A Hybrid Data Security And Identification Mechanism In Cloud Computing

Megha Vashishtha, Dr Pradeep Chouksey

Abstract: In this paper a secure cloud computing environment has been presented. In our approach improved Rivest Cipher (RC6) mechanism along with blowfish algorithm has been used. Key generation has been adopted with the RC4 and RSA combination to improve the security mechanism. Blowfish algorithm is applied on images. In this process, firstly the cloud user has been registered by the cloud provider and authentication process has been completed. Then the user can upload the text and image data in the available four servers. The uploaded data by the self-authenticated account can be viewed directly without any restriction. But if those files are requested by the other cloud users the according to the data categorization encryption standard have been applied. The textual data is processed with the improved RC6 mechanism with key processing mechanism of RC4 and RSA algorithm. These keys are used for the data decryption from the other side. The try access (TA) and server notification (SN) time is noted for the proper notification to the respective client and server. In the initial process of data processing in the cloud the data recorder of all the user cloud recorded all the information. Separate data recorder reference has been provided for each cloud user. This recorder records the authentication (with complete detail along with the prefix tally). The prefix tally that is the TA provides the information of the mismatch in the last prefix of the combination of the user detail and the data. If it's not match then the data blocker algorithm will corrupt the data and no meaningful information has been visualized and any type of violation is recorded at the admin and the cloud user both.The overall parametric comparison suggests that the performance of our framework is better in comparison to the traditional techniques...

Index Terms: Cloud Computing, RC6, RSA, RC4,Blowfish

1. INTRODCUTION

In Cloud computing provides the flexibility to allow the uses of the resources as per the need with minimum cost [1−3]. It provides the virtualization aspects with on demand resource service [4]. There is the need of security as to maintain the integrity, confidentiality and availability [5−9]. There is multiple security issue, which can be handling in the way that the cloud user can associate the data with the self-protection and alert [10−13]. There is thinking in different aspects in the cloud computing area is import with the level wise security concern [14−16]. In general there are three cloud computing model namely Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). It generally incorporates virtualization circumstances as purchased organizations instead of physical or conferred PC equipment. Remembering the ultimate objective to deal with the issue of data reliability checking, various plans are proposed under particular systems and security models [16−22]. In spite of the way that designs with private auditability can achieve higher arrangement profitability, open auditability grants anyone, not just the client (data proprietor), to challenge the cloud server for rightness of data storing while at the same time keeping no private information. By then, clients have the ability to select the appraisal of the organization execution to a self-ruling untouchable evaluator, without responsibility of their estimation resources. In the cloud, the clients themselves are dishonest or will doubtlessly be not able manage the cost of the overhead of performing ceaseless genuineness checks. As needs be, for even minded usage, it gives off an impression of being sounder to outfit the check tradition with open auditability, which is depended upon to accept a more basic part in achieving economies of scale for Cloud Computing. Also, for viability thought, the outsourced data themselves should not to be required by the verifier for the check reason. Diverse different methodologies are likewise proposed toward cloud security have been exhibited in [23−30].In this paper an efficient security mechanism along with the identification techniques has been applied for the cloud data security.

- *Megha Vashishtha is currently pursuing Phd degree program in Computer Science engineering in Mewar University, chittorgarh Rajasthan India Ph-9977303113. E-mail: sumitvbpl@gmail.com*
- *Dr Pradeep Chouksey is currently Associate Professor in Computer Science engineering in LNCT Bhopal, India, PH-9229233462 E-mail: Dr.Pradeep.Chouksey@gmail.com*

2 RELATED WORK

In 2018, HouraniandAbdallah [31] suggested the impact of cloud computing in the organization growth and development. It is helpful in the communication to the customers. They have also discussed the legal issues and security challenges and their prospective views and discussed some key issues.In 2018, Gordin et al. [32] suggested that due to public cloud benefits organizations have their own resources on demand. Some organizations have their own clouds which is private. They have suggested that the security is an issue in private clouds.They have performed the security analysis by outside and inside operations through OpenStack Pike, Nessus, Metasploitand OpenVAS. They have also check the isolations and validation by installing the virtual machines.In 2018, Lee et al. [33] suggested the example of Herokuas the PaaS. They have suggested regarding the support of several programming language for this platform. These are used for web application deployment. It also helps in deploying and useful in modern apps execution. They have suggested the need of data security in cloud computing environment. For this they have suggested advanced encryption standard (AES). Their performance evaluation results support the security enhancement and protection through AES mechanism.In 2018, Alsaidiand Kausar [34] suggested the use of internet of things (IoT)having the capability to improve the human life and prospective. They have suggested that the IoTand cloudcomputing hybridizationcan be useful in different areas including business prospective. The security threats are the main barrier according to the authors in the individual use and impact for the analysis of these methods. So they have proposed IoT which is cloud assisted for intelligenttransportation system, telemedicine and smart cities.They have concentrated on the unauthorized access and the information adulteration from different devices and network nodes.In 2018, Elliott et al. [35] suggested that the use of Docker, Kubernetes and LXC container services have been

