Mathematical Statistician and Engineering Applications
ISSN: 2094-0343
2326-9865

Three-Dimensional Authentication, Authorization & Access Control [AAA] Framework for Strong Authentication in Hybrid Cloud Environment

Megha Singh[1], Dr. Vijay R. Sonawane[2]

[1]Department of Computer Science & Engineering, Dr. A. P. J. Abdul Kalam University, Indore, India

Corresponding author: Megha Singh

maggii.megha@gmail.com

Article Info

Page Number: 7616 - 7629

Publication Issue:

Vol 71 No. 4 (2022)

Article History

Article Received*: 15 Oct 2022*

Revised*: 05 Nov 2022*

Accepted*: 10 Dec 2022*

Publication*: 30 Dec 2022*

Abstract

Cloud computing is the on demand sharing of resources, software and hardware solutions specially storage and applications in the way of services. It is widely adapted by many organizations due to versatile applications and use. Public infrastructure and heavy frequency use might make it vulnerable for different users. Cloud applications are vulnerable for several security threats and weaker authentication might be the reason for leakage of information or sensitive information. Poor authentication techniques and absence of proper authorization and access control might make such application entrusted and users might avoid its use. Data encryption could only provide safety on data over privacy or sensitivity but cannot prevent from unauthorized access. This research paper observes the need of authentication framework and hence proposed a three dimensional multi layer solution to improvise the strength of authentication along with authorization and access control. Some popular cases are considered to propose authentication layers for various scenarios. A java application was developed using Restful Api to implement concept of cloud computing and deployed and tested on EC2 instance of local hybrid cloud environment. The complete work ends with performance comparison based on computation time.

Keywords:-Cloud computing, Authentication, Authorization, Access Control, authentication framework, hybrid cloud

1. INTRODUCTION

Cloud computing is widely used and adapted by many organization. It is very popular because of the on-demand access of service. It provides services in all the possible ways whether it is in software, platform or infrastructure form. Many cloud vendors exists which are providing services free or in pay-per-use basis. Some vendors are providing free services to increase their business and enhancing the level of their company. These services are very supportive; lessen the computation time and requirement of memory. At every end cloud is trying its best to provide paramount

services to the users but major concern is the lack of security. Security can be achieved by encryption and vendors should also provide security feature to create compatible and secure environment [1].

Cloud security is the critical task, its services supports hardware and software which is used by the users conveniently. Some mechanism of encryption is performed to secure the data. Computations, operations and processing, these all are required to encrypt the data for security purpose. Cloud computing is an environment which creates the sharing of resources and storing of vast data. It is a storing centre whose limit ineffable. Virtualization, parallel computing, and distributed computing are the types of technologies on which cloud works. Important aim of cloud computing is that user can only utilize the required function and have to pay for what they use called as pay-per-use. Storing data in the cloud is a major data security issue, and storing data causes problems for users. Ensuring the accuracy of data provided by the service provider is also a big issue[2-3].

Cloud security refers to the set of technologies, applications, and infrastructure. Cloud computing allows storage of data through third party data centres. Using different service models like SaaS, PaaS, and IaaS organization avail cloud services. The service providers must ensure about the security of infrastructure and their client's data. It should be protected and must be authenticated rigorously [2-4]. Some of the instances are mentioned below which encourages a strong security mechanism for cloud storage.

1. Whenever any organization stores data on public cloud then there is a risk of accessing sensitive data, attackers may attack the data internally.
2. Cloud Security Alliance (CSA) is a threat awareness in cloud computing. So, the service provider must always check the authentication of user accessing to server.
3. More often the cloud service provider store data of many customers on same server, which results in access of user‟s private data. Thus, to handle and manage this type of issue cloud service provider should isolate data and store them logically.
4. Prevention and protection against unauthorized user leads to strong authentication.
5. Detection and prevention of attack on cloud system by monitoring cloud security.
6. Cloud service provider works as securing the hardware from unauthorized access and making system robust.

