ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2015

Confidential Data Sharing in Cloud using Anonymous Assignment Key

Pravin B. More[1], Yogesh B. Amane[2]

Assistant Professor, Dept. of CSE/IT, Adarsh Institute of Technology and Research Center, Vita (Maharashtra), India[1,2]

ABSTRACT: An algorithm for anonymous sharing of confidential data among parties is developed. This technique is used iteratively to assign these nodes key numbers ranging from 1 to N. This assignment is anonymous in that the identities received are unknown to the other members of the group. Resistance to collusion among other members is verified in an information theoretic sense when confidential communication channels are used. This assignment of serial numbers allows more complex data to be shared and has applications to other problems in confidential data mining, collision avoidance in communications and distributed database access. The required computations are distributed without using a trusted central authority.

Existing and new algorithms for assigning anonymous keys are examined with respect to trade-offs between communication and computational requirements. The new algorithms are built on top of a secure sum data mining operation using Newton's identities and Sturm's theorem. An algorithm for distributed solution of certain polynomials over finite fields enhances the scalability of the algorithms. Markov chain representations are used to find statistics on the number of iterations required, and computer algebra gives closed form results for the completion rates.

KEYWORDS: Anonymization and deanonymization cloud and distributed computing systems, multiparty computation, confidential data mining, confidential protection, security and trust in cooperative communications.

I. INTRODUCTION

The popularity of internet as a communication medium whether for personal or business use depends in part on its support for anonymous communication. Businesses also have legitimate reasons to engage in anonymous communication and avoid the consequences of identity revelation. For example, to allow dissemination of summary data without revealing the identity key of the entity the underlying data is associated with, or to protect whistle-blower's right to be anonymous and free from political or economic retributions. Cloud-based website management tools provide capabilities for a server to anonymously capture the visitor's web actions. The problem of sharing confidentially held data so that the individuals who are the subjects of the data cannot be identified has been researched extensively. Researchers have also investigated the relevance of anonymity and/or confidential in various application domains: The associate editor coordinating the review of this patient medical records, electronic voting, e-mail, social networking, etc. Another form of anonymity, as used in secure multiparty computation, allows multiple parties on a network to jointly carry out a global computation that depends on data from each party while the data held by each party remains unknown to the other parties. A secure computation function widely used in the literature is secure sum that allows parties to compute the sum of their individual inputs without disclosing the inputs to one another. This function is popular in data mining applications and also helps characterize the complexities of the secure multiparty computation.

This work deals with efficient algorithms for assigning identifiers (Keys) to the nodes of a network in such a way that the Keys are anonymous using a distributed computation with no central authority. Given nodes, this assignment is essentially a permutation of the integers with each Key being known only to the node to which it is assigned. Our main algorithm is based on a method for anonymously sharing simple data and results in methods for efficient sharing of complex data. There are many applications that require dynamic unique Keys for network nodes. Such Keys can be used as part of schemes for sharing/dividing communications bandwidth, data storage, and other resources anonymously and without conflict. The Keys are needed in sensor networks for security or for administrative tasks

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2015

requiring reliability, such as configuration and monitoring of individual nodes, and download of binary code or data aggregation descriptions to these nodes. An application where Keys need to be anonymous is grid computing where one may seek services without divulging the identity of the service requestor.

II . LITERATURE SURVEY

Q. Xie and U. Hengartner proposed an algorithm based upon permutations and substitutions. That algorithm supports fixed key size approach to secure the data. It is Specification for Advanced encryption standard provides the whole mechanism for encryption algorithm for which Rijmen provided the concept of AES. It mainly specifies the Rijndael algorithm a symmetric block cipher that can process data blocks of 128 bits, by using cipher keys. However, the lengths of Rijndael, which are required to handle additional key lengths and block sizes, are not adopted in this following standard.

This Algorithm provides flexibility to user to choose different key sizes. By using this algorithm throughput increases with increase in frequency level but the processing time is reduced at high frequency level. In this algorithm round time is the function of processing time so with frequency it also reduces. In this Rijndael provides a security equivalent to RSA of 3072 bit key and also overcome the drawbacks of DES and TDES. It is also concluded that if the throughput is increased then the same algorithm can be implemented on optical networks.

