www.ijemr.net ISSN (ONLINE): 2250-0758, ISSN (PRINT): 2394-6962

Vandana Publications
IJEMR

Volume-7, Issue-3, May-June 2017
International Journal of Engineering and Management Research
Page Number: 695-700

Protection and Security Models for Mobile Cloud Computing: A Review

Vishal[1], Bikrampal Kaur[2], Surender Jangra[3]
[1]Research Scholar, CSE-Department, PTU, INDIA
[2]Professor, CSE-Department, CGC, INDIA
[3]Assistant Professor, Department of CS, GTBC, INDIA

ABSTRACT

As mobile cloud computing increases its presence in the corporate sector, more and more business are seeking cloud services by various new applications in every field of human life. Every organization shifted their own business on mobile cloud and provides various facilities in packed environment. IT industries are misusing the comfort of mobile applications by producing many features of clouds to their clients. Mobile cloud computing environment has emanate as one major challenge in this regard is security. Security address as privacy, authentication and trust in mobile cloud computing environment .Many researcher introduces various mechanisms for mobile cloud data security. This paper focus on comparison of various current models for mobile cloud data security.

Keywords-- Mobile Cloud Computing (MCC), Data Owner (downer), Cloud Service Provider (CSP), Location Based Service (LBS)

I. INTRODUCTION

Everyone knows that computer future is related to mobile devices. As all user aware that mobile devices made competition with computers. This is the device not only for just calling, video chat, E-commerce etc. we can do every work which can be done by desktop and laptop. But in this performances of mobile devices can be achieved by mobile cloud environment. Mobile devices have their own issues like small power, low memory, slow processing and data Security. Desktop Cloud applications are different in comparison with mobile applications. Mobile applications are energy efficient in term of security, reliability, privacy. With applications of mobile cloud computing user can get information about real traffic updates with speed detector checks and data related to speed of vehicle forward on the cloud, MCC location based reminder system cloud database also provide near about information of hospitals, ATMs, Banks, Public transportation, restaurants, hotel etc. These all facilities we can achieve through sources of data by third party. Out sourcing of data to the cloud has created an efficacious trend in these days due to ability of inexpensive cloud services. Therefore, the major issues come out in mobile cloud applications is data security.

Paper divided into six sections, paper started with introduction of MCC environment and second section include the design structure of mobile cloud computing, Section three shows rerated work in security of mobile cloud computing environment while section four describes cloud computing concerns and issues which also include the literature survey of various models, approaches used for security of mobile cloud data owners and cloud providers. In section five, the pros and cons of various models are discussed; Section-six describes the conclusion and future work of the existing models.

II. DESIGN STRUCTURE OF MCC

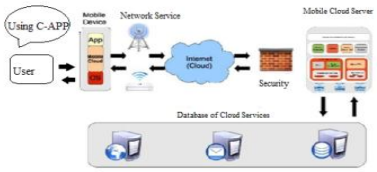

Figure1. Design structure of mobile cloud Environment

User cloud applications in mobile devices connect the link with mobile service provider via BS that establish the connection, control & manage functional interfaces between different networks (wireless access point) and mobiles. Mobile users' requests through the various applications in the mobile and information is transfer to network. System processor is associated with versatile cloud server and giving portable application administrations. The client demands are send to cloud servers by means of Internet servers. The cloud controllers handle the solicitations to offer data to the clients with the relating demand. [15]

III. RERATED WORK IN SECURITY OF MOBILE CLOUD COMPUTING ENVIROMENT

Existing models are based on three categories for mobile cloud computing security.

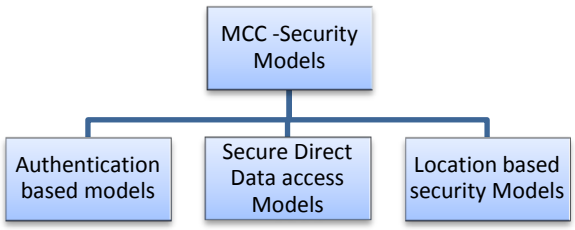

Figure 2. MCC Security Models

Authentication models: Identity based models **Data Access Models**:- Secure resource and allocation methods, Secure data access cryptographic schemes, web referral services methods, secure network channels, data privacy preserving approach, direct data access through attribute based encryption.

