Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 4, April 2014, pg.110 – 120

REVIEW ARTICLE

Review on "An analysis of the Management Security and Security Algorithms in Cloud Computing"

Nilesh N.Chawande[1]

[1]M.E(CSE) second semester

[1]Department of computer science & Engineering

[1]GHRCEM, Amravati, Maharashtra (India)

[1]EmailID- NileshChawande@gmail.com

Prof Jayant P.Mehare[2]

M.E(IT)

[2] Department of Information Technology

[2]GHRCEM Amravati, Maharashtra (India)

[2]EmailID- jayant.mehare@raisoni.net

Abstract -

Cloud computing has elevated IT to newer limits by offering the market environment data storage and capacity with flexible & scalable computing as well as processing power to match elastic demand and supply while reducing capital use. However the opportunity cost of the successful implementation of cloud computing is to effectively manage the security in the cloud applications, due to constantly increase in the popularity of cloud computing there is an ever growing risk of security. Thus security is becoming a main and top issue for security concern. In this paper, we have analyzed the management security and various security algorithms in cloud computing.

Keywords – Cloud computing; Security; Public cloud, Private cloud, Hybrid cloud, Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), Security requirements, security management, Cloud Governance, Cloud Transparency, Security algorithms, AES, Blowfish algorithms, Ciper cloud, DES, Homomorphic encryption, MD5, RSA

I. INTRODUCTION

The accomplishment of up to date advances very relies on upon its viability of the world's standards, its usability by end clients and in particular its level of data security and control. cloud computing is another and rising data innovation that changes the way IT compositional results are advanced by method for moving towards the subject of virtualisation of information stockpiling of nearby systems (foundation) and in addition programming [12-13]. In a study embraced by the International Data Corporation (IDC) bunch between 2008 and 2009, the greater part of outcomes point to utilizing Cloud figuring as a low-costviable alternative to clients

[14]. The effects additionally indicate that Cloud computing is best suited for people who are looking for a fast answer for new companies, for example, designers or examination activities and even e-business ambitious people. Utilizing Cloud computing can help within keeping one's IT plan to an absolute minimum. It is likewise preferably suited for advancement and testing situations. It is the simplest answer for test potential verification of ideas without contributing an excessive amount of capital. cloud computing can convey a boundless cluster of IT capacities progressively usingmany diverse sorts of assets, for example, equipment, software,virtual capacity once logged onto a cloud. cloud computing can additionally be a piece of a more extensive business result whereby prioritized provisions use Cloud computing practicality whilst other discriminating requisitions look after hierarchical assets according to typical. This takes into account expense sparing whilst supporting a safe level of control inside an orgainsation. Cloud computing is an innovation that keep up information and its application by utilizing web and focal remote servers [1]. Cloud computing might be viewed as another processing standard with suggestions for more amazing adaptability and accessibility at easier cost. As a result of this, cloud computing has been getting a great arrangement of consideration of late.

II. RELATED WORK

A abundant number of related works and distributions exist in the writing, accentuating the vitality and interest of security answers for distributed computing. On the other hand, that finished not distinguish any full scientific classification that addresses specifically the security viewpoints identified with cloud computing.

The remainder of this paper is structured as follows:

Section III introduces the different organisation models such as public cloud, private cloud, community cloud, and hybrid cloud,section IV that introduced cloud computing deployment model and section V and section VI introduced cloud computing concerns and cloud computing security requirements and section VII and VIII discuss cloud computing shortfalls and managing cloud computing security and section IX and X discuss about security concerns and explaination of various security algorithms.

III. ORGANIZATION MODELS

The four organization models worked by cloud computing are the: Public Cloud, Private Cloud, Community Cloud, and Hybrid Cloud as indicated in Fig 1.each model has its own particular characteristics and particular qualities that suits to the cloud clients' specific reasons in grasping cloud computing.

