Simulation of the Lightweight Blockchain Technique Based on Privacy and Security for Healthcare Data for the Cloud System

Preeti Rani, SRM Institute of Science and Technology, India
https://orcid.org/0000-0001-5655-975X

Sonia Verma, SRM Institute of Science and Technology, India

Satya Prakash Yadav, Department of Computer Science and Engineering, GL Bajaj Institute of Technology and Management (GLBITM), Affiliated to AKTU, Greater Noida, India*

Bipin Kumar Rai, ABES Institute of Technology, India
https://orcid.org/0000-0002-9834-8093

Mahaveer Singh Naruka, G.L. Bajaj Institute of Management and Technology, India

Devendra Kumar, Wachemo University, Ethiopia

ABSTRACT

Information about healthcare is derived from healthcare data. Healthcare data sharing helps make healthcare systems more efficient as well as improving healthcare quality. Patients should own and control healthcare information, one of their most valuable assets, instead of letting data be spread out among health care providers differ. This protects data from being shared between healthcare systems and privacy. Public ledger accompanied by a decentralized network of peer’s compromises patient has been demonstrated to be able to achieve trusted, auditable computing by blockchain. The use of access control and cryptographic primitives are insufficient in addressing modern cyber threats all privacy and security concerns associated with a cloud-based environment. In this paper, the authors proposed a lightweight blockchain technique based on privacy and security for healthcare data for the cloud system. The cost-effectiveness of our system’s smart contracts is evaluated, as well as the procedures used for data processing in order to encrypt and pseudonymize patient data.

KEYWORDS

Blockchain Model, Cloud System, Data Management, Health Care, Privacy and Security, IoT, Smart Contract, Smart System

DOI: 10.4018/IJEHMC.309436

*Corresponding Author

This article published as an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/) which permits unrestricted use, distribution, and production in any medium, provided the author of the original work and original publication source are properly credited.
1. INTRODUCTION

With an increasing amount of technological advancements being introduced around the world, health care and biomedicine have always been a major concern to be improved in every possible manner. In order to enhance health care services, trust, procedures, and efficiency, and provide qualified nutrition and care to patients are of primary importance. Currently, the world is seeing more people putting off taking care of their personal health until a major hardship occurs. This is often linked to a person’s over engagement to their lifestyle and accustomed busy schedule. Almost everything that is connected to the internet today performs data and access transfer through the Internet of Things (IoT). In the healthcare sector, IoT has also performed well by simplifying diagnostic procedures and ensuring more efficient monitoring of patients. As a result, IoT has revolutionized and disrupted nearly every industry that exists today, from education to supply chain management.

Blockchain technology coupled with IoT devices that have limited power and storage capacity creates complexity, including high computing costs and delays. The experiments adopted of blockchain model in IOT application are mentioned in figure 1. The healthcare Data types and their different type of healthcare data types are classified in figure 2, as well as the organizations that store, manage, and utilize them. It is clear that healthcare data extends beyond medical diagnosis reports and personal health information and the data pertains to health.

Table 1 compares the three blockchain frameworks: Bitcoin, Ethereum, as well as Hyperledger Fabric. Despite the lack of private channels in the Bitcoin and Ethereum frameworks, these technologies can still be used to transfer private and confidential information. Private data may then be stored off-chain (not on the blockchain) in those scenarios. A public network records only the pointers to the data, so its participants can only see the signatures of the data, but not the actual data. This keeps the actual private information from the general public. Off-chain storage loses some of blockchains advantages, such as redundancy that provides protection against security attacks (e.g., Ransomware and denial of service attacks) on data availability.

