Cloud Security Architecture Based on User Authentication and Symmetric Key Cryptographic Techniques

Abdul Raoof Wani[1], Q.P. Rana[2], Nitin Pandey[3]

[1]Amity University Noida, [2]Jamia Hamdard University [3]Amity University Noida
[1]wanirauf@gmail.com
[2]qprana@jamiahamdard.ac.in
[3]Npandey@gmail.com

***Abstract* — Cloud computing environment gives people to share resources, services and information. This environment is adopted by large number of organizations, so the rapid transition towards the cloud has fuelled concerns on security perspective. Encryption algorithms play main role in solving such kind of problems in the cloud computing environment. This paper proposes the structure for cloud security with efficient security in communication system and AES based file encryption system. This security architecture can be easily applied on PaaS, IaaS and SaaS and one time password provides extra security in the authenticating users. This paper presents the security of whole cloud computing environment.**

***Keywords* — AES, SHA3,Blowfish, Cloud Security Architecture, Cloud computing.**

I. INTRODUCTION

Cloud computing is having the capacity to dispose off the prerequisites for setting up high cost computing framework and promises to provide flexible architecture which is accessible from anywhere. The data in the cloud computing resides over an arrangement network resources which enables position of the requirements for setting up costly data centers framework and information to be acquired via virtual machines and these serves might be arranged in any part of the world. The cloud computing environment is adopted by large number of organizations so the rapid transition towards the clouds has fuelled concerns on security perspective. There are number of risks and challenges that have emerged due to use of cloud computing. Cloud computing is still an advancing innovation technology that exchanges current innovating technology and figuring thoughts into utility like arrangements. The relocation diminishes the cost and time of creation and offers better execution and unwavering quality [1].Cloud computing is a network access to the pool of resources well-defined which are convenient and well defined which require the minimum effort. [2]The advantages of distributed computing incorporate diminishing the equipment and support cost, accessibility around globe, adaptability and to a great degree mechanized process. It conveys unfathomable advantages to both Individuals and ventures by decreasing the requirement for client association by concealing specialized points of interest, for example updates, licenses and support from its clients. Cloud can like wises provide improved safety over single server arrangements subsequently cloud totals resources and permits licensed security individual while as the typical organizations are restricted with system and network admin who won't be well learned about cyber security issues .With rising concerns regarding the cloud computing and security of data the prominent security algorithms especially symmetric algorithms could be widely used in cloud application services which involve encryption techniques. Cryptography is used in hiding information from intruders and storing it confidentially so that only those users and are able to whom it is intended for and communication this information securely. The use security algorithms minimize security concerns with the help of cryptographic and authenticating techniques, cryptography is the process of crafting message securely altering the data to be sent with encrypting the plain text by taking user data and then executing the reverse process called as decryption which is returning back to original text. The cryptography can resolve the problems in cloud computing regarding network data and server security.

Encryption is the fundamental tool for protecting sensitive information. The goal of cryptography is keeping data secure from unauthorized users. With the swift development in science of encryption, an innovative area of cryptography can be classified as symmetric key cryptography.[3] Single key, one key also known as symmetric key cryptography uses the same key at both encryption and decryption process. Due to the use single key for encrypting the big quantity of data can be processed at a very fast speed. [4] .There is no defined process within the cloud service providers for safeguarding and securing data from threats and attacks. The target of the cyber attackers is end user data which is being secured by the cloud using encryption techniques which are intended to make it impossible for the attacker to decrypt the cipher text. The long length of the key makes harder to decrypt the classified text and makes them secure as compared to short keys.

Presently lot of security models in the cloud security has been deployed but they are unable to secure the cloud computing environment completely [5][6][7]. A high level security model

is needed in E-commerce and other different kind of online businesses. The present security models are not able to provide security to the whole cloud computing environment but some of the security models are able to secure communication channel but are not cost effective[8][9]. There are some proposed models which deal with hardware encryption system for securing communication system which is very hard to implement and is only helpful in database system and does not deal with other security issues [10].

This work deals with the new security structure for cloud computing security which uses high ranked symmetric key cryptographic algorithms for securing the communication process. The files are encrypted with symmetric key crypto system and the concept of distributive key is used to provide the maximum security [11][12]. This model helps in solving main security issue related to communication between user and server and Blowfish algorithm is being used for that purpose.

