Identity-Based Auditing for Shared Cloud Data with Efficient and Secure Image Based Sensitive Information Hiding

D. Dhanya
Associate Professor
Computer Science and Engineering
Mar Ephraem College of Engineering and Technology
Malankara Hills, Marthandam
Tamilnadu, India

Renu D. S
Assistant Professor
Computer Science and Engineering
Mar Ephraem College of Engineering and Technology
Malankara Hills, Marthandam
Tamilnadu, India

Shobhana. S
Assistant Professor
Computer Science and Engineering
Mar Ephraem College of Engineering and Technology
Malankara Hills, Marthandam
Tamilnadu, India

J. Benisha Janice
Assistant Professor
Computer Science and Engineering
Mar Ephraem College of Engineering and Technology
Malankara Hills, Marthandam
Tamilnadu, India

P. Mishma
PG Scholar
Computer Science and Engineering
Mar Ephraem College of Engineering and Technology
Malankara Hills, Marthandam
Tamilnadu, India

***Abstract*:- Remote data integrity auditing is proposed to guarantee the integrity of the data stored in the cloud.Using cloud storage services users could remotely store their data in cloud and access the data in ubiquitous manner. In certain cases, sensitive information's stored in common cloud storage may not be secure while the file from the common cloud is shared. In such cases, Encrypting the whole shared file may lead to sensitive information hiding. The problem still persist and data integrity auditing have still not yet explored completely. An efficient data integrity auditing scheme is proposed that realizes data sharing with image based sensitive information hiding in this project. The scheme is based on the LSB based data hiding algorithm which provides a fixed embedding capacity for images to embed authentication data. The proposed scheme is based on identity-based cryptography, the security analysis and the performance evaluation highly reduce the computation overhead.**

Keywords—Cloud Computing, Data integrity, Identity-based cryptography, Encryption

I. INTRODUCTION

Cloud computing may be a computing paradigm, where an outsized pool of systems are connected privately or public networks, to supply dynamically scalable infrastructure for application, data and file storage. With the advent of this technology, the cost of computation, application hosting, content storage and delivery is reduced significantly. Cloud computing may be a practical approach to experience direct cost benefits and it's the potential to rework a knowledge centre from a capital-intensive found out to a variable priced environment. The idea of cloud computing is predicated on a really fundamental principal of reusability of IT capabilities. The difference that cloud computing brings compared to traditional concepts of "grid computing", "distributed computing", "utility computing", or "autonomic computing" is to broaden organizational boundaries and provide pay per usage that provides more ease to users as well. Cloud computing relies on sharing of resources to realize coherence and economies of scale, almost like a utility over a network. At the inspiration of cloud computing is that the broader concept of converged infrastructure and shared services. The concept of cloud was introduced by Amazon. Amazon was within the business of selling goods and gift items. within the high season like Christmas, many people use to shop for gift items and other goods, therefore the load on their server increases to great extent. So as to run their business smoothly, they increased their server capability. But what about off season, the servers were idle and that they need to be kept running which successively consumes many power and at an equivalent time power was consumed in cooling them. therefore the Amazon decided to hire out their servers within the off season to others, such they will make money out of it.

The objectives of the proposed work is to achieve data sharing with sensitive information hiding in remote data integrity auditing, and propose a new concept called identity-based shared data integrity auditing with sensitive information hiding for secure cloud storage. In such a scheme, the sensitive information can be protected and the other information can be published. It makes the file stored in the cloud able to be shared and used by others on the condition that the sensitive information is protected, while the remote data integrity auditing is still able to be efficiently executed. To design a practical identity-based shared data integrity auditing scheme with sensitive information hiding for secure cloud storage. A sanitizer is used to sanitize the data blocks

corresponding to the sensitive information of the file. In our detailed scheme, firstly, the user blinds the data blocks corresponding to the personal sensitive information of the original file and generates the corresponding signatures, and then sends them to a sanitizer. The sanitizer sanitizes these blinded data blocks into a uniform format and also sanitizes the data blocks corresponding to the organization's sensitive information. It also transforms the corresponding signatures into valid ones for the sanitized file. This method not only realizes the remote data integrity auditing, but also supports the data sharing on the condition that sensitive information is protected in cloud storage. To the best of our knowledge, this is the first scheme with the above functions. Besides, our scheme is based on identity-based cryptography, which simplifies the complex certificate. management. The result shows that the proposed scheme achieves desirable security and efficiency

II. RELATED WORK

Cong Wang et.al [1] presented a survey on cloud secure storage: enabling public auditability for cloud storage is of critical importance so that users can resort to a third-party auditor (TPA) to check the integrity of outsourced data and be worry-free. To securely introduce an effective TPA, the auditing process should bring in no new vulnerabilities towards user data privacy, and introduce no additional online burden to user. A secure cloud storage system is proposed that supports privacy-preserving public auditing.

