Chapter 12
Hash Function Based Optimal Block Chain Model for the Internet of Things (IoT)

Andino Maseleno, Marini Othman, P. Deepalakshmi, K. Shankar, and M. Ilayaraja

12.1 Introduction

Internet of Things (IoT) is a type of network that is being utilized by wireless sensor associations and radio frequency identification (RFID) via network topology [1] to accomplish high reliability in transmission as well as intelligent processing [2]. IOT comprises three layers: the sensing layer, transport layer, and application layer. IOT has made a tremendous change in different areas such as business, agriculture, pharmacy, also in nuclear reactors [3]. To receive the IoT innovation, it is important to assemble the certainty among the clients about its security and privacy that it won't make any risk to their data integrity and authority [4]. In secure systems, the secrecy of the information is kept up, and it is ensured that at the processing of message exchange the information holds its inventiveness and no modification by the system [5]. Although the IoT can encourage the digitization of the data itself, the dependability of such data is as yet a key challenge by Bitcoin [6]. It's upheld by a protocol that points of interest the infrastructure responsible for guaranteeing that the data remains unchanging after some time [7]. Benefiting from blockchains power and versatility, in this work, propose an effective decentralized verification system [8]. The principle motivation behind network security data insurance is to accomplish secrecy as well as integrity. Security issues are of extraordinary significance in amplifying the size of network and gadgets [9]. Different cryptographic algorithms have been produced that tends to the said issue.

A. Maseleno (✉) · M. Othman
Institute of Informatics and Computing Energy, Universiti Tenaga Nasional, Kajang, Malaysia
e-mail: andino@uniten.edu.my; marini@uniten.edu.my

P. Deepalakshmi · K. Shankar (✉) · M. Ilayaraja
School of Computing, Kalasalingam Academy of Research and Education, Krishnankoil, Tamil Nadu, India
e-mail: deepa.kumar@klu.ac.in; ilayaraja.m@klu.ac.in

A. K. Singh, A. Mohan (eds.), *Handbook of Multimedia Information Security: Techniques and Applications*, https://doi.org/10.1007/978-3-030-15887-3_12

However, their use in IoT is questionable as the equipment we deal in the IoT is not appropriate for the execution of computationally costly encryption algorithms [10].

A blockchain is a database that stores every processed transaction—or information—in the subsequent request, in an arrangement of PC recollections that are carefully designed to foes. All users then share these exchanges by Minoli et al. in 2018 [11], More significantly, we talk about, how blockchain, which is the basic innovation for bitcoin, can be a key empowering agent to tackle numerous IoT security issues by Minhaj Ahmad Khan and Khaled Salah in 2018 [12]. It's additionally distinguished open research issues and difficulties for IoT security. One of the real issues of a clustering protocol is choosing an optimal group of sensor nodes as the group heads to isolate the network by Bennani et al. 2012 [13]. In any case, optimum clustering is an NP-Hard issue and solving it includes searches through large spaces of conceivable solutions. Two major periods of optimization, exploration, and exploitation, are structured by the social interaction of dragonflies in exploring, hunting foods, and keeping away from foes while swarming powerfully or factually by Mirjalili in 2015 [14]. In Emanuel Ferreira Jesus et al. in 2018 [15] the ideas about the structure and task of Blockchain and, mostly, investigate how the utilization of this innovation can be utilized to give security and privacy in IoT.

12.2 Security Issues in IoT Multimedia Information

Security approaches that depend greatly on encryption are not a solid match for these constrained gadgets since they are not equipped for performing complex encryption and decryption rapidly enough to have the capacity to transmit information safely in a progressive manner [16]. Some security challenges in IoT security are tag attack, Sybil attack, wormhole attack and, etc. [17–20]. Regardless, with traditional encryption procedures, before dealing with some sensitive data from customers, the third party administration (cloud) would decrypt this information and after that find that data [21–23]. Data that is very sensitive to bank account details, usernames, passwords need to encrypt with at least two-factor authentication procedures to guarantee security [24–26]. For enhancing the security in IoT data, BC is utilized. Now, the header turns out to be a piece of a cryptographic riddle which must be comprehended by the block chain's network of clients via a trial and error procedure, from trillions of opportunities—before it is included to the blockchain.