Figure 1. The challenges of adopting Blockchain in IoT
Figure 2. Healthcare data and its types

Table 1. Comparative analysis of blockchain frameworks for emerging healthcare applications

<table>
<thead>
<tr>
<th></th>
<th>Bitcoin</th>
<th>Ethereum</th>
<th>Hyperledger Fabric</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy features</td>
<td>No private transactions</td>
<td>Private transactions, experimental zero knowledge proofs</td>
<td>Private channels, private transactions, zero-knowledge proofs</td>
</tr>
<tr>
<td>Security</td>
<td>It is public, access permission is not required, and it is more prone to attack</td>
<td>Access is open, but permissioned networks are supported</td>
<td>Permissions and control over access are granular, so attacks are less likely</td>
</tr>
<tr>
<td>Speed</td>
<td>7 transactions per day second</td>
<td>A transaction per second of 15</td>
<td>Transactions every second are 3000</td>
</tr>
<tr>
<td>Scalability</td>
<td>Throughput of transactions is low</td>
<td>Throughput of transactions is low</td>
<td>Increasing transaction throughput</td>
</tr>
<tr>
<td>Transaction cost</td>
<td>High</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>Incentive</td>
<td>Cryptocurrency is required</td>
<td>Cryptocurrency is required</td>
<td>No Cryptocurrency is required</td>
</tr>
<tr>
<td>Smart contracts</td>
<td>Not available</td>
<td>Solidity</td>
<td>Java, Node.js, Go, Higher-level abstraction (composer, JavaScript)</td>
</tr>
</tbody>
</table>


2. LITERATURE SURVEY

(AI Omar et al., 2019) has proposed some national level frameworks for utilizing the cloud for electronic medical records. Protecting patient data privacy is one of the bottlenecks in Internet information fusion. For a trustworthy data access, a distributed dynamic authorization method based on blockchain is proposed in order to balance data processing capabilities with privacy concerns. Data access interfaces are indicated via URLs in the authorisation information, and patients’ privacy data is not stored on blockchain for better data processing efficiency (Xu et al., 2021a).

As healthcare data volumes increase and sensitivity of data increases, protecting healthcare data is important. Data is collected via Electronic Health Record (EHR), diagnostic images, x-rays, and IoT wearable devices with sensors that can be shared with stakeholders. A few blockchain based methods for securing healthcare data stored in the cloud have been investigated and analysed by the author (Roy & Singh, 2021). Benefits of sharing medical data with each other make it even more vulnerable.

Researchers studied methods for protecting data from unauthorized access. Researchers developed a program to study factors enabling effective and sustainable use of blockchain technology in health education and research. As proposed by the author (Usman et al., 2021), qualitative research is needed to help develop a market strategy for building an academic research lab that promotes the use of blockchain technologies in health. In order to build a market strategy for the use of blockchains in health, it is necessary to conduct qualitative research, as stated by the author (Usman et al., 2021).

Blockchain technology permits a distributed sharing of data in a secure and privacy-preserving way, whereas traditional health care systems utilize local databases to process health records. To ensure the confidentiality of Electronic Healthcare Data (EHD), and the layout of the Electronic Health Record (EHR) system are presented in the figure 3.

Author propose a secure framework for distributed sharing of the health record using blockchain technology. Blockchain technology will eliminate the need for a trusted third party to store data. For fine-grain access control, proposed method use Attribute-Based Encryption (ABE) with searchable keys. The simulation results indicate that our scheme is highly effective and secure. A blockchain-based transaction technology provides users with greater security. Bitcoin as well as blockchain have not experienced a failure since they were introduced (Sayyad et al., 2019). The blockchain network is shared, and information is shared between all members.

Hence, blockchain is very reliable due to its redundant processing (Sharples & Domingue, 2016). Blockchain is distributed but its parameters remain constant between nodes, strengthening its reliability (Xu et al., 2021b). The blockchains immutability cannot be challenged, and any attempt to do so will be very costly. A central database can be corrupted and needs a third party to maintain it. To alter data on the blockchain, an individual needs to control at least 51% of the chain. This immutable architecture (Böhme et al., 2015; Tanwar et al., 2020; Weber et al., 2016) contributions are helpful in archival science as well. Pseudonyms are used in the blockchain so that privacy is assured with utmost precision for its participants (Hull et al., 2016).