Kamalam G K et.al [2] proposed a survey on cloud storage: the privacy preserving public auditing mechanism for shared data in the cloud. Ring signatures is utilized to construct homomorphic authenticators, so the TPA is able to audit the integrity of shared data, yet cannot distinguish who is the signer on each block, which can achieve identity privacy. Public auditing for such shared data while preserving identity privacy remains to be an open challenge. Secure and effective methods are utilized to secure integrity and privacy data stored in cloud.

Lei Zhang et.al [3] proposed a survey on shared data on secure data storage. An efficient public auditing solution is used that can preserve the identity privacy and the identity traceability for group members simultaneously. Specifically, a new framework for data sharing in cloud is designed for shared cloud data supporting identity privacy and traceability. A group manager is introduced to help members generate authenticators to protect the identity privacy and two lists are employed to record the members who perform the latest modification on each block to achieve the identity traceability. Besides, the scheme also achieves data privacy during authenticator generation by utilizing blind signature technique.

Boyang et.al [4] projected the first privacy preserving public auditing mechanism for shared data in the cloud. Ring signatures are utilized to construct homomorphic authenticators, so the TPA is able to audit the integrity of shared data, yet cannot distinguish who is the signer on each block, which can achieve identity privacy.

Min G et.al [5] proposed remote data integrity checking (RDIC) that enables a data storage server Complex key management is one of the major issue. A new RDIC protocol is designed by making use of key-homomorphic cryptographic primitive to reduce the complexity and the cost for establishing and managing the public key authentication framework in PKI-based RDIC schemes.

Ravali et.al [6] suggest a key explore resistant in cloud computing. Most of the auditing protocols are based on the assumption that the client's secret key for auditing is secure. The security is not fully achieved, because of the low security parameters of the client. If the auditing protocol is not secured means the data of the client will exposed inevitably. In this paper a new mechanism of cloud auditing is implemented.

Qian Wang et.al [7] proposed storage security in cloud computing. Third party auditor eliminates the involvement of the client through the auditing of whether his data stored in the cloud is intact. Jinyuan Sun et.al [8] suggested across domain data sharing in distributed electronic health record system.Jia Yu et.al [9] suggested strong key exposure resilient auditing for secure storage. Key-exposure resilient auditing for secure cloud storage is designed. Chaowen Guan et.al [10] projected symmetric-key based proofs of retrievability supporting public verification. Proof-of-Retrievability scheme is proposed that provides public verification while the encryption is based on symmetric key primitives.

Sundaraj V et.al [11] projected energy efficient dynamic scheduling hybrid MAC protocol for heavy traffic load in wireless sensor networks. The algorithm helps in reducing the cost of locating optimal selection for the head nodes in the cluster. Vilaplana J et.al [12] proposed a queuing theory model for cloud computing to deliver guaranteed Quality of Service for the success of cloud platforms. Xie J et.al [13] proposed an energy-optimal scheduling for collaborative execution in mobile cloud computing. Storing of tasks in the cloud storage is energy consumed process. A hybrid optimization method based on Hybrid Whale Optimization algorithm(WOA) and Artificial Bee colony optimization algorithm(ABC) is proposed where the efficiency of the proposed scheme is evaluated on the basis of energy consumption, droop rate etc.

Zhang W et.al [14] projected the cloud-assisted collaborative execution for mobile applications with general task topology. MCC-assisted execution of multi-task scheduling problem is investigated in hybrid MCC architecture. Ant Colony optimization algorithm is put forward to tackle this problem, which considers task profit, task deadline, task dependence, node heterogeneity and load balancing. The experimental results shows that the proposed work is more efficient than a few typical existing algorithms. TayalS et.al [15] suggested task scheduling optimization for the cloud computing system. A Multi-objective task scheduling algorithm is proposed of mapping task to a VMs in order to improve the throughput and

reduce the cost without violating the Service Level Agreement.

Xu B et.al [16] proposed dynamic deployment of virtual machines in cloud computing using multi-objective optimization. In this paper, the efficient VM management strategy is proposed for energy saving, increasing profit, and preventing SLA violations. Altamimi M et.al [17] suggested energy cot models of smartphones for task. In this paper task offloading from smartphones to the cloud is proposed to enhance the computing capability of smartphones and to extend there battery life.