Location based security models: Outsourced data based model, group secure framework, Separate PPCCP model, Fine grained access control.

IV. CLOUD COMPUTING CONCERN AND ISSUES

Cloud computing is an on demand service based on personal and business enterprises solutions with provision of information technology in form of virtualization and distributed computing. MCC shared and abstracted resources like hardware, software applications, and database documents files with scalability, flexibility and provisioning parameters. Some other parameter measure the distributed computing execution is coordination, interoperability, openness, dependability, execution, security checked by disconnected and online get to. Different elements and changes secured by CSP Security of cloud measure with sifting, fix administration, risk administration, courses of events reaction to occurrences. Risk involved in MCC are loss of management, separation failure , insecure data protection, unnecessary data deletion, malevolent insider, customer safety aspects, service interface, standard data format, unknown risk profile. HTTP and XML based DOS attacks, traffic hijacking etc.

Today use of context aware (location, identity, activity, time) mobile cloud computing is increased. So that effect can be measured in term of Rabuse and accursed utilization of cloud computing, unprotected interfaces and undefined application descriptions, venomous insiders, data misplacement and leakage descriptions, account or service stolen description, hidden risk profile descriptions. Possible solution for these security issues are a) Cloud-Access Protection by authentication of true user by using OTP (One Time Password) and Biometric information. b) Use an Efficient and Enhanced key Algorithms (Encryption and Decryption).

Need of enhancing the efficiency of secure data access from cloud provider to cloud customer. Data owner or cloud customers choose the service provider on the basis of reputation of cloud provider for confidentiality and integrity which includes timely and effective updates.

This Literature Survey mainly focus on security concerns in mobile cloud computing and cloud computing environment. As it is the hottest fuzz word and has been considered for various types of online solutions. Mobile Cloud computing model leaves the clients naked to different types of attacks and threats. The strategies given beneath have been audited on the premise of security related issues in versatile cloud computing condition. Every one of them have their particular upsides and downsides.. All methods have their own pros & cons. This paper is included detailed description, methodology used and security result achieved by these methods. Some of security models and approaches are given below.

The efficient, secure, privacy preserving approach (ESPPA)*:* This approach utilized probabilistic public key encryption method for reducing calculation burden on data owners. This approach is using rank keyword searching on encrypted information for retrieving the data files back. The analysis on security that shows purpose of approach can be trusted under different interventions by this approach. ESPPA Approach is using probabilistic PKE (public key encryption) and RKS(remote key security). In this scheme, the downer creates an appropriate index for data collection on the basis of word count then encrypts the both index and file[1].ESPPA works in three phases first-setup, second-retrieval, third- integrity verification. First phase involved with algorithms key generation, Index creation, Privacy Preserving and encryption algorithms trapdoor generation, Ranked search Index, Data Decryption.[1] Second phase involved to calculate the performance measurement of proposed ESPPA plan on data set (RFC) request for comments included user and server. The user will be act as downer. In third phase server act as CP (cloud provider) and measurement of this scheme depends upon performance, efficiency in terms of computation costs. Algorithms use MATLAB Libraries and main server works on Linux programming. Syam Kumar Pasupuleti. et.al.[1]

Attribute based data access control*:* This Scheme divided into six sections –present fundamental concepts of identity based encryption proxy re encryption, Role based access control. Discussed concept of ABE (attribute based encryption) and set of descriptive attributes-KP-ABE (Key policy attribute), Cipher Text policy attribute based encryption. Attribute based cryptosystem comprised two components attribute and object. Attribute involves a unique identifying string and its hash (X, H_x) and objects indicate encrypted or recovered database on ABE method. An attribute policy

refers to a specification of as set of attributes and threshold ((as cryptographic operations) that can be used to encrypt an object. An attribute based access control in cloud storage. Attribute based access control by three groups such as Centralized, Decentralized and hierarchical access control (HIDE). A Taxonomy and comparison of attribute based encryption data access and performance of existing attributes based encryption methods measure by parameters cipher text size, private key size, re-keying size, computation and communication cost on the user. Mehdi Sookhak. et.al. [2]

