IJCTA, 9(26) 2016, pp. 121-128

Data Security Mechanism for Public Cloud through Cloud-Based Secure Authentication

R Tamilarasi[1] and S Prabu[2]

ABSTRACT

The data security in public cloud becomes a great challenge and becomes more and more important in cloud computing environment. Cloud computing gives the best platform or service to store the data and image for various organizations like small scale to large scale organizations. The public cloud gives access to all the authenticated users, it is mandatory to secure the data from unauthorized user's access. This paper discusses about the multiple encryption techniques with three level data protection mechanism for providing security to the data which is stored in public cloud. The study mainly focuses on security issues like Authentication, Confidentiality and Data leakage. This study provides security for data and image and also to handle Denial of Service attacks both internal and external, brute force attack and man-in-the-middle attack. Public Encryption Algorithm (an improvised AES) has been implemented to safeguard data through multiple encryptions for better data security in the public cloud. To improve the security, authentication, confidentiality of data and to avoid data leakage a three-level data protection is implemented. Cloud-Based Secure Authentication (CSA) protocol suite is implemented for providing secure authentication mechanism in public cloud. For confidentiality of data AES with multiple encryptions is implemented. This multiple encryption method provides better security than in existing AES single encryption method. The three-level data protection architecture provides confidentiality and also prevents the data and image leakage in public cloud computing.

Keywords: Advanced Encryption Standard; Authentication; Cloud computing; Public cloud DIMs security; Three-level data protection (TDP).

1. INTRODUCTION

The data security is one the most essential part in cloud storage in recent days. Data security is highly discussed issue in the field of computer science and information technology. The cloud computing plays a vital role in business and IT sector. Generally it is a web based program to access anything anytime. It is like to "Pay and Use" approach. In the below figure 1, we can see three service model of cloud computing in this paper, therefore.

- Saas (software as a service)
- Paas (Platform as a service)
- Iaas (Infrastructure as a service)

In SaaS representation the cloud provider design with perform the function programming in the cloud. The cloud consumer recovers an appliance and store within the web service, that one starting with cloud consumer. Next the Platform as a Service (PaaS) design the cloud supplier conveys the cloud platform that one incorporates working frameworks and software design implementation environment. The appliance designers are creating and run the operating systems in a cloud infrastructure. An administrator of the cloud requirement nor yet stress over the expanse and trouble in view for obtaining else requesting then taking

[1] Research Associate, MS by Research, VIT University, vellore-14, *E-mail: tamilarasi.r2014@vit.ac.in*

[2] Associate Professor, VIT University,vellore-14, *E-mail-sprabu@vit.ac.in*

care of the fundamental equipment and programming. This paper succeeds overview in regard to relevant security issues in cloud computing, for example, Authentication, Confidentiality and Data Leakage.

