Computer Systems Science & Engineering
DOI:10.32604/csse.2022.022997
Article

Tech Science Press

Cryptographic Lightweight Encryption Algorithm with Dimensionality Reduction in Edge Computing

D. Jerusha* **and T. Jaya**

CSI Institute of Technology, Nagercoil, India
*Corresponding Author: D. Jerusha. Email: jerushadudley@gmail.com
Received: 25 August 2021; Accepted: 29 September 2021

Abstract: Edge Computing is one of the radically evolving systems through generations as it is able to effectively meet the data saving standards of consumers, providers and the workers. Requisition for Edge Computing based items have been increasing tremendously. Apart from the advantages it holds, there remain lots of objections and restrictions, which hinders it from accomplishing the need of consumers all around the world. Some of the limitations are constraints on computing and hardware, functions and accessibility, remote administration and connectivity. There is also a backlog in security due to its inability to create a trust between devices involved in encryption and decryption. This is because security of data greatly depends upon faster encryption and decryption in order to transfer it. In addition, its devices are considerably exposed to side channel attacks, including Power Analysis attacks that are capable of overturning the process. Constrained space and the ability of it is one of the most challenging tasks. To prevail over from this issue we are proposing a Cryptographic Lightweight Encryption Algorithm with Dimensionality Reduction in Edge Computing. The t-Distributed Stochastic Neighbor Embedding is one of the efficient dimensionality reduction technique that greatly decreases the size of the non-linear data. The three dimensional image data obtained from the system, which are connected with it, are dimensionally reduced, and then lightweight encryption algorithm is employed. Hence, the security backlog can be solved effectively using this method.

Keywords: Edge computing (e.g); dimensionality reduction (dr); t- distributed stochastic neighbor embedding (t-sne); principle component analysis (pca)

1 Introduction

Edge Computing is an evolving archetype generally founded as one of the progressions of Information Technology that develops towards universal network of computing. This implies that conventional devices such as PCs, and other devices that have the facility to be connected with others can be counted on to be present and connected online. Sharing when all such devices are connected to a very large community will have major concerns on security issues, as a large number of devices will be connected, i.e., it is obvious that common dangers of security, and assaults from universal Information Technology systems

are ever present. Hence this is the reason why a network administration that are already in usage have basic predefined security facilities [1].

Cloud and edge perform operations that make up for each other to form an equally beneficial and inter-related service range. Some purposes are obviously more beneficial to carry out in centralized cloud, although others are better suitable at the edge. The real-time and low-latency services of Edge computing limits the devices capacity or time-delay. Time and power consumption of cryptographic algorithms is its limitation and there is also a lack of capability of smart devices to store a waste amount of keys which ensures the security of data transfer. It is tedious task to introduce private and Secure connection. It may lead doubts on the stability of connection between to unknown smart objects and the data that are exposed while to strange devices come into connection. Here users should clearly monitor data transfers and give access permissions accordingly. Little machines that don't even have a keyboard or a monitor and hence less efficient when processing and memory are concerned and hence security policies of the users get limited. These devices must be sometimes authorized blindly for a good connection experience [2].

Nowadays we have lot of algorithms in order to bring very large information into small spaces. The method of transferring a group of results of variables to a set of values from straight non-interactive variables called principal components is said to be principal component analysis [3]. The principal component analysis method is tracked by an inspection of the information contents of the principal component image bands, which exposed that only the first few bands include significant information. The use of the first few principal component images can yield about 70 percent correct classification rate. This study suggests the benefit and efficiency of using the principal component analysis technique as a preprocessing step for the classification of hyperspectral images [4]. But the algorithm of principal component analysis is radical. This can be met up by the usage of multicore central Processing units and graphic processing units [5–7].

Since PCA is linear it cannot sort non-linear data efficiently. The system of PCA is made use of determining the aspects of the data and assigning it in a certain extent of space and rejecting the unnecessary data's. A technique is to be determined to obtain nonlinear data pattern. Here encoding of data's which are of lower size to a higher sized. Kernel method is made use of to develop the nonlinear PCA. A principal component is located in varied areas by the help of kernel system. Finally, it's processed in a fresh space and larger values are obtained.

When principal component analysis is concerned, it is a traditional sorted out method in statistical researches. KPCA the data are driven from a group of clusters whereas the data has no standard procedure of disjunction. KPCA cannot evaluate the variables in the dataset precisely because of the internal calculation method. This method of selecting datasets from a group of clusters plays a major role in logical method. This nonlinear type of principal component analysis is called kernel principal component analysis and is able to obtain high level variables hence capable of generating more data [8].

