International Journal of Future Generation Communication and Networking
Vol. 9, No. 12 (2016), pp. 197-204
http://dx.doi.org/10.14257/ijfgcn.2016.9.12.18

Secure Mobile Commerce in Ad hoc Network Using CAEC^{2}M

Khaleel Ahmad[1], Md Shoaib Alam[2] and M A Rizvi[3]

[1,2]*School of CSIT, Maulana Azad National Urdu University, Hyderabad, India*
[3]*Departemt of CSE, NITTTR, Bhopal, India*
[1]*khaleelamna@gmail.com*, [2]*shoaib.al9@gmail.com*, [3]*marizvi@nitttrbpl.ac.in*

Abstract

M-Commerce applications in the world have grown exponentially over the years. It had set up for mobile users to engage wirelessly of ad hoc network infrastructure in online business irrespective of place or time. Providing anonymous, secure and trust based connection service in ad hoc network is quite a challenging task. Anonymity, security and privacy of the transaction or message transmission are the highest priority need to be delivered to the destination node on time. In this paper, a CAEC^{2}M (Cellular Automata Elliptic Curve Cryptography Mix network) algorithm to secure Mobile Commerce over ad hoc network is proposed. An attempt is made to design a mix-network (Mix-Net) using elliptic curve cryptography based on cellular automata which creates a hard to trace communication to protect the anonymity of the sender and encrypt the sensitive information to avoid any eavesdropper trying to access the data during transmission. CAEC^{2}M provides also confidentiality, integrity and authentication.

Keywords*: Elliptic Curve Cryptography, Cellular Automata, Mix-Net, Anonymity, Security.*

1. Introduction

Mobile ad hoc network is a revolutionary instance of wireless communication for handheld and mobile devices. Host maneuverability in ad hoc network prompts a regular change of network topology that is why thither is no established infrastructure. Every node communicates directly through wireless links which is surrounded by each others' radio range [1]. Ad hoc network facade both challenges & possibilities to accomplish security goals viz. Authentication, integrity, availability, confidentiality and access control. Mobile ad-hoc networks pose a lot of features such as dynamic topologies, no fixed infrastructure, resource constraints and limited physical security [2]. Customers through M-Commerce (Mobile Commerce) is buying and promoting of products using wireless handheld gadgets like multimedia phone, i-Pad, PDAs *etc*. The use of ad hoc wireless networks enables users to engage in mobile commerce transactions anywhere at any time [3]. To make secure mobile commerce in the ad hoc network environment is a big challenge in providing anonymous, secure and trust based connection service in a network [4]. Implementing a transparent encryption scheme and maintaining the confidentiality of data is the biggest concern. All most all applications do require anonymity which is the most important sub-discipline of information hiding. Mix-Networks can be defined as a multi-stage system which acts as a routing protocol which creates a difficult-to-find communication. A Mix-Net uses a chain of proxy servers, called as "Mixes" which accepts messages from different senders; it shuffles them and then sends to the next destination node in a random order [5]. A snooper can never identify or trace the end-to-end communication link as Mix-

ISSN: 2233-7857 IJFGCN

Networks break the link between the source and destination. Besides this mix nodes are aware only about the node which it immediately takes from or the next instant node which it has to transfer the shuffled message. It makes the network resistant to avoid any malicious node entering the network. The encryption of messages is done using public key cryptography for each proxy the resultant encryption is layered, followed by messages as an innermost layer. At every layer each proxy removes its own layer of encryption to identify where the next message should be sent. A tracer can compromise the security only at one proxy server, but can never identify where the message was originally generated and where it is going to be transmitted. Message encryption is performed under a sequence of public keys. The layer of encryption is removed by each mix-node by using its own private key. The node is responsible for performing shuffling of message and sending randomly to the subsequent node. A destination can reply to a sender by still maintaining the source anonymity [6][7][8].