A survey is done by Shen W et.al [18] on cloud storage auditing. It allows the user to store their data in cloud ensuring high security. Fu A et.al [19] proposed a new privacy aware public audit scheme for cloud data sharing with group users. To ensure the integrity of the shared data, the third party scheme have been designed. The proposed scheme, homomorphic veritable group signature ensure that group user can trace data changes through designated binary tree and recover the latest correct data block when the current data block is damaged.

Li Y et.al [20] projected fuzzy identity based on data integrity auditing for reliable cloud strong system. Ren K et.al [21] proposed an enabling cloud storage auditing verifiable outsourcing of key update that focus on how to make the key updates as transparent as possible for the client and propose the new scheme called storage auditing with verifiable outsourcing of key update.

Sundaraj, V et.al [22] proposed an optimized denoising scheme via opposition based self-adaptive learning PSO algorithm for algorithm for wavelet based ECG signal noise reduction. Since ECG signal is very challenge task, many researchers have been reported different methods for denoising the ECG signal in recent year. In this paper, an optimized threshold mechanism is proposed for wavelet based medical signal noise reduction.

Wei X et.al [23] proposed an application scheduling in mobile cloud computing with load balancing. In this paper the modern web application is proposed that helps in providing multiple services deployed through complex technologies. Shen W et.al [24] projected light-weight and privacy preserving secure cloud auditing scheme for group user. This scheme helps in reducing computational burden on the user side. Wang B et.al [25] proposed a public auditing for shared data with efficient user revocation in the cloud where the third party auditor is used to store the data and provide authorization the user.

III. PROPOSED MODEL

To efficiently support data sharing with sensitive information hiding in identity-based integrity auditing for secure cloud storage, is proposed. The objective is to improve the correctness:

a) Private key correctness: to ensure that when the PKG sends a correct private key to the user, this private key can pass the verification of the user.

b) The correctness of the blinded file and its corresponding signatures: To guarantee that when the user sends a blinded file and its corresponding valid signatures to the sanitizer, the blinded file and its corresponding signatures he/she generates can pass the verification of the sanitizer.

c) Auditing correctness: To ensure that when the cloud properly stores the user's sanitized data, the proof it generates can pass the verification of the TPA.

d) Sensitive information hiding: To ensure that the personal sensitive information of the file is not exposed to the sanitizer, and all of the sensitive information of the file is not exposed to the cloud and the shared users.

e) Auditing soundness: to assure that if the cloud does not truly store user's intact sanitized data, it cannot pass the TPA's verification.

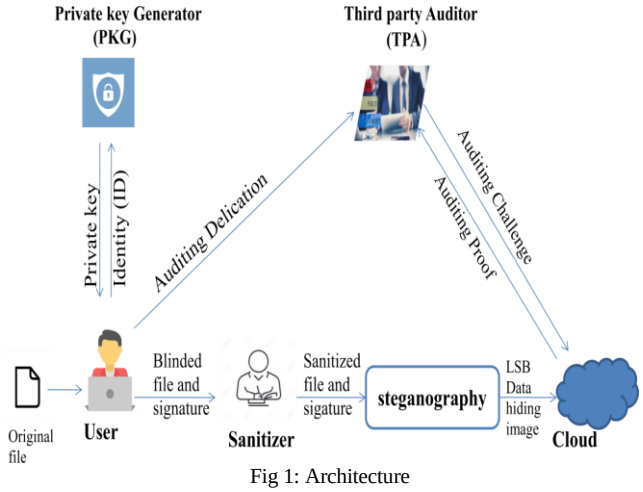

Fig 1: Architecture

To efficiently support data sharing with sensitive information hiding in identity-based integrity auditing for secure cloud storage, is proposed.