With the cryptographically authenticated time blocks with time-stamping, all the logs for users’ interactions in the blockchain can be available through the entire network. Blockchain ensures user identity can be verified. Apart from the attributes mentioned above, some authors also elaborate on the idea of trust enabling concept (Beck et al., 2016; Gerstl, 2016), consensus, transparency, and smart contracts. Blockchain provides a distribution-oriented service for storing information [Hussain, N., & Rani, P. (2020); Rani, Preeti, et al., (2021)].

(Coppi and Fast (2009) maintain that the records that can be stored in the blockchain all have smart contracts. Smart contracts are a form of code that grant programmers an enormous amount of control over the blockchain. In addition to providing accurate and reliable data storage to its users, blockchain technology protects data against tampering, theft, or corruption (Lemieux, 2016). Decentralized web platforms will become the future of this era if they retain decentralization, redundancy, and total
privacy (Garcia-Alfaro et al., 2015). The latest blockchain techniques features for the healthcare application are mentioned in table 2.

3. BLOCKCHAIN OVERVIEW

In which, authors study a blockchain network that records updates to the chain on an average of every 10 minutes. Proposed method can denote a round as $R^n$, each block as $B^n$ and the updated blockchain as $BC^n$, where $n = 0, 1, \ldots n$. The miners (nodes that proactively search for blocks) start computing new blocks during a round $R^n$. Once the block is computed, the first miner to achieve it announces it to the public blockchain, and then other nodes participate update their blockchains after they have confirmed their consensus on the announced block (all presumed equal to) $BC^{n-1}$ to $BC^n$ by appending $B^n$ to $BC^{n-1}$ after checking its validity (Nagori et al., 2020; Jakobsson & Juels, 1999; Cachin, 2016):

$$BC^n = BC^{n-1} \parallel BC^n$$

(1)

It is implicit the possibility of computing a new block each time of Eqn. (1). This is not a mandatory assumption, but this article will make use of this assumption for convenience. Assume...
## Table 2. Comparative blockchain techniques based on the healthcare applications

