Biometric Encryption & Cloud Computing

Lovely

Professional

University

REVIEW REPORT ON

Biometric encrypted key security and digital signature with RSA

&

Data Security in Cloud Computing

Submitted by

MANISHA RANA (11401860)

JOY BASAK (11402183)

SUBHA SANKAR CHAKRABORTY (11402181)

RAHUL BHARADWAJ(11402242)

KRISHNA KUMAR(11302033)

MEENA KUMARI(11308750)

CHANDAN PATHANIA(11310829)

To

Department of Computer Application

In partial fulfilment of the Requirement for the

Award of the Degree of

Master in Computer Application

Under the guidance of

Mr. Sahil Rampal

May, 2015

CERTIFICATE

This is to certify that **Manisha Rana, Subha Sankar Chakraborty, Joy Basak Krishna Kumar, Rahul Bharadwaj, Meena Kumari and Chandan Pathania** has completed dissertation on **"DATA SECURITIES IN CLOUD COMPUTING" & "Biometric encrypted key security and digital signature with RSA"** under my guidance and supervision. To the best of my knowledge, the present work is the result of his original investigation and study. The dissertation is fit for the submission and the partial fulfilment of the conditions for the award of Master in Computer Application.

Date:

Mr. SAHIL RAMPAL (The Advisor)
Assistant Professor
Lovely School of Computer Applications
Lovely Professional University
Phagwara, Punjab, India

ACKNOWLEDGMENT

We wish to thank to a great many people who helped and supported me during the writing of this thesis. My deepest thanks to the Assistant Professor of Lovely School of Computer Applications **Mr. Sahil Rampal** the advisor of this thesis project, for guiding and correcting various documents of mine with attention and care. He has assisted me throughout the project by His valuable comments on my work regularly and making necessary correction as and when needed. His encouragement and support has made us for continuous progress in the work and completing the thesis project on time.

We also extend my heartfelt thanks to my family and well-wishers who supported mentally for completing this thesis.

Lastly, we offer my regards to all of those who supported me in any respect during the completion of the project.

Date: ……..

MANISHA RANA

Registration Number: 11401860

JOY BASAK

RegistrationNumber: 11402183

SUBHA SANKAR CHAKRABORTY

Registration Number: 11402181

KRISHNA KUMAR

Registration Number: 11302033

MEENA KUMARI

Registration Number: 11308750

CHANDAN PATHANIA

Registration Number: 11310829

RAHUL BHARADWAJ

Registration Number: 11402242

Biometric encrypted key security and digital signature with RSA

Literature Review-

Biometric Encryption is a process that uses a biometric trait to create a cryptographic key which is further use to encrypt data [1].

The key is generated again only if the right biometric sample is provided at the time of authentication. The Biometric Digital key is arbitrarily generated at the time of enrolment of user in data base, so that no one is having information about it. This key is totally independent on the digital biometric key so, it can be updated or changed when needed. The choice for the storage of the biometric encryption template can be a database or it can be stored locally on any device. On verification, the user gives their newly generated biometric sample (which acts as decryption key), which retrieves the same key or password [2].

Biometric Encryption has several advantages:

No need to keep the biometric image or template. The Digital Biometric key is totally independent of biometric thus can easily be changed or updated. Multiple accounts can be controlled by single biometric. There is no need to remember any long Password or generate it again and again. Improved security of individual information and communications. Greater belief, trust, and demand of biometrics by the public.

Major challenges for Biometric Encryption:

- Loss of person’s access over one’s personal data.
- Data matching, supervision and summarizing.
- Centralized storage of biometric passwords poses security risks
- Compliance with privacy and data protection laws.
- Theft, Loss, misuse, abuse and of personal data.
- Fraud using hard copy picture while using face Recognition.

Biometric identifiers are the measurable characteristics that are used to uniquely identify individuals. These are categorized as behavioural and physiological characteristics. Behavioural characteristics are related to the pattern of behaviour of a person. Physiological characteristics are related to the shape or structure of the body. Characteristics which are widely used for the purpose of biometric identification include: **Face, Fingerprint, Hand geometry, Retina, Iris and Voice** etc.

Face recognition has shown improvements in past few years. Face recognition involves uniquely identifying a person on the basis of different properties of their face. Humans can differentiate each other by their own unique faces, but it is not known what are the most important properties used by a human to recognise another human face. That’s why there have been various propositions to characterize and identify human face in a biometric authentication system. Fundamental structure of the face is mostly used for this purpose.

In the last few years face recognition has shown a remarkable improvement in its performance and is widely used in applications, such as data security, image recovery, access control and law enforcement surveillance [3]. This has been possible because face recognition is non-intrusive and convenient [4] when it is compared to other commonly used biometric technologies.

In today’s world rapid and correct verification of individuals has become a necessity and a challenge 6] as well.Use of biometric encryption in deployment of the Face Recognition technology faces privacy and security concerns [6] [7]. Thus it is very challenging to develop a technology that can perform in a real-world environment, and provide significant privacy protection compared to basic facial recognition, without compromising the performance, security and functionality of system.

Many of today’s face recognition systems focus more on privacy and security concerns, meanwhile newer and more accurate ways to detect the face has always been in progress. Like, one of the methods developed, FARO divides the face into relevant regions (left eye, right eye, nose and mouth) and process and code them independently [8]. This method divide face into regions and also yield better performance. There is a need of more robust Face recognition systems to address challenges faced by organisations.

Multimodal Biometrics:

Unimodal biometric systems rely on single source of information for the unique identification of individuals and these are quite vulnerable and face many problems like incorrect data due to sensors or bad conditions, meaningless data from some individuals and spoof attacks [9]. This result in higher false acceptance and false rejection, restricted distinction capability, and reduced constancy.

For biometric identification to be more secure and accurate, more than one type of biometric trait can be used. Multimodal Biometric systems are able to use more than one physiological or behavioural property for recognition. Multimodal systems represent an emerging trend [10] and are more reliable due to use of multiple source of information.

In multimodal biometric systems more than one biometric characteristic are used for identification. Fusion is performed for these biometric characteristics. It involves merging data at different stages. Fusion in multimodal system can occur at 4 modules.

- Sensor module: This is the module to capture data from sensors. A composite biometric characteristic is obtained by combining captured data.
- Feature level fusion: Using fusion algorithm data of different characteristics are pre-processed and composite feature vector is obtained using fusion algorithm, which is the used for categorization.
- Matching score module: Each matching is done individually rather than combining feature vectors, then a matching score is obtained by performing fusion.
- Decision level: In this last results of different modules are combined.

