IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

Confidentiality Technique for Enhancing Data Security using Encryption and Obfuscation in Public Cloud Storage

S. Arul Oli[1], Dr. L. Arockiam[2]

Research Scholar, Department of Computer Science St. Joseph's College (Autonomous), Tiruchirappalli, India[1]

Associate Professor, Department of Computer Science, St. Joseph's College (Autonomous), Tiruchirappalli, India[2]

Abstract: Cloud computing with new techniques has become a rapid development in modern technologies. As the importance and usage of cloud demand more access, the problems of cloud security face lot more threats. The problems have caused great influences on the development and popularization of cloud computing. The data storage has become an indispensable part in cloud computing. The data could be either numeric or non-numeric. The data to be stored need to be protected with confidentiality measures. The data must be encrypted before deposited into cloud database. The cryptographic techniques play a vital role in enhancing the security. This paper proposes a technique to store the data of numeric and non-numeric type by obfuscation and encryption methods. This paper also proposes the technique to enhance security level. The paper produces minimum time data size and service while uploading into the cloud storage.

Keywords: Cloud Storage, Obfuscation, Encryption, Cryptography, Confidentiality.

I. INTRODUCTION

Cloud computing proposes new model for computing and its related issues like compute, storage, software. Cloud computing has several customers such as ordinary users, academia, and enterprises who have different motivations and purposes to move over to the cloud. If cloud users are academia, the security and performance of computing and the cloud service providers (CSPs) need to be efficient. Most of the enterprises possess lot of data and they look for a storage space in cloud environment to secure the data. Hence, security plays a vital role in protecting those sensitive data. There are many CSPs who provide the security of data of the users.

In the process of providing security for data, the CSPs develop a tendency to tamper or misuse the sensitive data without the prior knowledge of the users. So, the users are forced to hide the originality of their data before storing into cloud storage. There are many traditional existing cryptographic techniques which help the users to encrypt the data before storing into cloud storage. Every day the demand for these cryptographic techniques increases tremendously. The goal of encryption is to make data unintelligible to unauthorised users and extremely difficult to decipher when attacked. Encryption can provide strong security for data to give sensitive data the highest level of security [1].

The paper proposes a technique to encrypt the data before stored into cloud. The data could be numeric and alphanumeric and alphabetic. In order to protect the security of data, they must be encrypted. This paper proposes encryption technique to encrypt the non-numerical data and obfuscation technique to obfuscate the numerical data. By applying these techniques separately, service cost for processing will take more. Hence the proposed technique combines both the encryption and obfuscation methods to encrypt the data before uploading into cloud. Thus providing the methods, the confidentiality is maintained and the security of data is enhanced. This technique takes minimum time for process and consumes minimum data size. The desired results prove to be satisfactory by applying this technique.

The organisation of this paper is as follows: Section II enumerates the related works relevant to this paper. Section III provides the proposed confidentiality technique of encryption and obfuscation. The section also includes the sample data with expected results of confidentiality, thus enhancing security. Section IV concludes the paper.

II. RELATED WORK

Atiq U.R. Rehman et al. [2] proposed a framework to store sensitive data with a combination of encryption and obfuscation. The cloud users maintained data storage to store keys that are used for encryption. This paper further proposed mechanism to query over encrypted and obfuscated data on server side. Once the required data are filtered on server side, then data are transferred on user's side where de-obfuscation and decryption are performed. The authors [3] presented three approaches such as separating software and infrastructure service providers, hiding data owner's information in cloud and, data obfuscation technique for security. The approach was further presented by Manpreet Kaur et al [4] with two-step encryption process which is used to completely protect the encrypted sensitive data from users to cloud and cloud to users.

Yu et al. [5] proposed one of the first works, which combined ABE, Proxy Re-encryption and lazy encryption schemes for Cloud and security. The scheme works by data owner encrypting his data using a symmetric key and

then encrypting the symmetric key using a set of attributes according to KP-ABE scheme. The data owner determines minimum number of attributes to the new user to access and to update the data with the corresponding secret key. The secret keys of the remaining users will also be updated. Due to the heavy burden of the data owner which may require him to be online at all times to provide key updates, proxy re-encryption is introduced to allow the cloud to carry out these tasks. The data owner's data are kept secure and confidential at all times as the cloud is only exposed to the ciphertext and not the original data contents.

