Computer Systems Science & Engineering
DOI: 10.32604/csse.2023.029899
Article

Tech Science Press

Implementation of ID-based Audit Protocols to Enhance Security and Productivity

R. Hariharan[1,*], G. Komarasamy[2] and S. Daniel Madan Raja[3]

[1]Sri Ramakrishna Institute of Technology, Coimbatore, 641010, Tamilnadu, India
[2]VIT Bhopal University, Bhopal-Indore Highway Kothrikalan, Sehore, 466114, Madhya Pradesh, India
[3]Bannari Amman Institute of Technology, Sathya Mangalam, Erode, 638401, Tamilnadu, India
*Corresponding Author: R. Hariharan. Email: hariharanrcse@gmail.com
Received: 14 March 2022; Accepted: 24 June 2022

Abstract: Cloud storage has gained increasing popularity, as it helps cloud users arbitrarily store and access the related outsourced data. Numerous public audit buildings have been presented to ensure data transparency. However, modern developments have mostly been constructed on the public key infrastructure. To achieve data integrity, the auditor must first authenticate the legality of the public key certificate, which adds to an immense workload for the auditor, in order to ensure that data integrity is accomplished. The data facilities anticipate that the storage data quality should be regularly tracked to minimize disruption to the saved data in order to maintain the intactness of the stored data on the remote server. One of the main problems for individuals, though, is how to detect data integrity on a term where people have a backup of local files. Meanwhile, a system is often unlikely for a source-limited person to perform a data integrity inspection if the overall data file is retrieved. In this work, a stable and effective ID-based auditing setting that uses machine learning techniques is proposed to improve productivity and enhance the protection of ID-based audit protocols. The study tackles the issue of confidentiality and reliability in the public audit framework focused on identity. The idea has already been proved safe; its safety is very relevant to the traditional presumption of the Computational Diffie–Hellman security assumption.

Keywords: Machine learning; information processing; Bayes methods; cloud systems

1 Introduction

Users Customers are able to access their data anytime they require it because it is kept in the cloud, and there is no downtime associated in the process [1]. Customers have the ability to save their data in the cloud thanks to the cloud service, which offers a number of important advantages over traditional methods, such as automatically updating their expensive gear and software. Customers can retain their data in the cloud at no additional cost. However, after you migrate your data to the cloud, you will no longer have direct access to your data because it will no longer be preserved on your local machine. This means that you will no longer be

able to retrieve your data in a physical format. This means that you will no longer have any access to your data, regardless of how it was stored. Because of this, it is difficult to guarantee the integrity of the data that is stored in the cloud owing to unanticipated hardware and software failures as well as human errors [2,3].

Scanning biometric data such as fingerprints and irises is one example of how a private key can be put to use in a real-world scenario. This is one of the ways that private keys can be used. Because of the fact that a person biometric information is exclusive to them, it is possible to establish a connection between a person identity and their private key by using this information. Unfortunately, biometric data are measured at any moment with inherent noise, and they cannot be successfully replicated because changes in biometric data can be induced by a range of different causes. This makes it impossible to reliably duplicate biometric data. Biometric information cannot, therefore, be utilized directly as a private key for authentication in auditing data integrity [4].

In order to limit unauthorized access to network resources and data, data authentication in every cloud virtual node is necessary. Even for a cloud system, authentication is necessary to send the data securely without unauthorized access to data [5]. When it comes to establishing the authentication procedure, the cloud poses a number of significant obstacles as a result of its restricted resources, memory, energy, and communication/processing capabilities. When it comes to setting up the authentication procedure, the cloud, despite its numerous advantages, poses a major set of problems that must be overcome. A lightweight authentication system that does not influence network capacities is important to alleviate these concerns.

The major purpose of the technique provided is to enhance cloud authentication with low power usage. The following changes are contemplated across the network to attain such an objective: The critical details are updated with an ECC (Elliptic Curve Cryptography) algorithm with XNOR capabilities during the job planning process. This study applies a principle of insecurity to select additional communication with hostile nodes in the game model [6].

