Increasing System Security with Full Homo-morphic Encryption using Lagrange's Functions

Sonali Gaidhane, Shubhangi Rathkanthiwar, Sandeep Kakde, Kishore Kulat

Abstract*:Homo-morphic systems present a novel way to encrypt data, via which operations performed on the encrypted data are fully/partially reflected in the decrypted data. For example, if the input data D is homo-morphically encrypted to E, and if we perform X=E+N, then while decrypting X, we are bound to get D+N. Such a kind of encryption helps data owners to safely share their data among different analysers, without the risk of any kind of data leakages. Data analysers usually perform mathematical operations on the data which include addition, subtraction, multiplication and division. Homo-morphic systems which support addition & subtraction but do not support multiplication and division are termed as partially homo-morphic systems. While systems which support all the operations are termed as fully homo-morphic systems. In this paper, we have implemented a fully homo-morphic system based on Lagrange's functions. These functions help in improving the overall security of the system by adding stochastics to the input data, which ensures that the same input data has different cipher text, and full homo-morphism is achieved. Security of overall system increased by 40% by using FHE.

***Keywords* : Homo-morphic, encryption, Lagrange's, security, stochastic**

I. INTRODUCTION

In the present period of "distributed computing", quite a bit of people's and organizations' information is put away and figured on by outsiders like Google, Microsoft, Apple, Amazon, Facebook, Dropbox and loads of others. Traditionally, cryptography gave answers for shielding information moving from guide A toward point B. In any case, these aren't constantly adequate to monitor information very still and especially information being used. for example , assume that Alice has a few information x∈{0,1}^n (in present day applications x would prefer to be terabytes long or bigger) that she wishes to store with the cloud administration Bob, however is anxious about the possibility that that Bob will be hacked, subpoenaed or simply doesn't totally confide

in Bob. Encryption doesn't appear to immediately tackle the issue. Alice could store at Bob an encoded adaptation of the information and save the key for herself. Then again, she would be at a misfortune on the off chance that she needed to attempt to with the data anything very recovering specific squares of it. In the event that she needed to re-appropriate calculation to Bob additionally, and process f(x) for a couple of capacity f, at that point she would wish to impart the key to Bob, in this manner vanquishing the point of scrambling the data inside the primary spot.

For instance, after the registering frameworks of Office of Personnel Management (OPM) were found to be hacked in June of 2015, uncovering touchy data, including fingerprints and each one information accumulated during exceptional status checks of up to 18 million individuals, DHS colleague secretary for cybersecurity and correspondences Andy Ozment said that encryption wouldn't have helped forestalling it since "on the off chance that a foe has the accreditations of a client on the system, at that point they will get to information but it's scrambled, even as the clients on the system need to get to information". All in all, would we be able to encode information during a way that likewise permits some entrance and registering on it? As of now in 1978, Rivest, Adleman and Dertouzos considered this issue of a business that desires to utilize a "business time-sharing assistance" to store some delicate information. They imagined a potential answer for this errand which they called a security homomorphism. This idea later became alluded to as completely homomorphic encryption (FHE) which is an encryption that allows a festival (such on the grounds that the cloud supplier) that doesn't have the foggiest idea about the key to switch a ciphertext c encoding x to a ciphertext c' scrambling f(x) for each productively calculable f(). particularly in our situation above (see the fig), such a plan will permit Bob, given an encryption of x, to register the encryption of f(x) and send this ciphertext to Alice while never getting the key then while never picking up anything about x (or f(x) so far as that is concerned).

Revised Manuscript Received on May 15, 2020.
* Correspondence Author

Sonali Gaidhane*, is with Electronics Engineering department,Yeshawantrao Chavan College of Engineering, Nagpur University, Nagpur, India. Email: sonaligaidhane17@gmail.com

Shubhangi Rathkanthiwar, is with Electronics Engineering department, Yeshawantrao Chavan College of Engineering, Nagpur University, Nagpur, India. Email: svr_1967@yahoo.com

Sandeep Kakde, is with Electronics Engineering department, Yeshawantrao Chavan College of Engineering, Nagpur University, Nagpur, India. Email: sandip.kakde@gmail.com.