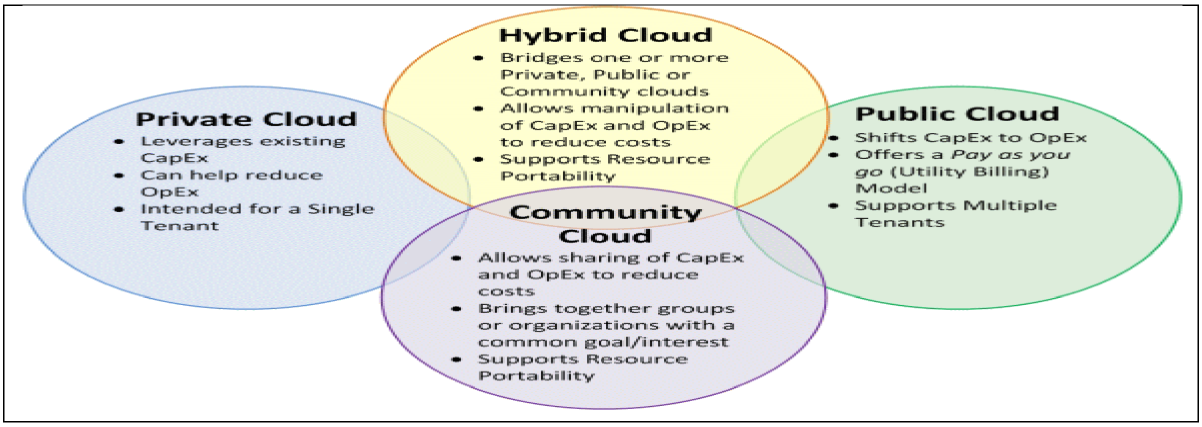
Hybrid Cloud
• Bridges one or more Private, Public or Community clouds
• Allows manipulation of CapEx and OpEx to reduce costs
• Supports Resource Portability
Private Cloud
• Leverages existing CapEx
• Can help reduce OpEx
• Intended for a Single Tenant
Public Cloud
• Shifts CapEx to OpEx
• Offers a Pay as you go (Utility Billing) Model
• Supports Multiple Tenants
Community Cloud
• Allows sharing of CapEx and OpEx to reduce costs
• Brings together groups or organizations with a common goal/interest
• Supports Resource Portability

Fig. 1 organization models operated by Cloud Computing

A. Public cloud - The cloud framework is made accessible to the overall population or a huge industry assembly and is claimed by an association offering cloud administrations and the correlation of private and open cloud as demonstrated in fig2.

B. Private cloud- The cloud framework is worked singularly for an association. It may be overseen by the association or an outsider and may exist on reason or off reason.

C. Community cloud -The cloud base is imparted by a few associations and backings a particular group that has imparted concerns (e.g., mission, security prerequisites, approach, and agreeability contemplations). It may be overseen by the associations or an outsider and may exist on reason or off reason.

D. Hybrid cloud - The cloud base is an organization of two or more mists (private, group, or open) that remain exceptional elements yet are bound together by institutionalized or exclusive engineering that empowers information and requisition transportability (e.g., cloud blasting for burden adjusting between mists).

IV. CLOUD COMPUTING DEPLOYMENT MODELS

Emulating on the cloud deployment model shows in figure 2, the following security thought that business administration must unpack identifies with the different cloud conveyance models.because of the payper use economy show that identifies with Cloud movement shows, the level of information security is composed towards holding quick to industry standards and authorizations around cloud shareholders. The building design of Cloud processing might be arranged as stated by the three sorts of conveyance models,namely Infrastructure as an service (Iaas), Platform an service (Paas),Software as an service(Saas).

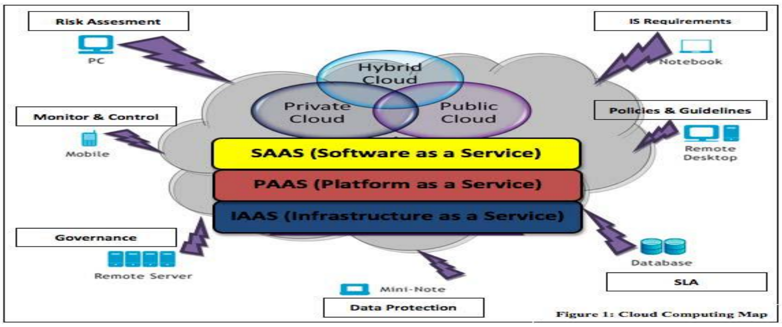

Fig. 2 cloud deployment model

1. Infrastructure as a Service (IaaS)

Framework as a Service is a procurement demonstrate in which an association outsources the supplies used to help operations, including stockpiling, fittings, servers and systems administration parts. The administration supplier possesses the gear and is answerable for lodging, running and looking after it. The customer commonly pays on a for every utilization support.Characteristics and components of IaaS include:Utility computing service and billing model.Automation of administrative tasks.Dynamic scaling.Desktop virtualization.Policy based services-Internet connectivity.