An access control display in view of reputation outline: This component demonstrates a reputation and configuration based dependable control modes (RMTAC) to contribute for security and protection in light of enormous information access. This model includes components of reputation design a) reputation module (RM),b)Vickrey clark groves module (VGC) c) distributed multilevel security computation module(DMSM). Evaluation of direct security level and reputation. performance measurement by simulation OPNET. The simulation area was 1000m*1000m including mobile users network consists of 5 users, use of mesh and cloud networks. Hui. Lin. et.al. [3]

Protection saving stage by utilizing LBS: This system used to encounter horrendous clients and their gadgets by utilizing IMSI (International Mobile Subscriber Identity) number validation. PPCCP is an interface amongst customer and LBS servers. The architecture depends on 128 bit encryption. In beginning substance secret keys is shared by utilizing Diffie-Hellman key exchange algorithm. The propose architecture divided into geographical space into clock regions of the world. PPCCP comprises following three participants (users, cloud based server, LBS provider).Identify two threat communication threat and location privacy threat. Location based services approaches transformation, private information retrieval, cloaking/anonymity. PPCCP (cloud based server) authenticate services by user hash table, region Id -table, computing modules by Euclidean distance formula. Fizza Abbas. et.al. [4]

Secure Framework using LBS: This is a security frame work to access data using location based services. Secure system is an extra layer in process and works with substantial accreditation and personality in the organization. User named as bonafide one. An LBS technique utilizes symmetric and asymmetric key encryption for secure information. Sender makes Geo mapping table maps the position, speed and time (PVT) of the client. AES (Advanced Encryption Standard) calculation is applied before PVT encryption. The end user decrypts the encrypted message using anti spoofing GPS positioning tool. Phases of frame work is created, checked and organized by administrator by user registration and login. The protected correspondence in light of RSA encryption algorithms. The interlopers and unapproved users are recognized in view of authorized number enlisted and refresh in cloud database. Mobile devices suitability checked by polygon restriction qualities and confirmed inside organization. Deepanshu Goyal. et.al. [5]

Enabling Location Based Services in MCC: This plan depends on the outline plan of spatial transient predicate encryption(STP) by methods for proficient, secure, propose integer number comparison scheme(ICS).This conspire primary deliver to obtain protection and security issue by developing area based adaptable access control. Need of new composed cryptosystem which can bolster adaptable access control over various sort of correlation based obliged one dimensional attribute control and multi-attribute control. Utilized encryption procedure changes over the outcome information into cipher messages that implant the vital access constraint and sends the message content to the user. A STP based encryption (ST-PBE) plot developed on key arrangement ABE model based on algorithm. - Setup, Genkey, encode, decode. ST-PBE based defines workflow of LFAC described in lightweight service authentication, query, LBS, information transmission. Performance evaluated of computational cost by ST-PBE scheme Qt/C++ on window server 2003 and disk operations on RAID disk array. Yan zhu. et.al. [6]

Centralized node and mobility node security models: This model address the issue of protection and the security of client in Cloud Computing. Personality Based Proxy Encryption plan create two models MNM (mobility node model) and COM (centralized owner model). This model handles the matter of security by the client of intermediary server. IBE protocol deal in steps: a) Setup, Key Generation, Encryption, Re-Encryption Key Generation, Re-encryption, Decryption. The scrambled message is transmitted on cloud by downer and Cloud control the capacity limit and computational power. Downer allows the versatile client to get to the information from cloud. The expansion of new client and encryption time, information get to were examined for both models. MNM is more confused regarding overhead and information access, new client expansion. MNM require another key each opportunity to deal with each demand other hand COM works with a similar encryption enter and quicker regarding encryption time as contrast with MNM. Ragini. et.al. [7]