Kishore Kulat, is with Electronics Engineering department, Visvesvaraya National Institute of Technology, Nagpur, India.

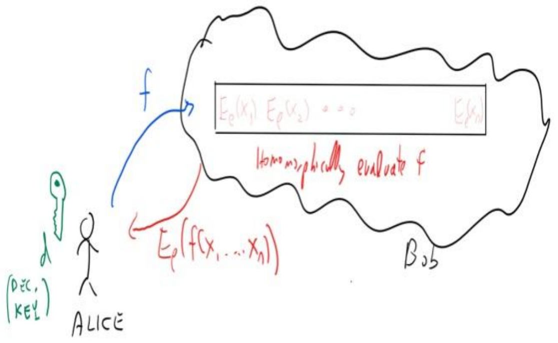
f
$E_p(x_1)$ $E_p(x_2)$ ... $E_p(x_n)$
Homomorphically evaluate f
$E_p(f(x_1 \ldots x_n))$
Bob
d
(DEC. KEY)
ALICE

Fig 1. Homomorphic encryption

A completely homomorphic encryption are frequently won't to store information on the cloud in scrambled structure, yet at the same time have the cloud supplier be prepared to assess works on the data in encoded structure (while never adapting either the sources of info or the yields of the capacity they assess).

Not at all like the instance of a trapdoor work, where it just took a year for Diffie and Hellman's test to be replied by RSA, inside the instance of completely homomorphic encryption for very 30 years cryptographers had no developments accomplishing this objective. Actually, a few people speculated that there's something innately inconsistent between the security of an encryption conspire and consequently the capacity of a client to perform of these procedure on ciphertexts. Stanford cryptographer Dan Boneh wont to joke to approaching alumni understudies that he will quickly sign the theory of any individual who thought of an absolutely homomorphic encryption. In any case, he never expected that he will really experience such a theory, until in 2009, Boneh's understudy Craig Gentry discharged a paper doing only that. Upper class' paper shook the planet of cryptography, and prompted a whirlwind of research results making his plan progressively proficient, decreasing the suppositions it depended on, expanding and applying it, and undeniably more. particularly, Brakerski and Vaikuntanathan figured out how to get an absolutely homomorphic encryption plot dependent on the preparation with Error (LWE) supposition we've seen previously.

In spite of the fact that there's an open source library, likewise as different executions, there's still a lot of work to be cleared out request to show FHE from hypothesis to rehearse. For a tantamount degree of security, the encryption and decoding activities of an absolutely homomorphic encryption plot are a few sets of size more slow than a standard open key framework, and (contingent upon its unpredictability) homomorphically assessing a circuit are regularly essentially all the more burdening. Be that as it may, this is frequently a quick advancing field, and as of now since 2009 huge improvements are found that decreased the computational and capacity overhead by numerous sets of extents. As freely key encryption, one would envision that for bigger information one would utilize a "half breed" approach of blending FHE with symmetric encryption, however one may got the opportunity to think of customized symmetric encryption plans which will be effectively assessed. To take the space among hypothesis and practice in context, it'd be helpful to consider the instance of checking calculation. inside the mid 1990's scientists (inspired at first by zero information proofs) concocted the thought of probabilistically checkable evidences (PCP's) which could yield in principle amazingly compact approaches to see accuracy of calculation.