But the development in Remote Sensing Technology has been drastic in satellite and Airborne. Here the size of the image information that is obtained by the remote sensor has been increased and stored in very large information storage devices. But the enormous increase in the size of the data obtained and when this happens as a daily task Areas where reduction of size of the data so that it gets interrupted regularly gets affected in several means and applications [9]. t-stochastic neighbor embedding another effective algorithm that is capable of size reduction of data that are not linear. It is commonly used for the purpose of data visualization but it can also be used when machine learning is concerned which include feature image data reduction and clustering. The process of reducing the size of the data is achieved by applying the method of spectral clustering and topological unsupervised learning and have preservation of data by topology plays a vital role. Finally, after the machine learns through t-SNE, the data that are likely are removed from the data that are not liable [10].

One of the ways to effectively find a solution for fast development of applications that greatly make use of Extraordinary Limited power demanding machines is lightweight cryptography. It comes under the category of 286A. It mainly aims for the protection of devices that effectively balance between safety privacy power demands and usage of Limited resource conditions. The particular recommendation is to improve the outcomes in plans with better balance in the midst of security, execution and resource necessities for specific resource crucial conditions. Particular connection of equipment and programming execution is problematic because of difference in estimations, proportions of ampleness, and executing stage, regardless of the route that there have been a couple touchtone examinations of both hardware and programming utilization [11].

2 Related Work

In [12] describes that ubiquitous transfer of data over internet leads to numerous attacks like eavesdropping, denial of service, fabrication attacks. To overcome these type of attacks in Internet of Things (IoT) needs a lightweight high encryption technique. The comparative analysis of various lightweight encryption technique remain listed and compared. In [13] explains that the Cryptographic encryptions are a decent technique to guarantee data security in the IoT. Yet numerous IoT devices not taken aback enough to help such powerful procedures. In this way, to empower them on the IoT, calculations should be less energy devouring, however ought not to think twice about their efficiency. In [14] make clear that as information's are getting discernible through IoT, security related threats have expanded complex. Security of data is substantial to protect it from any third individual. Notwithstanding this, issues identified with data ownership have to be sorted. Measures taken to sustain the user involvement in IoT framework. ISO/IEC 29192, Lightweight Cryptography intending to offer responses for rapidly creating applications that broadly use outstanding limited power for constrained devices. Lightweight cryptography is a subcategory of cryptography as 286 A. Shah and M. Specialist ensured by NIST. The particular suggestion is to use improvement that outcomes in plans with better equalize in the midst of security, execution and resource requirements for specific resource constraint environments [15]. Unmistakable connection of equipment and programming execution is problematic because of difference in estimations, proportions of sufficiency, and executing stage, notwithstanding the way that there have been a couple of examinations for both hardware and programming utilization [16].

"Lightweight Cryptography", in the IoT needs to accomplish end-to-end security; end hubs have an execution of a symmetric key efficiency. For the low resource-devices, for example battery-fueled devices, the cryptographic activity with a restricted measure of energy utilization is significant. Use of the lightweight symmetric key calculation permits lower energy utilization for end devices. The impression of the lightweight cryptographic natives is more modest than the traditional cryptographic ones. The lightweight cryptographic natives would open prospects of more organization associations with lower resource devices [17]. In [18] explains about the different encryption methods have been read for securing client information stored on a cloud worker from untrusted administrators or aggressors. Nevertheless, one burden of existing information encryption innovations is that they cannot be effortlessly applied to information dividing administrations between numerous clients over distributed storage. To resolve this issue, information can be overseen through the most essential plan, which is the encryption of stored information. In any case, existing basic encryption plans show issues with the entrance the executives of information stored in the cloud climate. That is, an enormous number of clients may wish to get to information in the cloud worker all the while, or different capacities might be required, counting access control as indicated by a client's position. Existing public or symmetric key-based encryption plans can neither tackle the key administration issue nor fulfill the access control prerequisites.

