International Journal of Engineering & Technology, 7(4.16) (2018) 218-224

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

An Enhanced Salted Challenge Response Authentication Mechanism (scram) for Secret Key Authentication and File Sharing Process in Cloud Storage

Atif M. Qatan, Ph.D.

Information Science Department, Faculty of Arts and Humanities
King Abdulaziz University, Jeddah, Saudi Arabia
**Corresponding author E-mail: amgattan@yahoo.com*

Abstract

In the present digital world, different types of organization generate a huge volume of sensitive data comprising with financial data, health records, electronic health records, personal information and so on. The volume of digital data is tremendously improving at a staggering rate and it is expanding almost each and every year and outperforming the ability of storage restriction. These data often required to be stored at multiple locations for a long time because of the regulatory compliance and operational purposes. The local management of such great volume of cloud data is costly as well as problematic because of the needs of qualified personnel capability and great storage capacity. While there is a secure drop in the cost of the storage management and hardware storage, cost has become more complex. The Storage-as-a-Service (SaaS) provided by CSPs is a developing solution to lessen the load of huge local data storage and data maintenance cost in terms of outsourcing data storage. In the scenario of outsourcing data, the organization delegates the management and storage of their data to a CSP in the exchange of already declared fees and it has been metered in GB per month. The number of outsourced data is stored on the remote server instead of using private computer systems. This research paper concentrates to provide secure cloud auditing process within the multiple groups of users. In addition this improves the data integrity, provable security and data recovery process. Thus it minimizes the communication complexity and storage cost. The proposed research work based on Enhanced Salted Challenge Response Authentication Mechanism (SCRAM) which is used for secret key authentication and sharing process.

Keywords: *Authentication; Cloud Computing; File Sharing;, SCRAM; Secret Key*

1. Introduction

Cloud Computing is also known as model of distributed computational over a huge number of shared pools with virtualized computing resources (network bandwidth, memory, service, application, storage and so on) [1]. Cloud computing signifies a vision of giving different kinds of services as different kinds of utilities, for example electricity and water [2]. The cloud computing architecture can be divided into different parts such as back end and front end [3]. The back end has a vast amount of network of data centers with countless number of data storage systems, system programs and different applications [4] The front-end signifies application, like web browsers, organizations and different kinds of cloud users [5].This process is symbolically believed that, the Cloud Service Providers (CSPs) almost have infinite storage capacity and computation power. The cloud computing architecture's conceptual framework is as shown in Figure 1

The considerable devotion of the different paradigm of cloud computing is because of the number of key benefits, which create it a motivating research area in both industry and academia [6]. However, the following are some of the significant paradigms of the cloud computing.

- Provisions for cost-effective means of processing business over a different kind of shared pool of resources, where the cloud user escapes from the capital expenditure on services, software, and hardware as they pay only for what they utilize at the time.
- The cloud computing process can give immediate access to a wide range of applications and low management overhead.
- Cloud computing process mainly minimizes the maintenance cost as a third party is accountable for running cloud process of storing data.