The authors proposed [6] a security policy and procedures to enhance data storage security in cloud. They had a Control Access Data Storage (CADS) to include the necessary policies, processes and control activities for the delivery of each of the data service offerings. The collective control data storage includes the users, processes, and technology to maintain an environment which supports the effectiveness of specific controls and the control frameworks. The effectiveness is guaranteed by providing security policy and procedure for data storage, defence in depth for data storage, correctness verification and error localization computing. These recommendations are only theoretically proposed.

Cunsolo et al. [7] proposed a mechanism to protect data in distributed systems (grid, cloud, autonomic, etc.). This technique consists of the use of combination of symmetric and asymmetric cryptographic algorithms. In this scheme, only data owner can access the data which contradicts the concept of sharing resources in cloud environment. S.Hadi et al. [8] proposed a new related-key impossible differential attack on 7-round AES-128. They attacked 7-round AES-128 with the time complexity of (105), the fastest attack of all the previous ones from time and pre-computation complexities points of views. A fundamental point to construct such attack is to use a special property of mix column operation of AES.

Kazys et al. [9] presented a new version of AES by generating random S-Boxes coinciding with every secret key generation. The authors described in details how to generate random S-Box, key-independent, and ratio of independence. The breach of this study was not debating any type of cryptanalysis attacks. However, contrast to the above studies, the first cryptanalysis was deployed by Alex B. et al. and Bernstein et al. [10] [11]. They evaluated the cost of cryptanalytic attacks on the full AES by using special-purpose hardware in the form of multi-core AES processors. Also, they analysed different time-cost trade-offs and evaluated the implications of progress in VLSI technology under the assumption that Moore's law will continue to hold for the next ten years. These calculations raised some concerns about the long-term security of the AES.

Zhao et al. [12] suggested a progressive elliptic curve encryption scheme (PECE) where a piece of data is encrypted a number of times using multiple keys and later decrypted using one key. This is an effective technique as it keeps data confidential as data are encrypted through the entire stages thus never allowing a malicious user to view the plaintext data. The main problem however with this technique is that it requires the data owner to be online at all times and hence makes it inefficient for everyday users. Attribute-Based Encryption (ABE) is an effective and promising technique that is used to provide fine-grained access control to data in cloud. Initially, access to data in the cloud was provided through Access Control Lists (ACLs). However, this was not scalable and only provided coarse-grained access to data [13]. This ABE was first proposed by Goyal et al. [14] to provide a more scalable and fine-grained access control to data in comparison to ACLs.

Tran et al. [15] used the idea of proxy re-encryption scheme where the data owner's private key is divided into two parts. One half is stored in the data owner's machine while the other is stored in the cloud proxy. The data owner encrypts the data with half of his private key, which then gets encrypted again by the proxy using his other half of the key. Another user who has been granted access rights will then have the same key divided with different parts. One half will be kept on the granted user's machine and the other half stored on the cloud proxy. The user who has access rights can then retrieve the data as the proxy will decrypt the ciphertext with half of the user's private key in the proxy and then decrypt again on the user's side to retrieve the full plaintext. When the data owner wishes to revoke a user from accessingdata, he simply informs the cloud proxy to remove the user's key piece.

As with the PECE scheme described above [16] this scheme doesnot allow outsiders to view the original plaintext at any point as the data remains in an unreadable format in the cloud. Only users with granted access rights can view the original plaintext. The main problem with this scheme is that of collusion attacks. If a revoked user and the proxy collude, then the entire users get access to private key in the group. Also, the proxy may suffer from too many encryption and decryption operations.

III.PROPOSED CONFIDENTIALITY TECHNIQUE

Cloud storage provides an efficient mechanism to store and retrieve the data. Ensuring data security is a prime concern of the user as the user deploys the sensitive data with the CSPs. This paper proposes confidentiality technique to avoid the problem of security issues. The Figure 1 depicts the procedure of data storage of non-numerical and numerical data using encryption and obfuscation technique respectively.

