International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-4, April 2019

Cloud Access with Load Balancing and Certificateless Signature Authentication

Manmohan Sharma, V.K. Jain

Abstract*: Cloud computing is one of the most emerging technology in the market which caters the demand of large people in an economic fashion. Nowadays most of the organizations are using cloud services directly or indirectly and they pay for these services on the basis of their usage. Another important property of cloud computing is on-demand services. Most of the organizations and individuals are using cloud services for storage of their data and retrieval of the data. In both the case there might be the chances of data loss and data hacking. So to ensure the security and integrity of the data we need to apply certain encryption techniques. We focus on security aspects in cloud ensuring load balancing and authentication using Certificateless public key cryptography technique.

***Index Terms*: Cloud computing, data security, an encryption technique, load balancing.**

I. INTRODUCTION

Cloud computing is an exceptionally current theme and the term has picked up a great deal of consideration as of late. It can be characterized as pay as per your usage of data, program, and platforms as and when required using any gadgets from anywhere. Human reliance on the cloud is clear from the way that today's most well-known social organizing, email, archive sharing, and web-based gaming destinations are facilitated on the cloud [1]. Google, Microsoft, IBM, Amazon, Yahoo and Apple among others are exceptionally dynamic in this field. One of the most important services offered by the cloud is the data storage. Users now days utilize cloud storage and can be completely released from the troublesome local data storage and maintenance. However, the data stored in others database possess risk related to confidentiality of the data. Specifically, the cloud servers maintained by cloud vendors are not fully trusted by users because the data might be sensitive and any leak results in complete failure of business plans. For data privacy preservation, the best solution is to encrypt the data file and then store the encrypted files on the cloud [2]. There is the number of challenges related to designing of secure and efficient data sharing schemes for groups of people in a cloud. Some of the challenges issues are:-The first issue is related to the privacy of the data. This is one of the major obstacles in the large-scale deployment of cloud computing. Users have a concern that their identity might be reviled to the attackers and cloud providers [4]. So they are looking for the guaranteed privacy of their identity. The second issue is related to providing full control of storing, reading and editing of data to multiple users. This system is also known as multi-owner system. On the other side in a single owner system, only the group manager can store and modify data in the cloud. Multi-owner system is more advantageous and flexible as compared to single owner system but is more prone to security threats. If every user has a right to edit and upload files in the cloud then might be some employees who left the company will store and edit some useful files in the cloud [5,6]. There might be the possibility that they share their credentials to hackers who intended to do some malicious actions. Last but not least, employees or user groups are dynamic in practice that means new staffs joining and current staff discontinues in a company. Membership changes create some issues related to secure data sharing in the cloud. There are numerous system challenges for new granted users for learning the contents of data files before storing. At the same time, these users also struggle with anonymous data owners for corresponding decryption keys of stored data files. On another side, membership revocation mechanism without updating the secret keys of the remaining users is also required to minimize key complexity management. Numbers of security schemes for data sharing on untrusted servers are proposed by many researchers. In those schemes, the data owner will store the encrypted data and share the decryption key with the authorized user. In this fashion, the unauthorized user and data servers cannot retrieve the content of the data files because they do not have decryption keys. To deal with the issues of accommodating huge volume of continuously increasing data we need the services of cloud with security and privacy. In this paper, we proposed a load balanced secure data sharing scheme. This scheme will overcome the issues related to load balancing, security, and confidentiality of the data. It also impacts the data retrieval efficiency while preserving the privacy. The paper is organized in the following sections:-Section 2 presented load balancing in cloud whereas section 3 focuses on security issues related to cloud access. Section 4 focuses on the literature review related to cloud load balancing and security. The proposed scheme is presented in Section 5 with an advantage of CL signature in Section 6 followed by the conclusion in section 7.

II. LOAD BALANCING

It disseminates the aggregate load to the individual machines of the framework in such a way that each and every hub successfully uses the assets and limits the reaction time.

Manuscript published on 30 April 2019.
***** Correspondence Author (s)
Manmohan Sharma*, CSE, SET, Mody University of Science and Technology, Lakshmangarh, Sikar, Rajasthan, India.
V.K. Jain, CSE, SET, Mody University of Science and Technology, Lakshmangarh, Sikar, Rajasthan, India.