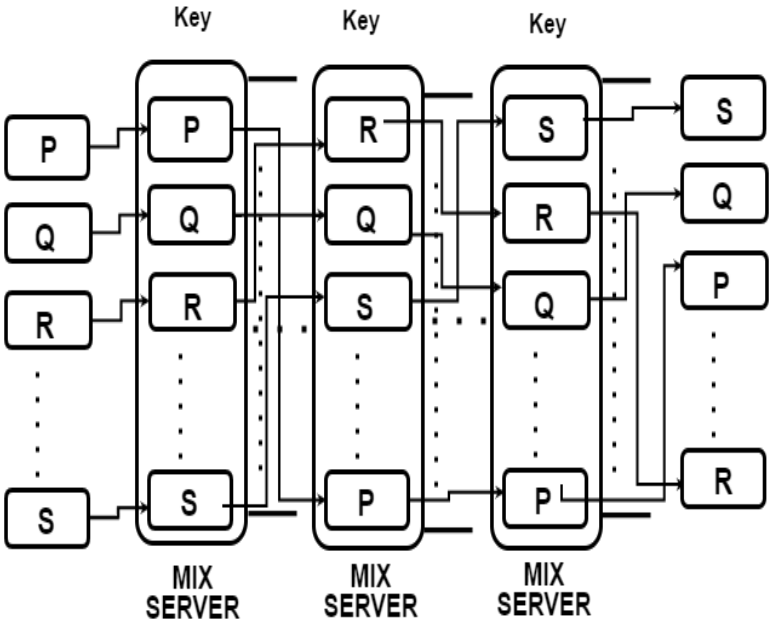

Figure 1. Mix-Networks

Node P produces a message which has to be delivered to Node Q, it appends a value r (Randomly generated) to the massage (M) and seals it with the recipients' public key K_{Pb} appending address of Q and also seals the result with mix's public key K_{Mix}. Now mix opens it using his private key and now he comes to know about Q's address and it sends K_{Pb} (M, r) to Q.

Message format:

$$K_{Mix}\, r_1,\ K_{Pb}(r_0, M),\ Q) \rightarrow (K_{Pb}(r_0,\ M),\ Q)$$

In order to achieve this the sender uses mix's public key (K_{Mix}), for encrypting an envelope consisting of a string (r_1) randomly generated, now this nested envelope is send to the recipient's public key (K_{Pb}), which also contains additional random string (r_0), followed by message which is being transferred. When top level encrypted envelope is received, the mix opens it using its own private key. The mix finds the address of B recipients address followed by an encrypted message. Now (r1) the random string is discarded.

Since r_0 is essential in the message to avoid or prevent any attack from guessing messages. Basically, r_0 function as a salt.

The message from P → Q
K_{Mix} (r_1, K_{Pb} (r_0, M, K_{Mix}(S_1, P), K_{PO}), Q) → K_{Pb}(r_0, M, K_{Mix} (S_1, P), K_{PO})
M = Message
K_{PO} = Public One-Time Key
K_{Pb} = Q's Public Key

S_1 can be defined as a key which can act as a random string to seal the reply messages.
The reply message or acknowledgement from Q → P:
K_{Mix}(S1, P), K_{PO}(S_0, response) → P, S_1 (K_{PO} (S_0, response))
The key size of ECC algorithm is roughly 5 times much less compared to RSA algorithm and also the ECC security degree is higher than RSA. Elliptic curve cryptography takes much less time to encrypt the message and also take much less reminiscence storage not like RSA algorithm. Cellular automate makes more robust to ECC algorithm more robust and secure than ECC and RSA algorithm. Cellular automata make more complex to elliptic curve cryptography [9].

2. Related Work

Jordi *et al*. [10] has introduced an efficient Mix-Net verification system which combines both the optimistic mining techniques as well as RPC by preserving the voter's privacy and high audit accuracy as well.