III. EXISTING SYSTEM

A secure computation function widely used in the literature is secure sum that allows parties to compute the sum of their individual inputs without disclosing the inputs to one another. This function is popular in data mining applications and also helps characterize the complexities of the secure multiparty computation. Existing and new algorithms for assigning anonymous IDs are examined with respect to trade-offs between communication and computational requirements.. Also, suppose that access to the database is strictly controlled, because data are used for certain experiments that need to be maintained confidential. Clearly, allowing Alice to directly read the contents of the tuple breaks the privacy of Bob; on the other hand, the confidentiality of the database managed by Alice is violated once Bob has access to the contents of the database. Thus, the problem is to check whether the database inserted with the tuple is still k-anonymous, without letting Alice and Bob know the contents of the tuple and the database respectively.

DISADVANTAGES OF EXISTING SYSTEM:

The algorithms for mental poker are more complex and utilize cryptographic methods as players must, in general, be able to prove that they held the winning hand. Throughout this paper, we assume that the participants are semi-honest, also known as passive or honest-but-curious, and execute their required protocols faithfully. Given a semi-honest, reliable, and trusted third party, a permutation can also be created using an anonymous routing protocol and The database with the tuple data does not be maintained confidentially.

IV. PROPOSED SYSTEM

This work deals with efficient algorithms for assigning key identifiers (keys) to the nodes of a network in such a way that the Keys are anonymous using a distributed computation with no central authority. Given N nodes, this assignment is essentially a permutation of the integers {1,…..N} with each key being known only to the node to which it is assigned. Our main algorithm is based on a method for anonymously sharing simple data and results in methods for efficient sharing of complicated data. Despite the differences cited, the reader should consult and consider the alternative algorithms mentioned above before implementing the algorithms in this paper. This paper builds an algorithm for sharing simple integer data on top of secure sum. The sharing algorithm will be used at each iteration of the algorithm for anonymous Key assignment (AKA). This AKA algorithm, and the variants that we discuss, can require a variable and unbounded number of iterations. The work reported in this paper further explores the connection between sharing secrets in an anonymous manner, distributed secure multiparty computation and anonymous Key assignment. The use of the term “anonymous” here differs from its meaning in research dealing with symmetry breaking and leader election in anonymous networks. Our network is not anonymous and the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2015

participants are identifiable in that they are known to and can be addressed by the others. Methods for assigning and using sets of pseudonyms have been developed for anonymous communication in mobile networks. The methods developed in these works generally require a trusted administrator, as written, and their end products generally differ from ours in form and/or in statistical properties.

ADVANTAGES OF PROPOSED SYSTEM:

Increasing a parameter in the algorithm will reduce the number of expected rounds. However, our central algorithm requires solving a polynomial with coefficients taken from a finite field of integers modulo a prime. That task restricts the level to which can be practically raised. We show in detail how to obtain the average number of required rounds, and in the Appendix detail a method for solving the polynomial, which can be distributed among the participants.

Modules:

1. Homomorphic encryption Module.
2. Generalization Module.
3. Cryptography Module.
4. User and Admin Module.

1. Homomorphic encryption Module:

This module to use the first protocol is aimed at suppression-based anonymous databases, and it allows the owner of DB to properly anonymize the tuple t, without gaining any useful knowledge on its contents and without having to send to it's owner newly generated data. To achieve such goal, the parties secure their messages by encrypting them. In order to perform the privacy-preserving verification of the database anonymity upon the insertion, the parties use a commutative and homomorphic encryption scheme.

