SURVEY ON SECURITY MECHANISM TO VALIDATE THE USERS IN CLOUD COMPUTITNG

R.Manjupargavi
Research Scholar
Dept.of Computer Science
STET women' s College
Mannargudi
mprithishni5@gmail.com

Dr.M.V.Srinath
Research Advisor
Dept.of Computer Science
STET women' s College
Mannargudi
sri_induja@rediffmail.com

Abstract

Most of the organizations are utilizing cloud computing to store their enormous information whereas cloud has performed as both server and Data Center (DC) which is placed at various locations and usage of applications from the users as pay-on-service with assistance of internet. It offers various services to Cloud Users (CU) via Cloud Service Providers (CSP) which isbased on Internet-based computing model. The major purpose for utilizing cloud is to access and store the information available in the cloud from anywhere and anytime. Therefore, the handling of physical storage space and software need not be worried from cloud user due to these reasons most of the users aretransferring their data on the cloud. One of the mainissues faced in the CC is based on security because of stored data present over cloud is indirectly managed by the service provider. There are several possibilities of unauthorized user to access or change the data while sending over internet. Therefore, this paper has completely focused on analyzing and identifying the issues due to cloud security can be able to resolve using different cryptographic algorithm which performs as a solution for security in cloud environment. It is also identified the numerous biometric fingerprint authentication technologies and described meritsand demerits in CC.

Keywords: Security Mechanism, Cloud Computing (CC), encryption, cryptographic

1. Introduction

Cloud computing is provided with lot of benefits like various dissimilar technological services and based on instances it is understood that cloud

environment can store a large amount of data. In addition, this platform has assisted in resolving an essential issue ,resource limitation and also reduced the service cost by distributing valuable resources to several users. Reliability and availability of services involves the platform which should be strong against safety threats [1].Cloud security is one of the most important subjects for CC research at current decade. Such investigations include security protection of data storage, protection of the network and security of the applications. A CC model has to empower convenient, resource pooling, omnipresent and provided with various types of CSP interface.Pay as You Go (PAYG) is followed with set of procedure for CC in which the clients simply paid for the software they use.According to the customer demands, PAYG model allows end user whichhas ability to computing resources, infrastructure, customize software and storage. Such advantages are the reason the scientific community has devoted a great deal of attention to this state-of - the-art concept [2].

In general, there are three basic modes of services available in CCwhich is discussed as follows:SaaS paradigm highlights the access management functions in systems such as security controls e.g.an individual can only access such details from apps. Currently, SaaS is sold by organizations such as Google, Dropbox, Microsoft Office 365, etc.In the PaaS model, the customer builds on the network provider which creates with their own programs. PaaS simply provides a combination of application server and OS such as, Google App Engine, Microsoft Azure, LAMP framework etc. This is interesting that one of the PaaS model's key priorities is data security. This storage as service has become essentially significant. This should be noted when this model can encrypt data but it should be mindful of regulatory problems and while being processed on a third-party network which may enforce the quality of data in different geographies. IaaS delivers processing and basic infrastructure resources as unified operation across the network. The fundamental virtualization approach is to organize and separate autonomous Virtual Machines (VM) and segregate it from general hardware and VMs.IaaS also focuses on firewall, VM control, intrusion detection and avoidance (IDS / IPS).CC is growing tremendously and exponentially also it is gradually being embraced by more and more companies every day. There are also related security problems that needs to be discussed.When sending their data to distant destinations, companies pick out certain reliable infrastructures. In this way, each client will usually use their own network software [4].

As discussed above, it provides more than conventional IT models but CC security issues remains a big challenge for its acceptance from the customer'sperspective [3]. Consumers are not willing to place their precious data in the cloud; their network feels more secure than cloud technology.Holding information causes uncertainty over the confidentiality, security, abuse of knowledge in an open network.The majority of users are not aware of the compliance controls, cloud operations, etc.Security is the main problem of CCadoption [5].This paper explores surveying numerous cryptographic and encryption algorithms based on techniques ofCC data security that are necessary to address issues in data security of cloud.

2. Security based challenges in CC

CC is an evolving computing model which carries with its significant amount of new data security issues, access management, etc. [6].several study papers have concentrated on the security issues present in the CC over past decade. Additionally, it is evident that many of the reviewed papers addressed a critical role in cloud security challenges and several significant and detailed studies in this field consists of such notable reviewed works.

