International Journal of Computer Engineering & Technology (IJCET)
Volume 9, Issue 3, May-June 2018, pp. 259–269, Article IJCET_09_03_031
Available online at http://www.iaeme.com/ijcet/issues.asp?JType=IJCET&VType=9&IType=3
Journal Impact Factor (2016): 9.3590(Calculated by GISI) www.jifactor.com
ISSN Print: 0976-6367 and ISSN Online: 0976–6375

TRENDING SECURITY MECHANISM IN CLOUD COMPUTING

Prince Jain
Research Scholar, MSIT Dep't MATS University, Raipur, Chhattisgarh India

Dr. Umesh Kumar Pandey
MSIT Dep't MATS University Raipur Chhattisgarh India

ABSTRACT

Cloud computing is a concept of modern and smart computing world. People buy high configuration computer system for their use but a little amount of the total capacity is used by them. So, computing power and money both becomes waste. The solution of this problem is cloud computing. In cloud computing environment the client's whole data is on cloud server which is offered by cloud service provider (CSP). Cloud service provider offers facility of processing power, storage space, software etc. The whole data of user is on cloud server and accessed by user through login credentials. Cloud computing reduces the on-demand hardware and processing power requirement of these days. While the need of cloud computing increases the security challenges also increases. This paper first describes the need of cloud computing and some security challenges and some proposed security solutions to it.

Key words: Cloud Computing, security in cloud, Authentication server.

Cite this Article: Prince Jain and Dr. Umesh Kumar Pandey, Trending Security Mechanism In Cloud Computing. *International Journal of Computer Engineering & Technology*, 9(3), 2018, pp. 250–258.
http://www.iaeme.com/ijcet/issues.asp?JType=IJCET&VType=9&IType=3

1. INTRODUCTION

Cloud computing has formed the basis for tomorrow's computing. In cloud, user or client's whole data is in cloud provider's server and computing capability is also provided by the same party their data is at the most concern. Now days everybody is using computer directly or indirectly and more and more users are learning how to run and use computing services, according to the statics of internet world stats 7,519,028,970 internet users till MARCH 25, 2017 statics and the number is growing rapidly and more and more users of computer uses more space and more computing power, according to computer giant IBM 2.5 billion gigabytes (GB) of data was generated every day in 2012 [1]. Researching on cloud computing and security of clients data or users data are in the core of research field, because the whole data of user is kept on third party server and accessed by virtual OS mechanism as on user requirement on rental basis.

In the figure 1 we can imagine how much of data is generating every minute and 24 hours of a day so to store these data more and more space and processing power is needed so new and new data centers and advanced pcs are installing every now and then we can see in the below figure 2 the no of pcs shipped from 2009-2016.

