Proceedings of to the 9th Scientific Conference of University of Garmian: Pure science and Technology Applications (SCUG-PSTA-2022). Kalar (46021) / Sulaymaniyah (26-27 Oct.2022) (Special issue for Passer journal of basic and applied sciences) Paper No. 03, 40-50

Secure Communication of the Integrated IoT and Cloud Computing

Avin Othman Abdalrahman[1], Khalid Kadhim Jabbar[2], Araz B. Karim[3]

Omar Younis Abdulhammed[4]

[1] Department of Civil engineering, University of Garmian, Kalar, Sulaymaniyah, Kurdistan, Iraq

[2]Collage of Education, University of Mustansiriyah, Baghdad, Iraq

[3] Department of Computer Science, College of Science, University of Garmian, Kalar, Sulaymaniyah, Kurdistan, Iraq

[4] Department of Computer Science, College of Science, University of Garmian, Kalar, Sulaymaniyah, Kurdistan, Iraq

Aveen.othman@garmian.edu.krd; Khalid.jabbar@uomustansiriyah.edu.krd; Araz.kareem@garmian.edu.krd; Omar.y@garmian.edu.krd

ABSTRACT

One advanced technology that is expanding quickly in the communications area is the integration of Cloud computing with the IoT. This is because it is quick, easy, and inexpensive to use. Since the information sent between the sender and recipient is vulnerable to threats and attacks through eavesdropping or unauthorized, in this paper, encryption technology is used to protect the information that is sent from the intelligent building to the smartphone-controlled, where the information sent between the two parties is encrypted by relying on the Henon map, new diffusion technique and the XoR function. Several measures were used to measure the quality of the proposed system as Histogram, NPCR, PSNR, SSIM, QIU, MAE, and Entropy, as the results proved the strength, high-security effectiveness, and robustness of the proposed system.

KEYWORDS: IoT, Cloud computing, Henon map, Encryption, Diffusion, and Confusion.

1 INTRODUCTION

It is significant to review the common technical aspects in the computer field. IoT and Cloud computing are two technologies that undoubtedly share many attributes. This technology can benefit from and be improved by combining many concepts [1,2]. The IoT is the network of physical things, gadgets, transportation, buildings, and other objects embedded in technology, software, sensor, and network access. [3,4]. IoT technology is the next significant advancement in new technology, but it differs significantly from previous advancements in that it brings about significant changes in corporate performance. In the upcoming years, it is anticipated that both the number of websites or intelligent devices and the features they will offer will grow [5]. One real benefit of the IoT concept is that it will significantly affect all facets of daily life as well as the behavior of potential customers. A user can immediately notice the Internet of Things' effects on the home and workplace environments. In the first state, an example of situations that can use this new model is the Internet of Things; it will be used in assisted living and e-health and reinforce education in the near future [6,7]. In the second state, business users may see identifiable challenges in other areas, such as the intelligent transmission of persons and products, logistics, industrialization, advanced manufacturing technologies, and business management. The IoT could be considered a flexible, worldwide network foundation that controls brilliant, self-configuring things. The Internet of Things is developing to the point that everything around us is connected to the Internet and can interact with minimal human effort [8]. The IoT consists of three major components: 1. The physical objects, 2. The networks of communication that connect physical objects, 3. Systems of computers that stream data to and from things.

There are currently safety and security issues due to many internet-connected items, and much information exchanged [9]. When we talk about security, we mean how well the IoT apps and infrastructures are protected. Given that so many gadgets use too few external services that are frequently unmanaged, they are reasonably simple to attack. When the network layer is breached, it is straightforward for attackers to seize control of the system and use the compromised initial node to use or target additional neighboring systems intentionally. The user's security must be maintained by preventing identification and unauthorized access. Confidentiality means that your information is under your control and not under the control of others. Another difficulty brought up by the IoT's significant reliance on data and connected devices are trusted (reliability). In addition to the Internet of Things, reliable data must be sent between devices and the Internet because giving inaccurate or unreliable information can result in unintended or incorrect effects [10].

2 CLOUD- BASED INTERNET OF THINGS

One of the most significant technologies in recent years has been the IoT. It enables the transmission and reception of data over the Internet and the connection of material things to the Internet. Machine learning, Sensors, embedded systems, and real-time analytics are just a few of the technologies that have emerged from the IoT concept. It involves intelligent hospitals and other technology that can be managed via wireless or wired Internet [11]. The IoT module diagram is depicted in Figure (1).