System Architecture:

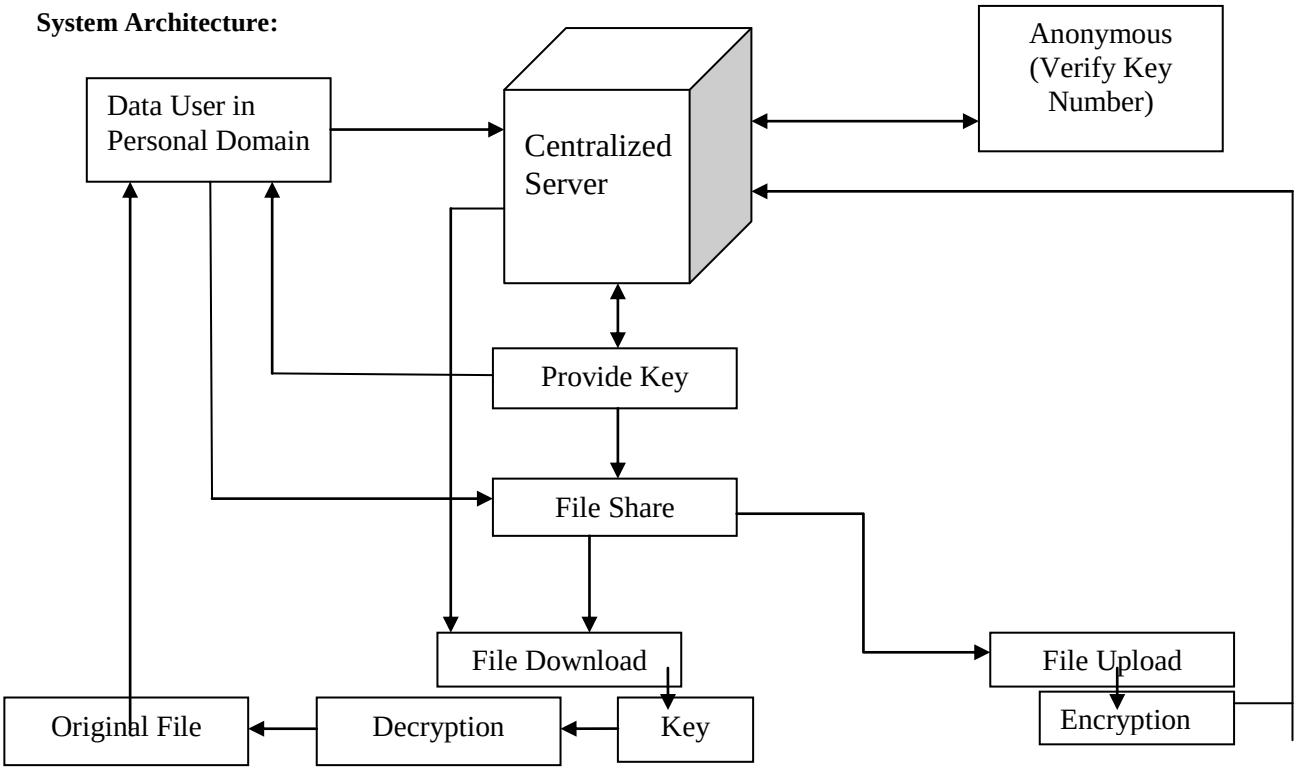

Fig 1: System Architecture

2. Generalization Module:

In this module, the second protocol is aimed at generalization-based anonymous databases, and it relies on a secure set intersection protocol, such as the one found in, to support privacy-preserving updates on a generalization based k-anonymous DB.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2015

3. Cryptography Module:

In this module, the process of converting ordinary information called plaintext into unintelligible gibberish called cipher text. Decryption is the reverse, in other words, moving from the unintelligible cipher text back to plaintext. A cipher (or) cypher is a pair of algorithms that create the encryption and the reversing decryption. The detailed operation of a cipher is controlled both by the algorithm and in each instance by a key. This is a secret parameter (ideally known only to the communicants) for a specific message exchange context.

4. User and Admin Module:

In this module, to arrange the database based on the patient and doctor details are recorded. The admin encrypts the patient reports using encryption techniques using suppression and generalization protocols.

Fig 1 Shows the System Architecture for Confidential Data Sharing in Cloud. When the data user in the personal domain wants to access the information he can make use of key provided by the centralized server. The user uses that key to decrypt the data. There is an anonymous user which verifies the key generated by the server. User can download the file that is uploaded by the other user and he can easily decrypt the data using the key provided by the server. File is uploaded to the server in the encrypted form. No other user can see the contents of file or he will not be able to download that file. After decryption user gets the original file.