increased day by day in the current scenario. This will increase the scope of the security system in vast aspects to secure the data as the use and applicability is rise. They have presented a novel management system for the container services. It includes the aspects and applicability of private, public, or hybrid clouds. The aim of their proposed approach is to improve the security and resiliency. The process and the containers are self and autonomous and provide the security aspect in the residing capability manner to provide it in the self-node behavior to achieve the high level security in all aspects. It is also useful for these services which are relies on these environment.In 2018, TarekeandDatta [36] suggested the nature of attackers have been changed day by dayand the procedure is different. So there is the need of intelligent security system is a must in the today's era. So they have suggested the need of an automated and cloud enabling cyber security.They have discussed the need of security, law pursuits, detection and monitoring. They have suggested the need to extent it in different organization prospective and analyze them with the greater extent to verify it and provide us a proper dynamic design and deployment model especially for the clod using infrastructure and organizations for the safety and security of the data. In 2018, Park [37] suggested ther privacy preserving and statistically analysable database (PPSADB) system. It is suggested to secure the health information system. Their approach is capable in handling inter-column operations and dynamic database.In 2018, Seng et al. [38] discussed the security aspects of web data. They have also suggested the different aspects of automated web application with the focus of penetration testing. They have conducted a systemic review procedure for the web data and provide an analytical aspect for analyzing the methodology and several aspects of issues in this area. Their main objectives are in the direction of maintain the integrity, analyzing the security concern and provide a discussion on them to analyze the pros and cons of different methodology in the comparative way.In 2018, Halabi et al. [37] suggested that in the current scenario business organization are highly intended and interned in cloud computing infrastructure for their business and client communication. But the security is the biggest threat and the obstacle in the complete adoption and changes in the complete deployment. If the security is increased it will also increase the trustworthiness of the cloud service providers(CSP). They have proposed for achieving this broker-based model. It is used for the resources allocation. They have used genetic algorithm (GA). For this they have maximized global security satisfaction of users' as the objective function. By adhering this approach authors are capable in achieving the security levels and profound the security in the aspect to achieve the same short of handling in the customer oriented services. The services also allows the restriction based on the performance and security vulnerability easements to make it secure in the way to handle the data. The results also show the effectiveness of their approach and provide the validation in the aspects of achieving security.

3 PROPOSED METHOD

In this paper a secure framework has been developed for cloud data communication.Figure 1 shows the overall security system presented in our framework. It shows the security system consideration according to the approach presented in this paper. It clearly shows the collaboration of identity and access control along with the data security standards may lead in better secure cloud communication which is centrally controlled.

