Vol. XV & Issue No. 01 January - 2022
INDUSTRIAL ENGINEERING JOURNAL

DESIGN XOR BASED ALGORITHM TO ENHANCE THE MOBILE COMPUTING CLOUD SECURITY

Sumant Raj Chauhan
Dr. Gagan Markan

Abstract

The cloud is a computing model used by numerous consumers, consisting of folks and data storage organization, but up to now has difficulty putting in place appropriate protection trial toward keeping the discretion and reliability of that information. There are many important issues in cloud computing, including issues of privacy, protection, confidentiality, communications power, government surveillance, accuracy, and responsibility. Encryption is a common technique for securing complex data that this paper has suggested for the cloud computing platform a new security framework that ensures safe communiqué structure with hides in sequence as of others. This model includes DES base file encryption structure with asynchronous key exchange method in favor of information otherwise fact exchanges. That representation also provides a special user authentication method encryption key through definition that planned algorithm incorporates two features fist one acknowledged algorithm called Ceaser cipher also second characteristic dependent cryptography. Text information is encrypted in this research work with "Caesar Cipher" and after that cipher data is another time encrypted with the projected algorithm using the 128-bit private key, the last step of the encryption process, cipher related text attributes are stored along with cipher-generated text once encryption that presents two steps authentication throughout decryption processes. To authenticate its efficacy, the security comes near planned with built used for data protection definition on the subject of elevated confidentiality with authenticity used for cloud data by cloud storage ending through research review. It is seen from the outcome review the projected procedure have superior Avalanche consequence with implementation point, the current procedure with being capable of therefore exist integrated into encryption/decryption method of some plain text otherwise key value.

Keywords: Cryptography, Caesar Cipher, Homomorphism Encryption, and Virtualization.

1. INTRODUCTION

Cloud computing be one of the most relevant technologies that evolve for developers and consumers alike. A preferred platform for people who are interrelated with the networking environment of the current world cloud computing is. Over the past few days, therefore, providing protection has become a major cloud computing technology and service running lying on a distributed network with virtualization resources accessible via regular Internet networking protocol and standard.

Cloud = Virtualization + Abstraction

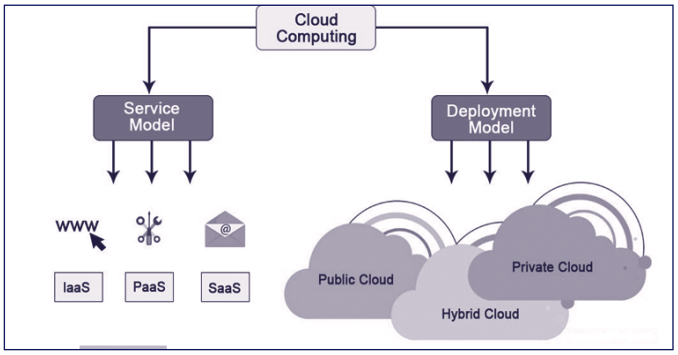
These abstract users device execution specifics with a developer. Applications run on the physical machine are not defined locally stored data be outsourced in the direction of new system administration unknown. Example Website AZURE, services AMAZON, GOOGLE, and so on. There are different kinds of clouds, each differing from the other. Public clouds offer on-line computing infrastructure and storage. Those are managed by third-party companies that manage and control all the equipment, software, and general infrastructure. Clients access services through accounts that just about anyone can access. Private clouds are reserved for particular clients, usually one business or organization. The data service center of the firm may host the service in cloud computing. Numerous private cloud computing services are available on a private network. As the name suggests, hybrid clouds are a combination of both private and public services. This form of the model provides more versatility for the user and helps to improve the infrastructure and protection for the user. Cloud manufacturing (CM) is an emerging concept extending and adopting the approach of cloud computing for manufacturing [1].