2. Platform as a Service (PaaS)

Stage as a Service (Paas) is an approach to lease equipment, working frameworks, stockpiling and system limit over the Internet. The administration conveyance model permits the client to lease virtualized servers and cohorted administrations for running existing requisitions or creating and testing new ones.

Stage as a Service (Paas) is an outgrowth of Software as a Service (Saas), a product circulation show in which facilitated programming provisions are made accessible to clients over the Internet. Paas has a few preferences for engineers. With Paas, working framework characteristics could be changed and updated much of the time. Geologically disseminated improvement groups can cooperate on programming advancement ventures. Administrations could be acquired from different sources that cross universal limits. Introductory and progressing expenses might be lessened by the utilization of foundation administrations from a solitary seller instead of supporting different fittings offices that frequently perform double capacities or experience the ill effects of inconsistency issues. General liabilities can additionally be minimized by unification of modifying improvement exertions.

3. Software as a Service (SaaS)

Programming as a Service (Saas) is a product dissemination show in which provisions are facilitated by a merchant or administration supplier and made accessible to clients over a system, ordinarily the Internet.saas is turning into an inexorably pervasive conveyance demonstrate as underlying advances that help Web administrations and administration turned building design (SOA) developed and new developmental methodologies, for example, Ajax, get mainstream. In the interim, broadband administration has gotten to be progressively accessible to help client access from additional ranges around the world.saas is nearly identified with the ASP (requisition administration supplier) and on interest processing programming conveyance models. IDC distinguishes two marginally distinctive conveyance models for Saas. The facilitated requisition administration (facilitated AM) model is like ASP: a supplier has economically accessible programming for clients and conveys it over the Web. In the product on interest model, the supplier gives clients system based access to a solitary duplicate of a requisition made particularly for Saas dispersion.

V. CLOUD COMPUTING CONCERNS

Upon deliberately settling on the fitting cloud conveyance and sending models to investigate, security officers ought to be mindful of the current Cloud processing concerns encountered in the nature's turf. Gartner has led an examination with respect to the data security issues that ought to be recognized when managing Cloud computing.the taking after rundown holds a few security issues highlighted by Gartner that associations and key chiefs, as an essential, ought to unpack with Cloud registering sellers [20].

• *Privileged access*: Who has specialised/privileged access to information? Who chooses about the procuring and administration of such managers?

• *Regulatory consistence*: Is the cloud seller ready to experience outer reviews or security accreditations?

• *Data area*: Does the cloud merchant take into account any control over the area of information?

• *Data isolation*: Is encryption accessible whatsoever stages, and were these encryption plans composed and tried by encountered experts?

• *Recovery*: What happens to information on account of a fiasco, and does the merchant offer complete reclamation, and, provided that this is true, to what extent does that process take?

• *Investigative Support*: Does the merchant can research any unseemly or illicit movement?

• *Long-term feasibility*: What happens to information if the cloud merchant goes bankrupt, is customers' information returned and in what position?

• *Data accessibility*: Can the cloud seller move all their customers' information onto an alternate environment ought to the existing environment get traded off or occupied? By recognizing the aforementioned cloud issues, executives can pick up a thorough seeing and measure the attainability of utilizing Cloud figuring answers for best match their Cloud methodology. The following area takes after on from the concerns said above and is pointed at helping IT directors evaluate business basic needs regarding data secur

VI. CLOUD COMPUTING SECURITY REQUIREMENTS

In the ISO 7498-2 standard [21], transformed by The International Standards Organization (ISO), Information Security ought to blanket various recommended subjects. Cloud computing security ought to likewise be guided in this respect keeping in mind the end goal to turn into a compelling and secure engineering result, outlining the data security necessities coupled with the Cloud processing organization model and conveyance models has been adjusted from Eloff et al [23]. In Figure 2, the diverse cloud conveyance models and arrangement models are matched up against the data security prerequisites with a "X" signifying obligatory necessities and an indicator (*) indicating discretionary prerequisites. However future work is required in exploring the ideal offset needed in securing Cloud computing ought to be seen in connection as a rule in evaluating the security level. Each of the security necessities will be highlighted underneath in setting of Cloud figuring.