The data to be stored in the cloud environment must be encrypted and obfuscated. By encrypting the non-numerical data and obfuscating the numerical data by single method cause more service cost and consumes time and size. By applying this technique both types of data are converted into unreadable types simultaneously. When this technique is applied by the user, the keys are generated in the cloud side. The keys are sent to the user and the process is done in the user's side.

DOI 10.17148/IJARCCE.2016.5294

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

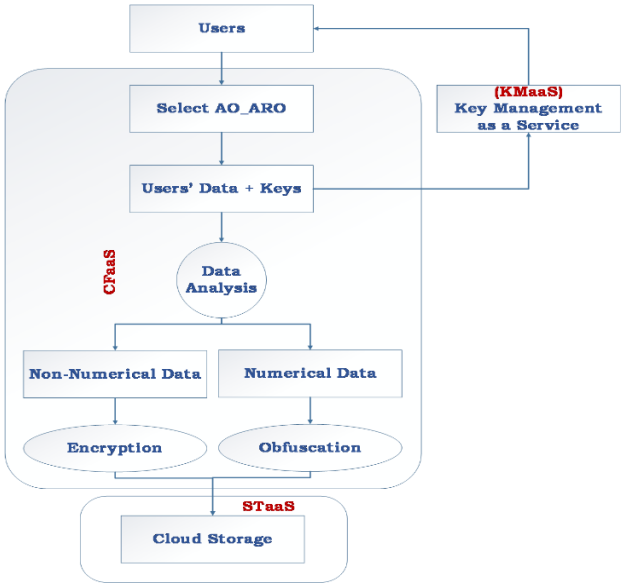

Fig.1. Proposed technique for encryption and obfuscation

Proposed AO_ARO EncObfus CT for CFaaS
The proposed technique is to encrypt the non-numerical and numerical data simultaneously, by applying the proposed algorithm. The algorithm uses both encryption and obfuscation techniques. When the particular technique is selected by the user, it works simultaneously to process both numerical and non-numerical data. The symmetric cryptosystem is used to encrypt the data due to its computational efficiency of handling large volume of data while compared with the asymmetric cryptosystem.

Alorithm #1 is used to find out the type of data to be encrypted and stored in the cloud storage. The data of different types will be applied on this technique by the user. If the data are non-numeric then the encryption technique will be activated. If the data are numeric then the obfuscation technique will be executed for the process. Both the techniques will be executed by call function simultaneously. The data are either encrypted or obfuscated and stored into the cloud storage

Algorithm #1
//Proposed AO_ARO EncObfus CT for CFaaS (Numerical and Non-numerical data)//

1. encry_obfus(PT)
2. start
3. PT←plaintext
4. Ki←keys from KMaaS submitted to the user
5. N←sizeof(PT)
   // Determine the numerical values in num
6. num(i)←isdigits(T(i))

// Determine the non-numerical in non-num

7. nonnum(i)←(!isdigit(T(i)))
8. Execute the encryption procedure for non-numerical valuesThread.encryption_text(nonnum(i),Ki)
9. Execute the obfuscation procedure for numerical valuesThread.obfuscation_digit(num(i),K)
10. Ciphertext(CT) is produced by the simultaneous execution of encryption_text() and obfuscation_digit()
11. End

Algorithm #2 is used for encryption. The algorithm is used for encryption of non-numerical data. The proposed encryption technique is used to protect non-numerical data in the cloud storage. When the user wants to hide only the non-numerical sensitive data, then this proposed encryption becomes very comfortable. This technique is based on symmetric cryptosystem. This algorithm uses three keys for encryption and decryption. Among the three keys two keys are integer and one is string type.

When users decide to protect non-numerical data then the proposed technique [17] is more suitable to them to secure their data in cloud. The proposed technique uses square matrix to manipulate the plaintext and it processes the users' data at three levels. First, the data are split based on even and odd column in the matrix. Second, the Key K1 and K2 are applied on the data alternatively. Third, data are filled in a square matrix in column-wise and read it in row-wise based on the order of characters in key K3. Finally, the ciphertext is produced for submitted plaintext. Decryption is done while reversing the process of encryption steps with same keys.