Sgandurra and Lupu[7] provided a taxonomy of attacks on virtualized environments at the different stages, goals and source of the attackers. In this case, the main focus is to discuss an evolution of threats, associated security and perceptions of trust in virtual systems at various levels including hardware, Software and application.

Kaur and Singh[8] offered an analysis of the security problems of CC. This research has addressed the issues of location, storage, reliability, availability and quality of data. This research work specifically focuses on one of the main security problems, but it is important to remember that the researcher simply tackle security issues without addressing potential solutions.

Kumar et.al [9] explained different forms of cloud storage data protection concerns and correspondingly proposed an approach which can resolve security problems in an environment of multi-tenant. The paper primarily focuses solely on data protection problems and also provides strategies for preserving the data and its privacy.

Khalil et.al [10] offer a summary of the security and privacy issues of CC. Different categories of established vulnerability risks and attacks are listed in this study, and various forms of cloud vulnerabilities are often defined. In addition, this analysis research examines the drawbacks of the existing approaches and explores potential opportunities for security.

Bashir and Haider[11] discussed to determine the most security vulnerable threats in CC. In addition, this analysis research addresses core security risks associated with cloud storage from both end-users and providers by presenting analyzes related to various models and tools for security.
Ryan[12] is proposing research based on securing data approaches that seek to keep data safe from CSP. In addition, this work discusses a browser key conversion mechanism that enables the secrecy service to be delivered by softwareprogram.

3. Security algorithms and principles based on cryptography

Through growing the number of privacy-related businesses, cryptography will contribute to dawn on the integration of CC. CC is the primary level of privacy where cryptography becomes secure and safe storage.Cryptography is used forsecurity for storing the data more secure in order to transform the raw data into unreadable types. Recent studies, cryptography is known as a set of three algorithms namely, symmetric key algorithm, hashing and asymmetric key [13][14].

3.1 Symmetric key algorithms

Symmetric key works on the principle of encryption and decryption. It can be used by single key. This system ensures the users with two channels whereas it allows only for authorization and authentication. These algorithms use only one key to each whereas the key is kept as confidential. The advantage of symmetric key has not computing too much of power and also it operates encryption at very high speed. There are two major types of algorithms namely stream cipher and block cipher. The block cipher input is dependent on the form of symmetric encryption algorithm which can be occupied as a plaintext block with fixed size and also it is added to plaintext block whereas the output block with same size can be obtained as the plaintext block. One bit is translated at a certain time in case of stream cipher. There are few popular CCsymmetric key algorithm which are described as follows [15][16].

A. Advanced Encryption Standard (AES)

AES is one of the major type of symmetry key encryption in cryptography [17]. It ensures there is a secure encryption of the hash code and also the size of block will be 128 bits per node. AES have various algorithmsnamely; initial round-round keys and key extension are added. Each type is replaced by table with one another using round, sub bytes of non-uniform replacement stage. Rows are moved by the process of transposition where a definite number of steps are regularlyprogressed from each row of the state whereas columns are varied by the process of mixing operation on the state columns and adding in 8 of each column with four bytes.

B. Data Encryption Standard (DES)

DES is symmetric key cryptography based on block cipher. DES produces a 64-bit cipher text by taking 64-bit plaintext at the encryption whereas 64-bit plaintext is produced by taking cipher text of 64-bit at the decryption process. The encryption and decryption process are used by same 56-bit cipher key. The encryption method is carried out using two permutations which can be 16 rounds of Fiestel and initial/final transformation. There are various kinds of 48-bit round key uses every round which is created by a predefined algorithm from the cipher key [15].

C. Blowfish Algorithm

Blowfish can be used as DES substitute which falls under symmetric block cipher. It needs 32 to 448 bits variable-length key and making it much easier for exportable and domestic use.Since it has been considerably tested, and as a good encryption algorithm is also called as slowly gaining popularity. It is non-patented and authorized which is obtainable free for all uses [16].

3.2 Asymmetric Key Algorithms

Unlike the symmetric cryptosystem it is fairly a new idea. For encryption and decryption there may be various keys are used. It is a property that sets its scheme apart from symmetric encryption scheme. Through receiver it maintains its own decryption keys which are commonly known as private key. The receiver must create an encryption key, which is referred as public key.

