The Scientific Temper (2023) Vol. 14 (1): 227-232
Doi: 10.58414/SCIENTIFICTEMPER.2023.14.1.29
E-ISSN: 2231-6396, ISSN: 0976-8653
https://scientifictemper.com/
RESEARCH ARTICLE

EAM: Enhanced authentication method to ensure the authenticity and integrity of the data in VM migration to the cloud environment

Raja Selvaraj and Manikandasaran S. Sundari

Abstract

Cloud is a prominent technology today to provide computing resources to users. In previous days, industries or enterprise users are maintaining their data on-premises. Therefore, it creates many management issues in the industries. Cloud gives solutions to industries to maintain their data in the cloud data center. As a result, many industries are outsourcing their data to the cloud. When outsourcing, the data are migrated along with Virtual Machines (VM). During the migration, the data are vulnerable to attack. As a result, the data may tamper with fault content by the adversarial. Therefore, it is necessary to maintain data authenticity and integrity verification during the migration. This paper proposes an authentication mechanism to verify the data authenticity when migrated from on-premises to off-premises. The paper proposes a novel procedure to migrate the data in the virtual machine. After migration, the data is verified for authenticity using the proposed mechanism. An enhanced hashing procedure is proposed in the paper to verify the data authenticity. The proposed authentication mechanism is simulated in the cloud environment, and results are given in the tables and graphs. The results show that the EAM efficiently provides authentication and integrity of data migrated from on-premises to the cloud data center.

Keywords: Data migration, Data authentication, Authenticity, Data integrity, Cloud security, Hashing.c

Introduction

Cloud computing is the only way to host the user's data and applications reliably. The cloud is a virtual space to keep the user's data and applications. In addition, it provides many benefits to the industry by maintaining its cloud database. As a result, since 2007, the cloud has dominated the IT world in all aspects (Arockiam, 2017). The main contribution of the cloud is self-cloud service in on-demand, more elastic service provisioning, multi-tenant service accessing; the online pool of servers is up and running 24/7, etc. In addition, the multiple cloud data centres situate everywhere to maintain hassle-free user data usage. The cloud can be categorized into public, private, community and hybrid (Xiaoyu, W, 2020). The cloud services are delivered as software, platform and infrastructure. The infrastructure holding all the cloud resources is a cloud data centre. Biggest IT industries like Google, Microsoft, Amazon etc., own the cloud data centre. They provide computing services to users based on their requirements. Therefore, the cloud delivers many benefits to small and medium-scale enterprises to improve their businesses by providing virtual computing resources (Alouffi, B, 2021). The concerned users access the virtual computing resources from their respective places worldwide. One of the main services of the cloud is to store users' data, which is returned to them when needed. Therefore, the cloud provides reliable storage to maintain the users' data.

Cloud is a domain of hosting applications and data quickly. As a result, the new application deployment and migration of existing applications are growing exponentially. Cloud maintains a user's data file in multiple places to provide reliable storage. Apart from all the benefits of the cloud, security issues are the biggest risk in cloud computing (Monikandan, S, 2015). There are many ways for unauthorized network parties to hack the data. As a result, users are interested in the cloud for migrating their data to cloud storage. Still, security challenges in the cloud create hesitation among users in thinking about data migration to the cloud. This is because of whether the users' data

Department of Computer Science, Adaikalamatha College, Vallam, Thanjavur, Tamil Nadu, India. Affiliated to Bharathidasan University, Trichy, Tamil Nadu, India.

***Corresponding Author:** Raja Selvaraj, Department of Computer Science, Adaikalamatha College, Vallam, Thanjavur, Tamil Nadu, India. Affiliated to Bharathidasan University, Trichy, Tamil Nadu, India, E-Mail: rajasjc@gmail.com

How to cite this article: Raja, S., Manikandasaran, S. S. (2023). EAM: Enhanced authentication method to ensure the authenticity and integrity of the data in VM migration to the cloud environment. The Scientific Temper, **14**(1):227-232

Doi: 10.58414/SCIENTIFICTEMPER.2023.14.1.29

Source of support: Nil

Conflict of interest: None.