Probabilistically checkable evidences are frequently thought of as "beefed up" renditions of NP fulfillment decreases and like these decreases, are for the most part utilized for negative outcomes, particularly since the underlying verifications were incredibly entangled and furthermore included tremendous concealed constants. Notwithstanding, with time individuals have gradually comprehended these better and made them increasingly proficient (e.g., see this review) and it's presently arrived at the reason where these outcomes, are almost commonsense (see additionally this) and really these thoughts underly at least one startup. Generally, developments for checking calculation have improved by at least 20 sets of extent in the course of the most recent 20 years . (We will specify some of these developments later during this course.) If progress on completely homomorphic encryption follows an indistinguishable direction, at that point we will anticipate that the street should reasonable utility to be long, yet trust it is anything but an "extension to no place".

Since enormous scope completely homomorphic encryption stays unreasonable, individuals are attempting to understand at least more vulnerable security objectives utilizing certain suspicions. particularly Intel chips have purported "Secure enclaves" which one can consider as a fairly alter ensured district of the processor that is affirmed to be far off for the surface world. the idea is that a cloud supplier customer would regard this enclave as a confided in party that it can speak with through the cloud supplier. The customer can store their information on the cloud scrambled with some key k, at that point discovered a protected channel with the enclave utilizing a verified key trade convention, and send k over. At that point, when the customer sends over a capacity f to the cloud supplier, the last party can recreate FHE by requesting that the enclave register the encryption of f(x) given the encryption of x. during this arrangement eventually the private key resides on the cloud supplier's PCs, and along these lines the customer must confide in the security of the enclave. Practically speaking, this may give sensible protection from remote programmers, yet (dissimilar to FHE) most likely not against modern aggressors (e.g., governments) that have physical access to the server. The next section describes different homo-morphic systems in detail, followed by our proposed system and it's result analysis. We finally conclude this text with some interesting observations about the proposed work, followed by some future research that can be carried out in this area.

In this paper, we are performed operations on cipher text Which creates secret codes by using homomorphic encryption with lagranges function ensures that same input with different cipher and homomorphism achieved. This paper is organized as follows: Section I gives an Introduction part. Section II focuses on the related work while section III explains the proposed methodology.

Section IV discusses the result part and section V concludes the paper.

II. PREVIOUS WORK

Because SSE, PIR and SMPC schemes focuses more on searching, retrieving and joint-computing in relation to encrypted data, Homomorphic schemes has become the most researched in recent times, this is because it has the ability to protect that data during transformation.

HE allows complex mathematical operation to be performed on encrypted data without exposing the encrypted data. It was previously called "privacy homomorphism" which was first exploited by Rivest, Adleman&Dertouzos (1978), shortly after the presentation of RSA cryptosystem in their classical work, in that work an intriguing question was asked, "Given an unbounded number is there any encryption scheme that will simultaneously permit the evaluation of both addition and multiplication the plaintext?" Multiplicative Homomorphic encryption scheme that is based on RSA are all asymmetric encryption system (ElGamal (1985); Rivest et al. (1978)), also some additive homomorphic encryption scheme exist (Okomoto & Uchiyama (1998); Paillier (1999)). However, Dahab, Galbraith &Morais (2015) that the NTRU based somewhat- homomorphic encryption scheme are subject to key recovery attacks.Fully Homomorphic Encryption is a scheme that is homomorphic with respect to all function f, (Hamlin, Schear, Shen, Varia&Yakoubou (2015), here the scheme is similar to the SWHE, the only difference is that there is no increase in accumulated noise during computation and it supports both additive and multiplicative homomorphism(Fun &Samsudin (2016)). Similarly, Boneh, Goh & Nissim (2005) gave an encryption scheme which is homomorphic with respect to quadratic functions f, however their scheme could only be multiplicative making it to fall short of the goal of being true fully homomorphic.

The first FHE scheme was theoretically demonstrated by Gentry (2009) and he based his works on a relatively new and untested cryptographic assumption, the quantum hardness of short-vector problem in ideal lattice, in his seminar work he was able to demonstrate that an encryption scheme that provides and Eval operation for an unbounded number of additions and multiplication. Gentry (2009) introduced the concept of bootstrapping into the somewhat homomorphic encryption scheme that permits a limited number of Eval operations.