2. PROBLEM STATEMENT

Authentication is one of the important and primary principles of cloud security. It ensures that request has arrived from authenticated users or not. Authentication not only lengthens the procedure but might result in information leakage or misuse of user rights if breached [5]. This work attempts to propose different ways to implement authentication and also estimate computation time to execute the same. Our study observes that more than 80% security breaches and information leakage can be prevented with strong authentication. Strong authentication would not only increase the time of execution but may examine the patience of user. The study addresses that sensitive data is not only concerned to user‟s personal data but it may also be relevant to information or part of

processing. In healthcare solutions; pathology reports, rape victim diagnosis report, pregnancy, or miscarriage reports, etc. are truly susceptible and leakage of such information may compromise life of someone. This study also observes that most of the solution also relies on third party for establishment of trust through strong authentication. This technique not only enhances the access time but also create dependency on third party services. Another concern is the issue of trust where third party organizations automate their data for use by consumers [6-7]. Client doesn't depend on outsiders or it much of the time happens that outcast authentication providers are not strong. Verification and approval are the significant security confers that should be addressed so that lone the endorsed individual is qualified for validation and access. The user, who plays out an unapproved action, is the malignant aggressor or looters that should be saved and analyzed for future security purposes at the ideal time. Finally this work observes that single authentication technique or authorization approach is insufficient to keep data safe and secure. Improvement is expected around all possible ways of authentication i.e. authorization and access control. Due to versatility and applications of different authentication, authorization and access control approaches may cause confusion in front of developers and they may compromise the data integrity and privacy due to lack of knowledge. This study addresses the need of authentication framework along with authorization and access control to improve the performance of security in cloud computing application.

3. METHODOLOGY

The current situation guarantees that protection and security are now unavoidably required. As the impact of new technology reaches its peak, the security scenarios are making retrograde development [8].The study of all existing solutions addressed that there is strong need to design and implement a strong authentication framework along with authorization and access control to improvise the performance of AAA and ensure reduction of information leakage. This research work considers that every authentication technique is important and could be used in cloud computing. Performance and use of authentication technique may vary application to application and sometimes it could be sluggish. For example, if Wikipedia integrates mobile OTP verification before displaying the search results it would not only create unnecessary cost of system but also be stagnant.

Following authentication techniques has been considered for authorization purpose.

1. Username and password
2. Word Captcha
3. I am not Robot Captcha
4. Security Questions
5. One Time Password using Security Token
6. OTP using Mobile Phone
7. Device Verification
8. IP & MAC address Verification
9. Server verification using Kerberos
10. Single Sign In using Wallet

11. Biometric Devices
12. Voice Authentication
13. OAuth2 Authentication
14. Google & Facebook Authentication

This work also examined that all authentication schemes produces delay in response time and some may apply it with common reason. This research classified all of the aforementioned techniques into the several groups listed below:

Table 1.Authentication Schemes

Category	**Techniques**
User Authentication	Username and password
	Security Questions
	One Time Password using Security Token
	OTP using Mobile Phone
	Biometric Devices
	Voice Authentication
Human Interaction Verification	Word Captcha
	I am not Robot Captcha
	One Time Password using Security Token
	OTP using Mobile Phone
	Device Verification
	IP & MAC address Verification
	Biometric Devices
	Voice Authentication
Real Time Verification to prevent replay attack and script.	Word Captcha
	I am not Robot Captcha
	Security Questions
	One Time Password using Security Token
	OTP using Mobile Phone
	Server verification using Kerberos
	Single Sign In using Wallet
	Biometric Devices
	Voice Authentication
	OAuth2 Authentication
	Google & Face book Authentication
Device Verification	Device Verification
	IP & MAC address Verification
	Server verification using Kerberos
	Single Sign In using Wallet
	Biometric Devices
	Voice Authentication
	OAuth2 Authentication
Social Media Authentication	OAuth2 Authentication
	Google & Face book Authentication

Furthermore, this research work also carried out the importance of authorization in strong authentication mechanism. It also investigates the relation between access control and authentication and address that all the security schemes should be integrated with access control to define who can access what. The purpose of this research model is to improve performance of AAA in cloud environment. The study also explored that there are multiple cases when user will try to get login into system. Here, few most popular cases are considered to propose authentication layer in particular situation.

Case 1: Guest from anywhere.

Case 2: Registered User from unauthorized network and unauthorized computer.

Case 3: Registered user login from unauthorized network but authorized regular machine.

Case 4:Registered user login from authorized network but regular unauthorized computer machine.

Case 5: Registered user login from authorized network & authorized computer machine.