In [19] Lightweight Attribute-based Encryption for the Internet of Things" proposed CP-ABE plot utilizing powerful pre-computation techniques. The key idea driving pre-computation techniques is to pre-register also, cache set sets gathered with normally extravagant cryptographic tasks. Pre-computation techniques based on the generator, the preprocessing calculations of the generator are executed by the equipment devices or confided in power. The pre-computation technique lessens the expense of CP-ABE encryption; the pre-computation technique utilized less computation and less energy channel than unique pattern. Edge Computing devices that have small storing capacities less memory and less effective processors are targeted to be benefited by the work of this paper. This compact device is not suitable for needs of security that are purely based on encryption. This is because of the inability of those devices to rapidly process the encryption and decryption in order to transfer data quickly and securely. Here is a model that is proposed to greatly help in optimizing storage memory processing and encryption problems. The arrangement of the whole proposal is as follows: we propose the system of implementing t-SNE for clearing out all limitations of the devices in Edge Computing in the First section. t-SNE is a key to reduce the dimension of three dimensional data into two dimensional data are discussed in second section. Section third addresses about the Lightweight encryption algorithm. In. Section Fourth comprises of various outputs and at last it is concluded.

3 Proposed Methodology

3.1 System Design

Edge computing provides profound aid to solve the problematic task in an effective way of involving the lightweight devices. The tremendous change in change in its development provoked numerous security backlogs and issues with complicated constraints. Fig. 1**.** shows the architecture of edge computing [20].

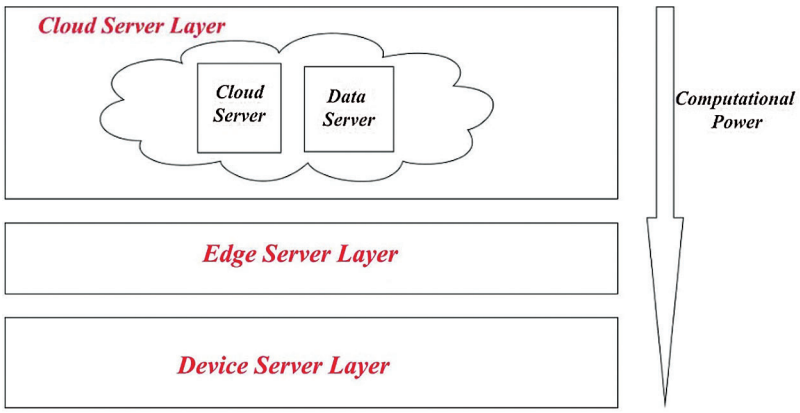

Figure 1: Architecture of edge computing

Edge computing devices has restricted amounts of storage capacity, memory, and process capability and that they typically ought to be ready to treat only on lower power. Security approaches that heavily depends on encryption technique which needs less space to update and utilize its ability to transmit data firmly in less period**.** Our proposed idea is to implement a t-Distributed Stochastic Neighbor Embedding (t-SNE) is a non-linear method for dimensionality reduction method to simplify the entire size of an image data. It greatly compresses the image size of the obtained image and makes the encryption technique more easy and compatible. The main usage of this neighbor embedding method is to dimensionally reduce the three dimensional data into two-dimension image data without losing its clarity. Here we make use of a lightweight encryption algorithm called Message Digest (MD5), which immensely contribute so much to diminish the disadvantages of the edge computing. Fig. 2 shows the architecture of proposed system design.

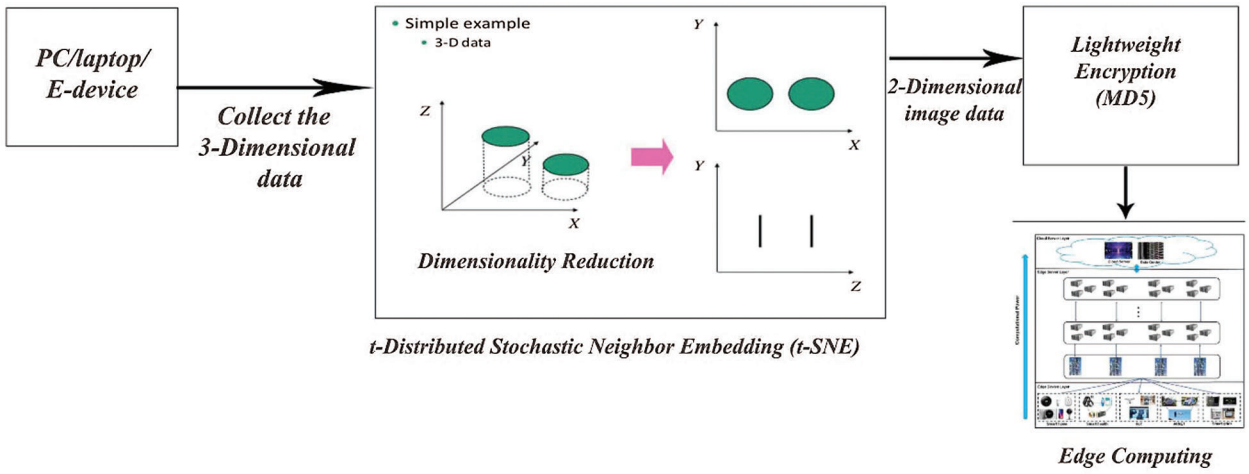

Figure 2: Architecture of proposed system design

3.2 t-Stochastic Neighbor Embedding (t-SNE Models)

t-distributed stochastic neighbor embedding is used for reducing dimensions which greatly fits in visualizing data sets that are greater in dimension.

