

Key management for bitcoin transactions using cloud based key splitting technique

Amar Buchade¹, Nakul Sharma¹, Varsha Jadhav², Jagannath Nalavade³, Suhas Sapate⁴, Rajani Sajjan³

¹Department of Artificial Intelligence and Data Science, Vishwakarma Institute of Information Technology, Savitribai Phule Pune University, Pune, India

²Department of Artificial Intelligence and Data Science, Vishwakarma Institute of Technology, Savitribai Phule Pune University, Pune, India

³School of Computing, MIT ADT University, Pune, India

⁴Computer Science Engineering Department, Dr. Bapuji Salunkhe Institute of Engineering and Technology, Kolhapur, India

Article Info

Article history:

Received Mar 27, 2024

Revised Oct 11, 2024

Accepted Oct 23, 2024

Keywords:

Bitcoin wallet

Blockchain security

Cloud computing

Key management

Secret key

ABSTRACT

Bitcoin wallet contains the information which is required for making transactions. To access this information, user maintains the secret key. Anyone with the secret key can access the records stored in bitcoin wallet. The compromise of the key such as physical theft, side channel attack, sybil attack, DoS attack and weak encryption can cause the access of transactional details and bitcoins stored in the wallet to the attacker. The cloud-based key split up technique is proposed for securing the key in blockchain technology. The key shares are distributed across virtual machines in cloud computing. The approach is compared to the existing key management approaches such as local key storage, keys derived from password and hosted wallet. It is observed that our approach is most suitable among the other key management approaches.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Amar Buchade

Department of Artificial Intelligence and Data Science, Vishwakarma Institute of Information Technology, Savitribai Phule Pune University

Pune, India

Email: amar.buchade@viit.ac.in, amar.buchade@gmail.com

1. INTRODUCTION

Bitcoin is digital currency, Satoshi Nakamoto in 2008 mentioned this word [1]. The bitcoins are stored in wallet called digital wallet. This wallet can also place on mobile, laptop, hardware [2]. Bitcoin transactions are happening without involvement of third party and in decentralized fashion. These transactions are in-creasing day by day in many applications. The applications such as online retailers, peer-to-peer transactions, investment and trading, crowdfunding, fundraising, smart contracts, and real estate. It now uses blockchain technology. As per statistical information, the number of blockchain wallet users has exponentially grown since 2011, leading to security issues for using blockchain technology [3].

There are numerous crypto currencies such Altcoin, Bitcoin, Ethereum, Litecoin, and Ripple. being used [4]. But mostly bitcoin is preferred crypto currency in the world and obviously the Bitcoin is attacker's choice. Thus, securities of Bitcoin transactions are important [5]. Bitcoin user uses private key for authentication as well as to access and spent the currency stored at wallet during the transaction. If the private key is lost or grabbed by attacker or intruder, bitcoin user will not able to do transactions and thus loose the currency.

The following types of attacks occurred on wallet and bitcoin transactions [6]–[11]. Attacks on wallet software – this is done by tampering or stealing the key. The attacker gets the control of wallet and grabs the money. Bitcoin exchange – in this system, user's private key is stored by another party such as a financial agency. The financial agency manages the bitcoin of the user on user's behalf. Since it involves another party, this is dangerous, and trust management between the user and the bank is essential. Denial-of-service attack – attacker attacks on nodes, servers thus users are unable to use the service. Sybil attack – in this attack, adversaries create multiple identities of the nodes which are involved in the Bitcoin transactions. The genuine users will be disconnected from blockchain network with this attack. Bait and switch – this attack is occurred when the code inserted in source code of software to steal the Bitcoins. OzCoin which is one of the largest Bitcoin mining pools confessed the attack by stealing BTC from Bitcoin wallet. Cross channel attacks can also cause to gain the key. Cross channel attacks [12]–[15] can be classified into time, traces and access on channel. In time-based attack, the cryptography operation time is monitored and analyzed to extract the key. In traced based attack, device power consumption or electromagnetic radiations are continuously monitored to extract the key. In access-based attack, attacker checks cache to extract confidential information and key, *e.g.*, data and instruction cache. Due to these attacks, it is possible to grab the key by the intruders.

