International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Security to Outsource Data in Community Cloud with the Trusted Tenant System

Kundan Kunal[1], Dr. Latesh Malik[2]

[1]M.E. Student Wireless Communication and Computing, GHRCE Nagpur, India

Head of Department of Computer Science and Engineering, GHRCE Nagpur, India

Abstract: ***Cloud Computing is the dreamed vision of next-generation IT infrastructure. In cloud architecture community cloud shared among several user or organization for the common purpose. In cloud environment application and data placed to centralized data centres through which user can enjoy service like on demand, location independent and relieve from burden of storage and maintenance of data and reduced hardware soft ware cost. Placing the critical data in the hands of a cloud provider that fact that users no longer have possession to outsource data so cloud environment should guarantee of security of data to the user and fully trustworthy to use. Security of outsource data is very challenging task in cloud environment. We propose tenant system that provides the security to community cloud that guarantee security of data stored in server or motion in channel. In this paper two different encryption methods RC6 and SHA1 is used to provide the security to cloud data and the database. This architecture used OAuth technique for the user authentication to access the system and for the secure sharing of data to different user with in the cloud TTLS (Tunnel transport layer security) technique is used for secured sharing. The results of this system provide highly secured environment for data to place in cloud server and result ensure about the security of outsource data with different techniques at different level.***

Keywords: Cloud computing, Security, RC6, OAuth SHA1, TTLS

1. Introduction

Cloud computing delivers services of scalable computing resources in IT industry with the help of internet based technologies and these resources shared among large number of consumers and provide the advantage of low cost of storage data and hardware software maintenance. Apart from these many other advantages associated with cloud computing and give the services like storing data in cloud remotely, on demand self-service, data access with geographical independent location[1]. All such advance facility associated with cloud all organization wanted to be part of it but still awaited to join the cloud technology because of data security. Data owner not have any control over their data once the data is placed to cloud server by the user. Cloud service provider has control on the user's data. That makes user mind to think about the security threat in cloud server. It inferred that security is very important issues while dealing with the cloud computing [2].

Cloud computing is basically four different deployed technique.
(i)Private cloud: In private cloud architecture in which organization operate solely the cloud infrastructure in which data are managed by a third party or organization that may exist on premise or off premise. (ii)Community cloud: The community cloud in which infrastructure is shared among the several user or organizations that has common concerns or similar requirement. (iii)Public cloud: The public cloud in which organization selling cloud services and cloud made available for general public. (iv)Hybrid cloud: The hybrid cloud infrastructure is basically a combination of two or more clouds infrastructure technique [3].

The common concerns of security in cloud that satisfy the various security parameters that are authentication, confidentiality, integrity and availability. Data confidentiality level means only authorized users can use the data. Authentication level is process of verifying the incoming user. Data integrity level mean the information saves by user that has not been modified other rather than user itself it remains untouched in cloud server. Availability level guarantees data will always available for use when it needed the relevant user data must be available in server [4][5].

Cloud computing has such massive use that generate the necessity give the security outsource data so user can take different service like remote access ,low hardware and software maintenance cost[6]. There are various technique are available that provide the security to data which outsource to cloud and the security to cloud architecture at different level. Proposed architecture which use the different security mechanism to satisfy the security at different level. RC6 encryption technique use to encrypt to outsource data SHA1 is used to encrypt the database entry. OAuth authenticate the incoming user to the system and TTLS is used to for secure sharing in the system with different user within the cloud system.

The rest of the paper is organized such as. In section II, related work is a described included Authentication and Encryption method available for the security of cloud computing. Section III describes the methodology for secure cloud environment. In section IV the methodology and algorithms described. In section VI the results of various technique gives and displayed with the help of screenshot. Section VII result analysis is done. In section VIII concludes the topic and followed by the references.

