itself.

3. HYBRID CLOUD

This is the combination of public as well as private cloud. It can also be explained as multiple cloud systems that are related in a way that permits programs and data to be moved comfortably from one system to another.

4. COMMUNITY CLOUD

The cloud is basically the mixture of one or more public, private or hybrid clouds, which is shared by many organizations for a single cause (mostly security).Infrastructure is to be shared by several organizations within specific community with common security, compliance objectives. It is managed by third party or managed internally. Its cost is lesser then public cloud but more than private cloud.

3.5 SECURITY GOALS

1. **Confidentiality:** Confidentiality refers to the prevention of intentional or unintentional unauthorized disclosure of information. Confidentiality in cloud systems is related to the areas of intellectual property rights, covert channels, traffic analysis, encryption, and inference:
2. **Integrity**: The concept of cloud information integrity requires that the following three principles are met:
   - Modifications are not made to data by unauthorized personnel or processes.
   - Unauthorized modifications are not made to data by authorized personnel or processes.
   - The data is internally and externally consistent — in other words, the internal information is consistent both among all sub-entities and with the real-world, external situation.
3. **Availability:** Availability ensures the reliable and timely access to cloud data or cloud computing resources by the appropriate personnel. Availability guarantees that the systems are functioning properly when needed. In addition, this concept guarantees that the security services of the cloud system are in working order. A denial-of-service attack is an example of a threat against availability.