PauceRibarski *et al*. [11] has discussed about the Chaumain Mix-Net and different approaches to implement Mix-Nets and analyzes four different types of Mix-Nets which includes one decryption and the other three encryption methods implemented in Java Programming languages. Anonymity of channels and message passing between peers has also been discussed. Alessandro Acquisiti [12] has discussed about a user centric Mix-Net protocol to preserve a user's privacy. Reliability and trust issues are also being discussed. It has focussed on how a mix approach can be implemented to put the user in centre of protocol and in control of it also discussed about the tradeoffs which arise from this proposed approach. Philippe Bulens *et al*. [13] analyzed implementing Mix-Net based elections using Helios. A variant of Helios has been presented which allows proficient Mix-Net based tallying procedure and also various choices which are made for election workflow and algorithm selection. A modified version "TDH2 scheme" of Shoup and Gennaro for encryption of ballots has been proposed. Masayuki ABE [14] focused on the construction of Mix-Networks on permutation network, which is a combination or group of switches which transposes two inputs. Also analyzed and presented two universally verifiable Mix-Net schemes which stamp outs the tiresome process of cut and choose the method. The schemes discussed here more suits mostly to small to middle scale secret ballot systems for electronic elections. Doublas Wikstrom discussed about a sender verifiable Mix-Net protocol and also a new proof a shuffle. Also introduced first El Gamal based Mix-Net in which re-encryption is not required. A decryption permutation shuffle is constructed. The protocol introduced is vigorous under the strong RSA assumption [15].

3. Proposed Work

Prevent the M-Commerce transactions from intruders using Elliptic Curve Cryptography (ECC) based on Cellular Automata; the key is generated through cellular automata at the center of preventive mechanism. There is no central authority and central server in ad hoc network. For this, we had proposed Elliptic Curve Cryptography based on Cellular Automata (CA-ECC) algorithm to secure the M-Commerce. Each node has owned symmetric key referred to as neighborhood key

which is generated by cellular automata. For encryption and decryption process, every one node must get to alternate nodes' neighborhood key. At the sender's node, neighborhood key is encrypted through recipient public key and then send to the end node. At the receiving node, neighborhood key is decrypted with owning private key. It diminishes correspondence aloft with the ability to have dynamic keys. In this paper we used Mix-Network for protecting the anonymity of the sender, receiver and also the interim nodes. Here we use a CA-ECC algorithm to encrypt the message. Since we are using the Mix-Network to hide the anonymity and encryption process is performed by the CA-ECC even interim nodes cannot determine the source and destination nodes and message will be transferred in an unreadable form. We further use CA-ECC to check the authentication of the interim nodes and also maintain the confidentiality of stored data. Figure 1 depicts Anonymous, Secure, and Authentic communication in network Using Mix-Network using Elliptic curve cryptography based on cellular automata. If Source node wants to communicate with Destination node, then source node send the message to interim nodes, but before transferring the message Mix-Net protocol encrypts the message using CA-ECC algorithm and hide the source node address to make the anonymous and thereafter check the authentication of interim nodes to maintain the confidentiality of the message. After completing the process of Mix-Network then the message will be transferred from one node to another node. This process will be applied in the entire process until message does not reach at the destination node.

3.1. Flow Chart of Mix-Net based on CA-ECC

There are four basic components of flow chart:

- CA-ECC key generation
- Mixing
- Display Board
- Verifier

Display Board: It is public place, which is used to publish all the information, such as the public keys, cipher texts, re-encryptions and proofs.

3.2. Algorithm

I. Set Up Phase:

a. The first phase is setup phase, key generation, where the keys of the mix are generated with the help of CA (Cellular Automata).

b. Number of 1's in n^{th} generation of CA using Rule 30, started with a single 1.

1, 3, 3, 6, 4, 9, 5, 12, 7, 12, 11, 14, 12, 19, 13, 22, 15, 19 ... (sequence A070952 in OEIS) and is approximately n [16][17][18][19].

Let take random number K = 11 (from above generation of CA using Rule 30)

c. **Generate the Key:**

Randomly select **Private Key**: **X** ϵ [1, n-1], X = 17

Suppose Sender choose base point B = (2, 7)

Elliptic Curve: E_{11} (1, 6)

Y = X*B = 17(2, 7) = 17G = 13G+4G = 4G

Public Key: **Y** = (10, 2)