In the proposed model, an original file E is divided into n blocks (m1,m2,...,mn), where mi Z p denotes the i-th block of file E. Assume the user's identity ID is l- bit, which is described as ID = (ID1,ID2,...,IDl) $\{0,1\}^l$. A similar identity-based signature Sig is given, to guarantee the integrity of the file identifier name and the correctness of verification values. Signing private key is used to generate file tag in signature Sig that is held by user. Let K1 be the set of indexes of the data blocks corresponding to the personal sensitive information of the file F. Let K2 be the set of indexes of the data blocks corresponding to the organization's sensitive information of the file F. In order to preserve the personal sensitive information of the file from the sanitizer, the data blocks whose indexes are in the set K1 should be blinded before the file is sent to the sanitizer. Assume the blinded file is $F^*=(m_1, m_2,..., m_n)$ which is different from the original file F=(m1,m2,...,mn) in index set K1. The sanitizer needs to sanitize the blinded data blocks. Moreover, to protect the privacy of organization, the sanitizer also needs to sanitize the data blocks that corresponds to the organization's secret

information. The sanitized file is F0=(m0 1,m0 2,...,m0n) which is different from the blinded file F=(m1,m2,...,mn) in index set K1UK2. For example, the sensitive information of the EHRs only contain the fields such as patient's name, patient's ID number and hospital's name. Thus, in EHRs, only these fields containing the sensitive information need to be sanitized, and other fields do not need to be sanitized.

The Steganography system uses an image as the cover. The spatial domain techniques make the changes in the cover-image pixel bit values to embed the secret information. The secret bits are written directly to the cover image pixel bytes. The Least Significant Bit (LSB) is one of the main techniques in spatial domain image Steganography. The LSB is the lowest significant bit in the byte value of the image pixel. The LSB based image steganography embeds the secret in the least significant bits of pixel values of the cover image.

The simplest approach to hiding data within an image file is called least significant bit (LSB) insertion. In this method, we can take the binary representation of the hidden data and overwrite the LSB of each byte within the cover image. If we are using 24-bit colour, the amount of change will be minimal and indiscernible to the human eye. As an example, suppose that we have three adjacent pixels (nine bytes) with the following RGB encoding:

10010101 00001101 11001001
10010110 00001111 11001010
10011111 00010000 11001011

The system model involves five kinds of different entities: the cloud, the user, the sanitizer, the Private Key Generator (PKG) and the Third Party Auditor (TPA), as shown in Fig

1. Cloud: The cloud provides enormous data storage space to the user. Through the cloud storage service, users can upload their data to the cloud and share their data with others.
2. User: The user is a member of an organization, which has a large number of files to be stored in the cloud.
3. Sanitizer: The sanitizer is in charge of sanitizing the data blocks corresponding to the sensitive information (personal sensitive information and the organization's sensitive information) in the file, transforming these data blocks' signatures into valid ones for the sanitized file, and uploading the sanitized file and its corresponding signatures are hidden using stegnography to the cloud.
4. PKG: The PKG is trusted by other entities. It is responsible for generating system public parameters and the private key for the user according to his identity ID.
5. TPA: The TPA is a public verifier. It is in charge of verifying the integrity of the data stored in the cloud on behalf of users

The system model involves five different entities: the cloud, the user, the sanitizer, the Private Key Generator (PKG) and the Third Party Auditor (TPA)

- Cloud Storage
- Setup Phase
- Extract Phase
- Sanitizer Phase
- Stegno Image Phase
- ProofGen Phase
- ProofVerify Phase

The sanitizer is in charge of sanitizing the data blocks corresponding to the sensitive information (personal sensitive information and the organization's sensitive information) in the file, transforming these data blocks' signatures into valid ones for the sanitized file, and uploading the sanitized file and its corresponding signatures to the cloud. Sanitizer is a sensitive information sanitization algorithm run by the sanitizer. It takes as input the blinded file and its signature set. It outputs the sanitized file and its corresponding signature set. The sanitizer checks the validity of the file tag by verifying whether sig is a valid signature

To enhance the security for the data by hiding the signature steganographic technique is used. The signature which is hidden along with the EHR data is sent to the cloud. The receiver applies the steganographic technique to retrieve the message and then verifies the digital signature. Here, steganographic technique is Least Significant Bit embedding technique. This technique can be used for hiding images in 24-bit, 8-bit or gray scale format. In this technique, least significant bit of each pixel is replaced with secret message bit until message end. Data can be hidden in the least significant bits of the cover image and the human eye would be unable to notice the hidden image in the cover file. The TPA verifies the validity of the file tag. The TPA will not execute auditing task if the file tag τ is invalid; otherwise, the TPA parses o obtain file identifier name name and verification values g rID and g r , and then generates an auditing challenge as follows: Randomly picks a set I with c elements, where I [1, n]. Generates a random value vi = Z * p for each i = I. Sends the auditing challenge chal = {i, vi}iI to the cloud. After receiving an auditing challenge from the TPA, the cloud generates a proof of data possession as follows: Computes a linear combination of data blocks λ = P i*I m0 i vi . Calculates an aggregated signature Q σ = iI σ 0 i vi . Outputs an auditing proof P = {λ, σ} to the TPA.