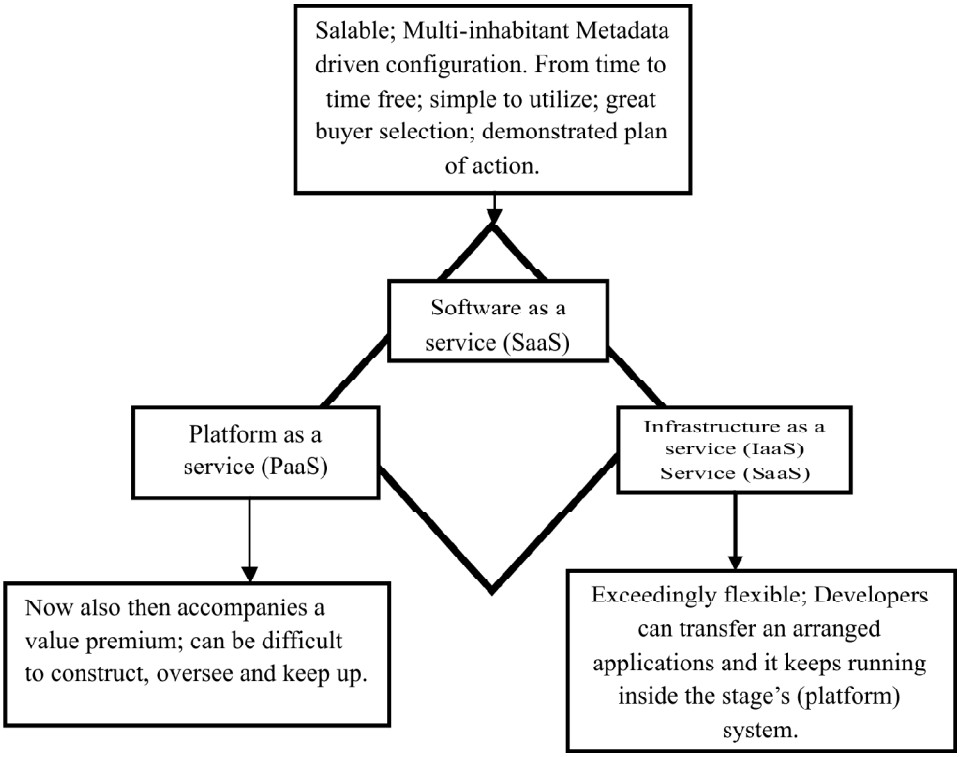

Figure 1: Cloud Service Model

2. RELATED WORK

Large number of work is completed in finding efficient procedures like authentication, confidentiality and data leakage in cloud computing. Our work is to provide high level data and image security in public cloud. Many authentication techniques are using in cloud computing. (Pradeep Kumar *et al.*, 2014) developed on Group Key Authentication protocol gives confirmationalso information protection along with sensible validation time likewise data diminish, data activity in the cloud computing and at the same time expands the Quality of Service (QoS).(Amlan *et al.*, 2011) inspect and additionally the point of solid client validation structure in considered in cloud computing as well as the considerable measure of security qualities in particular; character administration, common confirmation, a single-use symmetric key is understanding between the client, cloud service provider and client benevolence (i.e., secret word change extent)before go into the cloud. (Woei-JiunnTsaur *et al.*, 2012) Proposed a self-checked timestamp framework to offer the savvy (smart) card-based confirmation plan not just successfully accomplish secret key verified key agreements well as maintain a strategic distance from the trouble of actualizing check synchronization in multi-server environments. (Radhadevi and Kalpana, 2012) presents a use of AES (Advanced Encryption Standard) operations in image encryption and decoding. It expects to give client fulfillment by transmitting individual and sensitive data safely. (Anna Squicciarini *et al.*, 2010) proposed a three-level data protection structure comprising of three protection systems which contrast as indicated by the level of security required by the end-users.

3. BENEFITS OF AES ALGORITHM

(AJ Elbert *et al.*, 2007) presented the AES block cipher algorithms produce fitted and fast usage furthermore it used for the amount of data encryption. (Jyothi *et al.*, 2008) proposed hardware execution of AES algorithms

is faster and more secure than software execution. (Qing-Xiang et.al, 2009) presented AES algorithms it is a standout amongst the most developed secret key is symmetric key encryption algorithms. As well as its safety, adaptability, simple onto utilize highlights, in business part the AES algorithm is broadly utilizing. The utilization of advanced encryption standard method within bookkeeping data safety can be able to prevent spiteful stealing and leakage of bookkeeping data from inside to external for guaranteeing the security accounting data. (Sudha.M et.al, 2010) AES security system likewise is utilized to perform verification and encoded information transfer to assigned data confidentiality. (Deguang Le et.al, 2010) presented another techniques of AES parallel cipher text is an organized and added to a rapidly data encryption framework in view of GPU (Graphics Processing Units). (Ahmed B et.al, 2011) AES algorithm produce abnormal (important) state and safety using helpful (medical) picture encryption however which takes long time use. (AbhaSachdev and Mohit, 2013) presenting AES encoded algorithm, using this algorithm provides cloud users data safety and security on checking along with various attacks. Executing algorithm of AES is protecting of information output is more favorable circumstances of diminishing, it takes less memory and less execution time contrasted with various algorithms. (Quist-Aphetsi et.al, 2014) presented AES techniques and Visual cryptography are utilized to safety and secure unstablebiometric pictures. Cryptography strategy techniques of AES are one of the foremost by and large algorithms. (Kiruthika et.al, 2015) discussed AES encryption algorithm provides data security and also utilizes memory then it takes a lesser amount of evolution time. Likewise it provides wellbeingwith protecting the customer information contrasted with different algorithms.

Table 1
Comparison of Various Encryption Algorithms
(Chanderkani 2013), (Vanyadiwan 2014)

Characteristics	*AES*	*RSA*	*DES*
Established	2001	1997	1970
Key size	128,192 and 256	variant	56
Key type	Private key	Public key	Private key
Block size	128-bits	1024-bits	64-bits
Security	Wonderful	Good	Not enough
Implementation speed	More fast	Slow	Very slow
Number of rounds	128(10),192(12),256(14)	1	16

4. METHODOLOGY

In the proposed design, we have utilized three levels of protection structure in fig. 2.