The work also considers data into three forms which are cited below:

1. Non sensitive
2. Sensitive
3. General [May be sensitive may not]

The research work proposed a framework based on security best practices and experimental analysis. All authentication schemes are implemented using java technology and tested for response time/computation time. This comparison helped a lot to obtain an authentication framework which is derived from practical experience more devoted to real world applications. It is observed that every model depends upon three factors; data sensitivity, access environment and authentication technique. Due to three dimensional nature of framework it could be known as Three Dimensional Authentication Authorization and Access Control Framework or in short 3DAAA.

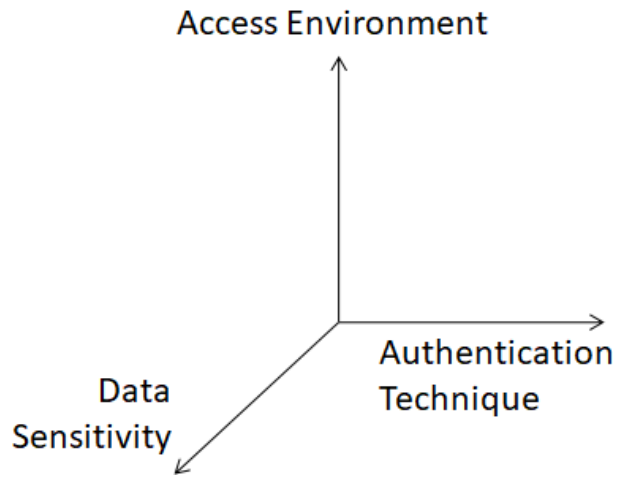

Figure1: Authentication Factors

With reference to different authentication, access environment and data sensitivity techniques multi layer framework has been recommended. Here, every individual layer represents access environment and rest data sensitivity differentiate the level of techniques at individual cases as layer. Methodology proposes different authentication techniques for different data sensitivity level for individual type of access environment. Here, this technique is a best practice for authentication and could be used as a combination to provide improvised authentication with authorization and access control.

Case 1: Guest Login from anywhere:

Since it is most insecure environment here, most authentication scheme with strong access control has been proposed. A framework for Case 1 is proposed below:

Framework for guest login from anywhere-

Table 2. Framework for Guest Login

Type of Data	**Authentication Technique**
Non Sensitive Data	Username and password
	I am not Robot Captcha
	OTP using Mobile Phone
	OAuth2 Authentication
	Google & Face book Authentication
Sensitive Data	Username and password
	I am not Robot Captcha
	OTP using Mobile Phone
	OAuth2 Authentication
General Data	Username and password
	I am not Robot Captcha
	OTP using Mobile Phone
	Server verification using Kerberos
	Single Sign In using Wallet
	OAuth2 Authentication
	Google & Facebook Authentication

Case 2: Registered user from unauthorized network and unauthorized computer

Verification of user registered need to be more strong because registered users have restricted rights and it need to be ensured using some access control scheme. Role based access has been proposed for this layer because it will classify the rights based on user rights and help to ensure „Who Can Access What".

Table 3.Framework for Registered User from unauthorized network and unauthorized computer

Type of Data	Authentication Technique
Non Sensitive Data	Username and password
	Word Captcha or I am not Robot Captcha
	One Time Password using Security Token or OTP using Mobile Phone
	Device Verification using IP & MAC address Verification
Sensitive Data	Username and password
	I am not Robot Captcha
	OTP using Mobile Phone
	Device Verification using IP & MAC address Verification
	Server verification using Kerberos
	Biometric Devices
	OAuth2 Authentication
General Data	Username and password
	I am not Robot Captcha
	Security Questions
	One Time Password using Security Token
	OTP using Mobile Phone
	Device Verification
	IP & MAC address Verification
	Server verification using Kerberos
	Single Sign In using Wallet
	Biometric Devices
	Voice Authentication
	OAuth2 Authentication
	Google & Facebook Authentication

Case 3: Registered user login from unauthorized network but authorized computer machine.

This user access case happens when user try to get login from home or another network but using regular or verified machine. Here, we can authorize user strongly and increase level of access by just assigning the role based access control. Attributes based access may be subject of choice of developer.

Table 4. Framework for Registered user login from unauthorized network but authorized computer machine

Type of Data	Authentication Technique
Non Sensitive Data	Username and password
	Word Captcha

	IP & MAC address Verification
	Single Sign In using Wallet
	OAuth2 Authentication
	Google & Face book Authentication
Sensitive Data	Username and password
	I am not Robot Captcha
	One Time Password using Security Token or OTP using Mobile Phone
	Device Verification using IP & MAC address Verification
	Server verification using Kerberos
	OAuth2 Authentication
General Data	Username and password
	I am not Robot Captcha
	Device Verification
	IP & MAC address Verification
	Single Sign In using Wallet
	OAuth2 Authentication
	Google & Facebook Authentication

Case 4: Registered user login from authorized network and unauthorized regular machine.