It tackles situations where a portion of the hubs is over stacked or under stacked. A dynamic calculation does not consider the past state & relies upon the present conduct of the framework. The key qualities utilized are the execution of framework, correlation of load, security of various framework, the collaboration between the hubs, estimation of load, choosing of hubs, nature of work to be exchanged and numerous different ones [3,7].

A. Static Load Balancing

Here the cloud supplier uses homogeneous assets. Here progressed provisioning is done in which the suppliers set up the suitable assets before the beginning of administrations as per the agreements did. Non-versatile assets are used due to the static condition. The cloud requires prior information of hubs limit, preparing power, memory, execution, and insights of client necessities which are not variable [8]. Examples of static load balancing techniques include round robin, central manager, threshold algorithm and randomized algorithm.

B. Dynamic Load Balancing

Heterogeneous assets are supplied by cloud here. Dynamic provisioning is done with adaptable assets in which the specialist co-op apportions more assets as they are expected to the client and expelled them when they are not utilized. Cloud does not require any previous learning [9] and the prerequisites of the clients are versatile. A dynamic condition is hard to be reproduced yet is very customizable with distributed computing condition. Dynamic load balancing techniques include Honey bee foraging, central queue, local queue, and least connection.

III. SECURITY ISSUES IN CLOUD

Cloud security is an important aspect of cloud usage. For some of the public services like banking services, we need at most security but for other services like e-commerce, telemedicine also requires some level of security. For voice we need less security whereas for the email we need to encrypt the messages for security purpose [4, 10]. The organization's willingness to join cloud having security as one of the major concerns.

If the security level is going to be increased more computing resources, memory and bandwidth are required, which in turn results in more complication to access the cloud resources. It means that ensuring security at higher level creates a number of other problems related to cloud access. We will discuss security from three different aspects:

1. Network Security: Data is more prone to the threat while in transient over the network. The main threats include denial of Services (DoS) attacks and fake identity usage. To protect against such attacks we use some of the mechanisms like IPSec, network-based intrusion detection and traffic cleaning etc.

2. Services Security: Cloud vendors will provide services which can be categories into Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). Service security mechanism includes authorization, authentication, data isolation, and virus detections. Services can protect from illegal control and intrusion detection and prevention.

3. Storage Security: It means Security related to data stored onto the cloud. When data is stored in the cloud it is in the hands of the cloud service provider which might use this data for their benefits. Might be the number of other users or hackers may use that data if not stored securely. So, before storing the data should be encrypted using proper techniques and decryption key must be shared with the authorized users only.

IV. LITERATURE REVIEW

Section 4 describes various work done in cloud computing and CL signature.

Kar Jayaprakash et. al. (2017) outlined an ID based signcryption scheme which was provably secure in the random oracle model [11]. They also presented formal proofs of security for signcryption. The scheme was secure against side channel, chosen message, chosen cipher and fault tolerant attack.

Hafizul Islam, S. K., et. al. (2017) proposed CL digital multi-signature scheme which seems to be more secure and efficient [12]. They designed CL- DMS without bilinear pairing attack.

Wei et. al. (2016 and MTS hash function. They demonstrated proposed approach is reliable against adaptively chosen message) demonstrated Sue. et al. ePASS attribute-based signature scheme failed to satisfy attribute signer privacy[13].

D. Chitra Devi and V. Rhymend Uthariaraj (2015) discussed how to overcome issues related to round-robin load balancing algorithm. He talked about the weighted round-robin scheme in which total turnaround time for each user job is improved [13].

HyungjinIm, Jungho Kangand Jong Hyuk Park talks about the limitations of existing authentication mechanisms and proposed CL-PKC using hierarchical identifier [14].

Chunming Rong, Hongbing Cheng (2012) proposed a secure data access mechanism based on identity-based encryption and biometric authentication. In this, they outlined the double protection system for confidential data access [15].

Sudha Senthil Kumar et. al (2017) talked about the improved version of the Honey bee foraging Algorithm. They did the addition of adaptive neighboring search and site abandonment strategy with Honey bee foraging algorithm. They figure it out that efficiency is improved using this combined approach [16].