Research shows that many prefer the fusion step at the match score. Also fusion improves over all accuracy, performance, efficiency, constancy, robustness and fault- tolerance of the system.

Advantages of Multimodal biometric systems:

- Accuracy of overall system improved.
- It can detect and prevent spoofing.
- Provides secondary means of identification in case sufficient data is not extracted from a biometric sample.
- More reliable.

Challenges for Multimodal biometric systems:

- The sensor must be consistent and capable of collecting quality images even from a distance under many environmental operations.
- Therefore selecting the best level of fusion will have the direct impact on performance and cost involved in developing a system.
- Information acquired from different sources can be processed either in sequence or parallel and thus it is challenging to decide the processing architecture to be used.

RESEARCH AND ANALYSIS

Abstract – The conventional methods of identification such as passwords, smart cards and personal identification numbers (PINs) can be compromised, stolen or forgotten. Biometric is the only way to uniquely identify an individual and hence used in many applications. The vulnerability of biometric authentication systems to attacks is now a widely accepted fact.

Biometric encryption systems are more secure and are widely used in many information security applications to conceal private keys by using biometric data. Major challenge that these systems face is how to protect private keys from attackers. Integration of biometrics with public key infrastructure using biometric based signature key generation based on iris recognition is secure, convenient, and fast and correctly identifies the person. This paper will explore integration of iris templates with two existing and widely used digital signature algorithm RSA. Problems associated with this is discussed.

1. Introduction

Securities in individual identification have been controlled by methods such as password, PIN, smart card etc. These methods also do not identify a person but some information related to the person. Moreover, these methods can be compromised, stolen or forgotten and is not a secure way to identify individuals. Limitation of such systems have encouraged the use of biometrics [1] to identify individuals. Now, biometrics have made things easier as people do not need to worry about forgetting their PIN or password or carrying identification means such as smarts cards. Biometric is unique to each individual and it is reliable. As biometric identification process provides many advantages over other identification techniques, it has been widely accepted as the method for unique identification of the user. It becomes critically important for biometric identification process to be safe from attacks in application where security is of high importance such as e-commerce.

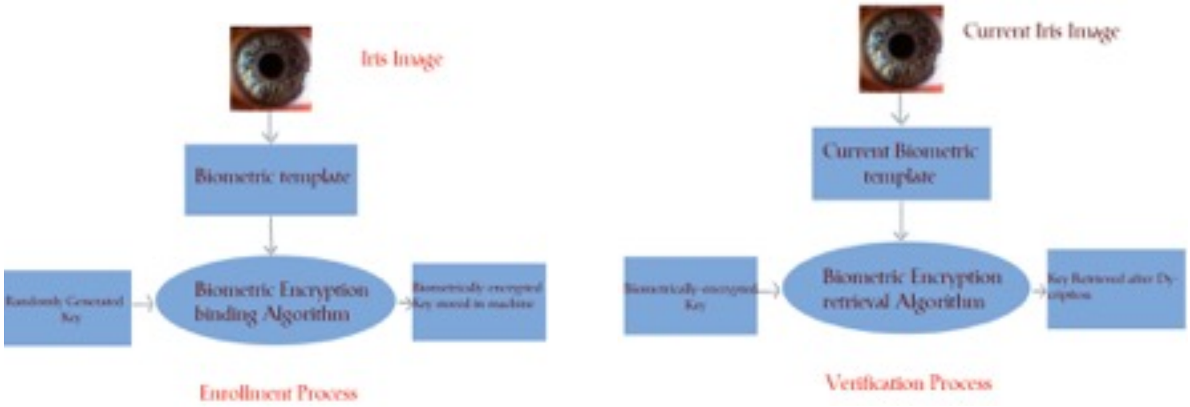
In today’s connected world with easy access to internet, security has become very important [2] and the reason to worry for the biometric authentication process. In the internet world identity theft has become the main threat and uniquely identifying an individual is proved to be their best protection. Secure and accurate user identification mechanism is needed for many applications for accessing sensitive database, storing and transmitting sensitive information etc. Biometric-PKI combination is being researched upon and explored for robust user identification techniques and security. Biometrics can be integrated with public key infrastructure using biometric based signature key generation based on iris recognition for secure, convenient, and fast user identification. Iris recognition itself provides accurate authentication [3] with very low equal error rate. Managing the private keys has remain the main concern with PKI algorithms. They are vulnerable to attacks for information theft. Using biometrics for private key access can resolve this key management concern.

A mechanism to secure the private key and prevent the risk for breach is required. This will prevent the hackers from stealing the private key.

2. Biometrics

A biometric is a unique biological characteristic or trait that can be measured to uniquely identify and recognize the person [4]. Biometrics is associated with the automatic system that analyses these biological characteristics and uses it to identify individuals. Biometrics is emerging and surely is technology that watch for security concerns that comes with it. The acceptance of biometrics has surged as it provides accurate identification of individuals in real time based on biological characteristics.

Biometric identification process involves two stages: enrollment and verification. Enrolment stage involves acquiring the biometric sample. This sample is used to extract unique features to form a biometric template for further comparison purposes.


Iris Image
Biometric template
Randomly Generated Key
Biometric Encryption binding Algorithm
Biometrically encrypted Key stored in machine
Enrollment Process
Current Iris Image
Current Biometric template
Biometrically encrypted Key
Biometric Encryption retrieval Algorithm
Key Retrieved after De-cryption
Verification Process

In the verification stage, new biometric sample is aquired again and unique features are extracted from it. These features are compared with the biometric template generated during the enrolment stage.

As it can accurately identify the users, many application can take full advantage of biometric identification process such as:

1. Boarding passes in case of air travel
2. E-commerce payment systems
3. Authentication for the purpose of government schemes or other organizations
4. Ticketing for events

5. Personal devices access
6. Voting

3. Issues with biometrics

Use of biometrics to uniquely identify individuals do suffer with various issues. For example, attackers creates a threat of accessing bank accounts of other individuals. Such acts of theft and misuse will prompt users for not choosing biometric way for authentication and storage of biometric over the internet. Another problem associated with biometric authentication is that biometric password cannot be changed often [6].

One of the solutions suggested to minimize risk of database template misuse is to use different versions of the biometric iris code (iris pattern after processing and encoding) template-generating algorithm per organization to prevent cross readability of templates between different organizations. Other solution is to use partial disclosure of the user template from client to the server [1]. Using these methods, one still needs to maintain iris code template database.