1.1 Delivery Method of Cloud Computing: Software-As-a-Service (SaaS) offering the software as a service to the customer. Example Google Drive, Gmail, DropBox, and so on. Platform-As-a-Service (PaaS) in which cloud provides users with network otherwise infrastructure for their Internet applications. Example: Microsoft Azure, Google Gears. Infrastructure-as-a-Service (IaaS) provides the user with computing storage with networking capability by that cloud service provider. The virtual version of the network is provided toward the users other than the real physical network be managed at remote locations by service providers. Example: Web Services from Amazon, the compute engine from Google.

1.2 Deployment Model of Cloud Computing: Private Cloud is own with use to manage the virtualized infrastructure for a single entity. Virtual Cloud is owned and distributed by a single agency or corporation for general public use to provide admittance toward computing services by nominal cost. Community Cloud is mutual by different companies otherwise organizations. Hybrid clouds mean a single cloud is formed by more than two clouds. There are set issues in the cloud computing environment, such as privacy, security, performance, load balance with consistency. Data security be mainly significant in that issue [2,3]. Safe cloud architectures

[4] are proposed for enhancing high-end data protection. Cryptography is the most effective method for protecting our records. Various data security encryption schemes have been in use for several decades.

Figure-1 the cloud computing deployment model



2. RELATED WORK

Various cloud computing security work has been conducted a day now. Several researchers have worked out classification base cloud computing security models [5]. Although identifying only actual user does not always provide relief from hacking or intruding data or information saved in the cloud environments database. Yao's Garbled Circuit be using in cloud servers to secure data saving [6]. But it is a research focused on recognition, too. It doesn't work with ensuring security on the entire platform of cloud computing. Research relating to ensure security in the entire cloud computing environment has previously worked out and shaped within various structures. AES file encryption scheme is used in some of the models that have been carried out. Also investigated is the DES-based file encryption system. But in one storage server, that model holds mutually the encryption key with the encrypted file. So, only tried and succeeded in hacking one of the servers will provide the hacker with all the knowledge about the file which is not desirable. Cloud Computing security can be broadly classified into three domains as Security Categories (Security issues faced by cloud providers and Customers) Security Dimensions (Security domain, risks, threats) Security in Service Delivery Models (Security issues in SaaS, PaaS, Iaas) [7]. For security in the cloud computing environment, some other models and secured architecture are proposed. While this model ensures safe communication between users and servers, the loaded information is not encrypted by these models. But the uploaded information needs to be authenticated to ensure the best security procedure so that nobody can know the details. The emergence of cloud computing has brought an evolution in many sectors like education, healthcare, governance, etc. Cloud computing is increasing of interest to the manufacturer, but cloud computing adoption rates are low in the manufacturing sector. Cloud production is at an early stage of development and is especially promising as a concept in additive manufacturing [9].

1.1 Modern Cryptography: Current encryption algorithms like RC6, AES, DES, 3DES, and Blow-Fish continue to cooperate with a critical responsibility within cloud computing data security. That assessment was carried out using NIST statistical research within cloud computing environments

2.2 Searchable Encryption: Searchable encryption is an outward form of encryption the deals with searching otherwise recovering data within encrypt data lacking decrypting the entire data. Using encryption/ searchable encryption technologies, cloud-secure architecture [8, 9] allows searching within the form of encrypted data and data reclamation within a safe approach.

2.3 Homomorphic Encryption: Homomorphic encryptions [5, 6] is a type of encryption method that performs a few cipher text computations with therefore generates match by the results of the plaintext process when decrypted. Typically speaking, Homomorphic methodology is about preserving data integrity in the clouds.

2.4 Attribute-based Encryption: Characteristic based encryption (ABE) [4] be one too many public-key encryptions which enables users toward encrypting also decrypt user base data. Present be two types of ABE schemes fist one is key policy ABE and second is text policy ABE cipher.