Peng Li, Song Guo et.al (2014) proposed oblivious RAM(ORAM) algorithm secure cloud data access with improved performance[17]. It works on the principle that periodic reshuffle data blocks stored in untrusted servers so that users credentials cannot be tracked.

S. R. Murugaiyan, D. Chandramohan, T. Vengattaraman, P. Dhavachelvan (2014) proposed a framework for preserving the privacy of the data stored in the cloud. It also focuses on identifying the introducers by continuously checking the logs maintained in the cloud [18].

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

Omer K. Jasim, Safia Abbas, El-Sayed M. El-Horbaty, Abdel-Badeeh M. Salem (2014) proposes a Cryptographic Cloud Computing Environment (CCCE) for more secure data transmissions. It resolves the problem of key generation and key distribution while doing key negotiation between the communication parties. Combination of quantum key distribution mechanisms (QKD) and advanced encryption standard (AES) is used for designing the framework [19].

V. PROPOSED WORK

To overcome the issues related to security or authenticity of the person who is accessing the cloud, the following procedure will work:-

A. Assumptions:

1. We assume that all the data center have n number of VM's with some varying capacity.
2. At the starting, the entire user is verified and got allocated VM's as per their demands.
3. The given below procedure will work once the start phase is over.
4. We used certificate less cryptography for authorization purpose whose algorithm is explained separately.

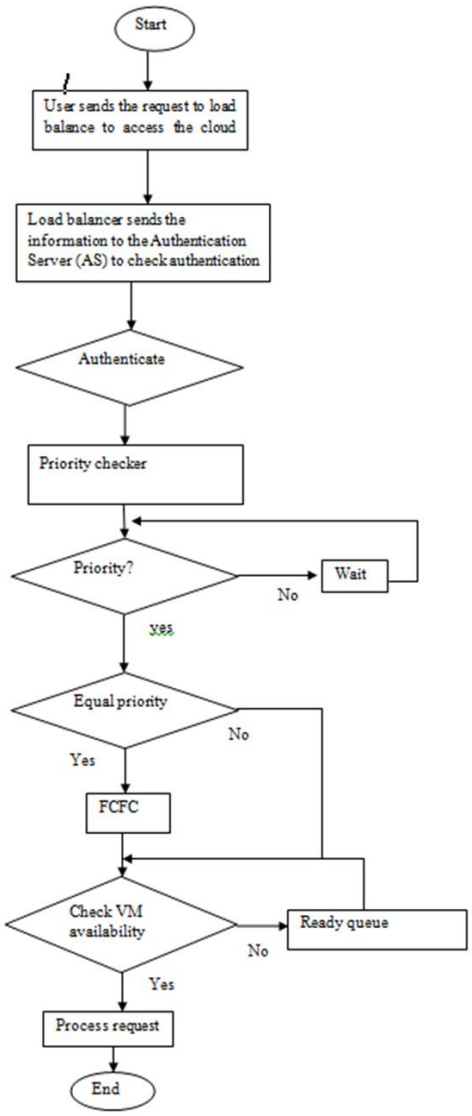

Figure 1: Block diagram of cloud load balancing with security feature

B. Procedure

1. As per the Figure 2, there are 7 users from different location who want to access the cloud services.
2. User first sends a request to the load balancer for access of the cloud as per his/her need. In the request he sends the information like his processing needs (in terms of CPU cycles, memory etc.), key and priority number.

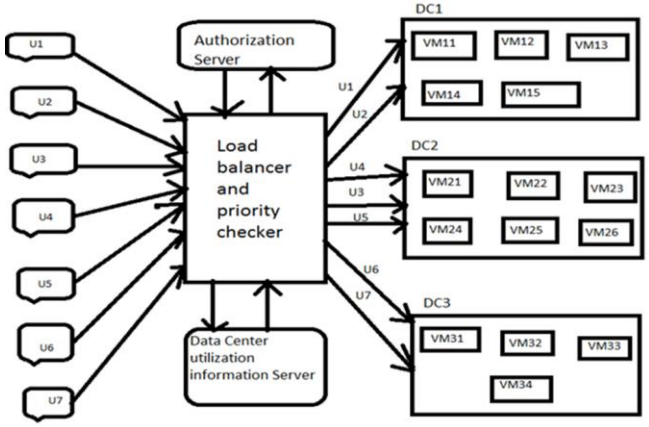

Figure 2: Architectural diagram of cloud load balancer with user authentication check

