

# Performance analysis of cryptography algorithms for implementation of secured cloud based online voting system

Karanam Subramanyam Gururaj<sup>1</sup>, Kampalappa Thippeswamy<sup>2</sup>

<sup>1</sup>Department of Computer Science and Engineering, GSSS Institute of Engineering and Technology for Women, Mysuru, India

<sup>2</sup>Department of Computer Science and Engineering, Visvesvaraya Technological University, Mysuru, India

## Article Info

### Article history:

Received Jun 9, 2022

Revised Dec 16, 2022

Accepted Jan 16, 2023

### Keywords:

Cloud based framework

Cryptography algorithms

Online voting system

Security

## ABSTRACT

Any democratic country intends to conduct the elections in a smooth and fair manner such all the citizens of the country participate and elect their leader who can involve himself/herself for the development of the country. In spite of wide publicity and measures taken for ensuring the participation of all the citizens in the election process, most of the countries are unable to achieve 100% voting rate in elections. Among the many reasons for reduction in voting rate, migration of the voters is one of the major reasons for reduction in voting rate. Even though technology and online services have been used in almost all the aspects of day-to-day activities, online features have not been utilized in the process of voting during elections. This paper tries to analyze the performance of the cloud based secured framework by implementing it using PHP and MySQL. Security of the framework is implemented using rivest shamir adleman (RSA), advanced encryption standard (AES) and Blowfish cryptography algorithms.

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



## Corresponding Author:

Karanam Subramanyam Gururaj

Department of Computer Science and Engineering

GSSS Institute of Engineering and Technology for Women

KRS Road, Metagalli, Hebbal Industrial Area, Mysuru, Karnataka 570016, India

Email: gururaj.k.s79@gmail.com

## 1. INTRODUCTION

Elections play a vital role in the development of a country. Many people are unable to participate in the election process due to various reasons such as migration from one place to another place, illiteracy, not interested in elections due to current political scenario to name a few. Non participation of such people in election may lead to the electing of person who may not be a suitable person for the position. Migration of people from one place to the other in search job, marriage, food and shelter affects the presence based election system as the voter should be present to participate in voting at their respective electoral zone. People who have migrated may or may not be able to participate in elections due to work pressure, longer distance from native, economical conditions and so on which leads to electing of a leader who is not a correct choice to lead the society [1]–[3]. Participation of everyone in voting is one of the major requirements of society's good move. Though they are interested to involve in voting, they do not have any facility for voting away from their polling places.

To enhance the voting and enable participation of voters from remote location, a highly secured, accessible cloud based online voting system is the required. Online opinion systems are available for providing opinion on many aspects such as products, venues, and events. Based on the rating provided by the users, customer satisfaction survey is carried out and the choice of the available options is made by the customers. There are many cloud services provided by the host as well as from the third party vendors to

ensure the data security, data integrity and privacy of cloud usage, but the online services from the perspective of online voting system is rare and such online elections are restricted to certain local bodies. Hence, an online voting system is required to enhance the voting rate which provides the opportunity to all for participation in elections.

## 2. LITERATURE SURVEY

The voting system used in elections play a vital role in the successful completion of elections. Several implementations of the voting system have been carried out in enhancing the effectiveness of the elections. Electronic voting systems are used in different countries to provide efficient voting procedures. However, the security issues related to electronic voting are the major topic of discussion. Lack of transparency is one of the major differences in traditional and electronic voting systems in which the operations on data cannot be observed [4], [5]. Mobile voting system is a convenient, easy and efficient way for overcoming the drawbacks of the traditional systems. Security is ensured using one time password (OTP) and captcha to ensure that humans are using the system. Eligibility of the voter is verified by using Aadhar card or any other age proof [5], [6]. One of the approaches for ensuring 100% voting is the use of finger print based voting system. Data from the Aadhar data base such as name, date of birth, finger print, iris image can be used to generate the voter ID and voter is authenticated using the data of the Aadhar database [7].