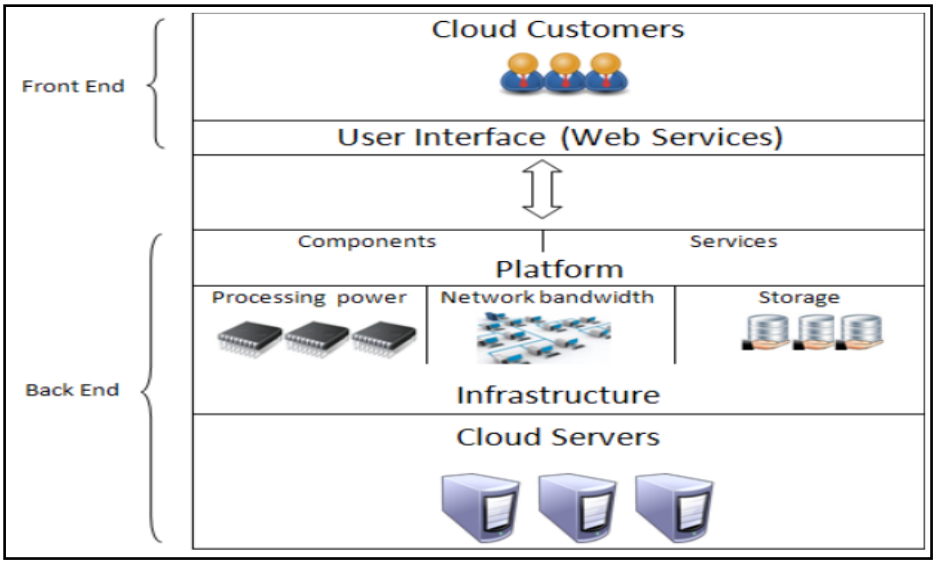

Fig. 1 Cloud Computing Architecture's Conceptual Framework

Basically, in cloud computing model it accepts the single point failure during the cloud servers have more attacks (Syed Rizvi and John Mitchell, 2015). According to the computational integrate the computation of outsourcing process is growing very well, which is used to constraint the client resources and as well as it gets benefit from the powerful cloud server [7]. The main characteristics in cloud computing are Authorization, Authentication and Accounting.

1.1 Data Sharing In the Dynamic Cloud Environment

The basic group sharing process is as shown in Figure 2.

Data owner permitted to upload their data on the cloud environment in terms of public or private use. Then the group user edited the stored data, auditor will report the original data owner about the altered cloud data. Once a cloud user is revoked from the specific group then he is efficiently resigned as revoked user in the particular block. Data owner will share the data among the group users and uploads the file have full rights to alter and download the whole data from the cloud environment. The data owner can also give the permission to download or edit the data with some constrains. Then Cloud Server permits only the authorized group user to store and share their data in the cloud environment which is provided by the cloud service provider, for example, SaaS and it does not permit the unauthorized group user to share and store their data in the cloud environment and its revocated.

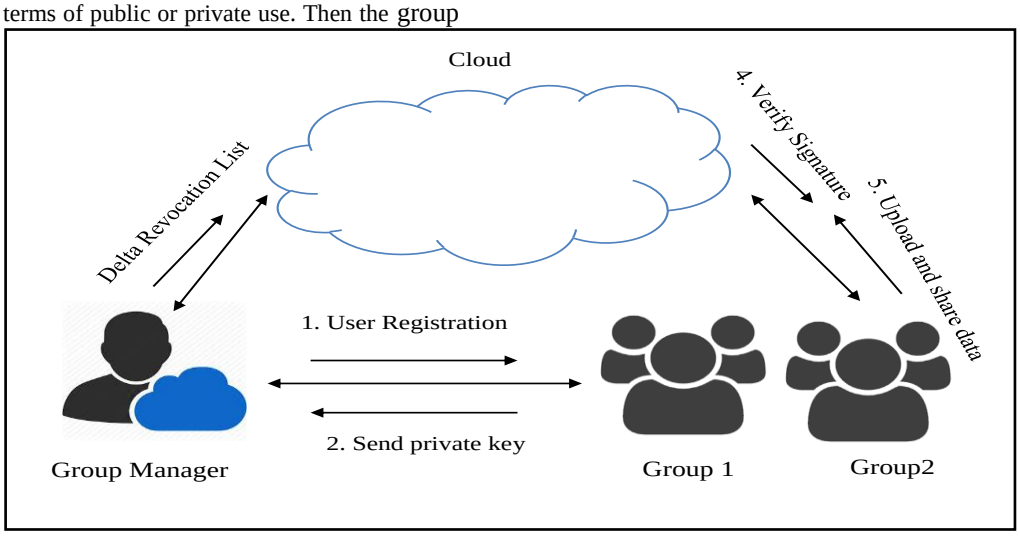

Fig. 2 Basic Group Sharing

The case in which user wishes to revoke from a particular group, this request is forwarded to the cloud auditor regarding revocation, where the auditor will monitor and check this process and revoke the particular user from the specific group. This user revocation process is also secure due to a reason of only existing group user are able to sign the data blocks in shared data in the cloud. Additionally, the re-signing key cannot create a valid signature for a subjective block on behalf of an existing group user. Additionally, being revoked from the specific group, a revoked group user is no longer in the group user list and he cannot generate the valid signature on the shared data.