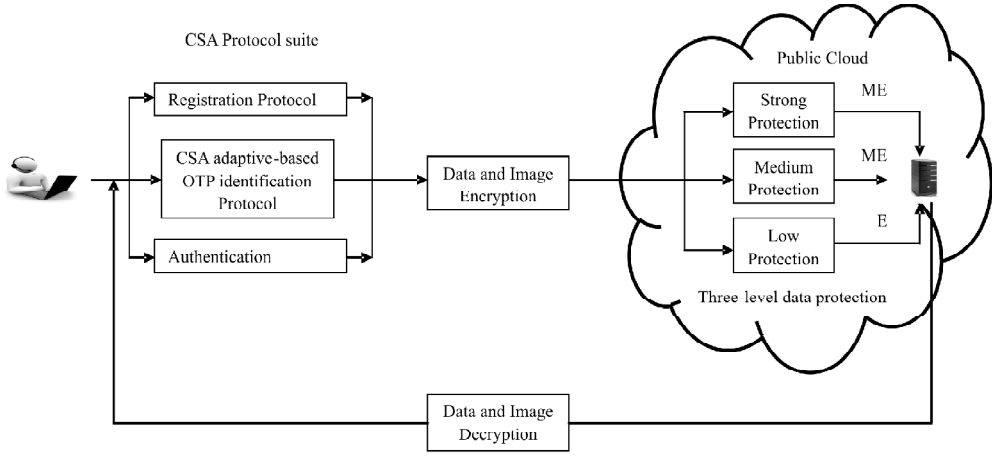

Figure 2: Proposed system architecture

In the first place explore the Cloud-Based Secure Authentication (CSA) Protocol suite, it is utilized to create the confirmation procedur.

(A) Cloud-Based Secure Authentication Protocol suite

The three stage Cloud-Based Secure authentication protocol suite proposed by Marwan Darwish el.al, (2015) has 1. Registration protocol, 2.CSA Adaptive-Based Identification Protocol. The private cloud has been considered only for SaaS under this CSA protocol. This paper proposes public cloud security for data and image (DIMs) in PaaS. The OTP identification protocol is used to stop brute force attack in a public cloud. The CSA protocol suite identifies Dos attacks (internally and externally) through the three secure strategies that is Registration protocol, CSA Adaptive-Based OTP Identification Protocol and Authentication Protocol (in fig. 3) this provides solid security for public cloud data and images in PaaS.