A. Rivest-Shamir-Adleman (RSA)

This is the most commonly used cryptographic key asymmetric algorithm. It uses different size of block data and different size keys [18].Generation of two prime number, encryption and decryption are the three stages which are broadly classified. Today RSA can be used for digital signatures,key exchange or small

data block encryption is used in hundreds of software products [19]. This algorithm is primarily used on an open communication platform to ensure safe communication and authentication.

B. Diffie-Hellman Key Exchange

In this key exchange protocol sender and receiver must have to use an insecure channel to set up a hidden key in their symmetric key network.Alice selects a random integer aE[1;n] which calculates ga to set up a key, correspondingly Bob calculates gb for random bE[1;n] and sends it to Alice.

C. Message-Digest algorithm (MD5- 5)

The commonly used hash function algorithm in cryptography has a message of variable length in a 128-bit fixed-length output. A commonly used hash function algorithm has 128-bit hash value in cryptography which is 128-bit fixed-length output based on message of variable length.

4. TECHNIQUES BASED ON SECURITY IN CLOUD

Encryption may not be the solution for datain the cloud that can maintain assurance in cloud security. This could be achieved while introducing existing security techniques such as encryption, access control, authentication and identification, integrity verification, data masking and secure deletion, all of which are relevant to data security techniques in cloud.

4.1 OTP Validation

In the current situation, several banks offer verification via the One Time Password (OTP) method that has been created randomly and then used to validate the user in cloud when it is system factor authentication for one time. Although it is often used as a multiple authentication factor named for two times authentication.

4.2 Integrity Verification

The integrity of cloud data seems to be only an authorized user can alter or access the cloud data. Simply stated, authentication method of cloud-based data guarantees their data remains unmodified, accurate anddata integrity strategies become Provable Data Prossession (PDP). This methodology guarantees

the quality of cloud data and the Proof of Retrievability (POR) procedure to acquire on a remote server and validate proof ensuring cloud data being stored on the computer by the customer is not altered [20].

4.3 Access Control

Access control implies cloud service, owner can perform any stringent authorization to access their service through cloud and approved user of data holder may access cloud data whereas unauthorized user cannot be secured from alteration or unauthorized disclosure of data due to access control cloud data.

4.4 Secure Deletion

Understanding how far the data is removed from the server is important. In this method, deletion uses different methods such as cleaning, we delete the data until they are reused which provides security at the same time data stored in the media until deletion. This kind of data is distributed frequently for lower classification level and security for accepting prior data is not provided by sanitization [21].

4.5 Data Masking

Masking is a method of protecting and covering intruder or hacker cloud data, but it also guarantees that the information becomes updated for logical but really not specific information. Although people use terms like data de-recognition interchangeably, cleaned up and word describing the confounding mechanism.The masking of data is not just an algorithm but also a compilation of public data. There may be various techniques or approaches used to mask cloud data, most of the companies use Static Data Masking (SDM) to build experiments using outsourced developers in either a separate website or business which are basically the only possible form of masking.In such instances, another replication of the database is needed. Dynamic Data Masking (DDM) offers exposure depending on the organization's role [22].

5. BIOMETRIC FINGERPRINT AUTHENTICATION TECHNIQUE IN CLOUD COMPUTING

Samadhan et.al [35] has suggested a multi-user authentication mechanism using thumb authentication based on cellular automatons. For this scheme the thumb is used to secure cloud storage as authentication.Here the whole fingerprint image

data is collected by the user. The same user will transfer the data to any other device with the same fingerprint image. The researchers suggested a method as User initial thumb authentication is performed to facilitate system administrators.

Single finger biometric scheme suggested by Al-Hamami and AL-Juneidi[36]. This system uses three user preference finger patterns and assigns only digit number in each of these three digits. These are used during app authentication. The elliptical algorithm can be used for encryption of stored images and is processed at the end of the service provider.

IehabALRassan and HananAlShaher [37] have suggested cell phone camera recognition system for fingerprints. This approach talks about how to explain fingerprint recognition can be used to protect smartphone. Now a day, the use of digital camera or web camera as sensor is much less work.It will be very expensive to install different fingerprint scanner or hardware. The proposed method is used to collect a fingerprint image by means of a cell camera to use a fingerprint recognition method.

