Indonesian Journal of Electrical Engineering and Computer Science
Vol. 15, No. 1, July 2019, pp. 328~335
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v15.i1.pp328-335

Cloud based secured framework for implementation of online voting system

Gururaj K S[1], K Thippeswamy[2]
[1]Computer Science & Engineering, Visvesvaraya Technological University, India
[2]Department of Studies in CS&E, PG Center, Visvesvaraya Technological University, India

Article Info

Article history:

Received Jan 3, 2019
Revised Feb 21, 2019
Accepted Feb 28, 2019

Keywords:

CloudSim
Cryptography
Online voting system
Security in cloud environment

ABSTRACT

Accessing and Utilization of data and information from remote location is one of the major requirements of present world. Due to the increase in the requirement of the data access from remote locations, challenges in the enhancement of technology based systems also have increased proportionately. Technology based solution for accessibility of remote data with available infrastructure is the need of the hour. Implementation of technology based solutions for the challenges may be expensive due to the current technical limitations. In this paper, we have attempted to design a secured cloud based framework for Online Voting System and analyzed its performance based on the three cryptographic algorithms namely Blowfish, AES and RSA.

Corresponding Author:

Gururaj K S,
Department of Computer Science & Engineering,
GSSS Institute of Engineering and Technology for Women,
KRS Road, Mysore, Karnataka, India.
Email: gururaj.k.s79@gmail.com

1. INTRODUCTION

Development of society depends of the choice of right person at right places through the free and fair elections with participation of all the citizens in the voting process. Due to various reasons, some of the citizens may not be able to take part in the election process. It may be due to lack of interest in election process, method of conduction of elections or non availability of the person at the polling location due to migration to faraway places in pursuit of food, shelter and job opportunities.

Non participation of people who migrate from one place to other place may lead to electing of person who may not be fit for the position and lead to spoil/corrupt the system. Though they are interested to involve in voting, they do not have any facility for voting away from their polling places. Hence Online Voting System (OVS) could be the better option for the participation of all the citizens including those who have migrated.

Cloud based system can be one among the approaches for effective implementation of better and error free Online Voting System. Cloud system supports the usage of large number of secured transactions at the same instance on large data sets [1, 2]. Inorder to analyse the performance of the system, the key features are to be analysed refered to as work load parameters. Speed and Security factors are the major performance measures corresponding to the analysis of these systems. As per the survey, higher the performance in speed obviously may decrease the security of the system and vice versa. Workload prediction is one of the major factors to be considered for the analysis of the cloud system [3, 4]. Cloud computing provides large scale economic and business computing environment with with virtualization aspects for development of parallel, distributed computing systems using internet [5]. Hence, we propose to design a cloud based framework using available technology, analyse it with respect to speed and security and conclude to utilise one among

the cryptographic algorithms (Blowfish, AES and RSA in the proposed system) for the specified cloud framework configurations.

2. LITERATURE SURVEY

2.1. Migration

In the current scenario, technology is growing rapidly which is a factor that makes us feel that world is very small with respect to communication and accessing of data from different part of the world. Young people working in industries of metropolitan cities usually migrate from one place to other in pursuit of career growth and improved life style [6].

Migration usually affects the voting rate in elections indirectly as the person needs be available at his location for voting during elections. Work pressure, longer distance from native, economical conditions and other factors force the person from being available at their location during election which leads to the downfall in the voting rate [7].

2.2. Computer Literacy

Computer and Mobile awareness has increased drastically in the last decade. Mobile usage has enhanced the accessibility and storage of data from various devices connected to each other. India has around 307 million smart phone users as on 2017. Figure 1 represents the increase in the number of smart phone users from 2008 to 2017. Security and speed of accessing the data stored on cloud is one of the major challenges in sharing of the huge data generated by the devices throughout the world. Ensuring the security and enhancing the speed of data access are the major requirements in cloud computing [9].