Secure Resource Allocation for Mobile Cloud: The scheme focus on resources request from cloud defined in level of security proposed in the form of ideal resource allocation algorithms. The issue of asset distribution is detailed with a limited state Semi Markov Decision Process under average cost formula . Markov-Decision is a procedure in which the time of move and choices having continues time random variable with same likelihood dissemination. The choice is made at each stride either accepting the demand or not. On the off chance that demand is acknowledged then productive asset distribution will be finished. The Semi Markov Decision Process procedure was assessed as far as demand blocking likelihood and framework remunerate. At the point when entry rate builds then framework blocking and turns out to be high. At same entry rates

which increase number of VMs and the block probability diminish. The traffic becomes heavier when system rewards grow. Liu.Y. et.al. [8]

Resource Allocation for Security Services: Mobile gadgets utilizes cloud for information searching, data preparing and information mining. So as to accomplish security in cloud administration is characterized into classifications to be specific normal security and critical security services. Basic security administration give solid assurance however expends more assets. Critical clients need to pay more than ordinary clients. To expand the framework compensate at most extreme, a security benefit confirmation display is proposed. Markov Decision handle is utilized to deal with the framework rewards. The portable clients pick some particular characterized security administration in view of their area. The cloud chooses whether to acknowledge or dismiss the demand. The blocking likelihood trademark QoS for portable cloud is contrasted and different characterized security administrations. Blocking probability is lower as separate with number of system assets and furthermore blocking probability is high with increment in arrival rate.

. Liang, H. et.al. [9]

A security framework: Many mobile and simple user applications providers outsource their database and shared assets in light of intense storage, simple to access and adaptability of cloud. Along these lines, a protected system concentrating on location of data at versatile terminals is utilized. For security issues of area based administrations a security demonstrate utilizing outsource database is introduced for LBS. A system is proposed which improved security and verification. LBS security show utilizing ODB based framework is surrounded and including between three sections clients, service provider and cloud databases. In the first place confirmation processor is actuated then check of client identity and device identity performed by IMSI-Based IJS secure calculation. This algorithm can hide the user's true identity. The different key generation functions comparison shows the precedence of network as differentiate to popular hash functions. Chen, Y.J et.al. [10].

A study of incremental cryptography: As the asset confinement of cell phones, the well being and security of the information must be checked before transferring on cloud. Numerous security plans execute complex security operation on cloud through outsider. This proposed incremental cryptographic plan EnS, CoS and SnS are contrasted and unique form on the premise of turnaround time and vitality utilization. To decrease the turnaround time and vitality utilization of information document amid alteration operation, information record is partitioned into pieces of equivalent size into n bits. Versatile clients give a secret key, at that point changed decoding and honesty keys. Each block of document is encoded and record is produced by playing out some connection operation by utilizing hash capacities. Each piece work with confirmation code. In the wake of transferring and downloading documents assess the execution regarding turnaround time and vitality utilization's. The proposed techniques just encode and transfer the adjusted square . It's also enhances turnaround time and vitality utilization of the mobile. Khan.A.N. et.al. [11]

Secure web referral administrations: Mobile clients are at an incredible risk because of the perusing of pernicious sites. With a specific end goal to accomplish security against phishing sites and SSL Strip-based MITM (Man In The Middle) assault , another protected web referral benefit called Secure Search Engine (SSE) for cell phones is proposed SSE includes distinctive parts like SSE Service, SSL Verifier, Phishing filters, SSE crawler, URL Service, DNS Service and Storage Service. The crawler gets a natural URL from the arrangement of URLs in the URL Service and after that sends HTTP request. Web-crawler infers the IP address in the URL with DNS Service and forward them to storage device. Web crawling services worked inside time interim. In the middle of this interim another phishing site can be issued. The execution of phishing filters was examination for false positive, false negative parameters. The rate of false negative program decreases and time allotment increments. The false positive are lessens and the outcome from SSE phishing filters are also decreases. Xu, L. et.al. [12]