Biometric authentication system presents various security risks that can be misused such as:

(1) Enabling unauthorized access and misuse of personal information
(2) Facilitating attacks on other systems and
(3) Creating risks to personal safety.

Major concern with PKI algorithms is managing the private keys. If stored on a server, it is susceptible to attacks and can be accessed by hackers. Storing on a smart card is also risky as it may be lost or stolen by a person. Using biometrics is the only solution to securely manage the key. In effort to minimise the risk of theft, generation of RSA keys on distributed servers has been researched upon and getting explored. This makes it difficult for the hacker to attack and misuse data and also ensures that such attacks are minimised.

4. Biometric Encryption

Biometric Encryption is a process to secure the private key [7] by associating a digital key [8] to a biometric or generating a key from the biometric. Private key is encrypted with the biometric and stored as a template such that neither the key nor the biometric can be obtained independently [9] from there. This key again can be decrypted on presenting the correct biometric sample during the verification stage. The whole process of encrypting and decrypting the key is complex as the biometric sample provided may be different each time.

Biometric encryption system has gained wide acceptance as it has some advantage:

1. No need to retain the biometric template.
2. Improved authentication security.
3. The key is completely independent of biometric and it can be easily updated.
4. Improved security of personal data and communications.
5. Single biometric can be used to manage different accounts.
6. Creates Greater trust and confidence in users.

Biometric encryption also faces many challenges in its implementation. Major challenges for Biometric Encryption are:

1. Loss of individual control over one’s personal data.
2. Overhead of Data matching, monitoring and profiling.
3. Significant security risks, especially when there are large centralized databases of biometric passwords.

4. Compliance with privacy and data protection laws.
5. Theft and misuse of personal data.

Confidence in biometric authentication system will depend on the protection it provides to people's privacy and the levels of security it guarantees to systems and processes. Whole system of biometric authentication system, which involves capturing features and comparing with stored template, must be designed with following features:

1. Biological feature should be unique to individuals and universal.
2. It should be difficult to reproduce otherwise.
3. Feature should be invariant and should not change with age or any disease.
4. Characteristics should be easy to capture
5. Characteristics should have enough unique features to distinguish individuals.
6. Feature should be able to be captured from majority of people.
7. Retrieved information should have property for further processing.
8. Characteristics should be difficult to alter and must be reliable.
9. Captured information should have the property to be able to compare with ease.

Robust and reliable security technologies and accurate user identification are required for systems involving communication of personal information such as online transaction. The reason is that biometrics may have been able to replace the need to remember password and carry cards, but it is still can be attacked and misused by hackers. Biometric-PKI combination largely explored to find system with greater security. Security is of prior importance for systems dealing with more critical information. Older methods to secure information by encryption key is no longer effective and are vulnerable to attacks. Biometric encryption provides a secure method for unique identification of individuals. As the password prone to attack and theft, managing the password is the most critical job in any cyptosystem.

5. Use of biometrics for digital signature

Reliable user authentication system is very important in the inline world. Digital signatures, uses cryptography to uniquely identify users and considered to be the technology which is effective in identification. Digital signatures are similar to the hand written signatures, as both attach some information that can be used to uniquely identify the person.

Biometric authentication using iris recognition provides higher performance with very low equal error rate. Its high precision may allow it to be used as cryptographic key directly. This will allow to directly generate private key for biometric template and can be used with PKI for digital signature. It also eliminates the communication of biometric templates over the internet. Such process of generating digital signature have following advantages:

1. No need to store biometric templates and removes risks associated with it.
2. Unique identification of individuals not the smart card etc.
3. Improves confidentiality hence security.
4. Elimination of need to transfer over internet reduces risk of attack.

Digital signature is term which is used to relate a data string which binds a digital information with a particular individual. It is gaining popularity in many information security applications like user authentication, information integrity. Automatic user identification has been considered the most acceptable use of biometrics. Digital signature in a way, can be related to a biometric signature that can be validated by comparing to a real signature. Applying biometrics for digital signature is difficult due to its inaccuracy and threat to attacks. Using biometrics for digital signature is getting explored few processes has already been established.

Digital signature can uniquely identify individuals and it uses a one-way and asymmetric function along with the person's private key for this purpose. For the communication between two parties, a public and private key pair is generated. Public key is used to decode the document digitally signed by person's private key. So for secure communication, sharing the public key is necessary. In the process, communication can be intervened or disrupted due to some act of hacking. Digital signatures can overcome this problem. It performs a one-way asymmetric hash function on the data for communication. Result if this is a function of the data for communication and once this data changes, the result will also change. Result is decrypted with the private key of sender. Now the receiver can identify the validity of data by successfully decrypting it. Receiver also applies one way function like the sender and verifies the validity of data by comparing the result with decrypted message. This way digital signature proved to be a trusted player in such communication and the real identification of persons.

For accurate biometric digital signature, we need a fast, easy to use and accurate biometric identification technique. Iris recognition allows unique identification with minimum error rate [10].

6. Digital signature using RSA algorithm

Many digital signature technologies has been researched upon and developed. One of such methods RSA is one of the most popular and widely used method [11].

The RSA algorithm [12] follows as:

1. Two large random and prime numbers p and q approximately equal in size are generated, such that their product n=pq results in the bit length (for example 512bits) required.
2. Modulus n=pq is computed.
3. Euler totient function, $\text{Ø}(n) = (p-1)(q-1)$ is computed
4. We choose an integer e (encryption exponent), $1<e< \text{Ø}(n)$, so that the greatest common diviser, gcd(e, Ø(n)=1 or e and Ø(n) are coprime.
5. Now compute d (decryption exponent) as $d \equiv e-1 \pmod{\text{Ø}(n)}$.
6. Public key is (e,n).
7. Private key is (d,n).

Private exponent d, must be kept secret. p, q, and Ø(n) must also be kept secret.

8. **Encryption:**
   - Obtain public key (e,n).
   - Compute message as a integer m, such that $0 \leq m<n$.
   - Compute cipher text $c= m^e \bmod n$.
9. **Decryption:**
   - Use private key (d,n)
   - Extract m from c as, $m=c^d \bmod n$.
   - Extract original message from m.

We can use RSA algorithm along with 512 byte iris template to generate a private key by equating the closest number which is relatively prime with Euler totient function, Ø(n) and using it as the decryption exponent, d.