Algorithm #2
//AO_Enc CT for CFaaS (non-numerical data)//

1. Start
2. Get the Plaintext (PT)
3. Find the size of the Plain text (N)
4. Covert the PT into ASCII code
5. Form a square based on N
6. Fill the SM [R] [c]by PT from left to right
7. Split the matrix into two blocks
   EB → Even column
   OB → Odd Column
8. Merge the EB and OB
9. Generate k1 and k2
10. Form a matrix by column in k3
11. Fill matrix by column by column
12. Read the matrix by row in order of k3 (AS)
13. Convert AS into ASCII character
14. Get the cipher text
15. End

Algorithm #3 is proposed for obfuscation technique to protect the numerical data in cloud storage. When the user wants to encrypt the sensitive numerical data by obfuscation, then this proposed technique is suitable and convenient. This technique is a symmetric cryptosystem. There are two keys used in this proposed algorithm for encryption. And both the keys are of integer values. With these two keys, the obfuscation of numerical data is possible for protecting the data in public cloud.

The proposed technique [18] uses five different mathematical operations such as mul(), pow(), rotate(), mod(), ascii() on numerical data. The two secret keys are generated in cloud side and forwarded to the users. The size of the given plain text is calculated for obfuscation technique. The plain text is multiplied with the sample value of K1 and deposited in the array. The square value is calculated for the multiplied value. The sample generated K2 is incremented by one and put into the square values.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

These values are rotated from left to right for each time for K2 times. In the next step, the mod value is found out by dividing 256. The ascii character is derived for each mod value. These ASCII values are the equivalent cipher text for the plaint text. These keys are maintained in the service provider called Key Management as a Service. (KMaaS). The entire work and result is compared with the existing techniques like Base32, Base64 and Hexadecimal Encoding.

Algorithm #3

//Proposed ARO_Obfus CT for CFaaS (numerical data)//

1. Users submit the plaintext (PT) and keys (K_i)
2. Determine the numerical values in the PT.
3. Find the number of values in the N=sizeof(PT)
4. Generate a key K_1 from cloud for ARO_Obfus CT
5. Find the Product(MT) of K_1 and PT
6. Calculate the square (SQ) for each value in the MT, SQ=square(MT).
7. Generate a key $K_2$from cloud for ARO_Obfus CT
8. Rotate SQ at K_2 number of times, K_2 is incremented by 1 for consecutive value in the SQ.

Rotation_SQ (RTN) = $R_{K+j}{}^{(SQ)}$ j = 1,2,…<N

//(R denotes Rotation)

9. Calculate modulus (MOD) for RTN by 256, MOD=RTN%256
10. Convert the MOD into ASCII code to produce ciphertext (CT).

For better understanding of the proposed cryptographic technique, sample transactions of students' details are considered as shown in Table 1. The data in Table 1 are the plaintext before being encrypted and obfuscated. The proposed technique is utilized to encrypt and obfuscate the data before stored into the cloud storage.

TABLE 1 Transactional Table with plain text

Reg. No	Name	M 1	M 2	M 3	Total	Grade
13UCS101	Stephen	60	92	72	224	B
13UCS102	Dalwin	59	96	56	211	C
13UCS103	Thivya	86	49	87	222	B
13UCS104	Raja	45	65	68	178	D
13UCS105	Rani	66	59	86	211	C
13UCS106	Carol	87	93	46	226	A

Proposed cryptographic technique is implemented in JAVA running in windows 7 operating system. As the proposed algorithm #1 is executed, the encryption algorithm #2 is called and the non-numerical data are encrypted in the Table 1. Table 2 represents the encryption of non-numerical data of the students by applying Algorithm #2, where the numerical data remain the same.

As the proposed algorithm #1 is executed, it invokes the proposed algorithm #3 for the obfuscation of numerical data in the Table 1.

TABLE 1I Transactional Table with text after Encryption

&^% $NJP	(*&	!*^	$%	+?>	<^%	!@^%
Ki*&^	#)(&	*&^	)#*	<o(	!+^	(*&
)((#% $	Mk& H	&^$	&^ %	?!(	&^%	$)&
MKJ$ #	J)(#	?>U	*Mj	~&?	$nK	#N)
)(*#!l	%N":	J7H	)><	^H %	?*%	?#C
NI(*$	@(^%	)$(	$*^	&^ %	#)%	G&%
+?<":	nH%! 0	&#B	!)(	(@*	*&^	H&#

Now the algorithm #3 is executed to obfuscate the numerical data and the data are shown as in Table 3. Hence Table 3 shows the data after encryption and obfuscation process. The data are stored in the cloud storage.

