IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Ingénierie des Systèmes d'Information
Vol. 25, No. 4, August, 2020, pp. 515-519
Journal homepage: http://iieta.org/journals/isi

Secure Data Uploading and Accessing Sensitive Data Using Time Level Locked Encryption to Provide an Efficient Cloud Framework

Vejendla Lakshman Narayana*, Arepalli Peda Gopi, Paturi Radhika, Kanumalli Satya Sandeep

Vignan's Nirula Institute of Technology & Science for Women, PedaPalakaluru, Guntur 522009, Andhra Pradesh, India

Corresponding Author Email: lakshmanv58@vignannirula.org

https://doi.org/10.18280/isi.250415

Received: 9 March 2020
Accepted: 26 May 2020

Keywords:
cloud computing, data security, data uploading, data accessing, data encryption, cloud user, cloud service provider

ABSTRACT

Executing cloud computing participate from multiple points of view for Web-based overseeing commitments to mark various issues. Here the assurance and data security has considered into a significant issue with downside that limits numerous applications that identified with cloud. These days cloud computing has been generally perceived as one of the most compelling data advances in view of its phenomenal focal points. Regardless of its generally perceived social and monetary advantages, in cloud computing clients lose the immediate control of their information and totally depend on the cloud to deal with their information and calculation, which raises huge security and protection concerns and is one of the significant obstructions to the appropriation of open cloud by numerous associations and people. In the proposed work a Time Level Locked Encryption (TLLE) framework is designed for deduplication of huge documents to accomplish space-proficient capacity in cloud and also to monitor data uploading and data access. The proposed model is compared with the traditional AES encryption model and the results show that the proposed model is exhibiting better performance.

1. INTRODUCTION

The popularity and no matter how you look at its usage of large information have brought remarkable convenience for data sharing and uploading in cloud. Cloud computing has been imagined as the cutting edge figuring model that originates from matrix processing, disseminated registering, equal processing, virtualization innovation, utility figuring and other PC advances [1]. This mix of registering models furnish cloud computing with more preferences, for example, huge scope calculation and information storage, virtualization, high expansibility, high unwavering quality and low value administration [2]. The cloud computing model is primarily founded on the system and has the arrangement of administration for the users [3]. These administrations can appear as application, programming, and framework and it very well may be considered to by clients from anyplace and whenever. Furthermore, these administrations can be shared among countless clients. For instance, the cloud storage can be shared by various clients and every client can increment or decline his assets of capacity dependent on his needs [4]. It offers an extent of organizations for end customers; The mainstream benefits that offered in the Cloud are:

• SaaS: Software as a Service, it is a procedure for turning in programming that offers remote get passage to the product as an electronic absolutely administration [5]. The product program supplier can be purchased with a month to month cost and pay as you cross.

• PaaS: Platform as a Service is making utilized for applications, and other improvement, while allowing cloud parts to programming. Stage as a Service makes the improvement, arrangement, and testing of uses better [6].

• IaaS: Infrastructure as a Service is a self-administration strategy for checking, and take care of remote district server group, as an example, a PC, organizing administrations, and capacity [7]. As opposed to purchasing equipment framework, clients can buy IaaS reliant on utilization, similar to control or diverse programming charging. Different Cloud services are depicted in Figure 1.

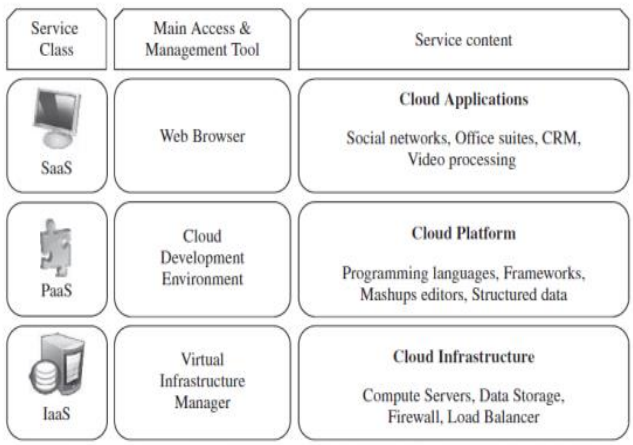

Figure 1. Cloud services

With evolving advances, there is an expansion deprived for better techniques with minimal effort and constrained weight for endeavors during reclamation of lost information from reinforcement duplicates [8]. With progressions in applications and nearness of various gadgets, there is an inclination for improvement in Backup and DR plans with

better information trustworthiness, capacity of taking care of multitudinous gadgets all the while and ability to recoup information efficiently [9]. Nonattendance of a reinforcement activity planned to happen in a venture may have an incredible money related effect on the endeavor because of cost of reproducing lost information, lawful activities that might be confronted, lower profitability which may gradually prompt the breakdown of business [10].