12.3 Methodology for IoT Information Security

The IoT visualizes a completely associated world, where things can convey estimated information and connect with one another. For enhancing the security dimension of the multimedia data's in IoT, optimal Block Chain (BC) security model is utilized, Its behinds the bitcoin concept a permanent open record of

data secured by a network of distributed members, its strategy that to enables exchanges to be confirmed by a gathering of untrustworthy on-screen characters. The fundamental of this proposed strategy is, enhance the secrecy as well as the reliability of the IoT data, Moreover, this BC, every block contains the number of transactions. For every transaction, the parameters are stored in the neighborhood BC. The objective of optimization (DA) in this safe procedure is, to select the group Head for IoT data. CH would have coordinate proof about CH if it confirmed a block created by different squares of data. The details of optimal CH with BC mechanisms explained in the below section.

12.3.1 Security and Privacy Analysis in IoT

Security in IoT is difficult because of low asset abilities of the vast majority of devices, huge scale, heterogeneity among the gadgets, and absence of standardization. Besides, a considerable lot of these IoT gadgets gather and offer a lot of information from our own spaces, in this way opening up noteworthy privacy concerns. Security and privacy risk analysis for a commonplace shrewd home engineering that depends on existing and promptly available market IoT gadgets and stages. As opposed to existing security and threat investigation of IoT situations, we focus on a genuine IoT smart home condition sent in our tested concentrating on the interactions among the diverse IoT parts.

12.3.2 IoT Information Generation

The new invention of IoT and multimedia data applications is necessary to address specific business solutions which require needs, for example, predictive maintenance, loss prevention, asset utilization, inventory tracking, disaster planning, and recovery, downtime minimization, energy usage optimization, device performance effectiveness. These datasets are particular in information structures, volume, get to procedures, and some unusual perspectives; they can scarcely be stored and gotten as well, its shows in Fig. 12.1. IoT applications have quite certain qualities; they produce extensive volumes of data and require network and power for significant time periods.

12.3.3 Pre-Processing

This underlying preprocessing IoT data are separated to choose the sensitive or quality information for security, the purpose behind preprocessing is diminishing the computational time. Moreover, the goal is to ensure strong security and improve

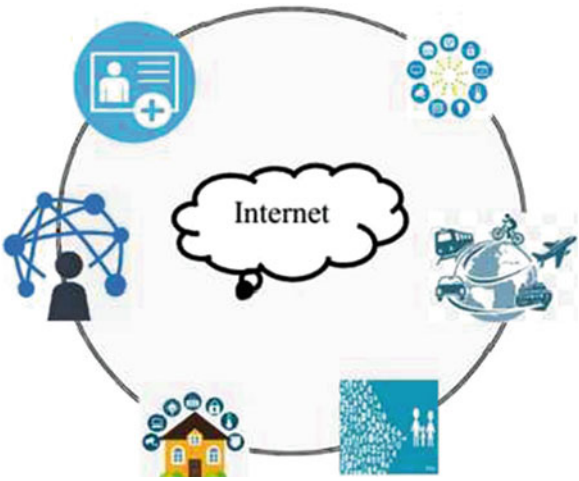

Fig. 12.1 IoT components

the performance of the model, and we secure sensitive data only. IoT data clustering using optimization Information is clustered by utilizing irregular clustering model with optimization. The weights of its cluster associations assess each data. Finally, among various nodes and as indicated by their weights a node is elected as the cluster head, for optimal cluster head selection dragonfly optimization is proposed. Finally, among various nodes and as shown by their information a node is elected as the cluster head.

12.3.4 Dragonfly Optimization Algorithm

The primary objective of any swarm is survival, so all of the individuals should be attracted towards food sources and distracted outward enemies. Considering these two behaviors, there are five main factors in position in swarms. This optimization technique based on the exploration and exploitation phases for cluster head selection for security model.