2. Problem Definition

Duplicate storage of data leads to more memory usage and cost for the cloud users. Different kinds of auditing techniques are processed during the cloud storage process which also manages the auditing cost and modified data in the cloud. However, it has some limitation in terms of client read-only data. Hence, this research mainly focuses on designing issue in dynamic cloud data operation such as the data storage in public audit ability and data dynamics.

3. Related Work

In a cloud computing environment the data outsourcing has recently becomes a familiar in academia [8] [9][10] , and industry. Some of the cloud storage systems are iCloud, Skydrive, Amazon S3, Google Drive, Box.net Dropbox and so on.

The most significant impediment to public adoption of cloud system is due to lack of some security assurances in the cloud data storage system [11],[12]. In a cloud storage system there are two main components, such as server and a client. The server used to store client's data and the client transmits their files to the cloud server, [13] [14]. Basically, the client outsources their data to the third party termed as data storage provider which means server, the server supposed to keep the client data intact and makes it available to the client [15][16].

However, still in cloud computing, the data storage process have some drawbacks, thus, this thesis addresses the data integrity issues of cloud user data, which is stored in different cloud servers [17] [18]. Here it is noted that the trustworthy brand is not sufficient for the cloud users, since malicious third parties, software and hardware failures may also cause the data corruption or data loss [19][20]. The data user should be able to securely and efficiently check the data integrity without downloading the whole data from the cloud server [21].

[22][23] The authors propose a flexible distributed storage integrity auditing mechanism using the distributed erasure-coded data and holomorphic token. [24] authors addresses the different kinds of challenges in terms of private cloud and also provide the integration process of data restore and backup, encrypting process and data uploading process.

[25] Authors investigate the issue of data security in a different kind of cloud storage system. To attain the quality and availability of cloud data storage they designed a distributed scheme with explicit dynamic data support and this process includes append, delete and update process of data blocks. This proposed approach works based on the erasure-correcting code in the distribution of a file to give guarantee for data dependability and redundancy parity vectors.

Basically, in the cloud computing process, the small files are accessed and stored using Hadoop Distributed File System (HDFS). However, this process has some burden in terms of the NameNode because it is distributed in the file system and which is not taken into account of data placement and prefetching mechanism. In the HDFS system it measures the cutoff point to enhance the input/output performance. From the taxonomic way, the cloud files are classified as logical, structural and independent files. Finally, prefetching methods are utilized to get better performance efficiency and it also takes an account of correlations when files are stored in the cloud.

Securely preserving the cloud data is not an easy work when there are numerous demands from countless applications for the cloud server. At the same time, cloud data storage is not trustable completely because the user did not have a local copy of the cloud data. To address these kinds of problems, the different types of methods is proposed in [26][27]. The server provider helps the cloud user to check the data integrity by using the proposed automatic data reading techniques.

4. Proposed Work

The Enhanced Salted Challenge Response Authentication Mechanism (SCRAM) techniques are used for secret key authentication and sharing process. This work is proposed for efficiently managing the cloud data storage process. This proposed authentication technique, authenticates the server and user's secret keys during the process of cloud data modification. This process can improve the error detection probability which can easily find the un-authorization process. Additionally in this proposed work it also considers the efficient public auditing and user revocation process

In this proposed group sharing approach there is a considerable enhancement in data integrity and reliability. It also manages the drawback in the file sharing process like the hanging of group manager or failure of group manager. In case if there are more number of requests from the user side this work handles it by sharing the workload with multiple group managers. Thus, the reliability and data integrity can increase and failure of group manager take place, this proposed system can use backup if group manager for processing the user requests as shown in Figure 3 This proposed method adopts a new Enhanced Salted Challenge Response Authentication Mechanism (SCRAM) with novel secret key sharing process in the cloud.