IV. PERFORMNANCE EVALUATION

In this section, the efficiency of the protocol is evaluated. Since the protocol is the only privacy preserving auditing protocol which enables data dynamics. In particular, several simulations are performed to evaluate the efficiency. The cryptographic algorithms are implemented using the pairing-based cryptography (PBC) library. The efficiency of the whole protocol is also dominated by the Audit phase. As mentioned, the TPA only needs to select c file blocks to be checked rather than all the file blocks. In order to achieve the high assurance, the value of c is usually selected to be 300 and 460 for the probability of 95% and 99% respectively.

The above analysis indicates that the protocols are also efficient in the Audit phase. Meanwhile, the TPA needs much less time to verify the response.

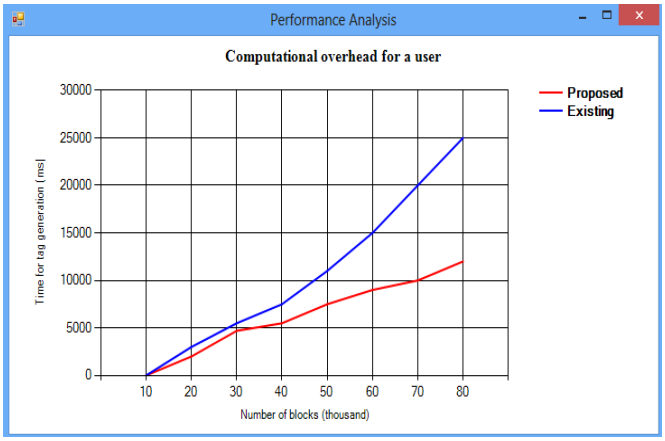

Fig2. Communication overhead

V. CONCLUSION

An identity-based data integrity auditing scheme is proposed for secure cloud storage, which supports data sharing with sensitive information hiding using stegnography. By using stegano-image, makessystems more secure and provides beneficial for applications such as in cooperate world, government sector and for personal use. The file stored in the cloud can be shared and used by others on the condition that the sensitive information of the file is protected. Besides, the remote data integrity auditing is still able to be efficiently executed. The security proof and the experimental analysis demonstrate that the proposed scheme achieves desirable security and efficiency. On future, the cloud storage auditing protocol can be proposed with verifiable outsourcing of key updates.

REFERENCES

[1] Y. Zhang, J. Yu, R. Hao, C. Wang, and K. Ren, "Enabling efficient user revocation in identity-based cloud storage auditing for shared big data," IEEE Transactions on Dependable and Secure Computing,2019

[2] Vinu Sundararaj, Selvi uthukumar, & Kumar, R.S.,"An optimal cluster formation based energy efficient dynamic scheduling hybrid MAC protocol",2Computer Secuirty, 2018.

[3] W. Shen, J. Yu, H. Xia, H. Zhang, X. Lu, and R. Hao, "Light-weight and privacy-preserving secure cloud auditing scheme for group users via the third party medium," Journal of Network and Computer Applications, vol. 82, pp. 56–64, 2017

[4] Sundaraj, V, "Optimized denoising scheme via opposition based self-adaptive learning for wavelet based ECG signal noise reduction". International Journal of Biomedical Engineering and Technology, 1(1), 2017.

[5] Y. Li, Y. Yu, G. Min, W. Susilo, J. Ni, and K. K. R. Choo, "Fuzzy identity- based data integrity auditing for reliable cloud storage systems," IEEE Transactions on Dependable and Secure Computing, 2017

[6] A. Fu, S. Yu, Y. Zhang, H. Wang, and C. Huang, "Npp: A new privacy-aware public auditing scheme for cloud data sharing with group users," IEEE Transactions on Big Data, 2017

[7] J. Yu and H. Wang, "Strong key-exposure resilient auditing for secure cloud storage," IEEE Transactions on Information Forensics and Security, vol. 12, no. 8, pp. 1931–1940, Aug 2017.