This is more sensitive case because someone who is not registered with the network is trying to get access into the system. So, access control and authentication need to be stronger. Combination of Role base Access Control and Attribute based Access Control has been proposed.

Table5. Framework for Registered user login from authorized network and unauthorized regular machine.

Type of Data	**Authentication Technique**
Non Sensitive Data	Username and password
	Word Captcha
	IP & MAC address Verification
	Single Sign In using Wallet
	OAuth2 Authentication
	Google & Face book Authentication
Sensitive Data	Username and password
	I am not Robot Captcha
	One Time Password using Security Token or OTP using Mobile Phone
	Device Verification using IP & MAC address Verification
	Server verification using Kerberos

	OAuth2 Authentication
General Data	Username and password
	I am not Robot Captcha
	Device Verification
	IP & MAC address Verification

Case 5: Registered user login from authorized network and authorized regular machine.

This case is regular useful case where user will login from regular network and regular machines. Here, we can authorize user strongly and increase level of access by just assigning the role based access control. Attribute based access may be subject of choice for the developer.

Table 6. Framework for Registered user login from authorized network and authorized regular machine.

Type of Data	**Authentication Technique**
Non Sensitive Data	Username and password
	Word Captcha
	IP & MAC address Verification
	Single Sign In using Wallet
	OAuth2 Authentication
	Google & Face book Authentication
Sensitive Data	Username and password
	I am not Robot Captcha
	One Time Password using Security Token or OTP using Mobile Phone
	Device Verification using IP & MAC address Verification
	Server verification using Kerberos
	OAuth2 Authentication
General Data	Username and password
	I am not Robot Captcha
	Device Verification
	IP & MAC address Verification
	Single Sign In using Wallet
	OAuth2 Authentication
	Google & Facebook Authentication

4. EXPERIMENTAL ANALYSIS

Proposed framework is developed using Java Technology, as backend technology, MySql for database and HTML, CSS & Bootstrap and deployed on local cloud server. Computation time has

been considered as performance comparison purpose and evaluation is based on different input file size.

1. Performance evaluation of different authentication techniques.
2. Performance evaluation of individual proposed framework
3. Performance comparison of all proposed solutions for sensitive data.

4.1 Performance evaluation of different authentication techniques.

Table7. Performance Evaluation

Authentication Practice	**Level of Security**	**Average Computation Time Sec.**	**Observations**
Username and password	Moderate	10	Good technique but easy to break and their vulnerability is very common. Still can be used as primary technique.
Word Captcha	Poor	20	Poor technique. Tough to understand and some times inoperative.
I am not Robot Captcha	Good	1	Great technique. Very popular nowadays and help a lot to ensure human interaction.
Security Questions	Poor	10	Old technique. Usually used in forget password only. Memory based technique can be compromised if security question is too simple.
One Time Password using Security Token	Moderate	180	Expensive and time consuming technique. Users are required to keep security token always to get login into system.
OTP using Mobile Phone	Strong	60	Very popular and strong technique to integrate two level authentication and also ensures human interaction.
Device Verification	Moderate	3	Very popular in intranet based solution but may be a reason for easy compromise of security.
IP & MAC address Verification	Moderate	3	Very popular in intranet based solution but may be reason for easy compromise of security.
Server verification using Kerberos	Very Strong	100	Very strong help to ensure third party authentication at request and server level.
Single Sign In using	Moderate	1	Provides automatic login facility but

Wallet			need third party storage may because of leakage of sensitive information.
Biometric Devices	Strong	30	Very strong but very expensive and inconvenient.
Voice Authentication	Poor	15	Soft biometric suitable for low sensitive data.
OAuth2 Authentication	Very Strong	35	Very strong and help to ensure allotment of all services and authorization.
Google & Face book Authentication	Moderate	15	Provide third party login but not recommended because it stores data at third party side.