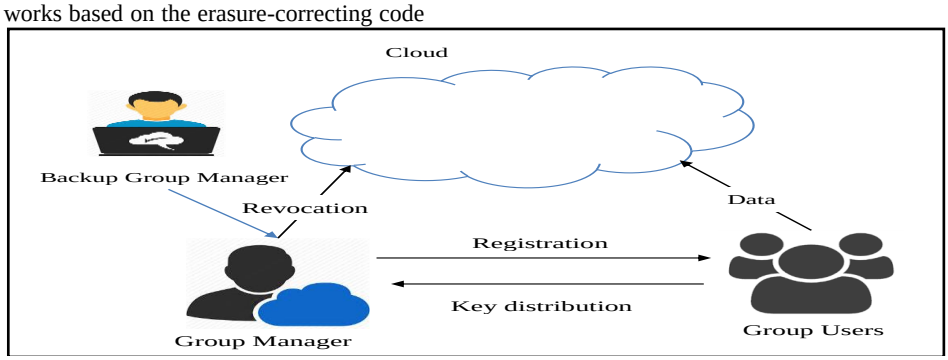

Fig. 3 Proposed Group Sharing

5. Scram Based Data Sharing

In scram based data sharing in dynamic cloud environment consider a cloud system which includes three different entities such as TPA (Third Party Administrator), group users and

cloud server as shown in Figure 3.3.Here the cloud server is termed as the third party who provides the data storage services to the appropriate user groups. A new SCRAM based data sharing method is done by using broadcast encryption methods and group signature application.

This work particularly focuses on how to manage the securely shared cloud data among differ group members. A number of general users, who is the owner of the shared data, can manage the group user's membership function. All group users can modify and access the data and the TPA represents to any sorts of the party that checks the data integrity during the cloud storage process.

As this research work permits the process of public integrity audition with the help of TPA, the TPA can use the long public key. Once the TPA finds about data corruption at the time of auditing process, that specific user wants to report about corruption to other group members. Assume that the data are stored in the form of files after that the files are divided into separate blocks. In the process of auditing in terms of integrity checking, every data block is attached with authentication tag which is originally generated by the master user [28].

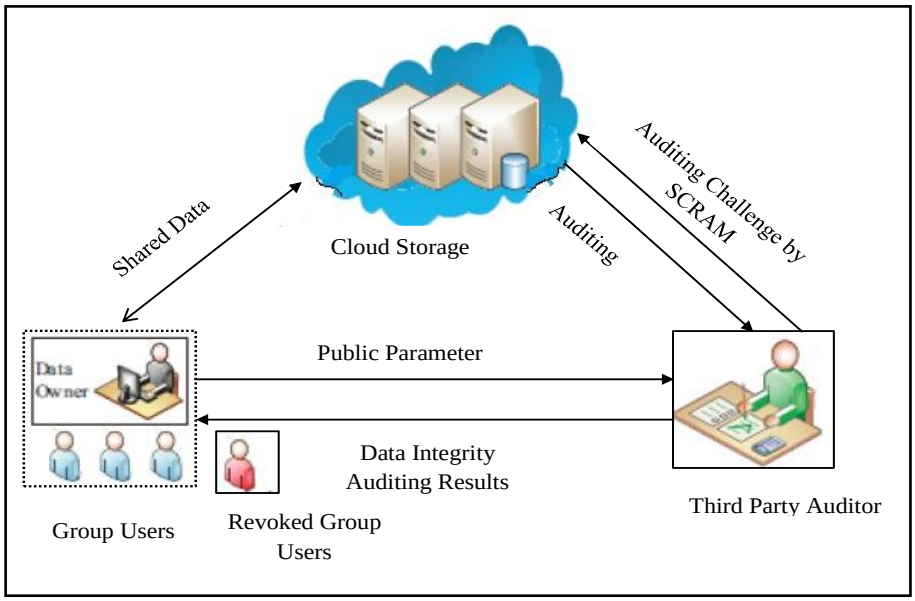

Fig. 4 System Model of Proposed Work

Data Owner: The person who creates the cloud data in terms as data owner and he has large amount of data to be stored in the cloud.

Cloud Storage Server (CSS): The cloud storage server is managed by CSP to give the data Storage Service in the cloud. The CSS is separated into two different components such as Data Server, which stores the client's data and Management Server, which manages the server.

Third Party Auditor (TPA): TPA has capabilities to monitor or manage outsourced data over the entrustment of the data owner. The file's hash values are stored at TPA.