Received: 18/01/2023 **Accepted:** 12/02/2023 **Published** : 25/03/2023

are securely migrated along with the Virtual Machine(VM) during the migration. Security mechanisms are available to ensure data security in the network, even though the security issues in the cloud are not addressed (Patil. D, 2021). According to various studies, researchers proposed various security mechanisms to keep the data secure, but important security parameters left it open. Cryptography is a mechanism to address security issues and challenges in the network. It provides various data security services, such as authentication, confidentiality and integrity (Subasini . C. A, 2021) (Pachaghare. S, 2020). Among them, authentication and integrity are used to ensure data security when the data are migrated from on-premises to the cloud data centres (Atiewi. S, 2020). This research work addresses data security when migrating it to the cloud. A data migration architecture is already proposed for secure migration (Manikandasaran. S. S, 2018). To continue the research to address the secured data migration, this paper proposes an authentication and integrity mechanism to ensure that the data is not modified and comes from the authorized user. The authentication discussed in this research concerns Data Origin Authentication (DOA), which ensures the receiver's data comes from an authentic sender. Integrity is a mechanism that verifies the data is not modified during migration (Wang. C, 2020). Authentication and integrity are used in this research to ensure data security in data migration.

Related Work

Cloud security is the most discussed topic among researchers. Most researchers are trying to address the security issues and challenges in the cloud. Such present techniques are discussed in this section.

Z. Ghaffar et al. (Ghaffar. Z, 2020) discussed that cyber-physical-social systems (SSPCs) represent an evolving paradigm, including the social, physical and cyber worlds. The vital goal of ROSS is to provide customized, high-quality, proactive services to end users. An ingenious framework for reliable services is needed to accomplish this objective. In this regard, cloud storage (consuming a great connection with the physical, cyber, and social world) necessitates a dependable framework for protected communication between the cloud and its users. Consequently, the document presented an improved, secure and practical system for data access. Besides, to add the flexible distribution of data controlled by the data owner, the protocol provides proxy re-encryption in which the cloud server utilizes the proxy re-encryption key. Then, the data owner generates the credential token during decryption to control the user's accessibility. The security analysis determines that the protocol resists numerous security attacks.

S. Nagaraju et al. (Nagaraju.S , 2020) developed an effective mutual authentication scheme for reliable cloud service provisioning. The performance is analyzed in terms of computational overhead and communication. An effective mutual authentication approach is described to mitigate the effect of insider threats, secret key leakage, impersonation, Sybil, and other major known attacks. The combination of a User ID and Password (what you know), MAC address (where you are) and OTP (what you have) are used for the user authentication. This approach will perform authentication parameter matching in the identity provider module. The access and authorization tokens generated by the identity provider will be verified in STM for each login session. The proposed approach allows users to use the same login credentials to access multiple cloud services of different cloud service providers. The proposed scheme withstands impersonation, inside threats, secret leakage, Sybil, collusion and other known attacks.

Y. Fan et al. (Fan, Y, 2020) designed a security scheme for the cloud environment of IoT. The credibility of data stored in the cloud can be ensured based on identity verification algorithms and blockchain technology. In contrast, the security of data transmission from the cloud to data consumers is achieved by the following procedure, 1) Build the previous nodes and the cloud under the same private blockchain. Data collected in different environments and transferred to the cloud later will be synchronously stored in the corresponding cloud storage through the chain. 2) The cloud storage, cloud service provider and each module of cloud computing are built under the same private blockchain to ensure the security of the information exchange process inside the cloud and improve efficiency. 3) The cloud service provider and the data consumer (such as individual users, applications and industrial enterprises, governments, etc.) are built under the same union blockchain, which aims to ensure that the data obtained in the previous steps can be safely and reliably delivered to the end users.

S. Gupta et al. (Gupta.S , 2020) developed reinforced security in authentication and offered a unique technique for authentication. They used user-specified cryptographic calculations for securing authentication. This authentication relies on random techniques for data securing. The login and registration sections are designed. Supported by the registration details, the arbitrary arrangement for the login section is generated that's getable to the user once he login inside the length is returned. This Patterns Square measures arbitrarily in that they are not reciprocated three times. A user enters the wrong arrangements greatly, and the login is blocked.