Policy based security channels: A segment of approach driven security convention is utilized for ensuring integrity, trust, secrecy, realness of information in versatile cloud computing. specialist substances, versatile and virtualized nature of cloud give vitality productive efficient key management mechanism.. Assessment is done in term of vitality utilization and execution time. This model utilized with versatile customer, cloud specialist organization, trusted key expert (KTA) which is trusted by both customer and CSP. Two security channels are utilized: open key based channel KTA and KVM. Symmetric key arrangement based security channel t secures genuine customer correspondence with virtualized administrations. Being used of four security conventions, three are steady convention and fourth one is primary convention. Asymmetric key administration diminishes the vitality utilization of the portable client and increment the service interaction time.. Itani, W. et.al. [13]

A security system for secure information storage on cloud: A protection safeguarding figure strategy attribute-based encryption centering with respect to security of clients is utilized. PP-CP-ABE gives security of light-weighted gadgets by substantial encryption and decoding. Quality based information storage framework is limited the burden of computational storage and communication. Encryption is done before sending information to SSP. The ESP gives encryption services to the downer without knowing the real information of encryption key. Then again decryption specialist gives decoding services required by customer. The DSP does not know the information content shape the center of the proposed framework; if

ESP, DSP and SSP impact information content can't be uncovered. The system was assessed for calculation, correspondence and capacity execution. Calculation load is direct for ESP and DSP and consistent for the user. SSP execute over 90% of the encryption and 99% of decoding. Zhou, Z. et.al. [14]

V. PROS AND CONS OF VARIOUS MODELS

The productive, secure, protection saving methodology utilizes low CPU time and memory energy of customer amid the encryption and decoding process. The thin customer approach has great data transfer capacity, CPU power, and memory. Nonetheless, this rank keyword search is inefficient at server when utilization of vast volumes of information, In enormous information condition, its prompt execution corruption.[1].It is a safe and dependable access control methods utilized and provide quick versatility, measured administration, insignificant forthright speculation, less upkeep cost and universal access to cloud administrations. This plan used to control the classification of the outsourced information. In any case, the mobile cloud computing need lightweight information auditing approach for in backward and forward security. [2] This approach control data spillage, various leveled secure access control. It opposes the interior assaults and gives enormous information security and protection. In future extension utilization of encryption or signature based privacy preserving innovation with the safe access control model to enhance the execution and performance of PP model. [3] This design ensures that an assailant can't abuse any data of a client, who is utilizing location based services namelessly through this server and furthermore keeps any pernicious movement from semi-genuine clients also. Nonetheless, additional time will be taken by the server to produce outcome about if the client characterizes a large area. [4] This approach builds up a safe system for approved and enrolled clients of the organisation. In any case, offloads the calculation and capacity to the cloud are asset compelled on mobiles. Future scope need to incorporate sensor characteristics and usefulness of applications. [5] The execution of model and comparing assessment talked about strategy. Be that as it may, Overall, diverse sizes of properties and obliges have influenced the execution up to some range. [6].More secure stockpiling, secure association between downer and cloud. In this way, it expanded security. MNM display is not reasonable for extensive condition and furthermore expansion of new client is extremely troublesome. In COM Model same key can be utilized for various portable clients. [7] The given system adequately meets the blocking probability and despite the fact that the demand movement is high. Notwithstanding, Sometimes VMs are ineffective for coming solicitation because of small framework limit and prompts dismissal of solicitations. Accordingly framework remunerate are influenced. [8] This model outcome in high system reward and diminished framework costs. Be that as it may, the client framework cost is high because of long service holding time. In this way, framework remunerate corrupts. In future ideal framework assets approach can be acquire most extreme reward. [9] In this approach IJS calculation enhances security, genuineness and progression. Approach does not consider sensible computational shortcoming of the client and power utilization issue of the device. In future to defeat this issue enhancement of encryption instrument in view of IMSI qualities should be possible. [10] Incremental scheme indicates striking advancement in execution of block(s) alteration operation. In any case, encryption and transferring demonstrates additional document management overhead and devour more assets. [11] In this internet searcher (SSE) phishing filters creates low false positive and false negative. Be that as it may, SSE benefit sets aside greater opportunity to react and fabricate a store. In future, other web assaults like cross-webpage scripting (XSS) can likewise be secured utilizing SSE. [12] In this protocol service interaction time increments and energy consumption time diminish. Notwithstanding, the assessment of time and vitality of security operation is not appeared in this convention. In future, to defeat this issue work should be possible utilizing symmetric key era. [13] This plan diminishes the weight of computational storage and communication. Utilizing PP-CP-ABE, light weight gadget can safely perform encryption and decoding operation without uncovering the information and perform outsourcing with service provider. Be that as it may, this plan experiences straight developing figure content size. In future, needs of new CP-ABE conspire with constant cipher text size. [14]