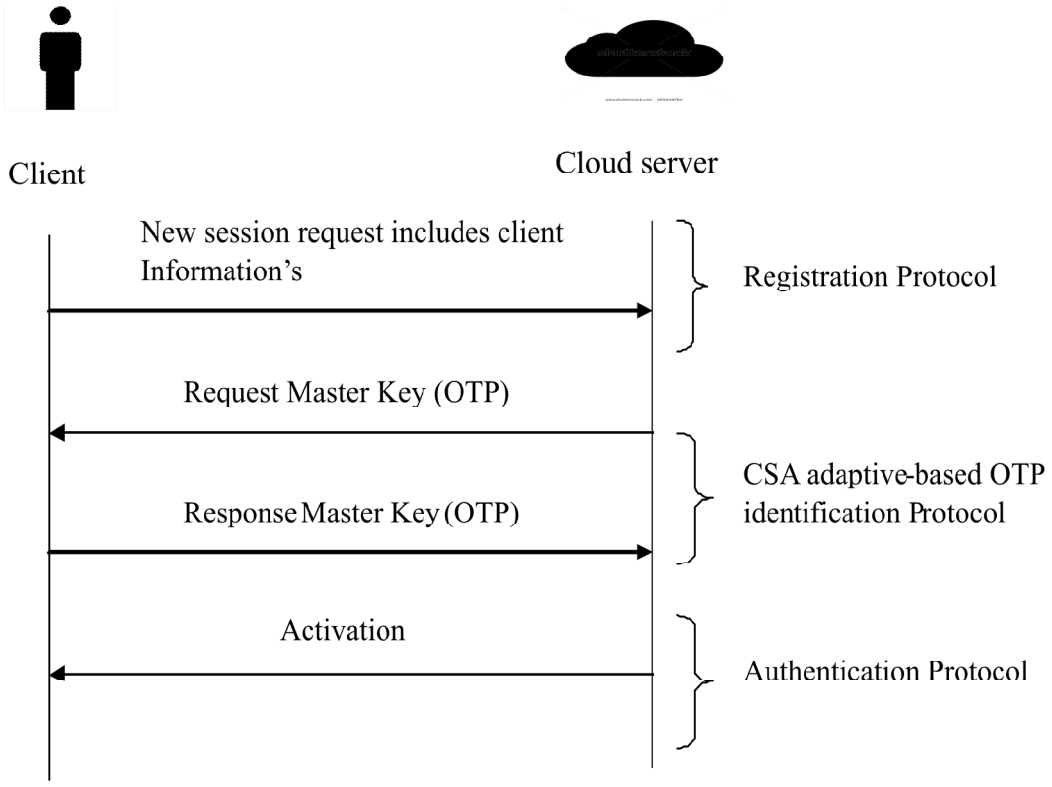

Figure 3: Cloud-Based Secure Authentication Protocol

(i) Registration Protocol: In the CSA enlistment (registration) convention, the cloud consumer and cloud server will allow the required identity data to enlist the cloud consumer into the cloud server database. As shown in fig.3, the registration process begins the registration process starts when the client submits all of the required data to cloud server. This information's includes username, password, age, gender, Email Address and Mobile number that are required by the cloud administration supplier. Then the cloud administrator will verify the client details, and also it's stored in cloud database server.

(ii) CSA adaptive-based OTP identification protocol: Cloud provider has to send master key to cloud user. Master key is nothing but OTP numbers. Generally, One-time password is send in four digits values or three digits values but here we using and sending five digits values to seven digits not only values including some special characters in order to achieve better security than the alphanumericalpassword, So it providesmore security and then aware of brute force attacks in internally and externally in public cloud computing.

(iii) Authentication protocol: At that point cloud server at last checked Cloud adaptive OTP recognizable proof convention and give confirmation activation procedure to cloud client.

B. AES Encryption Algorithm: This paper discusses with the Advanced Encryption Standard techniques for DIM's security in public cloud server. It provides more security and privacy of information as well as utilizes multi-level encryption procedures. AES considers three different key lengths: 128, 192, or 256 bits. Whereas Prasanthi O and Subbareddy (2012) developed one using just the 192-bit key Encryption comprises of 10 rounds of preparing for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys. In this paper we have examined 192 bits, 12 round and 24 bytes (fig.4) this applies for each encryption and decryption with the special case that every stage of around the decryption techniques is the opposite of its partner in the cipher text method. The four phases are as per the following: 1.Substitute bytes 2.Shift rows 3.Mix Columns 4.Add Round Key.

To appreciate the preparing steps utilized as a part of theone circular, it is foremost to think about 192-bits obstruct comprising of 4 × 6=24 bytes, organized to takes after:

Table 2
24 bytes matrix

byte0	byte4	byte8	byte12	byte16	byte20
byte1	byte5	byte9	byte13	byte17	byte21
byte2	byte6	byte10	byte14	byte18	byte22
byte3	byte7	byte11	byte15	byte19	byte23

The initial four bytes of 192-bit information square possess to start with a section in the 4 × 6 matrices of bytes.