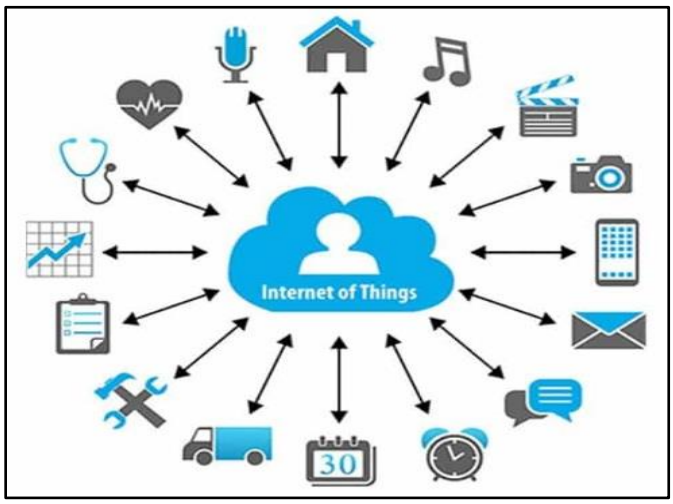

Figure 1: Block diagram of IoT

A shared pool of reconfigurable computing resources, such as network, server, storage, apps, and service, may be quickly deployed and released with very little administration work or service provider involvement thanks to the cloud computing concept [12]. There are four different deployment model types, three various service model types, and five fundamental features that make up cloud computing. Most cloud computing deployment strategies fall under the category of public clouds, in which resources are made accessible to users via the Internet. A profitable company typically owns public clouds [13]. On the other hand, a private Cloud's infrastructure is typically offered by a single company to meet the unique needs of its consumers [12]. The private Cloud provides an elevated level of security and control. Three levels of cloud computing are available: The Software as a Service (SaaS) model, which allows users to access software over the Internet [14], and the Platform as a Service (PaaS) model, which provides a more advanced innovative environment that can be used to develop, test, and deploy specialized software, and at last the Infrastructure as a Service (IaaS) model, which makes infrastructure like server, storage, devices available as a service [12]. Figure (2) shows that IoT and cloud computing are quickly evolving services with unique traits.

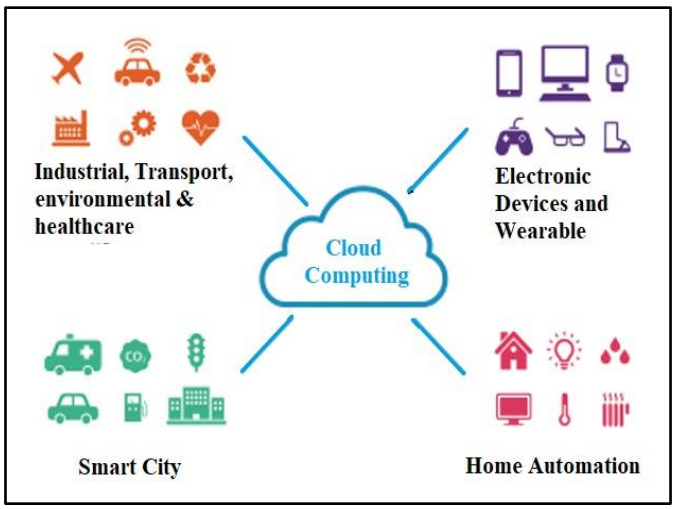

Figure 2: Integration of IoT and Cloud Computing

The IoT strategy, on the other side, is built on intelligent devices that connect through a worldwide network and dynamic infrastructure. The possibility of omnipresent computing is enabled. The IoT is often defined as widely dispersed devices with constrained processing and storage capacity. These devices have problems with dependability, security, privacy, and performance [15]. On the other side, cloud computing consists of a vast network with limitless computational and storage capacity. Additionally, it offers a robust, adaptable platform that enables dynamic data integration from diverse data sources [13]. Most of the IoT problems have been partly handled by cloud computing. A cloud-based Internet of Things system enables cost-effective and intelligent use of infrastructure, data, and applications. The IoT must deal with problems including security, performance, privacy, and dependability because it has limited processing power and storage capacities. The best solution to most problems is undoubtedly through IoT cloud integration. By extending its capabilities with physical things in a more dynamic and dispersed way and offering modern services to billions of devices in various real-world scenarios, the Cloud can profit from the IoT [15], [16]. Furthermore, the Cloud makes using services and applications for end consumers simpler and less expensive. The IoT data stream is also made simpler by the Cloud, which offers rapid, affordable installation and combination for complicated data processing and deployment [17].