National and international migration is a regular phenomenon these days for various reasons such as food, marriage, community, and in search of job. Urban net migration is one of the primary factors for one fifth of the urban population growth which has been observed during sixties and has been gradually reduced between 1991 and 2001 as compared to earlier decade [8], [9]. Better job opportunities are a major factor that affects the migration in most of the Indian districts. Male migration rate and female migration rates equally determine the economic factors which are very influential in the migration indicating very few single women migrations [10]. It can be observed that marriage and work are the two main factors for migration during the last decade. Work and marriage are the major factors for migrations from the perspective of males and females respectively [11]. Security of the system using online or offline approach in computing environment is an important and critical challenge which has to be dealt with to overcome the threats and vulnerabilities that can cause damage to the system [12]. Cloud environments require the efficiency in terms cost and administrative overheads. To achieve this, a framework is essential which encrypts data and provides secured, fair and concurrent information to the end users [13]–[15].

Blowfish is a 64 bits block cipher which was designed in 1993 but its usage exists even today in all the government and non-government applications. Blow fish generates a variable key of length ranging from 32 to 448 bits [16], [17]. Advanced encryption standard (AES) algorithm is another cryptographic algorithm considered in this research work or encryption and decryption activities of the ticket during its transmission. AES is symmetric key and encryption block cipher. Its key length ranges from 128 to 256 bits [18], [19] rivest shamir adleman (RSA) can also be used for encryption and decryption of ticket in the proposed system. Basically RSA is an asymmetric key cryptographic technique which uses two different keys for encryption and decryption activities [20]–[23]. Machine learning method can be used for detecting the security breach on systems designed as URL-based, domain-based, page-based, and content-based [24].

Analysis of the census data using Pearson's correlation coefficient has proved that the population growth rate has been one of the reasons for decrease in the voting rate due to the fact that most of the voters are unable to vote due to migration. Analysis based on the census data using Naive Bayes approach shows that probability of voting when literacy is given is 67% and probability of voting when given population growth is 32% [1]. Analysis of the data sets collected by the authors using Pearson's correlation coefficient and Naive Bayes algorithms through the questionnaire shared through Google Form and social media, reflects the opinion of the users with respect to computer literacy, voting mechanism and migration as a hurdle and results suggests that 65% of the users showed their interest towards the introduction of technology in voting system [2].

## 3. METHOD

Implementation of online voting is one the challenging tasks as large number of voters try to vote using the system simultaneously. Security, speed, ease of use, accessibility, consistency of results play an important role in execution of the framework for secured online voting system. Method for the performance analysis of cloud based framework for online voting system using cryptography algorithms such as RSA, AES and Blowfish is represented in Figure1.

### 3.1. Design of the cloud based framework for online voting system

Cloud based framework for design of online voting system is represented in Figure 2 [11]. Blowfish, AES and RSA algorithms are used to ensure secured communication between three modules across internet. Steps involved in the process of voting by the evoter using the above frame is described as:

- Step 1: eVoter module request for authentication ticket to continue further transaction with the cloud.
- Step 2: controller generates a unique ticket and shares the ticket to evoter and cloud module simultaneously. Validity of the ticket is intimated to the cloud module while ticket is communicated to the cloud module.
- Step 3: inorder to vote, eVoter attaches the copy of the ticket along with the transaction data of voting and sends it to the cloud module which declares transaction successful if the ticket matches.
- Step 4: cloud acknowledges the controller about the transaction carried out by the eVoter along with timestamp details.
- Step 5: cloud acknowledges the eVoter either about status of the transaction which it was requested [11].

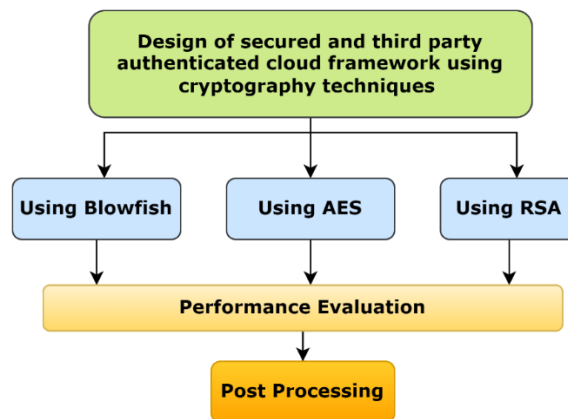


Figure 1. Method for performance analysis of the framework

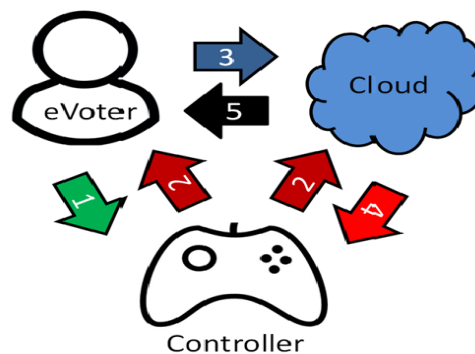


Figure 2. Cloud based framework for online voting system [11]