Cloud Service Provider (CSP): The CSP has significant computation recourse and storage space to maintain clients or user data.

Hence, this work proposed a secret key sharing and a secret key authentication mechanism to manage the cloud storage data which is done with the help of the Homomorphic secret sharing and Enhanced Salted Challenge Response Authentication Mechanism (SCRAM) techniques.

Basic share generation and secret reconstruction is as follows

5.1. Share generation

Dealer D picks a random polynomial f(x) of degree t-1;

$f(x) = a_0+a_1x+\ldots\ldots+a_{t-1}x^{t-1} \bmod p$, such that the secret is $s = f(0) = a_0$, and coefficients, a_i, i=0,1,….,t-1, are in GF(p), with p>s and p is a prime. D computes n shares, $y_r = f(x_r)$, r = 1,2,….,n, where x_r is the public information associated with shareholder, U_r.

Then, the dealer distributes each share, y_r, to corresponding shareholder U_r secretly.

5.2. Secret reconstruction

Assume that t shareholders, $\{U_1, U_2,\ldots\ldots..,U_t\}$, work jointly to recover the secret, s. Shareholders release their shares and use the

Lagrange interpolating formula,

$s = f(0) = \sum_{t-1}^{t} f(x_t) \prod_{y=1,y\neq l}^{t} \frac{-x_y}{x_t - x_y} \bmod p$, to recover the secret.

Sharmir's Secret Sharing (SSS) (ShlomiDolev and Yin Li 2015), (Maha TEBAA er al., 2012) (Karthik D U et al., 2014) scheme is formatted to share a $single\ secret\ valuess_j$ among $n\ server$ such that the shares must be extracted from any $k\ server$ so as to $nstructs_j$. The security rests of this schemes on the fact that as a minimum $k\ points$ are required to uniquely reconstruct a degree of polynomial $k-1$. Naturally, the coefficients points utilized in scheme of SSS can be extract from the field F. However, to utilize this scheme on finite-accuracy mechanisms, here need F to the finite field F_p where p is signified as the prime no.

To share s_j , -1 coefficients $a_1, j, \ldots, a_k - 1, j$ nominated randomly from F_p.select a prime $p > s_j$, and k then construct the polynomial function is as follows:

$$q_j(x) = s_j + \sum_{i=1}^{k} a_h, j^{x^h} mod\ p \quad (3.1)$$

After this process create a vector $X = (x_1, \ldots, x_n)$ of distinct elements in F_p, and for each and every data server DS_i, find the share $y_{i,j} = q_j(x_i)$. Together, x_i and $y_{i,j}$ form a point $(x_i, y_{i,j})$ over which polynomial $q_j(x)$ passes.

Certain any k such points $(x_1, y_1, j), \ldots, (x_k, y_k, j)$, here, can reconstruct the polynomial $q_j(x)$ utilizing Lagrange interpolation:

$$q_j(x) = \sum_{i=1}^{k} y_{i,j} l_i(x)\ mod\ p \quad (3.2)$$

where$l_i(x)$ is defined as the Lagrange basis polynomial is as follows

$$l_i(x) = \prod_{1 \le j \le k,\ j \ne i} (x - x_j)(x_i - x_j)^1\ mod\ p \quad (3.3)$$

and$(x_i - x_j)^1$is defined as the multiplicative inverse of $(x_i - x_j)\ modulo\ p$. The secret s_j is the polynomial q_j weighed at $x = 0$, so here get

$$s_j = \sum_{i=1}^{k} y_{i,j} l_i(0)\ mod\ p \quad (3.4)$$

Given only $k' < k$ shares, and thus only k' points, here cannot read anything about s, then for any value of s, could build a polynomial of degree $k - 1$ that passes over all k' points. Accordingly, Shamir's scheme provides perfect, theoretic information security against recuperating s_j from fewer than k $shares$.
Thus, in order to execute SSS, have to use following operations

$WRITE(X, Y)$: Write the data Y in address X.

$READ(X)$: Read the data at address X.

$JUMP(C)$: Transfers control to index C, process the branching operation.

$LOAD(H)$: Load the instruction in address H to the processor.