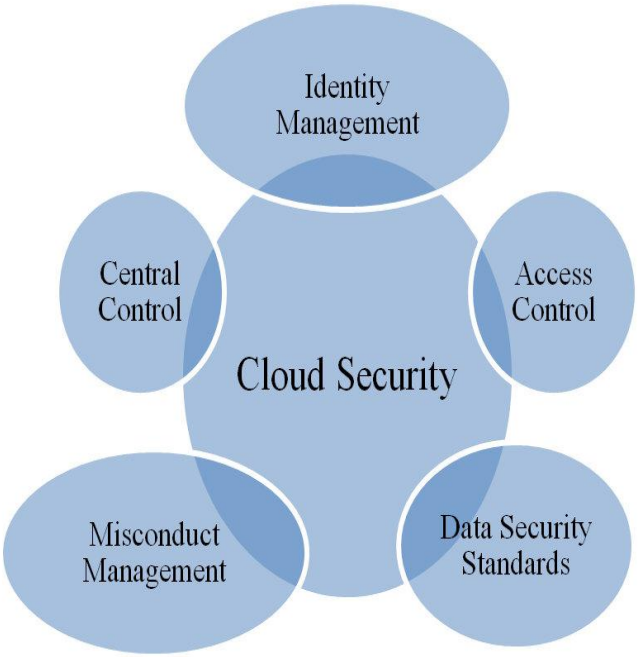

Figure 1 *Overall Cloud security System*

In this framework a centralized mechanism for the cloud security has been developed. In our approach improved Rivest Cipher (RC6) mechanism along with blowfish algorithm has been used. Key generation has been adopted with the RC4 and RSA combination to improve the security mechanism. RC6 provides variability in the block, key size and rounds of variable. The max key size variability support by RC6 is 2040 bits. This combination has been applied to text data. Blowfish algorithm is fast, easily applicable on images and need less memory. It is simple and secure. The key variability support by blowfish is 32-448 bit. It works on block data with the block size of 64 bit. The working of this algorithm is by key expansion and data encryption. In this process, firstly the cloud user has been registered by the cloud provider and authentication process has been completed. Then the user can upload the text and image data in the available four servers. The uploaded data by the self-authenticated account can be viewed directly without any restriction. But if those files are requested by the other cloud users the according to the data categorization encryption standard have been applied. The textual data is processed with the improved RC6 mechanism with key processing mechanism of RC4 and RSA algorithm. By this process three keys will be generated one RC6 key, one private key and the modulus key. These keys are used for the data decryption from the other side. For the image data blowfish algorithm has been applied and processed with single key for the encryption and decryption process. This process is capable in security enhancement.The above methodology is the principal approach to deal with the information security in the cloud condition as the recipient of the information should utilize legitimate unscrambling key to accomplish the information. Without this the information won't

be found. In the initial process of data processing in the cloud the data recorder of all the user cloud recorded all the information. Separate data recorder reference has been provided for each cloud user. This recorder records the authentication (with complete detail along with the prefix tally). The prefix tally provides the information of the mismatch in the last prefix of the combination of the user detail and the data. If it's not match then the data blocker algorithm will corrupt the data and no meaningful information has been visualized and any type of violation is recorded at the admin and the cloud user both. Flowchart is shown in figure 2.The algorithms used in our approach are shown below.

Algorithm 1: Improved RC6 algorithm
Input
Plaintext (Input registers (A, B, C, D))
Round (r) =>S[0……2r+3]
Word size (w)
Byte size (b)
Output
Cipher text
Step 1: B=B+S [0]
D=D+S [1]
Step 2: for i=1 to r do
t= (B * (2B +1)) <<<$\log_2 w$
u= (D* (2D +1)) <<<$\log_2 w$

A= ((A XOR t) <<<u) + s (2i)
C= ((C XOR u) <<<t) + S (2i+1)
(A, B, C, D) = (B, C, D, A)
Step 3: A= A + S (2r+2)
Step 4: C= C + S (2r+3)
Step 5: A1 & A2 variables are created and the initial values assigned are zero.
Step 6: A1 + 1 modulo 256
Step 7: A2= A1 [T [P1]] modulo 256
Step 8: Swapping according to the procedure completion.
Step 9: Modulus key generation
1< A2<ø (n)
ø (n)= (p-1) (q-1)
D= (k * ø (n) +1)/e
c= (msg ^ e) /n
m= pow (c,d)
Key= A2 XOR m XOR A/B/C/D
Step 10: End.

Algorithm 2: Blowfish algorithm
Key expansion
Step 1: This algorithm uses various subkeys. It consists of 18, 32 bit subkeys.
The entries for 32-bit boxes are as fiollows:
S[1,0], [1,1]…….S[1,255]
S[2,0], [2,1]……..S[2,255]
S[3,0], [3,1]…….S[3,255]
S[4,0], [4,1]……..S[4,255]
Step 2: Subkeys generation
First P-array have been initialized then from S boxes are initialized
S-Box let (P1, P2,P3…….Pn)
Step 3: P1 XOR Key (First 32 bit of the key)
P2 XOR Key (Second 32 bit of the key)
Pn XOR Key (n 32 bit of the Key)

Encryption
Step 1: Initialization of left and right bit
X_L – 32 bit
X_R– 32 bit
Step 2: for i=1 to 16
$X_L = X_L$ XOR P_i
$X_R = F(X_L)$ XOR X_R
Swap X_L & X_R
$X_R = X_R$ XOR P17
$X_L = X_L$ XOR P18
X_L and X_R are joining to form the cipher