V. RELATED WORK

To differentiate anonymous key assignment from anonymous communication, consider a situation where parties wish to display their data collectively, but anonymously, in slots on a third party site. The Keys can be used to assign the slots to users, while anonymous communication can allow the parties to conceal their identities from the third party. In another application, it is possible to use secure sum to allow one to opt-out of a computation beforehand on the basis of certain rules in statistical disclosure limitation or during a computation and even to do so in an anonymous manner. However, very little is known with respect to methods allowing agencies to opt-out of a secure computation based on the results of the analysis, should they feel that those results are too in for- motive about their data. The work reported in this paper further explores the con- section between sharing secrets in an anonymous manner, distributed secure multiparty computation and anonymous key assignment. The use of the term “anonymous” here differs from its meaning in research dealing with symmetry breaking and leader election in anonymous networks. Our network is not anonymous and the participants are identifiable in that they are known to and can be addressed by the others. Methods for assigning and using sets of pseudonyms have been developed for anonymous communication in mobile net- works . The methods developed in these works generally require a trusted administrator, as written, and their end products generally differ from ours in form and/or in statistical properties. To be precise, with nodes the algorithms of this paper distribute a computation among the nodes generating a permutation of chosen with a uniform probability of from the set of all permutations of where will know only. Such a permutation can also be produced by algorithms designed for mental poker. The algorithms for mental poker are more complex and utilize cryptographic methods as players must, in general, be able to prove that they held the winning hand. Throughout this paper, we assume that the participants are semi honest also known as passive or honest-but-curious, and execute their required protocols faithfully. Given a semi honest, reliable, and trusted third party, a permutation can also be created using an anonymous routing protocol. Despite the differences cited, the reader should consult and consider the alternative algorithms mentioned above before implementing the algorithms in this paper. This paper builds an algorithm for sharing simple integer data on top of secure sum. The sharing algorithm will be used at each iteration of the algorithm for anonymous Key assignment (AKA). This AKA algorithm and the variants that we discuss, can require a variable and unbounded number of iterations. Finitely-bounded algorithms for AKA are discussed in Section IX. Increasing a parameter in the algorithm will reduce the number of expected rounds. However, our central algorithm requires solving a polynomial with coefficients taken from a finite field of in tegers modulo a prime. That task restricts the level to which can be practically raised. We show in detail how to obtain the average number of required rounds, and in the Appendix detail a method for solving the polynomial, which can be distributed among the participants

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2015

VI. A SECURE SUM OF DATA ALGORITHM

Given nodes m1…….mN each holding a data item ti from a finitely represent able abelian group, allocate the value K = Σti between the nodes without revealing the values ti. Each node mi, i = 1 …N selects random values si,1……si,N such that si1,+…..+si,N= ti. Each random value si,j is conveyed from node mi to node mj . The sum of all these random numbers si,j, is the desired total K. Each node mj totals all the random values received as vj = s1,j+…..+sN,j. Each node mi merely broadcasts vi to all other nodes so that each node can compute: K = v1 +…..+vN. In the given **Fig 2**, the initial data items held by nodes m1, m2, m3 and m4 are t1=6, t2= 8, t3=6, t4=2 correspondingly. Node m2 would transmit 6, 2, -4, and 4 to nodes m1, m2, m3 and m4 respectively. Node m2 would receive -9, 2, 10, and -7 from nodes m1, m2, m3 and m4 respectively. Then node m2 would work out and broadcast the total v2 = -4 of the values received to all nodes. Finally, m2 would compute the total of all the second round transmissions received 22=16+-4+8+2.
The opportunity that more complicated data is to be shared among the participating nodes is to be considered. Each node mi has a data item ti of length u-bits which it wishes to put together it public anonymously to other participants. As the number of nodes and the bits per data item becomes larger, to accomplish this sharing, an indexing of the nodes was utilized as an alternative. Considering that each node mi has a unique identification number vi ϵ {1, 2…..N} and

Nodes	Si,1	Si,2	Si,3	Si,4	ti
mi=1	12	-9	5	-2	6
mi=2	6	2	-4	4	8
mi=3	-7	10	11	-8	6
mi=4	5	-7	-4	8	2
Vi=	16	-4	8	2	K=22