The primary goal of any swarm is survival, so the majority of the individuals ought to be pulled in towards food sources and distracted outward enemies. Considering these two behaviors, there are five principle factors in position updating of individuals in swarms, and this is done based on the exploration and exploitation phases for cluster head selection for security model.

12.3.4.1 Behavior of Dragonflies

The behavior of dragonflies can be composed as the combination of five stages, in particular, separation, alignment, cohesion, attraction towards a food source and distraction outwards an enemy.

12.3.4.2 Objective Function

To estimate the fitness of a solution, it is essential to design a target function to quantify the execution of every solution. In this part, the target work is figured as:

$$objective = \max(accuracy) \tag{12.1}$$

12.3.4.3 Updating New Cluster Head

Separation: Alludes to the static collision shirking of the individuals from other individuals in the area. *Alignment:* On account of the velocity matching of each dragonfly in the specific area, alignment is done. *Cohesion:* Cohesion implies the tendency of individuals towards the point of convergence of the mass of neighborhood; it's trailed by beneath conditions.

$$New\ centriod_{t+1} = (a_1 S_i + a_2 A_i + a_3 C_i + a_4 F_i + a_5 E_i) + w_i\ centroid_t \tag{12.2}$$

By the use of optimization strategy, distinctive explorative and exploitative behaviors can be accomplished. When there is no neighboring solution, the location of dragonflies is updated by methods for a random walk (Levy flight). For updating the position of the above equation, using the behavioral procedure that is

$$\textbf{Separation}\ \ S_i = \sum_{k=1}^{N} C - C_k \tag{12.3}$$

$$\boldsymbol{Alignment}: \quad A_i = \frac{\sum_{k=1}^{N} V_k}{N} \tag{12.4}$$

$$\boldsymbol{Cohesion}: \quad C_i = \frac{\sum_{k=1}^{N} C_k}{N} - C \tag{12.5}$$

$$\boldsymbol{Attraction\ towards\ a\ food\ Source}: \quad Food_i = C^{+} - C \tag{12.6}$$

$$\textbf{\textit{Distraction outwards an enemy}}: \quad Enemy_i = C^{-} + C \tag{12.7}$$

Based on the above condition, the term C indicates the current position of the individual C_k denotes the position of a k-th individual, N is the total number of neighboring individual in the search space. Alignment of dragonflies occurs dependent on the velocity V coordinating of individuals to that of different individuals in the area and a_1, a_2, a_3, $a_4 and\ a_5$ coefficient parameters. After the alignment procedure of individuals among the dragonflies, cohesion process is performed which implies the inclination of individuals towards the focal point of the mass of the area. The new position refreshed by utilizing the following condition

$$C_{t+1} = C_t + Levy\,(distance) * C_t \tag{12.8}$$

Food source and the enemy is selected over best and the most exceedingly terrible solutions obtained in the whole swarm at any minute. In light of above process choose optimal cluster head for IoT data clustering model. After that, the clustered data are secured by utilizing the BC technique.

12.3.5 Security Model: A Blockchain Model

In a BC, each transaction in the set that contains a block is hashed to produce a hash value. Hashes are combined into a Merkle Tree. Generally, the BC indicated a consistently maintained and controlled database considering developing variables and gathered information test sets. The key components of BC are a member made transactions and the recorder blocks of such exchanges. Here, the block checks whether transaction details were sustained in the correct grouping or not and this does not permit any altering of the data accessible.

12.3.5.1 Bitcoin

Bitcoin is cryptographic money and a digital payment system, in view of a public BC, each block of the Bitcoin blockchain. In Bitcoin, transactions are processed to check their integrity, authenticity, and accuracy by a gathering of creative network nodes called “Miners.” Specifically, rather than mining a single transaction, the miners package various transactions that are waiting for the network to get processed in a single unit called “block.”