The contribution of the entire work involves the following: The authors develop an authentic identity audit model using homomorphic signatures in an ID-based environment [7,8]. The study reduces the workload in the server using the identity audit model and it uses key management procedures. This model provides optimal security in the cloud model and that results in reduced workload problems.

2 Related Works

The concept of proven data possession is initially articulated by Ateniese et al. The sampling technique randomly and homomorphic linear authenticators have been used to develop a proven data possession scheme that allows an auditor to check the completeness of cloud data without downloading all cloud data [9].

The idea of proof of retrievability (PoR) introduced by Juels and Kaliski the suggested solution employs error correction and spot control methods to ensure that the data saved in the cloud can be retrieved and utilized [10].

Shacham and Waters have built two Proofs of Reputation (PoR) that can be controlled privately yet validated publically by utilizing pseudorandom and BLS (Boneh-Lynn-Shacham) signatures. The acronym for these PoR is BLS (Boneh-Lynn-Shacham). Zhu et al. developed a mechanism for ensuring the truthfulness of data that is predicated on index hash tables. This method is intended to facilitate the updating, inserting, and deleting of data by users [11].

In the course of their investigation into the validity of the data, Sookhak et al. colleagues looked into data dynamics as another potential problem. As a consequence of their investigation, they came up with an approach to auditing that is suitable for use with divide-and-conquer tables. The TPA is able to infer information provided by users during audits of the integrity of the public data by repeatedly examining

the same data blocks to validate their authenticity. This allows the TPA to infer information provided by users [12,13].

To preserve the privacy of data, Wang et al. have used a random masking approach to build the first system for the audit of public data integrity to protect privacy. Yu et al. suggested an audit scheme for cloud storage that preserved absolute privacy by taking no evidence of it [14,15].

3 Preliminaries

The ECC signature encryption algorithm contains 11 parameters that cannot be implemented directly. Choosing settings for authentication purposes is a vital task for efficient and secure functioning. The following is the background of the selected parameters:

a) Consider p, the odd prime number, with the ECC drawn by its elliptical curve on GF(p).
b) Take b, an entire with more than p i.e., $2^{(b-1)}$. The public keys have bits and $2b$ bits of signature. Here, b is regarded as several bytes (8). Therefore, the length of the signature and the public key are byte values.
c) Consider the finite Galois field GF(p) element encoding field with $b-1$ bits.
d) The necessary cryptographic hash function H needs to be utilized in order to offer an output length of 2 bits. This choice is superior than the others since it minimizes the damage caused by collisions and contributes to the preservation of available resources.
e) When multiplying the scalar ECC by 2^c, instead of using the standard multiplier, consider the integer c to be a $\log_2$ cofactor.
f) Consider the integer n, where. The ECC scalars are a secret with an bit that sets the top or $2n$ bit and releases the bottom and the c bit.
g) The use of a secret $n+1$-bit, when $c \leq n <$ b; ECC scalar is required in order to activate the top bit, which is also referred to as the 2n-bit, and releases the bottom bit, which is also referred to as the c-bit.
h) Take into consideration the infinite non-square Galois field element, which is denoted by GF(p).d.
i) Here, the accounts are taken into account to achieve suitable performance.

$$a = \begin{cases} -1 & p \bmod 4 = 1 \\ 1 & p \bmod 4 = 3 \end{cases}$$

j) Consider B to be an element that is part of the set $B! = (0,\ 1)$.

$$E = \left\{GF^2(x,\ y)\right\}$$

were, $ax^2 + y^2 = 1 + dx^2 + y^2$

k) Consider$L$, an odd primary $L[B] = 0$ or number between 0 and 2c, or $2^c \times L = \#E$.
l) Calculation of total points in the elliptical curve by means of standard data ($\#E$).
m) Take into account PH, prehash, or PH(M) = M with identity M. This contributes to decreasing the main output length even when the message size is high, i.e., PH(M) = SHA−512(M).
n) The elliptical curve is used to generate a group of points, where the XNOR operator assists bitwise to form the group, i.e., (X3, Y3) = XNOR ((X1, Y1), (X2, Y2)). The calculation formula is shown below:

$$y_3 = XOR((y_1y_2 - ax_1x_2),\ (1 - dx_1x_2y_1y_2))$$

$$x_3 = XOR((x_1y_2,\ x_2y_1),\ (1 + dx_1x_2y_1y_2))$$

It contains no exception for the supplied set of inputs with non-zero denominators. This objective is to decrease the reverse operation modulo p, which is regarded as a costly operation. In this regard, during the inversion procedure, we have exploited XNOR capabilities.