Wong and Kim[38]Fingerprint relates for an array of elevations and valleys on the finger exteriors which are strongly developed. Twin pattern shapes appear distinct from one another.Vallabhu and satyanarayana[39]discussed during the lifetime of human beings, structures will not change unless there is a notable accident which causes an everlasting scratch. Recognition of fingerprints denotes the mechanized way of assessing the uniqueness of an objectbased on comparing two impressions. Recognition of fingerprints is really common because it is easy to use, an ancient practice and is widely appropriate around the globe. The standardized way of validating a match between two human fingerprints [40] is referred to here.

This technique uses hamami and juneidi[41]fingerprint sensors. They have a scanned finger image. Using fingerprint a unique password is developed whereas CSP database can store fingerprint image and password. After authentication when the customer wishes to use the service again, the sensor detects his/her fingerprint and sent to CSP, where the task of matching by already registered image is completed.

Table.1 illustrates the major issue, techniques, advantages and limitations found in the study.

Table.1 variousmethods to authorize data security in CC

SI.No	Researcher	Challenges	Proposed technique	Advantages	Disadvantages
1.	V. Pant et.al[23]	To challenge problems based on security	Steganography, Cryptography	Providing the security based on image data	Systems are not strong, their capacity to hide data is poor
2.	Yellamma et.al[24]	In order tokeephuge data from unlicensed	RSA	Increaseof high possible data based on security	It is very Slow due to huge computationsmeasured
3.	A. Bhandari et.al[25]	To develop secure framework	RSA, AES	It has better computation time and easy for searching due to indexing.	It is not verified mathematically and time difficulty is not provided
4.	SK. Sood et.al[26]	Users privacy should be confidentiality, Data leakage, etc.	classification based data indexing	Enhanced flexibility than execution and provides good security.	Time taken is more
5.	A. Dhamija et.al[27]	Secure relocation of data	Steganography, Cryptography	Delivers to data as multilayered protection and less expensive app.	Implementation was poor and comparisons not given with other methods
6.	Wang et.al[28]	In order to eliminatethe overhead of heavy computational fine grained data	Substitution encryption, Sluggish re-encryption	Scalability, attaina fine grained-ness andwell-organized data sharing structure	It is not secureby user access privilege from the proxy server and also do not support liability of user secret key.
7.	Rewagad et.al[29]	To protect privacy	AES, Diffie Hellman key exchange	It is tough to crack by providing three way mechanism	More time consuming
8.	N. Surv	To	AES	Quick, versatile,	Too numerous keys to

	et.al[30]	allowconsistency in the system		safe mechanism supporting all data types (audio, text, video, etc)	differentiate.
9.	Somani et.al[31]	cloud storage and data protection are the major challenges	RSA	Increases security of network	Slow approach, not very effective for big data
10.	Prasad et.al[32]	To avoid data leakage and service denial etc.	3D technique	Flexible, able to tackle dynamic network problems	Data'sare accessed easily by unauthorized users
11.	Volker et.al[33]	To maintain the protection goals of the service users	Cloud Networking Service Model	Requires various forms of optimization such as latency reduction or network load	Want to expand infrastructure through auditing methods, service users need more accountability
12.	Sherif et.al[34]	Implementing and evaluating different encryption strategies in cloud security	Various encryption algorithms	To implement cloud security enhancement software	Time taken is more
13.	Samadhan et.al[35]	With its worldwide adoption, the cloud infrastructure idea is how data and applications can be managed and controlled by the customer.	A multi-user authentication system based on automatic mobile phones	The system suggested was compact, reliable and robust	It offers cloud data storage and data recovery in case of data corruption will occur.
14.	Hussein Al [36]	Identification problem in Mobile Cloud	Multi finger biometric system	The system being introduced simple and offers user multiple login choices.	New technology introduces new risks, and since there is no flawless defense.

		Computing (MCC)			
15.	IehabALRassan [37]	Challenges of security threats includesunlicensed resource access, occur in the mobile cloud.	Fingerprint recognition system with mobile phone camera	The procedure suggested is not only effective but also to defend against attacks by injection.	No improper attempts to access data are detected.

This paper providesa study of the different techniques for data protection.The Symmetric encryption algorithms, based on the analysis, are efficient in handling encryption for large volumes of data and efficient data storage speed in the cloud. Through the use of biometric identification framework, the cloud provider's security standard in terms of efficient identification is significantly enhanced. This paper includes numerous techniques of biometric authentication which are proposed for CCsystem by different researchers. The above discussed are possible approaches in depth. The biometric authentication methods from our research offer innovative approaches for authenticating users of cloud computing.