Vanajakshi Devi. K et al. (Vanajakshi Devi, K, 2020) proposed two secure systems, namely SecCloud and SecCloud+. SecCloud offers an auditing entity with an alimentation of a MapReduce cloud, which helps users generate data tags before uploading and auditing the integrity of data reserved in the cloud. This scheme fixes the problem of the earlier task: the computational load at the client or auditor is too bulky for tag generation. For completeness of fine-grained, the auditing functionality designed in SecCoud is sustained on both block and sector levels. SecCoud also facilitates secure deduplication. The "security" examined in SecCoud avoids leakage of side channel information. Inspired by the fact that clients always want to encrypt their data before uploading for reasons varying from personal security to corporate policy, we propose a key server into SecCloud and implement the SecCloud+ schema. Besides aiding integrity auditing and secure deduplication, SecCloud+ assures file confidentiality.

F. Chen et al. (Chen.F, 2022) presented a solution for the dynamic verifiable data access problem. To support data dynamics and verifiability and enhance a hash authentication tree built on a hash table with new semantics. With the enhanced hash authentication tree, the proposed protocol supports adding/deleting data in the outsourced storage while simultaneously satisfying the data access verifiability requirement. This open-source experimental evaluation shows that it only takes less than 0.1 ms to verify data access on a dataset with 400 items using a communication cost of around 1.7 KB.

Problem Definition

Migration of user data from on-premises to off-premises is a vital task. Migration is a huge procedure to be considered when transferring data. Moreover, the security of the data in the VM also needs to be ensured. The data are transferred to the open internet, and many adversarial are ready to huge the data being passed in the network. Unauthorized users may try to capture the data when migrated.

Further, the adversaries can inject fault content in the migrated data and send it to the cloud data centre. The hacker masquerades as the authorized user, captures data from the sender, changes the entire content, and then forwards the faulty data content as it sends by the authorized user. Therefore, the data's authenticity and integrity are being compromised by unauthorized users in the network. When the receiver receives data, they must verify that it arrives from the authentic sender. Data Origin Authentication (DOA) ensures the data arrives from the authentic user. The data integrity also verifies to ensure that any other network intermediate parties do not modify the data.

System Architecture

Cloud migration is the vital process of moving data, applications or other components into a cloud computing environment. The data are migrated with the VM. VM contains various data elements, including metadata about the data and configuration data, and it also contains actual data (customer's and user's data). The VM configuration data can be rebuilt if necessary, but the user's data is tampered with unwanted data during or before the migration starts. Various types of cloud migration are required to migrate into a modern cloud computing environment. Securing the data when migrating into the cloud or third-party location is mandatory. The proposed Cloud Architecture provides security and resilience to migrate the workload into Cloud computing [9]. Figure 1 shows the abstract diagram of the proposed architecture for data migration to the cloud.

The architecture contains different components; among them, the staging area is the proposed component in the research. The staging area represents the transportation of workloads between the on-premises data centre to the cloud data centre. It has segregation between multiple tenants to isolate secure transmission of workloads. The staging area prevents threats and malicious attacks from the cloud data centre. The data in the VMs are migrated to the staging area. The staging area has control and monitors the VM migration. In addition, the staging area fully monitors data authentication and integrity verification. The methodology procedure of the security mechanisms proposed to ensure authentication and integrity is discussed in the following sections.

Methodology

The proposed method ensures the authenticity and integrity of the data migrated from off-premises to on-premises. First, migrating data are verified for their authenticity. Are the data migrated from the right place? It ensures the Data Origin Authentication. The public key cryptosystem is used to verify the DOA. The digital signature method ensures the data is migrated from the right sender. Second, the integrity is verified by using the proposed hashing technique. A hash code is generated during the data migration to ensure the data's integrity. The proposed hash code is a mechanism for digesting the data migrated and generating a hashcode. As per the proposed procedures, the generated hashcode is encrypted using the sender's private key. The receiver retrieves the encrypted hash code and verifies its authenticity by decrypting it with the sender's public key.