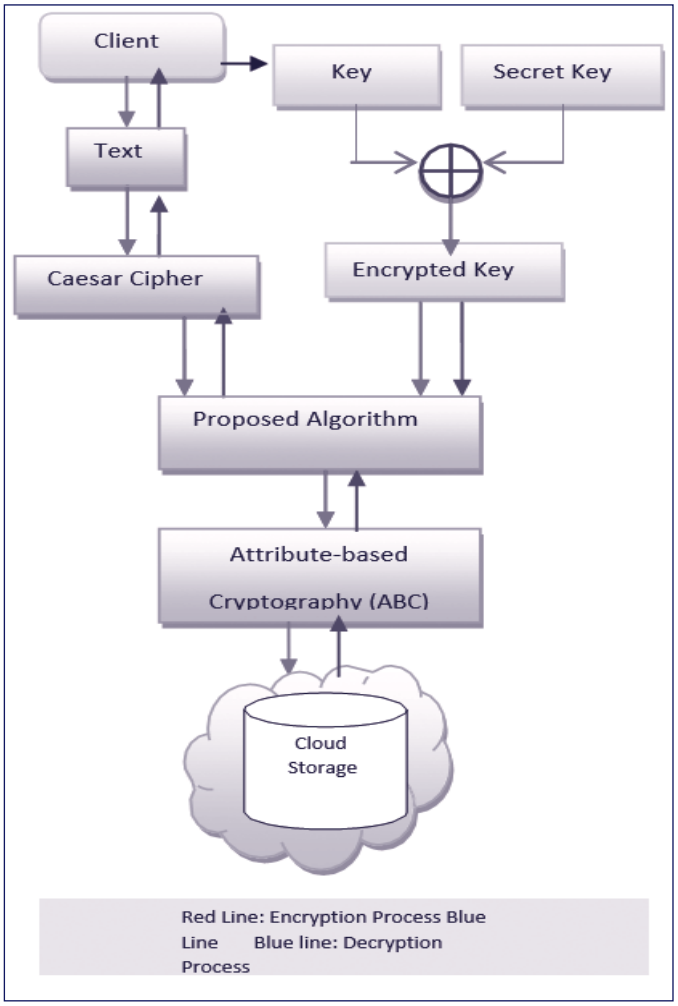
2.5 Hybrid Encryption: Hybrid encryptions are encryption modes which combine two otherwise extra encryption system to benefit commencing the strength of each encryptions type.

3. PROPOSED METHODOLOGY

When growing numbers of companies also individual continue toward subcontract that data to cloud storage, more attention is drawn to security and privacy protection for users new and new organization furthermore individual tends to outsource the data toward cloud storage, that security with user privacy fortification magnetizes extra consideration. Data file encryption also decryption is predominantly user-centric, allowing only authorized users to upload with admittance files, and deciding whatever a file be able to share with extra users. When we speak about data protection in a cloud environment, there are two endings. Second, data protection may be concerned because data passes through that networks following data was collected from the user site from every web-based applications. Then on the second closing stages, that security issue may be there on the server end while data be previously being processed in the server disk through the network. The key explanation for the proposed work is the second issue that the data file at the Server End is concerned about security when data being store in server disk. Holding securities in cloud storage researchers encompass provided the projected works, which is in nature hybrid comprising three phases, following the skeleton. As shown in Figure 1, the technique of Ceaser Ciphering [2] is used in the first step, providing initial level protection while, without doubt, providing more efficiency. The second step of the projected work deal with a freshly developed encryption algorithm base on the principle of symmetric cryptography (block-based). That work use 128-bit block size intended for the principle of encryption with that 128-bit block size offers a higher degree of protection with the same time the 128-bit block size be protected by the aid of that protected key which is besides 128-bit. The encrypted key is created to apply the XOR process over the user's private key with a cloud secret key. Therefore, via that newly developed

encryption algorithm, the data protection standard is doubled. Last but not least, it is very clear that cryptographic encryption procedures play a significant responsibility when thinking about data protection, but at the same time, it is necessary to verify the user's authentication rights who attempt to access such data stored on the cloud disk. User authentication or verification before granting cloud service access plays a very important role in security measures. Therefore, via the Attribute-Based Cryptography (ABC) techniques, that third step of the recently projected works concentrates on top of cloud user authentications[10]. Using this method, that algorithm produces an attribute related to ciphertext and will manage user requirement authentication based on this attribute. If the user meets this requirement, the newly introduced Cloud-based security checks for the key as well.