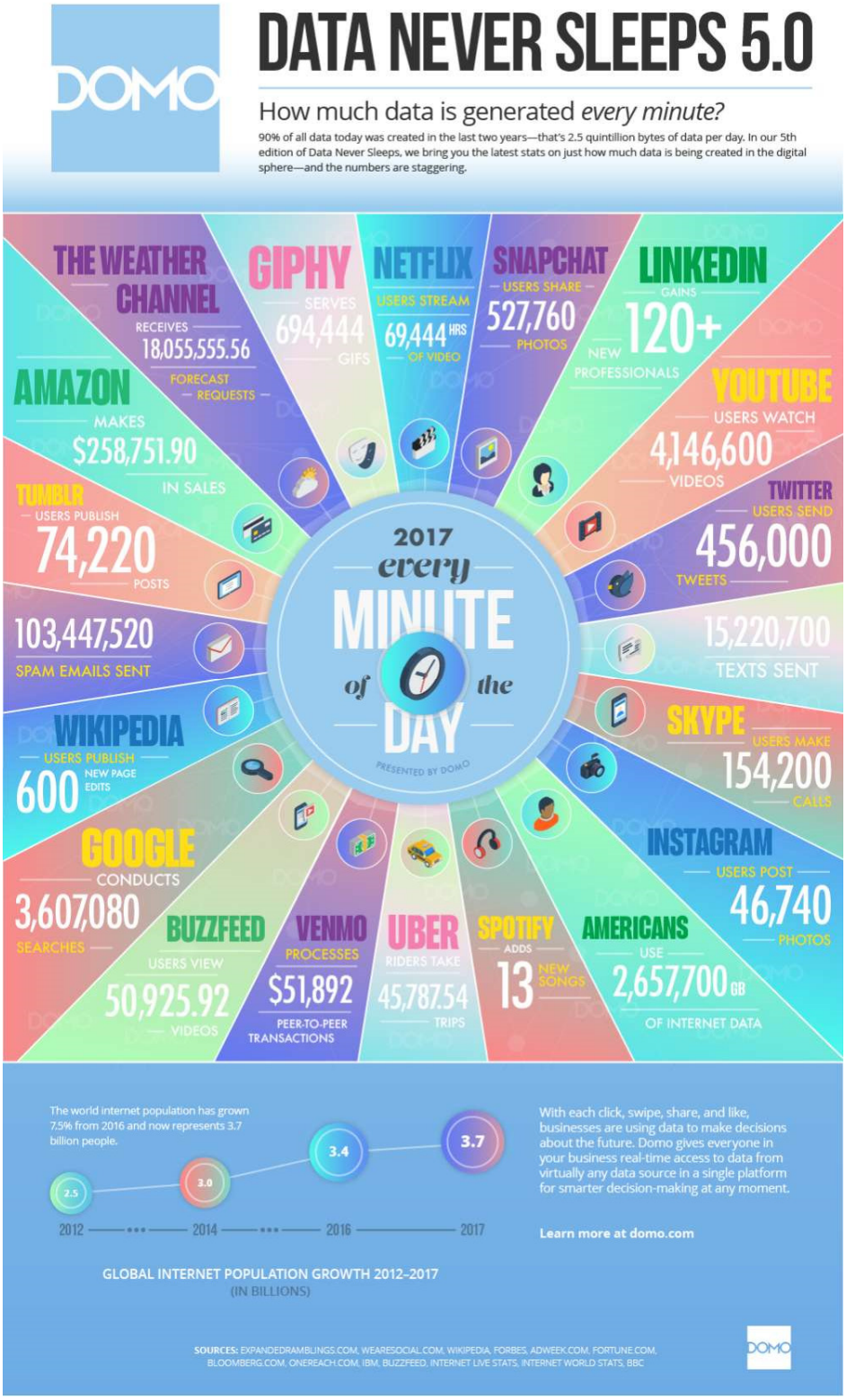

Fig: 1 Data Generated Every Minute [1]

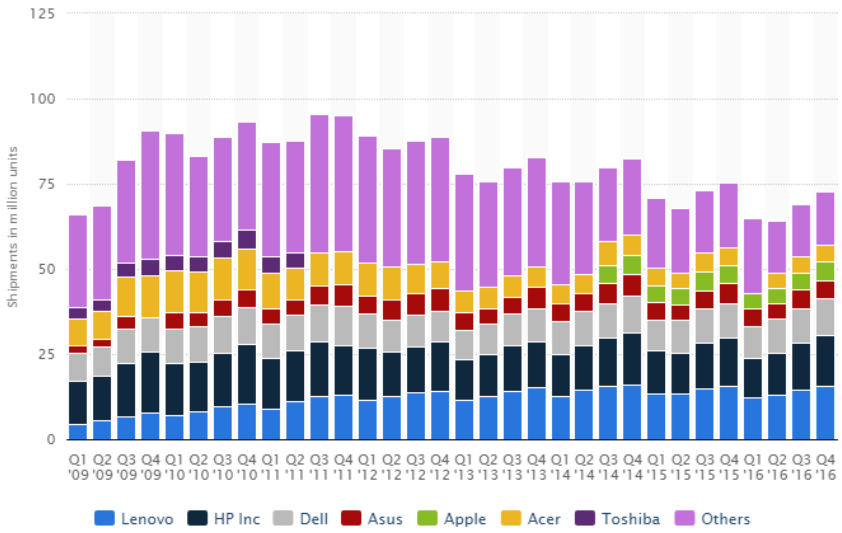

Fig 2 No of pc's shipped from 2009-2016 [2]

To full fill the data storage on internet as the internet users are increasing every day we can see in the figure 3 the internet users worldwide and the servers installed by only the big companies [5].