A. Identification & authentication

In Cloud processing, contingent upon the sort of cloud and additionally the conveyance model, specified clients should firstly be secured and supplementary access necessities and consents may be conceded in like manner. This methodology is focusing at checking and approving singular cloud clients by utilizing usernames and passwords assurances to their cloud profiles.*B. Authorisation*

Authorisation is an important information security requirement in Cloud computing to ensure referential integrity is maintained. It follows on in exerting control and privileges over process flows within Cloud computing. Authorisation is maintained by the system administrator in a Private cloud.

C. Confidentiality

In Cloud processing, privacy has real impact particularly in administering control over associations' information arranged crosswise over different appropriated databases. It is an unquestionable requirement when utilizing a Public cloud because of open mists openness nature. Declaring secrecy of clients' profile and securing their information, that is for all intents and purpose got to, takes into account data security conventions to be authorized at different distinctive layers of cloud requisitions..

D. Integrity

The honesty prerequisite lies in applying the duediligence inside the cloud area fundamentally when getting to information. Thusly ACID (atomicity, consistency, confinement and solidness) properties of the cloud's information ought to indeed be powerfully forced over all Cloud registering convey models

E. Non-repudiation

Non-repdiation in Cloud registering might be acquired by applying the conventional e-trade security conventions and token provisioning to information transmission inside cloud provisions, for example, advanced marks, timestamps and affirmation receipts administrations (computerized receipting of messages affirming information sent/received).

F. Availability

Accessibility is a standout amongst the most discriminating data security necessities in Cloud processing on the grounds that it is a key choice variable when settling on private, open or half breed cloud sellers and additionally in the conveyance models. The administration level assention is the most paramount archive which highlights the trepidation of accessibility in cloud administrations and assets between the cloud supplier and customer. Along these lines by investigating the data security necessities at each of the different cloud organization and conveyance models set out by the ISO, merchants and associations can get positive about pushing a very ensured protected and sound cloud structure.

VII. CLOUD COMPUTING SHORTFALLS

From the study finished by the International Data Corporation (IDC),shows in figure 3, we can take in enormous lessons from over a noteworthy time compass cloud players. The reference to the International Data Partnership, is key in light of the fact that it highlights the setbacks of Distributed registering and likewise customers' security fancies in Distributed processing. In the Cloud Computing Services Survey coordinated all around August 08/09 by IDC IT total (www.idc.com) [14], customers were asked to rate their issues and tests experienced with Cloud figuring. The conclusions showed in Figure 3 outline that security is the best concern.

Information security, availability and execution issues still stay in the fundamental 3 for both years the study was done. Security is the rule issue customers are concerned with when distinguishing Cloud figuring outcomes. Selecting and executing the suitable cloud security structural building is not as fundamental as it may seem, by all accounts, to be as showed up the survey above. Likely the most discriminating issues for associations to contemplate before taking an interest in Cloud figuring, highlighted from the audit above, are the suppliers' terms of organization, and additionally the range and data restrictions on information set away in the cloud. Down-time of cloud organizations is an exchange creating concern. Cloud suppliers have the right to peruse and make open information that is put in the cloud. There necessities to be a simple concordance between liability sufficiency in addition a smooth running of secure operations with the picked nature. From the cloud deficiencies showed at one time additionally by examining the information security concerns, prospective customers will become more everyday and aware of its potential and how Cloud handling could be used to better upgrade the way we do things whilst pushing the cutoff points of onventional principles balanced by social request. The best test in completing compelling Cloud handling developments is managing the security. Similarly with any new improvement redesigns, responses are dictated by caution of dark variables and movements to current control systems. In what limit can cloud stakeholders ensure and publicize the security of Cloud enlisting? By fixating more on information security care, cloud insurance and by ensuring fitting methodologies and technique are from the get go put situated up, Cloud enlisting can transform into the most possible information improvement result. Cloud security polices, cloud transparency and its security impact are the inside subjects in breaking down the basic information security of Cloud enlisting which will secured in the accompanying region. These subjects, once totally understood and researched by potential endusers can give the key mental aptitude in controlling the productive utilization of a secured cloud result.