Licensed Under Creative Commons Attribution CC BY

2. Related Work

Safeguarding the security work in cloud integrity availability and confidentiality is serious issue for cloud user to meets this attributes for the security various method are available those are encrypt data and placed in to cloud sever in the encrypted form that makes believe to user that the data stored by them is not modify by other .For Encryption various method are available that are biometric encryption, homomorphic encryption, searchable encryption, and elliptic curve cryptography(ECC), AES all the these encryption techniques are work with different advantage and disadvantage in the cloud environment[7].

The parameter through which we measure the advantage and disadvantage for the encryption in the cloud technique are Execution time, Algorithm size, Security Ensuring, Key length.

Parameter	*Biometric encryption*	*Holomorphic encryption*	*Searchable encryption*	*Elliptic curve cryptography*	*AES*
Execution Time	Less	Less	SSE- Less ASE-High	High	Less
Algorithm Size	High	High	High	Less	High
Security Ensuring	Less	Less	SSE- Less ASE-High	High	High
Key length	Not fixed	Not fixed	Not fixed	Not fixed	128 192 256

From the above table it's conclude that the AES and ECC Encryption technique have better side to use encryption in the cloud computing. In my proposed architecture AES implemented that the RC6 encryption technique give insurance of integrity of data in the cloud architecture. Similarly the encryption of database of cloud is also a need to meet confidentiality and availability and provide the data base as a service (DBaaS).Encrypted database support that only the authorizes user that can use the respective profile and their respective data[8][9].

Security of cloud computing is not fulfil until if security is not ensure to all the level. All parameter is not cover without the Authentication. The authentication of any identity is classified in three ways. First this is the basic authentication technique validate the identity with the user name and the password. Second the user token or card verification and at the last most widely method is biometric authentication.

To authenticate the user in the cloud there are various technique are available in the security world that are Kerberos Authentication, OAuth, and the biometric etc. In Kerberos technique in which the client verify his identity to the respective server and the servers doing the same to the user once the client and the server validate their identity they communicate to each other in the encrypted format and assure the integrity of data. Biometric encryption validation work is done by the various biometric data such as eye scan, fingerprint, voice recognition, facial recognition. Server previously stored the information of the data it verifies only at the time of user access. Server matches the request with the data base and according to result it gives the access of the server. The technique for authentication is used in my project that belongs to combination of token validation method is the OAuth technique and the basic method that is user name and password. The method OAuth in which the client or user request to the server for the token and the server verify the user detail within the data base after the verification server respond to the user and give the ticket to user only the authorized user get the ticket to access the cloud platform[10].

3. Methodology for Secure Cloud Computing

The following techniques are used for constructing the tenant system as that aim to provide the security of sharing in community cloud architecture and maintain the security of tenant. The overall design of the system is face challenge of security parameter in different security level. Firstly we describe the flow of project of and flow of data into the system and the various security technique are used in the architecture .Secondly described the encryption algorithm in the detail and further their result associated with the system..

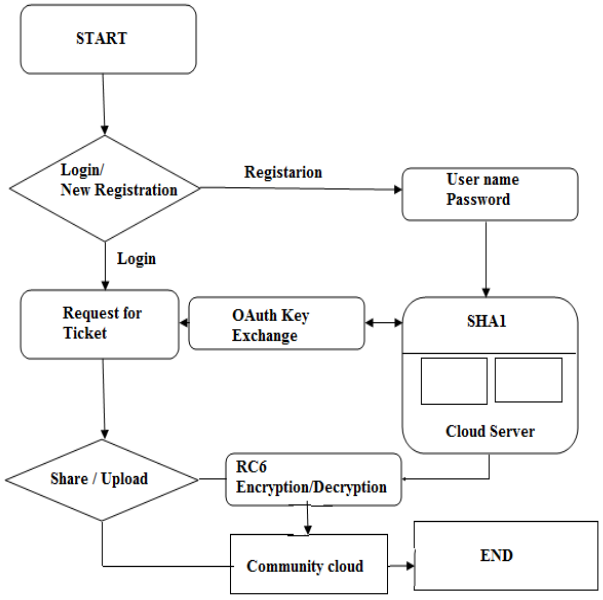

Figure1: Working of project

4. Methodology and Algorithm

The working of proposed architecture is the combination of various technique of security is applied to fulfill the requirement to design the secure environment of cloud computing. All the techniques are applied to overcome the security threat at the different level of the design architecture, and ensure the end user to outsource the data in to cloud environment securely.