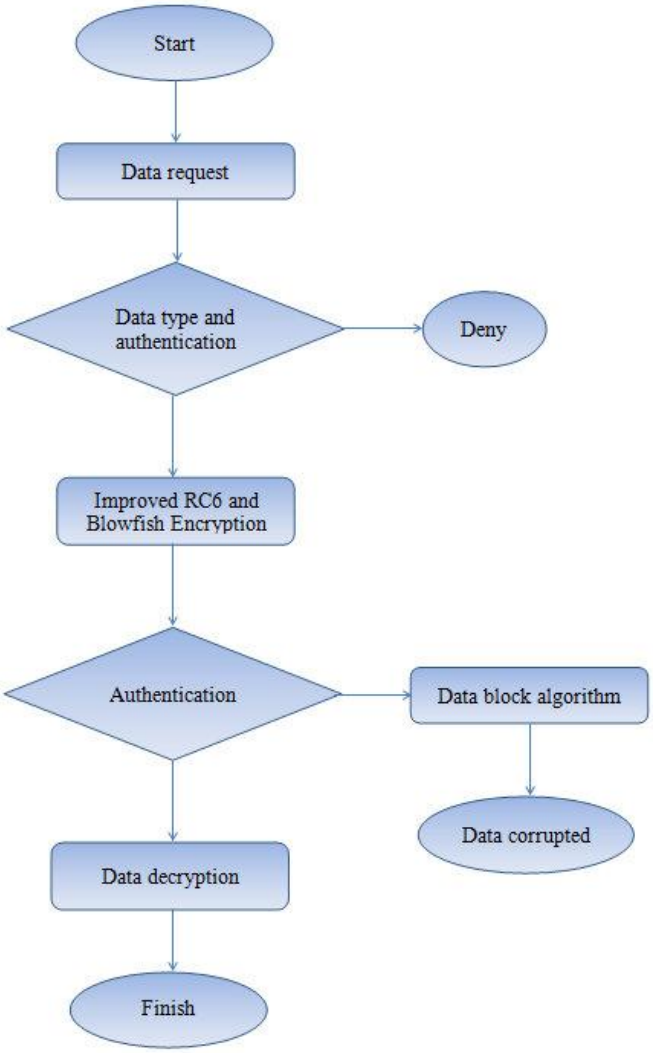

Figure 2 *Flowchart*

Step 3: The initial string has been encrypted using the subkey in the step 1 and 2.
Step 4: The obtained output of step 3 has been placed on P1 & P2.
Step 5: The output of step 4 has been encrypted by the modified subkey.
Step 6: The obtained output has been placed on P3 and P4.
Step 7: Process will continue till the end of the p process.
Step 8: End.

Algorithm 3: Data blocking algorithm
Step 1: Accept the original data as the input.

Step 2: Arrange it in a string array.
Step 3: for consideration an array size of 32 bits has been considered.
Step 4: byte [] b = new byte [32];
Step 5: The position of the array is initialized to 0.

```
do
{
x = x >> 1;
b[31-pos++] = (byte)(x % 2);
}
while(x > 0);
```

Step 6: The values have been received in the form of array.
Step 7: End.

4 RESULT ANALYSIS

In this section the comparison has been shown based on the security mechanism. Figure 3, 4 and 5 shows the RC6 encryption time (E) and decryption time (D) comparison for three different set. It is clear from the experimentation that the time taken for different files are not much varies and provides static time. This provides the time comparison in case of textual data only. The intermediate process time of RSA and RC4 is not included in this comparison. Figure 6 and 7 shows the blowfish encryption time (E) and decryption time (D) comparison for two different set. It is clear from the experimentation that the time taken for different files are not much varies and provides static time. This provides the time comparison in case of image data only. RC6 has a block size of 128 bits. The key variability supports by RC6 are 128, 192, and 256 bits up to 2040-bits with the element state table. The swapping is done at least once. RC4 key limited to 40 bits as the export restrictions but sometimes it uses 128 bit key. The key variability is 40-2048 bits. The standard key limitation in RSA is 1024 bits but it can be extended. In case of blowfish the key variability is 32 bits to 448 bits. So in our framework the secret key vary between 128 to 2040 bits. Therefore the key size varies between 2^{128} to 2^{2048}. So the brute force attack is very tough as comparison to the traditional mechanism. To detect the intermediate process in our approach is also very tough as the intermediate process confuses the attacker by the RC4 and RSA key generation approach in our mechanism. However the time taken is more. Figure 8 shows the key variability.In this section the comparison and analysis has been presented based on security breach. Figure 9 shows the security breach analysis graph. The try access (TA) and server notification (SN) time is noted for the proper notification to the respective client and server. It shows the variations in attack identification. In most of the set the variations is minor. Figure 10 shows the number of successful hits in identification in a single quarter. The single quarter period is of 60 seconds. It shows 1 for all the successful hits in a single quarter for two quarter it is 0.5. It is clear from our approach that this approach is able to hit successfully in a single quarter as the successful rates is higher. Figure 11 shows the identification time comparisons (ms). It shows the difference in TA and SN. Figure 12 shows the identification probability in a single quarter. For a single set 10 iterations are considered and counted the number of successful hits for the preparation of this graph. It is clearly indicated from this graph that the overall accuracy in the identification is very high.