The progression in systems administration innovations and ever-developing requirement for registering assets have advanced a crucial change in outlook in how individuals convey and figuring administrations: processing redistributing [11]. This new registering model, ordinarily alluded to as Cloud Computing, is a help model that offers clients on-request arrange access to a huge shared pool of processing assets, which is given by a Cloud Service Provider (CSP) [12]. Cloud computing comprises of different sorts of administrations. The primary sort is Infrastructure as a Service (IaaS), where a client utilizes the CSP's figuring, storage or systems administration foundation [13].

On one hand, aside from the encoded information, the cloud needs to store the keywords and henceforth cost extra space. Then again, the keywords joined to the encoded information may spill data about the relating scrambled information and annihilate the information security [14]. In this manner, the keywords ought to be encoded to ensure their security. Another protection issue is the strong security [15]. That is the point at which the client looks through the information in the cloud, the question ought not release any data to the cloud or other untrusted parties either. In addition, the reaction to an inquiry ought not have a long postponement, i.e., the calculation overhead of the server while coordinating scrambled information for the question ought to be low in any case that the CSP can't give great assistance which can decrease its fascination in the clients [16]. This requires the requirement for creating productive and secure looking through strategies over scrambled cloud information [17].

2. LITERATURE REVIEW

One of the fundamental reasons that make the two people and organizations use cloud storage supplier is to consistently have a reinforcement of their significant information [18]. This reinforcement will consistently make the information accessible whenever with the goal that the clients can without much of a stretch access it in whatever time and spot they need [19].

Subramanian and Jeyaraj [1] proposed a path for guaranteeing information security in transmission. All the information to be transmitted will be scrambled with homomorphic encryption, in this manner improving the security of information, regardless of whether the information is taken, there is no comparing key can't be reestablished. As it were, the client is the main individual who knows the key, while the mists don't have the foggiest idea about the key.

Mell et al. [2] proposes a solid client confirmation structure that gives personality the executives, shared validation, meeting key foundation between the clients and the cloud supplier. The proposed scheme guarantees that genuine client demonstrates his/her credibility before going into the cloud by utilizing two-advance confirmation to check the client realness. Additionally, the proposed model utilizes two separate communication channels to make it hard for the users to assault in two unique channels simultaneously.

Deka et al. [4] proposed the primary useful methodology for symmetric accessible encryption. In this methodology, each word in the record is scrambled with a unique two layered encryption calculation. Later on, clients can look through this scrambled information with specific keywords.

Roman et al. [5] attempt to conquer the inadequacies introduced by considering the versatile enemies which could create inquiries relying upon the results of past questions. A versatile security definition for accessible encryption conspires by utilizing "record" approach is considered. This approach assembles a key exhibit and a look-into table to get the whole record assortment.

3. PROPOSED METHOD

Data uploading and Data access in cloud is picking up consideration as being basic security instruments for information assurance in cloud applications by just permitting approved clients approach substantial information. Since huge measure of data put away in the cloud is delicate, care ought to be taken for getting control of this sensitive data [20]. Tragically, conventional information access control approaches used to take care of this issue accept that information is stored in a confided in information server for all clients and the CSP is accountable for authorizing the entrance strategy [21]. In any case, this supposition can't hold in cloud computing since this methodology gives CSP approaches the plain information. Furthermore, the information gets traded off once the CSP gets compromised.

The principal preliminaries to ensure delicate information partook in the cloud is to encode the information (utilizing either symmetric-key, otherwise called private-key encryption (PKE), or asymmetric key) before transferring it to the cloud storage, while the unscrambling keys are unveiled distinctly to approved clients. Be that as it may, this inconsequential arrangement prevailing to start with later on it acquires various issues. The main issue related with arrangement is that it requires an effective key administration instrument to convey unscrambling keys to approved clients, which has been demonstrated to be exceptionally troublesome. Additionally, with the wide spread of cloud computing, more clients joined the cloud which make embracing the past arrangement wasteful as it needs versatility and adaptability. Moreover, when an information owner needs to disavow an information client, all information identified with this client must be re-encoded and new keys must be circulated to the rest of the information clients. To wrap things up, information owners should be online constantly in order to scramble or re-encode information and convey keys to approve clients.