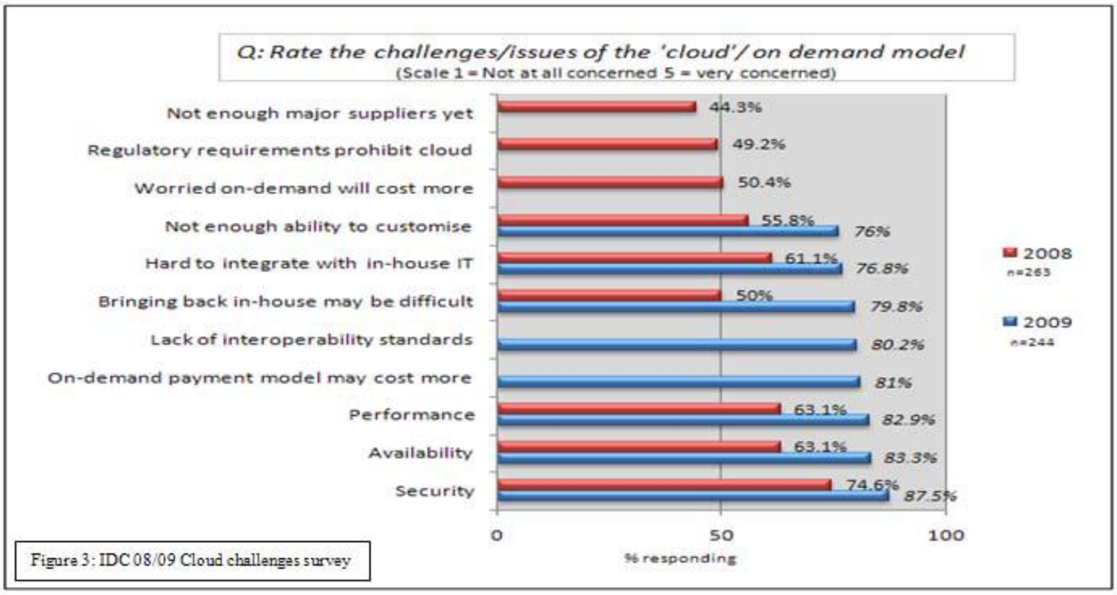

Fig. 3 IDC 08/09 cloud challenges survey

VIII. MANAGING CLOUD COMPUTING SECURITY

so as to adequately oversee and control the utilization of cloud engineering in an association, business and vital leaders need in any case surveying the potential effect of Cloud processing on their focused edge. Secondly,business discriminating security inquiries of executing cloud advances will then need to be assessed. Overseeing and controlling Cloud issues will need to deliver not restricted to the accompanying:

- how the association will manage new and current Cloud agreeability dangers. This will manage the potential effect which Cloud processing may have on the business concerning legislation and enactment.

- how Cloud registering may influence the association regarding its business insights and licensed innovation by possibly affecting its market separation.

In setting up a Cloud structure that specificall yaddresses,organisations' data security, senior experts and administration may look to adjust and fuse current information insurance, trust and protection arrangements in defining an extensive set of Cloud figuring rules. These rules may incorporate:

- establishing a general business Cloud registering arrangement that highlights the associations stance on data insurance.

- govern the establishment and correspondence of Cloud registering when IT choices are made.

- leverage of current IT review and TAX forms with the in inserting cloud security exposure and Cloud review hones.

Cloud computing rules ought to be seen as the foundation of the Cloud system with Cloud legislation and transparency shaping some piece of the security

A. Cloud Governance

Cloud computing policies and procedure ought to be placed set up in an exertion to secure the cloud from potential of threats, hacks and the misfortune of data. We must comprehend that it is important to plan protection inside the Cloud right from the start. The protection challenge for programming architects is to outline cloud benefits in such a route in order to reduction security dangers and to guarantee lawful agreeability. There are dangers connected with the information being put away, prepared remotely and an expanded utilization of virtualisation and imparting of stages between clients. Concerns emerge when it is not clear to people why their particular data is asked for or how it will be utilized or passed on to different gatherings. This absence of control prompts suspicion and at last doubt. The insurance of information in the cloud is a key shopper concern especially for submitting fake exercises and fiscal exploitation.with influence and security set up, Cloud registering could be utilized securely and with trust.

B. Cloud Transparency

Transparent security may incorporate cloud suppliers revealing adequate data about their security blueprints, mastermind, and chips away at, including uncovering fundamental endeavors to build wellbeing in orderly operations [20]. Open mists are more conceivable to be seen as having a more brilliant level of transparency as veered from the Hybrid or Private Cloud models. This is a consequence of open cloud merchants having an "institutionalized" cloud publicizing hence focusing on an all the more broad customer base. Private hazes are all things considered amassed for particular fellowships having more thought focused on offering customization and personalisation cloud reason.