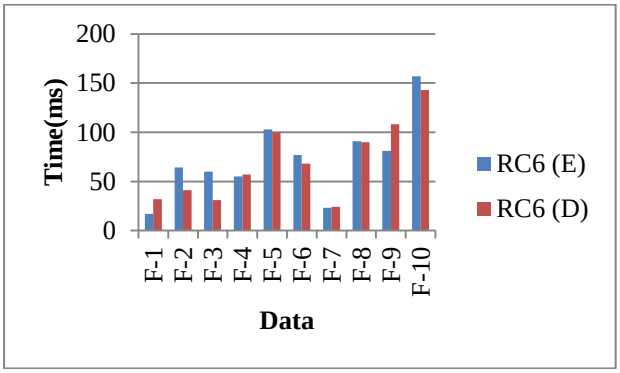

Figure 3 *RC6 (E) and (D) comparison for first set*

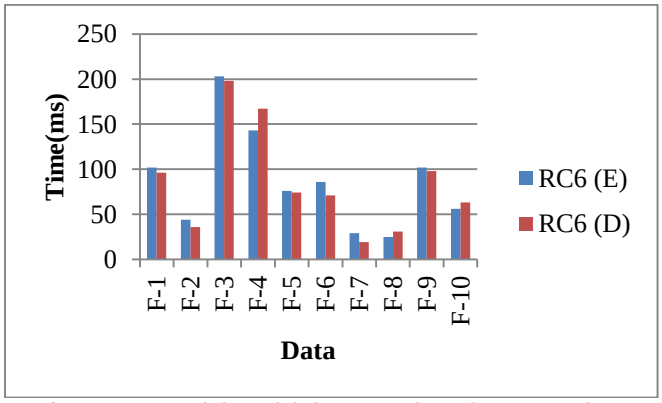

Figure 4 *RC6 (E) and (D) comparison for Second set*

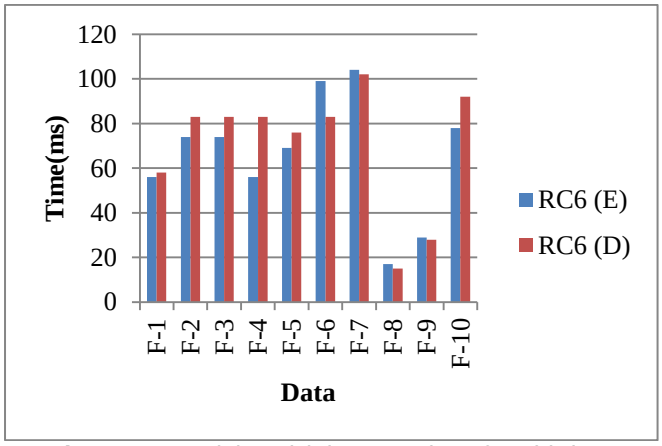

Figure 5 *RC6 (E) and (D) comparison for Third set*

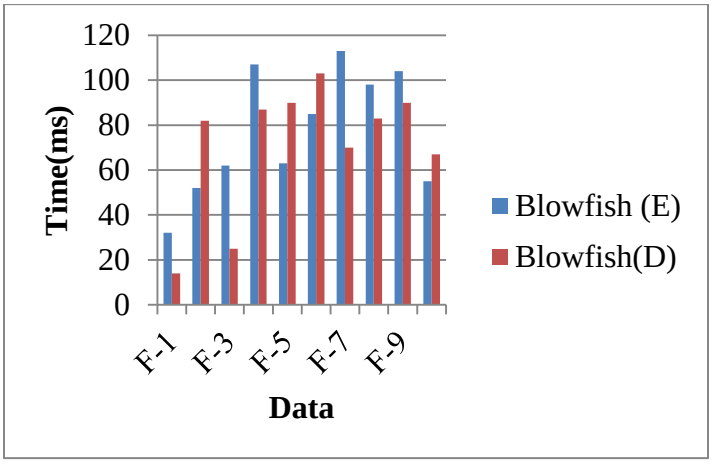

Figure 6 *Blowfish (E) and (D) comparison for first set*

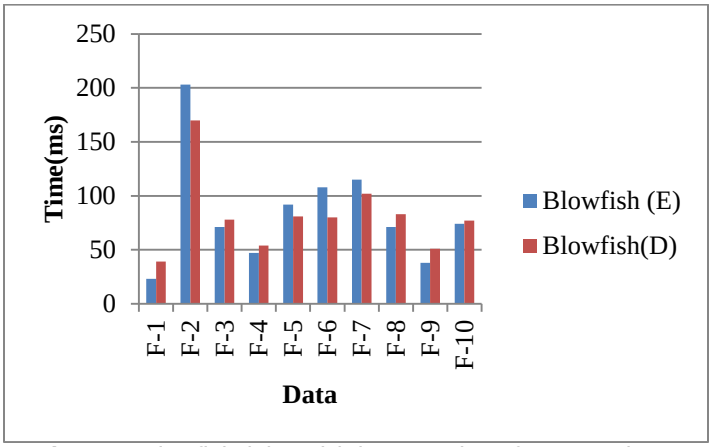

Figure 7 *Blowfish (E) and (D) comparison for second set*

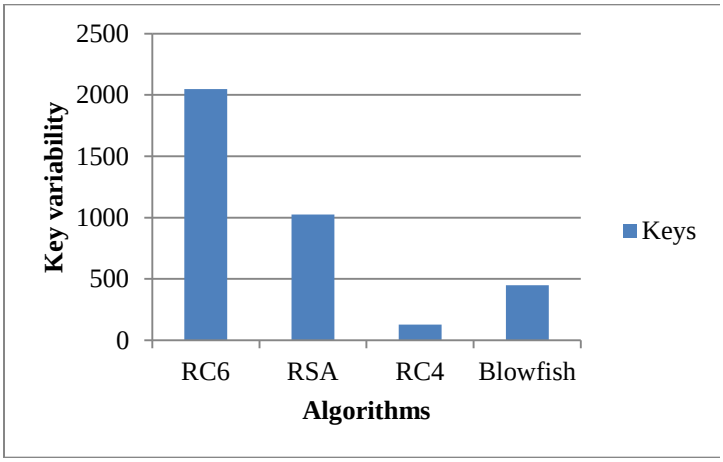

Figure 8 *Key variability analysis*

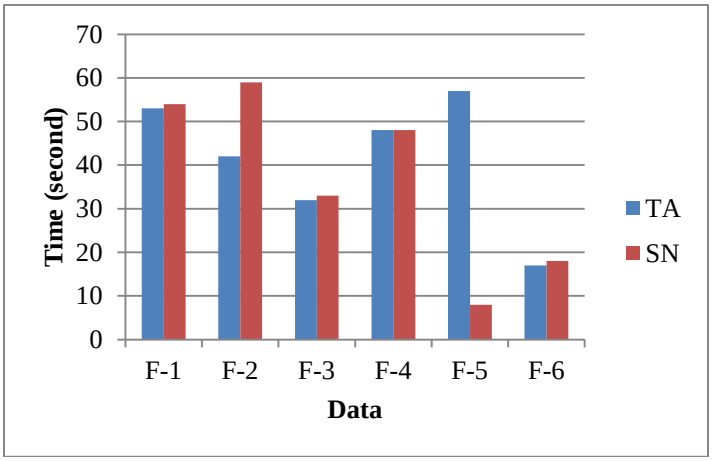

Figure 9 *Security breach analysis*

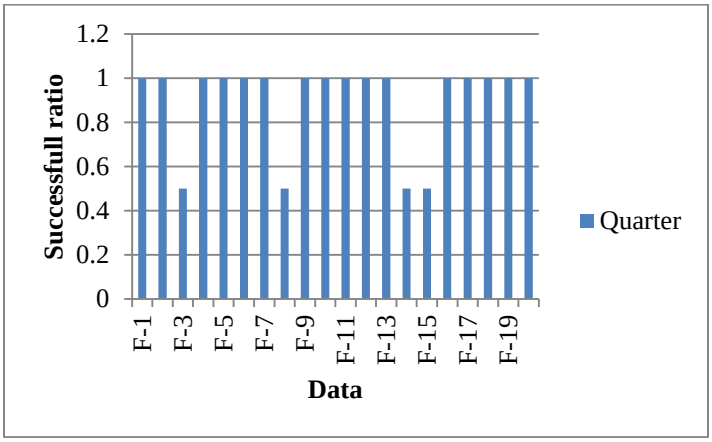

Figure 10 *Number of successful hits in a single quarter*

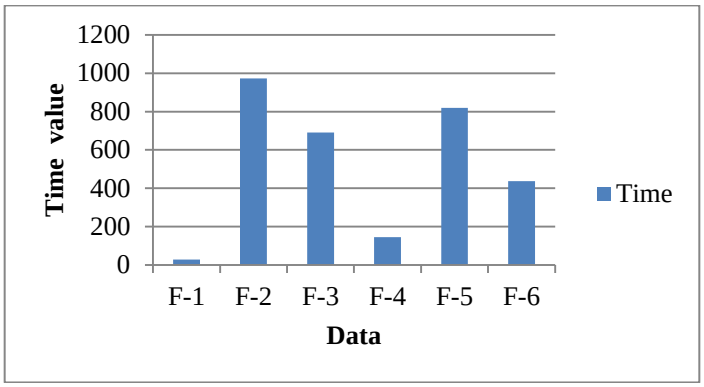

Figure 11 *Identification time comparisons (ms)*

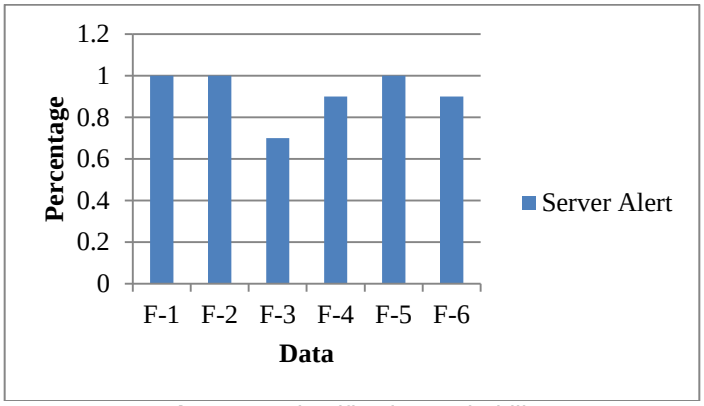

Figure 12 *Identification probability*

CONCLUSION

In this paper we have developed a secure centralized cloud framework for secure two way data communication. Our efficient framework is the collaboration of identity and access control along with the data security standards may lead in better secure cloud communication which is centrally controlled. In this environment first the data is processed in the cloud environment. Two types of data have been supported by this framework those are text and image data. Any authenticated and authorized cloud user can enter in the cloud environment with proper credential. There are total four servers for data uploading in our cloud environment. The cloud user can request other data in the environment. If the sender ready for the sending. RC6 algorithms along with the intermediate steps of RC4 and RSA have been applied before sending the data. This mechanism is applied on the textual