Over the years and based on Gentry's work various researchers have been working on how to achieve FHE where the noise can be removed if not completely but let it be very small.For instance, one of the key observations made by Gentry (2009) is that when the noise has grown so large that homomorphic operation can no longer be performed, the ciphertext itself is encrypted again that is the ciphertext is decrypted and re-encrypted again. Bootstrapping has been implemented by the following researchers (Smart &Vercautaren (2010); Dijk, Gentry, Halevi &Vaikuntanathan (2010); Stenle&Steinfield (2010); Gentry & Halevi (2011). Also, Brakerski&Vaikunathan (2011) introduced a technique to solve the computation overhead caused by bootstrapping, they called it modulus switching, this approach does not fully re-encrypt the ciphertext but limits the noise growth in the ciphertext during homomorphic computations. (Coron, Naccade, &Tibouchi (2012); Zhang, Liu &Xiaoyuan (2013); Rohloff& Cousins (2014) are some of the implementations of modulus switching in FHE. The challenge of the technique is that the message space is place in the "lower bits" of the decryption equation.

Brakerski (2012) introduced the scale invariant where the message space is placed in the "upper bit" of the decryption equation with that he was able to control the noise growth. However, the technique comes with a cost, which is more complex rounding operation is required in the multiplicative homomorphism.

Flattening was recently introduced by Gentry, Sahai& Waters (2013), this technique is based on the modulus switching, the variation here is that the ciphertext is presented in matrix form while the encryption key is in vector form, it was a trivial transformation where vectors are modified without affecting their dot product, thus making a better bound of the growth of the error. Doros&Sunar (2016) implemented the technique and is based on the NTRU which uses the lattice-based cryptography, here they stated that as long as NTRU ciphertext are secure their scheme is also secure. However, most NTRU based homomorphic encryption still suffers from computation, bandwidth and storage inefficiencies because of the bit by bit encryption. Also, it was recently shown by Morais& Dahab (2014); Dahab, Galbraith & Morais (2015); Chenal & Tang (2015) that the NTRU based homomorphic encryption scheme are subject to key recovery attacks. The next section describes the proposed algorithm, and the results & analysis of the integrated proposed algorithm is given in the next section.

III. PROPOSED METHODOLOGY

This journal uses double-blind review process, which means that both the reviewer (s) and author (s) identities concealed from the reviewers, and vice versa, throughout the review process. All submitted manuscripts are reviewed by three reviewer one from India and rest two from overseas. There should be proper comments of the reviewers for the purpose of acceptance/ rejection. There should be minimum 01 to 02 week time window for it.

FHE has been proposed using multiple variations in prime number operation arithmetic. There are generally 2 prime numbers p and q, and let n be a modulus,

$$n = pq$$

Let g be an integer of order $n \propto |n^2|$. The public key is,$PK = (n, g)$

and the secret key is,

$SK = \lambda(n) = 1cm((p-1),(q-1)).$

To encrypt a message $m \in Z_{n,}$ randomly choose r in Z_n^* and compute

$C = g^M r^n |n^2| \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots. (1)$

To decrypt c,

$$\text{compute}M = \frac{L\left(C^{\lambda(n)}|n^2|\right)}{g^{\lambda(n)}|n^2|}|n| \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots (2)$$

$$M = \frac{L\left(C^{\lambda(n)}|n^2|\right)}{g^{\lambda(n)}|n^2|}|n| \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots .. (3)$$