3 HENON MAP

Chaotic systems are dynamic systems that are very sensitive to initial conditions, are random, deterministic, and can be easily reconstructed after filling the picture [18]. So, they are perfect candidates for the generation of pseudo-random coding sequences. Henon map is one of the chaotic maps used to generate the Pseudo-random sequences needed for coding since it is computationally effective and has near-perfect random properties [19]. Henon proposed a two-dimensional chaotic system, the Henon map, as a

shorthand way to study the dynamics of the Henon attractor and the Lorenz system. Mathematically, Henon mapping can be determined via the following equations [20]:

$$X_{n+1} = 1 - a * X_n^2 + Y_n \quad (1)$$

$$Y_{n+1} = b * X_n \quad (2)$$

Where the value of n = (1,2,3,…) and a, b are Henon map parameters and their values are 1.4 and 0.3 respectively.

4 PROPOSED SYSTEM

Nowadays, using the IoT with cloud computing has become one of the critical and ordinary things that many companies and institutions use. One of the essential things that must be considered is security and the provision of a secure connection to transfer data between the sender (smart devices) and the recipient (smartphone controlled). This paper used encryption to provide security and secure communication between the sender and recipient, depending on the new substitution technology and Henon chaotic map. Figure (3) shows the block diagram of the suggested method.

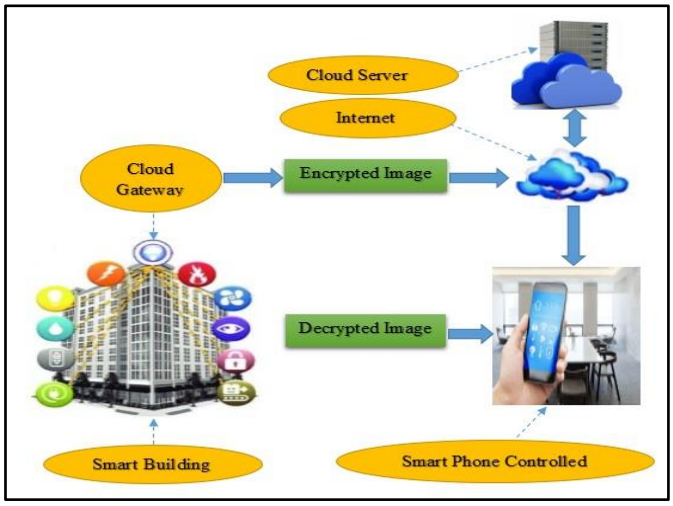

Figure 3: Block Diagram of the suggested method

The encryption process is done for the images captured by sensitive devices located in the building, where the process of capturing images is possessed in the event of abnormal movement or movement of people outside working hours, close to sensitive or prohibited places. The captured grayscale images are

encrypted with a dimension of 256 * 256 through the Henon map, diffusion technique, and XoR function; Algorithm (1) displays the steps of ciphering phase.

```
Input gray image
Output encrypted image
Begin
Step1: resize gray image into 2-D of 256*256 as p (x, y)
Step2: perform diffusion for each row of p (x, y) by circle shift every cell by 255
Step3: perform diffusion for each column of p (x, y) by circle shift every cell by 255
Step4: generate sequence number by using henon map as (gs)
Step5: store (gs) as array of one dimension with a length of 256
Step6: ss= mod (ceiling (abs (gs)*10000000000),256) + 1
Step7: summation of each row as (q) and each column (h)
Step8: perform wise confusion for each cell (ec) of each row with (ss) as
       wt = (ec + q) XoR (ss) mod 256
Step9: perform wise confusion for each cell (ecc) of each column with (ss) as  wtt= (ecc + h) XoR (ss)
       mod 256
End
```

Algorithm (1) Steps of Encryption

When the encrypted images are received by the recipient, they must be decoded, the steps of the decoding process are the opposite of the steps of the ciphering process as shown in the algorithm (2).

```
Input Encrypted image
Output gray scale image

Begin
Step1: generate sequence number by using henon map as (gs)
Step2: store (gs) as array of one dimension with length 256
Step3: ss= mod (ceiling (abs (gs)*10000000000),256) + 1
Step4: summation of each row as (q) and each column (h)
Step5: perform wise confusion for each cell (ecc) of each column with (ss) as  wtt= (ecc + h) XoR
       (ss) mod 256
Step6: perform wise confusion for each cell (ec) of each row with (ss) as
       wt = (ec + q) XoR (ss) mod 256
Step7: perform diffusion for each column of p (x, y) by circle shift every cell by 255
Step8: perform diffusion for each row of p (x, y) by circle shift every cell by 255

End
```