data. Blowfish algorithm is applied in case of image data security. The data is shared to the concern cloud user along with the try access (TA) bit. If the same user tries to open the file, the file will open after applying the shared password. The TA bit will be changed if it is access by any unauthorized user and the data blocking mechanism is applied to corrupt the data so that the data is protected from any misconduct. The main specialty of our approach is it supports proper security standard, key variability, data protection, authorization and authentication (AA) and breach identification.

.

REFERENCES

[1] Fox A, Griffith R, Joseph A, Katz R, Konwinski A, Lee G, Patterson D, Rabkin A, Stoica I. Above the clouds: A berkeley view of cloud computing. Dept. Electrical Eng. and Comput. Sciences, University of California, Berkeley, Rep. UCB/EECS. 2009 Feb 10;28(13):2009.

[2] Ruiz-Agundez I, Penya YK, Bringas PG. Cloud computing services accounting. International Journal of Advanced Computer Research. 2012 Jun 1;2(2):7.

[3] Singh A, Shrivastava M. Overview of security issues in cloud computing. International Journal of Advanced Computer Research. 2012 Mar 1;2(1):41.

[4] Ateniese G, Burns R, Curtmola R, Herring J, Kissner L, Peterson Z, Song D. Provable data possession at untrusted stores. InProceedings of the 14th ACM conference on Computer and communications security 2007 Oct 28 (pp. 598-609). ACM.

[5] Dubey AK, Dubey AK, Namdev M, Shrivastava SS. Cloud-user security based on RSA and MD5 algorithm for resource attestation and sharing in java environment. InSoftware Engineering (CONSEG), 2012 CSI Sixth International Conference on 2012 Sep 5 (pp. 1-8). IEEE.

[6] Juels A, KaliskiJr BS. PORs: Proofs of retrievability for large files. InProceedings of the 14th ACM conference on Computer and communications security 2007 Oct 28 (pp. 584-597). ACM.