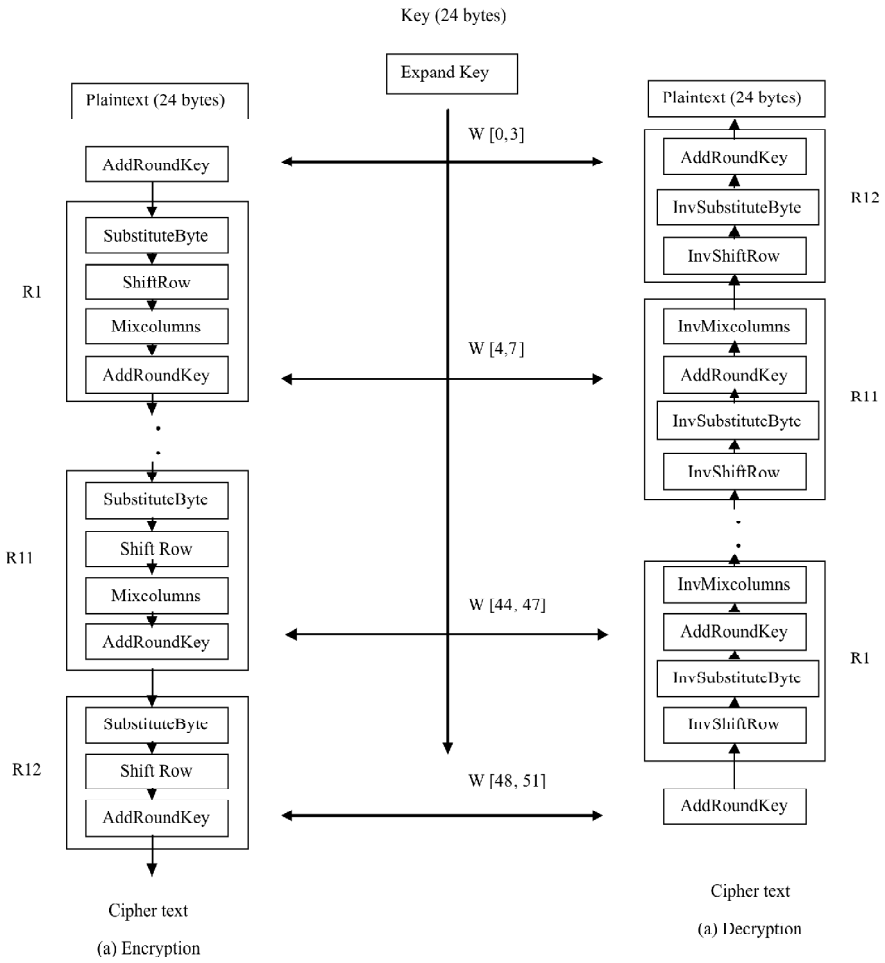

Figure 4: AES 192-bit Algorithm

(C) Three-level Data Protection Architecture (TDP)

The third level of proposed architecture is three-level data protection method which provides data and image (DIMs) security. This three level data protection architecture are used and implemented in the private cloud for protecting the data leakage (Anna Squicciarini, Smitha, Dan Lin, 2010). In this paper, we have proposed the three-level data protection (TDP) method in the public cloud using data and image security purpose. This TDP is having three level of protecting they are Strong protection (SP), Medium Protection (MP) and Low protection (LP)

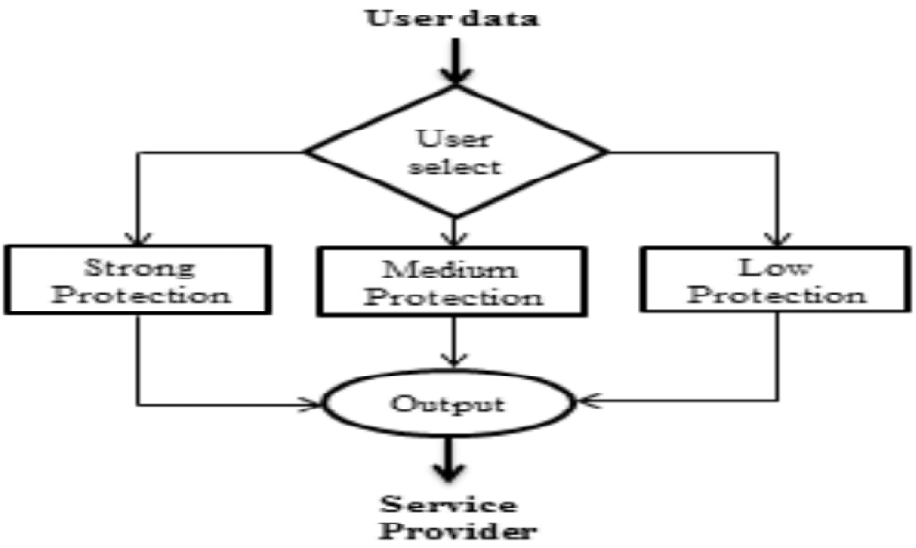

Figure 5: Three-level data protection Architecture

(i) Strong protection: In strong protection level hypersensitive data will be protected from other users. The risk of indexing being coordinated on a sensitive part of the report that cloud prompt protection leaks. Strong protection provides high- level of data and image security and also it hides the data from other users. To resolve the confidentiality problem of the data, multiple encryption was done in this strong protection security level. The user also cannot view the overview of the data or image in this security level, so the users can store confidential data like; Government data, military data, health records, etc. **(ii) Medium protection:** The index is built on the information available in the cloud. The medium protection provides strong data and image security of the available information, because in this protection level multiple encryptions was applied to the data and image. It shows only the index to other users but they cannot access data or image available in the cloud. **(iii) Low Protection:** A single encryption technique is used in the low protection level. In this technique, only the index is visible to the users and they cannot access that particular data.