Data in the VM is to be authenticated by the receiver. The EAM has a proposed enhanced hashing technique (EHT) to generate the hash code from the data. The proposed EHT generates a 64-bit hash code of the data. The hash code is

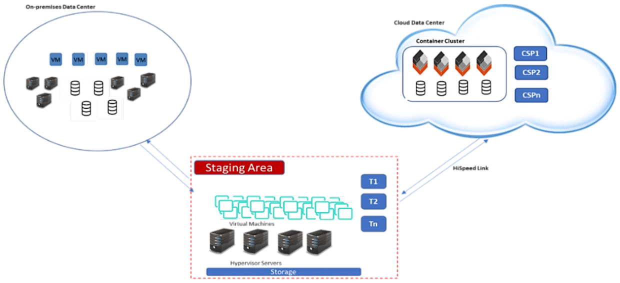

Figure 1: Secure Architecture for VM and Data Migration [17]

encrypted with public key encryption using the sender's private key, and the result is prepended to the plaintext data. The receiver decrypts the sender's public key and recovers the hash code. The encrypted hashcode can only decrypt using the sender's public key. Because the hashcode generated by EHT is encrypted using the sender's public key, called the sender's digital signature. If the receiver can't able decrypt the encrypted hashcode using the sender's public key, then it does not come from the authentic sender. Once the DOA is verified, the data is verified for its integrity. The recipient generates a new hash code for the plaintext data prepended with the encrypted hashcode and matches it to the decrypted hashcode. If the two match, the data is accepted as authentic; otherwise, the integrity of the data is lost, which denotes the data plaintext data is modified during the migration. Figure 2 represents the proposed methodological procedure to ensure the DOA and integrity of the data.

Proposed EHT Procedure

The data in the VM are secured before it migrates from the on-premises. Furthermore, the data are verified for authenticity and integrity after being received by the receiver. Before data migration, the data is secured using a digital signature and proposed EHT methods. The proposed EHT is responsible for verifying the data integrity at the receiver side. The proposed procedure does the generation of hashcode from the plaintext data. The following steps explain the proposed EHT procedure to generate the hash code from the plaintext data.

Steps involved in the generation of Hash code

1. The plain text PT data is considered as input for hash code generation
2. All PTs are converted into corresponding decimals and converted into binary values.
3. Find the size of the total bits.
4. Consider a single bit for 0 or 1 when they have occurred continuously for two times.
5. Divide the total block bits into two blocks
6. Consider 8 bits values of each block and find the XOR of both blocks of each 8 bits

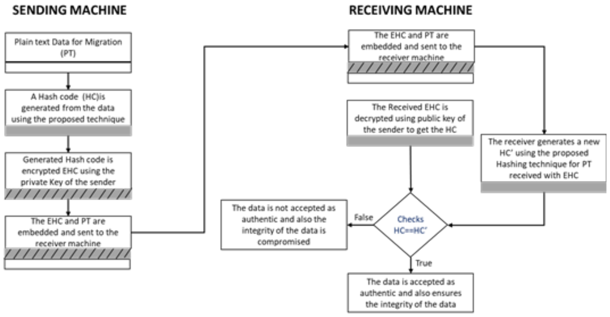
SENDING MACHINE
Plain text Data for Migration (PT)
A Hash code (HC)is generated from the data using the proposed technique
Generated Hash code is encrypted EHC using the private Key of the sender
The EHC and PT are embedded and sent to the receiver machine
RECEIVING MACHINE
The EHC and PT are embedded and sent to the receiver machine
The Received EHC is decrypted using public key of the sender to get the HC
The receiver generates a new HC' using the proposed Hashing technique for PT received with EHC
Checks HC==HC'
False
The data is not accepted as authentic and also the integrity of the data is compromised
True
The data is accepted as authentic and also ensures the integrity of the data

Figure 2: Methodology for Ensuring Authentication and Integrity in Migrated Data

7. Repeat steps 5 and 6 until whole bits come under or equal to 64 bits.
8. The result of 8bits blocks is converted into ASCII character code
9. The final Character code derived from step 8 is a tag for the encrypted data.