The challenge of managing secret keys in Bitcoin and blockchain technology in solving problem [16]. If the secret key is missed, owner will be unable to access their electronic assets. It poses risks in the event of bitcoin theft. Thus, key management is required to properly handle the key in a secure way. This paper discusses existing key management methods. The cloud based key split management with multilevel key splitting approach is proposed to protect the key from the attackers. This paper also describes and compares the existing approaches for key management. Our contributions in this paper are as follows: i) Study of existing key management techniques for handling bitcoin key; ii) Design and analysis of key split management technique with multilevel approach; and iii) Security analysis of key split technique.

2. EXISTING KEY MANAGEMENT TECHNIQUE

In order to protect the digital wallet, person handling the bitcoin transactions, keeps private key secure. Current approaches for key management of blockchain are discussed as below.

- Local key storage [17]–[19]: The key is stored at local storage. The advantage is that key can be easily accessed. But it is not safe due to attack on local storage by virus, malicious script, lack of updates, brute force attacks, human error, online attacks, and forgotten passwords.
- Wallet with password protection [20]–[22]: The wallet can be protected by the password. The disadvantage of this approach is that if password is lost or password is gained by attackers, the bitcoin owner will not be able to access the wallet. Finally, owner loses the currency stored in the wallet. Thus, it leads to loss of access of funds. If you forgot wallet password, recovery options are not also available. Thus, it challenges to regain the access of funds.
- Key storage at offline place [23], [24]: Keys are maintained at place in order to avoid online access of the same like universal serial bus (USB) or paper wallet. But it may not be easily accessed when it is required due to physical loss or damage, human error, limited accessibility, and lack of updates.
- Third party approach [25]: In this, keys are managed at third party by the owner of the key. The storing the key at third party is risky due to security concerns, centralization risks, regulatory risks, limited control of the user as well as service downtime.

Bitcoin uses blockchain for transactions. Figure 1 shows blockchain structure. Each block contains the current hash, previous block hash information, and transaction information.

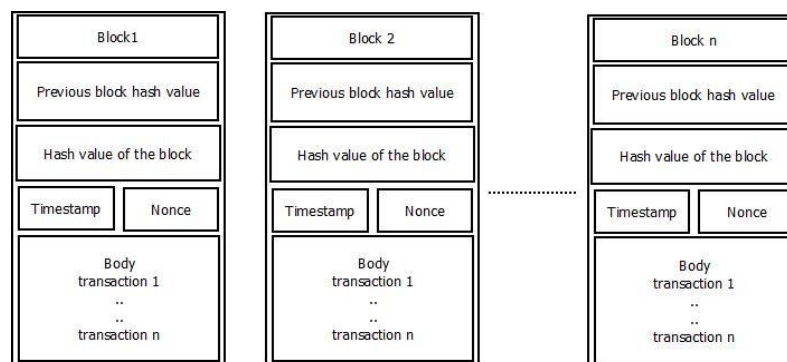


Figure 1. Blockchain structure

3. METHOD

Existing key management methods for bitcoin transactions have limitations as per discussed in the section 2. Safeguarding the key is important. Thus, novel methodology is introduced. The methodology indicates how to safeguards the key. Threshold cryptography with cloud enabling is presented. The owner splits the key into multiple splits. These multiple splits may be shared in virtual machines of cloud computing environment. Threshold is decided by the owner. If owner collects key splits at least threshold number of keys, complete key can be constructed otherwise key will not be reconstructed. The Figure 2 indicates that data/key owner splits the key into multiple key splits and distributes the key splits to virtual machines of the cloud environment.

Threshold cryptography based Shamir’s approach [26], [27] is used to divide the key into parts as per security requirements. The algorithm considers the threshold value. The key can be reconstructed from at least threshold number. The threshold value can be decided by the owner of the key. The algorithm provides flexibility for split and reconstructs the key. The threshold value is adjusted based on the security requirements. The threshold value can be decided by the owner of the key. The novelty of the approach is that the threshold value can be changeable as per owner of the key requirement. The increase in the threshold enhances the security. This changeable threshold property allows the key owner to adapt to security needs.