### 3.2. Algorithm for ticket management in cloud framework

Algorithm for ticket management mainly deals with two important security issues namely data/information security and voting system security. Data/information security issues include the first (standard) and second (local or defined by proposed security issues) level related to encryption, decryption activities. In first level, standard protocols are considered such as Session ID generation for a user when the voter tries to login into the system. This session ID is used to authenticate users for all their requests with the server. Apart from this security feature, second level security layer that can be established through a framework based approach is proposed for data security which is ensured using Blowfish, AES and RSA algorithms independently. Efficiency analysis of each algorithm implemented on the designed framework is carried out. For the confirmation of an authenticated voting, each voter is provided with 60 seconds or 1 minute of timestamp to decide on the voting person credibility so that he/she does not involve in

unauthenticated voting pattern and voter is identified by using the valid VID. The proposed third party authentication acts as a second level session and its duration will be only one minute.

- Step 1: eVoter requests the ticket by sending its voter ID (VID) (VID which is user at the end of login process) to controller. Example: Guru123
- Step 2: controller generates a unique 8-digit hexadecimal number (to cover more than 150 crores of voter accounts). Here the 8-digit hexadecimal number starts from 00000000 to FFFFFFFF. Assume DF83092A as a new id to be attached with VID of requested voter.

Ticket will be generated as:

TICKET=concatenation (Guru123, DF83092A)

TICKET=Guru123DF83092A

- Step 3: encryption.

To ensure the security of the system, cryptographic techniques are adopted in order to communicate the ticket. Current research work has tried to involve three popular cryptographic algorithms namely Blowfish, AES, and RSA. Generation of key: here system generates a random 10-digit key to encrypt the TICKET.

For encryption, one among the following algorithm will be considered

TICKET\_ENCRYPTED=Blowfish\_encrypt(key, TICKET)

TICKET\_ϒ\_ENCRYPTED=RSA\_ϒ\_encrypt(key, TICKET)

TICKET\_ϒ\_ENCRYPTED=AES\_ϒ\_encrypt(key, TICKET)

- Step 4: pass the ticket to eVoter and cloud modules

Controller sends TICKET\_ϒ\_ENCRYPTED to eVoter

Controller sends TICKET\_ENCRYPTED and key to cloud module

- Step 5: manage TICKET\_ENCRYPTED and key at cloud module.

Cloud receives TICKET\_ENCRYPTED and key. It decrypts using the respective cryptographic algorithm and stores it for further verification during voting process. Details of the request VID (8-digit hexadecimal number), key and current timestamp are stored in the database.

- Step 6: authentication for eVoter.

eVoter request the service from cloud module by communicating TICKET\_ENCRYPTED and its VID. Cloud module will search for key and TICKET\_ENCRYPTED from the database. Decrypt both the TICKET\_ENCRYPTED copies of eVoter and cloud module using one among the following decryption algorithm.

eVoter\_data=Blowfish\_decryption (TICKET\_ENCRYPTED of eVoter, key)

eVoter\_data=AES\_decryption (TICKET\_ENCRYPTED, key)

eVoter\_data=RSA\_decryption (TICKET\_ENCRYPTED, key)

Similar steps are followed for cloud TICKET\_ENCRYPTED

if (eVoter\_data=cloud\_data)

eVoter is authenticated and services will be provided

else

eVoter will be prompted as invalid user

- Step 7: manage duration

difference\_timestamp=curr\_timestamp - stored\_timestamp

if(difference\_timestamp<=60 seconds)

eVoter is authenticated and services will be provided

else

eVoter gets prompt as session expired or already voting is done.