i) The first step of the system is determining the amount of similarity of point in large spaces and calculating the same for spaces that a lesson dimension. This point similarity is determined based on the probability of point A to accept point B as its adjacent one where this happens based on the probability density by means of Gaussian located at A.

ii) The variations between the conditional probabilities for the process to be minimized so that the visualization of the spaces with large dimension are effective in low dimensional space.

iii) Gradient descent method is effectively used by t-SNE to diminish the sum of kullback-leiberdivergence which comprises all data points in order to determine the reduction of sum of variations of conditional probability.

The difference of one probability distribution from another probability distribution is determined by making use of kullback divergence. This helps in areas like individuating adjacent entropy in data algorithms, arbitrary that occur in continuous time series, and collection of information. Finally, zero output in kullback-leiber divergence shows that two distributions in a question are similar.

In favor of discrete probability distributions P and Q characterized on a similar probability space, the Kullback–Leibler divergence between P and Q is characterized to be

$$\sum_{x\in \mathrm{X}} F_x(\mathrm{P} \parallel Q) = \sum_{x\epsilon \mathrm{X}} \mathrm{P}(x) \log\left(\frac{P(x)}{Q(x)}\right) \tag{1}$$

$F_x(\mathrm{P} \parallel Q)$ is the discrete probability distribution of P & Q

The Kullback–Leibler divergence is considered as x, $Q(x) = 0 \Rightarrow P(x) = 0$

At whatever time P(x) is 0 the function of the consequent term is inferred as zero because

$$\lim_{x\to 0^+} x \log(x) = 0 \tag{2}$$

For distributions P and Q of a continuous random variable, the Kullback–Leibler divergence is defined to be the integral

$$P[\infty \leq x \leq \infty] = \int_{-\infty}^{\infty} P(x) \log\left(\frac{P(x)}{Q(x)}\right) dx \tag{3}$$

$P[\infty \leq x \leq \infty]$ is the continuous probability distribution of P and Q where P and Q represent the probability densities of P and Q.

In addition, if P and Q are probably regulated over a set X, and P is uninterrupted with deference to Q, then the Kullback–Leibler divergence from Q to P is termed as

$$P[x] = \int_{x}^{-x} \log\left(\frac{dP}{dQ}\right) dP \tag{4}$$

where $\frac{dP}{dQ}$ is the Radon–Nikodym derivative. Stipulated with an expression on the right-hand side. Consistently (by the chain rule), this can be written as

$$\upsilon(P \parallel Q) = \int_{x} \log\left(\frac{dP}{dQ}\right) \frac{dP}{dQ} dQ \tag{5}$$

which is the entropy of P comparative to Q. Remaining in this case, if μ is any measure on X for which and $p = \frac{dP}{d\mu}$ and $q = \frac{dQ}{d\mu}$ exist (involving that p and q are entirely continuous with regard to μ), then the Kullback–Leibler divergence from Q to P is given as

$$D_{KL}(P \parallel Q) = \int_{x} p \log\left(\frac{p}{q}\right) d\mu \tag{6}$$

Algorithm 1: t-Distributed Stochastic Neighbor Embedding

Data: $\chi = \{x_1, x_2, \ldots, x_m\}$

Factors:Dimension of a probability model used calculates a sample P

Optimization Parameters: total of reiterations T, learning rate α, momentum $p(t)$.