4 Proposed Method

This section explains the architecture proposed for the authentication of network nodes Fig. 1.

The three models proposed are structured in three ways:

a. Use the Machine Learning based XNOR functionality built into the algorithm to update crucial information during task scheduling.
b. Finally, when selecting the game model, it is possible to discover whether the nodes are acting maliciously or not.

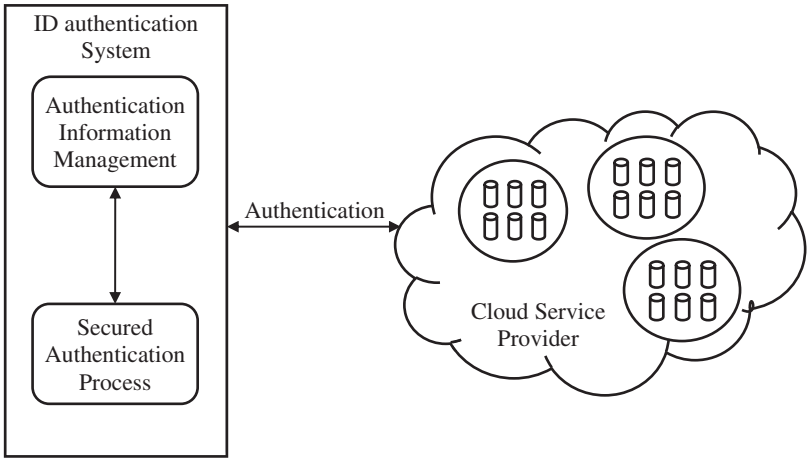

Figure 1: Proposed authentication model in distributed cloud

4.1 Verification of Nodes

In terms of security, sharing the resource among the nodes is essential. In such instances, it could be more motivating to involve more nodes in the network and to avoid malevolent nodes. This helps to avoid the overall network costs, and this may be done using the concept of game theory.

Consider two neighbors, n1 and n2, in the network. Node n1 selects two policies: the reward or the penalty and the communication request with the node n2; and node n1 contains two actions: accept and reject. The acts occur only when the n1 node is an odd node, otherwise, the actions will occur. Based on the checked signature, the odd node is selected, if successful, as an odd node. Choose the surly or wimpy node just during the node connection time or when the central server transmits a message.

Each node contains the relevant information, but not other node information. The paradigm is therefore based on insecurity or incompleteness between nodes.

The basic node n determines n1 on the basis of probability q and n1 on the basis of 1-q. n1 then requests either an award or a penalty for the selected message by properly selecting the strategies. However, if node n1 is wimpy, these solutions are regarded as unsuitable. However, if n2 accepts a message request based on an odd node, or reward, the message is probably sent q after proper authentication of the selected action. In contrast, the n2, following authentication of the surly node based on a selected action, loses the p messages if n2 refuses the request for a message.

Notations

Rw	is considered as the Reward
Pn	is considered as the Penalty
Su	is considered as the Surly
Wm	is considered as the Wimpy
Acc	is considered as the Accept
Rej	is considered as the Reject
β_1(a|b)	is considered as the c's probability on a virtual node n_1 after selecting the a
β_2(a|b)	is considered as the b's Probability on a virtual node n_1 after considering c
μ(a|b)	is considered as the probability of success on a virtual node n_2 from the selection of a node n_1
u_i(a|b|c)	is the Pay-off factor

Case* 1: *Surly* chooses *Reward* and *Wimpy* chooses *Penalty

$$\beta_1(Rw|Su) = 1,$$
$$\beta_1(Pn|Su) = 0,$$
$$\beta_1(Rw|Wm) = 0,$$
$$\beta_1(Pn|Wm) = 1,$$