Let assume both the data items and addresses are secret shared utilizing the same degree polynomials operation`, plus degree reduction step is as follows

The SSS- Plus Degree Reduction
Step 1:$procedure\ SSS - Degree\ Reduction\ (A, B, C)$
Step 2:$Decrease(A\|\|B\|\|C\|\|P\ C\ +\ 1, 3`, `)$
Step 3:$R1 \leftarrow READ(A)$
Step4:$R2 \leftarrow READ(B)$
Step5:$R\|\|Num\ =\ SSS - SUB(R1, R2)$
Step6:$DECREASE(R\|\|Num, *, `)$
Step7:$WRITE(B, R)$
Step8:$JUMP(Num \cdot C + (1 - Num) \cdot (P\ C\ + 1))$
Step9:*end*

The three parameters A, B, C where denoted as contents at $address\ B$ are subtracted from the substances at $address\ A$, and the product is stored at $address\ B$, and then, if the result is $not\ greater$ than 0. PC is defined as the $program\ counter$.

Although this process stores the secret shares using hashed values, it is yet unsecured in cloud if the hash values of the stored file is supposed to be known the hashed secret shares. Another drawback of this process is just hashing function alone is not enough for secure storing. Therefore a hash function should be Enhanced Salted to avoid against pre-computed hash table look-ups password. Thus, in this work the Enhanced Salted Challenge Response Authentication Mechanism (SCRAM) technique is used.

6. Performance Results

6.1. Authentication Signature Generation Time Of Scram

To present the performance of authentication signature generation, different numbers of blocks in the files ranges from 1000 to 1, 00,000. The signature generation time gradually rises when the number of blocks increases, 2.10sec to 99.24sec. Figure 5 shows that the signature generation time is comparative to the block size.

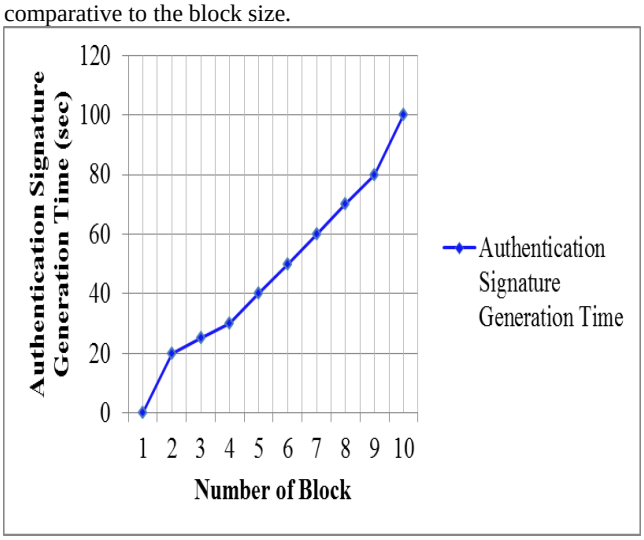

Fig. 5 Authentication Signature Generation Time of SCRAM

6.2. User Verification Time

Figure 6 shows the comparison results of proposed work of Enhanced Salted Challenge Response Authentication Mechanism (SCRAM) techniques with other two algorithms such as Asymmetric Group Key Agreement (ASGKA) scheme and Dynamic Provable Data Possession (DPDP) in terms of user verification time.

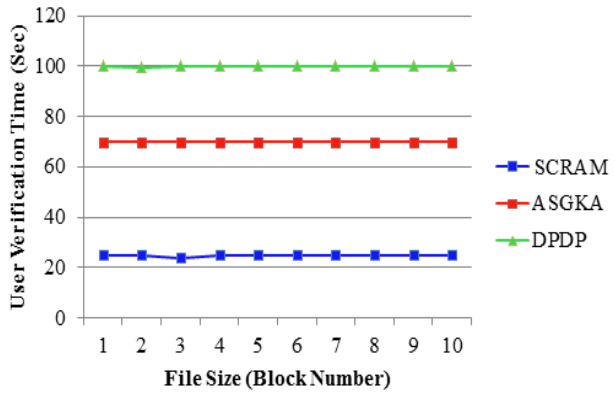

Fig. 6 User Verification Time of SCRAM

From the results it indicates that, ASGKA scheme and DPDP has comparable user verification time which is very high when compared with the proposed work. This is because ASGKA and DPDP need a number of multiplication operations and exponentiation operations on Group number of challenge blocks, which are constant accordingly.