II. RELATED WORK

With rise in the attacks, emphasis is by the clouds service providers at the users end to make data secure. The inconsistency in the selection of encryption decryption algorithms there has been given the low priority to the cloud performance. Cloud performance and data security can be achieved by using the appropriate cryptographic algorithm at end user. For unintentional and accidental use of algorithms, it is important to do the algorithm analysis to check the competency of that particular algorithm that may result in degradation of performance in encryption or decryption process. For applications which use real time data , an algorithm which might take long time would prove a hindrance for such applications such algorithms end up consuming a lot of power for computing and storage to execute, thus making the algorithm unusable in that environment.

There has been a lot of research in the field of cloud security and numerous security architectures has already been proposed. One of the proposed systems proposed by researchers is identification based security model but it's not sufficient to provide security to whole cloud computing environment [13]. Identifying the actual user is not sufficient to provide security in cloud computing. An identified based mechanism is used which is the part of Yao's Garbled circuit. It is used in securing data in cloud computing but its unable to provide security to whole cloud environment.[14][15].

Different encryption techniques are being used to secure cloud computing, AES encryption technique is used in lot of cloud security architectures but these models does not use the concept of distributed severs which makes them less secure and prone to attacks and only one successful attack is able to get control of the whole system. Some of these models provide secure communication but are not able to upload information in an encrypted form.[16][17][18]. Recently some other models are being research but they fail to meet the issues related to cloud computing environment.

III. PROPOSED ARCHITECTURE

We will use following encryption techniques in our propose model. The algorithms were selected on the basis of their performances on various parameters like encryption time decryption time memory usage, flexibility, scalability security AES for Secured file encryption.

- AES for file Encryption
- Blowfish algorithm for securing communication [19][20].
- SHA3 hashing to secure tables [21][22]
- One time password for authentication

Presently cloud security has become one of the greatest challenges to researchers all over the world, we have taken these issues in concern and tried to provide solutions to these issues. The data storage model for security in cloud computing is shown in figure 1

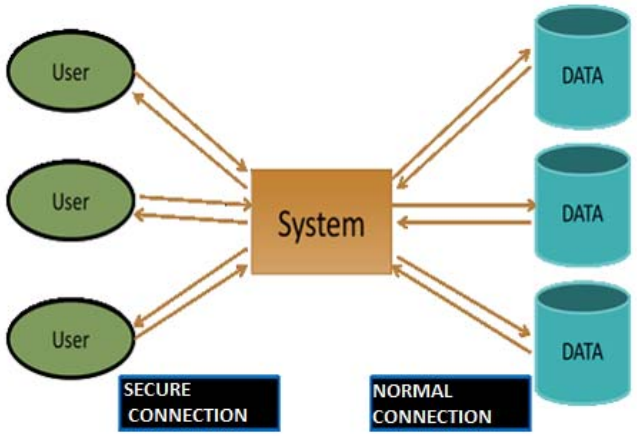

Fig. 1. Security Model

The users have to use the secure channel to the main system whether the user is new or old and the server computer is connected to data storage system. The servers in cloud computing are not dedicated but can be scaled as necessary. The proposed architecture uses blowfish algorithm to secure communication. The user requests for a file it is being served in the encrypted manner, encrypted with three fish algorithm , same applies with the password which are being used for the logging in the system. The files are later being decrypted on the receiving end with the blowfish algorithm resulting in the secure communication between user and system.

Every time the user wants to login he will require a onetime password. One time password keeps the user account secure from unauthorized access. The one time password is done randomly because the user defined passwords can be easily compromised. The newly generated password automatically erases the older password from the system and one password is for one time use only. The password is automatically sent to the registered mail account or the mobile number which will be verified for the authorized user. The generated password will be covered by the SHA 3 hashing to secure the tables. The

main purpose of this technique is to make system more secure and not to provide any loop holes for the unauthorized access.

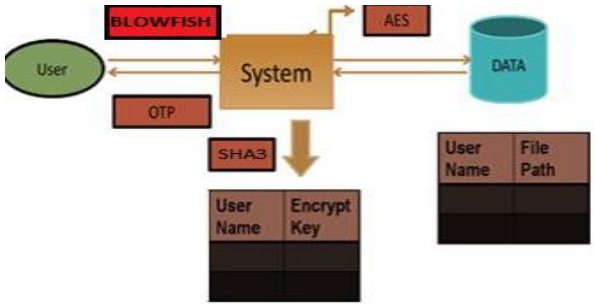

Fig. 2. Security Model Archictecture

The user can first time only upload the file after connecting to the system but afterwards it can both upload and download the file. The uploaded file is being encrypted by AES encryption algorithm. The architecture uses 128 bit keys for encryption but we can also use 192 and 256 bits. The keys generated by the system are random and are used only once in the system. The encryption and decryption process is done by the same key. The SHA3 hashing technique is used to secure the user accounts which makes sure that the unauthorized user doesn't gain access by checking the database table.