Algorithm (2) Steps of Decryption

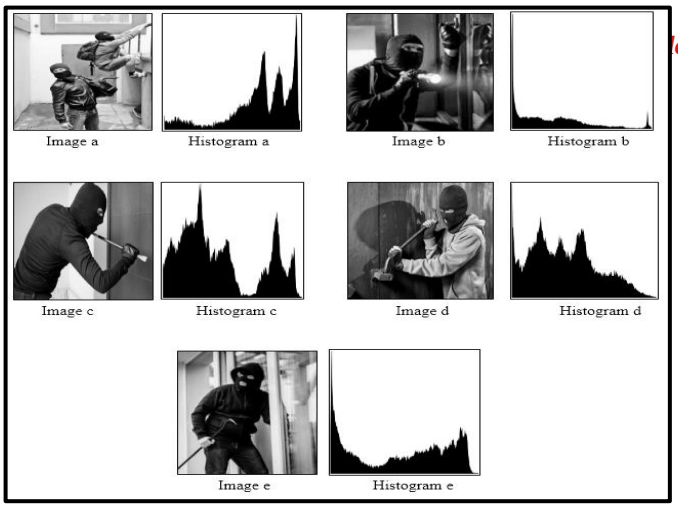

Figure 4: Original images with their histograms

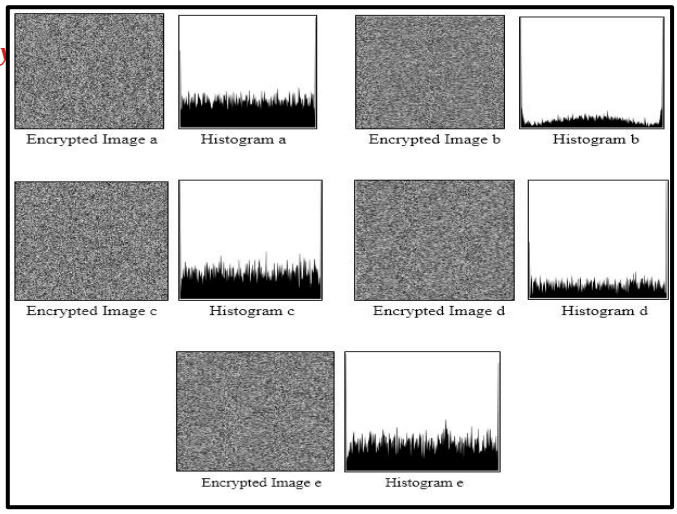

Figure 5: Encrypted images with their histograms

5 RESULT

To evaluate the effectiveness of the proposed method, we have implemented some tests in statistical or security dissection. The histogram anatomy goodness appreciates any ciphering method. An image histogram displays the pause division of every grayscale image which supplies the quantity data of the image. Every ciphering method should have the capability to create a regular and entirely diverse histogram for every image. By relying on figure (4) which shows the five captured images with their histogram and figure (5) which shows the encrypted images with their histogram, it was noted that there is no similarity between the encrypted image and the original image, as the pixels in the encrypted image were distributed equally, also the all encrypted image is not obvious, unrecognizable, incomprehensible, and no information can be extracted from it. Hence, the suggested method withstands the statistical offensive, is achieved confidentially, and has the best confusion characteristics.

Encryption algorithms must be resistant to attacks, therefore, in this proposed system, several criteria were used to measure the algorithm's ability to resist attacks. where the NPCR measures the ratio of the number of different pixels between the original image and the encrypted image, the UACI measures the percentage change in density between the two images and the MAE measures mean absolute error where its value must be very large to indicate the robustness of the coding system. By looking at acquired outcomes in the table (1) and figure (6) obviously reverberates that the evaluated values of NPCR and UACI are so near to the theoretic values, which sanctify the authenticity of theoretic values, also the value of MAE is very high. Therefore, the suggested enciphering technique is resistant to differential attacks.