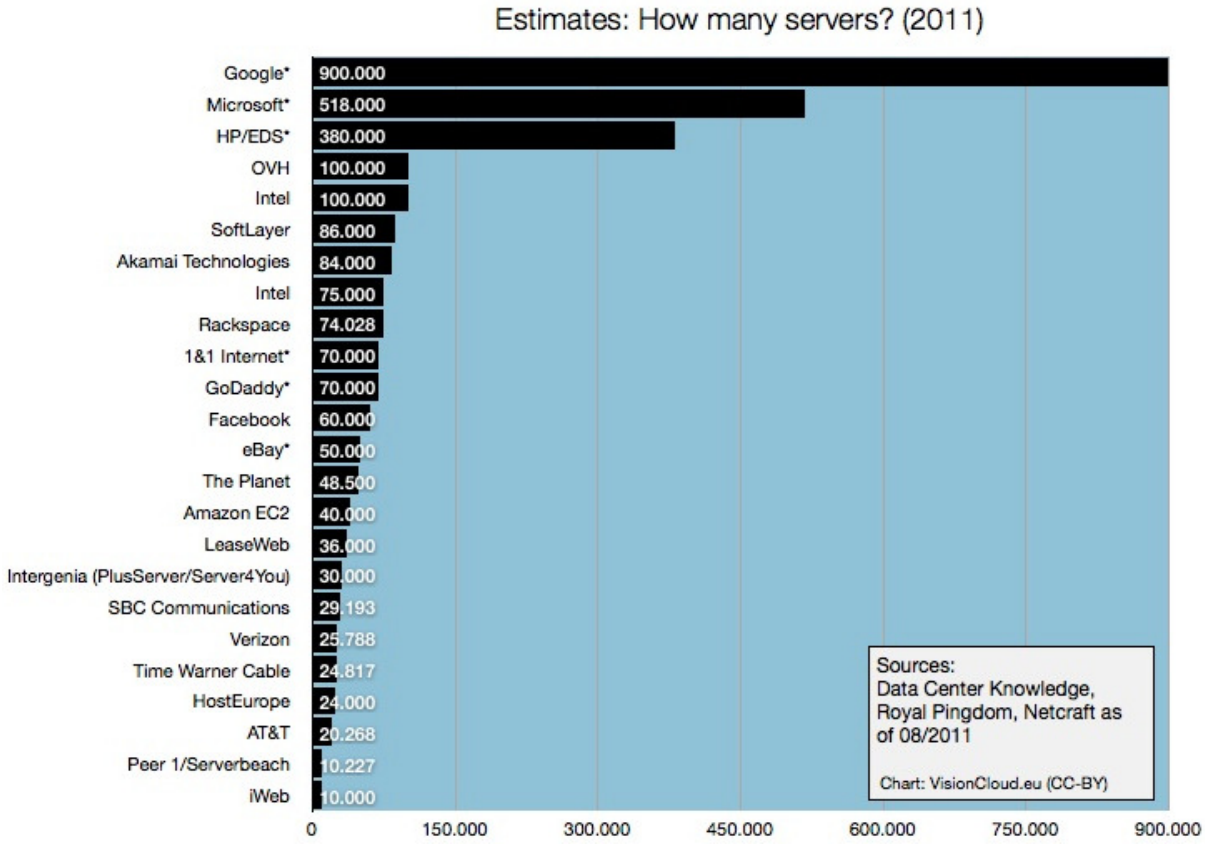

Fig 3 Internet users worldwide and the servers installed by only the big companies. [3]

2. CLOUD COMPUTING AND ARCHITECTURE

Cloud computing is the form of computing based on delivery of computing services such as databases, servers, storage, software, networking, analytics and more over the Internet ("the cloud") [6][4].

There are mainly 3 different types of cloud: public cloud, private cloud and hybrid cloud shown in Figure 4.

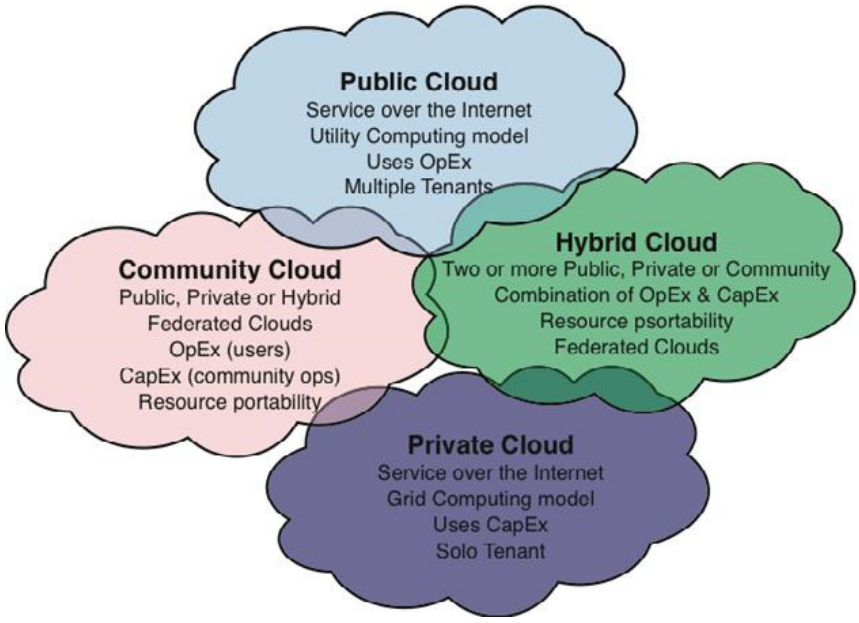

Fig 4 Mainly 3 Types of cloud [8]

2.1. Public cloud is a cloud service which is provided by cloud service provider it is free or may be pay to use plan. In this cloud service user data is less secure and visible to public.