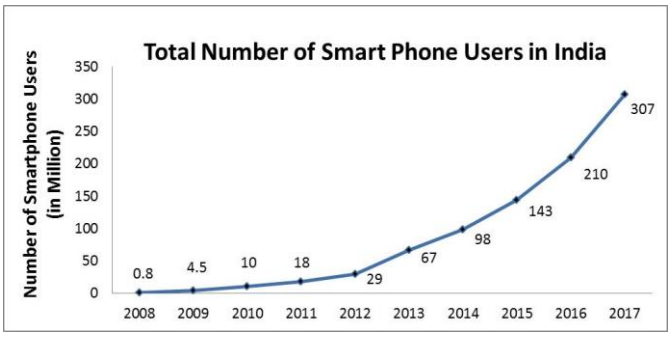

Figure 1. Statistics of smart phone users in India [8]

2.3. Voting Systems

Diagrammatic representation of the online voting system is represented in Figure 2 in which the voters can cast their vote from remote places using mobiles and computers. Separation of data content reduces the web content replication and the representation of data is incorporated using extensible markup language.

Generic requirements for a voting system should involve the following factors:

Authenticity: Eligible and valid voters vote using the system.

Integrity/accuracy: Once the vote is casted system should not permit for multiple voting by same voter and allow for modifications in the vote.

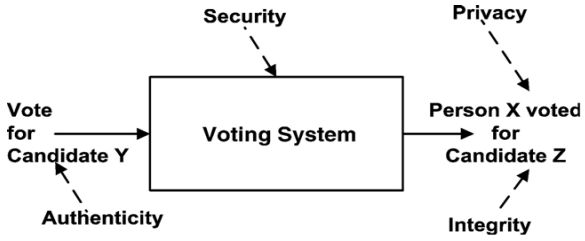

Figure 2. Generic set of requirements for voting system.

Privacy: Details of the vote casted should be kept confidential from the external users.
Security: Voting process should be tamper proof and unauthorized access to the process should be avoided.
Democracy: System should provide provision for all eligible voters to vote and without any fear and from all parts of the world [10].

Finger-print based application is another approach for remote system approach for voting. System generates the voter id for all the eligible voters using the data provided in the aadhar database which ensures that all the eligible voters are listed out and involve in the voting process. Voter id is generated using all the information available in the aadhar database such as name, DOB (Date of Birth), finger print and iris scan image information. When the voter tends to vote during the elections, voter id can be downloaded from the mail and can be used during voting. In order to vote, voter has to login with the finger print which will be authenticated using the data provided in the aadhar data base. Multiple voting is avoided by blocking the user from voting once the voter has logged in once and casted the vote [11].

Electronic voting is an approach for carrying out the election process in an efficient and secured manner. It can be utilized for conducting the election in a fair manner. Voting system is a simple representation of the decision system which is further enhanced to implement the features of voting process. Security is preserved by ensuring the integrity and authentication of the vote and the voter respectively during the voting process [12]. Integrity, confidentiality and availability are the key components of an Online Voting System [13]. Key components of the voting system can be ensured through cryptographic algorithms such as Blowfish, AES and RSA.

The advantages of Electronic Voting are:
Portability: Device can be used on public and private network.
Modes of operation: System can be used as online/offline mode as based on the requirement.
Two-way Authentication: Authentication is ensured by sending OTP (One Time Password) through mail and SMS.
Custom Applications: System can be used as survey system or Ballot based Voting System.

2.4. Cloud Security

Government and industry are concerned with dealing with unexpected persistent security threats of Cloud Computing Systems (CCS). Various estimates for analyzing the extent of confidentiality and integrity provided by Cloud Service Providers (CSP) are provided in different Cloud Architecture Reference Models. Cloud-Trust is considered as a useful parameter for assessing the security aspects of multi-tenant cloud architectures which provide Infrastructure as a Service. Cloud Security Penetration rate increases to maximum if the system has very less security controls. Rate of Cloud penetration decreases substantially if the security level is increased to protect the virtual machine (VM) instances which in execution along with the access control for the administrators by employing the network surveillance and discovery of live virtual machines [14]. Cloud Security Alliance (CSA) defines the boundries between the Service provider and the service user with maximum responsibilities at the SaaS and least services at the IaaS for the provider. Handling of security responsibilities is tedious task even though the responsibilities have defined boundries due to various constraints such as non detection of vulnerabilities and threats at early stage [15].

Rashidah Funke Olanrewaju et.al. says that data in transit can be protected from unauthorized injections using a validation protocol algorithm based on hash functions which uses a one time security header for transferable files [16]. Along with speed and security of the data in Cloud environment, Data Integrity also plays a very important role. Neha Narayan Kulkarni et.al. proposes a new data integrity framework to retain data integrity in cloud environment using Identity Based Remote Data Integrity Checking and recovery using the XOR operation [17]. Compatibility, integrity, availability and confidentiality has to be ensured for a succesful implementation of a system on a cloud environment [18].

