A dynamic data encryption method based on addressing the data importance on the internet of things

Dana Khwailleh, Firas Al-balas
Department of Computer Science, Jordan University of Science and Technology, Ar-Ramtha, Jordan

Article Info

Article history:

Received May 24, 2021
Revised Sep 19, 2021
Accepted Oct 10, 2021

Keywords:

Block cipher
Security over internet of things
Stream cipher

ABSTRACT

The rapid growth of internet of things (IoT) in multiple areas brings research challenges closely linked to the nature of IoT technology. Therefore, there has been a need to secure the collected data from IoT sensors in an efficient and dynamic way taking into consideration the nature of collected data due to its importance. So, in this paper, a dynamic algorithm has been developed to distinguish the importance of data collected and apply the suitable security approach for each type of data collected. This was done by using hybrid system that combines block cipher and stream cipher systems. After data classification using machine learning classifiers the less important data are encrypted using stream cipher (SC) that use rivest cipher 4 algorithm, and more important data encrypted using block cipher (BC) that use advanced encryption standard algorithm. By applying a performance evaluation using simulation, the proposed method guarantees that it encrypts the data with less central processing unit (CPU) time with improvement in the security over the data by using the proposed hybrid system.

Corresponding Author:

Firas Albalas
Department of Computer Science, Jordan University of Science and Technology
Ar Ramtha 3030, Ar-Ramtha, Jordan
Email: faalbalas@just.edu.jo

1. INTRODUCTION

The internet of things (IoT) is defined as connecting all objects in different environments through the internet. These objects collect different data, and sometimes data may be of high importance, whether it is about the surrounding environment or the user itself [1]. Therefore, it is necessary to ensure that only the receiver can safely recover this information [2] and to protect this information from any risk that may occur to it, such as penetration by unauthorized persons or eavesdropping by a third party [3]. Figure 1 shows the definition of IoT. To get the widespread of internet IoT obtained that by enabling easy access and collaboration with a large number of devices, for example, personal appliances, control cameras, sensors, motors, and screens, the IoT will promote development through application, in order to massively use risks, and attack information provided by these creatures to provide new services to citizens, companies, and public administrations [4].

Today, there are many uses of the internet such as making data globally available to authorized users and online data processing units. Of course, the data can be sensitive and this violates the privacy of users. This risk is exacerbated by the trend to separate the sensor network infrastructure and applications. Therefore, a security solution must be provided to achieve an appropriate level of security for the IoT [5]. Due to the lower cost and the time of marketing, IoT manufacturers did not give the security issue a priority to be part of their IoT devices. Few manufactured devices include a software-based security programs like firmware, however, the previous solutions do not take into consideration the different usage patterns of IoT when compared to personal computers, which proves to be irrelevant at times [6]. Moreover, focusing on software-based protection systems often leaves the device unintentionally weak, enabling new offensive vectors [7].

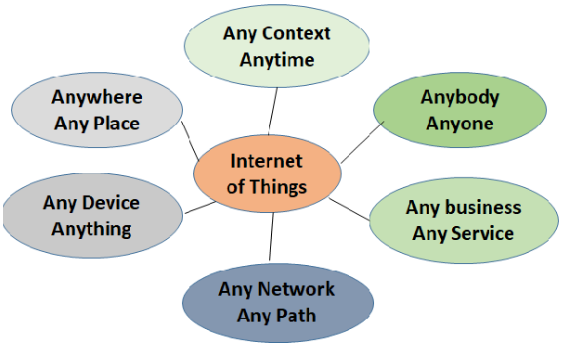

Figure 1. Definition of IoT [5]

Network security and data encryption are currently a very important topic in the modern communications network research areas. When we send some confidential matters from one customer to another customer that data should not be intercepted by an unauthorized person. Cryptography is now an emerging research field as scientists try to develop a good encryption algorithm so that no hacker can intercept the encrypted message. This means that whenever we want to send messages to someone, they must be encrypted so that no one can decrypt them without knowing the key to the decryption process [8] as shown in Figure 2.