A champion around the most chief gatherings in guaranteeing transparency inside Cloud figuring is the SLA. The SLA is the major true blue seeing between the association supplier and customer and its centrality is colossally dissected in the article titled "Cloud Security Issues" [24]. The rule imply that the cloud supplier can get the trust of customers is through the Sla,therefore the SLA must be organized. The crucial points of view as a guideline, which the SLA holds, may be:

- Services to be passed on, execution,

- Tracking and Reporting

- Problem Management

- Legal Compliance

- Resolution of Disputes Customer Duties

- Security commitment

- Confidential Information Termination.

One of the standard tests of Cloud computing is that software vendor should need commitment with respect to caring for the order and ensuring quality of service.

IX. SECURITY CONCERNS

A.data? The principle thing that is the place the information is on account of the information is in cloud so the cloud supplier ought to consent to give security to the information of our clients

B.access? What's more second thing that who has entry to the information that is at cloud. On the off chance that anybody utilizing the cloud needs to take a gander at who is dealing with their information and what sorts of controls are connected.

C.training to Employees? Train the workers on the grounds that the representatives need to know how to get to the information looking after security.

D.data Classification? Since there is information of distinctive client so the inquiry is ―is Data Classified‖

E. administration level assention (SLA) ? The SLA serves as a contracted level of ensured administration between the cloud supplier and the client that defines what level of administrations will be given.

F.what happens if there is a security rupture? On the off chance that a security episode happens, what help will you accept from the cloud supplier? While numerous suppliers advertise their administrations as being unhackable, cloudbased administrations are a magnetic foc

X. SECURITY ALGORITHMS

A. AES

In cryptography, the Advanced Encryption Standard (AES) is a symmetric-key encryption standard. Each of these figures has a 128-bit piece size, with key sizes of 128, 192 and 256 bits, individually [11]. AES calculation guarantees that the hash code is encoded in an exceedingly secure way. AES has a settled piece size of 128 bits and utilization a key size of 128 in this paper.. Its algorithm is as follows: 1. Key Expansion 2. Initial Round 3. Add Round Key 4. Rounds 5. Sub Bytes—a non-linear substitution step where each byte is replaced with another according to a lookup table. 6. Shift Rows—a transposition step where each row of the state is shifted cyclically a certain number of steps. 7. Mix Columns—a mixing operation which operates on the columns of the state, combining the four bytes in each column 8. Add Round Key—each byte of the state is combined with the round key; each round key is derived from the cipher key using a key schedule. 9. Final Round (no Mix Columns) 10. Sub Bytes 11. Shift Rows 12. Add Round Key

B. Blowfish algorithm

Blowfish is a symmetric-key square figure, planned in 1993 by Bruce Schneier and included in countless suites and encryption items. Blowfish gives a great encryption rate in programming and no powerful cryptanalysis of it has been found to date. Then again, the Advanced Encryption Standard (AES) now accepts more consideration. Schneier outlined Blowfish as an universally useful calculation, proposed as an elective to the maturing DES and free of the issues and demands connected with different calculations. At the time Blowfish was discharged, numerous different plans were restrictive, hindered by licenses or were business or government mysteries. Schneier has expressed that, "Blowfish is unpatented, and will remain so in all nations. The calculation is therefore set in the general population area, and might be uninhibitedly utilized by anybody."

Blowfish, another mystery key piece figure, is proposed. It is a Feistel system, repeating a straightforward encryption work 16 times. The square size is 64 bits, and the key might be any length up to 448 bits. In spite of the fact that there is a complex instatement stage needed before any encryption can occur, the genuine encryption of information is extremely effective on expansive chip.

C. Ciper cloud

Ciphercloud utilizes AES 256-bit encryption, the most noteworthy monetarily accessible level of encryption.

Ciphercloud is one of a kind in conveying the largest amounts of security, while saving the purpose of encoded information and the client experience. Protected SSE engineering gives secure virtual indexing at the entryway while sending the emphatically encoded information to the cloud. This exceptional result empowers regular dialect seeks, priveleged cases, Boolean expressions and backing for adaptable inquiry terms, for example, "begins with" or "closes with", good with today's Internet look gatherings.