<table>
<thead>
<tr>
<th>Author and Year</th>
<th>Objectives</th>
<th>Strength</th>
<th>Problem Findings</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Yue et al., 2016)</td>
<td>With the aid of an intelligent healthcare system built with a blockchain-based architecture, this article proposes an app architecture for patients to share and access data securely.</td>
<td>Proposed Method develop a healthcare data gateway application, but it can’t be properly tested or validated.</td>
<td>The designed application is not decentralized. Security and smart-contact issues are briefly discussed.</td>
</tr>
<tr>
<td>(Zheng et al., 2017)</td>
<td>The purpose of this survey is to review the Blockchain technology comprehensively</td>
<td>Health information was considered as one of the major applications of blockchain technology</td>
<td>Comprehensive overviews do not provide enough detail</td>
</tr>
<tr>
<td>(Witchey, 2019)</td>
<td>As presented, the healthcare transaction validation system and methods used in a chain of transaction blocks are considered to include a patient’s any inputs and outputs in their clinical trials by putting them in a blockchain network.</td>
<td>This article presents a detailed description of healthcare record validation with a systematic blockchain creation. An innovative process of monitoring and verification is proposed to ensure safe data transfer throughout the system.</td>
<td>With the integration of interesting food trends and enhanced security primitives and protocols, processes like cloud computing, conjugative computing, mobile computing, Artificial Intelligence (AI), and Machine Learning (ML) at 17 people will be able to meet future demands.</td>
</tr>
<tr>
<td>(Ben Basat &amp; Ronca, 2019)</td>
<td>To measure the effective application of blockchain technology to the digital healthcare system in Sweden quantitatively and qualitatively</td>
<td>To accept the technology widely in the healthcare industry, the study took into consideration the advantages of blockchain including globalization, data privacy, data security, and data ownership.</td>
<td>A small-to-medium-scale implementation of technology with its benefits would be more beneficial to the healthcare industry than using it on a large scale.</td>
</tr>
<tr>
<td>(Hussien et al., 2019)</td>
<td>This study has presented a comprehensive review of a healthcare blockchain application and system that is developing using blockchain technology.</td>
<td>In the simulation healthcare system, the roles of various stakeholders in the healthcare system were defined and simulated using well-designed algorithms in order to analyze the performance of the simulated system.</td>
<td>There is an opportunity to survey the use of blockchain technology in healthcare-related fields in depth by including a comprehensive survey of existing blockchain based applications.</td>
</tr>
<tr>
<td>(Tanwar et al., 2020)</td>
<td>The primary purpose of this project is to design, develop, explore and analyze a healthcare 4.0 application based smart healthcare system and overcome limitations of traditional healthcare systems to integrate chain code concert using Hyper Ledger Caliper for electronic storage of healthcare data and to make recommendations.</td>
<td>With the simulation healthcare system, the working of various stakeholders in the healthcare system were defined and simulated with well-designed algorithms to analyze the performance of the simulated system.</td>
<td>Instead of increasing the number of participants or large hospital inputs a mathematical model is used to test the scalability of the proposed approach rather than designing and integrating smart contracts. The proposed approach could be well validated with a model as opposed to simulation to convey the system’s functionality.</td>
</tr>
<tr>
<td>(Nagori et al., 2020)</td>
<td>The objective is to propose a system based on embedded multi-chain networks to be used in medical facilities to store health records electronically with security, decentralization, and data integrity.</td>
<td>Data transparency for the healthcare block chain network off-chain and among the three chains, in addition to authorized drug supply traceability</td>
<td>Implementation of simulation in the proposed approach does not invalidate it</td>
</tr>
</tbody>
</table>
that $R^{[n]}_n$, is the current round, a miner is recording transactions $t^{[n]}_1, \ldots, t^{[n]}_r$ in blockchain, and $h^{[n-1]}_n$ represents the hash value of $B^{[n]}$ (a further explanation of what a hash value is will follow). To mine a new block (it refers to the act of finding a no proof of work (PoW) was found for these):

**PoW**: Given, $h^{[n-1]}_n$, $t^{[n]}_r$, identify a nonce so as to:

$$H\left(h^{[n-1]}_n \ || \ t^{[n]}_r \ || \ r\right) \in y_{0,M} \ (1 \leq M \leq 256) \quad (2)$$

where:

$$t^{[n]}_r = t^{[n]}_1 \cdots t^{[n]}_r$$

According to the Eqn. (2), assume H is the Hash function of cryptographic SHA-256, used in Bitcoin:

$$0_M: M - \text{bits of 0s} \quad (4)$$

and:

$$Y_x: \text{set of 256 - bits whose first } X \text{ bits } = X \quad (5)$$

The hash value $h^{[n]}_n$ of the block $B^{[n]}_n$ is defined as the length of $X$. Therefore, $y_{0,M}$ is the set of 256-bits for which the first $M$ bits are all 0s:

$$h^{[n]}_n = H\left(h^{[n-1]}_n \ || \ t^{[n]}_r \ || \ r\right) \quad (6)$$

The chaining structure of the traditional blockchain model. Authors note that any single change in transactions $t^{[n]}_1, \ldots, t^{[n]}_r$ demands a re-computation of $r^{[n]}_r$ in PoW by Eqn. (2) and hence affects $h^{[n]}_n$ of $B^{[n]}_n$. This leads to a chain reaction to all $r^{[n]}_r$ and $h^{[n]}_n$ for $n > n$. The immutability of blockchain refers to its inability to modify any transaction deep within it, without making traces of it. As a result, traditional blockchain offers little to no immutability.