The exceptional component of this system arrangement is that it uses abnormal strategy of encryption and decoding relying upon creating a key method. The structure arrangement gives administrations to stop assaults. The purpose of the technique is finished in giving an intricate security instrument that licenses keeping up of information safely in various cloud stages to affirm the customer for any radical exercises. The targets of the procedure are according to the accompanying: The validation process is depicted in Figure 2.

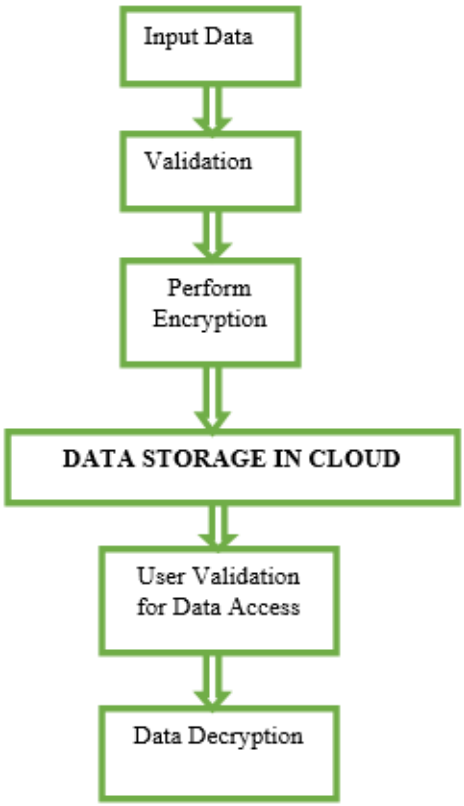

Figure 2. Process of data storage and accessing data in cloud

In the process of data storage and accessing in cloud, initially the data is given as input that needs to be stored in the cloud. The data owner who needs to store the data in the cloud has to be validated and then the data is encrypted and stored in the cloud.

If any cloud user needs to access the data, then request has to be submitted to the CSP. The CSP validates the user and then access control is given to the cloud user. Finally the data is decrypted by the CSP and then shared to the cloud user.

Arrangement. C runs Setup (1') to create the open boundaries params and runs KeyGen (1') to produce the mystery open key pair (SK, PK).

It at that point sends the open boundaries params with the open key PK to A.

Stage 1. A can adaptively question the decoding model. A presents a ciphertext CT to CN, where CT = Enc (param, PK, M). CN runs Dec (params, SK, CT) and reacts A with K. This inquiry can be made on different occasions. Challenger. A submits two messages M1 and M2 with equivalent length. C arbitrarily chooses L and figures CT∗ = Enc (params, PK, L), where b ∈ {0, 1}. C reacts A with CT∗.

Stage 2. A can adaptively question the decoding model. A presents a ciphertext CT to CN, where the main limit is CT = CT∗. Stage 1 is rehashed again. This inquiry can be made on different occasions. A yields his speculation b 0 on b. A dominates the match if b 0 = b.

In the proposed Time Level Locked Encryption (TLLE) model, there is a position that is liable for quality administration and key appropriation. The authority can be the enrollment office in a college, the human asset division in an organization, and so on. The information owner characterizes the entrance strategies and scrambles information under the approaches.

Every client will be given a secret key as per its characteristics. A client can decode the ciphertext just when its traits fulfill the entrance strategies. Additionally, in TLLE Model, the keys are valid only for a particular time interval and then they are not used for performing encryption or decryption. The CSP will check the timestamp of the available keys and then recomputes the keys whenever necessary. The user validation strategy checking is verifiably directed inside the cryptography. Therefore, the focal authority would be a defenseless point for security assaults and a presentation for huge scope frameworks. To conquer this issue, proposed model uses a multi-authority property based access control plans without a focal authority introduced secure multi-authority TLLE model uses that expel the focal authority by utilizing an appropriated pseudo-irregular capacity. Be that as it may, it has a similar impediment of characterizing a pre-decided number of experts in the framework instatement. Also, they can endure conspiracy assaults for up to N-2 specialists' trade off. The process for storing and accessing data is depicted in the algorithm