D. DES

The Data Encryption Standard (DES) is a piece figure that uses imparted mystery encryption. It was chosen by the National Bureau of Standards as an authority Federal Information Processing Standard (FIPS) for the United States in 1976 and which has in this manner appreciated broad utilize universally. It is dependent upon a symmetric-key calculation that uses a 56-bit key. The calculation was at first dubious with characterized outline components, a generally short key length, and suspicions around a National Security Agency (NSA) secondary passage. DES therefore went under powerful scholastic investigation which inspired the cutting edge understanding of piece figures and their cryptanalysis.

DES is now considered to be insecure for many applications. This is chiefly due to the 56-bit key size being too small; in January, 1999, distributed.net and the Electronic Frontier Foundation collaborated to publicly break a DES key in 22 hours and 15 minutes (see chronology). There are also some analytical results which demonstrate theoretical weaknesses in the cipher, although they are infeasible to mount in practice. The algorithm is believed to be practically secure in the form of Triple DES, although there are theoretical attacks. In recent years, the cipher has been superseded by the Advanced Encryption Standard (AES). Furthermore, DES has been withdrawn as a standard by the National Institute of Standards and Technology (formerly the National Bureau of Standards).

E. Homomorphic encryption

Homomorphic encryption is a manifestation of encryption which permits particular sorts of reckonings to be completed on ciphertext and produce a scrambled outcome which, when unscrambled, matches the consequence of operations performed on the plaintext. This is an attractive characteristic in present day correspondence framework architectures. Homomorphic encryption might permit the tying together of diverse administrations without presenting the information to each of those administrations, for instance a chain of distinctive administrations from diverse organizations could

- ascertain the duty
- the cash conversion scale
- transportation,

on a transaction without uncovering the decoded information to each of those services.[1] Homomorphic encryption plans are pliable by configuration. The homomorphic property of different cryptosystems might be utilized to make secure voting systems,[2] impact safe hash capacities, private data recovery plots and empower across the board utilization of distributed computing by guaranteeing the secrecy of transformed information. There are a few effective, in part homomorphic cryptosystems, and various completely homomorphic, however less proficient cryptosystems. In spite of the fact that a cryptosystem which is unintentionally homomorphic might be liable to assaults on this support, if treated painstakingly homomorphism can likewise be utilized to perform processings safely.

© 2014, IJCSMC All Rights Reserved

F. MD5

(Message-Digest algorithm 5), a broadly utilized cryptographic hash capacity with a 128-bit hash worth, forms a variable-length message into an altered length yield of 128 bits. The information message is split up into pieces of 512-bit squares . the message is cushioned with the goal that its length is separable by 512.

In this sender utilize people in general key of the beneficiary to encode the message and recipient utilize its private key to decode the message.

G. RSA

is a calculation for open key cryptography, includes an open key and a private key. People in general key might be known to everybody and is utilized for scrambling messages. Messages encoded with people in general key must be decoded utilizing the private key. client information incorporate encryption preceding stockpiling, client verification methodology before capacity or recovery, and building secure channels for information transmission.

XI. CONCLUSION AND FUTURE WORK

cloud computing is changing how data innovation assets and administrations are utilized and oversaw, yet the unrest dependably accompanies new issue, In spite of the fact that Cloud processing might be seen as another marvel which is situated to upset the way we utilize the Web, there is much to be wary about. There are numerous new innovations developing at a quick rate, each with mechanical headway and with the potential of making human's lives simpler. However one must be extremely watchful to comprehend the impediments and security dangers postured in using these innovations. cloud computing is no exemption.

The rise of the cloud and its security

As more and more small businesses adopt cloud software, it’s increasingly likely that users will begin to store data on their own cloud servers and rely less on huge software like Facebook or Dropbox to hold their files.

In future the rise of the cloud and its security base on management and using various algorithms.

REFERENCES

[1] Priyanka Arora, Arun Singh, Himanshu Tyagi ―*Analysis of performance by using security algorithm on cloud network‖ in international conference on Emerging trends in engineering and management* (ICETM2012), 23-24 june, 2012.

[2] ―*"Swamp Computing" a.k.a. Cloud Computing". Web Security Journal.* 2009-12-28. Retrieved 2010-01-25.

[3]""Thunderclouds: Managing SOA-Cloud Risk", Philip Wik". Service Technology Magazine. 2011-10. Retrieved 2011-21-21.

[4] Winkler, Vic. "*Cloud Computing: Virtual Cloud Security Concerns".* Technet Magazine, Microsoft. Retrieved 12 February 2012.

[5] Hickey, Kathleen. "*Dark Cloud: Study finds security risks in virtualization*". Government Security News. Retrieved 12 February 2012.