[8] Y. Yu, M. H. Au, G. Ateniese, X. Huang, W. Susilo, Y. Dai, and G. Min, "Identity-based remote data integrity checking with perfect data privacy preserving for cloud storage," IEEE Transactions on Information Forensics and Security, vol. 12, no. 4, pp. 767–778, April 2017

[9] J. Yu, K. Ren, and C. Wang, "Enabling cloud storage auditing with verifiable outsourcing of key updates," IEEE Transactions on Information Forensics and Security, vol. 11, no. 6, pp. 1362–1375, June 2016

[10] G. Yang, J. Yu, W. Shen, Q. Su, Z. Fu, and R. Hao, "Enabling public auditing for shared data in cloud storage supporting identity privacy and traceability," J. Syst. Softw., vol. 113, no. C, pp. 130–139, Mar. 2016

[11] B. Wang, B. Li, and H. Li, "Panda: Public auditing for shared data with efficient user revocation in the cloud," IEEE Transactions on Services Computing, vol. 8, no. 1, pp. 92–106, Jan.-Feb. 2015

[12] J. Yu, K. Ren, C. Wang, and V. Varadharajan, "Enabling cloud storage auditing with key-exposure resistance," IEEE Transactions on Information Forensics and Security, vol. 10, no. 6, pp. 1167–1179, 2015

[13] Altamimi, M., Abdrabou, A., Naik, K., & Nayak, A. "Energy cost models of smartphones for task", IEEE Transactions Emerging topics in Computing, 3(3), 384-398, 2015.

[14] Xu, B., Peng, Z., Xiao, F., & Yu, P, "Dynamic deploymaent of virtual machines in cloud computing using multi-objective optimization." Soft computing, 19(8), 2265-2273,2015.

[15] Xie, J., Dan, L., Yin, L., & Sun,Z, "An energy optimal scedulimg for cllabrative execution in mobile computing". In 2015 international conference and workshop on cloud computing and communication(pp.1-6). IEEE, 2015.

[16] C. Guan, K. Ren, F. Zhang, F. Kerschbaum, and J. Yu, "Symmetric-key based proofs of retrievability supporting public verification," in Computer Security– ESORICS 2015. Cham: Springer International Publishing, 2015, pp. 203–223.

[17] Vilaplana, J., Solsona, F., Teixido, I., & ritus,J. "A queuing theory model for cloud computing ". Journal of Supercomputing, 69(1), 492-507, 2015.

[18] Wei, X., Fan, J., & Ding, K, "Application scheduling in mobile cloud computing with load balancing". Journal of Applied Mathematic, 2013.

[19] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for secure cloud storage," IEEE Transactions on Computers, vol. 62, no. 2, pp. 362–375, 2013.

[20] Zhang, W., Wen, Y., & Wu, D."Energy-efficient scheduling policy for collaborative execution in mobile cloud computing", Iin 2013 Proceedings IEEE(pp. 190-194) 2013.

[21] K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69–73, Jan 2012

[22] B. Wang, B. Li, and H. Li, "Oruta: Privacy-preserving public auditing for shared data in the cloud," in 2012 IEEE Fifth International Conference on Cloud Computing, June 2012, pp. 295–302

[23] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling public auditability and data dynamics for storage security in cloud computing," IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 5, pp. 847–859, May 2011

[24] Arivudainambi D, Dhanya D "Scheduling optimized secured virtual machine using cuckoo search and flow analyzer." Journal of computational and Theoretical Nanoscience 14(16),2017.

[25] Arivudainambi D, Dhanya D , "Three phase optimization for qualified and secured VMs for resource allocation". International Journal of Enterprise and Network Management. Inderscience publisher 09(3/4) 273–293, 2018

[26] Arivudainambi D, & Dhanya D, "Towards optimal allocation of resources in cloud modified mapreduce using genetic algorithm."IIOAB JOURNAL, 8(2):162–171, 2017

[27] Tayal, S., "Tasks scheduling optimization for the cloud computing systems", IJAEST-International Journal of advanced Engineering Sciences and Technologies, 1(5), 111-115, 2011.

[28] J. Sun and Y. Fang, "Cross-domain data sharing in distributed electronic health record systems," IEEE Transactions on Parallel and Distributed Systems, vol. 21, no. 6, pp. 754–764, June 2010.

[29] G. Eason, B. Noble, and I. N. Sneddon, “On certain integrals of Lipschitz-Hankel type involving products of Bessel functions,” Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955.

[30] J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[31] I. S. Jacobs and C. P. Bean, “Fine particles, thin films and exchange anisotropy,” in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350

[32] R. Nicole, “Title of paper with only first word capitalized,” J. Name Stand. Abbrev., in press.

[33] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, “Electron spectroscopy studies on magneto-optical media and plastic substrate interface,” IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[34] M. Young, The Technical Writer’s Handbook. Mill Valley, CA: University Science, 1989.