Figure-2 Conceptual design block diagram



3.1 Certain meanings: K< -- Private key specified through the user.

Secret Key < -- Gen(s): be a key generator the take input key size 's' with generate output secret key 'SK' of size 's'.

CT_1:= Caesar (T, 5): an algorithm to take text 'T' like an input encrypt by the shift of 5 characters also generates ciphertext CT_1.

Encrypted Key: = Encrypted (Key, Secret Key): algorithms that encrypt K through SK and generate encrypted key EK.

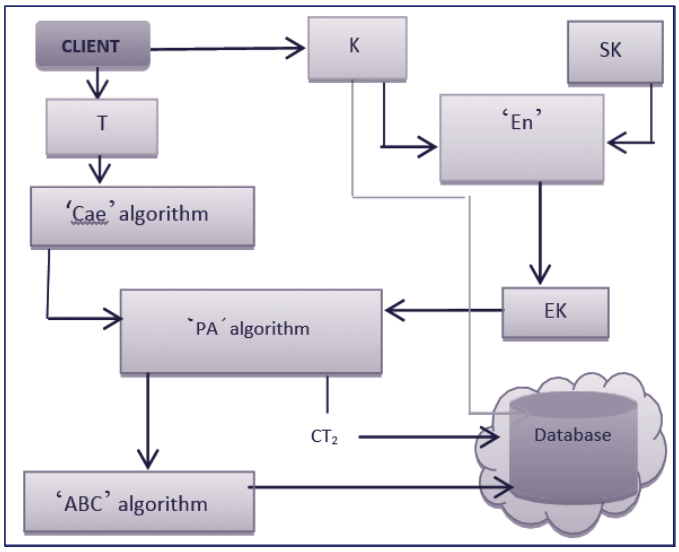
CT_2:= Propose algorithm for encryption (CT_1, EK): an algorithm to take input ciphertext 'CT_1' with encrypting it by EK also generates output ciphertext 'CT_2'.

α:= ABC(CT_2, K): an algorithm to take CT_2 and K like input and generate an attribute α.

CT_1:= Propose algorithm for decryption (CT_2, EK): an algorithm to take input ciphertext 'CT_2' plus decrypt it through EK and generate output ciphertext CT_1' such that CT_1' == CT_1

T:= Cad(CT_1, 5): an algorithm to take text CT_1' like input and encrypt by a reverse shift of 5 characters and generatesT' such that T' == T.

Figure-3 Encryption while the data is stored



3.2 Save System (Figure 3): The method of storing or encrypting text data, as shown in Figure. 3 Where CT2 = T (Caesar, PAE, ABC), ciphertext be generating with apply Caesar, PAE, ABC more text algorithms with store in the cloud storage. Comprehensive encryption method step is explained below:

Step-1: Start

Step-2: Attach Cloud User's text information (T) with the private key (128-bits) (K).

Step-3: Data (T) with key (K) of the user text hit Cloud Server Start.

Step-4: Read data with key (128-bits) in favor of user text on Cloud End

Step-5: Using Caesar algorithms on T.

Step-6: Produced Text CT1 preliminary cipher level.

Step-7: Prepared Encrypted (EK) Keys.

Step-7.1: Generated SK with the 'Gen' algorithm.

Step-7.2: To produce EK, apply 'En' algorithms.

Step-8: Move the CT1 and EK algorithm to the next point.

Step-9: Use the 'PAE' algorithm to produce the second level of CT2 ciphertext.

Step-10: Pass CT2 to the 'ABC' algorithm to create an 'α' attribute.