4.1 Secure outsource data into cloud using the RC6 method

In the cryptography of data symmetric encryption is very common for the integrity. RC6 is the technique of encryption which comes under the advance encryption standard (AES). Symmetric key encryption code divided into two part block cipher and the stream cipher. This RC6 block cipher

Licensed Under Creative Commons Attribution CC BY

technique done the work of encryption with various operations .

The operation used in RC6 are defined as following.

- A+B integer addition modulo 2^w.
- A-B integer subtraction modulo 2^w.
- A⊕B Bitwise exclusive-or of w-bit words.
- A*B integer multiplication modulo 2^w.
- A<<<B rotation of the w-bit word A to the left by the amount given by the least significant w bits of B.
- A>>>B rotation of the w-bit word A to the right by the amount given by the least significant lg w bits of B.
- F(x)=x(2x+1)mod 2^w.

In the above operation in the RC6 is specified more accurately as the RC6 w/r/b in which the "w" is the data block or the word size in the bits, r denotes the number of non-negative round. The length of key for the encryption denoted by b with the key length of 16, 24 and 32 byte key length [11].

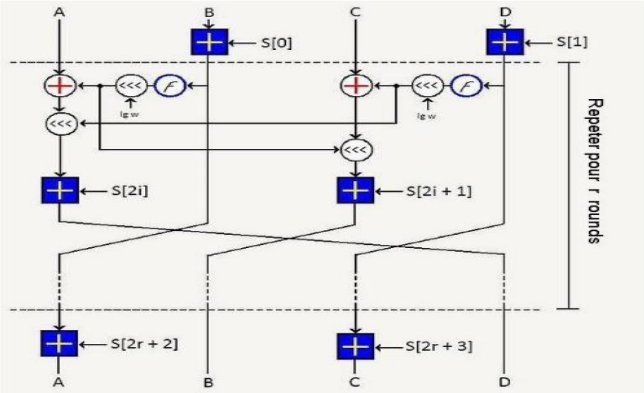

Figure 2: Process of RC6 [12].

Work of RC6 is assign with four w bit register A, B, C, D that takes the input as plain text and gives the output cipher text after the encryption most significant bit of plain text placed in the least significant bits. The assignment value of RC6 operation after applying the A,B,C,D register plain text converted into the cipher text and loading the cipher text in such manner (A, B, C, D) = (B, C, D, A)[13].

4.2 Secure the channel through which data is moving

The second most important work to do for the security in the cloud computing that secure the channel through which the data is moving the ultimate aim of the channel security that if data is on motion in channel no one can access the channel and ensure about the data confidentiality and the integrity. Method which I used for the channel security is the that Tunnel transport layer security(TTLS) this TTLS method is working on the transport layer whenever the user want to communicate with the server or different user this TTLS form the secure tunnel and share the data from the secure channel.

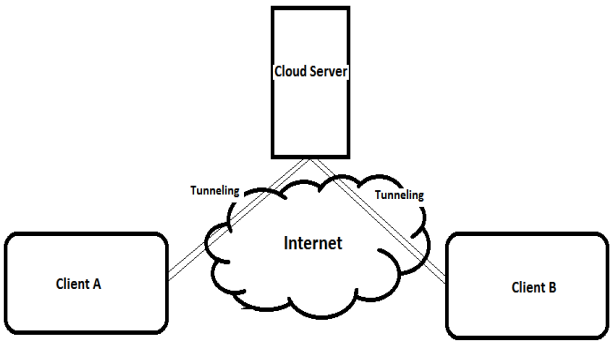

Figure 3: Process of TTLS within the Server

4.3Secure the data base Entry using the SHA technique

In all the security aspect the encryption of database entry is most important all of them because encrypted database entry it near to impossible to generate the threat to the system. If the unauthorized party get entered into the system by any hacking technique that will get nothing and the end because the database entry is already in the encrypted format. For encryption of database entry is done in my project is with the SHA 1algorithm. The hash value is placed at the database table rather than the plaintext [14]. The operations which are used to perform the SHA1 for a single iteration function are as follows**:**

- A,B,C,D and E are 32-bit words of the state.
- F is a nonlinear function that varies.
- $<<<_n$ denotes a left bit rotation by n places.
- n varies for each operation.
- W_t is the expanded message word of round t.
- K_t is the round constant of round t.
- ⊞ denotes addition modulo 2^{32}.