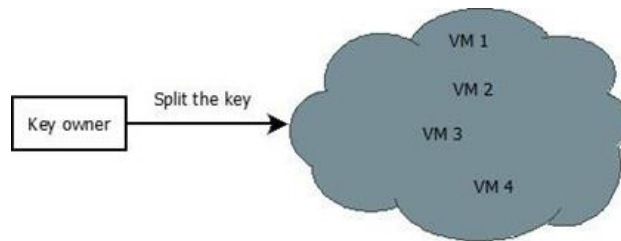


Figure 2. Key split up for blockchain key management

3.1. Increasing degree of security by multiple splits

The key can be safe guarded by dividing it into multiple level. Initially, key is divided into n key parts. At the subsequent level, each split of the key can be further divided into n partial key parts and so on. It uses threshold cryptography (t, n) scheme. Figure 3 shows the multilevel key split by using threshold cryptography (t, n) approach into key shares. The number of key parts at each level can be given by formula:

$$N = n^l$$

where n is number of key parts after key divides at each level and l is number of levels up to which key divide has to be performed. For reconstruction of the key, back tracking up to level 0 is required. For each level, threshold number of partial key shares needs to be collected to get back the key.

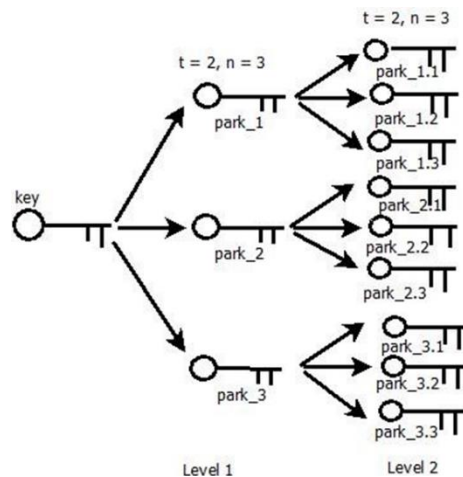


Figure 3. Key split up time

4. RESULTS AND DISCUSSION

Safeguarding the key is important for the security of bitcoins stored in wallet. The key divide is employed to safeguard the key from various attacks. This section assesses the performance of the technique by measuring the time taken for key divide. The security analysis is conducted in section 5.

The experiment was conducted by considering Shamir's secret sharing algorithm. Key split up time for different key sizes is calculated to see how much time is needed to divide the key. Key size was taken as 256 bits similarly as advanced encryption standard (AES) algorithm. Initially threshold value was taken as 2. That means if any two key shares are taken from the pool of key parts that are spreader across the virtual machines, complete key can be reconstructed. The total number of key splits varied from 10.50. The key split time was as taken as performance indicator. It is found that as key shares are varied as 10, 20, 30, 40, and 50, the key split up time is increasing. It is mentioned in Figure 4. This experimentation is performed because there should not be any delay to access the bitcoin wallet due to such factors such key split and key formation after getting threshold number of key splits (assume t). Obviously through our experiment, it is observed that key split up time varying with increasing key size and number of key shares.

We have also compared our approach to other key management methods such as keys in local storage, password driven keys and hosted wallet. The Table 1 gives the comparisons. The parameters such as malware resistance, offline key, trusted third party, resistant to physical theft, resistant to password loss and cross device portability [14]. It is found that our approach of key management supports all these parameters and secure from other methods.

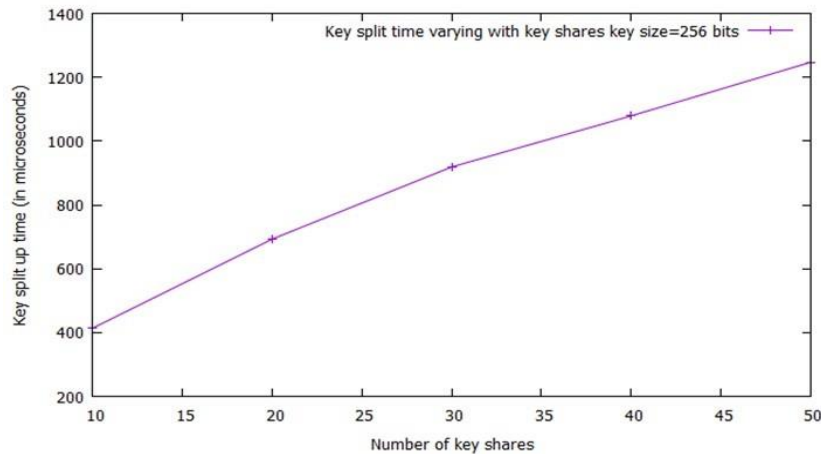


Figure 4. Key split up time

Table 1. Comparison of existing key management methods

| Parameters approach | Malware resistance | Offline key | None trusted mediator | Physical barrier | Resiliency | Cross device portability |
|-----------------------|--------------------|-------------|-----------------------|------------------|------------|--------------------------|
| Ours | Yes | Yes | Yes | Yes | Yes | Yes |
| Keys in local storage | | | Yes | | | |
| Password driven keys | | Yes | Yes | | | Yes |
| Hosted wallet | | | | | Yes | |