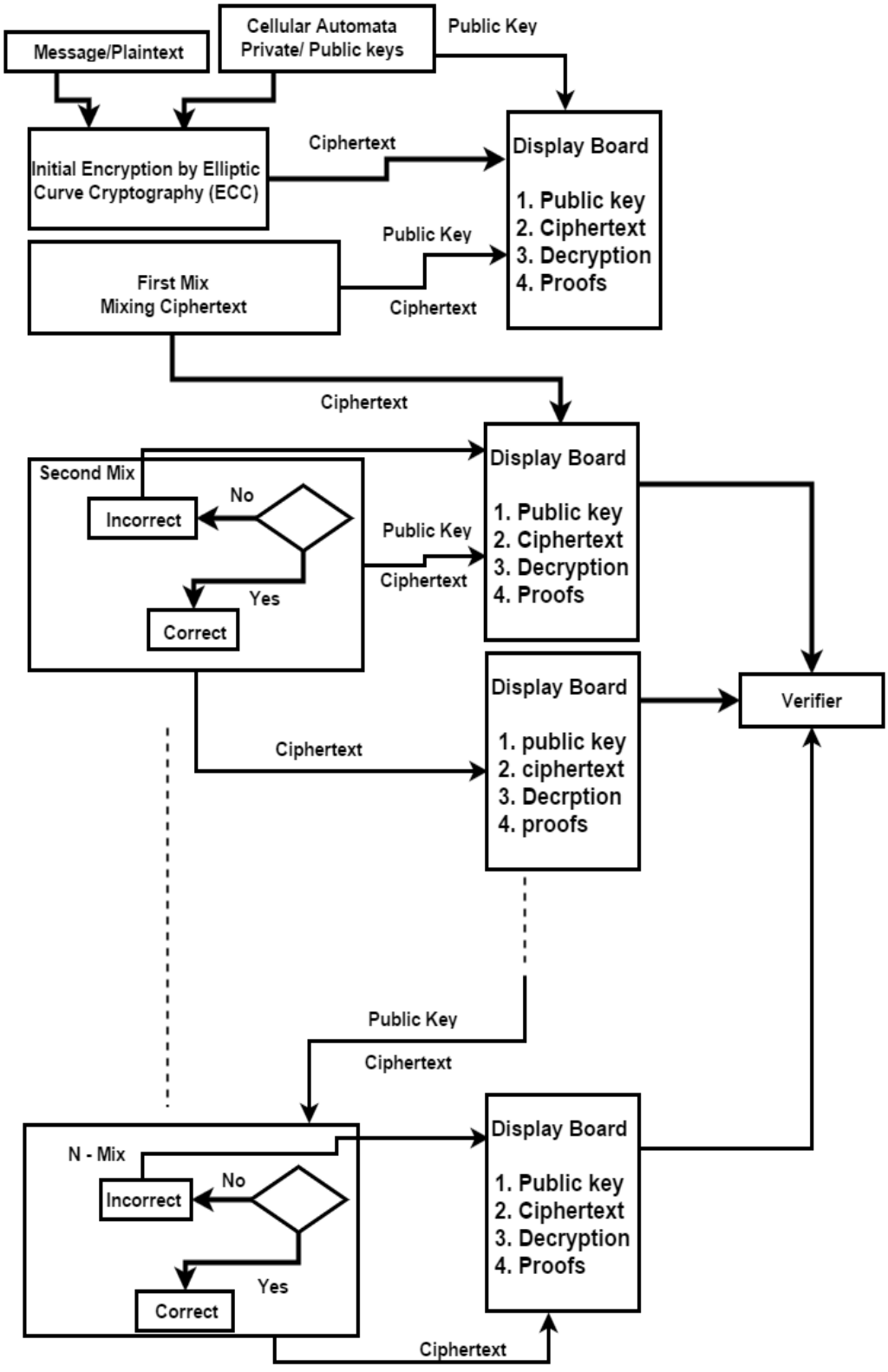

Figure 2. Flow Chart

II. Encryption Phase:

a. We use P, Q, R and S nodes, encryption of message **M** with public key **Y** and the decryption of cipher text C with private key **X.** Consider a mixnet **N** which consists of 4 mix servers.

b. Each mix server N_i (i= 1... 4) generates its public key Y_i and private key X_i of P, Q, R, S and R denote the initial encryption phase of input plaintexts M_j (j= 1... 4), whose outputs are sent to the first mix server.

c. Encrypt the message:

Cipher text: **C**=kB, P =M+kY, Q = M+ kY, R= M+kY, S=M+kY

Message: M (7, 9)

Select random number using cellular automata, k = 19

C = 19(2, 7), C = (7, 9)

P= (7, 9) +19(10, 2), Q = (7, 9) +19(10, 2), R= (7, 9) +19(10, 2),

S = (7, 9) +19(10, 2)