The login process makes sure whether the user is authentic or not. When user want to retrieve a file from the system, the main server serves the key which then matches the user account which is already being saved in the database secured with SHA3 hashing. The location of the encrypted file is only know to the main server. Figure 2 represents the proposed security architecture.

AES

AES symmetric block cipher feistel structure that means it uses same key for both encryption and decryption AES algorithm can only accept a block size of 128 bits and a choice of three a128, 192, 256 key length permuted with variable 10, 12 and 14 rounds.

The variable nature of Rijndeal provide it with a great security and the key size up to 256 gives it a resistance to the future attacks [23].

Blowfish

Blowfish is a feistel structure symmetric key algorithm. It has a 64 bit block size and the key varies from 32 to 448 bits it uses 16 rounds and has large key dependent s box. There are 4 S boxes in blowfish algorithm and same algorithm is used in inverse for decryption [24][25][26].

Blowfish security lies in the key size providing high level of security. It is invincible against different key attacks because of many round which are being used by master key making such attacks infeasible.

SHA3

Secure Hash Algorithm is the cryptographic algorithm producing hash values of 224, 256,348,512 bits by using internal 1600 bits.SHA3 can vary according to the earlier two versions requirement and length of the message is of infinite length which makes it powerful from the earlier two versions.

The sponge function used by SHA3 makes it more secure than SHA2 and SHA1 and it minimizes the chance of collision using large number of bits

IV. PERFORMANCE EVALUATION MATRIX

The experimental design was performed on laptop with core i7 processor on windows 10 environment with the input files ranging from 83.3 Kb to 1.54 Mb. The language used to check the space and complexity was java. Time and space complexity depends on lots of things like hardware, operating system, processors, etc. but we have only taken execution time into consideration. The objective we tried to achieve in terms of memory occupied by an algorithm during the course of execution was obtained by the methods like

- getruntime().freememory()
- getruntime().totalmemory()

with the run time memory management options compiling heap memory, stack memory etc. The other objective was how much time an algorithm takes right from the input of a file to the desired output.

The evaluation parameters are

- Encryption time
- Decryption time
- Memory usage
- Flexibility
- Scalability
- Security

TABLE 1: ENCRYPTION TIME (MILLISECONDS)

KB	AES	DES	3DES	BLOW FISH	RC4	IDE A	TEA
83.3	625	41	43	8	15	16	54
108	31	47	47	16	16	125	15
249	468	47	47	47	15	32	16
333	32	47	64	281	15	63	10
416	46	48	94	343	31	127	16
1370	141	110	243	78	47	78	41
2740	62	172	361	93	62	205	97
5480	78	296	749	156	63	325	170
10003	723	484	749	531	141	397	357
15483	798	690	1401	601	198	758	475
Average	300.4	198.2	397.8	215.4	60,3	212.6	125.1

TABLE II: DECRYPTION TIME (MILLISECONDS)

KB	AES	DES	3DES	BLOW FISH	RC4	IDEA	TEA
83.3	24	10	25	17	5	16	15
108	15	16	31	10	6	943	16
249	16	32	31	15	4	31	10
333	16	46	17	16	7	31	12
416	10	47	125	17	10	47	16
1370	31	78	187	62	12	45	40
2740	47	141	359	78	17	129	96
5480	31	225	678	156	48	218	158
10003	62	484	1346	234	55	351	304
15483	88	680	1988	305	89	597	545
Average	34.4	178.6	497.6	91	25.3	155.9	121.2

TABLE III: MEMORY USAGE (KB)

KB	AES	DES	3DES	BLOWFISH	RC4	IDEA	TEA
83.3	11014064	10081304	992712	580824	980952	259080	2097168
108	985312	10390693	20853952	1142800	1961832	2097168	259080
249	11244008	11169376	11169376	10968120	3211080	5497720	2097168
333	2230250	1061603	4256520	10791776	4629096	2097168	259000
416	4186640	5167096	7498084	3010032	33160	3124168	209040
1370	7063848	11187024	1321440	85711216	8675472	5172418	2349040
2740	6361832	125688808	10698640	17228432	12568808	2097168	2347008
5480	34660616	9927424	18077072	16506648	11823224	20971862	8963325
10003	60697448	60721016	120146520	59702576	130702776	12031904	17514192
15483	40728 9063	70648440	138223590	76209224	142526000	2097168	32708440
Average	54573308.1	31604278.4	33323790.6	28185164.8	317112400	5544582.4	6880346.1