End result:Dimensionally reduce the data

Begin

Perform the operations of pairwise resemblances with predicted model

Set $p_{ij} = \frac{P_{j|i} + P_{i|j}}{2m}$

Check out intial solutions $\mathrm{Y}^{(T)} = \{y_1, y_2, \ldots, y_m\}$

for t = 1 to T do

perform operations on low-dimensional data

calculate $\frac{\delta C}{\delta y}$

set $\mathrm{Y}^{(t)} = \mathrm{Y}^{(t-1)} + \alpha \frac{\delta C}{\delta y} + p(t)(\mathrm{Y}^{(t-1)} - \mathrm{Y}^{(t-2)})$

end

end

3.3 Lightweight Encryption Algorithm

Here we are utilizing MD5 lightweight encryption algorithm structure in Fig. 3. It is described as below:

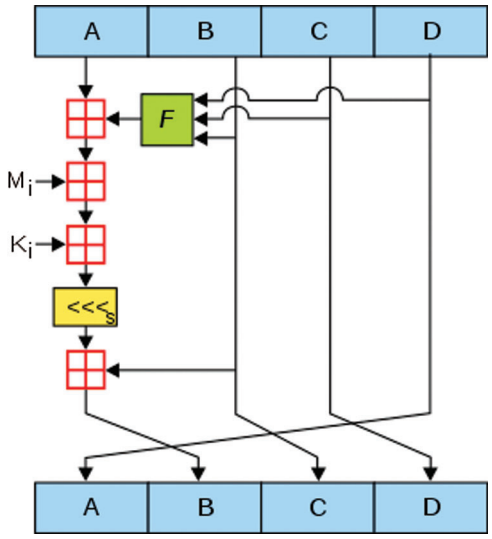

Figure 3: MD5 algorithm

MD5 Algorithm:

MD5 is a hash algorithm instigated by professor Ronald Rivest [21]. It is an enhanced version of its predecessor MD4 [22]. MD5 is commonly used in several public key cryptographic algorithms and Internet communication in common. MD5 evaluates a 128-bit digest for an arbitrary b-bit message and it involves of the following steps in Fig. 3.

Hashing the element using MD5 algorithm involves the generation of hexadecimal values by sequentially applying the following series of methods.

Appending padding bits: The element x, which initially is a string is converted into bits. Now, at the end of the 'b' bit message, a single '1' bit is added so that the message becomes divisible either to 448 or to 512.

Appending Length: In case, the obtained output is a multiple of 448, it has to be made divisible to 512, which can be achieved by means of addition of 64-bit representation.

Buffer Initialization: This is a process of dividing the b bit outcome of the previous step into a four-word buffer (A, B, C, D) each being 32-bit registers. These registers are made usage of in 128-bit message digest derivation. They are initially hexadecimal and in low order bytes.

Processing the message: The message is processed as 16 words with four auxiliary functions and various processing of steps yield the needed output. The plain text is now changed to cipher text and the message digest is obtained as an output.

3.4 Analysis Results

In the analysis of different factual techniques, proficiency is a proportion of nature of, an estimator, of a trial structure, or of a speculation testing system. Basically, an increasingly proficient estimator, test, or test needs less perceptions than a less productive one to accomplish a given presentation.

t-Stochastic Neighbor Embedding (t-SNE models)

Discrete probability distributions P and Q symbolized on a related probability space, the t-Stochastic Neighbor Embedding (t-SNE models) between P and Q is characterized to be

$$Y^{(t)} = Y^{(t-1)} + \alpha \frac{\delta C}{\delta y} + p(t)(Y^{(t-1)} - Y^{(t-2)}) \tag{7}$$

The t-Stochastic Neighbor Embedding (t-SNE models) between p(x) and q(x) of two beta distribution can be illustrated by a graph plot against beta(x;α,β) which is on y-axis and x(x-axis) in Fig. 4.

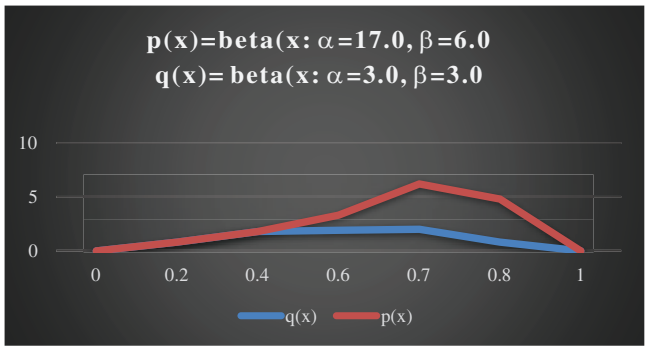

Figure 4: Performance evaluation of t-SNE

Since we have understood the algorithm, it is time to examine its performance. As you might have noticed that, the algorithm computes pairwise conditional probabilities and tries to limit the amount of the distinction of the probabilities in higher and lower measurements. This includes a lot of calculations and computations. Therefore, the algorithm is quite hefty on the system assets.