Cloud Data TLLE Algorithm

Step-1: Start the Cloud User Registration.
Step-2: Connect the users with the database.
Step-3: Perform User Validation for the users who have registered.
Step-4: CSP uses a centrl authority for Key generation and key distribution.
Step-5: For everu key generated, CSP allot a Timestamp for the key for reducing attacks.
Step-6: If(clouduser(CU)==Validate(CU,CSPID,TS))
Step-7: Allow Data Owners (DO) to upload or access cloud resources or data.
Step-8: Foreach CUs with PubK and PriK
{
If $CU_{(A,B)}.DO == CSP(ID)\varepsilon M$
$PriK'_{(DO)}=f(CU_{(ID)} \oplus PubK)$
If $PriK_{(CU)}.DO == CSP(PriK(cu))$
Then
$Cloud\ memory \leftarrow$ DO(data)
}
Step-9: CSP removes the keys used for validation and accessing cloud resources.
Step-10: Central authority monitors the cloud users and their operations on cloud.
Step-11: Data and access permissions are given to authenticated cloud users.

KeyGen ('). Taking as information the security boundary ', it yields people in general/private key pair of the collector as (pkR, skR). PEKS (pkR, kw). Taking as info the open key pkR and the catchphrase kw, it yields the PEKS ciphertext of kw as CTkw. Trapdoor (skR, kw0). Taking as info the mystery key skR and the watchword kw0, it yields the trapdoor of kw as Tkw0. Test (pkR, CTkw, Tkw0). Taking as info the open key pkR, the PEKS ciphertext CTkw and the trapdoor Tkw0, it yields T mourn if kw = kw0, in any case yield False. The keys used for encryption or decrption is generated as

PubK(CU)→ CU(ID)+TS (TS=Time stamp)

Consider 3 numbers x,y and z randomly such that x>y<z AND x!=z

Foreach i in (range(x+z-y))

PriK(CU) = TS XOR CU(ID)

ID++

PubK(CU)→CSP(ID)
CSP → PubK(CU) XOR PriK(CU(ID))

Keypair KP ← {PubK,PriK}

The proposed arrangement attempts to forestall the data secured storage if there should arise an occurrence of agreement between a client and the Cloud Service Provider by utilizing information circulation procedure. Dissimilar to the proposed c model that experiences issues in the re-approval of repudiated clients, who rejoin the framework however with various access benefits, and connection between a client and the Cloud Service Provider. The proposed model attempts to offer one arrangement that understands the accompanying issues:

1) accomplish fine-grained information sharing and access authority over information in the cloud;
2) forestall the removal of unapproved information when a repudiated client rejoins the framework;
3) forestall relation between a client and the Cloud Service Provider.

4. RESULTS

The Proposed model is implemented in java that establishes a cloud environment which allows cloud users to register with the cloud service provider and get relevant permissions for uploading data into cloud and also to get access to use data from the cloud. The proposed model is compared with the traditional AES based cloud encryption model and the results depicts that the proposed model is better in performance. The proposed model data transmission rate is high that is depicted in Figure 3.

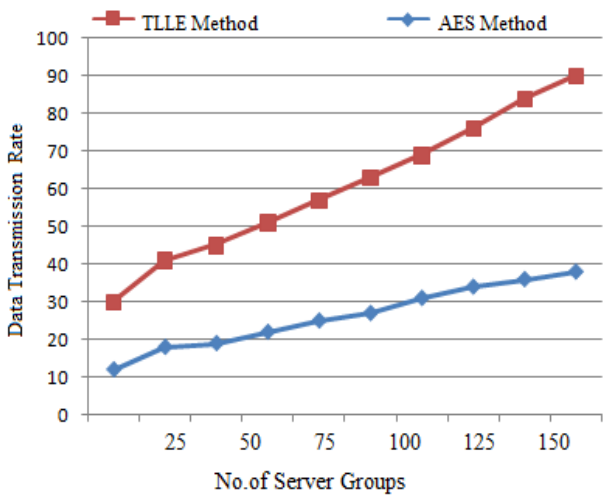

Figure 3. Transmission rate compared between AES and TLLE

The transmission range of the data in the proposed model is compared with the traditional model and the results show that the transmission rate of the proposed model is high when compared to the traditional AES model.

Above result is the output of the TLLE methodology and compared with the AES algorithm in calculating encryption time (Figure 4). The encryption time is reduced when compared it with the AES algorithm.