SHA-1 takes the message which length less than 264bits and gives the 160-bit hash value. The generated cipher text is in the hexadecimal number. The overall bit register of input and the output give the result in the format of (A,B,C,D,E) = (B,C,D,E,A)[15].

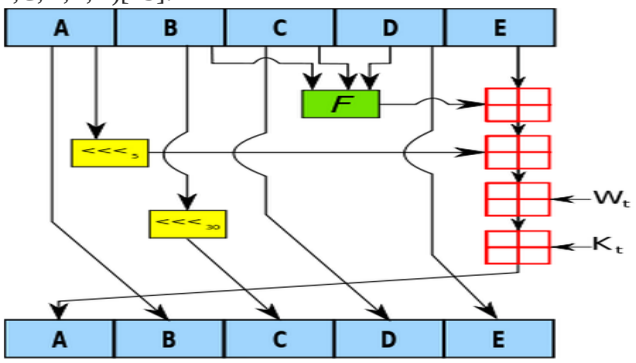

Figure 4: SHA1 Working [16].

4.4Authentication of user with combination of password and OAuth technique

Authentication of the user is necessary when the user want to access the system and used the service of cloud computing, In my system the authentication of user done with the combination of password and OAuth technique .OAuth is basically the web based protocol which have major role in

Licensed Under Creative Commons Attribution CC BY

cloud environment[17]. This protocol has the control over the services which provided to the user. This protocol work when user want to use the service of cloud computing, user send the request of credential or ticket and service owner server has to share the ticket to requesting user to use the service of the cloud environment.

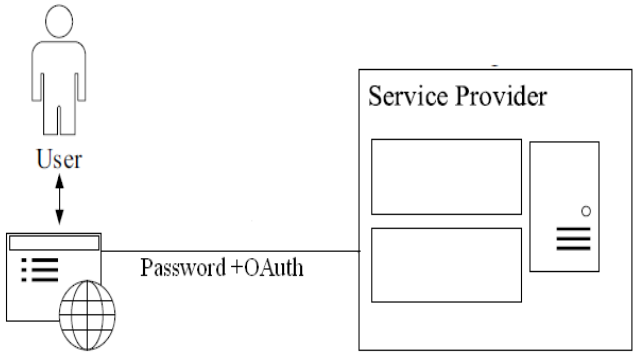

Figure 5: OAuth Verification

5. Result

The result evaluation of architecture is work on four different level of security for the cloud computing and gives result of the secured system.

5.1 RC6 Encryption

Firstly select the file which to upload in a cloud server and result of encryption algorithm placed data into the encrypted format. The upload process work three step process (i) Selects the file and converts into byte array of data (ii) Key expansion function generate key and (iii) Pass data byte array to the key expansion generate the result and store into the cloud server.