Fully Homomorphic is an approach for protecting users' data using Fully Homomorphic Encryption (FHE) scheme deals with protection and processing of cloud environment. Optimal Fully Homomorphic Encryption (O-FHE) is a novel FHE Scheme which deals with solving the issues involved in design of FHE. Higher efficiency and accuracy is achieved using Kronecker Product (KP) properties. Non noise computations for cipher-texts is achieved by O-FHE and the plain-text outputs are extracted within a specified time frame using decryption. Homomorphic mathematical computations are computed using multiplications and additions [19].

Security system for cloud storage using Third Party Authentication, proper key management scheme using load balancing and low computational complexity is another approach for providing security for cloud systems. Such a System Model involves three key components namely the User, Cloud Service Provider (CSP) and Third Party Authenticator (TPA) [20].

2.4.1. AES Algorithm, Blowfish Algorithm and RSA Algorithm

Protection and privacy of the data can be achieved by using sophosticated mechanisms such as encryption techniques which depends on the number of key points used and the sequence of steps involved in encryption and decryption process [21]. AES algorithm is a symmetric key algorithm which means that the key used for encryption and decryption is the same key. It has mostly replaced the traditional DES algorithm which was very popular earlier and is now been replaced by AES and is also used for encrypted confidential information used by the United States government. Algorithm consists of 128 bit block size and the key size varies from 128, 192 or 256 bits and the number of repetitions of the cycle depends on the key size standing at 10, 12 and 14 cycles respectively corresponding to the three key sizes.

Blowfish algorithm basically is a block cipher having a size of 4 to 56 bytes of block. The procedure for decryption is the same as for encryption which means to say that it is a symmetric algorithm. Apart from being open source, it also has the advantages of being fast and secure.

Encryption and decryption of data in modern computer systems and other electronic devices is carried out using RSA algorithm. It is an asymmetric cryptographic algorithm which requires two unique keys for encryption and decryption of data. RSA is public key crypto system where one of the unique key is shared to all the users [22, 23].

2.4.2. Cloudsim Tool

Cloudsim tool is used to simulate the cloud environment. It is an open source tool consisting mainly of Java libraries developed for various tasks which emulate a real cloud environment setup in the virtual mode. It supports for modeling and simulation of virtualized Cloud-based data center environments with dedicated management interfaces for (Virtual Machines) VMs, memory, storage, and bandwidth. It can be used to address the issues related to provisioning of hosts to VMs, managing application execution, and dynamic system state monitoring, are handled by this layer. It is an efficient tool for for studying the efficiency of different policies in allocating its hosts to VMs and the strategies at different layers [24, 25].

3. PROPOSED METHODOLOGY

Figure 3 depicts the proposed methodology, where the focus is more on the design of Cloud framework and its performance (speed and security) with respect to cryptographic algorithms.

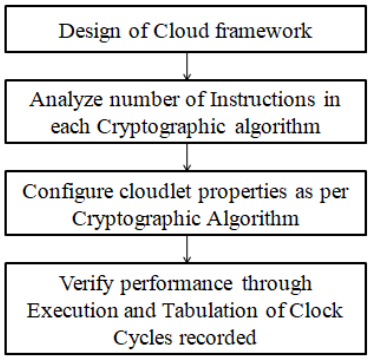

Figure 3. Proposed methodology - cloud based secured framework for implementation of online voting system

4. PROPOSED CLOUD FRAMEWORK

Figure 4 depicts the proposed framework for implementation of secured cloud environment to enable online voting system. Proposed framework involves the third party authentication server which can be regarded as a controller. Controller generates ticket and grants access only to authorized voters through online. Cloud can permit access the account or the information only to the users providing authorized ticket from the controller. Finally cloud acknowledges the controller regarding the account access by the eVoter.

To ensure or establish the secured communication between the components, a cryptographic algorithms namely Blowfish, AES and RSA are employed. In Normal circumstances, as the requirement for the security increases, the performance of the system reduces considerably. Hence the performance analysis of these algorithms is done by considering key tasks in the system and simulated cloud environment using

CloudSim tool. In the above proposed cloud framework, certainly the encryption, decryption tasks at controller, cloud and user plays a very important role. Around four key tasks are identified in the proposed framework for the analysis. Since the bandwidth and other parameters of the internet are relative to the environment and not definite or unknown, the performance of only these key tasks is considered for the evaluation.