VI. CONCLUSIONS AND FUTURE WORK

Writing audit identified with security strategies in versatile cloud computing condition are secured for investigation .These techniques have been inspected on the premise of security related issues in mobile cloud computing condition. Every one of them have their particular upsides and downsides. Many models increment protection and also execution of the framework, secure capacity of information is ensured by two plans. One model guarantees greatest framework reward and diminishes costs as well. Another approach is more proficient as far as vitality utilization. But, still significant need of improvement in various security aspects of user data on cloud.

Comparative analysis is done to discover various aspects of existing models and schemes. Framework for security of mobile cloud computing environment and also result achieved by these methods are taken into consideration. The customary encryption plans can't function admirably in cloud condition. Today professional programmers are not considering energy saving factors. The traditional cryptographic schemes using ample processor time, memory, battery power of

the client device between data encrypt and decrypt process. There are also need of efficient data access schemes between downer and CSP. In future, there is a need of improved encryption and decryption scheme.

REFERENCES

[1] Syam Kumar Pasupuleti, Subramanian Ramalingam, Rajkumar Buyya, "An efficient and secure privacy - preserving approach for outsourced data of resource constrained mobile devices in cloud computing", Journal of Network and Computer Applications, Elsevier Journal, Pages: 1-11, (2016).

[2] Mehdi Sookhak, F. Richard Yua , Muhammad Khurram Khan , Yang Xiang , Rajkumar Buyya, "Attribute-based data access control in mobile cloud computing: Taxonomy and open issues", Future Generation Computer Systems, Pages: 1-14,Elsevier Journal (2016).

[3] Hui Lin, Li Xu, Xinyi Huang,Wei Wu,Yijie Huang, "A trust worthy access control model for mobile cloud computing based on reputation and mechanism design" , Ad Hoc Networks Pages: 51–64, Elsevier Journal homepage: www.elsevier.com/locate/adhoc, (2015).

[4] Fizza Abbas; Rasheed Hussain; Junggab Son; Heekuck Oh,"Privacy Preserving Cloud-Based Computing Platform (PPCCP)for Using Location Based Services" IEEE/ACM 6th International Conference on Utility and Cloud Computing (UCC), Dresden, Germany , Pages: 60 - 66, IEEE Conference Publications,9-12 December(2013).

[5] Deepanshu Goyal, M. Bala Krishna, "Secure Framework for Data access Using Location Based Service in Mobile Cloud Computing", Annual IEEE India Conference, IEEE INDICOM, Pages: 1-6, (2015).

[6] Yan zhu, Di ma ,Dijiang,Changjun, "Enabling secure location-based services in mobile cloud computing", pages :27-32,Hongkong ,China,ACM-(2013).

[7] Ragini., Mehrotra, P., Venkatesan, S.: An Efficient Model for Privacy and Security in Mobile Cloud Computing. International Conference on Recent Trends in Information Technology, 1-6 (2014).

[8] Y. Liu. , Lee, M.J.: "Security-Aware Resource Allocation for Mobile Cloud Computing Systems". Computer Communication and Networks (ICCCN), 24th International Conference on, 1-8 (2015).