Fig 2: A Secure Sum Execution Transmitting The Random Number

additionally, assume that no node has knowledge of the unique identification number vi of any other node, and that v1…..vN are a random permutation of 1,…N ., and is termed an Anonymous Key Assignment and may possibly be used to allocate slots with reverence to time or space for storage or communications It may be promising to minimally have a database by means of central storage locations Ei such that each node merely stores its data there setting Evi :=ti. A simple algorithm was presented for finding an AKA which has quite a few variants depending on the selection of the data sharing method. Random integers or slots between 1 and P are chosen by each node at one step. The position of the node will be determined by means of its position among the selected slots; however provisions must be prepared for collisions. The parameter should be selected so that P ≥N. The technique of confidential data sharing of Anonymous Data Sharing with Power Sums is challenging to the collusion of any subset of the participating nodes while based on the secure sum Algorithm. For the reason that the input data is present as a multi set in the output of each party and all parties are semi-honest the consequence is implied by the secure sum Algorithm. The data sharing is anonymous in the intellect that the sources of the data items cannot be traced. Certainly, it is potential that a given data value would make logic only for a definite participant due to several factors such as the participants relative sizes.

VII. THE ALGORITHM TO FIND AN AKA

In this algorithm It requires the random numbers be shared anonymously and we consider three methods which are variants of that procedure and require the parameter P in each case. The expected numbers of rounds rely simply on the selection of P and not on the variant selected. In the slot selection method the variant of the algorithm has its main negative aspect as the very long message lengths that are encountered while using large P to maintain the number of expected rounds small. In the Prime Modulus AKA: A prime R > P is chosen. In general, R will be chosen as small as potential subject to this restriction. This variant will be seen to outcome in shorter message lengths intended for communication among nodes. Again, the computation necessary to find the roots of the Newton polynomial can be delayed and consequently overlaps any supplementary required rounds. It is probable to keep away from solution of the Newton polynomial completely. Sturm's theorem permits the determination of the number of roots of a real polynomial q(x) in an interval (g, h) based on the signs of the values of a sequence of polynomials derived from q(x). The succession of polynomials is attained from a variant of the Euclidean Algorithm. By means of Sturm's theorem is not at

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2015

Present reasonable with the variety of methods of polynomial solution using the prime modulus method and runs twice as slow at best. The application of Sturm's theorem necessitates usage of an ordered field resulting in large polynomial coefficients.

VIII. PROPOSED ALGORITHM

This paper builds an algorithm for sharing simple integer data on top of secure sum. The sharing algorithm will be used at each iteration of the algorithm for anonymous Key assignment (AKA). This AKA algorithm, and the variants that we discuss, can require a variable and unbounded number of iterations. Increasing a parameter in the algorithm will reduce the number of expected rounds. However, our central algorithm requires solving a polynomial with coefficients taken from a finite field of integers modulo a prime. That task restricts the level to which can be practically raised.

Sturm's Theorem:
The usage of secure multiparty computation is being avoided with the usage of Sturm's theorem to make sure that the information about the nodes are not revealed. In the current system the main goal is to provide anonymous key for each node. Each node will have a secure communication of simple and complicated data. Those data's may be from static data or dynamic data. By implementing secure sum hides permutations method and anonymous key assignment (AKA) method the permutation methods are kept anonymous to each other.