During the most recent decade, there has been a lot of examination into researching the plan's security, expanding its usefulness, and improving its productivity. This intrigue is expected essentially to some one of a kind properties of this plan. Since this plan is "homomorphic", "self-blinding", and "probabilistic". The plan is named a homomorphic conspire which by and large implies that there are sure number-crunching activities that when completed in the ciphertext space relate to a realized math activity happening in the cleartext space. On account of this proposed cryptosystem, the fully homomorphisms apply. We modified the existing cryptosystem by adding Largange’s equality to equation 1 and 2. Where, equation 1 was modified to the following form,

$$C = g^{(1:k-1)} * r + s \dots \dots (3)$$

Where, g is the polynomial variable, r is the random process, k is the part polynomial degree and s is the input plain text. Following this equation, the decryption equation was modified as,

$$M = Y * L_j$$

$$L_j = \frac{\delta(a - X)}{\delta(xk - X)}$$

$$\delta = x(1:k)$$

where, k is the part polynomial degree, xk is the value of the polynomial at k, X is the polynomial, a is the cipher text constant, and Y is the cipher text Due to the added Lagrange’s equalities to the cipher and decipher processes, the overall complexity of the algorithm increases. Which increases the overall encryption quality of the system. We analysed these results and evaluated the parameters like delay of computation, security level and signal to noise ratio of the proposed scheme against simple fully homo-morphic scheme and advanced encryption standard. The results are shown in the next section.

IV. RESULTS AND DISCUSSION

In our evaluation, we found out the following parameters,

- End to end delay: This is the delay needed to encrypt and decrypt the plain text data, and obtain the cipher text, and the regenerated plain text
- Signal to noise ratio: This is the ratio of the signal power to the noise power of the plain text and the decrypted cipher text
- Security factor: This is the total length of the cipher text to the length of the input text. This factor must always be more than 1, and should be high for more secure systems

Table 1. Delay comparison between different algorithms

Input Length (Bytes)	Delay (ms) AES	Delay (ms) FHE	Delay (ms) Proposed
10	1.20	0.80	0.78
20	2.60	1.50	1.46
50	5.90	5.10	4.85
100	10.80	9.72	8.96
200	22.60	20.80	18.20
500	56.71	49.89	45.07
1000	113.35	100.02	90.27
2000	226.33	200.57	180.92
5000	565.51	501.32	451.86
10000	1131.60	1003.00	903.81

Similar comparisons were made for signal to noise ratio by adding and multiplying data with the encrypted text, and then decrypting the same. Due to addition and multiplication of data, there is modification of the cipher text, due to which AES is not able to decrypt the data, while the FHE and the proposed FHE are able to decrypt the data with high SNR. The table 2 showcases these results.

Table 2. SNR comparison

Input Length (Bytes)	SNR (dB) AES	SNR (dB) FHE	SNR (dB) Proposed
10	12.30	32.60	33.10
20	12.25	32.70	33.15
50	12.40	32.90	33.47
100	12.62	33.60	33.59
200	12.36	33.68	33.90
500	12.39	34.01	34.05
1000	12.40	34.32	34.26
2000	12.43	34.63	34.46
5000	12.44	34.93	34.67
10000	12.40	35.24	34.87

Due to addition of Lagrange’s equalities to the system of FHE, there is an increase in the length of the cipher text, due to which there is an exponential increase in the security level of the algorithm. We found out the security factor of the proposed algorithm, and compared it with the existing techniques. The following results were obtained,

Table 3. Security factor comparison

Input Length (Bytes)	SF AES	SF FHE	SF Proposed
10	1.00	1.20	1.50
20	1.00	1.30	1.70
50	1.00	1.40	1.90
100	1.00	1.45	2.30

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

200	1.00	1.46	2.60
500	1.00	1.47	2.80
1000	1.00	1.40	2.90
2000	1.00	1.52	3.10
5000	1.00	1.53	3.50
10000	1.00	1.55	3.70

From the above comparisons it is clear that the proposed algorithm is not only delay efficient, but also possesses high level of security when compared to other algorithms.

V. CONCLUSION

It is observed that addition of Lagrange's equalities to the system under test adds to the overall security of the system, due to which the security level of the system is increased by 40%, while the delay is reduced by 20% when compared with AES and standard Pallier-based fully homo-morphic systems. Moreover the SNR is also high due to the fully homo-morphic support provided by the system.