Step-11: Stop

3.2.1 Propose step encryption algorithms (Figure 4): Note: CT1 = Cipher Text generate following level one encryption, EK = Encrypt Key, L = Left of CT1, R = Right of CT1, 1K64 & 2K64 = Sub-Key of EK, CT2 = Cipher Text generate following level two encryptions.

Step-1: input CT_1 & EK

Step-2: divide CT_1 = L & R

Step-3: divide EK = $^1K_{64}$ & $^2K_{64}$

Step-4: L>>r -----> L (2-bit Right Circular shift)

Step-5: L⊕R ------ > L (XOR operations)

Step-6: R>>r -----> R (2-bit Right Circular shift)

Step-7: exchange L & R

Step-8: L⊕ $^1K_{64}$ -------> L

Step-9: L << l -----> L (2-bit Left Circular shift)

Step-10: L⊕R ------> R

Step-11: R << l-----> R (2-bit Right Circular shift)

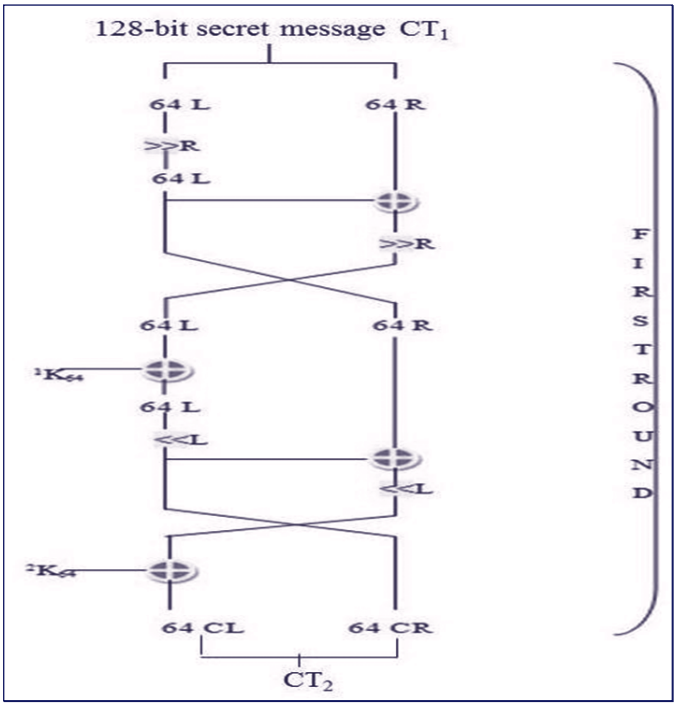
Step-12: exchange L & R

Step-13: L⊕$^2K_{64}$ > L

Step-14: replicate steps 4 to 13 through 10 round

Step-15: CL+CR=CT2

Figure.4: Suggested Encryption Architecture



3.3 Retriever (Figure 5): The recovery with the decryption procedure of text data performs as shown in Figure.4 where T = CT2 (ABC, PAD, Cad), the text is generated with apply Cloud storage algorithm ABC, PAD, Cad larger than ciphertext recovered. See below for a thorough step of the decryption processed.

Step-1: Start

Step-2: Use 'K' with 'α' to enter. Cloud App (for User Authentication).

Step-3: At Cloud Server End the user key 'K' and 'α' reaches.

Step-4: Verify Authentication

Step-4.1: By combining 'K' and 'α' in storage in the cloud.

Step-4.2: If user authentication occurs at step 4.1, the next step will be the cloud security system. Otherwise, the cloud protection program prevents the user from accessing the file rights.

Step-5: By applying the 'En' algorithm, prepare EK.

Step-6: Move EK with CT2 into 'PAD' algorithms.

Step-7: Generate the initial cipher level text, CT1 "such that, CT1'==CT1.