### 3.3. Performance analysis of key tasks

Four key tasks identified in the proposed frame for online voting system. These key tasks are not involved are not influenced by any external parameters that influence the performance. Some of the parameters that are not considered for performance analysis of the framework are:

- a. Internet speed: this is volatile parameter and subjected to regional/environmental conditions. Hence these parameters cannot be predicted precisely.
- b. Server hardware/software configurations: server configurations are not specifically notified. There may be virtual hosting in the cloud. Hence this parameter cannot be predicted precisely.
- c. Time taken with respect to requests and responses: requests and responses in the internet are directly proportional to the speed of the internet. Internet speed is not precisely predictable and hence these parameters are also same.

The key tasks carried in the designed cloud framework are: i) K1: encryption of ticket at the controller; ii) K2: decryption of ticket at the cloud; iii) K3: encryption of ACK at the cloud;

iv) K4: decryption of ACK at the controller [11]. Performance analysis of three algorithms implemented on the designed framework is carried out by recording the readings of the execution time of five hundred voters on a predefined software and hardware environment. Results obtained are scaled down to ten users for representation where values of each row represent the average of the first 50 voters. Similarly, values are computed for rest of the 450 voters and represented in ten rows in each of the tables representing performance analysis with respect to Blowfish, AES, and RSA algorithms.

#### 4. IMPLEMENTATION

Secured cloud-based framework is implemented by using the cloud environment. Webpages are designed using PHP and MySQL. Three modules are developed separately for the purpose for analysing the performance of the different cryptography algorithms on the proposed framework: i) voter module; ii) controller module, and iii) cloud module. Voter module provides the options to the voter for the following aspects: i) create new accounts for voters; ii) voter login; iii) list of election candidates; and iv) cast vote.

Figure 3 represents the login page for the voter for registration and voting process. When the voter logs into the system, it gives two options to the voter either to CAST VOTE or to logout. Here voter may choose CAST VOTE option work. As per the proposed framework, the voter has to request controller for the TICKET. So, the controller generates a TICKET and distributes them among VOTER and CLOUD. This encrypted TICKET is shown in Figure 4. 92c00aa424ab4c18c8295b268cb0e2d9 is the 32 bits ticket generated by controller module based on a request from voter. Figure 5 represents the list of candidates contesting from a specific constituency. The selection is also accompanied with the ticket from the voter. Cloud module decrypts the ticket and authorizes the voter for selection.

Various status of ticket is indicated in different colors as shown in Figure 6. Voter has to request TICKET to proceed with voting. It is indicated by PINK color, whether voter is requested for the ticket or not. TICKET generation and distribution are indicated using RED color. Once the voter has chosen the candidate from the list as shown in Figure 4 and completes the selection process, then (which is generated for a particular voter) TICKET is blocked and is indicated in GREEN color. Additional security parameter ensures the security feature of the proposed cloud framework during the following scenarios: i) voter may try to request for another TICKET; ii) voter may request CLOUD more than once during the selection process; iii) there may be certain SQL injections; and iv) controller is essential for the entire voting process; hence voting can be disabled by turning off the controller.

Figure 3. Voter login and registration

Figure 4. Encrypted ticket using cryptography

Figure 5. Candidate list for voter

Candidate Name	Status
User1	Ticket Generated (Pink)
Guru	Ticket Generated (Pink)
Gururaj	Ticket Generated (Pink)
Saritha	Voting Done (Green)
User5	Voting Done (Green)
Swetha	Voting Done (Green)
User7	Voting Done (Green)
User8	Voting Done (Green)
User9	Ticket Generated (Pink)
User10	Ticket is not Generated (Red)
User11	Ticket is not Generated (Red)
User12	Ticket Generated (Pink)
User13	Ticket Generated (Pink)
User14	Ticket Generated (Pink)

Figure 6. Ticket status at controller module

## 5. PERFORMANCE ANALYSIS

Performance analysis of three algorithms implemented on the designed framework is carried out by recording the readings of the execution time of five hundred voters on a predefined software and hardware environment. Results obtained are scaled down to ten users for representation where a value of each row represents the average of the first 50 voters. Similarly values are computed for rest of the 450 voters and represented in ten rows in each of the tables representing performance analysis with respect to Blowfish algorithm in Table 1. Similarly execution time is computed for AES and RSA algorithms respectively. Table 2 represents the average execution time of the all the three cryptography algorithms used in the designed frame for online voting system and Figure 7 represents the graphical representation of results of execution time.