VI. FUTURE WORK

Due to the emerging nature of block chain based techniques, researchers can try to integrated block chain into the proposed chatbot and observe the result improvements in chatbot's authentication performance and removal along with the overall security of the bot. This will help the researchers to further study the effects of blockchain in chatbots and explore more areas in the field of application.

REFERENCES

1. Abbasi, A, Sarker, S & Chiang, R. H. L. (2016). data Research in Information System: Towards an inclusive research Agenda. Journal of the Association for Information Systems, 17(2),p.l-XXXll.
2. Abdalla, M., Bellare, M., Catalano, D., Kiltz, E., Kohno, T., Lange, T,…, P., &Sho, H. (2005). Searchable encryption revisited consistency properties, relation to anonymous IBE and extensions. In CRYPTO 2005, Vol. 3621 of LNCS, pages 205 – 222. Springer.
3. Abdullah, N., Ismali, S.A, Sopiayati, S. & Sam, S. M. (2015). Data Quality in data; A review. International Journal of Advances in SoftComputing and Its Applications. Vol. 7, No 3, November 2015. ISSN 2074 – 8523
4. Arora, S. &Safra, S. (1998). Probabilistic checking of proofs: A new characterization of NP. J. ACM, 45(1):70122, January 1998.
5. Asanov, A. (2001). Private Information Retrieval. GI Jahrestagung(2) pp. 889 – 894.
6. Bassi, S., & Chaudhary, A. (2015). Cloud Computing Data Security – Background and Benefits. IJCSC, Vol. 6, Number 1, September – March, pp 34 - 40.
7. Boneh, D., di-Crescenzo, G., Ostrovsky, R., &Persiano, G. (2004). Public key encryption with keyword search. In proceedings EUROCRYPT 04, 506 – 522.
8. Boneh, D., Goh, E., & Nissim, K. (2005). Evaluating 2-DNF formula on ciphertext in Theory of cryptography(TCC). 235 – 341.
9. Brakerski, Z. (2012). "Fully Homomorphic Encryption without Modulus Switching from Classical GapSVP," LNCS, vol. 7417, pp. 868–886.
10. Brakerski, Z. &Vaikuntanathan, V. (2011). "Efficient Fully Homomorphic Encryption from (Standard) LWE," in Proc. of IEEE 52nd Annu. Symp. on Found. of Comp. Sci., CA, pp. 97–106.
11. Cartlidge, J., Smart, N.P.,2 &Alaoui, Y. T. (2018). Defense Advanced Research Projects Agency (DARPA) and Space and Naval Warfare Systems Center, Pacific (SSC Pacific) under contract No. N66001-15-C-4070.
12. Chor, B., Kushilevtz, E., Goldriech, O. & Sudan, M. (1998). Private Information Retrieval. Journal of the ACM 45(6) 965 – 981.
13. Cloud Security Alliance (2010). Top Threats to Cloud Computing V1.0 Prepared by the Cloud Security Alliance March 2010.
14. Cloud Security Alliance (2013). The Notorious Nine Cloud Computing Top Threats in 2013.
15. Cloud Security Alliance (2016). Big Data Security and Privacy Handbook: 100 Best Practices in Big Data Security and Privacy.
16. Cloud Security Alliance (2016), The Treacherous 12 – Cloud Computing Top threats in 2016.
17. Curtmola, R., Garry, J., Kamara, S., & Ostrovsky, R. (2006). Searchable Symmetric Encryption: Improved Definitions and Efficient Constructions. Proceedings of the 13th ACM conference on computer and Communication Security. 79 – 88.
18. Dani, V., King, V., Movahedi, M., Saia, J. & Zamani, M. (2017). Secure Multi-Party Computation in Large Networks*. NSF CAREER Award 0644058 and NSF grants CCR-0313160 and CCF-1320994.
19. ElGamal, T. (1985). A private key cryptosystem and a signature scheme based on discrete logarithms. In advances in Cryptology CRYPTO. Lecture notes in Computer Science Vol. 196 Berlin Springer-Verlag. 10 -18.
20. Nirmalkar, Nitish, Shailesh Kamble, and Sandeep Kakde. "A review of image forgery techniques and their detection." In *2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)*, pp. 1-5. IEEE, 2015.
21. Fun, T. S., &Samsudin, A. (2016). A survey of Homomorphic Encryption for Outsourced data Computation.
22. Hatwar, R.B., Kamble, S.D., Thakur, N.V. and Kakde, S., 2018. A review on moving object detection and tracking methods in video. *International Journal of Pure and Applied Mathematics*, *118*(16), pp.511-526.
23. Bhanuse, Shraddha S., Shailesh D. Kamble, and Sandeep M. Kakde. "Text mining using metadata for generation of side information." *Procedia Computer Science* 78 (2016): 807-814.
24. Gentry, C. (2009). "A Fully Homomorphic Encryption Scheme," Ph.D. Dissertation, Dept. of Comp. Sci., Standford University, Stanford, CA.
25. Gentry, C. & Halevi, S. (2011). "Fully Homomorphic Encryption without Squashing Using Depth-3 Arithmetic Circuits," in Proc. of IEEE 52nd Annual Symp. Found. Computer Science, Palm Springs, pp. 107-109.
26. Gentry, C., Sahai, A., & Waters, B. (2013). "Homomorphic Encryption from Learning with Errors: Conceptually-simpler, Asymptotically-faster, Attribute-based," LNCS, vol. 8042, pp. 72-92.
27. Goldriech, O., & Ostrovsky, R. (1996). Software protection and simulation on oblivious RAMs. Journal of the ACM 43(3): 431 – 473.
28. Goldriech, O., Micali, S., &Wigderson, A. (1987). How to play the mental game. In proceeding of the 19th Annual ACM Symposium on Theory of Computing, STOC. 218 – 229. New York, USA ACM. ISBN 0-89791-221-7.