5. SECURITY ANALYSIS

The security analysis deals with how it is difficult to attack by adversaries to get the key. The key parts can be sent to virtual machines in cloud environment. It is not possible to form the key since adversaries have to compromise at least threshold number of key splits. Further the key splits can refresh at each virtual machine. Therefore, reconstructing the key from its parts is not feasible. Even if attackers obtain fewer than threshold number of key parts, they cannot assemble the key through the key parts. The use of threshold-based Shamir's secret sharing prevents the attackers to capture the side channel information by refreshing the key shares at virtual machines. Thus, it does not cause side channel attack. Even if the less than t number of virtual machines crashed/becomes faulty, the key cannot be formed. Thus, it is resilience to loss/fault. Multilevel key split up approach is enhancing key security at multiple levels. User has to define the levels up to which key can be split up. Thus, enhancing the key security in blockchain network.

6. CONCLUSION




Key management is crucial in case of Bitcoin management. The cloud-based key split up technique is used to protect the key against intruders. Multilevel key splitting approach further enhances the security of key management. We compared our approach to other approaches to in the context of security the key for blockchain transactions. It is found that our approach is proving the best compared to others. The security assessment reveals that reconstructing the complete key is challenging for an attacker, thereby preventing access to the Bitcoin wallet.

REFERENCES




- [1] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system," *Unpublished*, pp. 1–9, 2008.
- [2] "What is a Bitcoin wallet?," *Bitcoin.com*. <https://www.bitcoin.com/get-started/what-is-a-bitcoin-wallet/> (accessed Jan. 26, 2024).
- [3] "Number of blockchain wallet users worldwide from November 2011 to November 17, 2022," *Statista*. <https://www.statista.com/statistics/647374/worldwide-blockchain-wallet-users/> (accessed Jan. 26, 2024).
- [4] D. K. Soni, H. Sharma, B. Bhushan, N. Sharma, and I. Kaushik, "Security issues & seclusion in bitcoin system," in *Proceedings - 2020 IEEE 9th International Conference on Communication Systems and Network Technologies, CSNT 2020*, 2020, vol. 2020-Janua, pp. 223–229, doi: 10.1109/CSNT48778.2020.9115744.
- [5] P. K. Kaushal, A. Bagga, and R. Sobti, "Evolution of bitcoin and security risk in bitcoin wallets," in *2017 International Conference on Computer, Communications and Electronics, COMPTTELIX 2017*, 2017, pp. 172–177, doi: 10.1109/COMPTTELIX.2017.8003959.
- [6] S. Shalini and H. Santhi, "A survey on various attacks in bitcoin and cryptocurrency," in *Proceedings of the 2019 IEEE International Conference on Communication and Signal Processing, ICCSP 2019*, 2019, pp. 220–224, doi: 10.1109/ICCSP.2019.8697996.
- [7] S. Singh, A. S. M. Sanwar Hosen, and B. Yoon, "Blockchain security attacks, challenges, and solutions for the future distributed IoT network," *IEEE Access*, vol. 9, pp. 13938–13959, 2021, doi: 10.1109/ACCESS.2021.3051602.
- [8] N. D. Bhaskar and D. L. K. Chuen, "Bitcoin Exchanges," *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data*, pp. 559–573, 2015, doi: 10.1016/B978-0-12-802117-0.00028-X.
- [9] R. Chaganti *et al.*, "A comprehensive review of denial of service attacks in blockchain ecosystem and open challenges," *IEEE Access*, vol. 10, pp. 96538–96555, 2022, doi: 10.1109/ACCESS.2022.3205019.