3.6 CHALLENGES OF CLOUD COMPUTING

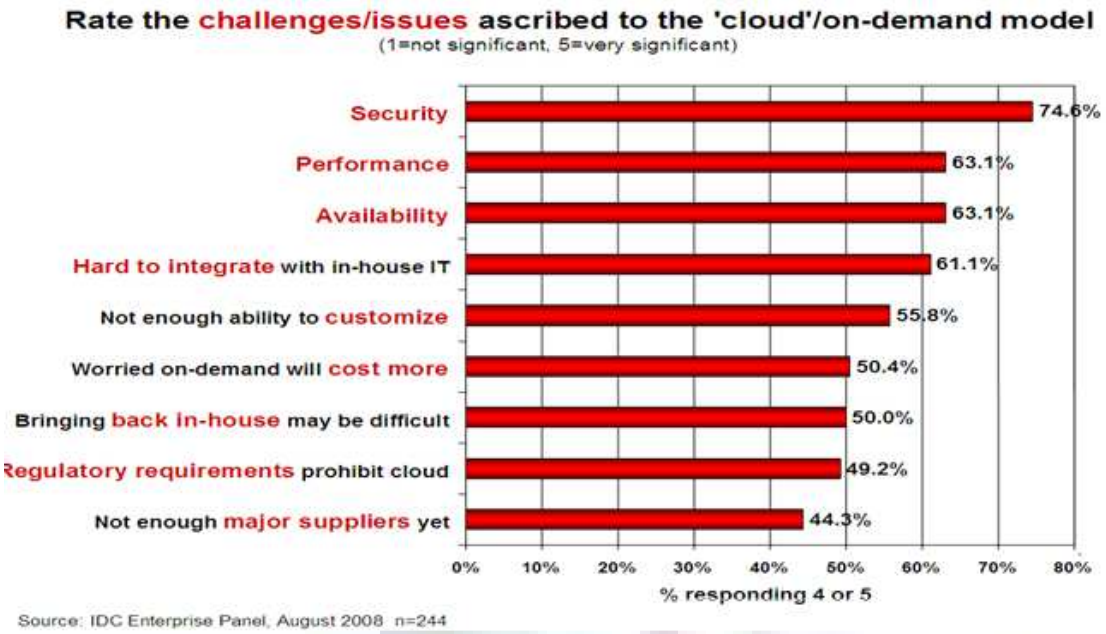
1. SECURITY AND PRIVACY

According to the survey of International Data Corporation (IDC), Security, Performance and Availability are the three biggest issues in cloud adoption. The critical challenge is how it addresses security and privacy issues which occur due to movement of data and application on networks, loss of control on data, heterogeneous nature of resources and various security policies. Data stored, processing and movement of data outside the controls of an organization poses an inherent risk and making it vulnerable to various attacks. The security threats can be of two types viz. internal and external. The external risk is posed by various persons and organizations e.g. enemies or hackers that do not have direct access to the cloud. The internal security risk is a well-known issue which can be posed by organizational affiliates, contractors, current or former employees and other parties that have received access to an organization's servers, networks and data to facilitate operations. Cloud computing poses privacy concerns because the service providers may access the data that is on the cloud that could accidentally or deliberately be changed or even removed posing serious business trust and legal consequences.

2. PERFORMANCE

According to IDC's survey, performance is the second biggest issue in cloud adoption. The cloud must provide improved performance when a user moves to cloud computing infrastructure. Performance is generally measured by capabilities of applications running on the cloud system. Poor performance can be caused by lack of proper resources viz. disk space, limited bandwidth, lower CPU speed, memory, network connections etc. Many times users prefer to use services from more than one cloud where some applications are located on private clouds while some other data or applications being on public and/or community cloud. The data intensive applications are more challenging to provide proper resources. Poor performance can results in end of service delivery, loss of customers, reduce bottom line revenues etc.

FIGURE 6: CHALLENGES IN CLOUD COMPUTING



3. RELIABILITY AND AVAILABILITY

Any technology's strength is measured by its degree of reliability and availability. Reliability denotes how often resources are available without disruption (loss of data, code reset during execution) and how often they fail. One of the important aspect that creates serious problems for the reliability of cloud computing is down time. One way to achieve reliability is redundant resource utilization. Availability can be understood as the possibility of obtaining the resources whenever they are needed with the consideration to the time it takes for these resources to be provisioned. Regardless of employing architectures having attributes for high reliability and availability, the services in cloud computing can experience denial of service attacks, performance slowdowns, equipment outages and natural disasters. Data shows that some of the current cloud computing providers have some frequent outages last year. e.g Amazon EC2 outage. In order to remove FUDD (fear, uncertainty, doubt, and disinformation), probably the reliability, availability and security are the important and prime concern to an organization. Therefore, the level of reliability and availability of cloud resources must be considered as a serious issue into the organization's planning to set up the cloud infrastructure in order to provide effective services to consumers.

4. SCALABILITY AND ELASTICITY

Scalability and elasticity are the most amazing and unique features of the cloud computing. These features provide users to use cloud resources being provisioned as per their need in unlimited amount as required. Scalability can be defined as the ability of the system to perform well even when the resources have been scaled up. Elasticity, on the other hand, is the ability to scale resources both up and down as and when required. Elasticity goes one step further, though, and does also allow the dynamic integration and extraction of physical resources to the infrastructure. The elastic cloud computing means that allocation of resources can get bigger or smaller depending on the requirement. Elasticity enables scalability—which means the system can easily scale up or down the level of services to which the user has subscribed. Scalability can be provided in two ways- horizontally and vertically whereby horizontal scalability (Scale Out) refers to addition of more nodes to the system such as adding a new computer to an existing service provider system while vertical scalability (scale up) refers to addition of resources to a single node in the system, typically involving the addition of memory or processors to a single computer.

5. INTEROPERABILITY AND PORTABILITY

Interoperability is the ability to use the same tools or application across various cloud service providers platforms. The interoperability can be defined at various levels viz. application, service, management and Data interoperability. Cloud users must have the flexibility of migrating in and out and switching to clouds whenever they want without no vendor lock-in period. One of the adoption barriers in cloud computing interoperability is the vendor lock-in risk. The main

problems to realize it are the lack of open standards, open APIs and lack of standard interfaces for VM formats and service deployment interfaces. Cloud portability ensures that one cloud solution will be able to work with other platforms and applications as well as with other clouds.