Frame work and the environment designed has to be easily configurable, flexible, time synchronized, efficient, and reliable to allow researchers to experiment on varying parameters for analysing different algorithms [25]. As per the literature survey, AES replaced DES cipher due to advances in cryptanalysis and the power processing that was no longer considered to be secure in addition to the vulnerable to the brute force attack. Blowfish is the fastest encryption algorithm with 128-bits block size, AES is the most secure and efficient in encrypting data in comparison to Blowfish which uses small block size of 64-bits, Blowfish is more vulnerable to attacks than AES. AES is more secured compared to RSA as AES is a symmetric key cipher that processes 128-bits blocks and support key-lengths of 128-bits as compared to RSA algorithm which is asymmetric cryptography algorithm with public and private keys. Based on the extent of securing the data and the number of bits used for keys generated by the algorithms the security levels are assigned to the three algorithms with 1 as highly secure and 3 as least secured as shown in Table 3 [15]–[17]. Table 3 represents the average performance parameter in addition to the security parameter of the cryptographic algorithms. The graph in Figure 7 indicates that AES is more secured but it consumes more time. RSA consumes less time but the security level rating is least. Blowfish algorithm has average time consumption and it has average rating with respect to security level.

Table 1. Keytask performance of Blowfish algorithm

Voter	K1 (sec)	K2 (sec)	K3 (sec)	K4 (sec)	Total
1	0.0200791	0.0210791	0.0216548	0.0224965	0.0853096
2	0.0200700	0.0201700	0.0197699	0.0213865	0.0813967
3	0.0167980	0.0177980	0.0172876	0.0267745	0.0786581
4	0.0170071	0.0180071	0.0151768	0.0184365	0.0686275
5	0.0197899	0.0193899	0.0183865	0.0187784	0.0763448
6	0.0204210	0.0205210	0.0233667	0.0213542	0.0856630
7	0.0185890	0.0184890	0.0193367	0.0182765	0.0746912
8	0.0168938	0.0178938	0.0176654	0.0177683	0.0702215
9	0.0201499	0.0211499	0.0218824	0.0215436	0.0847260
10	0.0181770	0.0193546	0.0187688	0.0193425	0.0756430
Average=0.07812818					

Table 2. Average execution time for three algorithms

Sl. No	Algorithm	Average performance (sec)
1	Blowfish	0.07812818
2	AES	0.21322248
3	RSA	0.01590439

Table 3. Security vs execution time performance

Sl. No	Algorithm	Security level	Average performance(sec)
1	AES	1	0.213222489
2	Blowfish	2	0.078128181
3	RSA	3	0.015904399

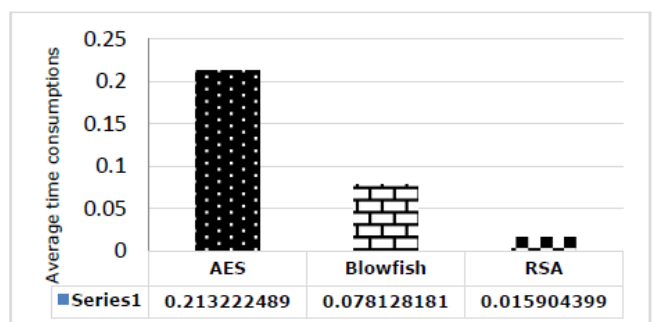


Figure 7. Average time consumptions of cryptography algorithms

## 6. CONCLUSION

From this research work, we conclude that the voting rate failures are due to migration of voters to different places from their voting place in pursuit of job, marriage and other opportunities. Hence, it emphasizes that there is a need for enhancing the voting rate in elections in order to elect a right leader. A cloud-based framework for implementation of the online voting system was designed and analysed in terms of security and execution time. RSA algorithm took less time when implemented on the designed framework but it was less secure compared to Blowfish and AES. AES was more secured algorithm but its efficiency in execution time was less as it took more time than Blowfish algorithm. Therefore, from this research work we conclude to utilize the Blowfish algorithm for its security implementation as it is better in terms of execution speed and security.