Sturm's Theorem AKA
It is possible to avoid solution of the Newton polynomial entirely. Sturm's theorem allows the determination of the number of roots of a real polynomial p(x) in an interval (a, b) based on the signs of the values of a sequence of polynomials derived from p(x). The sequence of polynomials is obtained from a variant of the Euclidean Algorithm. As in the previous variant, the power sums are collected and the Newton Polynomial is formed. However, the field used for computation is the field of rational numbers Q. The test p′(ri)=0 is again sufficient to determine whether or not ni has received. There is a computational advantage which is arises in that nodes which do not need to solve the Newton polynomial p(x) to determine the (now implicitly) shared values. Assume that x=0 is not a root of p(x) as xk has been factored out immediately if applicable. Each node ni which has received an assignment must count separately multiple roots and also forms g(x)=gcd(p(x), p′(x)). A multiple roots version of Sturm's theorem is then applied to calculate the number of roots for the polynomial p(x) in the range (0,ri). (Note that ri itself is not a multiple root allowing application of the theorem). The polynomial g(x)=gcd(p(x),p′(x)) is a byproduct of this computation. The same Sturm procedure is applied to g(x) thus obtaining a count of the multiple roots in the same range,(0,ri). The collected power sums Pi are integers. To guarantee the privacy and the compute sums using a field GF (P) with P greater than any possible value of Pi. Our timings showed that using Sturm's theorem is not currently competitive with the various methods of polynomial solution using the "prime modulus" approach and runs twice as slow as best. Although, the construction is straight forward. The application of Sturm's theorem requires the use of an ordered field resulting in the large polynomial coefficients. Unfortunately, the analog of this result which is usable for a finite field of the corresponding polynomial coefficient. Still, some results in this direction are available.

IX. CONCLUSION AND FUTURE WORK

The required computations are distributed without using a trusted central authority. Any person can be use private communication channel then access the database. The algorithms for assigning the anonymous key is examined by the trade-offs between the requirements of communication and computations. The new algorithms are built on top of a secure sum data mining operation using Newton's identities and Sturm's theorem. An algorithm for the distributed solution of certain polynomials over finite field will enhances the scalability of the algorithms.

REFERENCES

1. Shamir, "How to share a secret," Commun. ACM, vol. 22, no. 11, pp. 612–613, 1979.
2. Friedman, R. Wolff, and A. Schuster, "Providing k-anonymity in data mining," VLDB Journal, vol. 17, no. 4, pp. 789–804, Jul. 2008.
3. F. Baiardi, A. Falleni, R. Granchi, F. Martinelli, M. Petrocchi, and A. Vaccarelli, "Seas, a secure e-voting protocol: Design and implementation,"Comput. Security, vol. 24, no. 8, pp. 642–652, Nov. 2005.
4. D. Chaum, "Untraceable electronic mail, return address and digital pseudonyms," Commun. ACM, vol. 24, no. 2, pp. 84–88, Feb. 1981.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2015

5. Q. Xie and U. Hengartner, "Privacy-preserving matchmaking for mobile social networking secure against malicious users," in Proc. 9th Ann. IEEE Conf. Privacy, Security and Trust, Jul. 2011, pp. 252–259.
6. O. Goldreich, S. Micali, and A. Wigderson, "How to play any mental game," in Proc. 19th Ann. ACM Conf. Theory of Computing, Jan. 1987
7. A. Yao, "Protocols for secure computations," in Proc. 23rd Ann. IEEESymp. Foundations of Computer Science, pp. 160–164, IEEE Computer Society, 1982.
8. A. Clifton, M. Kantarcioglu, J. Vaidya, X. Lin, and M. Y. Zhu, "Tools for privacy preserving distributed data mining," ACM SIGKDD ExplorationsNewsletter, vol. 4, no. 2, pp. 28–34, Dec. 2002.
9. J. Wang, T. Fukasama, S. Urabe, and T. Takata, "A collusion-resistanta pproach to privacy-preserving distributed data mining," IEICE Trans. Inf. Syst. (Inst. Electron. Inf. Commun. Eng.), vol. E89-D, no. 11, pp. 2739–2747, 2006.
10. J. Smith, "Distributing identity [symmetry breaking distributed access protocols]," IEEE Robot. Autom. Mag., vol. 6, no. 1, pp. 49–56, Mar.1999.

BIOGRAPHY

Mr. P. B. More is an Assistant Professor in the Computer Science and Engineering/Information Technology Department of Adarsh Institute of Technology and Research Center, Vita. Shivaji University, Kolhapur (Maharashtra), India. He received Master of Technology (M .Tech) degree in the year 2015 from JNTU, Hyderabad, India.

Mr. Y. B. Amane is an Assistant Professor in the Computer Science and Engineering/Information Technology Department of Adarsh Institute of Technology and Research Center, Vita. Shivaji University, Kolhapur (Maharashtra), India He received Master of Technology (M .Tech) degree in the year 2013 from JNTU, Hyderabad, India.