2.2. Private cloud implies this cloud focuses on the privacy-based environment in which only specified user can operate. Private cloud provides services over the internet or in a private network to specified user rather than to general public which is sometimes termed as corporate cloud.

2.3. Hybrid cloud is a cloud service which incorporates cloud services of both private and public clouds to perform different functions in the same organization.

3. CLOUD COMPUTING SERVICES

Cloud computing services are primarily offered in the three format IaaS (Infrastructure as a Service), PaaS (Platform as a Service) and SaaS (Software as a Service).Wherever computing offers IaaS (infrastructure as a service), PaaS (platform as a service).

A. Infrastructure-as-a-service (IaaS)

In this cloud service client or user is provided hardware as a service and that to on-demand here meaning of on-demand is providing user with scalable hardware at any time and that to online for example if a user wants octa core CPU, 10 GB Ram in few minutes s/he can get easily and that on hourly basis. In this service of cloud hardware is provided as service and resources are provided via API or via control panel provided by cloud service provider as service. IaaS users can make their own "virtual data center" in the cloud and can outsource them without physical maintenance and management of it. There are many providers who provide Infrastructure as a Service such as Amazon Web Services (AWS), Google Compute Engine and Windows Azure.

B. Platform as a service (PaaS)

Platform as service is a cloud service which works at lower level then SaaS; here client does not have to think about the complexity of maintaining of infrastructure. PaaS service can be delivered in two ways firstly as a public cloud service where the client controls the software

deployment with minimum options for configuration, and the cloud provider provides the storage, (OS) Operating system, servers, middleware, database and other services for client application hosting. Secondly PaaS can be provided as private service or as software on a public infrastructure. Examples of PaaS providers are Google App Engine, and Red Hat's.

C. Software as a service (SaaS)

In SaaS Cloud provider provides every software as a service in which client does not have to buy that software for yearly bases or for forever, s/he have to pay only for the time period for which it have to be used and here a very big advantage is user does not have to worry about hardware configuration to run it that to can be get as service and on rental base. Client does not have to worry about maintaining and upgrading of software and does not have to worry about its license. Examples of SaaS are: Google Apps, Salesforce, Concur, Citrix GoToMeeting, and Cisco WebEx.

Many services are provided by cloud and it is very flexible to user requirements, as the services are provided to the user anywhere and at anytime, and user can access his/her data, this user data is very crucial and as it is on the cloud service provider side it become more crucial and raises many security issues and challenges some of them are discussed below.

4. KEY SECURITY ISSUES IN CLOUD COMPUTING

Cloud computing has infrastructure, platform and software components. Each component has its own task and offers different products for businesses and individuals according to individual need across the globe. The business application includes Utility Computing, Software as a Service (SaaS), Web Services, Managed Service Providers (MSP), Platform as a Service (PaaS), Service Commerce and Internet Integration. Following are the various security concerns in a cloud computing environment [9].

Table 1 Various security concerns in a cloud computing environment

Access to Servers & Applications	Data Transmission	Virtual Machine Security	Security Policy and Compliance
Data Privacy	Data Security	Data Integrity	Data Location
Data Availability	Data Segregation	Network Security	Patch management

5. LITERATURE REVIEW

Raina P and Patel B in their paper proposed an authentication theme which uses algorithmic program for user validation. In the proposed model user is checked before giving access to the cloud services. In their model they also proposed a separate server for doing encryption and decryption. For authenticating user a different server termed as authenticating server is used and a MDHA agent is also deployed in SaaS layer [10].

R.Prema, P.Shanmugapriya in their paper they proposed a face recognition system (FRS) which overcome all drawbacks of traditional and other biometric authentication techniques, and provides better Security. This technique enables only authorized users to access data or services from cloud server [11].

A.Amali Mary Bastina, N.Rama in their paper presents a mobile biometric authentication in cloud environment. This method uses finger print as biometric authentication. By this fingerprint biometric a secret code is generated by uncertain value. In their model user request for authentication to the authorized person and that person sends the authorization through mobile by finger print authentication through Bluetooth which generates a secret code and this

fingerprint is verified by the database in desktop computer if it matches access is granted to the requesting person [12].

Hong N, Kim M, Jun M and Kang J in this paper a study on a JWT-Based User Authentication and API Assessment Scheme Using IMEI in a Smart Home Environment is done. In this paper author propose a user authentication method using the JSON Web Token (JWT), and International Mobile Equipment Identity (IMEI) number in the smart home, and solved the problem of unauthorized smart home device registration of hackers, by the application of IMEI and JWT technology [13].