## ACKNOWLEDGEMENTS

Authors would like to thank all the people who directly or indirectly supported us in carrying out this work. We would like to thank centre for PG studies, regional center, Visvesvaraya Technological University, Mysuru and GSSS Institute of Engineering and Technology for Women, Mysuru for their kind support.

## REFERENCES





- [1] K. S. Gururaj and K. Thippeswamy, "Computing model to analyze voting rate failure in election system using correlation techniques," in *Recent Findings in Intelligent Computing Techniques: Proceedings of the 5th ICACNI 2017*, 2018, pp. 505–510. doi: 10.1007/978-981-10-8636-6\_53.
- [2] K. S. Gururaj and K. Thippeswamy, "An analysis: need of technology in voting system," in *International Conference on Recent Trends in Computational Engineering & Technologies (ICRT CET-18)*, 2018, pp. 608–612.
- [3] K. S. Gururaj and K. Thippeswamy, "Naïve bayes model for analysis of voting rate failure in election system," *International Journal on Recent and Innovation Trends in Computing and Communication*, vol. 6, no. 5, pp. 171–173, 2018.
- [4] K. S. Gururaj and M. C. Lavanya, "Designing online voting system for general elections," *International Journal of Applied Engineering Research*, vol. 10, no. 48, pp. 32583–32589, 2015.
- [5] S. Kremer, M. Ryan, and B. Smyth, "Election verifiability in electronic voting protocols," in *15<sup>th</sup> European Symposium on Research in Computer Security*, 2010, pp. 389–404. doi: 10.1007/978-3-642-15497-3\_24.
- [6] C. Sontakke *et al.*, "Online voting system via mobile," *International Journal of Engineering Science and Computing*, vol. 7, no. 5, pp. 12176–12178, 2017.
- [7] B. R., R. B. S., S. P., and K. V. K. G., "Smart voting," in *2017 2nd International Conference on Computing and Communications Technologies (ICCT)*, Feb. 2017, pp. 143–147. doi: 10.1109/ICCT2.2017.7972261.
- [8] R. B. Bhagat, "Internal migration in India: are the underclass more mobile?," in *India Migrations Reader*, New Delhi: Routledge India, 2012, pp. 122–140. doi: 10.4324/9780203085264-9.
- [9] J. Stone, R. M. Dennis, P. S. Rizova, A. D. Smith, and X. Hou, *The Wiley Blackwell encyclopedia of race, ethnicity, and nationalism*. Chichester: John Wiley & Sons, 2015. doi: 10.1002/9781118663202.
- [10] K. Koser, "Introduction: international migration and global governance," *Global Governance: A Review of Multilateralism and International Organizations*, vol. 16, no. 3, pp. 301–315, Dec. 2010. doi: 10.1163/19426720-01603001.
- [11] K. S. Gururaj and D. K. Thippeswamy, "Cloud based secured framework for implementation of online voting system," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 15, no. 1, pp. 328–335, Jul. 2019. doi: 10.11591/ijeecs.v15.i1.pp328-335.
- [12] R. C. Bhaddurgatte, V. K. B. P., and K. S. M., "Adoption of blockchain for security in IoT considering QoS," *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 9, no. 5, pp. 7040–7051, Oct. 2020. doi: 10.30534/ijatcse/2020/24952020.
- [13] A. S. Ashoor, "Challenges analysis security for cloud computing," *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 9, no. 5, pp. 7213–7217, Oct. 2020. doi: 10.30534/ijatcse/2020/47952020.
- [14] S. Wiriya, W. Wongthai, and T. Phoka, "The enhancement of logging system accuracy for infrastructure as a service cloud," *Bulletin of Electrical Engineering and Informatics*, vol. 9, no. 4, pp. 1558–1568, Aug. 2020. doi: 10.11591/eei.v9i4.2011.
- [15] Y. Yan, H. Xiaohong, and W. Wanjun, "Location-based services and privacy protection under mobile cloud computing," *Bulletin of Electrical Engineering and Informatics*, vol. 4, no. 4, pp. 345–354, Dec. 2015. doi: 10.11591/eei.v4i4.548.
- [16] T. Nie and T. Zhang, "A study of DES and Blowfish encryption algorithm," in *TENCON 2009 - 2009 IEEE Region 10 Conference*, Nov. 2009, pp. 1–4. doi: 10.1109/TENCON.2009.5396115.
- [17] P. C. Mandal, "Superiority of Blowfish algorithm," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 2, no. 9, pp. 2277–128, 2012.
- [18] R. Arora and A. Parashar, "Secure user data in cloud computing using encryption algorithms," *International journal of engineering research and applications*, vol. 3, no. 4, pp. 1922–1926, 2013.
- [19] V. R. Pancholi and B. P. Patel, "Enhancement of cloud computing security with secure data storage using AES," *International Journal for Innovative Research in Science & Technology (IJIRST)*, vol. 2, no. 9, pp. 18–21, 2016.
- [20] P. Kalpana, "Data security in cloud computing using RSA algorithm," *International Journal of research in computer and communication technology (IJRCCT)*, vol. 1, no. 4, pp. 143–146, 2012.
- [21] M. S. A. Mohamad, R. Din, and J. I. Ahmad, "Research trends review on RSA scheme of asymmetric cryptography techniques," *Bulletin of Electrical Engineering and Informatics*, vol. 10, no. 1, pp. 487–492, Feb. 2021. doi: 10.11591/eei.v10i1.2493.
- [22] A. K. Dubey, A. K. Dubey, M. Namdev, and S. S. Shrivastava, "Cloud-user security based on RSA and MD5 algorithm for resource attestation and sharing in java environment," in *2012 CSI Sixth International Conference on Software Engineering (CONSEG)*, Sep. 2012, pp. 1–8. doi: 10.1109/CONSEG.2012.6349503.
- [23] M. B and A. Dharani, "Necessitate for security in wireless sensor network and its challenges," *International Journal of Research in Computer Applications & Information Technology*, vol. 1, no. 1, pp. 21–25, 2013.