[9] Liang, H., Huang, D., Cai, L.X., Shen, X., Peng, D.: Resource Allocation for Security Services in Mobile Cloud Computing. IEEE INFOCOM 2011 Workshop on M2MCN, 191-195 (2011)

[10] Chen, Y.J., Wang, L.C.: A Security Framework of Group Location- Based Mobile Applications in Cloud Computing. International Conference on Parallel Processing Workshops, 184-190 (2011).

[11] Khan, A.N., Mat Kiah, M.L., Khan, S.U., Maddani, S.A, Khan, A.R.: A Study of Incremental Cryptography for Security Schemes in Mobile Cloud Computing Environments. EEE Symposium on Wireless Technology and Applications (ISWTA), September 22-25, 2013, Kuching, Malaysia, 62-67 (2013)

[12] Xu, L., Li, L., Nagaranjan, V., Huang, D., Tsai, W.T.: Secure Web Referral Services for Mobile Cloud Computing. IEEE Seventh International Symposium on Service-Oriented System Engineering, 584-593 (2013).

[13] Itani, W., Kayssi, A., Chehab, A.: Policy Based Security Channels for Protecting Network Communication in Mobile Cloud Computing. Security and Cryptography (SECRYPT), Proceedings of the International Conference, 450-456 (2011)

[14] Zhou, Z., Huang, D.: "Efficient and Secure Data Storage Operations for Mobile Cloud Computing". Network and service management (cnsm), 2012 8th international conference and 2012 workshop on systems virtualiztion management (svm), 37-45 (2012).

[15] "Introduction to Mobile-Cloud Computing",https://www.cs.purdue.edu/homes/bb/cloud/MCC.pptx.

[16] Prashant Pranav,Naela Rizvi, "Security in Mobile Cloud Computing: A Review",International Journal of Computer Science and Information Technologies, Vol. 7 (1), (2016).

[17] Pawan Kumar, and Surender Jangra, "Design and Implementation of Encryption based Data Security Algorithm for Cloud Environments", Published in, "Int'l J. of Control Theory and Applications", Vol. 10, Issue No. 15, Pg. 163-171, ISSN: 0974-5572(2017).

[18]Pawan Kumar, SurenderJangra and Sawtantar Singh, "Exclusive OR (XOR) based Enhanced Data Security Algorithm for Cloud Environment" published in " Int'l J. of Advanced Research in Computer Science ", Vol. 8, No. 5, ISSN No. 0976-5697, Pg. 1482-1485 May-June (2017).

[19]Akhilesh Kumar Bhardwaj, Rajiv Mahajan and Surinder, "Improved Load Management in Cloud Environment Using MHT Algorithm", published in, "Int'l J. of Control Theory and Applications" Vol. 9(22), pg. 301-305, **ISSN:** 0974-5572,(2016).

[20]Akhilesh Kumar Bhardwaj, Rajiv Mahajan and Surender, "TTP based Vivid Protocol Design for Authentication and Security for Cloud", published in IEEE Xplore; " 3rd Int'l Conf. on Computing for Sustainable Global Development" Pg. 3275-3278,(2016).

[21] Naveen Garg, Sanjay Singla and SurenderJangra, "Challenges and Techniques for Testing of Big" published in the Journal, "Procedia Computer Science (Elsevier)", 85, Pg. 940-948, DOI: 10.1016/j.procs.2016.05.285, ISSN: 1877-0509, (2016).

[22] Abishek gupta, Mr. Vishal Garg, Dr.Mohan Lal "Congestion control schemes in wireless communication-review," in proceedings of IEEE- 2nd international advance computing Conference, 2010, Vol: 02, pg no. 248-253, TIET-Thaper, February 2010

[23] Mr.Vishal Garg Ashutosh dhamija, SangeetaKamboj, "Emerging Trends in Cryptography," International Journal of Advanced Research in Computer Science and Software Engineering Volume-3, Issue-8, august 2013.