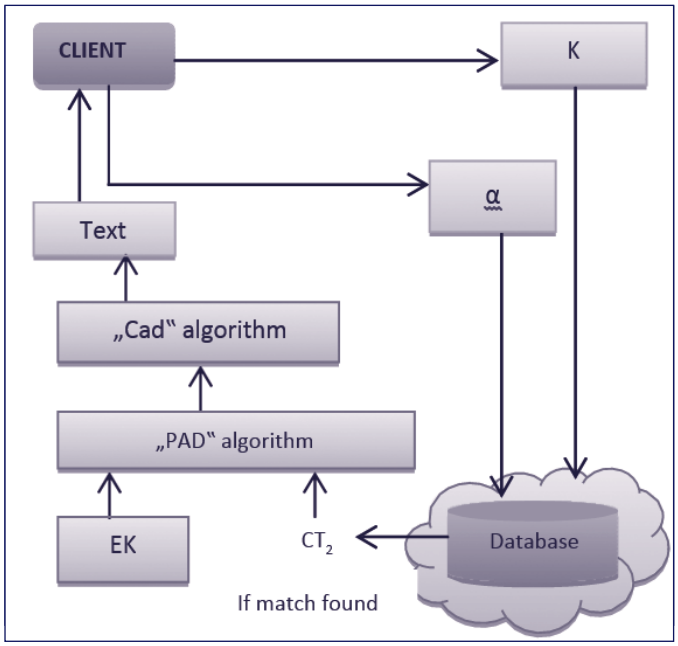
Step-8: Pass CT1' to algorithm 'Cad.'

Step-9: Generates data from the user Text, T' such that T'==T.

Step-10: Return user text to the user end (another end of the cloud environments).

Step-11: Stop.

Figure- 5: The method of decryption when recovering data



3.3.1. Proposed move to decode algorithm (Figure 6): Note: CT2 = Database Cipher Text, EK = Encrypt Key, CL = Left part of CT2, CR = Right part of CT2, 1K64 & 2K64 = Sub-Keys of EK, CT1 = Cipher Text generate following the PAD algorithm decryption processed is completed.

Step-1: Input CT_2 & EK

Step-2: Divide CT_2 = CL & CR Step 3: Divide EK = $^1K_{64}$ & $^2K_{64}$

Step-4: CL⊕$^2K_{64}$> CL(XOR operations)

Step-5: exchange CL&CR

Step-6: CR>>R>CR(2-bit Right circular shift)

Step-7: CL⊕ CR------> CR

Step-8: CL >> R> CL (2-bit Right circulars shift)

Step-9: CL⊕$^{1}K_{64}$ ------ > CL

Step-10: exchange CL & CR

Step-11: CR <<L> CR (2-bit Left circular shift)

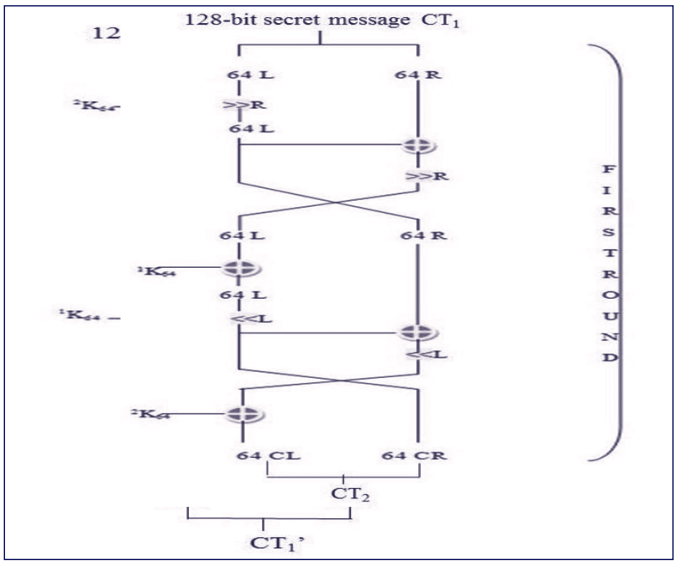
Step-12: CL ⊕ CR> CR

Step-13: CL << L>CL(2-bit Left circular shift)

Step-14: replicate steps 4 to 13 through 10 round

Step-15: CL+CR ------ > CT_1"

Figure-6: Suggested Encryption structural design



3.4 Principal feature of propose works: • Three level Concepts for Security. • Core Theory for Generators. • Block encrypted key concept cipher. • Text Data confidentiality with User Authentication.