12.3.5.2 Blockchain Hash Function

A cryptographic hash function maps the data of arbitrary size to a settled size string. A cryptographic hash function is a precise mapping for which it is computationally difficult to find a data object that maps to a given hash result or to find two information protests that map to a similar hash result. The yield of this hashing procedure is added to the block's header, along with a hash of the previous block's header and a timestamp. The new header is a contribution to a cryptographic procedure to create a nonce, and this hash function appears in Fig. 12.2. Normal employment of hashing is one-path to secure PC passwords retained in storage or to deliver cryptographic condensations of IoT data. The procedure of blockchain is characterized in the following condition (12.9).

Encryption
Encryption system function as given a message and a key, it creates a ciphered message to be transmitted over unprotected channels, without any risk being comprehended by other people who don't have the decryption key. For the security purpose, the key generation dependent on the two sets, one public and one private. The first to encrypt and the second to decrypt and the vice versa; this is conceivable because of the utilization of some mathematical functions that have the property of being irreversible.

For encrypted and decrypted information

$$Enc = hash\ (\inf o\ group, hash, publickey, IP) \tag{12.9}$$

$$\text{Each block of data encrypted by } E \Rightarrow m^k \mid \bmod \inf o \mid \tag{12.10}$$

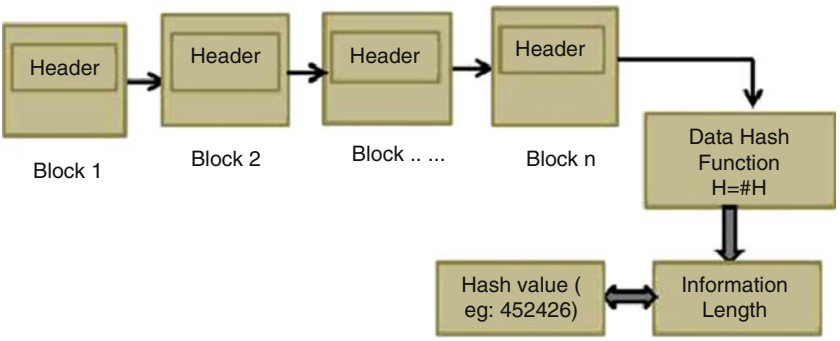

Fig. 12.2 Hash function model

$$\text{Encrypted data are decrypted by } D \Rightarrow \left(\left(m^k\right) | \bmod \inf o(E)|\right) * \Pr ivate\ key \tag{12.11}$$

Hash function proficiently changes over a finite input string to an output string with a fixed length known as hash value. Based on this value, the IoT multimedia information is secured by the end to end BC mechanism, the private keys with restricted randomness can be exploited to compromise the BC accounts. Helpful mechanisms yet should be characterized to guarantee the privacy of transactions at the same time avoid race attack.

12.4 Results and Analysis

Our proposed IoT, information security model, is executed in the Java programming language with the JDK 1.7.0 in a windows machine enclosing the configurations such as the Intel (R) Core i3 processor, 1.6 GHz, 4 GB RAM, and the operating system platform is Microsoft Window7 Professional. This proposed security analysis is compared with other techniques.

Table 12.1 shows the result of the proposed clustering model. Here we select the number of clusters based on the size of the database. We take the size of the database depends on kilobytes, for example, we choose 10–50 kb. For 10 kb, the proposed model achieves cluster 1 as 3, cluster 2 as 4, cluster 4 as 0 and cluster 5 as 3. Similarly, the other databases produce the best selection in the DOA model. The above-said procedures are visualized in below Fig. 12.4.

Table 12.2 and Fig. 12.3 shows the result of proposed parameters which obtains in the study. Depends on file size, we find encryption size, decryption size, memory and execution time. The result depicts that encryption size and decryption increases if the file size increased, the execution time also increased. But compared to other techniques proposed model secure the IoT data in a high manner.