Table 1 Values of NPCR, MAE, UACI

Image	NPCR	MAE	UACI
a	99.6401	92.3509	33.4645
b	99.6387	92.1011	33.4479
c	99.6183	91.4575	33.4210
d	99.6499	92.8109	33.4701
e	99.5934	90.4301	33.4029

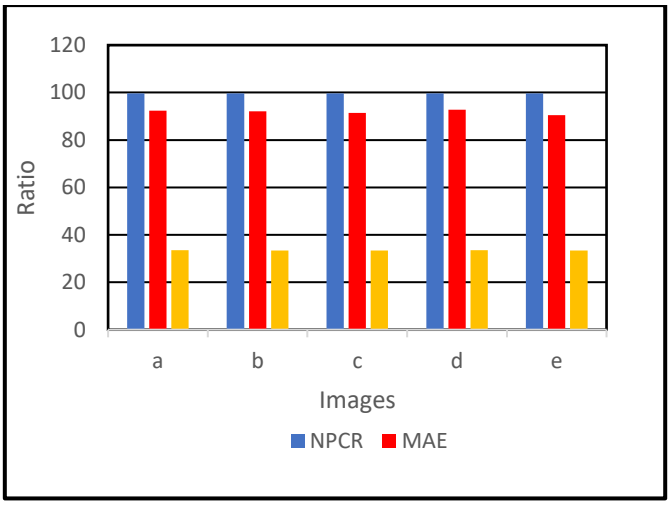

Figure 6: Results of NPCR, MAE, and UACI parameters

Table (2) and figure (7) show the results for four parameters which are: SSIM, UIQ, PSNR, and entropy, where SSIM and UIQ are utilized to measure the constructional resemblance between two plain and encrypted images, the significant resemblance between the images will be realized where the value is near to 1, The results of the table showed that there is no resemblance between the plain and encrypted image. The PSNR appreciates the ciphering method impartially by deeming the plain and encrypted image as a signal and noise, respectively. The low value of the PSNR points to the major versus amidst the plain and encrypted images. The outcomes clearly show that the ciphering quality is best as the PSNR value of each image is small (less than 8 dB). To measure the randomness of images, entropy was used, where the best entropy value for an encrypted image is approximately 8. Based on the entropy results, the encryption method was effective and robust.

Table 2 Values of SSIM, PSNR, UIQ, Entropy

Image	SSIM	PSNR	UIQ	Entropy
a	0.02746	7.6921	0.7387	7.9833
b	0.02300	7.6999	0.7301	7.9687
c	0.01687	7.7671	0.6278	7.9538
d	0.02894	7.6743	0.7453	7.9895
e	0.01065	7.7230	0.6212	7.9482

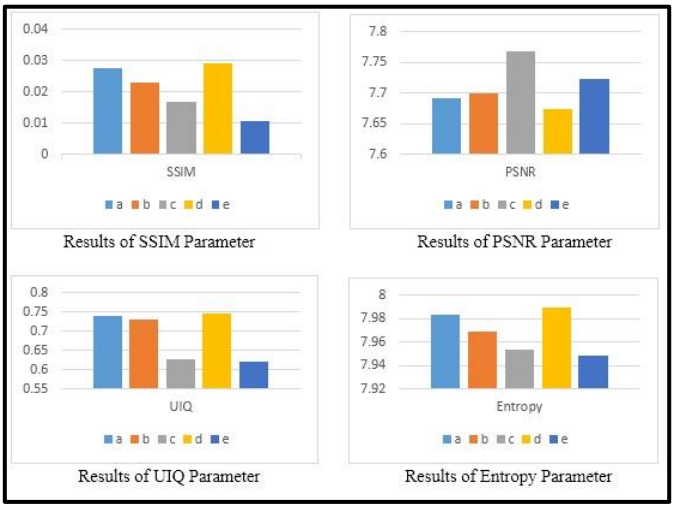

Figure 7: Results of SSIM, PSNR, UIQ, and Entropy parameters

6 CONCLUSION

The IoT and cloud computing techniques are essential, especially when integrated. Most companies and government institutions depend directly on these technologies in their work, providing ease and speed in work and reducing costs and simplicity of use. In this paper, an integrated security system was designed for intelligent building by integrating IoT and cloud computing. The critical information is encrypted and sent from the sender to the recipient. There is more than one technology in the encryption and decryption process, and several parameters were used to measure the method's effectiveness. The experiment outcomes showed that the proposed system is strong, effective, secure, and able to withstand many attacks.