AUTHOR PROFILE

Sonali Gaidhani obtained her bachelor degree in Electronics Engineering from G. H. Raisoni Women's College of Engineering, and Technology Nagpur. She is pursuing her master degree in Electronics Engineering discipline from Yeshwantrao Chavan College of Engineering, Nagpur. Her areas of work includes Cryptography, Encryption Algorithms, Homo-morphic Encryption, Decoding Algorithms. She is a Graduate Student Member of IEEE.

Dr. Shubhangi Rathkanthiwar, a renowned academic personality has achieved continued success in her role as a scholastic intellectual leader. She is currently working as Professor in Department of Electronics Engineering, Yeshwantrao Chavan College of Engineering, Nagpur, Scholar of international repute, Prof. Dr. Shubhangi Rathkanthiwar holds brilliant academic achievements along with a long list of publications. She has total 95 research articles published in International journals, and proceedings of International and National conferences. 13 research papers are available on IEEExplore, 14 research papers are indexed by Scopus, 2 research papers are published in Book chapters. Her book titled **'**An Intelligent WLAN system: Performance Evaluation in fading multi-path environment', published in Germany, is available in all countries. 3 patent applications are published by Govt. of India and 2 copyrights for DTEL material has also been granted to her by Govt. of India. Her tutorial excellence, especially the various innovative teaching / learning practices adopted by her marks her out as a distinguished luminary in academic circles. Her educational qualifications include B.E. (Electronics and Telecommunications), M.Tech. (Electronics Engineering), Ph.D. in Electronics Engineering discipline.