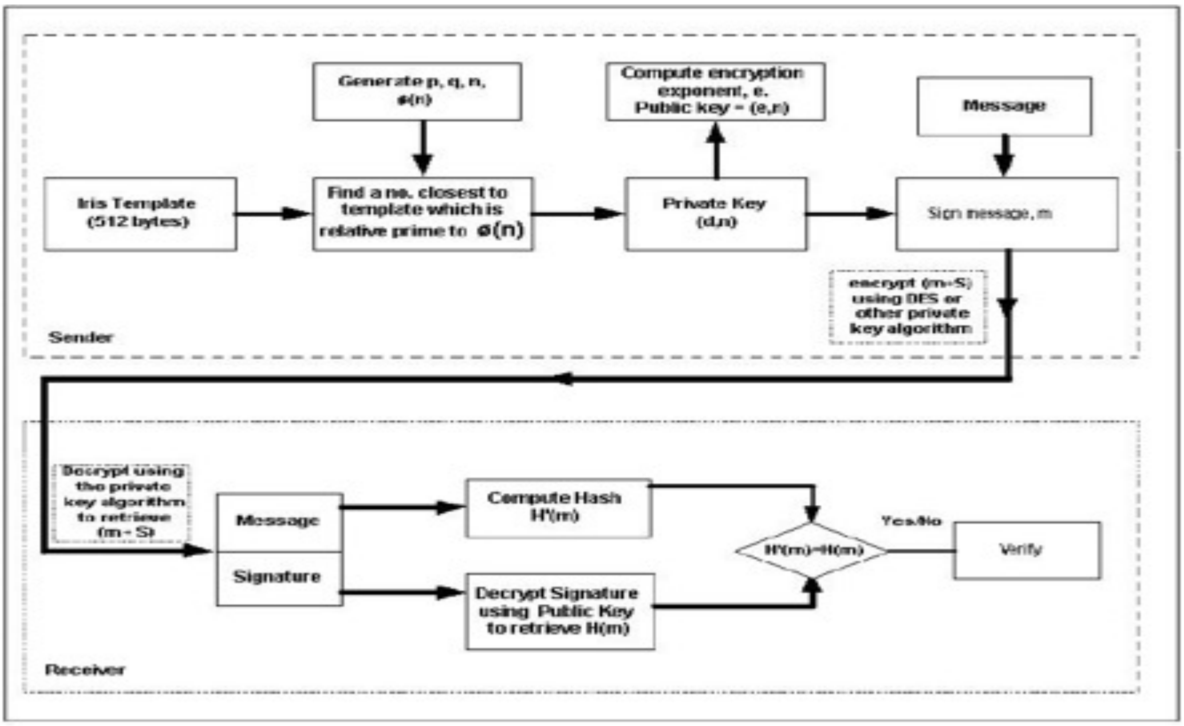

Generate p, q, n, ø(n)
Compute encryption exponent, e. Public key = (e,n)
Message
Iris Template (512 bytes)
Find a no. closest to template which is relative prime to ø(n)
Private Key (d,n)
Sign message, m
encrypt (m+S) using DES or other private key algorithm
Sender
Decrypt using the private key algorithm to retrieve (m - S)
Message
Signature
Compute Hash H'(m)
Decrypt Signature using Public Key to retrieve H(m)
H'(m)=H(m)
Yes/No
Verify
Receiver

Fig. Digital signature using RSA algorithm

In this method private key is generated when the iris sample is provided before the camera and combined with Euler totient function.

7. Finding

Generating biometric digital signature with RSA algorithm has a major problem with it. Template size used in this method is large (512 bytes) and the generated key will be even larger. This large size associated with the method will increase the computation time. This process can be made faster by using a 128 byte template using function that will generate unique iris template.

8. Conclusion

Biometric authentication using iris recognition provides higher performance with very low equal error rate. Its high precision may allow it to be used as cryptographic key directly. This will allow to directly generate private key for biometric template and can be used with PKI for digital signature. RSA algorithm is commonly used to generate this digital signature. This process can be made faster by making the template size down to 128 bytes.

REFERENCES:

[1] Sim Hiew Moi, Puteh Saad, Nazeema Abd Rahim, Subariah Ibrahim, “ERROR CORRECTION ON IRIS BIOMETRIC TEMPLATE USING REED SOLOMON CODES” Department of Software Engineering, Department of System & Communication, Faculty of Computer Science And Information System, Universiti Teknologi, Malaysia Johor, Malaysia, 2010 Fourth Asia International Conference on Mathematical/Analytical Modelling and Computer Simulation.

[2] M Y SIYAL, “A BIOMETRIC BASED E-SECURITY SYSTEM FOR INTERNET-BASED APPLICATIONS” School of EEE, Information Engineering Division
Nanyang Technological University
SINGAPORE 639798.

[3] “Iris Recognition - How it works,” http://www.iriscan.com/.

[4] Colin Soutar, Danny Roberge, Alex Stoianov, Rene Gilroy, and B.V.K. Vijaya Kumar, “Biometric Encryption” Bioscrypt Inc. (formerly Mytec Technologies Inc.), 5450 Explorer Drive, Suite 500
Mississauga, ONT

[5] Simon Liu, Mark Silverman, “A Practical Guide to Biometric Security Technology,” IT Professional, http://computer.org, Jan, 2001.

[6] Ari Juels, Martin Wattenberg, “A Fuzzy Commitment Scheme,” ACM CCS’99.

[7] Ann Cavoukian and Alex Stoianov, “Biometric Encryption Chapter from the Encyclopedia of Biometrics” Office of the Information and Privacy Commissioner, Toronto, Ontario, Canada.

[8] Dr. George Tomko, OECD Report on Biometric-Based Technologies, Directorate for Science, Technology and Industry, Committee for Information, Computer and Communications Policy , 2004.

[9] Ann Cavoukian, Max Snijder, “The Relevance of Untraceable Biometrics and Biometric Encryption: A Discussion of Biometrics for Authentication Purposes” Information and Privacy Commissioner Ontario, Canada, August 2009.

[10] Wildes, R.P., Iris Recognition: An Emerging Biometric Technology, Proceedings of the IEEE, vol. 85, No. 9, September 1997.

[11] D. Boneh, “Twenty years of attacks on the RSA cryptosystem,” Notices of the American Mathematical Society (AMS), vol. 46, no. 2, pp.203-213, 1999.

[12]http://en.wikipedia.org/wiki/RSA_(cryptosystem) ,http://www.dimgt.com.au/rsa_alg.html

Data Security in Cloud Computing

INTRODUCTION

When we store our photos online instead of on our home machine, or usage webmail or a long range interpersonal correspondence site, we are using a "Distributed computing" organization. If we are an affiliation, and we have to use, for example, a web invoicing organization rather than redesiging the in-house one we have been using for quite a while, that web invoicing organization is a "Distributed computing" organization. Conveyed figuring insinuates the movement of preparing resources over the Internet. Instead of keeping data in solitude hard commute or overhauling applications for your needs, we use an organization over the Internet, at a substitute territory, to store our information or use its applications. Doing as such may offer move to certain security recommendations.