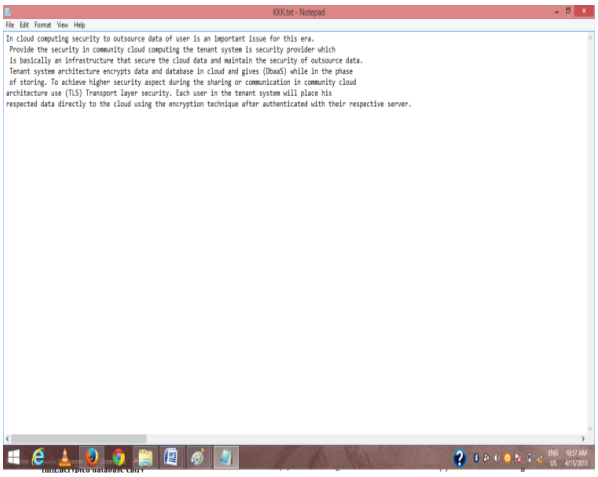

Figure 6: Plain Text

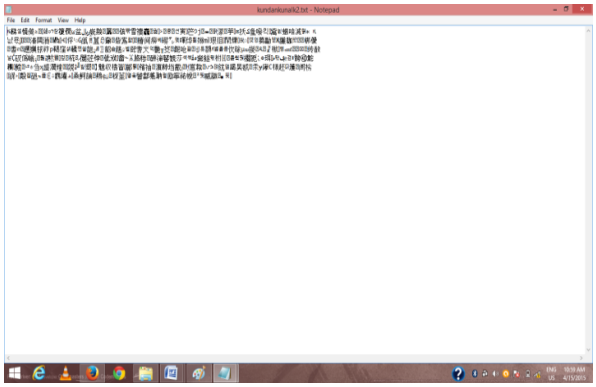

Figure 7: Cipher Text

As shown in the figure the text data which is upload in to the server with the use of RC6 algorithm and generate cipher text store into server. Result of the encryption process gives the unreadable form of data at the server.

5.2TTLS sharing

Tunnel transport layer security shares the data with the secure tunnel. In any communication between the user or server TTLS give the confidentiality and integrity about the data which is moving within the channel. Give the information regarding the Source address and destination address.

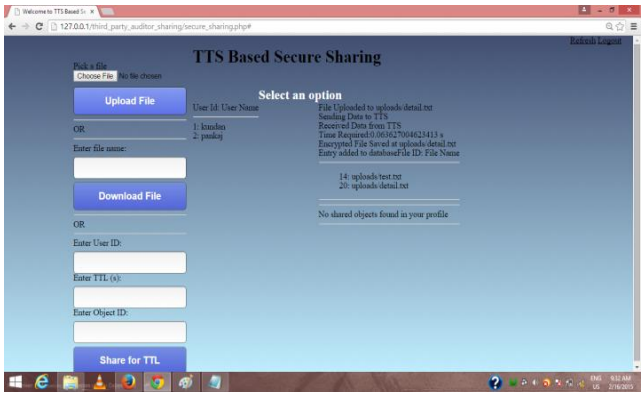

Figure 8: TTLS

Shared document with the user in the community cloud is live in the destination server only the time period that is given by the sending user. The receiving user use that file only for that time Stamp and it remove from the server.