3. The load balancer is associated with the Authorization server, priority checker and Data Centre utilization information (DCUI) server. The Authorization server is responsible for the authenticity check of the user using some cryptographic technique. Priority checker is used to checking the priority of the incoming user request. DCUI information is used to check the utilization of a particular DC.DCUI is updated simultaneously once there is any change(either VM's are allocated or deallocated) in DC occurs.
4. Once the load balancer receives the request from the users the following steps would happen:
4.1. If the user is an authenticated user (Authorization is done with the help of CL-PKC) then allows accessing of the cloud based on his priority.
4.2. If the user is not authenticated user then reject the request.
5. Once the user is done with his authentication process its priority is going to be checked. Priority is assigned to the users at the time of registration with the cloud vendor on the basis of SLA with the cloud owner.
6. On the basis of user's priority (highest priority request processed first, then second highest and follow on…) VM allocation process is done.
7. Before allocation of the VM's DCUI checks for the availability of the VMs as per the demands of incoming user requests.
If VM's are available then these VM's are allotted. If VM's are not available then these requests are going to be waiting in a ready queue in a priority order sequence.
8. If two user requests have the same priority number then the first come first serve policy is applied to allocate the VM's to the users.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

C. Certificateless public key cryptography algorithm

References

Certificateless cryptography is a public key scheme that gives security without the validation of public key. In this section, we proposed an efficient pairing free Certificate Less Digital Signature scheme based on ECC. Al-Riyami and Paterson [Al-Riyami, Sattam S., ; Kenneth G. Paterson] in 2003, proposed new scheme for public key encryption that removes the disadvantages of both public key encryption and IBE keeping in mind the end goal to determine the key escrow issue. The new scheme is known as Certificate less –Public Key encryption (CL-PKE). Today gadgets having constrained computational resources and communication bandwidth discover CL public key cryptography extremely appealing and imperative to reduce stack on the system.

If this CL signature technique is applied in cloud for data security and authentication that will reduce attacks on the data as well as bandwidth constrained can also be removed. Used abbreviations are represented in Table 1.

The following steps are required for CL-DS are:-

Setup: For given security parameter *params*, Authentication Server (AS) produces System *parameters* in the represented manner:

- To choose the tuple $\{F_q, E/F_q, G_q, P\}$, AS selects a K bit prime number q.
- Select secure arbitrary number $s \in RZ^*_q$ for the master private key and determine master public key $P_{pub} = sP$.
- Selects one way hash functions H_0, H_1, H_2, H_3 :$\{0,1\}^*$--> $\{0,1\}^K$
- Publish system $\{F_q, E/F_q, G_q, P, P_{pub}, H_0, H_1, H_2, H_3\}$.

Key Generation: AS executes the Setup algorithm to generate system parameters and a master key. It extracts the partial private key by running private key extract algorithm for each user. Each user selects a secret value and computes its own private and public key.

Set Secret Key: Let User U_i is the sender. AS computes private and public key pairs for each user U_i with identities of $UID_a \in \{0,1\}^*$.

The U_i with UID_a select a secure random number $x_a \in RZ^*_q$ as their secret key and computes the scalar multiplication $X_a = x_aP$ for the mathematical related public key.

Partial Private Key Extract: After computing X_a, U_i send (UID_a, X_a) to the AS. AS chooses a random number $r_a \in RZ^*_q$ and computes $R_a = r_aP$. AS also computes secret key $d_a = r_a + sq_a \bmod q$ where

$$q_a = H_0(UID_a \| R_a \| X_a)$$

The private key d_a and R_a are sent to the user with UIDa by AS via secure channel. The corresponding ID-based public key of user Q_a is computed by $Q_a = R_a + q_aP_{Pub}$. Now the private/public key (d_a , Q_a) pair can be verified by checking the equation $Q_a = R_a + q_aP_{Pub} = d_aP$.