Distributed computing is the movement of preparing organizations over the Internet. Cloud organizations license individuals and associations to use programming and hardware that are directed by outcasts at remote zones. Tests of cloud organizations fuse online archive stockpiling, long range interpersonal correspondence areas, webmail, and online business applications. The dispersed figuring model licenses access to information and machine resources from wherever that a framework affiliation is open. Distributed computing gives a conferred pool of advantages, including data storage space, frameworks, machine changing force, and particular corporate and customer applications. The accompanying meaning of distributed computing has been produced by the U.S. National Institute of Standards and Technology (NIST): *"Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models."*

Cloud administrations are well known on the grounds that they can decrease the expense and multifaceted nature of owning and working PCs and systems. Since cloud clients don't need to put resources into data innovation base, buy equipment, or purchase programming licenses, the advantages are low in advance expenses, quick quantifiable profit, fast arrangement, customization, adaptable utilization, and arrangements that can make utilization of new developments. Also, cloud suppliers that have spent significant time in a specific region, (for example, email) can bring propelled administrations that a solitary organization may not have the capacity to manage the cost of or create.

Some different advantages to clients incorporate versatility, unwavering quality, and productivity. Adaptability implies that distributed computing offers boundless transforming and stockpiling limit. The cloud is solid in that it empowers access to applications and records anyplace on the planet by means of the Internet. Distributed computing is regularly viewed as productive on the grounds that it permits associations to free up assets to concentrate on development and item advancement.

Objectives

- Present cloud issues/characteristics that create security problems
- Identify a few security issues within this framework
- Propose some approaches to addressing these issues

– Preliminary ideas to think about

Methodology

At an uncommon pace, Cloud registering has at the same time changed business government, and made new security challenges. The change of the cloud organization model passes on business-supporting designing more viably than at some other time. The development from server to organization based believing is changing the way building workplaces consider, arrangement, and pass on figuring advancement and applications. Yet these advances have made new security vulnerabilities, including security issues whose full impact is even now creating. Among the most essential security perils associated with dispersed registering is the affinity to evade information designing (IT) divisions and information officers. But moving to cloud propels just is sensible and fast, doing as such undermines vital business-level security courses of action, routines, and best practices. Without these rules, associations are unprotected against security cracks that can quickly erase any increases did by the change to Saas. Seeing both the surety of disseminated processing, and the threats joined with it, the Cloud Security Alliance (CSA) has led the making of wide gages for practical cloud security. Of late, CSA released the "Security Guidance for Critical Areas in Cloud Computing" and the "Security as an issue Implementation Guidance." These records have quickly transformed into the business standard rundown of best practices to secure appropriated figuring, altogether keeping an eye on this inside the thirteen regions of CSA Guidance and ten groupings of organization joined with the Secaas Implementation Guidance game plan. Successfully, various associations, affiliations, and governments have combined this course into their cloud techniques. In any case, CSA sees that a central piece of managing risks in dispersed figuring is to appreciate the method for security perils.The purpose of the **“The Notorious Nine: Cloud Computing Top Threats in 2013” [14]** report is to furnish associations with a breakthrough, master educated understanding of cloud security dangers so as to make taught hazard administration choices in regards to cloud appropriation systems. The top dangers report reflects the current agreement among specialists about the most noteworthy dangers to cloud security. While there are numerous vulnerabilities to cloud security, this report concentrate on dangers particularly identified with the imparted, on-interest nature of distributed computing. To recognize the top dangers, CSA directed a review of industry masters to incorporate proficient conclusion on the best vulnerabilities inside distributed computing. The Top Threats working gathering utilized these review comes about close by their mastery to art the last 2013 report. The overview procedure approved that the risk posting reflects the most present concerns of the business. In this latest release of this report, specialists recognized the accompanying nine basic dangers to cloud security (positioned in place of seriousness):

1. Data Breaches
2. Data Loss
3. Account Hijacking
4. Insecure APIs
5. Denial of Service
6. Malicious Insiders
7. Abuse of Cloud Services
8. Insufficient Due Diligence
9. Shared Technology Issues

LITERATURE REVIEW

While there are advantages, there are security and security concerns as well. Information is going over the Internet and is put away in remote areas. Moreover, cloud suppliers frequently serve different clients all the while. The greater part of this may raise the scale of introduction to conceivable breaks, both incidental and intentional.

Concerns have been raised by numerous that distributed computing may prompt "capacity creep" — employments of information by cloud suppliers that were not foreseen when the data was initially gathered and for which assent has regularly not been gotten. Given that it is so cheap to keep information, there is minimal motivating force to expel the data from the cloud and more motivations to discover different things to do with it.

Security issues, the need to isolate information when managing suppliers that serve various clients, potential optional employments of the information these are territories that associations ought to remember when considering a cloud supplier and when arranging contracts or exploring terms of administration with a cloud supplier. Given that the association exchanging this data to the supplier is eventually responsible for its insurance, it needs to guarantee that the individual data is proper taken care of.

“**Mr.wei Liu et al** told about the enormous information issue in their Security-mindful middle of the road information arrangement method paper". Monstrous processing force and capacity limit of distributed computing frameworks permit conveying information concentrated applications without the framework speculation; this huge information issue additionally presents a lot of people new difficulties for information security when the clients outsource delicate information for imparting on the cloud servers, which are not inside the same trusted space as the information managers. This test is further muddled by the security obligations on the potential delicate information for the experimental work processes in the cloud. Presently the greater part of the application is utilized the idea of Grid processing. Since it can offer high computational limit and huge stockpiling. Be that as it may they recognized the favorable circumstances of distributed computing over the matrix registering. They likewise propose the idea of distributed computing.

The developing pattern towards distributed computing has incited new information administration frameworks, for example, Google File System and Hadoop. These frameworks go about as information stockpiling foundations in cloud that additionally give some fundamental information administration capacities, e.g. unapproved access, information piece stockpiling, and fiasco recuperation. The innovations in enormous information administration have turned into a vital issue [1].