**4. METHODOLOGY**

In this section article present the architectural as well as the design view of our platform. The proposed technique model is presented in the figure 4.

The patient is the data sender and is responsible for sending her personal healthcare data to the system. A patient plays a major role in protecting the patient’s data. The data that will be sent
to the system must be accurate, otherwise any incorrect data will be detrimental to the patient, as the entire treatment depends on this sensitive information. Nevertheless, our system will take the encrypted data from the users. Encryption of data will happen at the beginning of proposed technique process execution. Data receivers will request for data after authenticating themselves to the system. Registration Unit will serve as an authenticator.

The proposed technique accepts encrypted data from users. Encryption of data will happen at the beginning of the process execution. Data recipients will request data after authenticating themselves to the system. Registration Unit will serve as the authentication system. After authentication, both parties will be able to interact with Private Accessible Units (PAUs) to move their private data around the cloud. They just need to log into the system and access through a secure channel. Through the PAU, it will send the private data of the users to the System. The PAU is the intermediary unit that connects the elements of the two levels in our system. Our PAU requires a secure channel of communication for it to interact with PAU.

The blockchain will store the data of the users. The transactions in the blockchain will return an identifier, which will help the users access the data further. For a better understanding, our system is divided into two levels. The User will interact with our system through the Graphical User Interface (GUI). Elements of Level-1 are: Registration Unit and PAU. During our second level - Level-2 - article will interact with low level elements of the system through PAU. An example of this is the element of level-2: blockchain. In our healthcare data repository, blockchain technology is being utilized. These techniques are using permissioned blockchain technology, which requires authentication. Our steps are as follows:

**Step-1:** In order to access the system, the data sender will provide his $ID$ (ID of the user) and $PWD$ (Password of the user).

**Step-2:** After gaining access to the system, the data sender will send data to PAU for storing.

**Step-3 and 4:** The third and fourth steps of our system would occur at level-2, where PAU would send $U_{ID}$ (Block id, where user data will be saved) to the blockchain and the blockchain would return $U_{ID}$ so that users could access the blockchain in the future and to locate the exact Block where the data was saved.

**Step-5:** The $U_{ID}$ generated by blockchain, PAU will be returned to Data sender in this next step.
Step-6: From this step, the rest of the steps are related to Data receiver. This step requires sign in as well as step-1, and after sign in, Data receiver can request data.

Step-7: In this step Data receiver will request for the data to Private accessible Unit along with the UID. PAU will receive the $U_{ID}$ for further use.

Step-8 and 9: PAU will request the blockchain along with the $U_{ID}$ in step-8 and the blockchain will return it to PAU in step-9. Step 8 & 9 are the same as steps 3 & 4 but the data are different.

Step-10: PAU sends the private data to the Data receiver at this point.

4.1 Cryptographic Tools

This paper describes elliptic curve cryptography (ECC) (Koblitz, 1987) for creating cryptographic functionality that is suitable for users. The formal definition of ECC will be provided here.

Definition 1: In Cryptography using elliptic curves, the trapdoor function is utilized. The trapdoor function computes B from A regenerating A from B is mathematically impossible:

$\overline{A \rightarrow B}$

There is a detailed description of all of ECC’s functionalities.

4.1.1 Encryption Scheme

Select the smallest value of $n$ for that $nG = 0$ to be a very large prime number. Elliptic group $E_p(a,b)$ and generator point, $G \in E_p(a,b)$.

There is an encoded message $(M)$ called, $P_m \in E_p(a,b)$. A private key is selected by both sender and receiver, $n_A < n$ . Compute public key $P_A$ in such a way that $P_A < n_A G$.

Cipher text point:

$P_c = \left[ (K G), (P_M + KP_B) \right]$ \hspace{1cm}

There is a random integer $K$ and a public key $P_B$.

4.1.2 Decryption Scheme

Plaintext point:

$P_M \leftarrow \left[ (P_M + K n_B G) \right] \leftarrow P_M + KP_B$ \hspace{1cm}

Private key $n_B$ can only be retrieved by receiver’s knowledge, $P_M$ can be removed, $K n_B G$.