• Comprehensible. • Robustness. • Small Time to Execute

4. CONCLUSION

The present research work focused on the data protection techniques of cloud computing. The drawing of an algorithm is mutual using the two extra encryption schemes called caser cipher and ABC attributes. These encryption schemes ensured data safety and security of cloud data storage at cloud ends. Such techniques have enhanced the security of the cloud using the key generators to produce random keys of different lengths also increases productivity in terms of implementation time to protection. This paper has five contexts focused on 1) Security, 2) Technical, 3) Organizational Challenges, 4) Environmental, and 5) External Pressure. The authors also discussed various advantages of the proposed strategy together with a variety of encryption schemes using systems XOR methods based on the common key type. The methodology suggested offers a confidentiality structure. The approach we used in this paper will help to make cloud computing a strong structure for data security. This needs top management support as well as overwhelming issues of security and reliability.

5. REFERENCES

[1]. Vaibhav S. Narwane & Balkrishna E. Narkhede & Bhaskar B. Gardas & Rakesh D. Raut, 2019 "Cloud manufacturing issues and its adoption: past, present, and future," International Journal of Management Concepts and Philosophy, Inderscience Enterprises Ltd, vol. 12(2), pages 168-199.

[2] Ramgovind S, Eloff MM, Smith E, "Cloud Computing Security Management," IEEE, 2010.

[3] Eduardo Fernández-Medina, Keiko Hashizume, David G Rosado, Eduardo B Fernandez, Journal of Internet Services and Applications, "Analysis of security issues in cloud computing," Springer, 2013.

[4]. Raut, Rakesh, Narkhede, B., Patil, B., 2013. Clouds Computing Architecture: How SMEs, Can Manage? 4th International Case Conference, September 24-26, 2013.

[5]. "Identity-based Cloud Computing Authentication," Hongwei Li, Yuanshun Dai, Ling Tian, and Haomiao Yang.

[6]. Ahmad-Reza Sadeghi, Sven Bugiel, Stefan Nurnberger, Thomas Schneider, "Twin Clouds: Low Latency Secure Cloud Computing," CASED, 2011.

[7]. Rakesh D. Raut, Vaibhav S. Narwane." Adoption of Cloud Computing in Manufacturing: SWOT Analysis" Proceedings of the International Conference on Industrial Engineering and Operations Management Paris, France, July 26-27, 2018.

[8] Saleh M. Al-Saleem, Hamdan M. Al-Sabri, "Building a Cloud Storage Encryption (CSE) Software Security Enhancement Framework" IJCSI International Journal of Computer Science Issues, Volume 10, Issue 2, 2013.

[9] Trend Micro, Mao-Pang Pang Lin, Taiwan, Wei-Chih Hong, Chih-Hung Chen, Chen-Mou Cheng, International Conference on Privacy, Security and Trust 'Design and Implementation of Multi-User Secure Indices for Encrypted Cloud Storage, IEEE 2013.

[10] Jian Mao, Fang Liu, John Messina, Jin Tong, Robert Bohn, Lee Badger, and Dawn Leaf, US Department of Commerce, NIST Cloud Computing Reference Architecture, Gaithersburg, MD, 2011.

AUTHORS

Sumant Raj Chauhan, Research Scholar, Department Computer Science & Engineering, NIILM University, 9 Km Milestone, NH-65, Kaithal - Ambala Road, Kaithal – 136 027, (Haryana)
Email: sumantraj2003@gmail.com / Cell: 081260 74144

Dr. Gagan Markan, Associate Professor, Department Computer Science & Engineering, NIILM University, 9 Km Milestone, NH-65, Kaithal - Ambala Road, Kaithal – 136 027, (Haryana)
Email: ovloxindia@gmail.com