- [24] J. A. Jupin, T. Sutikno, M. A. Ismail, M. S. Mohamad, S. Kasim, and D. Stiawan, "Review of the machine learning methods in the classification of phishing attack," *Bulletin of Electrical Engineering and Informatics*, vol. 8, no. 4, pp. 1545–1555, Dec. 2019, doi: 10.11591/eei.v8i4.1344.
- [25] T. R. Murgod and S. M. Sundaram, "A comparative study of different network simulation tools and experimentation platforms for underwater communication," *Bulletin of Electrical Engineering and Informatics*, vol. 10, no. 2, pp. 879–885, Apr. 2021, doi: 10.11591/eei.v10i2.1466.

## BIOGRAPHIES OF AUTHORS



**Dr. Karanam Subramanyam Gururaj**     received his Ph.D. and M.Tech. from Visvesvaraya Technological University, Belagavi, India, he Completed his Engineering from Karnataka University, Dharwad. He has a total 20 years of Teaching Experience and currently working as Professor and Head, Department of ISE at GSSS Institute of Engineering and Technology for Women, Mysore, India. He has carried out his research titled "Design of an Effective and Secured Cloud Based Online Statistical Analysis of Voting System" from VTU, Belagavi under the Guidance of Dr. K Thippeswamy, Professor, Department of Computer Science and Engineering, VTU PG Centre, Mysuru. His research interest includes cloud computing and security, data mining, data analytics and image processing. He has published around 12 papers which include International Journals, International Conferences and National Conferences. He has guided around 35 Engineering Projects, 10 PG Projects and published papers in international conferences and Journals. His research interests include data mining, data classification and analytics, cloud security. He has delivered talks on Cloud Platforms, Roadmap for Publishing in Quality Journals, NEP-2020 initiatives and IoT & Machine Learning. He is a Life member of ISTE, CSI, and IAENG. He can be contacted at email: gururaj.k.s79@gmail.com.



**Dr. Kampalappa 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 24 years of Teaching and 8 years Research experience. He has published around 53 papers which include International Journals, International Conferences and National Conferences. He is a Life member of ISTE, CSI, and IAENG. He can be contacted at email: thippeswamy@vtu.ac.in.