t-SNE makes some quadratic Time and space complexity in the quantity of data points. This makes it particularly lethargic and asset depleting while at the same time applying it to data sets involving in excess of 10,000 observations. t-SNE works really hard in separating data points with 2 components. We cannot utilize this for transforming new data, implies it is not helpful for ordering a different set of data. Perplexity guarantees the quantity of neighbors t-SNE is safeguarding based on distance metric. Try perplexity esteem in the scope of 5 to 50, as suggested in our research paper. Try multiple worth of steps until changes in cluster is saturated. Distance between clusters may not be helpful. t-SNE by and large extends thick cluster and psychologist inadequate cluster. t-SNE like numerous unsupervised learning algorithms often give an unfortunate chore, for example obtaining early insight on whether or not the data is divisible, testing that it has some identifiable structure, and inspecting the nature of this structure.

n_components = 2, random_state = 0, perplexity = 30.0, learning_rate = 200.0, n_iter = 10000, n_iter_without_progress = 300 is shown in Fig. 5.

n_components = 2, random_state = 0, perplexity = 50.0, learning_rate = 200.0, n_iter = 10000, n_iter_without_progress = 300 is shown in Fig. 6.

n_components = 2, random_state = 0, perplexity = 5.0, learning_rate = 200.0, n_iter = 10000, n_iter_without_progress = 300 is shown in Fig. 7.