3.7 COMPARITIVE ANALYSIS

METRICS OF CLOUD COMPUTING SECURITY

1. FLEXIBILITY

So many Peoples love to use the cloud computing because of the great advantage of flexibility, users can access stored data anywhere in the world, but the thing is you need a computer/laptop/smart phone/Android /Blackberry and other applicable devices with internet connections. Staff can access the data and files outside the office at any time.

2. LOW COST

This is the very great advantages for organizations to reduce their cost by having the cloud computing service. And also Organization can concentrate more to expand their business rather than concentrating on Software and hardware updates. Everything is stetted up in host, which automatically saves the time and money for any organizations.

3. HIGHLY AUTOMATED

No need to purchase updated soft wares, everything has been set – up and ready to use. Here you can also cut an employee, who takes care of software updates, this result to hire another employee to expand/improve business. It's a like G-Mail or Hotmail, which can use by creating account within in seconds/minutes. In other hand it's tough to download software and again have to install then use it, also have to update software by paying extra money.

4. FAST SERVICE

Cloud computing service providers having infrastructure so server always in up-time. This results you no destruct ions in business. Depending upon business needs have to choose plans for fast access service.

5. MORE STORAGE CAPACITY

No need to worry about your lot of data and files to store, this provides more data to save the files in server. Here depending upon the data and usage you can choose the plans, available in different modes. Everything is online, store your entire data in cloud and can access at any time in browser.

6. COST SAVINGS

Companies can reduce their capital expenditures and use operational expenditures for increasing their computing capabilities. This is a lower barrier to entry and also requires fewer in-house IT resources to provide system support.

TABLE 1: COMPARISION OF ENCRYPTION ALGORITHM

Features	AES	RSA	BLOWFISH	DES	3DES	RC5	ECC
Platform	Cloud Computing	Cloud Computing	Cloud Computing	Cloud Computing	Cloud Computing	Cloud Computing	Cloud Computing
Key Size	128,192,256 bits	1024 bits	32- 448 bits	56 bits	168,112bits	Max 2040	135bits
Scalability	Scalable	Not Scalable	Scalable	Scalable	Scalable	Scalable	Less Scalable
Security	Secure for both provider and user.	Secure for user only	Secure for both providers and user/client side	Security applied to both providers and user	Adequate	Secure for both provider and user	Less Secure
Data Encryption Capacity	Used for encryption of large amount of data	Used for encryption of small data	Less than AES	Less than AES	Less than AES	Less than AES	Used for encryption of small data
Authentication Type	Best authenticity provider	Robust authentic implementation	Comparable to AES	Less authentic than AES.	Less authentic than AES	Less authentic than AES	Robust authentic implementation
Memory Usage	Low RAM needed	Highest memory usage algorithm	Can execute in less than 5 kb	More than AES	More than AES	More than AES	High memory usage
Execution Time	Faster than others	Requires maximum time	Lesser time to execute	Equals to AES	Very Slow	Slow	Fastest

4. CONCLUSION

In this encryption algorithms have been proposed to make cloud data secure, vulnerable and gave concern to security issues, challenges and also comparisons have been made between AES, DES, Blowfish and RSA algorithms to find the best one security algorithm, which has to be used in cloud computing for making cloud data secure and not to be hacked by attackers. Encryption algorithms play an important role in data security on cloud and by comparison of different parameters used in algorithms, it has been found that AES algorithm uses least time to execute cloud data. Blowfish algorithm has least memory requirement. DES algorithm consumes least encryption time. RSA consumes longest memory size and encryption time. In today's era demand of cloud is increasing so the security of the cloud and user is on top concern. Hence, these algorithms are helpful for today's requirement. In future several comparisons with different approaches and results to show effectiveness of proposed framework can be provided.