P = (10, 2), Q = (10, 2), R = (10, 2), S= (10, 2)

III. Mixing and Prove Phase

a. In Mix phase, the Mix Server N_i use the secret keys X to decrypts of the cipher text. The Mix server employs the Y to decrypt the cipher text and X is used the message during Mix phase. Private keys could be shared among a set of Mix server. Each Mix server keeps its local random number k, in decryption phase the cipher text decrypted using X.

b. Decrypt the message:

Plaintext: M = P - (X*C), M=Q- (X*C), M=R- (X*C), M=S- (X*C)

M = (10, 2) – 17*(7, 9) = 4G – 17*6G = 4G – 102G = -98G = -7G = - (7, 2),

M = (7, 9)

c. Verifiers: This function block executes the process of verifying the proof by mix server. As the proofs are published on the display board, anybody can verify them. The verifier reads the related parameters, cipher texts and decryption from the display board and checks the correctness of the Mix process. If the process is correct that is the acts of Mix server are correct, it accepts the proof, otherwise reject it.

IV. Diffie-Hellman Secret Key Exchange Using CA-ECC

a. Sender and Receiver choose Elliptic curve E11 (1, 6) and a base point B (2, 7) on the curve.

b. Sender choose a secret integer $I_s = 9$ *i.e.* $I_s < I$ (I=13) G. Sender generates point: $G_s = I_s*B = 9(2, 7) = 9G = (10, 9)$ on the elliptic curve. Sender sends G_s to Receiver.

c. Receiver choose a secret integer $I_R = 12$ *i.e.* $I_R < I$ and generates point $G_R = I_R*B = 12(2, 7) = 12G = (2, 4)$ on the Elliptic curve. Receiver sends G_R to Sender.

d. Sender and Receiver calculate a shared secret key:

$K_{sender} = I_S*G_R = 9(2, 4) = 108G = 104G+ 4G = 4G$

$K_{sender} = (10, 2)$

$K_{receiver} = I_R*G_S = 12(10, 9) = 12*9G = 108G = 104G+4G = 4G$

$K_{receiver} = (10, 2)$

$K_{sender} = K_{receiver} = (10, 2)$

4. Conclusion and Future Work

This paper gives a gentle introduction to mix-networks (mix-net) about anonymity, security, privacy and trust in the ad hoc network. In this paper, a new method for Mix-Network using elliptic curve cryptography based on cellular automata to make the

node anonymous, message encryption, node authentication and message confidentiality is proposed. In this depth review, it is found that CAEC^{2}M provide the security to some extent, compared to an earlier proposed mix-network. In future, secure data transmission based on CAEC^{2}M protocol will be implemented in real time scenario.