5. Conclusion

In CC data protection has been found to be a difficult task. Based on increase in demand for CC, need for cloud services increases with malicious unauthorized access in cloud have been increased from the user end as well. This paper provided a study of the different techniques for data protection. The analysis has shown clearly that each strategy has its advantages and limitations. The Symmetric encryption algorithms, based on the analysis, are efficient in handling encryption for large volumes of data and efficient data storage speed in the cloud. This technique combines the use of biometrics, one-time pass code and the usual key to validate the user / device at the time of log-on to access the cloud services. It will help them save time and it will come with more reliable results. In addition, the more attention would be paid by integrating various data protection algorithms to highly sensitive data on users.

Reference

[1] Subramanian N and Jeyaraj A,“Recent security challenges in CC”,Computer Electrical Engineering,Vol-71, pg:28–42 Issuse-2,2018.

[2] Xu X, “From CC to cloud manufacturing”, Robot ComputerIntegerManufuringVol:28, issues-1,pg:75–86,2012.

[3] Satyakam Rahul, Sharda, "CC: Advantages and Security Challenges" International Journal of Information and Computation Technology, vol. 03, 2013.
[4] Hamed Tabrizchi and Marjan Kuchaki Rafsanjani, "A Survey on Security Challenges In CC: Issues, Threats, and Solutions",the Journal of Supercomputing, 2020.
[5] NasarulIslam.K.V and Mohamed Riyas.K.V, "Analysis of Various Encryption Algorithms in CC", IJCSMC, Vol. 6, Issue. 7, pg.90 – 97, July 2017.
[6] Yu S, Wang C, Ren K, Lou W, "Achieving secure, scalable, and fine-grained data access control in CC",In: Proceedings of the IEEE INFOCOM,2010.
[7] Sgandurra D and Lupu E, "Evolution of attacks, threat models, and solutions for virtualized systems", ACM Computer Survey vol-48, issues-3, pg-1–38, 2016.
[8] Kaur M and Singh H, "A review of CC security issues", International Journal Advance Engineering Technology, vol- 8, issues: 3, pg: 397–403, 2015.
[9] Kumar PR, Raj PH and Jelciana P, "Exploring data security issues and solutions in CC", Process Computer Science, vol-125, pg: 691–697, 2018.
[10] Khalil I, Khreishah A and Azeem M, "CC security: a survey", Computers, vol-3, issues-1, pg:1–35,2014.
[11] Bashir SF and Haider S, "Security threats in CC", In: Proceedings of the International Conference for Internet Technology and Secured Transactions, pp 214–219, 2011.
[12] Ryan MD, "CC security: the scientific challenge, and a survey of solutions", Journal System Software, vol-86, issues: 9, pg: 2263–2268, 2013.
[13] RashmiNigoti, ManojJhuria and Dr. Shailendra Singh, "A survey of Cryptographic algorithms for CC", International Journal of Emerging Technologies in Computational and Applied Sciences, ISSN (online)-2279-0055, March, 2013.
[14] RishavChatterjee and Sharmistha Roy, "Cryptography in CC: A Basic Approach to Ensure Security in Cloud", International Journal of Engineering Science and Computing, vol-7, ISSUSE-5, 2017.
[15]P. Kumar and V. K. Sharma, "Information security based on steganography & cryptography techniques: A review," International Journal, vol. 4, no. 10, 2014.
[16] Gunavathy.S and Dr.Meena.C, "A Survey: Data Security In Cloud Using Cryptography And Steganography", International Research Journal of Engineering and Technology, Volume: 06 Issue: 05 , May 2019.
[17] BokefodeJayant.D, UbaleSwapnaja A, Pingale Subhash V., KaraneKailash J. , ApateSulabha S, "Developing Secure Cloud Storage System by Applying AES and RSA Cryptography Algorithms with Role bases Access Control Model", International Journal of Computer Applications, Volume 118-No.12, May2015.