4.2 Performance Evaluation of individual proposed framework

Table 8: Average Computation Time

Cases	Non sensitive	Sensitive	General Data
Case 1	198	250	238
Case 2	189	266	236
Case 3	179	265	228
Case 4	175	245	239
Case 5	169	223	195

4.3 Performance evaluation of individual proposed framework

The graph represents the above mentioned cases of the proposed framework and their performance comparison. The comparative graph is based on the computation time (in seconds) for non sensitive data, sensitive data, and general data.

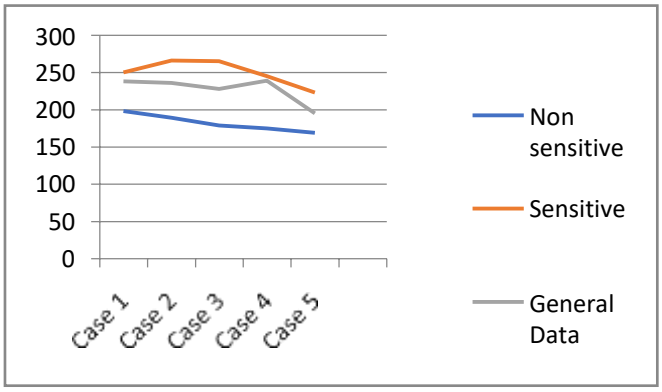

Figure 2.Performance Comparison of Different Proposed Framework [Computation Time -Seconds]

5. CONCLUSION

Starting with the requirement for variable authentication techniques combined with authorization and access control, this research study was initiated. It also investigated different authentication schemes and combined all as basic techniques to ensure all authentication schemes at one place. Detailed study helped, to divide them into different categories based on their need and use. Subsequently, data is also classified into three category based on their sensitivity. This research work observes that user access environment is very important and it may play the vital role before giving rights of access to any user. Therefore the research work proposed a 3 Dimensional Authentication framework for different cases. The complete work has been implemented using java technology for cloud environment and evaluated based on computation time. The complete observation concludes that:

1. Authentication does not refer to login, but it also ensures authorization and access rights.
2. Authentication and user rights allotment not only depend upon user roles but also on the user‟s environment and data sensitivity.
3. Proposed framework took high time in unauthorized network and unauthorized machines for registered users.
4. For authorized network with trusted machines it took less time and required less authentication strength.

Finally, work ends with five different three dimensional frameworks proposed to implant with five different conditions for better and affordable security.

REFERENCES

1. Joseph Emeras, SébastienVarrette, ValentinPlugaru and Pascal Bouvry “Amazon Elastic Compute Cloud (EC2) vs. in-House HPC Platform: a Cost Analysis” published in IEEE Transactions on Cloud Computing, San Francisco, CA, 2016, pp. 284-293.
2. Y. Xin et al., "Machine Learning and Deep Learning Methods for Cybersecurity," in IEEE Access, vol. 6, pp. 35365-35381, 2018.
3. C. Elbaz, L. Rilling and C. Morin, "Reactive and Adaptive Security Monitoring in Cloud Computing," 2018 IEEE 3rd International Workshops on Foundations and Applications of Self* Systems (FAS*W), Trento, 2018, pp. 5-7.
4. A. Akinbi and E. Pereira, "Mapping Security Requirements to Identify Critical Security Areas of Focus in PaaS Cloud Models," 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing, Liverpool, 2015, pp. 789-794.
5. Djellalbia, S. Benmeziane, N. Badache and S. Bensimessaoud, "An adaptive anonymous authentication for cloud environment," 2015 International Conference on Cloud Technologies and Applications (CloudTech), Marrakech, 2015, pp. 1-8.