5. ANALYSIS OF THE SCHEME

(i) Man-In-The-Middle : Our plan can oppose against man in the middle attack utilizing the procedure of a one-time secret word utilized as a part of the three-level protection plan, so regardless of the possibility that a malevolent client captures the password during the confirmation stage, the secret key would have lapsed (expired) and couldn't be utilized for the following session.**ii.Brute-force attacks:** The plan opposes against word reference and brute-force attacks. In fact, the plan utilizes a two-element authentication [<Un , Ps >, OTP] so regardless of the fact that a brute-force or a word reference or dictionary attack could be connected and regardless of the fact that the secret word is uncovered, it will be a lapsed password. Then couldn't found the OTP no in light of the fact that the three-level assurance strategy is utilizing some extraordinary characters, so why to attempt to split such an out of date watchword? Clearly, these assaults are completely

wiped out.**iii.Denial-of-service attack:** DoS attacks can bring about a major break in security.DoS attacks speak to significant security dangers in a cloud computing environment, where the resources are shared by numerous clients. DoS attacks focus on the resources or services trying to render them inaccessible by flooding the framework with substantial measures of simulated movement. ManagingDoS attacks at all layers of cloud frameworks is a noteworthy test because of the trouble of recognizing the aggressors' solicitations from legitimate client demands, especially when the information are exchanged between the layers of the cloud computing framework.It is useful now to give a correlation amongst three-level protection and some current cloud authentication. Table 5 is given as an aftereffect of the examination study.

Table 5
Comparison between 3LP and some existing cloud authentication

	[19]	*[20]*	*[21]*	*[22]*	*[23]*	*[24]*	*[3LP]*
Man in the Middle	x	0	-	0	x	x	O
Brute-Force Attack	0	0	-	0	x	x	O
Denial of Service Attack	x	0	-	0	x	x	O
				Features			
Cloud-based Protocol	0	0	x	0	x	x	O
One-time Password	0	x	x	x	x	x	O

Table 5 Demonstrates a correlation between our plan and some authentication schemes for the cloud and customary frameworks published as of late, especially, Fred Cheng et.al (19), Ali A.Yassinet.al (20), Tzong-Sun Wu et.al (21), Nimmy KandSethumadhavan M (22), RichaChowdharyandSatyakshmaRawat(23), V.Sathana and J.Shanthini (24). on the off chance that the scheme prevents an attack or satisfies the feature, the symbol "o" is utilized and if the plan neglects or fails to prevent an attack or does not satisfy the feature, the symbol x is used the 3LP is improvement of this paper system in terms of authentication time and ease of use.

6. CONCLUSION

The paper is concluded with an implementation of these AES encryption algorithm using multiple encryptions in cloud-based secure authentication protocol suite. This ensures confidentiality in the public cloud and three-level data protection which found to be effective in preventing the data leakage. Also the multiple encryption method yields better security than the existing AES single encryption method which has overcome the limitation of private use of cloud alone. The paper aims for the development and implementation of encryption algorithm on hybrid cloud computing for security purpose as a future work.

REFERENCES

[1] Pradeep Kumar, Selvamani K, Kanimozhi S, "An Authentication approach for data sharing in cloud Environment for dynamic Group,"*2014 International Conference on issues challenge in Intelligent Computing Techniques*,262-267,2014.

[2] AmlanJyotiChoudhury, Hyotaek Lim,"A Strong User Authentication Framework for Cloud Computing,"*IEEE Asia-Pacific Services Computing Conference*, 110-115, 2011.

[3] Woei-Jiunn, Jia-Hong Li b, Wei-Bin Lee b,"An Efficient and Secure Multi-server Authentication scheme with key agreement,"*The Journal of System and Software*,4,876-882,2012.

[4] Radhadevi, Kalpana,"Secure Image Encryption using AES," *International Journal of Research in Engineering and Technology*, 1, 2,115-117, 2012.

[5] Anna Squicciarini, Smitha, Dan Lin,"Preventing Information Leakage from Indexing in the Cloud," *IEEE 3'rd International Conference on Cloud Computing*, 188-195, 2010.