"**Diogo A. B. Fernandez et al** take a survey and point out the works on cloud security issues, making a comprehensive review of the literature on the subject. They told their paper that Distributed computing is these days commanded by an extensive number of difficulties. Because of its fast development and on the grounds that virtualization is a moderately new engineering, a blast of security issues have been found and mulled over by both the educated community and industry. Cybercriminals take after patterns, and distributed computing unquestionably does not get away from that course. Cybercrime is progressively getting to be more advanced. Vindictive performing artists collaborate and structure malware sequential construction systems, on which everyone has a particular errand, such as composing the malware, characterize spam strategies, outline a social building part, et cetera. The undertaking system security is at present under very unpredictable conditions, and the security scene gets darker when stirring up cloud situations with the rate of the expanding and enhanced digital guiltiness [2].

O. M. Fal'a and V. F. Kozak told about the "PERSONAL DATA PROTECTION PROBLEMS ASSOCIATED WITH CLOUD COMPUTING" in their paper. In their paper they point out that Cloud computing is analyzed from the viewpoint of personal data protection. Recommendations for cloud providers and cloud customers on implementing the principles of personal data processing are considered. A few procurements of the undertaking of a worldwide standard on the insurance of individual information in the distributed computing are figured. The issue of insurance of individual information gets to be progressively topical particularly regarding various productions finding certainties of illicit utilization of this information. In Ukraine, different exploratory specialized exercises are given at the present time which inquiries of individual information assurance and disadvantages of the precise materials gave to individual information security are considered [3].

Cloud computing service is widely used not only to manage the users' IT resources, but also to use enterprise IT resources in an effective manner. Various security threats have occurred while using cloud computing and plans for reaction are much needed, "**An Na Kang et al**" told the security problem which is faced in a enterprise IT resources. In their paper, they will also eventually elevate to security threats to enterprise information. They also work on Virtualization techniques that how this technology effects the cloud servers. Because the virtualization technology totally work on distributed server. So there is a conceivable risk that information would be lost or the nature of information will be low when it achieves its goal server. They told their paper that "Distributed computing is focused around virtualization engineering and it is utilized to impart IT assets, for example, server, stockpiling, and SW through the Internet. Keeping in mind the end goal to utilize virtualization engineering, hypervisor is utilized to convey and exchange information among the virtual machines. Shortcomings of virtualization uncovered distributed computing environment to numerous security dangers, for example, Information spillage from conferring data, administration impediments because of offering and incorporating assets, challenges in applying insurance in view of circulated transforming, and legitimate issues [4].

As we all realize that Distributed computing is the nearing new period of data handling and has demonstrated its advantages in high versatility and useful differing qualities. Be that as it may, practically all distributed computing architectures including Saas, Paas, and Iaas are powerless against genuine security issues. Additionally, Portable Distributed computing (MCC) is key to overcoming versatile restricted stockpiling and processing capacities. **Taeshik Shon et al told about "Advanced Mobile Cloud Computing for the Internet of Things: Current Issues" in their paper**.They describe that "*MCC authentication and authorization issues must be provided on two levels: login password control and the environment from where the cloud is accessed. MCC has overcome the barrier of limited storage by providing remote storage but requires a strict security system that is responsible for retrievability, integrity, and seamless storage access. Elasticity and connectivity are also of major concern in MCC because delays and jitters cause degradation in the user experience*". Distributed computing structural engineering makes more difficulties in keeping up security due to the freedom of clients to pick any MCC construction modeling. They talk about present distributed computing issues and future bearings. The center of this paper is on the o`pen difficulties that MCC is confronting and the conceivable arrangement inside a certain nature of administration. Accordingly, this paper has introduced the security issues through six conceivable spaces from client verification and capacity administration to MCC building design and connectivity. They additionally concentrate on which Cloud Security Alliance (CSA) portrays the current cloud environment issues [5]

"(1) Abuse and Nefarious Use of Cloud Computing
(2) Insecure Application Programming Interfaces
(3) Malicious Insiders
(4) Shared Technology Vulnerabilities
(5) Data Loss/Leakage
(6) Account, Service & Traffic Hijacking
(7)Unknown Risk Profile

Cloud computing has become a hot topic both in research and in industry and when making decisions on deploying/adopting cloud computing related solutions, security has always been a major concern. **Gansen Zhao et al summarizes security related issues in cloud computing in their articles**.They told their paper that The security worries that clients may have when embracing distributed computing, including flaw resistance and administration accessibility, information movement, and information privacy and trustworthiness. the ramifications of distributed computing administration models in connection to specialized, lawful and moral issues for overseeing dangers emerging from malware and digital assaults. Various information security and information protection vulnerabilities have been recognized and the suggestions for associations choosing these cloud administration models identified.they additionally proposed that distributed computing related security can be ordered into three classes: distributed computing security, security for distributed computing, and distributed computing for security [6] .

Distributed computing security alludes to the security of a distributed computing framework's foundation that ensures framework privacy, respectability, and accessibility [6].

Security for distributed computing alludes to the trust on the administrations that clients appreciate when the clients work with the administrations conveyed utilizing distributed computing innovation [6].

Distributed computing for security includes utilizing distributed computing advances to create and convey security answers for IT frameworks [6].

‘Cloud computing 'build, challenges in keeping up information security and information protection have additionally been perceived as critical vulnerabilities. These vulnerabilities create a scope of inquiries identifying with the limit of associations depending on cloud answers for adequately oversee hazard. This has ended up especially the case as the dangers confronted by associations have moved progressively far from random malware to more focused on digital assault apparatuses. From measurable registering viewpoint it has likewise been perceived that 'cloud arrangements' posture extra difficulties for legal processing pros including discoverability and chain of confirmation. In any case, to date there has been little attention of how the contrasts between random malware and focused on digital assault instruments further problematize the limit of associations to oversee hazard. **Vlasti Broucek & Paul Turner has commenced a discussion in their paper on the implications of cloud computing service models in relation to technical, legal and ethical issues for managing risks arising from malware and cyber-attacks**.They told their paper that Various information security and information protection vulnerabilities have been distinguished and the suggestions for associations choosing these cloud administration models recognized. The paper has additionally attempted to highlight how these ramifications change along a continuum of advancement in connection to the nature, extension and scale of the assault from random malware to focused on digital assault devices. The paper has additionally talked about how 'cloud arrangements' stance extra difficulties for criminological registering pros including discoverability and chain of proof. At the point when things do happen and mischief is brought about, there may be constrained choices for specialized, legitimate or even moral reactions open. It is expected that by investigating these dangers and separating between the specialized, lawful and moral predicaments represented, the give their thought to raising authoritative consciousness of the extra dangers confronted by associations choosing to move to cloud arrangements [7].