According to the Bayes's rule:

$$\mu(Su|Rw) = \beta_1(Rw|Su)(q)\left(\frac{1}{\beta_1(Rw|Wm)(1-q)}\right) + \left(\frac{1}{\beta_1(Rw|Su)(q)}\right)$$

$$\mu(Su|Rw) = 1$$

Further,

$$\mu(Su|Rw) = \beta_1(Pn|Wm)(1-q)\left(\frac{1}{\beta_1(Pn|Wm)(1-q)}\right) + \left(\frac{1}{\beta_1(Pn|Su)(q)}\right)$$

$$\mu(Su|Rw) = 1$$

The computation is given as below:

$$u_2(Rw,\ Rej,\ Su) = 0 < u_2(Rw,\ Acc,\ Su) = \rho - 1, \text{ and}$$
$$u_2(Pn,\ Acc,\ Wm) = -1 < u_2(Pn,\ Rej,\ Wm) = 0.$$
$$\beta_2(Rej|Pn) = 1,$$
$$\beta_2(Acc|Rw) = 1$$

In addition, node n2 is able, on the basis of the request and the award decision of node n2, to recognise participants. n2 knows, and takes its judgement, that n1 is a nasty type. The n1 is classified as wimpy when the node n2 observes a penalty, and the action selected is denied. The observation shows that the n2 node responds to Acc's action Rw and Rej's action Pn. However, if the n1 node learns the choice, the node Wm decides to recompense 1 instead of 0.

Case* 2: *Reward* selects *Surly* and *Penalty* chooses *Wimpy

$\beta_1(Rw|Su) = 0,$
$\beta_1(Pn|Su) = 1,$
$\beta_1(Pn|Wm) = 0,$
$\beta_1(Rw|Wm) = 1.$

The computation is given as below:

$$\mu(Su|Pn) = \beta_1(Pn|Su)(q)\left(\frac{1}{\beta_1(Pn|Wm)(1-q)}\right) + \left(\frac{1}{\beta_1(Pn|Su)(q)}\right)$$

$\mu(Su|Pn) = 1$

Further,

$$\mu(Wm|Rw) = \beta_1(Rw|Wm)(1-q)\left(\frac{1}{\beta_1(Rw|Su)(q)}\right) + \left(\frac{1}{\beta_1(Rw|Wm)(1-q)}\right)$$

$$\mu(Wn|Rw) = \frac{1 \times (1-q)}{1 \times (1-q) + 0 \times q} = 1$$

The computation is given as below:

$u_2(Pn,\ Rej,\ Su) = -\pi < u_2(Pn,\ Acc,\ Su) = 1$
$u_2(Rw,\ Acc,\ Wm) = -1 < u_2(Rw,\ Rej,\ Wm) = 0.$
$\beta_2(Acc|Pn) = 1,\ \ \beta_2(Rej|Rw) = 1,$

Case* 3: A node selects *Reward

$\beta_1(Pn|Su) = 0,$
$\beta_1(Rw|Su) = 1,$
$\beta_1(Pn|Wm) = 0,$
$\beta_1(Rw|Wm) = 1,$

The computation is given as below:

$$\mu(Su|Rw) = \beta_1(Rw|Su)(q)\left(\frac{1}{\beta_1(Rw|Su)(q)} + \frac{1}{\beta_1(Rw|Wm)(1-q)}\right)$$

$\mu(Su|Rw) = q$

Further,

$$\mu(Wm|Rw) = \frac{\beta_1(Rw|Wm)(1-q)}{\beta_1(Rw|Su)(q) + \beta_1(Rw|Wm)(1-q)}$$

$\mu(Su|Rw) = 1 - q$

Then,

$u_2(\mu,\ Acc|Rw) = q\rho - 1$

and

$u_2(\mu,\ Rej|Rw) = 0$:

$$(\mu,\ Rw) = \begin{cases} Accept & \text{if } q \geq \dfrac{1}{\rho} \\ Reject & \text{if } q \leq \dfrac{1}{\rho} \end{cases}$$

Note that if $q = 1/\rho$, Acc and Rej will result, and n2 will choose each strategic one. In $q > 1/\rho$, n2 will select Acc and the result will be 1 for n1 and the best probability is regarded the correct selection.