6. Wei Li, "An adaptive security model for communication on cloud," Proceedings of 2011 International Conference on Computer Science and Network Technology, Harbin, 2011, pp. 1964-1967.
7. K. K. Mar, Z. Hu, C. Y. Law and M. Wang, "Securing cloud data using information dispersal," 2016 14th Annual Conference on Privacy, Security and Trust (PST), Auckland, 2016, pp. 445-448.
8. Kharade, K. G., Kharade, S. K., Sonawane, V. R., Bhamre, S. S., Katkar, S. V., &Kamat, R. K. (2021). IoT Based Security Alerts for the Safety of Industrial Area. In Recent Trends in Intensive Computing (pp. 98-103). IOS Press.
9. Nhlabatsi et al., "Traceability for Adaptive Information Security in the Cloud," 2014 IEEE 7th International Conference on Cloud Computing, Anchorage, AK, 2014, pp. 958-959.
10. I. A. Althamary and E. M. El-Alfy, "A more secure scheme for CAPTCHA-based authentication in cloud environment," 2017 8th International Conference on Information Technology (ICIT), Amman, 2017, pp. 405-411.
11. M. Kim, H. Jeong, E. Choi, "Context-aware Platform for User Authentication in Cloud Database Computing," International Conference on Future Information Technology and Management Science and Engineering Lecture Notes in Information Technology, vol.14, pp. 170-176, 2012.
12. E. Guermazi, M. Ben Ayed and H. Ben-Abdallah, "Adaptive security for Cloud data warehouse as a service," 2015 IEEE/ACIS 14th International Conference on Computer and Information Science (ICIS), Las Vegas, NV, 2015, pp. 647-650.
13. Krithikashree.L, S. Manisha, Dr.Sujithra.M. Audit Cloud: Ensuring Data Integrity for Mobile Devices in Cloud Storage. 9th ICCCNT, IISC, Bengaluru India, July 10-12, 2018.
14. Nan Zhangl, XiaoyuWul, Cheng Yangl, YinghuaShenl, YingyeChengl, “A lightweight authentication and authorization solution based on Kerberos”. Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC). 3rd, 5th October, 2016 IEEE.
15. AnshuKirar, Arun Kumar Yadav and SupriyaMaheswari, “An Efficient Architecture and Algorithm to Prevent Data Leakage in Cloud Computing using Multi-tier Security Approach”, Proceedings of the SMART -2016, IEEE, 5th International Conference on System Modeling& Advancement in Research Trends , 25th _27'h November, 2016.
16. Xiong H, Zhang H, Sun J (2018) Attribute-based privacy-preserving data sharing for dynamic groups in cloud computing. IEEE Syst J.
17. Algarni A (2019) A survey and classification of security and privacy research in smart healthcare systems. IEEE Access
18. Ali M, Dhamotharan R, Khan E, Khan SU, Vasilakos AV, Li K et al (2015) SeDaSC: secure data sharing in clouds. IEEE Syst 11:395–404.
19. Al-Assam H, Hassan W, Zeadally S (2019) Automated biometric authentication with cloud computing. In: Biometric-based physical and cybersecurity systems. Springer, pp 455–475.

20. A. Cecil Donald, A. Jenis and L. Arockiam, "An Authentication Mechanism to Enhance Security in the Cloud Environment," International Journal of Current Engineering and Technology, vol.4, no.5, 2014.
21. A. Gupta, P. Faraboschi, F. Gioachin, L. Kale, R. Kaufmann, B.-S. Lee, V. March, D. Milojicic, and C. Suen, "Evaluating and improving the performance and scheduling of hpc applications in cloud," Cloud Computing, IEEE Transactions on, vol. PP, no. 99, pp. 1–1, 2014.
22. A. Marathe, R. Harris, D. K. Lowenthal, B. R. de Supinski, B. Rountree, M. Schulz, and X. Yuan, "A comparative study of high-performance computing on the cloud," in Proceedings of the 22nd international symposium on High-performance parallel and distributed computing. ACM, 2013, pp. 239–250.
23. D. Moody, R. Perlner, A. Regenscheid, A. Roginsky and L. Chen. Report on Pairing-based Cryptography. Journal of Research of the National Institute of Standards and Technology 2015, Volume 120, pp. 11-27.
24. AkshitaBhandari, Ashutosh Gupta, Debasis Das, "A framework for Data Security and Storage in Cloud Computing", 2016 International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT).
25. Nair, Nikhitha K., K. S. Navin, and Soya Chandra. "Digital Signature and Advanced Encryption Standard for Enhancing Data Security and Authentication in Cloud Computing." (2015).
26. Hyun-Suk Yu, Yvette E. Gelogo, K J Kim, "Securing Data Storage in Cloud Computing", J. of Security Engineering, June 2012, pp.252-259.
27. KhushbuJakhotia, RohiniBhosale, Dr.Chelpa Lingam, "Novel Architecture for Enabling Proof of Retrievability using AES Algorithm". Proceedings of the IEEE 2017 International Conference on Computing Methodologies and Communication (ICCMC).
28. Amrita Jain, VivekKapoor, "Secure Communication using RSA Algorithm for Network Environment", International Journal of Computer Applications, Vol. 118, No. 7, May 2015.