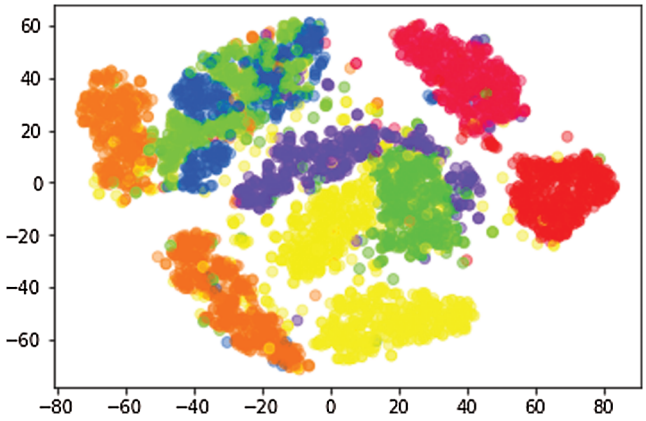

Figure 5: Data visualization of t-SNE when perplexity = 30.0

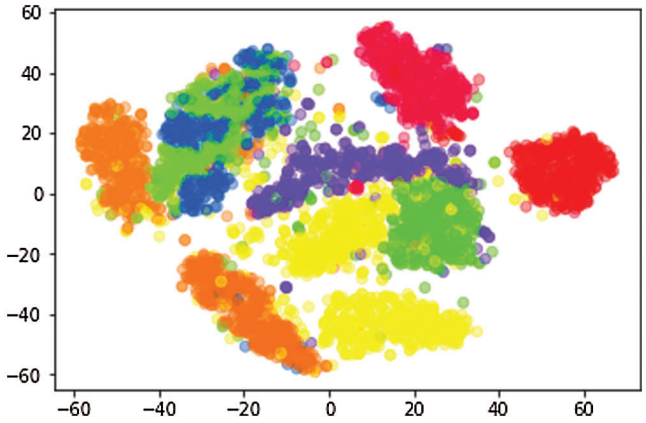

Figure 6: Data visualization of t-SNE when perplexity = 50.0

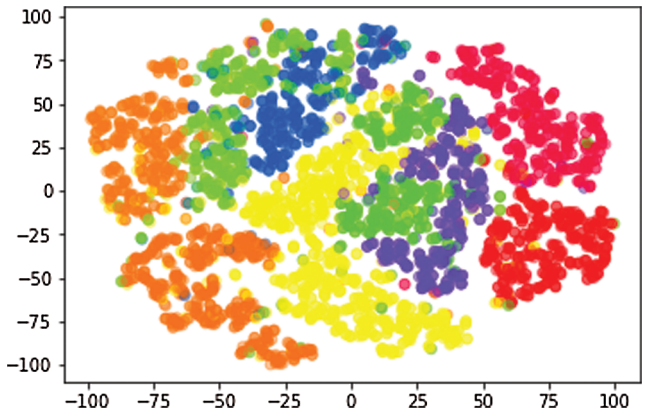

Figure 7: Data visualization of t-SNE when perplexity = 5.0

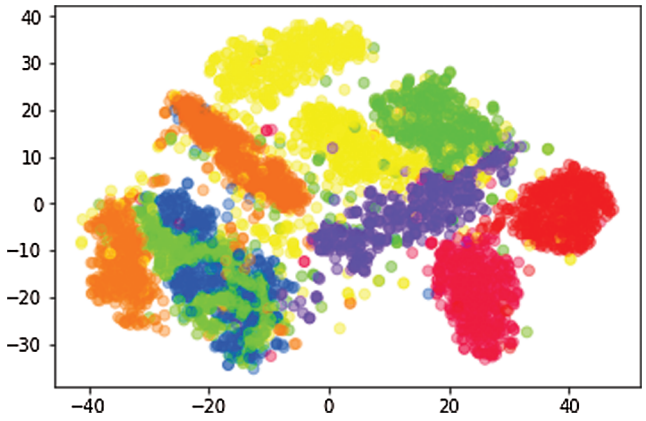

Figure 8: Data visualization of t-SNE when perplexity = 100.0

n_components = 2, random_state = 0, perplexity = 100.0, learning_rate = 200.0, n_iter = 10000, n_iter_without_progress = 300 Fig. 8**.**

MD5 Algorithm efficiency:

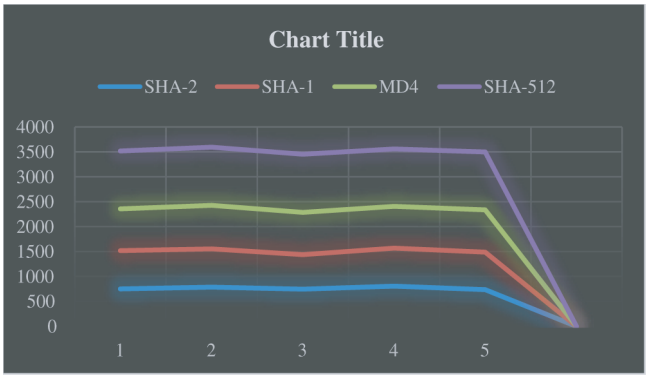

Figure 9: Algorithm Efficiency of SHA-2, SHA-1, MD-4, SHA-512

It requires only less space and the time taken to complete the action are fast and acceptable. The graph is plotted against the number of bits to be executed with respect to time is shown in Fig. 9.

Data to encode is "Cryptographic Lightweight Encryption Algorithm with Dimensionality Reduction in Edge computing" characters in length 85 (**44f4ebf0314eaf64ed78c29741380fb4**) is shown in Tab. 1.

Table 1: Time taken chart MD5 *vs.* MD4 *vs.* SHA-1 *vs.* SHA-2

Hash	1 ms	2 ms	3 ms	4 ms	5 ms	Average per min
SHA-2	751	789	745	806	737	765.6
SHA-1	768	765	694	763	751	748.2
MD4	842	876	848	839	850	851
MD5	1161	1164	1168	1154	1163	1158.8

4 Conclusion

Edge computing platforms operate and deliver varied reasonable intelligence and communication employing data's. They assist to gather information, thrusting it and sharing it with an entire network of connected devices. All this collected information makes it doable for devices to separately operate, and therefore the whole scheme is changing into "smarter" each day. As the demand increases the concerned industry has some drawbacks to overcome. Constrained space and ability of Edge Computing is one of the most challenging task. To prevail over from this issue we are proposing a Cryptographic Lightweight Encryption Algorithm with Dimensionality Reduction in Edge Computing. t-Distributed Stochastic Neighbor Embedding is one of the efficient dimensionality reduction technique. This method not only considers the linear data but also concentrates on non-linear data. The images obtained from the sensors are reduced dimensionally and employ the lightweight encryption. One of the most well-known Lightweight encryption method is MD5 Algorithm. This helps the dimensionally reduced data to encrypt and decrypt the optical images. They are in the lead of their efficacy and feasibility. The proposed technique completely overcomes the defects and disabilities of the Edge Computing devices.

Funding Statement: The authors received no specific funding for this work.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present work.

References

[1] S. Meng, Q. Li, T. Wu, W. Huang, J. Zhang *et al.,* "A fault tolerant dynamic scheduling method on hierarchical mobile edge cloud computing," *Computational Intelligence*, vol. 35, pp. 577–598, 2019.

[2] S. K. Sharma and X. Wang "Live data analytics with collaborative edge and cloud processing in wireless IoT networks," *IEEE Access*, vol. 5, pp. 4621–4635, 2017.

[3] D. Rajesh and T. Jaya, "Exploration on cluster related energy proficient routing in mobile wireless sensor network," *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, vol. 8, no. 4, pp. 93–97, 2019.