Table III Transactional Table with text after encryption and obfuscation

&^%$NJ P	(*&	!*^	$%	+?>	<^ %	!@ ^%
Ki*&^	#)(&	*& ^	)#*	<o(	!+^	(*&
)((#%$	Mk& H	&^ $	&^ %	?!(	&^ %	$)&
MKJ$#	J)(#	?> U	*Mj	~& ?	$nK	#N)
)(*#!l	%N":	J7H	)><	^H %	?*%	?#C
NI(*$	@(^ %	)$(	$*^	&^ %	#)%	G& %
+?<":	nH%! 0	&# B	!)(	(@*	*&^	H& #

From the observation of the above three tables, it is shown that combination of encryption and obfuscation is possible at simultaneous process and it gives more security to the data stored in the cloud storage. The proposed technique gives better results of minimum data size, produces minimum process time, and minimum service cost. The proposed technique produces better security since it encrypts and obfuscates the data. Supposing a hacker tries to tamper or retrieve the data from the table. By decrypting the non-numerical data alone, the hacker will not achieve his goal, Or by de-obfuscating the numerical data alone, it is of no use for the hacker. Hacker will not fulfil his malicious attacks by partially hacking the data. Hence the proposed technique is proved to be better in security.

IV. CONCLUSION

With modern scientific advancements, cloud computing is a technology of rapid development. However, the security problems have become obstacles to make the cloud computing more popular. Various existing techniques are utilized to solve these security problems. This paper

proposed a technique to protect the confidentiality of data of numeric and non-numeric data by obfuscation and encryption. Encryption of non-numeric data alone will not provide security. In the same way, obfuscation of numerical data alone will not provide security to the stored data. So, the encryption and obfuscation process are needed for confidentiality of data. Both these techniques are processed simultaneously in order maintain confidentiality. The proposed technique also reduced the service cost, minimized the data size and process time while uploading into the cloud storage. This technique put forward a series of solutions for the present security problems that cloud computing meet. This technique proved to be better in providing confidentiality of data stored in the cloud storage. Hence security is enhanced.

ACKNOWLEDGMENT

Wish to acknowledge and thank **Dr. S. S. Manikandasaran**, Dean and Professor, Christhuraj Institute of computer Application, Christhu Raj College, Trichy for guiding me to publish this paper.

REFERENCES

[1] Dr. L. Arockiam,S. Monikandan, "Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm", International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), Volume 2, Issue 8, ISSN : 2278-1021, August 2013, pp. 3064-3070.

[2] Atiq U R Rehman, and M. Hussain, "Efficient cloud data confidentiality for DaaS", International Journal of Advanced Science and Technology, Vol. 35, 2011, pp. 1-10.

[3] [Yau SS, An HG, "Confidentiality protection in cloud computing systems", International Journal Software Informatics, Vol. 4, Issue 4, 2010, pp. 351-365.

[4] ManpreetKaur and Rajbir Singh, "Implementing Encryption Algorithms to Enhance Data Security of Cloud in Cloud Computing", International Journal of Computer Applications, Vol. 70, Issue 18, 2013, pp. 16-21.

[5] Yu S, Wang C, Ren K, Lou W, "Achieving secure, scalable, and fine-grained data access control in cloud computing", In: INFOCOM, 2010 proceedings IEEE, pp. 1–9.

[6] Nashaat el-Khameesy, Hossam Abdel Rahman, "A Proposed Model for Enhancing Data Storage Security in Cloud Computing Systems", Journal of Emerging Trends in Computing and Information Sciences, Volume 3, Issue 6, 2012, pp. 970-974.

[7] V. D. Cunsolo, S. Distefano, A. Puliafito, and M. Scarpa, "Achieving information security in network computing systems", Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing (DASC'09.), 2009, pp. 71-77.