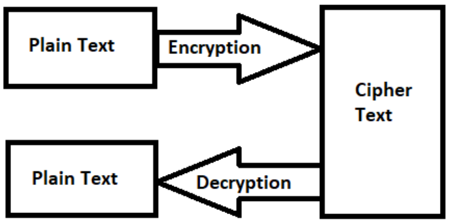

Figure 2. Encryption and decryption process [9]

For this type of security, two methods of encryption/decryption process are introduced: Symmetric and asymmetric. In symmetric encryption one key is used for both operation encryption/decryption data [10]. This security key implemented in algorithms which classified into either stream or block ciphers also depends on the size of the key. Stream cipher has two main components: the mixing function and the key stream. The first component is the exclusive OR (XOR) function, while the second component is the generator which considered the main unit of the stream cipher (SC) encryption. Block cipher (BC) algorithms that generalize N-bit blocks of plaintext data under the secret key selection and generate N-bit blocks of encrypted data for anything else [11].

In the last few years, the stream cipher has been widely used, to be replaced by a block cipher. This is due to a number of reasons, including security, which is one of the weaknesses of the stream cipher and is much lower than the security provided by the block cipher. The other reason is the efficiency that has been reduced in many applications where the stream cipher is used so it had to be addressed to solve this problem [12]. In this work, we compared the SC, BC and hybrid system methods shown in Figure 3. Rivest cipher 4 (RC4) is used for Stream cipher, while AES for block cipher. We designed a hybrid system that take advantages from both block and stream cipher [13]. The stream cipher [14] consists of an initial step, called the warm-up phase, which produces a key and an internal IV value that will produce the first output bit or bytes. The time required to perform "Key Setting", and "IV setting" is then tested. Moreover, one of the main advantages of a stream cipher is that it is able to produce long sequences at a high speed required for the encryption process. A stream cipher is usually used when wireless communication is required because it can reach significant flows for limited costs and the use of encryption "one-time panel" does not deploy errors caused by the channel connection. Block cipher [15] is a type of symmetric encryption that works on blocks of data. Modern block blades typically use a block length of 128 bits or more, including data encryption standard (DES), advanced encryption standard (AES), RC6 and international data encryption algorithm (IDEA) that supports key sizes of 128, 192, and 265 bits [16]. There are supported symmetrical key block encryption algorithms that have a 128-bit block size and cannot be used with a 64-bit block size such as cipher block chaining-message (CCM) authentication code algorithm [17], in block cipher the length of the plaintext is known, block cipher must be used in ciphertext stealing or residual block termination mode to avoid padding [18]. When the block of data that the BC want to encrypt/decrypt it shorter than the block size then BC cannot directly work on it.

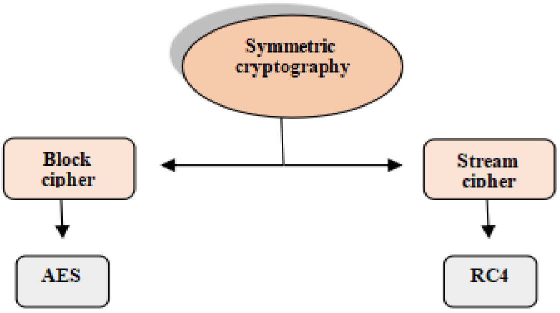

Figure 3. Block and stream algorithms considered for this work [19]

With the rapid increase in the volume of information, text classification has become an important issue in dealing with this huge volume of data. Text classification techniques are used to categorize news stories, to find interesting information on world wide web (WWW), and to guide user search through hypertext [20], [21]. The most common classifiers are: support vector machine (SVM), naïve Bayes (NB) and K-nearest neighbor (KNN) [22] that divide data into two parts: important and more important. In the paper [23], [24] the authors compare block cipher algorithms that include: IDEA, Blowfish, RC2, Serpent, Cast5, RC6, and stream cipher algorithms that include: Salsa 20, HC-128, VMPC, RC4, HC-256, Grain, in terms of CPU time and productivity as shown in Table 1. They concluded that the SC is faster than the BC.