[4] C. Esposito, A. Castiglione, F. Pop and K. R. Choo, "Challenges of connecting edge and cloud computing: A security and forensic perspective," *IEEE Cloud Computing*, vol. 4, no. 2, pp. 13–7, 2017.

[5] L. Odysseas, P. Dionisis and G. John, "A novel combination of distributed ledger technologies on internet of things: Use case on precision agriculture," *Applied System Innovation*, vol. 2, no. 30, pp. 1–31, 2019.

[6] M. Q. Tran, D. T. Nguyen, V. A. Le, D. H. Nguyen and T. V. Pham "Task placement on fog computing made efficient for IoT application provision," *Wireless Communications and Mobile Computing*, vol. 2019, pp. 1–17, 2019.

[7] D. Rajesh and T. Jaya, "A mathematical model for energy efficient secured ch clustering protocol for mobile wireless sensor network," *Wireless Personal Communications*, vol. 112, no. 1, pp. 421–438, 2020.

[8] N. Fernando, S. W. Loke and W. Rahayu, "Computing with nearby mobile devices: A work sharing algorithm for mobile edge-clouds," *IEEE Transactions on Cloud Computing*, vol. 7, no. 2, pp. 329–343, 2019.

[9] K. Zhu, Z. Chen, Y. Peng and L. Zhang, "Mobile edge assisted literal multi-dimensional anomaly detection of in-vehicle network using LSTM," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 5, pp. 4275–4284, 2019.

[10] D. Rajesh and T. Jaya, "Enhancement of network lifetime by fuzzy based secure CH clustered routing protocol for mobile wireless sensor network," *Journal of Ambient Intelligence and Humanized Computing (JAIHC)*, pp. 1–11, 2021.

[11] X. Sun and N. Ansari, "EdgeIoT: Mobile edge computing for the internet of things," *IEEE Communications Magazine*, vol. 54, no. 12, pp. 22–29, 2016.

[12] D. Rajesh and D. G. Kiruba, "A probability based energy competent cluster based secured CH selection routing EC^2SR protocol for smart dust," *Peer-to-Peer Networking and Applications*, vol. 14, pp. 1976–1987, 2021.

[13] A. Botta, W. D. Donato, V. Persico and A. Pescapé, "Integration of cloud computing and internet of things: A survey," *Future Generation Computer Systems*, vol. 56, pp. 22–29, 2016.

[14] Z. Wu, Y. Li, A. Plaza, J. Li, F. Xiao *et al.,* "Parallel and distributed dimensionality reduction of hyperspectral data on cloud computing architectures," *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, vol. 9, no. 6, pp. 2270–2278, 2016.

[15] A. Whitmore, "The internet of things-A survey of topics and trends," *Information Systems Frontiers*, Springer, vol. 12, no. 2, pp. 261–274, 2015.

[16] D. Rajesh, M. Firoja Banu, D. Stella and A. P. Grace, "Ch panel based routing scheme for mobile wireless sensor network," *International Journal of MC Square Scientific Research*, vol. 8, no. 1, pp. 183–198, 2016.

[17] D. Rajesh and T. Jaya, "ECIGC-MWSN: Energy capable information gathering in clustered secured CH based routing in mwsn," *In Materials Today: Proceedings*, vol. 43, no. 3, pp. 3457–3462, 2021.

[18] W. Shi, J. Cao, Q. Zhang, Y. Li and L. Xu, "Edge computing: Vision and challenges," *IEEE Internet of Things*, vol. 3, no. 5, pp. 637–646, 2016.

[19] S. Wang, T. Tuor, T. Salonidis, K. K. Leung, C. Makaya *et al.,* "Adaptive federated learning in resource constrained edge computing systems," *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 6, pp. 1205–1221, 2019.

[20] Y. Chang, "Research on de-motion blur image processing based on deep learning," *Journal of Visual Communication and Image Representation*, vol. 60, pp. 371–379, 2019.

[21] M. Gochoo, T. Tan, S. Liu, F. Jean, F. S. Alnajjar *et al.,* "Unobtrusive activity recognition of elderly people living alone using anonymous binary sensors and DCNN," *IEEE Journal of Biomedical and Health Informatics*, vol. 23, no. 2, pp. 693–702, 2019.

[22] S. Teerapittayanon, B. McDanel and H. T. Kung, "Distributed deep neural networks over the cloud, the edge and end devices," in *IEEE 37th Int. Conf. on Distributed Computing Systems*, Atlanta, GA, USA, pp. 328–339, 2017.