[6] AJ Elbert, Member, IEEE,"Fast and Efficient Implementation of AES,"*International Conference on Advanced Information Networking and Application Networking and Application Workshops*, 1, 55-69, 2007.

[7] JyothiYenuguvanilanka, OmarElkeelany,"Performance Evaluation of Hardware Models of Advanced Encryption Standard Algorithm," *South Easton, 2008 Proceedings IEEE*, 222-225, 2008.

[8] Qing-Xiang, Lu Li, Jing Liu, Nan Xu,"The Analysis and design of According Information Security System Based on AES Algorithm,"*Eighth International Conference on Machine Learning and Cybernetics, Baoding*, 2713-2718, 2009.

[9] Sudha.M, Bandaru Rama Krishna Raoet, "A Comprehensive Approach to Ensure Secure Data Communication in Cloud Environment,"*International Journal of Computer Applications*, 12, 8, 19-23, 2010.

[10] Deguang Le, Jinyi Chang, Xingdou Gou, Ankang Zhang, Conglan Lu,"Parallel AES Algorithm for fast data encryption on GPU,"*2'nd International conference on computer engineering and technology*,6,2010.

[11] Ahmed B. Mahmood, Robert D. Dony, "Segmentation Based Encryption Method for Medical Images,"*6th International Conference on Internet Technology and Secured Transactions*, 596-601, 2011.

[12] AbhaSachdev, Mohit,"Enhancing Cloud Computing Security using AES Algorithm,"*International Journal of Computer Application*,67, 9, 19-23, 2013.

[13] Quist-Aphetsi, Laurent Nana, Anca Christine Pascu, SophieGire, J.M.Eghan, NiiNarkuQuaynor,"Feature Based Encryption Technique for Securing Forensic Biometric Image Data using AES and Visual Cryptography,"*2nd International Conference on Artificial Intelligence modeling and simulation*,199-204, 2014.

[14] Kiruthika, Keerthana.S, Jeena.R,"Enhanced Cloud Computing Security Using AES Algorithm,"*International Journal of advanced research in computer science and software engineering*, 5, 3, 630-635,2015.

[15] ChanderKani, Yogesh Sharma,"Enhanced Security Architecture for Cloud Data Security,"*International Journal of advanced research in computer science and software engineering*,3,5, 570-575, 2013.

[16] Vanyadiwan, ShubhraMalhotra, Rachna Jain,"Comparison among Various Cryptographic Algorithms," *International Journal of advanced research in computer science and software Engineering*, 4, 4, 1146-1148, 2014.

[17] Marwan Darwish, AbdelkaderOuda, Luiz Fernando Capretzet,"A Cloud-based secure Authentication (CSA) protocol suite for defense against denial of service (DoS)," *Journal of Information Security and Application*, 1-9, 2015.

[18] Prasanthi O, subbareddy M, "Enhanced AES algorithm,"*International Journal of Computer Applications in Engineering Sciences*, 2, 2,114-118,2012.

[19] Fred Cheng,"Security attack Safe Mobile and Cloud-based one time Password Tokens Using Rubbing Encryption Algorithm,"*International Technological University and FPC Consultancy (Springer)*,305-336,2015.

[20] Ali A.Yassin, Hai Jin, Ayad Ibrahim, WeizhongQiang, DeqingZou,"A practical privacy password Authentication Scheme for cloud computing,"*IEEE 26'Th International Parallel and distributed processing symposium workshops and PhD Forum*,1210-1217,2012.

[21] Tzong-Sun Wu, Ming-Lun Lee, Han-Yu Lin, Chao-Yuan Wang, "Shoulder-surfing-proof graphical password authentication scheme,"*Springer*, pp.246-254, 2013.

[22] Nimmy K and SethumadhavanM,"Novel Mutual Authentication Protocol for Cloud Computing using Secret Sharing and Steganography," *Applications of Digital Information and Web Technologies IEEE*, 101-106,2014.

[23] RichaChowdhary andSatyakshmaRawat,"One Time Password for Multi-Cloud Environment,"*International Journal of Advanced Research in Computer Science and Software Engineering*, 3, 3,594-597, 2013.

[24] V.Sathana and J.Shanthini, "Three Level Security System for Dynamic Group in Cloud," *International Journal of Computer Science Trends and Technology*, 1, 2, 23-28.