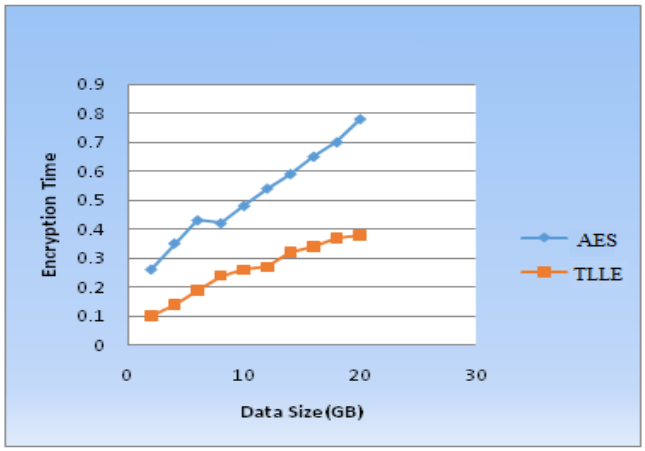

Figure 4. Encryption time levels

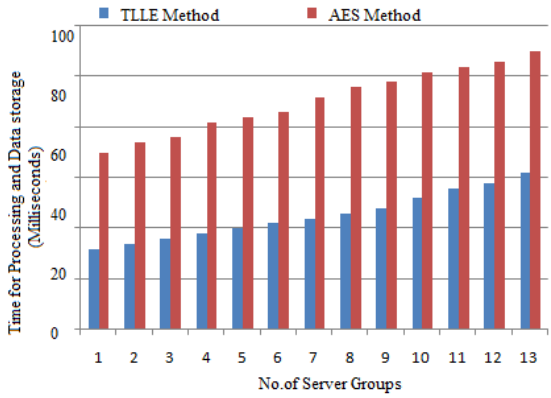

Figure 5. Data storage time levels

The proposed TLLE model takes less time to process the data of the data owner and store it in the cloud. The comparison levels are depicted in Figure 5. The storage overhead levels of the proposed method is very less than the traditional AES method. The overhead levels are depicted in Figure 6.

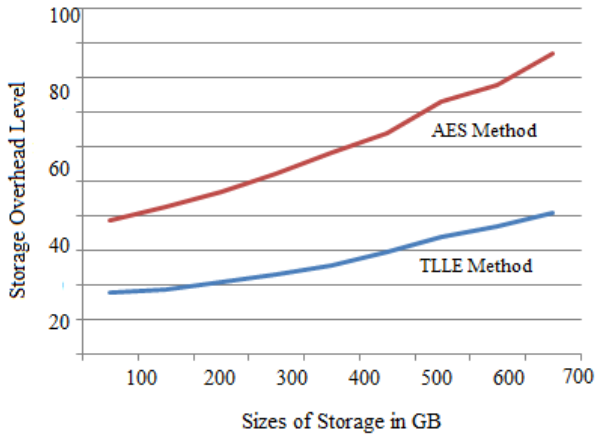

Figure 6. Clous overhead levels

5. CONCLUSION

Cloud storage administrations give a financially better results for managing the issue of on request information access or for data sharing to cloud. These administrations empower

their supporters of offer, team up, document and synchronize information across various gadgets and space, without the worries of information provisioning and accessibility. Cloud framework related with these administrations is claimed, overseen and worked by an un-believed substance called CSP. Since, CSP is responsible for preparing, enduring and provisioning of re-appropriated information there is a lot of protection concerns when classified information is recloud to such administrations. To guarantee information protection and classification frequently cryptographic strategies are utilized be that as it may, these philosophies are insufficient to accomplish fine-grained get to control. Access control arrangements guarantee fine-grained get to control. Be that as it may, traditional approaches were intended to limit unlawful information access in a confided in space in which just client getting to information could carry on malignantly. As opposed to that, cloud storage administrations were provisioned from open area by an untrusted element.

REFERENCE

[1] Subramanian, N., Jeyaraj, A. (2018). Recent security challenges in cloud computing. Computers & Electrical Engineering, 71: 28-42. https://doi.org/10.1016/j.compeleceng.2018.06.006

[2] Mell, P., Grance, T. (2018). SP 800-145, The NIST Definition of cloud computing. CSRC (online) Csrc.nist.gov. https://csrc.nist.gov/publications/detail/sp/800-145/final, accessed on Dec. 11, 2018.