[7] Shacham H, Waters B. Compact proofs of retrievability. InInternational Conference on the Theory and Application of Cryptology and Information Security 2008 Dec 7 (pp. 90-107). Springer, Berlin, Heidelberg.

[8] Bowers KD, Juels A, Oprea A. Proofs of retrievability: Theory and implementation. InProceedings of the 2009 ACM workshop on Cloud computing security 2009 Nov 13 (pp. 43-54). ACM.

[9] Naor M, Rothblum GN. The complexity of online memory checking. InFoundations of Computer Science, 2005. FOCS 2005. 46th Annual IEEE Symposium on 2005 Oct 23 (pp. 573-582). IEEE.

[10] Tsai WT, Sun X, Balasooriya J. Service-oriented cloud computing architecture. InInformation Technology: New Generations (ITNG), 2010 Seventh International Conference on 2010 Apr 12 (pp. 684-689). IEEE.

[11] Patra GK, Chakraborty N. Securing cloud infrastructure for high performance scientific computations using cryptographic techniques. International Journal of Advanced Computer Research (IJACR). 2014;4(1):66-72.

[12] Pachorkar N, Ingle R. Multi-dimensional affinity aware VM placement algorithm in cloud computing. International Journal of Advanced Computer Research. 2013 Dec 1;3(4):121-5.

[13] http://www.dialogic.com/~/media/products/docs/whitepapers/12023-cloud-computing-wp.pdf

[14] Geramiparvar S, Modiri N. Security as a Serious Challenge for E-Banking: a Review of Emmental Malware. International Journal of Advanced Computer Research. 2015 Mar 1;5(18):62.

[15] Venaik A. Qualitative risk level estimation of Business Process Re-engineering efforts and effects (With special reference to IT-sector). International Journal of Advanced Computer Research. 2015 Mar 1;5(18):11.

[16] Seng LK, Ithnin N, Said SZM. The approaches to quantify web application security scanners quality: a review. International Journal of Advanced Computer Research. 2018; 8 (38): 285-312.