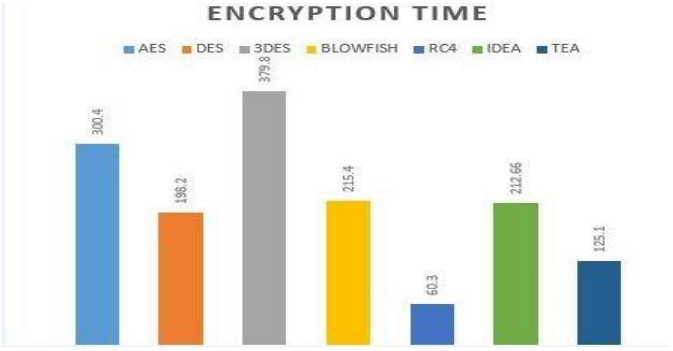

Fig. 3. Encryption time in milliseconds

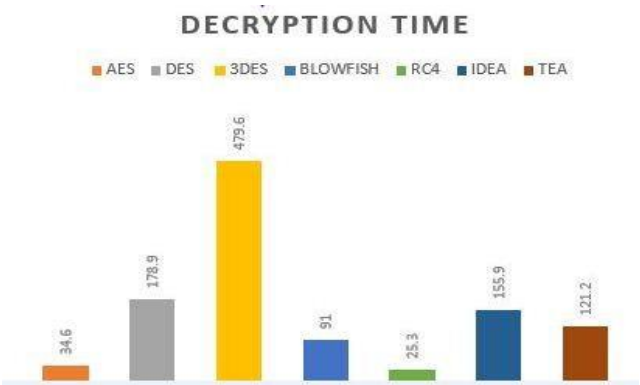

Fig. 4. Decryption Time milliseconds

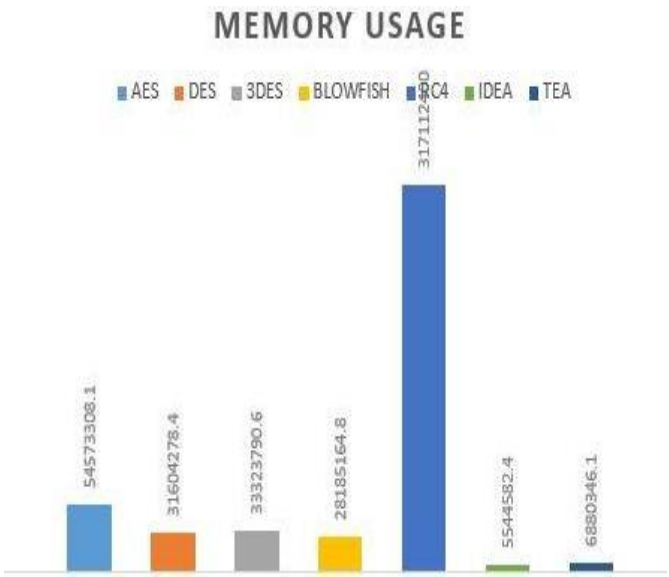

Fig. 5. Memory Usage in kilobytes

Experimental results of encryption algorithms are shown which shows all algorithms use same text files for ten experiments. By analysing the table RC4 is taking less encryption time while as the 3DES is taking maximum encryption time. In the second table RC4 and AES are having very less decryption time while 3DES is having maximum of all the algorithms. (Table 3) depicts the memory usage of all the algorithms in which IDEA and TEA are having very less memory usage while as RC4 is taking the maximum memory of all the algorithms. During the analysis it was found that AES will be best among all the algorithms in terms of flexibility, security, memory performance and usage. Blowfish is the second best parameters such as security, flexibility, encryption decryption time, scalability and memory usage, so we have used AES and blowfish in our proposed architecture

V. LEVEL OF SECURITY

Level of security of a particular algorithm depends on key size, the greater the key size stronger the algorithm and encryption.