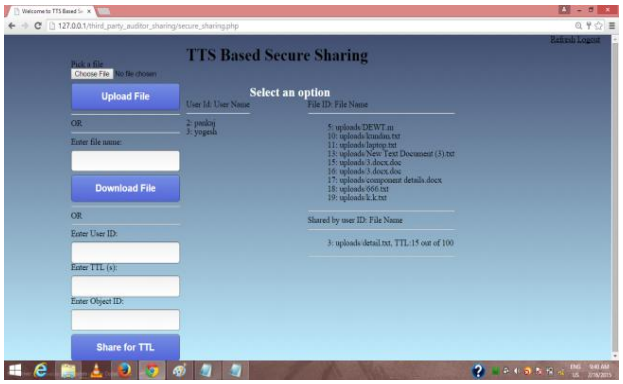

Figure 9: Data within the Client

Licensed Under Creative Commons Attribution CC BY

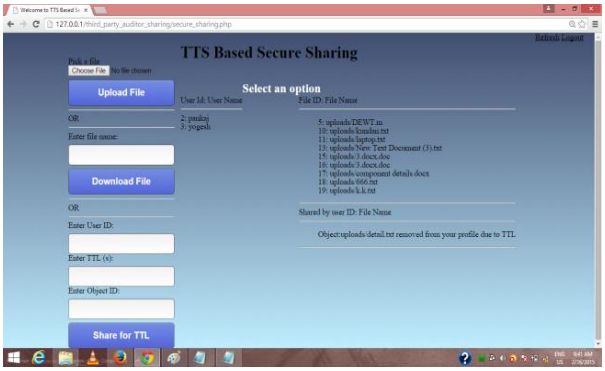

Figure 10: Data Removed from client side

5.3SHA1 Algorithm

In cloud computing the database encryption is most important because the application and the database both are placed at the untrusted environment. If we secure the database we can ignore the most of the threat which is coming to the architecture. We used the SHA 1 algorithm to encrypt the database entry. When the user entered the user name or password the algorithm store the encrypted from of password.

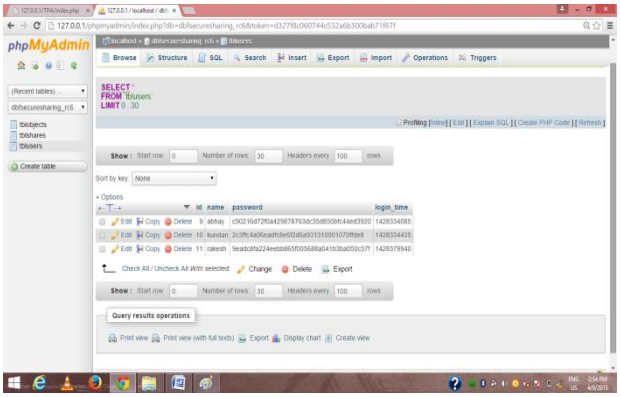

Figure 11: Encrypted database

5.4OAuth Technique

The user OAuth technique is used for the authentication with combination of password verification technique. In given architecture the user firstly give the information user name and password through which server can verify the user and give change to generate the operation of resource sharing. User request for key to the server, Server responding according to it and generate the key using that key user use the resource.

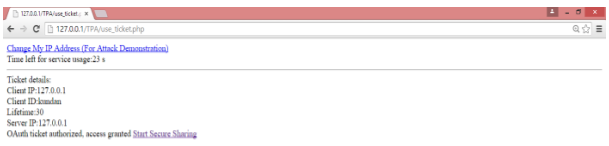

Figure 12: Request for Key

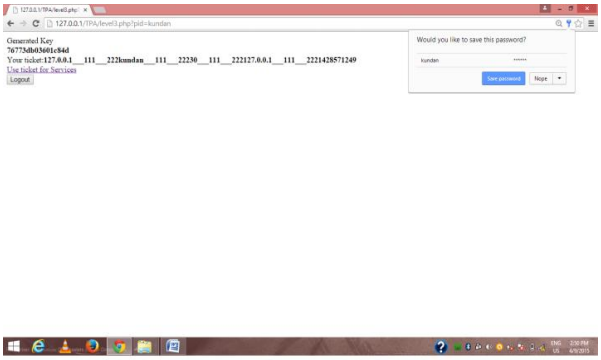

Figure 13: Generated key

6. Result Analysis

All the security encryption technique. The ultimate aim is achieved and designed the tenant system that securing the outsource data and the application to community cloud computing environment and securely share the data among the user. That user have faith over the cloud service provider that the data is placed within the cloud is secure. Flow of data rate in our system during the uploading and downloading time that are as follows:

Table 2: Flow of data rate in tenant system

Size	Upload(sec)	Download(sec)
50byte	0.02134490011226	.01927541986681
4kb	0.27714490890503	0.23589411585885
8kb	2.4702920913696	1.8461265465451
24kb	8.1579029560089	6.8515551162113
50kb	18.03256811142	15.24468122456

7. Conclusion and Future Scope

The architecture secure Tenant system for community cloud gives the security to data which placed in the cloud environment or share the data to different user for the common concern. This support for in each platform like ubuntu, window etc. To break the security of the database 2^{160} operation is required which is almost impossible, no threat reported for this value.