- [10] M. Platt and P. McBurney, "Sybil in the haystack: a comprehensive review of blockchain consensus mechanisms in search of strong sybil attack resistance," *Algorithms*, vol. 16, no. 1, 2023, doi: 10.3390/a16010034.
- [11] N. Tovanih, N. Soulie, N. Heulot, and P. Isenberg, "The evolution of mining pools and miners' behaviors in the bitcoin blockchain," *IEEE Transactions on Network and Service Management*, vol. 19, no. 3, pp. 3633–3644, 2022, doi: 10.1109/TNSM.2022.3159004.
- [12] P. C. Kocher, "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 1109, pp. 104–113, 1996, doi: 10.1007/3-540-68697-5_9.
- [13] A. Moradi, "Differential power analysis," *Encyclopedia of Cryptography, Security and Privacy*, pp. 1–3, 2023, doi: 10.1007/978-3-642-27739-9_1794-1.
- [14] K. Gandolfi, C. Mourtel, and F. Olivier, "Electromagnetic analysis: concrete results," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 2162, pp. 251–261, 2001, doi: 10.1007/3-540-44709-1_21.
- [15] Y. Xu, M. Bailey, F. Jahanian, K. Joshi, M. Hiltunen, and R. Schlichting, "An exploration of L2 cache covert channels in virtualized environments," in *Proceedings of the ACM Conference on Computer and Communications Security*, 2011, pp. 29–39, doi: 10.1145/2046660.2046670.
- [16] M. Rahouti, K. Xiong, and N. Ghani, "Bitcoin concepts, threats, and machine-learning security solutions," *IEEE Access*, vol. 6, pp. 67189–67205, 2018, doi: 10.1109/ACCESS.2018.2874539.
- [17] O. Pal, B. Alam, V. Thakur, and S. Singh, "Key management for blockchain technology," *ICT Express*, vol. 7, no. 1, pp. 76–80, 2021, doi: 10.1016/j.icte.2019.08.002.
- [18] S. Eskandari, D. Barrera, E. Stobert, and J. Clark, "A first look at the usability of bitcoin key management," *arXiv preprint arXiv:1802.04351*, 2015.
- [19] X. He, J. Lin, K. Li, and X. Chen, "A novel cryptocurrency wallet management scheme based on decentralized multi-constrained derangement," *IEEE Access*, vol. 7, pp. 185250–185263, 2019, doi: 10.1109/ACCESS.2019.2961183.
- [20] S. Suratkar, M. Shirole, and S. Bhirud, "Cryptocurrency wallet: a review," in *2020 4th International Conference on Computer, Communication and Signal Processing (ICCCSP)*, Sep. 2020, pp. 1–7, doi: 10.1109/ICCCSP49186.2020.9315193.
- [21] J. Han, H. Kim, H. Eom, and Y. Son, "A decentralized document management system using blockchain and secret sharing," in *Proceedings of the ACM Symposium on Applied Computing*, 2021, pp. 305–308, doi: 10.1145/3412841.3442077.
- [22] Y. Liu *et al.*, "An efficient method to enhance Bitcoin wallet security," in *Proceedings of the International Conference on Anti-Counterfeiting, Security and Identification, ASID*, 2017, vol. 2017-October, pp. 26–29, doi: 10.1109/ICASID.2017.8285737.
- [23] N. M. Mukhammadovich and A. R. Djuraevich, "Working with cryptographic key information," *International Journal of Electrical and Computer Engineering*, vol. 13, no. 1, pp. 911–919, 2023, doi: 10.11591/ijece.v13i1.pp911-919.
- [24] D. Wang, J. Zhao, and Y. Wang, "A survey on privacy protection of blockchain: the technology and application," *IEEE Access*, vol. 8, pp. 108766–108781, 2020, doi: 10.1109/ACCESS.2020.2994294.
- [25] A. R. Buchade and R. Ingle, "Key management for cloud data storage: Methods and comparisons," in *International Conference on Advanced Computing and Communication Technologies, ACCT*, 2014, pp. 263–270, doi: 10.1109/ACCT.2014.78.
- [26] D. Gooch, "Communications of the ACM," *XRDS: Crossroads, The ACM Magazine for Students*, vol. 18, no. 2, p. 6, 2011, doi: 10.1145/2043236.2043240.
- [27] L. T. Brandão, "Towards standardization of threshold schemes at NIST," *Proceedings of ACM Workshop on Theory of Implementation Security Workshop*, 2019.