Figure 12.4 shows the graph of security level based on some blocks. Here, we compare the security result with the proposed method to existing techniques such as bitcoin and ECC. The graph depicts that blockchain reaches optimal security in the range of 82–91.23% compared to the other two. Figure 12.5 shows the security

Table 12.1 Results for Proposed clustering analysis

	Number of clusters (kb)			
Size of the database (kb)	Cluster 1	Cluster 2	Cluster 4	Cluster 5
10	3	4	0	3
20	6	7	2	5
30	10	14	4	2
40	16	8	10	6
50	13	11	16	10

Table 12.2 Proposed (blockchain) Security analysis results

File size	Encryption size	Decryption size	Memory (byte)	Execution time (ms)
10	23	10	1,242,488	94,523
20	34	20	374,528	105,481
30	44	30	312,458	98,450
40	49	40	412,141	112,345
50	56	50	423,412	112,482

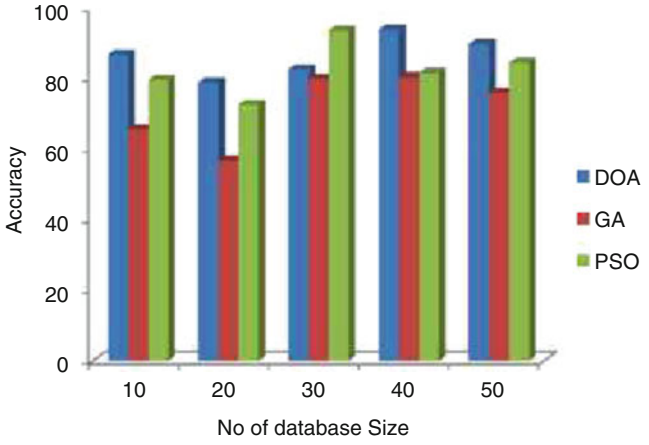

Fig. 12.3 Comparison of clustering accuracy

level based on the database size. The hash blockchain performs an optimal security level for every database size. The security level reaches a maximum at 90% in hash blockchain function.

12.5 Conclusion

In this chapter, the IoT multimedia information's security model with help hash function based blockchain was discussed. Like this, the advantages of applying BC to the IoT ought to be examined precisely and taken with caution. Also, this chapter provided an analysis of the main difficulties that blockchain and IoT must address for them to effectively cooperate. This blockchain technology can help to improve IoT applications and also this data clustering cluster head selection by DOA, and its give better accuracy. However, it is still in the beginning periods of creating block chains, and these obstructions will be defeated, opening the best approach to numerous potential outcomes. One of the principle concerns about blockchain, and especially cryptocurrencies, resides in its volatility which has also been exploited