REFERENCES

1. R. Buyya, C. Shin, S. Venugopal, J. Broberg, and I. Brandic, "Cloud computing and emerging IT platforms_: Vision , hype , and reality for delivering computing as the 5th utility," Futur. Gener. Comput. *Syst.*, 2009, pp. 599–616.
2. H. F. Atlam, A. Alenezi, A. Alharthi, "Integration of Cloud Computing with Internet of Things: Challenges and Open Issues," IEEE International Conference on Internet of Things and IEEE Green Computing and Communications and IEEE Cyber, Physical and Social Computing and IEEE Smart Data, 2017.
3. L. Atzori, A. Iera, G. Morabito," The Internet of Things: A survey," Volume 54, Issue 15, 28 October 2010, Pages 2787-2805.
4. S. Roy, R. Bose, D. SarddR," A fog-based DSS model for driving rule violation monitoring framework on the Internet of things," International Journal of Advanced Science and Technology Vol.82 (2015), pp.23-32 http://dx.doi.org/10.1425 7/ijast.2015.82.03
5. C. Stergiou, K. E. Psannis, B. Kim," Secure integration of IoT and Cloud Computing," Future Generation Computer Systems 78 (2018) 964–975, http:// dx.doi.org/10.1016/j.future.2016.11.031
6. M. Swan, "Sensor Mania! The Internet of things, wearable computing, objective metrics, and the quantified self 2.0," J. Sens. Actuator Netw. 2012, 1, 217-253; http://dx.doi.org/10.3390/jsan1030217, 8 November
7. M. A. Alsmirat, Y. Jararweh, I. Obaidat," Internet of surveillance: a cloud supported large scale wireless surveillance system, J. Supercomput. (2016) Springer. https:// doi.org / 10.1007/s11227-016-1857-x
8. R. Shanbhag and R. Shankarmani, "Architecture for Internet of Things to minimize human intervention, 2015 Int. Conf. Adv. Comput.Commun. Informatics, 2015, pp. 2348–2353.
9. X. Xiaohui, "Study on Security Problems and Key Technologies of The Internet of Things," Fifth International Conference on Computational and Information Sciences (ICCIS), pp. 407–410, 2013.
10. S. A. Kumar, T. Vealey, H. Srivastava, "Security in Internet of Things: Challenges, Solutions and Future Directions," 2016 49th Hawaii International Conference on System Sciences. DOI 10.1109/HICSS.2016.714
11. O. Y. Abdulhammed, " Load balancing of IoT tasks in the cloud computing by using sparrow search algorithm," The Journal of Supercomputing https://doi.org/10.1007/s11227-021-03989-w, (2021).

12. B. B. P. Rao, P. Saluia, N. Sharma, A. Mittal and S. V. Sharma, "Cloud computing for Internet of Things & sensing based applications," 2012 Sixth International Conference on Sensing Technology (ICST), Kolkata, 2012, pp. 374-380.
13. J. Zhou, T. Leppänen, E. Harjula, "CloudThings: A common architecture for integrating the Internet of Things with Cloud Computing," Proceedings of the 2013 IEEE 17th International Conference on Computer Supported Cooperative Work in Design (CSCWD), 2013, pp. 651-657.
14. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, and I. Stoica, "A View of Cloud Computing," Commun. ACM, vol. 53, no. 4, 2010, pp. 50–58.
15. A. Botta, W. De Donato, V. Persico, and A. Pescapé, “Integration of Cloud computing and Internet of Things_: A survey,” Futur. Gener. Comput. Syst., vol. 56, 2016, pp. 684–700.
16. S. M. Babu, A. J. Lakshmi and B. T. Rao, "A study on cloud based Internet of Things: CloudIoT," 2015 Global Conference on Communication Technologies (GCCT), 2015, pp. 60-65.
17. S. K. Dash, S. Mohapatra, P. K. Pattnaik,"A survey on applications of wireless sensor network using cloud computing." International Journal of Computer science & Engineering,Technologies, 2010, pp. 50-55.
18. S. Ibrahim, A. Alharbi, "Efficient Image Encryption Scheme Using Henon Map, Dynamic S-Boxes and Elliptic Curve Cryptography," IEEE Acess, 2020.
19. B. Song and Q. Ding, "Comparisons of typical discrete logistic map and henon map," in Intelligent Data analysis and its Applications, vol. 1, J.-S. Pan, V. Snasel, E. S. Corchado, A. Abraham, and S.-L. Wang, Eds. Cham, Switzerland: Springer, 2014, pp. 267_275.
20. 20- V. Rathore, A. K. Pal, " An image encryption scheme in bit plane content using Henon map based generated edgemap," Multimedia Tools and Applications, https://doi.org/10.1007/s11042-021-10719-0. 2021.