BIOGRAPHIES OF AUTHORS






Amar Buchade    received Ph.D. from Savitribai Phule Pune University under research center College of Engineering Pune. He has received B.E. and M.E. in computer engineering from Walchand College of Engineering, Sangli in 2002 and 2005 respectively. He is a member of IEEE and life member of ISTE. His research area is distributed system, cloud computing and security. He is currently working as associate professor, with Department of AI-DS at VIIT, Pune. He can be contacted at email: amar.buchade@gmail.com.






Nakul Sharma    completed his B.Tech. in information technology from Bharati Vidyapeeth College of Engineering, Pune in 2009. He completed Master of Engineering from Thapar University, Patiala, Punjab in the area of software engineering in 2011. He finished his Ph.D. degree in CSE from Koneru Lakshmaiah Education Foundation University. He is currently working as assistant professor, with Department of AI-DS at VIIT, Pune. He has over 12 years of experience in teaching engineering students. He has published several papers in national, international journal and conferences. His has to his credit more than 10 design patent published in reputable Patent Offices. His research interest includes source code analysis, NLP, ML, IoT, empirical research, human health. He can be contacted at email: nakul777@gmail.com.






Varsha Jadhav    presently working in artificial intelligence and data science Department of Vishwakarma Institute of Technology, Pune. She has 20 Years of experience in teaching field. She has been awarded Ph.D. in computer engineering from Dr. Babasaheb Ambedkar Marathwada University, Aurangabad. She has published more than 45 research papers and has also authored a book “Multivariate analysis for data science.” Her areas of interest are multivariate analysis, probability and statistics, artificial intelligence, generative AI, machine learning, data science, design and analysis of algorithms, data structures. She has received 03 Best paper awards at international conferences, Global Eminent teacher award 2022 by VIJ Trust Thirunindravur, Dr. Sarvepalli Radhakrishnan Best Faculty and Researcher Award-2022 by International Multidisciplinary Research Foundation Institute of Higher Education and research Vijayawada Andhra Pradesh India. She can be contacted at email: drvarshajadhav22@gmail.com.







Jagannath Nalavade    completed Ph.D. in computer engineering from Vel Tech Rangrajan Dr. Sagunthala Research and Development Institute of Science and Technology, Chennai. Currently, he is working as an associate professor at MIT ADT School of Engineering Pune. His research areas are data mining, machine learning, artificial intelligence. He has 16 years of teaching experience. He has published more than 21 research papers in peer reviewed international journals like Springer, Elsevier Procedia. He is working as reviewer for Springer and Elsevier Journals (information sciences, journal of intelligent systems, computers and electrical engineering, international journal of bioinformatics research and applications). He can be contacted at email: jen20074u@gmail.com.



Suhas Sapate    completed his B.E. and M.E. in CSE from Walchand College of Engineering, Sangli in the year 2000 and 2007 respectively. He earned his Ph.D. in CSE at “Center of excellence in signal and image processing” of SGGGS Institute of Engineering and Technology, Nanded during Sept 2014 to Sept 2017. He has taught many UG and PG courses at Mumbai University, Visveswaraya Technological University, Belgaum, DBATU Lonere and Shivaji University, Kolhapur. He has published 10 journal articles including his research work on automatic breast cancer detection in Springer’s Medical Imaging in Clinical Applications, Elsevier’s Computer Methods and Programs in Biomedicine, Elsevier’s Biocybernetics and Biomedical Engineering. He has published his 8 research articles in national conferences and 14 articles in international conferences. He is approved PhD research co-supervisor in Lovely Professional University Phagwara Punjab, one student has completed his Ph.D. under his supervision and other two are working. He is also approved PhD re-search co-supervisor at Visveswaraya Technological University Belagavi Karnataka and two students are working under his supervision. He is reviewer of few international peer reviewed journals of good repute

including computers in biology and medicine, computer methods and programs in biomedicine. Currently, he is working as professor in CSE Department, as well as Principal of Dr. Bapuji Salunkhe Institute of Engineering and Technology, Kolhapur in Maharashtra. He can be contacted at email: suhasgsapate@gmail.com.



Rajani Sajjan     completed his B.E. in CSE from Walchand College of Engineering, Sangli, and M.Tech. in computer science engineering from Visvesvaraya Technological University and Ph.D. from Shivaji University. She is working as an associate professor at MIT ADT School of Engineering Pune. She has 21 years of teaching experience. Her research is cloud computing, networking, security and machine learning. She can be contacted at email: rajani.sajjan@mituniversity.edu.in.