Lee W and Lee R in their paper they proposes a user authentication scheme, in which authentication of smart phone user is done with the help of sensors in smart watch. Author in this model proposes a authentication system termed as iAuth for continuous, implicit authentication of the end-user based on his or her behavioral characteristics, by using the sensors built in the smart watch, in this small training is also given to the system about user behavior pattern for future authentication phones [14].

Sarddar D, Nandi E in their proposed model Cloud Service provider (CSP) is responsible for all decisions. They also introduce Authenticating server and storage server, authenticating server for user authentication and storage server for storing user data. The proposed model totally works on set of private key and public key. In this model if any client wants to used or access data then they have to communicate with CSP first and if Cloud Service provider grants permission to client then s/he can access his/her data in cloud. In this method third party never knows the public key of Authenticating server and Data server but can communicate with them securely. In this model three layer of security is performed in which there is no direct communication between data server and authenticating server [15].

K.Satyanarayana in his paper proposes an algorithm termed as multilevel algorithm. In this method plain text is encrypted two times, first by applying DES algorithm and the data which is generated, it is second time encrypted by applying RSA algorithm and then stored into data base. For decryption purpose data is read from data base then RSA algorithm is applied and first level decrypted data is generated and on that data DES is applied and user readable format data or plain text is get [16].

Sivakumar K in his paper focuses on providing security to the user data by the process of encryption. Here author in this paper also deals with various security problems related to securing user data. In this paper author also discussed various block cipher algorithm like Blowfish square measure, RSA to secure cloud. Proposed system each time generate totally different secret key each time and increases performance of cloud service [17].

Praveen Kumar Shrivastava, Vibha Sahu, and Dr. S.M.Ghosh in their authentication technique a double sided authentication between the service provider and the user's are arranged. According to the proposed method it effectively prevents middleman attack, reduces information leakage and provides secure communications. This paper also deals the authentication management like security audit mechanism, access control mechanism with the use of OTP [18].

Farhana J. Zareen, Kashish A. Shakil, Mansaf Alam, Suraiya Jabin and Shabih Shakeel in their paper a Cloud based mobile biometric authentication framework (BAMCloud) are proposed. This technique for performing authentication uses dynamic signatures. It includes the steps involving data capture using any handheld mobile device, then storage, preprocessing and training the system in a distributed manner over Cloud. For this purpose they have implemented it using MapReduce on Hadoop platform and for training Levenberg-Marquardt back propagation neural network has been used. The methodology according to author achieves a performance of 96.23% and speedup of 8.5X [19].

S. A. Alhumrani and Kar J in their paper reviewed and analyze some of the famous cryptographic protocols used for encryption used in cloud, which helps in establishing a secure communication in cloud. In this paper they discussed about secure shell protocol, Kerberos, WI-Fi Protocol Access, Wired Equivalent Privacy (WPE), and Internet Protocol Security. This paper also discusses how these protocols are applied in cloud, and advantage of these protocols on cloud communication [20].

Mrs. S. M. Barhate, Dr. M. P. Dhore in their paper author discussed various security issues, and about User Authentication and Authorization and Techniques used in user Authentication and Authorization and Protocols Used In this Process of User Authentication and Authorization in detail [21].

B. Chavan S and Kumar A in their research user data is first encrypted and cipher text is generated, after which it is extracted to make it incomplete to make user data safe from attacks like traditional cryptanalysis and brute-force. The decrypted key and extracted cipher text are distributed into the DHT (Distributed Hash Table) network. All this happens in time server and authentication server [22].

Amavi A. Vispute, Prof. H. A. Hingoliwala in the proposed work they are using encryption concept and send all the chunks in encrypted format. And for encryption they are using AES algorithm which is a symmetric block cipher. And for providing more security over network author is applying data integrity verification by using hashing algorithm like SHA-1 and do encryption/decryption by AES algorithm [23].

Vishal R. Pancholi, Dr.Bhadresh P. Patel in their paper presents the AES (Advanced Encryption Standard) symmetric cryptographic algorithm. This algorithm is based on several permutation transformation and substitutions [24].

My Abdelkader Youssefi in his paper proposes digital certificates authentication for user in cloud computing. Here in this paper users are authenticated using private public key infrastructure (PKI). This method provides session key establishment, identity control and mutual authentication between cloud server and the users [25].

Xiaohui Li, Jingsha He, and Ting Zhang in their paper author propose a service-oriented identity authentication privacy protection method. In this paper author define cloud service access control as a process and extending the cloud client related information into a fuzzy set as the authentication condition for the exchange, according to the amount of information security level, dynamic opening the corresponding service access control and providing fine-grained service-oriented identity authentication, guarantees global minimal sensitive information disclosure, and maximize protects individual privacy [26].