5. RESULT AND ANALYSIS

The proposed approach tested by scripting the program on Solidity and Java 1.8.0.112 platform. The graphical representation of the performance values is designed on the MATLAB 2021a software on window 10, 8GB RAM operation system with line and bar chart. All the function and programs are written in Dev C++, MATLAB and Java. For the performance verification of the proposed approach
few performances metric is considered such as encryption time, decryption time, computation cost of key and block id in the blockchain model.

Figure 5 shows the encryption time (milliseconds) versus input size (KB) of the healthcare data. The proposed techniques are calculating the encryption time during the generation of the cipher text at the sender side. In which, this technique consider the various input size to see the rate of the growth changes of the encryption time along with the input size. The input size is varied from 5 to 30 KB of the data to simulate the encryption time.

Figure 6, Shows the transaction cost versus execution cost of smart contract. The string length (number of character) are used to calculate the computation cost. The string length is varied from the 5 to 100 number of characters. To have a correct interpretation of the performance outcome,
proposed method run the smart contract with various input string length sizes. As conclude from the figure 6, the computation cost is increasing with the string length or number of the characters. But the transaction and execution cost intervals are increased linearly and transaction cost is little bit higher as compare to the execution cost.

Figure 7, Shows the block-id generation versus string length of smart contract. One of the key terms to be ensured while writing smart contracts was block-id generation. The string length is varied from the 5 to 100 number of characters. As conclude from the figure 7, the block-id generation is interestingly almost constant with the string length or number of the characters. The block-id generation is same it’s not change with the block-id generation for both transaction and execution cost. The transaction cost is higher as compare to the execution cost but constant.

Figure 8, shows the decryption time (milliseconds) versus input size (KB) of the healthcare data. The proposed techniques are calculating the decryption time during the generation of the plain text.

Figure 7. Block id-generation cost versus string length (number of character)

![Figure 7](image1)

Figure 8. Decryption time (milliseconds) versus input size (Kb)

![Figure 8](image2)
at the received side. In which, article consider the various input size to see the rate of the growth changes of the decryption time along with the input size. The input size is varied from 5 to 30 KB of the data to simulate the decryption time.

Both input and output are generated independently. Encryption takes place in the process of providing input, and decryption occurs once output is provided. Figure 9. Illustrates how two processes take very different amounts of time while being executed. Both time and length increase as strings get longer, but encryption requires more time than decryption. Encryption takes approximately 80 to 90 milliseconds while decryption takes less than 10 milliseconds.

6. CONCLUSION

The management of healthcare data has gained increasing attention in the last few years due to its capability of improving accuracy, enhancing efficiency, and lowering costs. Due to its ability to address issues such as single points of failure, data stewardship, system vulnerabilities, distributed information, and high security and privacy risks existing in client-server cloud based existing healthcare systems, blockchain technology can improve the management of medical data. In our paper, proposed method describe a privacy-preserving platform in the cloud for healthcare data. This technique defines and argue why such attributes are essential for a cloud-based data management system for healthcare. According to our analysis, our platform can meet all these requirements. Experiments have shown that this platform works well in the blockchain environment. In the future, proposed technique will be exploring how different healthcare processes interact, and another direction would be improving key theft mechanisms and key distribution methods.
REFERENCES


Gerstl, D. S. (2016). Leveraging bitcoin blockchain technology to modernize security perfection under the uniform commercial code. *International Conference of Software Business*, (pp. 109–123). doi:10.1007/978-3-319-40515-5_8


Preeti Rani is a Research Analyst in the Wireless Communication System, Ghaziabad India. She received his bachelor’s degree in Electronics & Communication Engineering from the Raj Kumar Goel Institute of Technology for Women, Ghaziabad. She did her M. Tech. (Remote Sensing) from Banasthali Vidyapeeth, Rajasthan. She obtained her one year research from CSIR-NIO, Dona Paula Goa in the area of Satellite Communication.