6.3. Communication Cost Evaluation

Figure 7 shows the comparison result of proposed work namely Enhanced Salted Challenge Response Authentication Mechanism (SCRAM) techniques with other two algorithms such as Asymmetric Group Key Agreement (ASGKA) scheme and Dynamic Provable Data Possession (DPDP) in terms of Communication Cost.

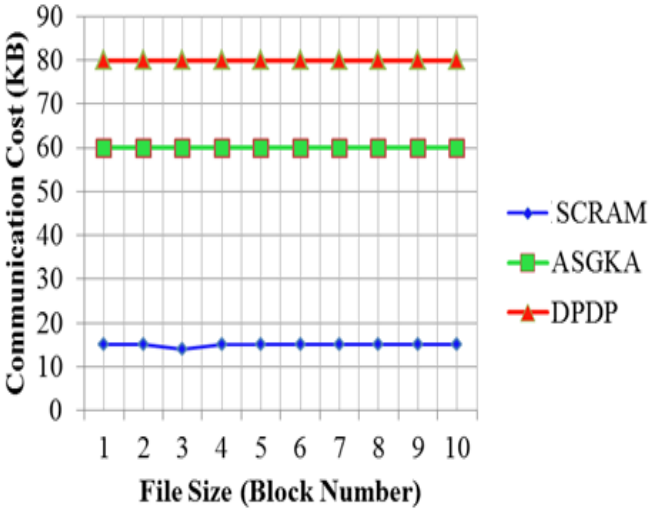

Fig. 7 Communication Cost of SCRAM

From the results indicates that, ASGKA and DPDP have comparably high communication cost while compared with proposed work and its computational cost also increases based on the TPA.

7. Discussion

This proposed work offers some unique features when compared with some of the existing work as follows

- It offers strong security which is essential to maintain and store the confidential data in a cloud environment.
- This system functions against different attacks at the user side.
- This system offers rigorous security utilizing secret key authentication and sharing process.

This proposed system also efficiently supports the dynamic group which means that the user revocation process and joining new user process are effortlessly attain without involving the other user in that group.

8. Conclusion

This paper presents a novel secret key sharing process and a mechanism of secret key authentication to manage the cloud storage data which is accomplished by using new Enhanced Salted Challenge Response Authentication Mechanism (SCRAM) approach. This approaches can authenticate the server and user secret key while altering the cloud files. It also improves the probability of error detection, public auditing process, and user revocation process.

References

[1] Kaushal, V., Bala, A. (2011),"Autonomic fault tolerance using haproxy in cloud environment", International Journal of Advanced Engineering Sciences and Technologies, Vol.7, No.2, PP.54-59

[2] VeeralakshmiPonnuramu, LathaTamilselvan (2012), "Data Integrity Proof and Secure Computation in Cloud Computing",Journal of Computer Science, Vol.8, No.12, PP.1987-1995.

[3] Sultan Aldossary, William Allen (2016), "Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions",International Journal of Advanced Computer Science and Applications (IJACSA),Vol. 7, No. 4.

[4] JasbirKaur, SupriyaKinger (2014), "Analysis of Different Techniques Used For Fault Tolerance", International Journal of Computer Science and Information Technologies, Vol. 5, No.3, PP.4086-4090

[5] SABAHI. F (2011), "Cloud computing security threats and responses", IEEE 3rd International Conference on Communication Software and Networks (ICCSN), PP.245 – 249

[6] Akhilesh Kumar Bhardwaj, Surinder, Rajiv Mahajan (2015), "A Modified Heuristic-Block Protocol Model for Privacy and Concurrency in Cloud", International Journal of Advanced Computer Science and Applications, Vol. 6, No. 9, PP. 179-184.

[7] AnamikaSirohi, Vishal Shrivastava (2015), "Implementing Data Storage in Cloud Computing with HMAC Encryption Algorithm to Improve Data Security", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 8, PP. 678-684.