B.Jondhale N, K.Kadam S, B. Shinde S, N. Dumbare A in their paper proposes a Geo-Encryption Authentication and Time Based Data Access in cloud. The term “geo-encryption” or “location-based encryption” is authentication algorithm that limits the decryption or access of information content to specified locations and/or times [27].

Moghaddam F, Rouzbeh S, Varnosfaderani S in their paper proposes a User Authentication Scheme for Cloud Computing Environments which is very Scalable and Efficient. In the proposed method user identity is confirmed at client side for this a user authentication agent is introduced in client side to confirm the identity of the user. A cloud based SaaS (software as a service) application is also introduced for unregistered devices to confirm the process of authentication and there are two separate server storing cryptography and authentication details. An agent for cryptography is also introduced for encrypting resources before storing [28].

Sahni M in his paper briefly describes about IMEI number and GSM networks it also proposed the solution to avoid change of IMEI number. In this paper also discussed various method of changing IMEI number [29].

P.Shenbagam, C. Namasivayam in their paper develop a "Persuasive Cued Click-Points", "Alphanumerical authentication", "Sound Signature" and "Draw-a-Secret" method system. According to author this can overcome the problem of usability and security. Author in his paper also proposes mobile security techniques that can enhance the security; this is done by sending message to the mobile phone when ever any one enters into the system [30].

V.Gujar G, Sapkal S, V.Korade M In this paper author proposes a password authentication and generation technique by session management and step-2 authentication in cloud environment. The proposed technique works in different modules they are user authentication, user registration and password change [31].

Huang J and M Nicol D in their paper did a survey of existing mechanisms for trust establishing and discussed about their limitations. In their paper they also propose mechanism which is based on attribute certification, validation and evidence. Author's in their paper concluded by proposing a framework which integrates various trust mechanisms together for providing trust in cloud [32].

Kok-Seng Wong and Myung Ho Kim in their paper a biometric-based authentication protocol is proposed for authentication of user in cloud environment. Author in this paper proposed incorporation of many biometric templates of the user. In the proposed technique these biometric templates are stored in cloud storage and all the user authentication in cloud is done without leakage of sensitive information [33].

Kim J and Hong S in their paper the current user authentication for device and user both are analyzed and security available credential (SACRED) standards are also analyzed. In the proposed model author design a N-screen based user authentication that meets privacy protection requirements and credential requirements in cloud environment [34].

Jeong H and Choi E in their paper proposed a high-level security for mobile environment. Author in this paper uses authentication using profiling technique for access control and user authentication [35].

Ristov S, Gusev M and Kostoska M in their paper analyzes almost all cloud service providers and evaluated that most of the main cloud service providers are at minimum, ISO 27001:2005 certified. In this paper they also analyze main industrial and international standards which target security of information and their commitment with cloud computing. In this paper author also proposes extension to the ISO 27001:2005 standard for generic control objective for virtualization. Author in this paper also proposes some solutions for risks reduction [36].

S.C. Wang, M.L. Chiang, K.Q. Yan, S.S. Wang, S.H. Tsai in their paper proposed Group Key Authentication (GKA), a protocol, so that the time of authentication and data traffic can be reduced and Quality of Service (QoS) can be increased in Cloud computing [37].

Huan Liu, San Jose in this paper describe a DOSattack which is of very new kind, which effects network in cloud computing, this type of attack can effect cloud infrastructure. Author in this paper also describe a mechanism to eradicate this type of attack [38].

Senaka Buthpitiya, Ying Zhang, Anind K. Dey, and Martin Griss in their paper present a model for a user's mobility patterns based on n-gram based modeling. They take Markovian assumption as their base that any user's location at any time t depends only on the last location. According to author a user's individual location patterns can be model through a collection of n-gram geo-labels with estimated probabilities of each. They also show that the model is able to obscure user's exact location by use of a hierarchical location partitioning system to protect privacy [39].

Jyh-haw Yeh in his paper discuss about how to protect client's data from employees of cloud service provider (CSP) and also proposes a PASS scheme for Authentication and Secret Sharing [40].

L. Hong and A. Jain in their paper proposed a prototype biometric system with integration of fingerprints and faces. According to them this system overcomes the limitations of both the systems face recognition system and fingerprint verification. According to the author the identity established by proposed system is more reliable than face recognition system. The proposed scheme of decision fusion improves performance by integrating multiple cues with various confidence measures. According to proposed scheme their Experimental results system performance is well and it meets time and accuracy requirements [41].