Sonia Verma earned his M.Tech. degree in Computer Science and Engineering from Shubharti University, Meerut, India, in 2014. She is currently pursuing Ph.D and worked as a research scholar. She has more than 9 years of experience in teaching, industry and administration. She is currently working as an Research Scholar at SRM IST Delhi-NCR Campus, Ghaziabad (U.P.). Her area of interest includes Machine learning, Artificial intelligence, IOT, Cloud computing etc. She has published total 4 research papers in international journals and conferences etc.

Satya Prakash Yadav is currently the Associate Professor of the Department of Computer Science and Engineering, GL Bajaj Institute of Technology and Management (GLBITM), Greater Noida (India) and perusing Postdoctoral Research Fellow under the supervision Prof. (Dr.) Victor Hugo C. de Albuquerque, from Federal Institute of Education, Science and Technology of Ceará, Brazil since February 01, 2022. He has awarded his PhD degree entitled “Fusion of Medical Images in Wavelet Domain” to Dr. A.P.J. Abdul Kalam Technical University (AKTU) (formerly UPTU). A seasoned academician having more than 15 years of experience, he has published four books (Programming in C, Programming in C++ and Blockchain and Cryptocurrency) under I.K. International Publishing House Pvt. Ltd. Including Distributed Artificial Intelligence: A Modern Approach, Published December 18, 2020 by CRC Press. He has undergone industrial training programs during which he was involved in live projects with companies in the areas of SAP, Railway Traffic Management Systems, and Visual Vehicles Counter and Classification (used in the Metro rail network design). He is an alumnus of Netaji Subhas Institute of Technology (NSIT), Delhi University. A prolific writer, Dr. Satya Prakash Yadav has published two patents and authored many research papers in web of science indexed journals. Additionally, he has presented research papers at many conferences in the areas of Image Processing, Information retrieval, Features extraction and Programming, such Digital Image Processing, Feature Extraction, Information Retrieval, C, Data Structure, C++, C# and Java. Also, he is a Editor in Chief in Journal of Cyber Security in Computer System (MAT journals), Series Editor in Bentham Science and Lead Editor in CRC Press, Taylor and Francis Group Publisher (U.S.A), Tech Science Press (Computer Systems Science and Engineering), International Springer Publisher, Science Publishing Group, (U.S.A), and Eureka Journals, Pune (India).

Bipin Kumar Rai is Professor in the Information Technology Department, ABES Institute of Technology (ABESIT), Ghaziabad (India). He is B.Tech(CSE) from UPTU Lucknow, India, M.Tech(CSE) from RGPV Bhopal, India and Ph.D. from Banasthali University Rajasthan, India. He has more than 16 years of experience, published three books, two patents and authored 20+ research papers in the reputed Journals/Conferences

Mahaveer Singh Naruka earned his B.E. in Electrical Engineering from Govt Engg College, Kota and M. Tech. degree in Power System From Rajasthan University. He is awarded Ph.D. on "Power Quality Aspects for Switched Reluctance Motor Drives" from Uttarkhand Technical University, Dehradun. He has a rich experience of 18 years in academics and has published more than 15 research papers in peer reviewed and indexed international journals. He is a Member of IEEE, Life member of ISTE, Nominated member of Script Review committee in Tata McGraw-Hill Publication, Peer Reviewer of American Journal of Electrical & Computer Engineering, New York, U.S.A., Member of Program Committee of International IEEE Conference on Automation, Computational & Technology Management & International IEEE Conference on Automation & Computational Engineering. His areas of interest include Power Quality, Power Electronics and Drives, Custom Power Devices, Power factor correction techniques etc.

Devendra Kumar is working as an Assistant Professor in the Dept. Of Computer Science, Wachemo University, Durame, Ethiopia.