[18] ShashiMehrotra Seth, Rajan Mishra, "Comparative Analysis of Encryption Algorithms for Data Communication", IJCST Vol. 2, Issue 2, June 2011.
[19] Aman Kumar, Dr. SudeshJakhar, Mr. Sunil Makkar, "Comparative Analysis between DES and RSA Algorithm's", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 7, ISSN: 2277 128X, July 2012.
[20] G. L. Masala, P Ruiu, E Grosso, "Biometric Authentication and Data Security in CC," Computer. Network. Security. Essentials, pp. 337–353, 2017.
[21]Cloud Codes [online] https://www.cloudcodes.com/blog/ dataprotection-controls-techniques.html (Accessed 20 December 2019).
[22] G.K. Ravikumar "Design of Data Masking Architecture and Analysis of Data Masking Techniques for Testing", International journal of engineering science and Technology, vol. 3, no. 6, pp. 5150-5159, 2011.
[23]V. Pant, J. Prakash, A. Asthana, " Three Step Data Security Model for CC Based on RSA and Steganography Techniques", In International Conference On Green Computing and Internet of Things(ICGCIoT) pg-490-494, IEEE,2015.
[24]Yellamma P, Narasimham C, Sreenivas V, "Data Security In Cloud using RSA", In Computing Communication and Networking Technologies (ICCCNT), Fourth International Conference, july 4,pp. 1-6, IEEE,2013.
[25]D. Das, A. Bhandari, A. Gupta, "A Framework for Data Security and Storage in CC", In International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT), IEEE,2016.
[26]Sandeep K Sood, "A combined approach to ensure data security in CC", Journal of Network and Computer Applications, Elsevier, vol-35, pg-1831-1838, 2012.
[27]V. Dhaka and A. Dhamija ," A Novel Cryptographic and Steganographic Approach for Secure Cloud Data Migration", In International Conference On Green Computing and Internet of Things(ICGCIoT), IEEE, pg.1-6, 2015.
[28]S. Yu, C. Wang, K. Ren, Wenjing Lou, " Achieving Secure, Scalable, and Fine-grained Data Access Control in CC", IEEE INFOCOM,2010.
[29]P. Rewagad, Y. Pawar, "Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in CC," In International Conference on Communication System and Network Technologies (ICCCNT), pg-437-439, IEEE,2013.
[30]N. Surv, B. Wanve, R. Kamble, S. Patil, J. Katti, "Framework for Client Side AES Encryption Techniques in CC", International Advance Computing Conference (IACC), pg-525-528, IEEE,2015.

[31]U. Somani, K. Lakhani, M. Mundra, "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in CC", 1st International Conference on Parallel, Distributed and Grid Computing (PDGC), pg-211-216, IEEE,2010.
[32]P. Prasad, B. Ojha, R. Shahi, R. Lal, "3 Dimensional Security in CC", In Computer Research and Development(ICCRD), IEEE, vol-3,pg-198-208, 2011.
[33]V. fusenig, A. Sharma, "Security Architecture for Cloud Networking", International Conference on Computing, Networking and Communications, CC and Networking Symposium, IEEE,2012.
[34]S. Etriby, E. Meslhy, H. Elkader, "Modern Encryption Techniques for CC Randomness and Performance Testing", In the third International Conference on Communications and Information Technology (ICCIT), 2012.
[35]SamadhanPagar, Vaibhav Gore, DarshanSant and PoojaSatpute, "The Thumb Authentication on Cloud Computing",International Journal ofEngineering Research & Technology(IJERT), ISSN: 2278-0181, Vol. 3 Issue 5, May –2014.
[36]Alaa Hussein Al-Hamami and Jalal Yousef AL-Juneidi,"Secure Mobile Cloud Computing Based-On Fingerprint",World of Computer Science and Information TechnologyJournal (WCSIT), ISSN: 2221-0741, Vol. 5, No. 2, 23-27, 2015.
[37] IehabALRassan and HananAlShaher, "Securing Mobile CloudUsing Finger Print Authentication", International Journal ofNetwork Security & Its Applications (IJNSA), Vol. 5, No. 6,November 2013.
[38] Wong KS and Kim MH, "Towards Biometric-Based Authentication for Cloud Computing", In 2nd International Conference on Cloud Computing and Services Science,2012.
[39] Vallabhu H and Satyanarayana R , "Biometric Authentication as a Service on Cloud: Novel Solution", Int J Soft ComputEng 2: pp-163-165,2012.
[40] Edward Guillen MM and Alfonso L , "Vulnerabilities and Performance Analysisover Fingerprint Biometric Authentication Network",Proc World CongrEngComputSci 2,2012.
[41] Al-hamami H and Al-juneidi JY, "Secure Mobile Cloud Computing Based-On Fingerprint", International Journal of Networks and Applications 5, pp-41-53,2015.