[3] Shi, B., Cui, L., Li, B., Liu, X., Hao, Z., Shen, H. (2018). Shadow monitor: An effective in-VM monitoring framework with hardware-enforced isolation. International Symposium on Research in Attacks, Intrusions, and Defenses. Springer, Berlin, pp. 670-690.

[4] Deka, G.C., Das, P.K. (2018). Application of virtualization technology in IaaS cloud deployment model. Design and Use of Virtualization Technology in Cloud Computing: IGI Global, 29-99. https://doi.org/10.4018/978-1-5225-2785-5.ch002

[5] Roman, R., Lopez, J., Mambo, M. (2018). Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges. Future Generation Computer Systems, 78(Part 2): 680-698. https://doi.org/10.1016/j.future.2016.11.009

[6] Csrc.nist.gov (2018). SP 500-299 (DRAFT), NIST Cloud Computing Security Reference Architecture. CSRC (online). https://csrc.nist.gov/publications/detail/sp/500-299/draft, accessed on Sept. 11, 2018.

[7] Kumar, P.R., Raj, P.H., Jelciana, P. (2018). Exploring data security issues and solutions in cloud computing. Procedia Computer Science, 125: 691-697. https://doi.org/10.1016/j.procs.2017.12.089

[8] Ahmed, M., Litchfield, A.T. (2018). Taxonomy for identification of security issues in cloud computing environments. Journal of Computer Information Systems, 58(1): 79-88. https://doi.org/10.1080/08874417.2016.1192520

[9] Zhang, Y., Chen, X., Li, J., Wong, D.S., Li, H., You, I. (2017). Ensuring attribute privacy protection and fast decryption for outsourced data security in mobile cloud computing. Information Sciences, 379: 42-61. https://doi.org/10.1016/j.ins.2016.04.015

[10] Anusha, P., Ravikiran,V.A., Narayana, L. (2020). Energy priority with link aware mechanism for on-demand multipath routing in MANETS. International Journal of Advanced Science and Technology, 29(3): 8979-8991.

[11] Maddumala, V.R. Lakshmi, K.M., Anusha, P., Narayana, V.L. (2020). Enhanced morphological operations for improving the pixel intensity level. International Journal of Advanced Science and Technology, 29(3): 9191-9201.

[12] Rao, B.T., Narayana, V.L. (2020). Use of blockchain in malicious activity detection for improving security. International Journal of Advanced Science and Technology, 29(3): 9135-9146.

[13] Bharathi, C.R., Narayana, V.L. (2020). Unlimited bandwidth for RF applications using design and examination of CMOS LNA. International Journal of Advanced Science and Technology, 29(3): 9056-9062.

[14] Naresh, V., Narayana, L. (2020). Energy consumption reduction in cloud environment by balancing cloud user load. Journal of Critical Reviews, 7(7): 1003-1010. https://doi.org/10.31838/jcr.07.07.184

[15] Sarada, K., Narayana, V.L. (2020). Improving relevant text extraction accuracy using clustering methods. TEST Engineering and Management, 83: 15212-15219.

[16] Sarada, K., Narayana, V.L. (2020). An iterative group based anomaly detection method for secure data communication in networks. Journal of Critical Reviews, 7(6): 208-212. https://doi.org/10.31838/jcr.07.06.39.

[17] Mounika, B., Anusha, P., Narayana, V.L. (2020). Use of BlockChain Technology in providing security during data sharing. Journal of Critical Reviews, 7(6): 338-343. https://doi.org/10.31838/jcr.07.06.59

[18] Narayana, V.L., Sudheer, B.N. (2020). Fuzzy base artificial neural network model for text extraction from images. Journal of Critical Reviews, 7(6): 350-354. https://doi.org/10.31838/jcr.07.06.61

[19] Narayana, V.L., Gopi, A.P. (2020). Accurate identification and detection of outliers in networks using group random forest methodoly. Journal of Critical Reviews, 7(6): 381-384. https://doi.org/10.31838/jcr.07.06.67

[20] Pasala, S., Pavani, V., Lakshmi, G.V., Narayana, V.L. (2020). Identification of attackers using blockchain transactions using cryptography methods. Journal of Critical Reviews, 7(6): 368-375. https://doi.org/10.31838/jcr.07.06.65

[21] Bharathi, C.R., Narayana, V.L., Ramesh, L.V. (2020). Secure data communication using internet of things. International Journal of Scientific & Technology Research, 9(4): 3516-3520.