References

[1] H. Jiang, "Study on Mobile E-commerce Security Payment System", 2008, International Symposium on Electronic Commerce and Security, doi:10.1109/isecs.2008.64, **(2008)**.
[2] F. Tian, X. Han and Y. Wei, "Application and Research of Mobile E-commerce Security Based on WPKI. 2009 Fifth International Conference on Information Assurance and Security", doi:10.1109/ias.2009.243, **(2009)**.
[3] X. Zheng and D. Chen, "Study of mobile payments system. IEEE International Conference on E-Commerce", CEC 2003, doi:10.1109/coec.2003.1210227, **(2003)**.
[4] J. Ren, Y. Li and T. Li, "Providing source privacy in mobile ad hoc networks", 2009 IEEE 6th International Conference on Mobile Adhoc and Sensor Systems, doi:10.1109/mobhoc.2009.5336980, **(2009)**.
[5] S. Jiang and N. Vaidya, "A mix route algorithm for mix-net in wireless mobile ad hoc networks", 2004 IEEE International Conference on Mobile Ad-hoc and Sensor Systems (IEEE Cat No04EX975), doi: 10.1109/mahss.2004.1392180, **(2004)**.
[6] D. Wikstrom, "A Sender Verifiable Mix-Net and a New Proof of a Shuffle", https://www.iacr.org/archive/asiacrypt2005/268/268.pdf.
[7] https://en.wikipedia.org/wiki/Mix_network. Last Accessed, **(2016)**.
[8] A. B. E. Masayuki, "Mixnetworks on Permutation Networks. In: Advances in Cryptology – ASIACRYPT'99", Springer Lecture Notes in Computer Science, vol. 1716, **(1999)**, pp. 258-273.
[9] http://math.boisestate.edu/~liljanab/MATH508/GuideEllipticCurveCryptography.PDF. Last accessed, **(2015)**.
[10] J. P Allepuz and S. G. CastellóScytl, "Universally Verifiable Efficient Re-encryption Mixnet", Secure Electronic Voting. http://neu.e-voting.cc/wp-content/uploads/Proceedings%202010/7.1.Puiggali_2010.pdf
[11] P. Ribarski and L. Antovski, "Mixnets: Implementation and Performance Evaluation of Decryption and Re-Encryption Types", pp. 493-498, ISSN:1334-2762, Print ISBN:978-1-4673-1629-3, INSPEC Accession Number: 3000996.
[12] A. Cquisti, "An User-centric MIX-net Protocol to Protect Privacy", UC Berkeley Workshop on Privacy in Digital Environments: Empowering Users CSCW, **(2002)**, http://smg.media.mit.edu/**cscw2002-**privacy/submissions/alessandro.pdf.
[13] P. Bulens, B. Krypt, O. B. D. G. BlueKrypt and O. B. O. Pereira, "Running mixnet-based elections", with HeliosUniversit´ecatholique de Louvain ICTEAM – Crypto Group B-1348 Louvain-la-Neuve – Belgium.
[14] "Mix-Networks on Permutation Networks", Advances in Cryptology - ASIACRYPT'99 Lecture Notes in Computer Science, vol. 1716, **(1999)**, pp. 258-273.
[15] D. Wikstrom, "A Sender Verifiable Mix-Net and a New Proof of a Shuffle", https://www.iacr.org/archive/asiacrypt2005/268/268.pdf.
[16] D. Gage, E. Laub and B. Mcgarry, "Cellular Automata: Is Rule 30 Random?", pp. 1-10.
[17] J. Jose and D. R. Chowdhury, "Four Neighbourhood Cellular Automata as Better Cryptographic Primitives", pp. 1-9.
[18] L. Wentian and N. Packard, "The Structure of the Elementary Cellular Automata Rule Space", pp. 1-17.
[19] S. Wolfram, "Cryptography with Cellular Automata", pp. 1-4.

Authors

Khaleel Ahmad, he is currently an Assistant Professor in the School of Computer Science & Information Technology at Maulana Azad National Urdu University, Hyderabad. Prior to this he has worked at prestigious universities and institutions of national repute. He holds a PhD in Computer Science & Engineering and M.Tech in Information Security. His research area is Information Security, Cyber Security, Cryptography, Opportunistic Network, and Cloud Computing. He has 40

published papers in refereed national/international journals and conferences (viz. Elsevier, ACM, IEEE, and Springer), 6 book chapters (CRC Press, Taylor & Francis Group, IGI Global, IGNOU New Delhi). He has delivered guest lecturers in the Central University of Haryana, India and Telangana University, India and also chaired the session in an international conference in Hyderabad. He is also the life member of various international/national research societies viz. ISTE, CRSI, ISCA, IACSIT (Singapore), IAENG (Hong Kong), IAOE (Austria), ISOC (USA) *etc*. In addition, he is associated with many international research organizations as editorial board member and reviewer.

Md Shoaib Alam, he is an M.Tech Computer Science student at the Department of Computer Science & Information Technology, Maulana Azad National Urdu University, Hyderabad, India. He had completed his B.Tech from Rashtrasant Tukadoji Maharaj Nagpur University, India. He had worked 5 years as a software engineer in the reputed MNCs viz. Tata Business Support Services, Tausch Technologies. He had official visit to UAE as a software developer.

M. A. Rizvi, he has obtained his Doctorate in Computer Science from Maulana Azad National Institute of Technology (MANIT) Bhopal. Presented Research in an International Conference at University of California San Francisco, USA where it was rated second. Dr. Rizvi has more than 25 years of experience in the field of Computer Science and Applications as faculty (Associate Professor) in NITTTR, Bhopal. He has published approximately 80 research papers in reputed International Journals and International Conferences across the globe. He was invited in many International conferences as keynote speaker, session chair and invited talk.