TALBE IV: LEVEL OF SECURITY

Encryption Algorithms	Plain Text/Cipher Text)	Length Key Length (bits	No Rounds (bits)
DES	64 bit	56	16
3DES	64 bit	168	48
AES	128 bit	128,192,256	10,12, 14
BLOWFISH	64 bit	32-448	16
RC4	40 -2048 bits	variable	256
IDEA	64bits	128	8.5
TEA	64bits	128	32 cycles

TABLE V: flexibility and scalability

Algorithm	Flexibility	Modification	Comments
DES	No	None	No modifications are supported by DES
3DES	Yes	168	The DES key is extended to 168 bits.
AES	Yes	128,192,256	The AES is expandable and support modifications.
BLOWFISH	Yes	32-448	The structure of BLOWFISH is extendable to 448 bits
RC4	Yes	variable	Modifications supported
IDEA	No	128	No modifications supported.
TEA	No	128	No modifications supported.

TABLE VI: ADVANTAGES OF PRAPOSED ARCITECTURE

Discussion points	Ways of ensuring security	Information leakage probability	Complexity
Identification Based Model	Only identify the authorized person, so hacker can get access on database	Medium	Low
File encryption based Model	Key and file both remains in one server. So, getting access on one server helps to get all information	Medium	Medium

TABLE VII: ADVANTAGES OF PRAPOSED ARCITECTURE

Discussion points	Cost of establishing and maintaining	Ensuring User Authentication	Security Breaking probability
File encryption based Model	Medium	If key is chosen by user, then slightly authenticate users	Medium
Secured channel using model	High	Probably not maintained	Medium
Proposed Architecture	Medium	One time password system is used for user authentication	Lower than others

VI. CONCLUSION

This paper proposes a new security architecture for cloud security which uses symmetric cryptographic algorithms for encryption purposes. This architecture uses AES, Blowfish and SHA3 and one time password to secure the whole system. The proposed system is very secure which makes it difficult for intruders to get into the system because the intruders need to get control over all the servers. The execution time can be low because of the implementation of algorithms on different servers. In our future work we would like to find out the execution results which would help our proposed architecture to demonstrate with better results. We will work on different users and conditions to prove the efficiency of this architecture. We would also work on the lighter encryption techniques which will reduce the execution time of the proposed architecture.

REFERENCES

[1] Munir, Kashif, and Sellapan Palaniappan. "Framework for secure cloud computing." *Advanced International Journal on Cloud Computing: Services and Architecture (IJCCSA)* 3.2 (2013).

[2] Mell, Peter, and Timothy Grance. "The NIST Definition of Cloud Computing, Jan, 2011."

[3] Meyer, Carl H. "Cryptography-A state of the art review." *CompEuro'89., 'VLSI and Computer Peripherals. VLSI and Microelectronic Applications in Intelligent Peripherals and their Interconnection Networks', Proceedings.* IEEE, 1989.

[4] Krutz, Ronald L, and Russell Dean Vines. *Cloud security: A comprehensive guide to secure cloud computing*. Wiley Publishing, 2010..

[5] Bhadauria, Rohit, et al. "A survey on security issues in cloud computing." *IEEE Communications Surveys and Tutorials* (2011): 1-15.

[6] A Vouk, Mladen. "Cloud computing–issues, research and implementations." *CIT. Journal of Computing and Information Technology* 16.4 (2008): 235-246.

[7] Hu, Ye, et al. "Resource provisioning for cloud computing." *Proceedings of the 2009 Conference of the Center for Advanced Studies on Collaborative Research*. IBM Corp., 2009.

[8] Catteddu, Daniele. "Cloud Computing: benefits, risks and recommendations for information security." *Web application security*. Springer, Berlin, Heidelberg, 2010. 17-17.

[9] Chigozirim, Ajaegbu. "Towards building a secure cloud computing environment." *International Journal of Advanced Research in Computer Science* 3.4 (2012).

[10] Ngongang, Guy. "Cloud Computing Security." (2011).

[11] Kanmani, P., and S. Anusha. "A novel integrity scheme for secure cloud storage." *Intelligent Systems and Control (ISCO), 2015 IEEE 9th International Conference on*. IEEE, 2015..

[12] Kumar, Gunasekar, and Anirudh Chelikani. "Analysis of security issues in cloud based e-learning." (2011).

[13] Wu, Jiyi, et al. "Recent Advances in Cloud Security." *JCP* 6.10 (2011): 2156-2163.