K.Madhavjee Sunjiv Soyjaudah, G.Ramsawock, M.Yaasir Khodabacchus in their paper author proposes the use a cancellable biometric authentication system. In this concept a biometric image is used which is distorted which is derived from the original image used for authentication. In this concept a data hiding technique is also used to embed demographic information in the biometric image, by which the original biometric image is hidden [42].

6. CONCLUSION AND FUTURE WORK

Cloud computing is the need of today's world and it is use is spreading rapidly in the world. When any organization moves to the cloud the company loses control over its data, so there should be proper measures to secure user's data in cloud, in this paper we discussed about cloud architecture, its services and security issues related to it and some of the security measures proposed by different researchers. In spite of many different security challenges cloud computing has very bright future.

REFERENCES

[1] http://www.iflscience.com/technology/how-much-data-does-the-world-generate-every-minute/

[2] https://www.statista.com/statistics/263393/global-pc-shipments-since-1st-quarter-2009-by-vendor/

[3] http://orlodelboccale.blogspot.in/2014/05/quanti-server-ci-sono-nel-mondo.html

[4] http://conceptdraw.com/news/cloud-computing-diagrams-solution

[5] http://www.internetworldstats.com/stats.htmCloud

[6] https://azure.microsoft.com/en-in/overview/what-is-cloud-computing/ 7.

[7] http://conceptdraw.com/news/cloud-computing-diagrams-solution

[8] http://cloudcomputingnet.com/cloud-computing-deployment-models/cloud-computing-user-types/

[9] Rabi Prasad Padhy, Manas Ranjan Patra, Suresh Chandra Satapathy, "Cloud Computing: Security Issues and Research Challenges" "IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS) Vol. 1, No. 2, December 2011

[10] Palak Raina and Bhavik Patel, "Authentication Scheme in Cloud Computing Environment", International Journal of Advanced Research in Computer Science , Volume 8, No. 3, March – April 2017.

[11] R.Prema, P.Shanmugapriya, "A Novel Method for User Authentication on Cloud Computing Using Face Recognition System". IIR International Journal of Computing Paradigms Volume: 01 Issue: 01, September 2017, Pages: 19-22 ISSN: XXXX-XXXX.

[12] A.Amali Mary Bastina, N.Rama, "Biometric Identification and Authentication Providence using Fingerprint for Cloud Data Access", Vol. 7, No. 1, February 2017, pp. 408~416, ISSN: 2088-8708, DOI: 10.11591/ijece.v7i1.pp408-416.

[13] Namsu Hong, Mansik Kim, Moon-Seog Jun and Jungho Kang, "A Study on a JWT-Based User Authentication and API Assessment Scheme Using IMEI in a Smart Home Environment", http://creativecommons.org/licenses/by/4.0/.

[14] Wei-Han Lee, and Ruby Lee, "Implicit Sensor-based Authentication of Smartphone Users with Smart watch", arXiv: 1703.03523v1 [cs.CR] 10 Mar 2017, http://dx.doi.org/10.1145/2948618.2948627.

[15] Debabrata Sarddar, Enakshmi Nandi, "An Authenticate Cryptography based security model for handling multiple request from multiple devices for Mobile Cloud Computing". International Journal of Advanced Research in Computer and Communication Engineering Vol. 5, Issue 1, January 2016.

[16] K.Satyanarayana, "Multilevel Security for Cloud Computing using Cryptography". International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 5 Issue 2, February 2016.

[17] Sivakumar K, "Trusted Cloud Computing Methods using to Protected File Encryption Performance". International Journal of Scientific Engineering and Applied Science (IJSEAS) – Volume-2, Issue-3, March 2016 ISSN: 2395-3470.

[18] Praveen Kumar Shrivastava, Vibha Sahu, Dr. S.M.Ghosh, "STUDY ON SECURITY MANAGEMENT WITH OTP USING CLOUD COMPUTING". 3RD International Conference on Recent Trends in Engineering Science and Management, 10 April 2016, ISBN: 978-81-932074-4-4.

[19] Farhana J. Zareen, Kashish A. Shakil, Mansaf Alam, Suraiya Jabin and Shabih Shakeel, "BAMCloud: A Cloud Based Mobile Biometric Authentication Framework", arXiv.org > cs > arXiv:1601.02781, May 2017, v2

[20] S. A. Alhumrani and Jayaprakash Kar, "Cryptographic Protocols for Secure Cloud Computing", International Journal of Security and Its Applications Vol. 10, No. 2 (2016), pp.301-310 http://dx.doi.org/10.14257/ijsia.2016.10.2.27

[21] Mrs. S. M. Barhate, Dr. M. P. Dhore, "User Authentication Issues In Cloud Computing". IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727 PP 30-35

[22] Sangita B. Chavan and Ashish Kumar, "Self-Destructing Scheme in Cloud Computing for Data Security", International Journal of Current Engineering and Technology, Vol.6, No.1 (Feb 2016)