The above procedure is explained in pseudo-code as follows,

Pseudo Code of EHT

```
sub eht(PTD)
    1. $PTD \leftarrow Plain\ Text\ Data$
    2. $N \leftarrow sizeof(PTD)$
    3. $PT_D[N] \leftarrow array(PTD)$
    4. $for\ i \leftarrow 1\ to\ N$
        1. $A_{SC}PT_D[i] \leftarrow asciideci(PT_D[i])$
        2. $BinPT_D \leftarrow append(asciibin(AscPT_D[i]))$
    5. $next\ i$
    6. $end\ for$
    7. $NPT_D \leftarrow BinPT_D$
    8. $do$
      1. $j \leftarrow 0$
      2. $for\ i \leftarrow 0\ to\ size(NE_D)$
        1. $j \leftarrow j+1$
        2. $if(NE_D[i]==0 \&\& NE_D[i+1]==0)$
            1. $SE_D[j] \leftarrow 0$
            2. $next\ i+2$
        3. $else\ if(NE_D[i]==1 \&\& NE_D[i+1]==1)$
            1. $SE_D[j] \leftarrow 1$
            2. $next\ i+2$
        4. $else$
            1. $SED[j] \leftarrow NED[i]$
        3. $next\ i$
        4. $end\ for$
        5. $m \leftarrow SE_D/2$
        6. $s \leftarrow 0$
        7. $Blk_1 \leftarrow split(SE_D,\ s,\ s+(m-1))$
        8. $s \leftarrow s+m$
        9. $Blk_2 \leftarrow split(SE_D,\ s,\ s+(m-1))$
      10. $NE_D \leftarrow Blk_1\ Blk_2$
    9. $end\ while(sizeof(NE_D)>64)$
    $Blck \leftarrow sizeof(NE_D)/8$
    $m \leftarrow 1$
    for $i \leftarrow 1$ to $Blck$
        $DecU_D[i] \leftarrow asciideci(split(BinU_D, m, m+7))$
        $AscU_D[i] \leftarrow asciibin(DecU_D[i])$
        $AscBuff \leftarrow append(AscU_D[i])$
        $m \leftarrow m+8$
    next i
    $T_G \leftarrow AscBuff$
end sub
```

The proposed EHT generates the hashcode. It is used to verify the data's integrity after receiving it from the sender to the receiver. From the research methodology, the data is involved in two security checks. First, the data are verified for the DOA by the public key system alone with EAM procedures, and the data is verified for its integrity by the EHT. The following section explains how the proposed procedure is set up in the cloud environment.

Experimental Setup

An Amazon micro server is rented to experiment with the proposed EAM and EHT. In addition, a Software as a service cloud-based application is developed. The cloud application is coded for EAM and EHT. The cloud application is hosted in the cloud server. The local machine is connected to the Amazon server using the Windows operating system's remote procedure call. The sample data in the local Windows machine is considered for migrating to the cloud server per the proposed research. The data is hashed with EHT before migration and encrypted as per the procedure of EAM. The encrypted hashcode is prepended with plaintext data and migrated to the Amazon server. The encrypted hash code is decrypted to ensure the DOA and a new hash code is generated using EHT in the Amazon server. The decrypted hash code and new hash code are verified for data integrity. The proposed EAM and EHT efficiently processed the data for migration, reduced the time, and improved the data's authenticity and integrity. Figure 3 represents the experiment setup designed for the proposed research work.

Results and Discussion

The proposed EAM and EHT has experimented with in the cloud server, and the performance is analyzed based on the computation taken for each proposed procedure. The EHT performance is measured from the computation time for generating the data's hashcode. The EHT is tested with different data sizes, and time is calculated in milliseconds. Figure 4 shows the computation time comparison of EHT with the traditional hashing technique.

The EHT computation time comparison shows that the proposed EHT generates the hashcode for the different data sizes in less computation time than the existing technique. Similarly, the EAM performance is measured by the computation time taken for the authentication verification process. Figure 5 shows the computation time comparison of EAM with the traditional authentication mechanism.