Ye Du et al. Cloud computing is a guaranteeing registering model that empowers helpful and on-interest system access to an imparted pool of configurable processing assets. The initially offered cloud administration is moving information into the cloud: information managers let cloud administration suppliers have their information on cloud servers and information customers can get to the information from the cloud servers. This new ideal model of information stockpiling administration likewise presents new security challenges, on the grounds that information holders and information servers have distinctive characters and diverse business engages. Thusly, a free inspecting administration is obliged to verify that the information is effectively facilitated in the Cloud [8].

In rundown, focal control of the whole cloud framework is created altogether. What's more, security of individual autonomous assets must be kept up. Consequently, In the instance of offering an open application of restricted assets or the current shutting framework is can be keep up by a patch or enough security arrangement. This is not, in any case, sufficient for a cloud environment. Since wellbeing of the whole framework must take need, an open security structural engineering is needed

Results and Performance evaluation

Pradeep Kumar et al. [9] proposed a plan for security in distributed computing utilizing Hidden Markov model (HMM) and Clustering. This plan performs interruption identification taking into account the likelihood of the conduct. Bunching is utilized for giving just those information that are needed by the client. Bunch gives a smaller perspective of information in cloud environment. It is utilized for extortion recognition and is used to lessen the information looking for time. In [9], HMM model screens the client conduct consistently and illuminates the overseer with the assistance of channel system. Firewall passage is utilized here to piece the SSH administration, which is utilized for obtaining entrance to the server from anyplace on the planet. It just drops the parcels that originate from any IP address which is not inside its learning. It is the obligation of the framework overseer to keep the information safe. The framework chairman quickly makes the move if any pernicious action identified with information mining is distinguished by the channel arrange in the wake of getting info from the HMM. In this plan, the distributed computing environment has a module joined with it. It can help the proposed model to reinforcement and recuperate information if there should be an occurrence of crisis. It can be effectively joined with whatever other cloud environment if necessary. Subsequently, the heap on the servers of a cloud could be minimized. Thus, a gatecrasher can be effortlessly gotten regardless of the fact that he has the stolen ID and/or watchword. This environment has ordered the information into two classes. One class incorporates typical information looking for from the database. Then again, Second classification includes looking for delicate information that must be kept shielded from unauthenticated access.

Palivela Hemant et al. [10] have presented another model framework where a focal server will spare all the data in its switch table that can be valuable for back following the server or client. The switch table contains cloud id, client id, the genuine server id to which the client is uniting, server name, aggregate time of synchronization, bundle size, lease time, source ip and destination ip. It likewise contains the parcels every second exchange rate which is the genuine measure of information stream. There will be application level firewalls which won't just check the undesirable sites taking into account their ip addresses however they will likewise follow along if the bundles are noxious. They can record the exercises of the client. The client side contains individual firewall and the network in the middle of client and the focal server will be encoded utilizing SSL encryption benchmarks. At the point when any client needs to unite with a specific server then his/ her data gets put away in the table. In the event that, the client is not able to associate with the server, the server can be effectively backtracked from the focal server's directing table. A hefty portion of the security necessities are satisfied in this model because of twofold encryption.

Shuai Han et al. [11] proposed an outsider evaluator conspire in distributed computing for guaranteeing information stockpiling security. Outsider evaluator (TPA) gives trustful validation to the client who stores their information in the cloud. TPA is capable than the cloud purchasers and makes each information access be in control. Clients can't totally depend whether their information is safe on the cloud suppliers. TPA can audit and decipher the information put away in the cloud in the interest of the clients upon solicitation. It can give a log report to the clients. The creators have proposed another building design for distributed storage, where the outsider evaluator and the cloud administration supplier have been joined together. The customary system building design [11] comprises of three substances which are clients, Cloud administration supplier and TPA. Clients have vast information records to be put away in the cloud. They are dynamic members and can be singular shoppers or associations. Cloud administration supplier has sufficient storage room and also reckoning assets for keeping up the information put away by the clients. In this plan RSA has been utilized to encode the information stream between servers in the development cloud administration supplier. It utilizes Bilinear Diffie-Hellman calculation for trading keys. Clients and cloud administration supplier can correspond with one another utilizing a message header without an outsider inspector. Each of the distributed storage servers can include, recognize and upgrade the message header for clients whose duplicate will be sent to the trustful association server interestingly. A couple of keys is distributed to every client for getting to the cloud. In this plan, clients include a message header before sending it to the cloud. The information bundles are scrambled with the designated keys utilizing RSA calculation. Trustful association servers which are kept up by trustful association's that execute as a guard dog for each entrance enters in cloud administration supplier, involves couple of number of servers. The clients and cloud administration supplier can't get any verification data from trustful association without a certain module. The Trustful association server is in charge of keeping up all the keys which are put away in distributed storage servers.

As per **Mohammed A. Alzain et al.** [12], moving from single cloud to multi-cloud is imperative for guaranteeing the security of client's information. Creators proposed that, there are three fundamental security components of (information uprightness, information interruption and administration accessibility) that needs to be considered as the significant sympathy toward distributed computing. They have proposed another model called Multi-cloud Database Model (MCDB). A strategy named Shamir's mystery imparting calculation, which is taking into account polynomial introduction has been fused in the plan. As per the calculation, if an information D is imparted into n pieces, in such a path, to the point that D is effortlessly recreate capable from k pieces, however even finish learning of k-1 pieces uncovers truly no data about D. The creators have recommended that Cloud Computing ought not end with a solitary cloud. In their work, they have thought about Amazon cloud administration which is single cloud with their proposed multi-cloud model. This model ensures the security and protection of information in multi-cloud utilizing multi offers strategy rather than single cloud. The information is recreated among a few cloud by utilizing mystery imparting methodology. The operations between the customers and the cloud administration suppliers are controlled by Database Management System (DBMS). Information is being put away by cloud administration suppliers in the wake of being partitioned by MCDB. Division of the information relies on the quantity of cloud administration suppliers.

In 2011 **Mahbub ahmed et al** [13], introduced a system for giving trust and security in SAAS. As indicated by his thought the control over information, client's enlistment, and access to the outsourced information will be under the control of information proprietor. The information proprietor issues a trust ticket for the enlisted client and the information proprietor keeps record of every enrolled client. The information proprietor sends the trustID, client's open key, ability rundown to the CSP. Henceforth the enlisted client when presents the appeal for the CSP and it will be distinguished by the CSP whether he is a substantial client or not. They formulated an algorithmic convention for the sending of an information proprietor produced Trust Ticket. This Trust Ticket is a thought of trust from the point of view of an information proprietor's control over information and an enlisted client. In this component da ta proprietor encodes the information with secret key (KO) and outsources the encoded information to a CSP. An information proprietor offers KO with a client toward the end of that client's enrollment. An information proprietor is the backer and merchant of the Trust Ticket amid a client's enrollment.