Case* 4: A virtual node selects *penalty

$\beta_1(Rw|Su) = 0,$
$\beta_1(Pn|Su) = 1,$
$\beta_1(Rw|Wm) = 0,$
$\beta_1(Pn|Wm) = 1,$

According to the Machine learning based Bayes's rule:

$\mu(Su|Rw) = q$

Further,

$$\mu(Wm|Pn) = \beta_1(Pn|Wm)(1-q)\left(\frac{1}{\beta_1(Pn|Wm)(1-q)} + \frac{1}{\beta_1(Pn|Su)(q)}\right)$$

$\mu(Su|Rw) = 1 - q$

Then,

$u_2(\mu,\ Acc|Pn) = -1$

and

$u_2(\mu,\ Rej|Pn) = -q\pi$:

$$(\mu,\ Pn) = \begin{cases} Acc & \text{if } q \geq \dfrac{1}{\pi} \\ \text{Re}j & \text{if } q \leq \dfrac{1}{\pi} \end{cases}$$

Note that if $q = 1/\pi$, Acc and Rej and n2 will decide which of them to do. For $q > 1/\pi$, the n_2, n2 selects Acc and the result is 1 for n1, which is the most likely pick.

5 Performance Evaluation

The public audit system is evaluated and simulated using a cloudsim simulator for its performance. The solution suggested consists of a public audit architecture with four modules/case authentication, signature, and verification phases. This public audit technique is simulated in the cloud as independent modules.

Figs. 2 and 3 show that the delay has been greatly decreased by authentication ECC with signature generation and verifying. However, with increasing key size, the latency increases linearly. The signature

phase graph shows a greater delay than the ECC method in the conventional technique. In addition, the usage of machine learning based XNOR reduces the delay for each key size substantially.

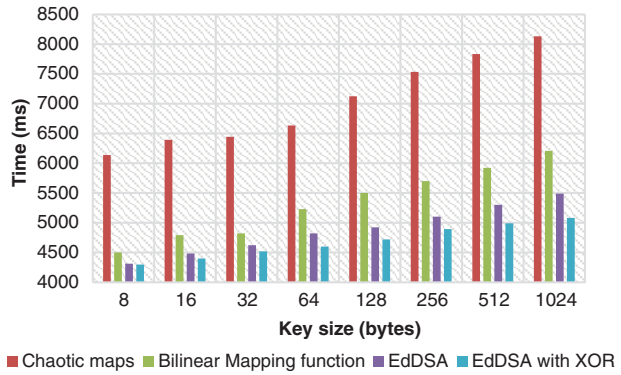

Figure 2: Key generation phase validation when utilizing various key size

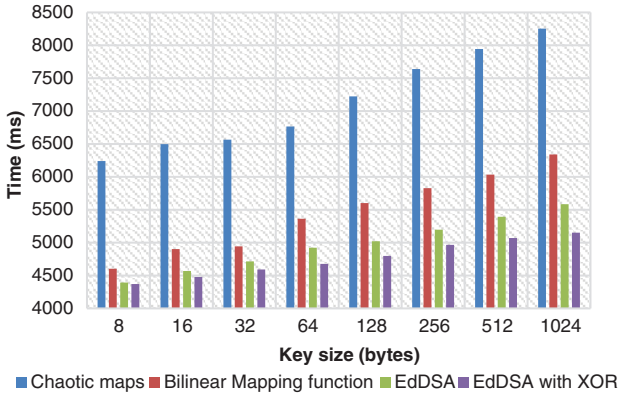

Figure 3: Verification phase validation when utilizing various key size

The network performance is tested with different key sizes from 8 bits to 1024 bits during authentication with the ECC technique. It is shown that the method with respect to has a vast difference in delay. For instance, the time spent authenticating the node with the ECC technique has fallen by 29 percent over chaotic 8-bit maps. It is also observed that node authentication is significantly higher than the chaotic maps with a key size of 1024 bits, or 38 percent.