REFERENCES

1. "A Comparative Analysis of Encryption Techniques and Data Security Issues in Cloud Computing". (June 2014) International Journal of Computer Applications (0975 – 8887) Volume 96– No.16.
2. Dr. L. Arockiam1, S. Monikandan2, (August 2013) "Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm" International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 8.
3. K. S. Suresh, Prof K. V. Prasad, "Security Issues and Security Algorithms in Cloud Computing" International Journal of Advanced Research in computer Science and Software Engineering.
4. Kuyoro S. O., Ibikunle F. & Awodele O,(2011) "Cloud Computing Security Issues and Challenges" International Journal of Computer Networks (IJCN), Volume (3): Issue (5).
5. Omer K. Jasim, Safia Abbas,(November – December 2013) "Efficiency of Modern Encryption Algorithms in Cloud Computing" International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) Volume 2, Issue 6.
6. Parsi Kaplana, SudhaSingaraju "Data Security in Cloud Computing using RSA Algorithm" International Journal of Research in Computer and Communication Technology.
7. "Privacy and Security on Cloud Data Storage Using Hybrid Encryption Technique",(January 2014) International Journal of Emerging Technology and Advanced Engineering, Volume 4, Issue 1.
8. Randeep Kaur1, Supriya Kinger2,(March 2014) "Analysis of Security Algorithms in Cloud Computing" International Journal of Application or Innovation in Engineering & Management (IJAIEM) Volume 3, Issue 3.
9. Vanya Diwan1, Shubhra Malhotra2, Rachna Jain3,(April 2014) "Cloud Security Solutions: Comparison among Various Cryptographic Algorithms" Volume 4, Issue 4. International Journal of Advanced Research in Computer Science and Software Engineering.

REQUEST FOR FEEDBACK

Dear Readers

At the very outset, International Journal of Research in Computer Application & Management (IJRCM) acknowledges & appreciates your efforts in showing interest in our present issue under your kind perusal.

I would like to request you tosupply your critical comments and suggestions about the material published in this issue as well as on the journal as a whole, on our E-mail**infoijrcm@gmail.com** for further improvements in the interest of research.

If youhave any queries please feel free to contact us on our E-mail infoijrcm@gmail.com.

I am sure that your feedback and deliberations would make future issues better – a result of our joint effort.

Looking forward an appropriate consideration.

With sincere regards

Thanking you profoundly

Academically yours

Sd/-
Co-ordinator

DISCLAIMER

The information and opinions presented in the Journal reflect the views of the authors and not of the Journal or its Editorial Board or the Publishers/Editors. Publication does not constitute endorsement by the journal. Neither the Journal nor its publishers/Editors/Editorial Board nor anyone else involved in creating, producing or delivering the journal or the materials contained therein, assumes any liability or responsibility for the accuracy, completeness, or usefulness of any information provided in the journal, nor shall they be liable for any direct, indirect, incidental, special, consequential or punitive damages arising out of the use of information/material contained in the journal. The journal, neither its publishers/Editors/ Editorial Board, nor any other party involved in the preparation of material contained in the journal represents or warrants that the information contained herein is in every respect accurate or complete, and they are not responsible for any errors or omissions or for the results obtained from the use of such material. Readers are encouraged to confirm the information contained herein with other sources. The responsibility of the contents and the opinions expressed in this journal are exclusively of the author (s) concerned.

ABOUT THE JOURNAL

In this age of Commerce, Economics, Computer, I.T. & Management and cut throat competition, a group of intellectuals felt the need to have some platform, where young and budding managers and academicians could express their views and discuss the problems among their peers. This journal was conceived with this noble intention in view. This journal has been introduced to give an opportunity for expressing refined and innovative ideas in this field. It is our humble endeavour to provide a springboard to the upcoming specialists and give a chance to know about the latest in the sphere of research and knowledge. We have taken a small step and we hope that with the active co-operation of like-minded scholars, we shall be able to serve the society with our humble efforts.

Our Other Journals