Set Private Key: Determined $sK_a = (d_a , x_a)$ as a private key for user with ID_a.

Set Public Key: Determined $pK_a = (X_a , R_a)$ as public key for user with UID_a.

CL-DS-Sign

In order to generate the signature on the request message *m* user performs the following steps:-

Sign (m, X_a , UID_a , AID_b , d_a , t): The algorithm works as follows:-

- User sends $D = E_{PKAS}(t)$ to load balancer.
- User selects a random number $y \in RZ^*_q$ and compute $Y = yP$.
- And computes

  $h_1 = H_1(Y)$.

  $h_2 = H_2(UID_a , X_a , Y , AID_b , h_1)$.

  $h_3 = H_3(m, UID_a , X_a , Y, AID_b , t, h_2)$, where t is time when request was sent.
- Computes $V = (y + h_2x_a + h_3d_a) \bmod q$.
- Alice Computes

$$C = (m \| V) \oplus h_2.$$

$$Z = VP$$

And returns signature $\sigma = (C, Y, Z)$ on message m.

Verification of CL-DS

To validate the signature $\sigma = (C, Y, Z)$ on request message m, the verifier AS carried out the following steps:

- AS decrypts $t = D_{SKAS}(D)$ to extract message signature time.
- Computes $h_1 = H_1(Y)$.
- $C \oplus h_2 = (m \| V)$.
- Before verification AS first of all computes h_2 , h_3 , Q_a.

$$h_2 = H_2(UID_a , X_a , Y , AID_b , h_1).$$

$$h_3 = H_3(m, UID_a , X_a , Y, AID_b , h_2)$$

$$Q_a = R_a + q_aP_{Pub}.$$

Where $q_a = H_0(ID_a \| R_a \| X_a)$

Notion	Meaning	Notion	Meaning
UID_a	User ID	(d_a , Q_a)	private/public key
AID_b	Authentication server ID	D	Encrypted timestamp
X_a	User Secret key	sk_a	Private key
R_a	Partial public key	pk_a	Public key
σ	Signature		

Table 1: Notions and their meanings

And then verifies the following equation

$$Z = Y + h_2X_a + h_3Q_a.$$

Checks whether the equation Z = VP. If it verifies the verifier accepts the signature $\sigma = (C, Y, Z)$ otherwise rejects it.

VI. ADVANTAGES OF USING CL-PKC

1) Low bandwidth and low storage are required to do this authentication process. This will help to access the data securely with minimum bandwidth and the cost related to authentication of a person is also very low. This property helps to increase the usage of the cloud as internet speed requirement is minimum for secure data access.
2) There is no need to verify the certificate that will reduce latency in the data fetch from the cloud.
3) A higher degree of privacy is preserved. Privacy ensures the users that his sensitive information is protected from unauthorized users or wrong people.
4) Cloud owner cannot be able to recover the session key nor does any hacker.
5) Signature forgery cannot happen.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

VII. ISSUES WITH CL-PKC

The two main issues with CL-PKC are:

1) It is not purely identity-based cryptographic technique because identifier and public key are required for encryption of the message.
2) Revocation of the certificate is another issue with CL-PKC.

VIII. RESULT AND CONCLUSION

Cloud computing is the latest technology that is being widely used all over the world. Load balancing is one of the major challenges along with secure access and storage in the cloud. In this paper, we clubbed together load balancing with the security of the cloud.

Authors	Load Balancing	Authentication	Encryption	CL-DS
D. Chitra Devi and V. Rhymend Uthariaraj	√	×	×	×
Sudha Senthil Kumar et. al.	√	×	×	×
D. Puthal, P. Nanda, S.P.Mohanty, A.Zomaya [22]	√	√	×	×
Proposed Scheme	√	√	√	√

Table 2: Result Comparison with other authors

For load balancing, we used the priority-based model where priority is assigned at the time of registration of the user on the basis of SLA's. For secure data access, we adopted CL-PKC which is having numerous advantages. We use this technique because it requires low bandwidth and the higher degree of privacy is preserved. These are the two major concerns in the mind of cloud users. So by combining these two techniques together, we proposed an approach which is more secure and properly balanced. We compare our approach with other load balancing methods without security like round robin, honey bee foraging etc. and we found our approach is far better in terms of load balancing and security. Table 2 depicts the comparison of the proposed approach with other researchers. The result of the comparison is shown using vein diagram (Figure 3). In the future, we will work on improving the efficiency of cloud servers that results in low carbon emissions, low power consumptions with proper load balancing that result in green cloud effects [21].