Addressed Security Risks	**[10]**	**[9]**	**[12]**	**[13]**	**[11]**
Data Integrity	√	√	√	√	X
Data Intrusion	X	√	√	√	√
Service Availability	√	√	√	√	X
Data Confidentiality	√	√	√	X	√
Non-Repudiation	√	X	X	√	√

Table 1: Various Schemes and their support of features

PROPOSED SOLUTION

In our paper we are proposing a Multi-cloud Database Model (MCDB) which utilizes multi-cloud rather than single cloud administration supplier, for example, in Amazon cloud administration.

Furthermore, it utilizes Shamir's mystery offering way to deal with guarantee security of the put away information in the cloud. Moreover, it embraces a triple particular repetition (TMR) procedure which is a sort of uninvolved equipment excess. In TMR procedure, three indistinguishable modules execute the same errand in parallel. In the event that one of the three models was flawed, the other two models will veil and conceal the aftereffect of the broken module. This system is utilized with successive strategy to enhance the dependability of the framework and multi offers method to enhance the security of the framework. The successive voting technique diminishes the quantity of execution cycles. At the point when the information is isolated by the cloud director, then it will be sent and put away specifically into the cloud. There is no requirement for putting away a duplicate of the client information in the cloud director. It is the capacity of cloud administrator segment to create and figure the polynomial capacities. From there on the premise of larger part voting of the yield comes about that has originated from cloud the flawed cloud inside the super cloud supplier is identified. All the shares from diverse cloud will experience voter inside the cloud chief. The consequence of the voting does not get influenced by the execution of the third cloud's outcome, if two outcomes out of the three cloud were same.

Couple of significant security issues, for example, information respectability, information privacy, administration accessibility and information interruption have been comprehended. In our paper TMR system serves to keep up respectability by distinguishing the accessibility of cloud and it can focus the broken cloud. Information honesty is kept up in [12], in light of the fact that guarantees that, if an information D is isolated into n pieces. Information D must be remade when a sufficient number of shares are consolidated together. That is individual shares are of no utilization all alone. In [4] and [9], information classifiedness is kept up by putting away the information in numerous cloud administration suppliers and cloud separately by utilizing Shamir's mystery imparting methodology [9]. In [12], TMR strategies are utilized to determine the Data Intrusion issues. In this plan, it is anything but difficult to identify the broken cloud and can investigate where the interruption has occurred. Interruption can be anticipated in [4], in light of the fact that if the programmer hacked the secret key from one cloud administration supplier, regardless they need to hack the third cloud administration supplier for its watchword. It is hard for a programmer to recover the secret key from all the cloud administration suppliers. Administration accessibility is ensured in [12] and [11], as the information is conveyed in distinctive cloud administration suppliers and cloud individually. Accordingly, the danger of information misfortune gets minimized. The issue of non- revocation have not been dealt with in the plans

CONCLUSIONS

Information security is an extremely discriminating issue in distributed computing. In cloud information stockpiling framework, clients store their information in the cloud can't have the information by regional standards. Clients are not mindful of the physical area of their information. It is not clear how safe their information is and responsibility for is additionally indistinct when these administrations are utilized. Distributed computing organizations say that the information put away are totally sheltered. Be that as it may, it is too soon to remark on the unwavering quality issues asserted by them. The put away information may experience the ill effects of harm that happens amid information move operations from or to the cloud supplier. Information are not generally safe when they are put away inside cloud suppliers. For tending to these issues a few calculations have as of now been proposed and there is a colossal extension for work in the range of information security in distributed computing.

REFERENCES

1 Security-aware intermediate data placement strategy in scientific cloud workflows
Wei Liu · Su Peng · Wei Du · Wei Wang ·Guo Sun Zeng
2) Security issues in cloud environments: a survey
Diogo A. B. Fernandes · Liliana F. B. Soares · João V. Gomes ·
Mário M. Freire · Pedro R. M. Inácio
3) PERSONAL DATA PROTECTION PROBLEMS ASSOCIATED WITH CLOUD COMPUTING
O. M. Fal'a and V. F. Kozak
4) A strengthening plan for enterprise information security based on cloud computing
An Na Kang · Leonard Barolli · Jong Hyuk Park ·Young-Sik Jeong
5) Toward Advanced Mobile Cloud Computing for the Internet of Things: Current Issues and Future Direction
Taeshik Shon & Jaeik Cho & Kyusunk Han & Hyohyun Choi
6) Reference deployment models for eliminating user concerns on cloud security
Gansen Zhao · Chunming Rong ·Martin Gilje Jaatun · Frode Eika Sandnes
7) Technical, legal and ethical dilemmas: distinguishing risks arising from malware and cyber-attack tools in the 'cloud'—a forensic computing perspective
Vlasti Broucek · Paul Turner
8) Research on a security mechanism for cloud computing based on virtualization
Ye Du · Ruhui Zhang · Meihong Li
9)Pradeep Kumar, Nitin, Vivek Sehgal, Kinjal Shah, Shiv hankar Prasad Shukla and Durg Singh Chauhan, "A Novel approach for Security in cloud computing using Hidden Markov model and Clustering", *Proc. of Information & Communication Technologies (WICT)*, pp. 810-815, 2011.
10) Palivela Hemant, Nitin.P.Chawande, Avinash Sonule,
Hemant Wani. "Development of servers in cloud computing to solve issues related to Security and Backup", *Proc. of IEEE international Conference on Cloud Computing & Intelligence Systems (CCIS),* pp. 158-163, 2011.
11) Ian Foster, Yong Zhao, Ioan Raicu and Shiyong Lu, "Cloud Computing and Grid computing 360-Degree Compared", Grid Computing Environments Workshop, 2008, GCE'08 , pp. 1-10,2008.
12) Mohammed A. Alzain, Ben Soh and Eric Pardede, "MCDB: Using Multi Clouds to ensure Security in Cloud Computing", Proc. of the 2011 IEEE 9th
13) Mahbub Ahmed, Yang Xiang,Trust Ticket Deployment: A Notion of a Data Owner's Trust in Cloud Computing, IEEE 2011.
14) The Notorious Nine Cloud Computing Top Threats in 2013