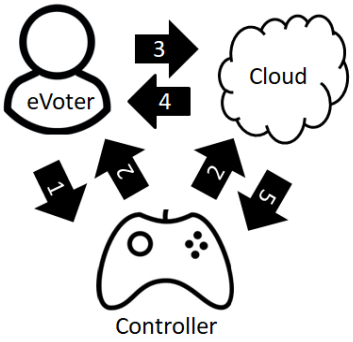

Figure 4. Proposed framework for secured cloud based OVS

Key tasks are:
K1: Encryption of ticket at the controller
K2: Decryption of ticket at the cloud
K3: Encryption of ACK at the cloud
K4: Decryption of ACK at the Controller

Better performance of these encryption and decryption activities at various stages of the system plays an important role in the implementation of the proposed online voting system. Hence the algorithm has to be efficient enough to implement the same.

5. RESULTS OR PERFORMANCE ANALYSIS

Figures 5, 6 and 7 represent the cloudlet properties configured for RSA, Blowfish & AES algorithms respectively. Figure 8 reflects the virtual machine configuration for the implementation of the specifiifed algorithms. Length of the algorithm indicates the total number of instructions in the program required to generate the output file from input file. Number of instructions (N) executed of each algorithm is described in the Table 1.

```
// Cloudlet properties
int id = 0;
long length = 50000;
long fileSize = 188000;
long outputSize = 256000;
```

Figure 5. Cloudlet properties of RSA algorithm

```
// Cloudlet properties
int id = 0;
long length = 196486;
long fileSize = 188000;
long outputSize = 188000;
```

Figure 6. Cloudlet properties of Blowfish algorithm

```
// Cloudlet properties
int id = 0;
long length = 246792;
long fileSize = 188000;
long outputSize = 188000;
```

Figure 7. Cloudlet properties of AES algorithm

```
// VM description
int vmid = 0;
int mips = 1000;
long size = 10000; // image size (MB)
int ram = 1024; // vm memory (MB)
long bw = 1000;
int pesNumber = 1; // number of cpus
String vmm = "Xen"; // VMM name
```

Figure 8. Virtual Machine description

Number of instructions (N) for each algorithm is computed based on the number of rounds of each algorithm(R), number of statements in the core level (S) and number of times the instructions has to be repeated (n) as specified in (1). Number of repetations (n) depends on the input file size (F) and the number of bits (B) for each algorithm as represented in (2).

$$N = (R*S)*n \quad (1)$$

$$n = F/B \quad (2)$$

Table 1. Cloudlet Configurations for the Proposed Cryptographic Algorithms

	No. of Instructions	File size	Output size
Blowfish	((16*4)+3)*2938 196846	188000	188000
AES	(14*6)*2938 246792	188000	188000
RSA	50000	188000	256000

Cloudlets are the tasks containing the routine or the functionality properties to execute in cloud environment. Hence, each algorithm is considered as a cloudlet configuring the properties of the cloudlet for each algorithm appropriately. Table 2 depicts the performance of the three algorithms, which is as per the analysis of the number of statements required to run the algorithms.

Table 2. Simulated Performance of Three Cryptographic Algorithms with Respect to Four Key Tasks

	No. of Key tasks * performance
Blowfish	4 * 196.49 clocks
AES	4 * 246.79 clocks
RSA	4 * 50 clocks

Performance estimation is multiplied with 4 (number of key tasks), which may be the overall clocks (assumed time unit) required to satisfy one individual voting. As per the survey Blowfish is one the secured and efficient algorithm when compared to AES and RSA. Hence the experimental graph which is shown in Figure 9 clearly reflects the strength and efficiency of Blowfish algorithm.

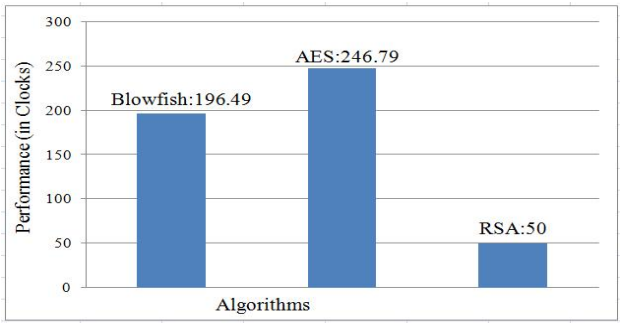

Figure 9. Performance graph of three cryptographic algorithms with respect to four key tasks