[8] Hadi, S., Alireza, S., Behnam, B. and Mohammadraze, A., "Cryptanalysis of 7-Round AES-128", International Journal of Computer Application, 10, 2013, pp. 21-29.

[9] Kazys, A. and Janus, K., "Key-Dependent S-Box Generation in AES Block Cipher System. Informatica"20, 2012, pp. 23-34.

[10] Alex, B. and Johann, G., "Cryptanalysis of the Full AES Using GPU-Like Special-Purpose Hardware, Journal Fundamental Informatics—Cryptology in Progress", 10th Central European Conference on Cryptology, 10-12, 2010, Vol. 114, pp. 221-237.

[11] Bernstein, D., Chen, H., Chen, M., Cheng, C., Hsiao, C. and Lange, T., "The Billion-Mulmod-Per-Second PC", In SHARCS '09: Special-Purpose Hardware for Attacking Cryptographic Systems, Lausanne, 2009, pp. 131-144.

[12] Zhao G, Rong C, Li J, Zhang F, Tang Y, "Trusted data sharing over untrusted cloud storage providers", IEEE second international conference cloud computing technology and science (CloudCom) 2010, pp 97–103.

[13] Li J, Zhao G, Chen X, Xie D, Rong C, Li W, Tang L, Tang Y, "Fine-grained data access control systems with user accountability in cloud computing", IEEE second international conference on cloud computing technology and science (CloudCom) 2010, pp. 89–96.

[14] Goyal V, Pandey O, Sahai A, Waters B, "Attribute-based encryption for fine-grained access control of encrypted data", 13th ACM conference on computer and communications security (CCS '06) 2006, pp. 89–98.

[15] Tran DH, Nguyen HL, Zha W, Ng WK, "Towards security in sharing data on cloudbased social networks", 8th International conference on information, communications and signal processing (ICICS) 2011, pp. 1–5.

[16] Zhao G, Rong C, Li J, Zhang F, Tang Y, "Trusted data sharing over untrusted cloud storage providers", IEEE second international conference cloud computing technology and science (CloudCom) 2010, pp. 97–103.

[17] S. Arul Oli and L. Arockiam, "Confidentiality Technique for Data Stored in Public Cloud Storage", International Journal of Engineering Research and Technology (IJERT), Vol. 5, Issue 2, 2016, ISSN: 2278-0181,pp. 44-48.

[18] S. Arul Oli and L. Arockiam, "Confidentiality Technique using Data Obfuscation to Enhance Security of Stored Data in Public Cloud Storage", International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE), Vol. 5. Issue 1, 2016, ISSN: 2278-909X, pp. 169-174.

[19] Dr. L. Arockiam, S. Monikandan, G.Parthasarathy "Cloud Computing: A Survey", International Journal of Internet Computing, Vol. 1, Issue 2, ISSN: 2231 – 6965, 2011, pp. 26-33.

BIOGRAPHIES

S. Arul Oli received his Master's in Computer Science from Bharathidasan University, Tiruchirappalli, India. Currently, he is a Ph.D. research scholar in the Department of Computer Science at St. Joseph's College (Autonomous), Tiruchirappalli affiliated to Bharathidasan University, India. He has published Research Papers in International Journals with Impact Factor. His main area of research is Cloud Computing. He has attended several National and International Conferences and workshops.

Dr. L. Arockiam is working as Associate Professor in the Department of Computer Science, St. Joseph's College, Tiruchirappalli, Tamil Nadu, India. He has 26 years of experience in teaching and 18 years of experience in research. He has published more than 235 research articles in the International & National Conferences and Journals. He has also presented 3 research articles in the Software Measurement European Forum in Rome, Bali and Malaysia. He is also the Member of IEEE, Madras Section. He has chaired many technical sessions and delivered invited talks in National and International Conferences. He has Co-authored 5 books. His research interests are: Cloud Computing, Big Data, Cognitive Aspects in Programming, Data Mining and Mobile Networks. He has been awarded "Best Research Publications in Science" for 2009, 2010, 2011 & 2015 and ASDF Global "Best Academic Researcher" Award from ASDF, Pondicherry for the academic year 2012-13 and also the "Best Teacher in College" award for the year 2013 & 2014.

DOI 10.17148/IJARCCE.2016.5294