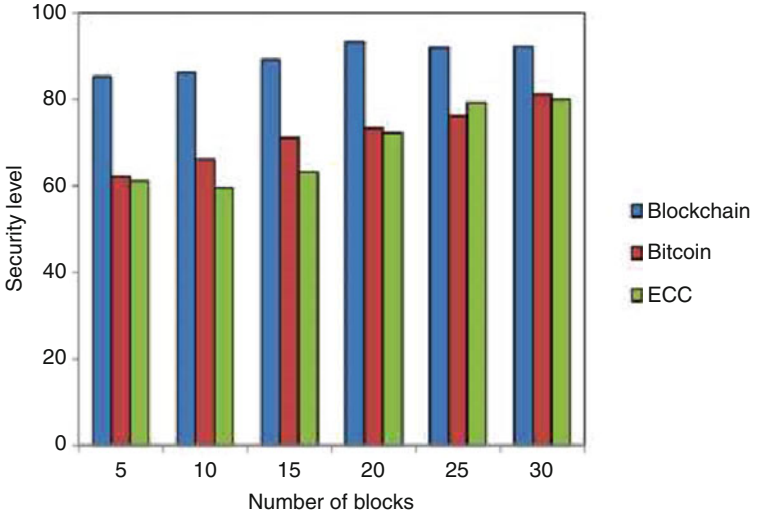

Fig. 12.4 Number of blocks Vs. hash value

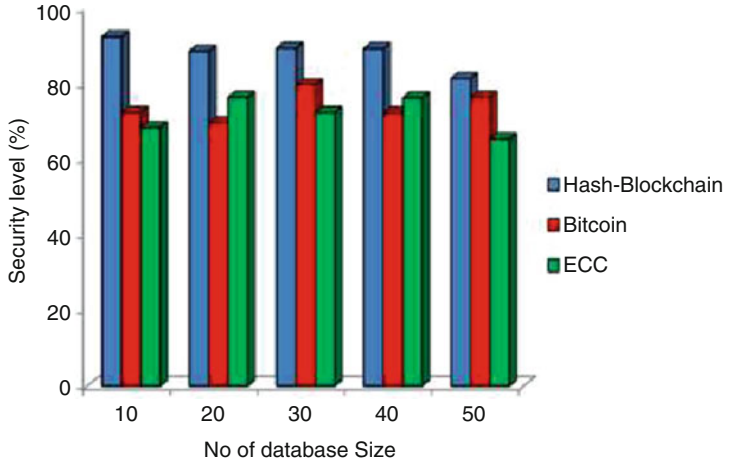

Fig. 12.5 Security Level comparative analysis

by individuals to take unfair advantage of this situation. The incorporation of the IoT and blockchain will extraordinarily increase the security level.

References

1. Alshehri, M.D., Hussain, F.K. and Hussain, O.K., 2018. Clustering-Driven Intelligent Trust Management Methodology for the Internet of Things (CITM-IoT). Mobile Networks and Applications, pp.1-13.
2. Safi, A., 2017. Improving the Security of the Internet of Things Using Encryption Algorithms. World Academy of Science, Engineering and Technology, International Journal of Computer, Electrical, Automation, Control and Information Engineering, 11(5), pp.546-549.
3. Lo'ai, A.T., and Somani, T.F., 2016, November. More secure Internet of Things using robust encryption algorithms against side channel attacks. In Computer Systems and Applications (AICCSA), 2016 IEEE/ACS 13th International Conference of (pp. 1-6). IEEE.
4. Sundaram, B.V., Ramnath, M., Prasanth, M. and Sundaram, V., 2015, March. Encryption and hash based security in internet of things. In Signal Processing, Communication and Networking (ICSCN), 2015 3rd International Conference on (pp. 1-6). IEEE.
5. Bhatia, S. and Patel, S., 2015. Analysis on different Data mining Techniques and algorithms used in IOT. Int. J. Eng. Res Appl, 2(12), pp.611-615.
6. Wang, C., Shen, J., Liu, Q., Ren, Y. and Li, T., 2018. A Novel Security Scheme Based on Instant Encrypted Transmission for Internet of Things. Security and Communication Networks, 2018.
7. Chhabra, A., Vashishth, V., Khanna, A., Sharma, D.K. and Singh, J., 2018. An Energy Efficient Routing Protocol for Wireless Internet-of-Things Sensor Networks. arXiv preprint arXiv:1808.01039.
8. Xingmei, X., Jing, Z. and He, W., 2013, October. Research on the basic characteristics, the key technologies, the network architecture and security problems of the internet of things. In Computer Science and Network Technology (ICCSNT), 2013 3rd International Conference on (pp. 825-828). IEEE.
9. Srinidhi, N.N., Kumar, S.D. and Venugopal, K.R., 2018. Network optimizations in the Internet of Things: A review. Engineering Science and Technology, an International Journal.
10. Reyna, A., Martín, C., Chen, J., Soler, E. and Díaz, M., 2018. On blockchain and its integration with IoT. Challenges and opportunities. Future Generation Computer Systems.
11. Minoli, D. and Occhiogrosso, B., 2018. Blockchain mechanisms for IoT security. Internet of Things, 1, pp.1-13.
12. Khan, M.A. and Salah, K., 2018. IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems, 82, pp.395-411.
13. Bennani, K. and El Ghanami, D., 2012, November. Particle swarm optimization based clustering in wireless sensor networks: the effectiveness of distance altering. In Complex systems (ICCS), 2012 international conference on (pp. 1-4). IEEE.
14. Mirjalili, S., 2016. Dragonfly algorithm: a new meta-heuristic optimization technique for solving single-objective, discrete, and multi-objective problems. Neural Computing and Applications, 27(4), pp.1053-1073.
15. Jesus, E.F., Chicarino, V.R., de Albuquerque, C.V. and Rocha, A.A.D.A., 2018. A Survey of How to Use Blockchain to Secure Internet of Things and the Stalker Attack. Security and Communication Networks, 2018.
16. K. Shankar, Mohamed Elhoseny, E. Dhiravida chelvi, SK. Lakshmanaprabu, Wanqing Wu, An Efficient Optimal Key Based Chaos Function for Medical Image Security, IEEE Access, November 2018. https://doi.org/10.1109/ACCESS.2018.2874026
17. Mohamed Elhoseny, K. Shankar, S. K. Lakshmanaprabu, Andino Maseleno, N. Arunkumar, Hybrid optimization with cryptography encryption for medical image security in Internet of Things, Neural Computing and Applications - Springer, October 2018. https://doi.org/10.1007/s00521-018-3801-x
18. Lakshmanaprabu SK, K. Shankar, Ashish Khanna, Deepak Gupta, Joel J. P. C. Rodrigues, Plácido R. Pinheiro, Victor Hugo C. de Albuquerque, "Effective Features to Classify Big Data using Social Internet of Things", IEEE Access, Volume.6, page(s):24196-24204, April 2018.