[14] Shimbre, Nivedita, and Priya Deshpande. "Enhancing Distributed Data Storage Security for Cloud Computing Using TPA and AES Algorithm." *Computing Communication Control and Automation (ICCUBEA), 2015 International Conference on*. IEEE, 2015..

[15] Sadeghi, Ahmad-Reza, Thomas Schneider, and Marcel Winandy. "Token-based cloud computing." *International Conference on Trust and Trustworthy Computing*. Springer, Berlin, Heidelberg, 2010.

[16] A. Pandey, S. Som (2016), "Applications and Usage of Visual Cryptography: A Review" International Conference on "Reliability, Infocom Technologies and Optimizations (Trends and Future Directions) ICRITO 2016, 7-9 September 2016, IEEE Conference, indexed with **SCOPUS**, Amity University Uttar Pradesh, India, p.p. 375-381.

[17] Lenka, Sudhansu Ranjan, and Biswaranjan Nayak. "Enhancing Data Security in Cloud Computing Using RSA Encryption and MD5 Algorithm." *International Journal of Computer Science Trends and Technology (IJCST)–Volume* 2 (2014).

[18] Li, Hongwei, et al. "Identity-based authentication for cloud computing." *Cloud computing* (2009): 157-166.

[19] S. Som, S. Sinha, R. Kataria (2016) "Study On SQL Injection Attacks: Mode, Detection And Prevention", International Journal of Engineering Applied Sciences and Technology, Indexed in Google Scholar, ICI etc., Impact Factor: 1.494, Vol. 1, Issue 8, ISSN No. 2455-2143, Pages 23-29, June - July 2016.

[20] Kaur, Manmeet, et al. "Comparison of TACIT Encryption Algorithm with Various Encryption Algorithms." *International Journal of Electronics and Computer Science Engineering, page (1-10)* (2012). (2006).

[21] Cheong, Hon-Sang, and Wai-Kong Lee. "Fast Implementation of Block Ciphers and PRNGs for Kepler GPU Architecture." *IT Convergence and Security (ICITCS), 2015 5th International Conference on*. IEEE, 2015.2015.

[22] Arshad, Alia, and Arshad Aziz. "Compact implementation of SHA3-512 on FPGA." *Information Assurance and Cyber Security (CIACS), 2014 Conference on*. IEEE, 2014.

[23] Meera, K., P. Krishna Sankar, and K. Sriram Kumar. "Redundant file finder, remover in mobile environment through SHA-3 algorithm." *Electronics and Communication Systems (ICECS), 2015 2nd International Conference on*. IEEE, 2015.

[24] Kumar, Ashish, and Vishal Arora. "Analyzing the performance and security by using SHA3 in WEP." *Engineering and Technology (ICETECH), 2015 IEEE International Conference on*. IEEE, 2015.

[25] Phul S., Som S., (2016) "Symmetric Cryptography using Multiple Access Circular Queues (MACQ)", 2nd International Conference on Information and Communication Technology for Competitive Strategies (ICTCS-2016), Conference Proceedings by ACM – ICPS Proceedings Volume ISBN No 978-1-4503-3962-9, 4 – 5 March, 2016.

[26] Schneier, B. "Blowfish: One Year Later." *Dr. Dobbs Journal* (1995).

[27] Singh, Simar Preet, and Raman Maini. "Comparison of data encryption algorithms." *International Journal of Computer Science and Communication*2.1 (2011): 125-127.

[28] Ajay Vikram Singh, Moushumi Chattopadhyaya, "Mitigation of DoS Attacks by Using Multiple Encryptions in MANET", 2015 4th IEEE International Conference on Reliability, Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions), 2015 at AUUP, NOIDA, India, September 02-04, 2015.

[29] Ajay Vikram Singh, Bani Singh, M. Afshar Alam, "Issues and Challenges associated with Secure QoS aware Routing in MANETs" , International Journal of Research and Reviews in Ad Hoc Networks (IJRRAN), Vol. 1, No. 3, pp. 73-76,ISSN: 2046-5106, Science Academy Publisher, United Kingdom, September 2011.

[30] Seema Nath, Subhranil Som (2017), "Security and Privacy Challenges: Internet of Things", Indian Journal of Science and Technology, Scopus Indexed, included in 'Web of Science' and included in the list of journal recommended by UGC, Vol 10(3), DOI: 10.17485/ijst/2017/v10i3/110642, ISSN (Print) : 0974-6846 ISSN (Online) : 0974-5645, January 2017.