6. CONCLUSION

In this paper we have tried to provide sufficient statistics for the need of online voting system in the current society. We also have proposed a secured cloud framework as a technology solution which may enhance the voting rate in elections. Security of the proposed Cloud framework for online voting system is achieved at two levels namely, with the help of encryption and decryption of token at voter and controller by denying direct access of the cloud to the voter. This will reduce the payload on the cloud as the controller shares the majority of the voter related activities. Proposed framework has been designed by analyzing and recommends an efficient cryptographic algorithm for ensuring the security of the online voting system. This paper concludes that the Cloud based framework designed for online voting is secured with better

performance (in terms of speed) when implemented using Blowfish algorithm since it is faster than AES (as per analysis) and secured than RSA (as per survey) corresponding to specified configurations.

ACKNOWLEDGEMENTS

Authors would like to thank all the people who have directly or indirectly supported in the preparation of this paper. We would like to thank Regional Center, VTU, Mysuru and GSSS Institute of Engineering and Technology for Women, Mysuru for their kind support.

REFERENCES

[1] Abdullah MohammedAl-Faifi n, BiaoSong, Mohammad Mehedi Hassan, AtifAlamri, AbduGumaei, "Data on performance prediction for cloud service selection", *Data in Brief* 20(2018) 1039–1043.
[2] Bautista Villalpando et al., "Performance analysis model for big data applications in cloud computing", *Journal of Cloud Computing: Advances, Systems and Applications* 2014.
[3] In Kee Kim, Wei Wang, Yanjun Qi, Marty Humphrey, "CloudInsight: Utilizing a Council of Experts to Predict Future Cloud Application Workloads", 2018 IEEE 11th *International Conference on Cloud Computing*.
[4] Jiang Zhou, Dong Dai, Yu Mao, Xin Chen, Yu Zhuang, Yong Chen, "I/O Characteristics Discovery in Cloud Storage Systems", 2018 IEEE 11th *International Conference on Cloud Computing*.
[5] Peng Wang, Robert X. Gao, Zhaoyan Fan, "Cloud Computing for Cloud Manufacturing: Benefits and Limitations", *Journal of Manufacturing Science and Engineering,* August 2015.
[6] R. Srivastava and S. Sasikumar, "An overview of migration in india,its impacts and key issues impacts of internal and international migration on indian development," in Paper for Regional Conference on Migration, Development and Pro-Poor Policy Choices in Asia, 2003.
[7] L. Ezzarqui, "Research paper on migration," Alliance of civilizations, 2006.
[8] http://www.dartconsulting.co.in/market-news/e-commerce-industry-current-online-retail-e-commerce-market-scenario-in-india/, Accessed on 02/05/2017
[9] D. A. Fernandes, L. F. Soares, J. V. Gomes, M. M. Freire, and P. R.In´acio, "Security issues in cloud environments: a survey," *International Journal of Information Security*, vol. 13, no. 2, pp. 113–170, 2014.
[10] G. Z. Qadah and R. Taha, "Electronic voting systems: Requirements, design, and implementation," *Computer Standards & Interfaces*, vol. 29, no. 3, pp. 376–386, 2007.
[11] R. Bhuvanapriya, P. Sivapriya, V. Kalaiselvi et al., "Smart voting," in Computing and Communications Technologies (ICCCT), 2017 2nd International Conference on. IEEE, 2017, pp. 143–147.
[12] A. J. Chemmanam, S. Sreelekshmi, K. S. Faris, M. V. Sairam, and B. A. Jose, "Portable e-voting decision system," in *Computer Communication and Informatics (ICCCI)*, 2017 International Conference on. IEEE, 2017, pp. 1–6.
[13] Amarjeet Singh, Ramakanth Kumar P, Nagarj G Choolli, "Empowering E-governance with E-voting", in *Indonesian Journal of Electrical Engineering and Computer Science*, Vol 12, No. 3, December 2018, pp. 1081-1086.
[14] D. Gonzales, J. M. Kaplan, E. Saltzman, Z. Winkelman, and D. Woods, "Cloud-trust a security assessment model for infrastructure as a service (iaas) clouds," *IEEE Transactions on Cloud Computing*, vol. 5, no. 3, pp. 523–536, 2017.
[15] Shaz Alam, Mohd Muqeem, Suhel Ahmad Khan, "Review on Security Aspects for Cloud Architecture", *International Journal of Electrical and Computer Engineering (IJECE)*, Vol. 8, No. 5, October 2018, pp. 3129~3139.
[16] Rashidah F O, Thouhedul Islam, Othman O K, Fawwaz E F, "Data in Transit Validation for Cloud Computing using Cloud based Algorithm detection of Injected Objects", *in Indonesian Journal of Electrical Engineering and Computer Science*, Vol 10, No. 1, April 2018, pp. 348-353.
[17] K. Neha Narayan Kulkarni, Shitalkumar A. Jain, "Checking integrity of data and recovery in the cloud environment", in *Indonesian Journal of Electrical Engineering and Computer Science*, Vol. 13, No. 2, February 2019, pp. 626-633.
[18] Sugandh Bhatia, Jyoteesh Malhotra, "CSPCR: Cloud Security, Privacy and Compliance Readiness - A Trustworthy Framework", *International Journal of Electrical and Computer Engineering (IJECE)*, Vol. 8, No. 5, October 2018, pp. 3756~3766.
[19] K. Gai and M. Qiu, "An optimal fully homomorphic encryption scheme," in Big Data Security on Cloud (BigDataSecurity), *IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS)*, 2017 IEEE 3rd International Conference on. IEEE, 2017, pp. 101–106.
[20] J.-S. Chueh and M.-T. Sun, "Design and implementation of security system for cloud storage," in *Network Operations and Management Symposium (APNOMS)*, 2017 19th Asia-Pacific. IEEE, 2017, pp. 129–134.
[21] D. Ramesh, B. Rama, "Secure Privacy Implications for Clients and End-users through Key Assortment Crypto Techniques Implicated Algorithm", *International Journal of Electrical and Computer Engineering (IJECE)*, Vol. 8, No. 6, December 2018, pp. 5443~5448.
[22] RSA Key Length, http://www.javamex.com/tutorials/cryptography/rsakeylength.shtml, Accessed October 23, 2017.