19. T. Avudaiappan, R. Balasubramanian, S. Sundara Pandiyan, M. Saravanan, S. K. Lakshmanaprabu, K. Shankar, Medical Image Security Using Dual Encryption with Oppositional Based Optimization Algorithm, Journal of Medical Systems, Volume 42, Issue 11, pp.1-11, November 2018. https://doi.org/10.1007/s10916-018-1053-z
20. K.Shankar and P.Eswaran. "RGB Based Multiple Share Creation in Visual Cryptography with Aid of Elliptic Curve Cryptography", China Communications, Volume. 14, Issue. 2, page(s): 118-130, February 2017.
21. Nur Aminudin, Andino Maseleno, K. Shankar, S. Hemalatha, K. Sathesh kumar, Fauzi, Rita Irviani, Muhamad Muslihudin, "Nur Algorithm on Data Encryption and Decryption", International Journal of Engineering & Technology, Volume. 7, Issue-2.26, page(s): 109-118, June 2018.
22. K. Shankar and P. Eswaran. "RGB Based Secure Share Creation in Visual Cryptography Using Optimal Elliptic Curve Cryptography Technique", Journal of Circuits, Systems, and Computers, Volume. 25, No. 11, page(s): 1650138-1 to 23, November 2016.
23. K. Shankar, Lakshmanaprabu S. K, "Optimal key based homomorphic encryption for color image security aid of ant lion optimization algorithm", International Journal of Engineering & Technology, Volume. 7, Issue. 9, page(s): 22-27, 2018.
24. K. Shankar and P.Eswaran. "A Secure Visual Secret Share (VSS) Creation Scheme in Visual Cryptography using Elliptic Curve Cryptography with Optimization Technique". Australian Journal of Basic and Applied Sciences. Volume: 9, Issue.36, Page(s): 150-163, 2015.
25. K. Sathesh Kumar, K. Shankar, M. Ilayaraja, M. Rajesh, "Sensitive Data Security in Cloud Computing Aid of Different Encryption Techniques", Journal of Advanced Research in Dynamical and Control Systems, Volume. 9, Issue. 18, page(s): 2888-2899, December 2017.
26. K. Shankar and P.Eswaran. "ECC Based Image Encryption Scheme with aid of Optimization Technique using Differential Evolution Algorithm", International Journal of Applied Engineering Research, Volume: 10, No.5, pp. 1841–184, 2015.