The EAM computation time comparison shows that the proposed EAM verifies the DOA for the different data sizes in less computation time than the existing technique.

The proposed EAM and EHT are designed to secure the data based on authentication and integrity. The proposed Authentication method is based on the public-key cryptosystem. The public-key cryptosystem helps to ensure that the data is sent from the authorized user. The proposed hashing technique differs from existing hashing techniques. The existing hashing techniques generate 32-bit hashcode. The proposed techniques generate 64-bit. In addition, the proposed techniques use XoR to hash the plaintext data. Existing hashing techniques procedure is trackable and easy to disclose the hashcode. The proposed procedure is strong to protect hackers from disclosing the hashcode

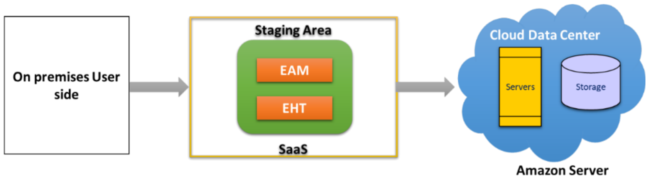

Figure 3: Experimental Setup of EAM and EHT

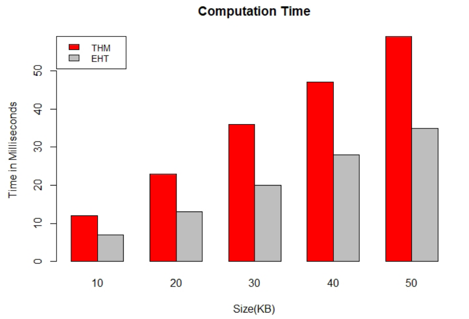

Figure 4: Comparison of EHT Computation Time

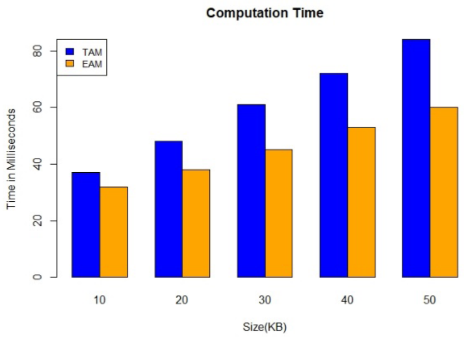

Figure 5: Comparison of EAM Computation Time

generated by the EHT. Hence, the proposed techniques are more suitable to deploy in the cloud environment.

Conclusion

Migration is the most vital process in the cloud. However, cloud data are more vulnerable to attacks during migration. This paper proposed a mechanism for data origin and integrity verification authentication. For both authentication and integrity, different procedures are proposed. Data authentication is verified using the public key cryptosystem, and the proposed hashing technique verifies integrity. There is an architecture for secured migration. In the architecture, the staging area is responsible for the secured migration of the data. The architecture is helpful for the smooth and steady migration securely in a monolithic and microservice architecture. Cloud service providers and end users have a cost-effective architecture for application modernization. The proposed hashing method is used to generate the hash code. The receiving machine in the transmission verifies the data origin authentication. The proposed mechanism efficiently verifies the data authentication on the receiving side. The proposed EAM and EHM are evaluated in the cloud environment. Results show the proposed methods produce better results concerning the computation time.

References

Arockiam, L., Monikandan, S., & Parthasarathy, G. (2017). Cloud computing: a survey. *Journal of Computer and Communication Technology*, 8(1), 21-28, https://doi.org/10.47893/IJCCT.2017.1393

Alouffi, B., Hasnain, M., Alharbi, A., Alosaimi, W., Alyami H. and Ayaz, M. (2021). A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies. *IEEE Access*, 9, 57792-57807, https://doi.org/10.1109/ACCESS.2021.3073203.

Chen, F., Li, Z., Jiang, C., and Li, J. (2022). Verifiable Cloud Data Access: Design, Analysis, and Implementation. *IEEE Systems Journal*, 16(1), 1135-1146, https://doi.org/10.1109/JSYST.2020.3034105.