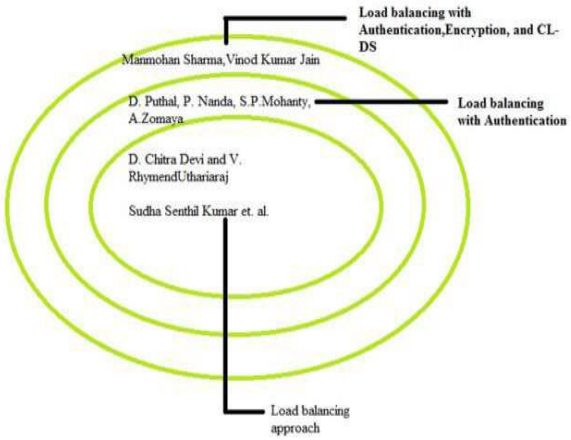

Figure 3: Results based on parameters given in table 2.

REFERENCES

1. Santosh Kumar and R. H. Goudar (2012), "Cloud Computing –Research Issues, Challenges, Architecture, Platforms and Applications: A Survey", International Journal of Future Computer and Communication, Vol. 1, No 4, 356-360.W.-K. Chen, Linear Networks and Systems (Book style). Belmont, CA: Wadsworth, 1993, pp. 123–135.
2. Kaur, M. and Singh, H., (2015), "A review of cloud computing security issues", International Journal of Advances in Engineering & Technology, Vol. 8,No. 5, 215-222.
3. Khiyaita, A., H. El Bakkali, M. Zbakh, and Dafir El Kettani (2012), "Load balancing cloud computing: state of art", In National Days of Network Security and Systems (JNS2), 106-109.E. H. Miller, "A note on reflector arrays (Periodical style—Accepted for publication)," IEEE Trans. Antennas Propagat., to be published.
4. Anuj Kumar Gupta, (2015), Cloud Computing: Concepts and Challenges", Asian Journal of Computer Science and Technology, Vol. 4 No. 2, 27-30.C. J. Kaufman, Rocky Mountain Research Lab., Boulder, CO, private communication, May 1995.
5. S. Sasikala, T. Karthick (2014), "Privacy Preserving and Load Balancing For Secure Cloud Storage", IOSR Journal of Computer Engineering, e-ISSN: 2278-0661, p- ISSN: 2278-8727, vol. 16, Issue 1, Ver. IV, 102-106.
6. Kang, Seungmin, Bharadwaj Veeravalli, and Khin Mi Mi Aung (2014), "Scheduling Multiple Divisible Loads in a Multi-cloud System", In Utility and Cloud Computing (UCC), IEEE/ACM 7th International Conference on Utility and Cloud Computing, London, United Kingdom.
7. Cao, Qi, Zhi-Bo Wei, and Wen-Mao Gong (2009), "An optimized algorithm for task scheduling based on activity based costing in cloud computing",3rd International Conference on Bioinformatics and Biomedical Engineering, ICBBE 2009, Beijing, China
8. Z. Chaczko, V. Mahadevan, S. Aslanzadeh, and C. Mcdermid (2011), "Availability and load balancing in cloud computing," in International Conference on Computer and Software Modeling, Singapore, 14.
9. Choudhary, Monika, and Sateesh Kumar Peddoju (2012), "A dynamic optimization algorithm for task scheduling in cloud environment", International Journal of Engineering Research and Applications (IJERA), vol. 2(3), 2564-2568.
10. S. Sasikala, T. Karthick (2014), "Privacy Preserving and Load Balancing For Secure Cloud Storage", IOSR Journal of Computer Engineering (IOSR-JCE), vol. 16(1), Ver. IV, 102-106.
11. Kar Jaya prakash and Naik KSHIRASAGAR (2017), "Security Analysis and Implementation issues of Signcryption Scheme for Smart card", A Journal of the Academy of Business and Retail Management (ABRM), vol.1(2) , 24-36.
12. Hafizul Islam, S. K., Mohammad SabzinejadFarash, G. P. Biswas, Muhammad Khurram Khan, and Mohammad S. Obaidat (2017), "A pairing-free certificateless digital multisignature scheme using elliptic curve cryptography", International Journal of Computer Mathematics, vol. 94(1), 39-55.
13. Wei, Jianghong, Wenfen Liu, and Xuexian Hu (2016), "Security pitfalls of ePASS",Journal of Information Security and Applications, vol. 30(C), 40-45.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