Similarly, with the key size of 8 to 1024 bits, a reduction rate of 4–18 percent was shown in comparison results with bilinear mapping functions. The suggested ECC with XNOR function also displays an authentication rate of 0.3–7.0% with 8–1024-bit key size, which is lower in terms of signature generation than the ECC Algorithm. The statistics show that there is an average delay of 100–120 ms during a major signature and verification step. The ECC algorithm is, nevertheless, more verifiable than the other algorithms, using the machine learning-based XNOR function. This shows that the authentication rate of the system is faster than the traditional one. Therefore, the processing time is particularly critical for analysis for further authentication of messages. The results of the verification signature and mutual authentication are illustrated in Figs. 4 and 5.

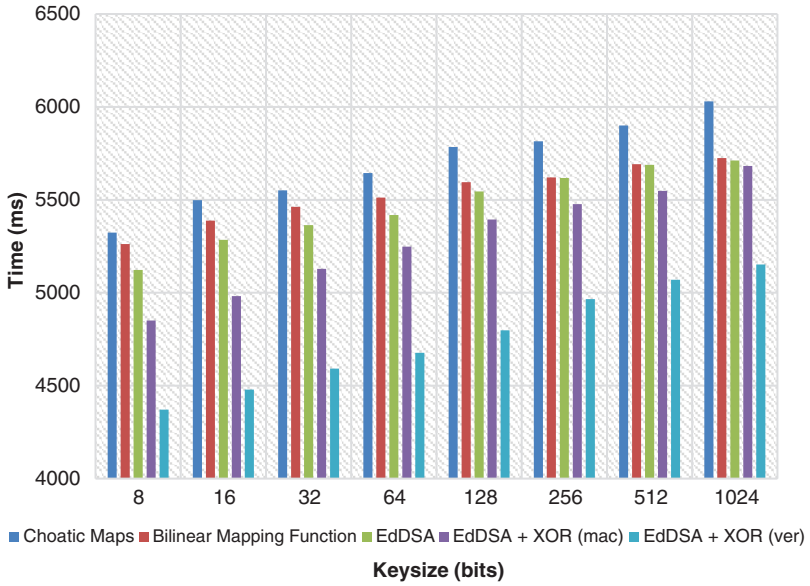

Figure 4: Time consumption (ms)

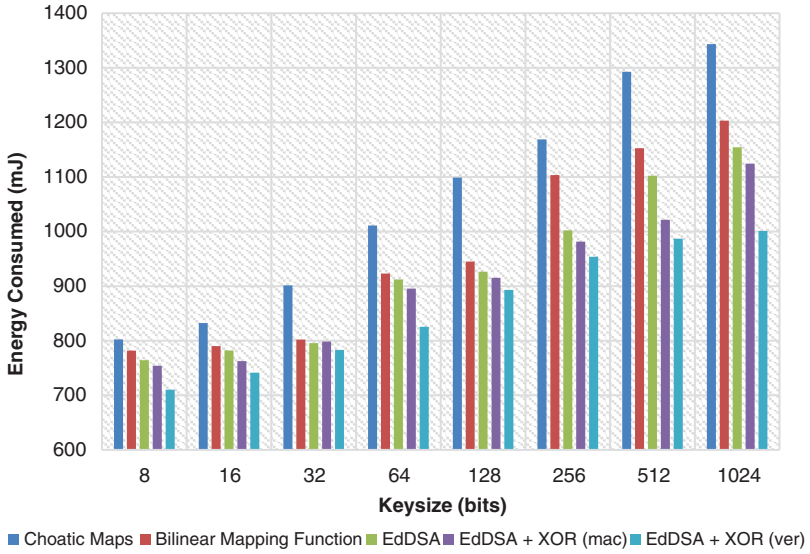

Figure 5: Energy consumed (mJ)

Different key dimensions are evaluated for the computer time of mutual authentication and signature verification. The key size of time and energy consumption grows linearly with the increasing key dimension. In addition, the reciprocal authentication phase doubles cloud energy duration and consumption.