Ghaffar, Z., Ahmed, S., Mahmood, K., Islam, S. H., Hassan, M. M., and Fortino, G. (2020). An Improved Authentication Scheme for Remote Data Access and Sharing Over Cloud Storage in Cyber-Physical-Social-Systems. *IEEE Access*, 8, 47144-47160, https://doi.org/10.1109/ACCESS.2020.2977264

Gupta, S., Singh, D. P., and Sharma, P. (2020). A Novel Approach for User Specified Cryptographic Calculation for Securing Authentication. *International Conference on Data, Engineering and Applications (IDEA)*, Bhopal, India, 1-5, https://doi.org/10.1109/IDEA49133.2020.9170687.

Manikandasaran, S. S., and Raja S. (2018). Security architecture for multi-tenant cloud migration. *International Journal Future Computer Communication,* 7(2), 42-45. https://doi.org/10.31224/osf.io/5c6es

Manikandasaran, S. S., and Raja, S. (2018). Secure architecture for virtual machine to container migration in cloud computing. *Journal of Physics: Conference Series*, 1142, 1, 1-8. http://dx.doi.org/10.1088/1742-6596/1142/1/012017

Monikandan, S., and Arockiam, L. (2015). Confidentiality Technique to Enhance Security of Data in Public Cloud Storage Using Data Obfuscation. *Indian Journal of Science and Technology,* 8(24), 1-10, https://doi.org/10.17485/ijst/2015/v8i24/80032.

Nagaraju, S. , Jayakumar, S. K. V., and Priya, C. S. (2021). An Effective Mutual Authentication Scheme for Provisioning Reliable Cloud Computing Services. *International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)*, Greater Noida, India, 314-321, https://doi.org/10.1109/ICCCIS51004.2021.9397113.

Pachaghare, S. and Patil, P. (2020). Improving Authentication and Data Sharing Capabilities of Cloud using a Fusion of Kerberos and TTL-based Group Sharing. *International Conference on Communication and Electronics Systems (ICCES)*, Coimbatore, India, 1401-1405, https://doi.org/10.1109/ICCES48766.2020.9137934

Patil D. and Mahajan, N. (2021). An Analytical Survey for Improving Authentication levels in Cloud Computing. *International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*, Greater Noida, India, 6-8, https://doi.org/10.1109/ICACITE51222.2021.9404644.

Saleh Atiewi, Amer Al-Rahayfeh, Muder Almiani, Salman Yussof, Omar Alfandi, Ahed Abugabah, Yaser Jararweh, (2020). Scalable and Secure Big Data IoT System Based on Multifactor Authentication and Lightweight Cryptography. *IEEE Access*, 8, 113498-113511, https://doi.org/10.1109/ACCESS.2020.3002815.

Subasini, C. A. and Nikkath Bushra, S. (2021). Securing of Cloud Data with Duplex Data Encryption Algorithm. *International Conference on Computing Methodologies and Communication (ICCMC)*, Erode, India, 252-256, https://doi.org/10.1109/ICCMC51019.2021.9418247.

Vanajakshi Devi, K., Shrenika, S., Jyothi, N. (2016). A Study on Data Integrity and Storage Efficiency Services in Cloud. *International Journal of Engineering Research*, 5(4), 340-346, https://doi.org/10.17950/ijer/v5s4/427.

Xiaoyu W and Zhengming G. (2020). Research and Development of Data Security Multidimensional Protection System in Cloud Computing Environment. *International Conference on Advance in Ambient Computing and Intelligence (ICAACI)*, Ottawa, Canada, 67-70, https://doi.org/10.1109/ICAACI50733.2020.00019.

Y. Fan, Y., Zhao, G., Shang, W., Shang, J., Lin W., and Wang, Z. (2020). A Preliminary Design for Authenticity of IoT Big Data in Cloud Computing. *International Conference on Computer Communications and Networks (ICCCN)*, Honolulu, HI, USA, 1-2, https://doi.org/10.1109/ICCCN49398.2020.9209646.