[6]Winkler, Vic (2011*). Securing the Cloud: Cloud Computer Security Techniques and Tactics*. Waltham, MA USA: Elsevier. pp. 59. ISBN Securing the Cloud Cloud Computer Security Techniques and Tactics.

[7] "*4 Cloud Computing Security Policies You Must Know". CloudComputingSec*. 2011. Retrieved 2011-12-13.

[8] "*Gartner: Seven cloud-computing security risks".* InfoWorld. 2008-07-02. Retrieved 2010-01-25.

© 2014, IJCSMC All Rights Reserved

[9] "*Security Guidance for Critical Areas of Focus in Cloud Computing*". Cloud Security Alliance. 2011. Retrieved 2011-05-04.

[10] "*Cloud Security Front and Center*". Forrester Research. 2009-11-18. Retrieved 2010-01-25.

[11] M. Sudha , Dr.Bandaru Rama Krishna Rao , M. Monica ―*A Comprehensive Approach to Ensure Secure Data Communication in Cloud Environment,‖ in International Journal of Computer Applications* (0975 – 8887) Volume 12– No.8, December 2010.

[12] Leavitt N, 2009*, 'Is Cloud Computing Really Ready for Prime Time?'*,Computer, Vol. 42, pp. 15-20, 2009.

[13] Weinhardt C, Anandasivam A, Blau B, and Stosser J, '*Business Models in the Service World', IT Professional*, vol. 11, pp. 28-33, 2009.

[14] Gens F, 2009,' New IDC IT *Cloud Services Survey: Top Benefits and Challenges',IDC eXchange*, viewed 18 February 2010, from <http://blogs.idc.com/ie/?p=730>.

[15] A Platform Computing Whitepaper, '*Enterprise Cloud Computing:Transforming IT'*, Platform Computing, pp6, viewed 13 March 2010.

[16] Dooley B, 2010, '*Architectural Requirements Of The Hybrid Cloud'*, Information Management Online, viewed 10 February 2010, from <http://www.information management.com/news/hybrid-cloudarchitectural-requirements-10017152-1.html>.

[17] Global Netoptex Incorporated , 2009, *Demystifying the cloud. Important opportunities, crucial choices*, http://www.gni.com, pp 4-14, viewed 13 December 2009.

[18] Lofstrand M, '*The VeriScale Architecture: Elasticity and Efficiency for Private Clouds*", Sun Microsystems, Sun BluePrint, Online, Part No 821-0248-11, Revision 1.1, 09/22/09

[19] Brodkin J, 2008, '*Gartner: Seven cloud-computing security risks*',Infoworld, viewed 13 March 2009, from <http://www.infoworld.com/d/security-central/gartner-seven-cloudcomputing-security-risks-853?page=0,1>

[20] ISO. ISO 7498-2:1989. *Information processing systems- Open Systems Interconnection*. ISO 7498-2

[21] Klems, M, Lenk, A, Nimis, J, Sandholm T and Tai S 2009, '*What's Inside the Cloud? An Architectural Map of the Cloud Landscape',* IEEE Xplore, pp 23-31, viewed 21 June 2009.

[22] Dlamini M T, Eloff M M and Eloff J H P, '*Internet of People, Things and Services – The Convergence of Security, Trust and Privacy'*, 2009.

[23] Balachandra R K, Ramakrishna P V, Dr. Rakshit A, '*Cloud Security Issues'*, 2009 IEEE International Conference on Services Computing, viewed 26 October 2009, pp 517-520.

[24] S. Arnold, 2009,*' Cloud computing and the issue of privacy'*, KM World, vol July/August 2008, www.kmworld.com, viewed 19 August 2009, pp 14-22.

[25] Soghoian C, 2009 *'Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era',* The Berkman Center for Internet & Society Research Publication Series: http://cyber.law.harvard.edu/publications, viewed 22 August 2009.

216] Gruschka N, Iancono LL, Jensen M and Schwenk J, '*On Technical Security Issues in Cloud Computing', '09 IEEE International Conference on Cloud Computing*, pp 110-112, 2009.

[27] Armbrust M, Fox A, Griffith R, Joseph D A, Katz H R, Konwinski A, Lee Gunho, Patterson A D, Rabkin A, Stoica A, Zaharia M, (2009), Above the clouds: *A Berkeley view of Cloud Computing,* UC Berkeley EECS, Feb 2010.