6 Conclusion

In this paper, ECC is used to encrypt the message, where the game model used to verify the identities of the network nodes that make up the network. By making use of a technique known as structured authentication with two factors, we are able to present a novel perspective. The game model offers a method for mutual authentication between virtual nodes in all four possible node scenarios, as well as a

technique to test for the uncertainty of the nodes in the surrounding area. These two activities are compatible with one another and can be performed in the same setting. Not only does the application of XNOR function greatly reduce the amount of time necessary for computation, but it also significantly cuts down on the amount of energy that is necessary. The findings of the simulations carried out on authenticating nodes show that implementing the proposed strategy resulted in an increase and a decrease in the total amount of energy that was consumed. Due to the fact that this latency increases in a linear rather than a progressive form, it is not particularly helpful for calculations that involve a great number of important dimensions.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] N. Garg, S. Bawa and N. Kumar, "An efficient data integrity auditing protocol for cloud computing. Future generation computer systems," *Journal of Network and Computer Applications*, vol. 109, pp. 306–316, 2020.

[2] N. Garg and S. Bawa, "Comparative analysis of cloud data integrity auditing protocols," *Journal of Network and Computer Applications*, vol. 66, pp. 17–32, 2016.

[3] Y. Natarajan and G. Dhiman, "Task scheduling in the cloud using ACO," *Recent Advances in Computer Science and Communications*, vol. 13, pp. 1–6, 2021.

[4] Y. Li, Y. Yu and K. K. R. Choo, "Fuzzy identity-based data integrity auditing for reliable cloud storage systems," *IEEE Transactions on Dependable and Secure Computing*, vol. 16, no. 1, pp. 72–83, 2017.

[5] N. Lu, Y. Zhang, W. Shi, S. Kumari and K. K. R. Choo, "A secure and scalable data integrity auditing scheme based on hyperledger fabric," *Computers and Security*, vol. 92, pp. 101741, 2021.

[6] N. V. Kousik and R. Mahaveerakannan, "Improved density-based learning to cluster for user web log in data mining," in *Inventive Computation and Information Technologies*, Singapore: Springer, pp. 813–830, 2021.

[7] S. Jayasri, A. Daniel and P. Rajakumar, "A survey on various load balancing algorithms to improve the task scheduling in the cloud computing environment," *Journal of Advanced Research in Dynamical and Control Systems*, vol. 11, no. 8, pp. 2397–2406, 2019.

[8] J. Shen, D. Liu, D. He, X. Huang, and Y. Xiang, "Algebraic signatures-based data integrity auditing for efficient data dynamics in cloud computing," *IEEE Transactions on Sustainable Computing*, vol. 5, no. 2, pp. 161–173, 2017.

[9] W. Shen, J. Qin, J. Yu, R. Hao and J. Hu, "Enabling identity-based integrity auditing and data sharing with sensitive information hiding for secure cloud storage," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 2, pp. 331–346, 2018.

[10] R. Raja, V. Ganesan, and S. G. Dhas, "Analysis on improving the response time with PIDSARSA-RAL in ClowdFlows mining platform," *EAI Endorsed Transactions on Energy Web*, vol. 5, pp. 20, 2018.

[11] B. Shao, G. Bian, Y. Wang, S. Su and C. Guo, "Dynamic data integrity auditing method supporting privacy protection in vehicular cloud environment," *IEEE Access*, vol. 6, pp. 43785–43797, 2018.

[12] W. Luo, W. Ma and J. Gao, "MHB* T based dynamic data integrity auditing in cloud storage," *Cluster Computing*, vol. 24, pp. 1–18, 2021.

[13] Y. Ren, J. Shen, Y. Zheng, J. Wang and H. C. Chao, "Efficient data integrity auditing for storage security in mobile health cloud," *Peer-to-Peer Networking and Applications*, vol. 9, no. 5, pp. 854–863, 2016.

[14] R. A. Raja, T. Karthikeyan and N. V. Kousik, "Improved privacy preservation framework for cloud-based internet of things," in *The Internet of Things*, 1st ed., CRC Press, pp. 165–174, 2020.

[15] J. Wei, R. Zhang and Y. Yao, "Dynamic data integrity auditing for secure outsourcing in the cloud," *Concurrency and Computation: Practice and Experience*, vol. 29, no. 12, pp. 4096, 2017.