[23] Ahmed Eskander Mezher, "Enhanced RSA Cryptosystem based on Multiplicity of Public and Private Keys", *International Journal of Electrical and Computer Engineering (IJECE)*, Vol. 8, No. 5, October 2018, pp. 3949~3953.
[24] Rodrigo N. Calheiros, Rajiv Ranjan, Anton Beloglazov,C´esar A. F. De Rose, Rajkumar Buyya, "CloudSim: a toolkit for modeling and simulation of cloudcomputing environments and evaluation of resourceprovisioning algorithms", Software – Practice And Experience, 2011;41:23–50.
[25] Taskeen Zaidi, Rampratap, "Virtual Machine Allocation Policy in Cloud Computing Environment using CloudSim", *International Journal of Electrical and Computer Engineering (IJECE)*, Vol. 8, No. 1, February 2018, pp. 344~354

BIOGRAPHIES OF AUTHORS

Dr.K.Thippeswamy: Received his Ph.D. degree from the Department of Computer Science and Engineering, Jawaharlal Nehru Technological University, Ananthapur, Andra Pradesh in the year 2012, M.E degree in Computer Science and Engineering from University Visvesvaraya College of Engineering (UVCE), Bangalore in 2004 and Bachelors Degree in Computer Science and Engineering from University B.D.T College of Engineering (UBDTCE), Davangere in the year 1998. He is currently heading the Department of Computer Science and Engineering, Visvesvaraya Technological University, PG Center, Mysore, Karnataka, where he is involved in research and teaching activities. His major areas of research are Data Mining & Knowledge Discovery, Big data, Information Retrieval, and Cloud Computing. He is having 19 years of Teaching and 3 years Research experience. He has published around 40 papers which include International Journals, International Conferences and National Conferences. He is Reviewer Committee Member for the international Journal Bioinformatics and Data Mining. He has organized one International Conference and two National Conference and many workshops. Currently he is working as Professor and Chairman, Dept. of Studies in Computer Science & Engg. VTU, PG Centre, Mysuru.

Gururaj K S: Pursuing his Ph.D. degree in Visvesvaraya Technological University, Belagavi, India and Working as a Associate Professor in GSSS Institute of Engineering and Technology for Women, Mysore, India. He has totally 16 years of teaching experience in engineering colleges of Karnataka. He completed his BE from Karnatak University, Dharwad and Masters Degree from VTU, Belagavi, Karnataka, India.