[8] AutadeDhanshri P, Raut S.Y (2015), "Review of Public Integrity Auditing and Group User Revocation for Shared Dynamic Cloud Data", International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering, Vol. 3, Issue 12, PP. 48-52.

[9] Aameek Singh, Ling Liu (2008), "Sharoes: A data sharing platform for outsourced enterprise storage environments", In Proceedings of the 24th International Conference on Data Engineering, ICDE, IEEE, PP.993-1002.

[10] AkankshaRana (2015), "Security in Cloud using Implicit Security Model and OTP", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 4, Issue 3, PP.554- 555.

[11] Ankush R. Nistane, ShubhangiSapkal, R. R. Deshmukh (2016), "Privacy Preserving Public Auditing and Data Integrity for Secure Cloud Storage Using Third Party Auditor", International Journal of Advanced Engineering, Management and Science (IJAEMS), Vol-2, Issue-2, PP. 30- 34.

[12] Aarthi T, Rathi G, Prabakaran R. S (2014), "Towards Secure and Dependable Storage Services in Cloud Computing", International Journal of Modern Engineering Research (IJMER), Vol.4 Issue.1, PP. 194-197.

[13] E. Aguiar, Y. Zhang, and M. Blanton (2014), "An overview of issues and recent developments in cloud computing and storage security", High Performance Cloud Auditing and Applications, Springer, PP.3–33.

[14] ÁineMacDermott, Qi Shi, KashifKifayat (2015), "Detecting Intrusions in Federated Cloud Environments Using Security as a Service", International Conference on Developments of E-Systems Engineering (DeSE), PP.91 – 96.
[15] F. S. Al-Anzi, A. A. Salman, N. K. Jacob, J. Soni (2014), "Towards robust, scalable and secure network storage in cloud computing," in Digital Information and Communication Technology and it's Applications (DICTAP), Fourth International Conference on IEEE, PP. 51–55.
[16] Bo Donga, QinghuaZhenga, FengTiana, Kuo-Ming Chaoc, RuiMaa, RachidAnanec, (2012), "An optimized approach for storing and accessing small files on cloud storage", Journal of Network and Computer Applications, 35 (6), PP.1847–1862.
[17] BadiAlekhya (2013), "Improving Data Dynamics and Storage Security In Cloud Computing", International Journal of Advancements in Research & Technology, Vol.2, Issue 4, PP. 327- 332.
[18] R. Buyya, C.S. Yeo, S. Venugopal, J. Broberg, I. Brandic (2009), "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility," Future Generation Computer Systems, Vol.25,No.6, PP. 599-616.
[19] Boyang Wang, Baochun Li, Hui Li (2015), "Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud", IEEE Transactions on Services Computing Vol. 8, Issue.1, PP. 92 – 106.
[20] M. Bellare, P. Rogaway (1966), "The exact security of digital signatures: How to sign with RSA and Rabin", In U. Maurer, editor, Proceedings of Eurocrypt, Springer-Verlag, Vol.1070, PP. 399–416.
[21] Borja Sotomayor, Rub´en Santiago Montero, Ignacio Mart´ınLlorente, Ian Foster (2008), "Capacity Leasing in Cloud Systems using the OpenNebula Engine",http://haizea.cs.uchicago.edu/pubs/Haizea_CCA08.pdf.
[22] D. Bogdanov, S. Laur, J. Willemson (2008), "Sharemind: A Framework for Fast Privacy-Preserving Computations," the 13th European Symposium on Research in Computer Security (ESORICS), https://eprint.iacr.org/2008/289.pdf
[23] Cash, D., Kup¸cu, A., and Wichs, D. (2013), "Dynamic proofs of retrievability via oblivious ram", 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, 26-30.
[24] Cong Wang, Qian Wang, KuiRen, Ning Cao, Wenjing Lou (2012), "Towards Secure and Dependable Storage Services in Cloud Computing", IEEE Transactions on Cloud Computing, Vol.5, Issue.2, PP.1-14.
[25] Cong Wang, Sherman S.M. Chow, Qian Wang, KuiRen, Wenjing Lou (2013), "Privacy-Preserving Public Auditing for Secure Cloud Storage", IEEE Transactions On Computers, Vol. 62, No. 2, PP. 362 – 375.