[23] Amavi A. Vispute, Prof. H. A. Hingoliwala, "Implement PACK with AES in cloud Computing", Volume 4, Issue 2, February 2016 ISSN: 2321-7782

[24] MVishal R. Pancholi, Dr. Bhadresh P. Patel, "Enhancement of Cloud Computing Security with Secure Data Storage using AES",IJIRST –International Journal for Innovative Research in Science & Technology| Volume 2 | Issue 09 | February 2016 ISSN (online): 2349-6010

[25] MY ABDELKADER YOUSSEFI, "Securing Cloud Computing Services Using Strong User Authentication With Local Certification Authority", (IJITR) INTERNATIONAL JOURNAL OF INNOVATIVE TECHNOLOGY AND RESEARCH Volume No.3, Issue No.6, October - November 2015, 2493 – 2497.

[26] Xiaohui Li, Jingsha He, and Ting Zhang, "A Service-oriented Identity Authentication Privacy Protection Method in Cloud Computing", International Journal of Grid and Distributed Computing Vol. 6, No. 1, February, 2013

[27] Nilesh B.Jondhale, Sonal.K.Kadam, Shweta B. Shinde, Amol N. Dumbare, "Security in Cloud Computing: Using Geo-Encryption Authentication and Time Based Data Access", International Journal of Advance Research in Computer Science and Management Studies, Volume 2, Issue 10, October 2014.

[28] Faraz Fatemi Moghaddam,Sohrab Rouzbeh, Shirin Dabbaghi Varnosfaderani, “A Scalable and Efficient User Authentication Scheme for Cloud Computing Environments”, https://www.researchgate.net/publication/264197050.

[29] `Mayank Sahni, "DETECTING AND AUTOMATED REPORTING OF CHANGE IN IMEI NUMBER”, International Journal of Advancements in Research & Technology, Volume 3, Issue 5, May-2014 ISSN 2278-7763

[30] P.Shenbagam, C. Namasivayam,"4 Level Authentication Security In Cloud Computing", International Journal of Innovative Research in Computer and Communication Engineering, Vol.2, Special Issue 1, March 2014

[31] Ganesh V.Gujar, Shubhangi Sapkal, Mahesh V.Korade,"STEP-2 User Authentication for Cloud Computing", International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 10, April 2013

[32] Jingwei Huang and David M Nicol, "Trust mechanisms for cloud computing", Advances, Systems and Applications 2013, 2:9 http://www.journalofcloudcomputing.com/content/2/1/9

[33] Kok-Seng Wong and Myung Ho Kim, "Secure Biometric-Based Authentication for Cloud Computing", https://www.researchgate.net/publication/259441835

[34] Jaejung Kim and Seng-phil Hong, "A Consolidated Authentication Model in Cloud Computing Environments”, International Journal of Multimedia and Ubiquitous Engineering Vol. 7, No. 3, July, 2012

[35] Hoon Jeong and Euiin Choi, "User Authentication using Profiling in Mobile Cloud Computing", AASRI Conference on Power and Energy Systems Procedia 2 (2012) 262 – 267

[36] Sasko Ristov, Marjan Gusev and Magdalena Kostoska, "CLOUD COMPUTING SECURITY IN BUSINESS INFORMATION SYSTEMS", International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.2, March 2012

[37] S.C. Wang, M.L. Chiang, K.Q. Yan, S.S. Wang, S.H. Tsai, "A New Group Key Authentication Protocol in an Insecure Cloud Computing Environment", 2011 International Conference on Advanced Information Technologies (AIT)

[38] Huan Liu,San Jose,"A New Form of DOS Attack in a Cloud and Its Avoidance Mechanism",CCSW’10, October 8, 2010, Chicago, Illinois, USA.

[39] Senaka Buthpitiya, Ying Zhang, Anind K. Dey, and Martin Griss, “n-Gram Geo-trace Modeling”, Carnegie Mellon University, 5000 Forbes Avenue, Pittsburgh, PA 15213, USA.

[40] Jyh-haw Yeh, "A PASS Scheme in Cloud Computing - Protecting Data Privacy by Authentication and Secret Sharing", http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.218.719&rep=rep1&type=pdf.

[41] L. Hong and A. Jain, “Integrating faces and fingerprints for personal identification”. Pattern Analysis and Machine Intelligence, IEEE Transactions on, 1998.

[42] Krishnaraj Madhavjee Sunjiv Soyjaudah, Gianeswar Ramsawock, Muhammad Yaasir Khodabacchus, "Cloud computing authentication using cancellable biometrics", IEEE, 10.1109/AFRCON.2013.6757821, Sept. 2013