14. HyungjinIm, JunghoKang , and Jong Hyuk Park (2015),“ Certificateless based Public Key Infrastructure using a DNSSEC”, Journal of Convergence , vol. 6(3), 26-33.
15. Chunming Rong, Hongbing Cheng (2012), “A Secure Data Access Mechanism for Cloud Tenants”, CLOUD COMPUTING 2012: The Third International Conference on Cloud Computing, GRIDs, and Virtualization, IARIA, Nice, France.
16. Sudha Senthil kumar, K.Brindha, Rathi, Angulakshmi, Jothi and Yash Vardhan Thirani (2017), “Honey-Bee Foraging Algorithm for Load Balancing in Cloud Computing Optimization”, International Journal of Engineering Science and Computing, pp. 15840-15844.
17. Peng Li, Song Guo (2014),”Load balancing for privacy-preserving access to big data in cloud.”, IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), April 2014, Toronto, ON, Canada.
18. S. R. Murugaiyan, D. Chandramohan, T. Vengattaraman, P. Dhavachelvan (2014)“A Generic Privacy Breach Preventing Methodology for Cloud Based Web Service” International Journal of Grid and High Performance Computing, 6(3), pp. 53-84.
19. Omer K. Jasim, Safia Abbas, El-Sayed M. El-Horbaty, Abdel-Badeeh M. Salem “Cryptographic Cloud Computing Environment as a More Trusted Communication Environment” International Journal of Grid and High Performance Computing, 6(2), pp. 38-51.
20. Al-Riyami, Sattam S., and Kenneth G. Paterson (2003), “Certificateless public key cryptography”, International Conference on the Theory and Application of Cryptology and Information Security, Springer , 2003 , 452-473, Berlin, Heidelberg.
21. Ahuja, Sanjay P., and Karthika Muthiah (2016), “Survey of state-of-art in green cloud computing”, International Journal of Green Computing (IJGC) , vol. 7(1), 25-36.
22. D. Puthal, P. Nanda, S.P.Mohanty, A.Zomaya(2018) “Secure and Sustainable Load balancing of Edge Data centers in Fog Computing”, IEEE communication Magazine 56(5):60-65.

AUTHORS PROFILE

Mr. Manmohan Sharma pursed Bachelor of Engineering from Rajasthan University in 2005 and Master of Engineering from BITS Pilani in year 2009. He is currently pursuing Ph.D. and currently working as Assistant Professor in Department of Computational Sciences, CET-Mody University, and Lakshmangarh since 2012. He is a member CSI since 2011. He has published more than 10 research papers in reputed international journals including Thomson Reuters (ESCI & Web of Science) and conferences including IEEE and it’s also available online. His main research work focuses on Cloud computing, Data mining, Software testing. He has 8 years of teaching experience and 3 years of Research Experience.

Dr.V.K.Jain pursed M. Sc. (Electronics), MBA, M. Tech (CS) and PhD in Computer Science and Engineering from Devi Ahilya University, Indore. He is currently working as Dean of CET-Mody University, Lakshmangarh since 2016. He is a member of IEEE , CSI and ISTD since 2013 .He has published more than 190 research papers and articles in reputed international journals including Thomson Reuters (SCI & Web of Science) and conferences including IEEE and it’s also available online. His main research work focuses on ERP, RFID and EDI Technologies; IT enabled SCM, e- Governance, Software Engineering, Total Quality Management and Research Methodology. He has 22 years of teaching experience and 10 years of Research Experience.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)