Her PhD work carries great relevance to technological developments in Wireless Communications using intelligent techniques and is of importance in solving problems pertaining to current and future generation wireless communications. Dr. Rathkanthiwar is recipient of 'Best Scientist Award', conferred by RTMNU, Nagpur in 2017, 'Best Research presentation award' conferred at International level by IET UK in international conference SEISCON-2011. She was nominated to receive 'Best paper award' in the world congress WCECS 2008 held at University of California, Berkley, USA. She received 'Reviewer recognition award' by world recognized refereed journal 'Science Direct', viz. 'Elsevier Journal on Applied Soft Computing' in 2015. Dr. Shubhangi Rathkanthiwar is Recipient of the 'Best Teacher Award' (Maharashtra Teacher's council) in 2010-11 and 'Shikshak Ratna Award' conferred by St. Tulasidas Rashtriya Sahitya Sangha, New Delhi in 2011-12 for her significant contribution in academics and students centric Teaching/ Learning activities.She has served as reviewer for IEEE Access, IEEE Trans. On Signals and Systems, IEEE Communication Letters, IEEE Communications Survey and Tutorials, 'IEEE Transactions on Vehicular Technology' and 'IEEE Transactions on Industrial Electronics' and 'Elsevier Journal on Applied Soft Computing'. She is Associate Editor of one National journal & Editorial board member of 7 international journals She has served as Technical program committee member and reviewer of several IEEE conferences.

Sandeep Kakde (S'14-M'17, SM'19) is currently working as the Assistant Professor in Yeshwantrao Chavan College of Engineering, Nagpur. He has over thirteen years of industry and university experience, worked as a Senior Design Engineer at Bharat Electronics Limited, Bangalore, as a Senior Design Engineer in Sanyo LSI Technology India Private Limited, ITPL Park, Bangalore, deputed as a Senior Design Engineer in Sanyo Semiconductors, Japan and as an Assistant Consultant in Tata Consultancy Services, Bangalore. He obtained his B.E. degree in Electronics Engineering Department from the Visvesvaraya Regional College of Engineering (renamed Visvesvaraya National Institute of Technology), Nagpur, India; M. Tech degree in VLSI Design discipline from Electronics Engineering Department, Yeshwantrao Chavan College of Engineering, Nagpur, India and pursuing Ph. D degree in Electronics Engineering from the University of Nagpur. He is teaching Basic CMOS VLSI Design, Digital System Design, Logic Design, ASIC Design, Solid State Devices & Modeling, Verification and Testing of VLSI Circuits to undergraduate and postgraduate students in Yeshawantrao Chavan College of Engineering, Nagpur. He has published more than seventy papers in IEEE International Conferences and thirty papers in International Journals of repute. He is also reviewer in many international journals and conferences. He is also a reviewer for IEEE Transaction on VLSI Systems. His areas of work include Decoding Algorithms, Analog and Mixed Signal Circuit Design, Full Custom Layout Design, Data Path Layout, Memory Layout Design and Semicustom Layout Designs, VLSI testing, Low-Power design, and Verification of IC's,Ultra Low Power VLSI/ULSI Design and Technology, Digital VLSI Circuit Design, and Reconfigurable FPGA Implementation. He is the recipient of Best Teaching and Research Excellence Award for the year 2017 from IRDP Publisher. He is a Senior Member of IEEE, Member of British Council, Life Member of (ISTE) India, Society of Technical Education and a Member of Institute of Engineers Association.

Dr. Kishore Kulat is currently a Professor with the Department of Electronics and Communication Engineering, Visvesvaraya National Institute of Technology, Nagpur. He has authored or co-authored over 100 plus papers in international/national journals and conferences. His current research interests include wireless, communication systems, networking, Internet of Things, MIMO communication, S-parameters, UHF antennas, Wi-Max, antenna radiation patterns, audio coding, channel coding, cognitive radio, data compression, encoding, error correction codes, feedback, forward error correction, machine-to-machine communication, meta material antennas, Micro-strip antennas, multimedia communication and real-time embedded system design. He is Associate Editor of one National journal & Editorial board member of many National and International journals. He has served as Technical program committee member and reviewer of several IEEE conferences. He is a Life Member of the Indian Society for Technical Education, a Fellow Member of the Institution of Electronics and Telecommunication Engineers, and a member of the Institution of Engineers.