[17] Mohamed MH, Waguih HM. A proposed academic advisor model based on data mining classification techniques. International Journal of Advanced Computer Research. 2018 May 1;8(36):129-36.

[18] Shrimali B, Bhadka H, Patel H. A fuzzy-based approach to evaluate multi-objective optimization for resource allocation in cloud. International Journal of Advanced Technology and Engineering Exploration. 2018 Jun 1;5(43):140-50.

[19] Kumar M, Katti CP. An efficient ID-based partially blind signature scheme and application in electronic-cash payment system. ACCENTS Trans. Inf. Secur. 2017;2(6):533-47.

[20] Saqib SM, Mahmood K, Naeem T. Comparison of LSI algorithms without and with pre-processing: using text document based search. Accent. Trans. Inf. Secur. 2016;1(4):44-51.

[21] Chang EC, Xu J. Remote integrity check with dishonest storage server. InEuropean Symposium on Research in Computer Security 2008 Oct 6 (pp. 223-237). Springer, Berlin, Heidelberg.

[22] Shah MA, Swaminathan R, Baker M. Privacy-Preserving Audit and Extraction of Digital Contents. IACR Cryptology ePrint Archive. 2008 Apr 30;2008:186.

[23] Bhardwaj A, Subramanyam GV, Avasthi V, Sastry H. Review of solutions for securing end user data over cloud applications. International Journal of Advanced Computer Research. 2016 Nov 1;6(27):222.

[24] Manimaran A, Durairaj M. The conjectural framework for detecting DDoS attack using enhanced entropy based threshold technique (EEB-TT) in cloud environment. International Journal of Advanced Computer Research. 2016 Nov 1;6(27):230.

[25] Shobha K, Nickolas S. Time domain attribute based encryption for big data access control in cloud environment. ACCENTS Transactions on Information Security. 2017; 2(7):73-77.

[26] NaikMR, Sathyanarayana SV. Key management infrastructure in cloud computing environment-a survey. ACCENTS Transactions on Information Security. 2017; 2(7):52-61.

[27] Alotaibi MB. Antecedents of software-as-a-service (SaaS) adoption: a structural equation model. International Journal of Advanced Computer Research. 2016 Jul 1;6(25):114.

[28] Tiwari R, Sinhal A. Block based text data partition with RC4 encryption for text data security. International Journal of Advanced Computer Research. 2016 May 1;6(24):107.
[29] Fan Z, Wu Q, Zhang M, Zheng R. Popularity and gain based caching scheme for information-centric networks. International Journal of Advanced Computer Research. 2017 May 1;7(30):71.
[30] Soni A, Hasan M. Pricing schemes in cloud computing: a review. International Journal of Advanced Computer Research. 2017 Mar 1;7(29):60.
[31] Hourani H, Abdallah M. Cloud Computing: Legal and Security Issues. In2018 8th International Conference on Computer Science and Information Technology (CSIT) 2018 Jul 11 (pp. 13-16). IEEE.
[32] Gordin I, Graur A, Potorac A, Balan D. Security assessment of OpenStack cloud using outside and inside software tools. In2018 International Conference on Development and Application Systems (DAS) 2018 May 24 (pp. 170-174). IEEE.
[33] Lee BH, Dewi EK, Wajdi MF. Data security in cloud computing using AES under HEROKU cloud. InWireless and Optical Communication Conference (WOCC), 2018 27th 2018 Apr 30 (pp. 1-5). IEEE.
[34] Alsaidi A, Kausar F. Security Attacks and Countermeasures on Cloud Assisted IoT Applications. In2018 IEEE International Conference on Smart Cloud (SmartCloud) 2018 Sep 21 (pp. 213-217). IEEE.
[35] Elliott D, Otero C, Ridley M, Merino X. A Cloud-Agnostic Container Orchestrator for Improving Interoperability. In2018 IEEE 11th International Conference on Cloud Computing (CLOUD) 2018 Jul 1 (pp. 958-961). IEEE.
[36] Tareke TA, Datta S. Automated and Cloud Enabling Cyber Security Improvement in Selected Institutions/Organizations. In2018 Second International Conference on Computing Methodologies and Communication (ICCMC) 2018 Feb 15 (pp. 533-538). IEEE.
[37] Park HA. The modeling of privacy preserving and statistically analysable database (PPSADB) system. International Journal of Advanced Computer Research. 2018; 8(38): 229-239.
[38] Seng LK, Ithnin N, Said SZM. The approaches to quantify web application security scanners quality: a review. International Journal of Advanced Computer Research. 2018; 8(38):285-312.
[39] Halabi T, Bellaiche M, Abusitta A. Online Allocation of Cloud Resources Based on Security Satisfaction. In2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE) 2018 Aug 1 (pp. 379-384). IEEE.