The tenant system used 128 byte key length for the faster execution. The secured architecture also block the various threat to the system by applying the various security mechanism, threat which are generally access the unauthorized source of cloud computing . Architecture gives a highly secure cloud environment where user has trust on it and ensures about the data security. The architecture is being developed can be used in the various real world scenario like college, hospital, organization. Where users have needed to placed their data to cloud server or share with the other user for the common purpose. The data are shared by user to cloud computing are secured and enhanced the use of field like cloud computing.

Licensed Under Creative Commons Attribution CC BY

Reference

[1] P. Mell and T. Grance, "Draft nist working definition of cloud computing," Referenced on June. 3rd, 2009 online at http://csrc.nist.gov/groups/SNS/cloud-computing/index.html, 2009.
[2] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the clouds: A berkeley view of cloud computing," UCB-EECS-Feb 2009.
[3] Xiaojun Yu, Qiaoyan Wen,"A View about Cloud Data Security from Data Life Cycle", International Conference on Computational Intelligence and Software Engineering (CISE), IEEE, Dec 2010.
[4] Simarjeet Kaur, "Cryptography and Encryption in Cloud Computing", VSRD International Journal of Computer Science & Information Technology, VSRD-IJCSIT, 2012.
[5] Dr. S.Sakthivel, B.Dhiyanesh" A Privacy-Preserving Storage Security for Spatial Data in Dynamics Cloud Environment" 4th ICCCNT, IEEE 2013.
[6] Priyanka Arora, Arun Singh, " Evaluation and Comparison of Security Issues on Cloud Computing Environment",WCSTT2012
[7] Malek Najib Omar, Mazleena Salleh, Majid Bakhtiari, "Biometric Encryption To Enhance Confidentiality in Cloud computing", International Symposium on Biometric and Security Technology 2014.
[8] Maha TEBAA and et.AI, "Homomorphic Encryption Applied to the Cloud Computing Security", Proceedings of the WorldCongress on Engineering, 2012.
[9] Neha A Puri,Ajay R Karkare,Rajesh C Dharmik, "Deployment of Application on cloud an Enhanced Data Security in Cloud Computing Using ECC Algorithm", ICACCCT 2014.
[10] Noureddine, Bashroush R., " A Provisioning Model Towards Oauth 2.0 Performance Optimization" Cybernetic Intelligent Systems (CIS), IEEE 2011.
[11] Narendra Chandel, Sanjay Mishra, Neetesh Gupta, Amit Sinhal "Creation of Secure Cloud Environment using RC6" International Conference on Intelligent Systems and Signal Processing (ISSP) 2013.
[12] Verma, H.K. Singh, R.K." Enhancement Of RC6 Block Cipher Algorithm And Comparison With RC5 & RC6" Advance Computing Conference (IACC), 2013 IEEE.
[13] Gil-Ho Kim ; Jong-Nam Kim ; Gyeong-Yeon Cho" An improved RC6 algorithm with the same structure of encryption and decryption" International Conference on Advanced Communication Technology,. ICACT 2009.
[14] Feng Ge ; Jain, P. ; Ken Choi" Ultra-low power and high speed design and implementation of AES and SHA1 hardware cores in 65 nanometer CMOS technology "Electro/Information Technology, 2009.
[15] Fatang Chen ; Jinlong Yuan" Enhanced Key Derivation Function of HMAC-SHA-256 Algorithm in LTE Network" Multimedia Information Networking and Security (MINES), 2012.
[16] Ahmed, H.E.H. ; Kalash, H.M. ; Allah, O.S.F." Encryption Efficiency Analysis and Security Evaluation of RC6 Block Cipher for Digital Images " International Conference on Electrical Engineering, ICEE '07.
[17] Shehab, M. ; Mohsen, F." Towards Enhancing the Security of OAuth Implementations in Smart Phones" Mobile Services (MS), IEEE International Conference 2014

Author Profile

Kundan Kunal received the B.E degree from BAMU and corrently persuing ME in Wireless Communication and Computing from G.H.Raisoni College of Engineering. Recently student in G.H.Raisoni College of Engineering.

Licensed Under Creative Commons Attribution CC BY