Table 1. Comparison between block cipher algorithms and stream cipher algorithms [24]

	AES	3DES	DES	Cast-5/Blowfish	VMPC/Salsa 20
Key length	128,192, or 256 bits	(k1, k2, k3)168 bits (k1 and k2 is same)112 bits	56 bits	128,192, and 258 bits	128,192, and 258 bits
Cipher type	Symmetric block cipher	Symmetric block cipher	Symmetric block cipher	Symmetric block cipher	Symmetric stream cipher
Block size	128,192, or 256 bits	64 bits	64 bits	64 bits	128 bits
Security	Considered secure	One only weak which is exit in DES	Proven inadequate	Provide stronger security	Provide stronger security
Number of Rounds	16 rounds	48 rounds	16 rounds	Fixed	8, 12 or 20 rounds

It is a machine learning algorithm; the goal of this algorithm is to find a hyper plane that classify data points in a dimensional space. Hyper plane dimension relies on features number. Data points is considered support vectors because it helps in building the support vector machine model. The output of SVM is a hyper plane that separate classes and classify new data points. The setting parameters in SVM are kernel, regularization, gamma, and margin. Kernel transform the problem using linear algebra to learn the hyper plane in linear SVM model. In linear kernel we predicate the new instance using this equation that compute the products of new instance vector with each support vector in the training data.

$$F(x) = B\,(0) + sum\,(ai * (x, xi)) \tag{1}$$

In the polynomial kernel the prediction is done using (2).

$$K\ (x, xi)\ =\ 1\ +\ sum\ (x\ *\ xi)\ \hat{}d \tag{2}$$

In the exponential kernel the prediction is done using (3).

$$K\ (x, xi)\ =\ exp\ (-gamma\ *\ sum\ ((x—xi^2)) \tag{3}$$

The regularization parameter specifies how much to keep away from errors in classification. Large values give higher accuracy, smaller values give lower accuracy results. Gamma parameter specify the closeness of points to the separation line. Low gamma value that data point is far from the separation line and high gamma value mean that data point is close to the separation line. Margin is the distance between the line and the closest data points, larger margin value is a good to avoid crossing multiple classes [25]. It is a supervised machine learning algorithm that calculate feature probabilities and choose the feature with the highest probability. In this rule P (A|B) consider the probability of A given that B happen. This classifier gives a good performance recommender systems and text classification. Naïve Bayes take into account that features are independent.

$$P\ (A|B)\ =\ (P(B\,\big|\,A)\ P(A))/P(B)$$

Multinomial naïve Bayes is a version from naïve Bayes classifier that suppose the independency of features and between attributes, also it gives efficient performance [25]. It is a classification technique that depend on neighbor's majority voting, new input is assigned with the common class label of its neighbors. K is number of neighbors to be considered in voting. After applying classification for the testing domain, we calculate the performance of our classifier and use the evaluation metrics precision, recall, f-measure, and accuracy [25].

- $Precision = TP/(TP + FP)$
- $Recall = TP/(TP + FN)$
- $Accuracy = TP + TN/(TP + TN + FP + FN)$
  $F - measure = 2 * (Precision * Recall/(Precision + Recall))$

We find that KNN give us the best results when we increase the training set. In this paper, the proposed method and methodology is presented in detail in the second section. In the third section, the simulation environment and the result discussion are presented and explained. By the last section the article idea is concluded.

2. THE PROPOSED METHOD

As mentioned, securing data collected from IoT devices should be classified according to its importance to be able to get fast and accurate security output. The proposed method starts with classifying the data sets collected from IoT devices by using the most appropriate machine learning classifier algorithm then each type of classified data is inserted into the relevant type of security method depends on the data importance.

2.1. Data set

The data that used in this article can be accessed from [26], this data set has two classes: Normal patients which represents 100 patients and Abnormal patients which represents 210 patients. Each raw represents a patient attribute (6 attributes): pelvic incidence, pelvic tilt, lumbar lordosis angle, sacral slope, pelvic radius, and grade of spondylolisthesis.

2.2. Data classification

Selecting the best classification method to categorize the data is a very important step and the section should be done depending on our own experiments or previous study. So, we went to machine learning algorithms, we tested three classifiers: KNN, SVM, and NB [27]. We used Waikato environment for knowledge analysis (WEKA) which is free software that contains tools and algorithms for data analysis. Which is used to train the classifiers to get the performance for each one. We made 10 times cross-validation in the data with different training set sizes 60, 70, 80 and with 70% training data and 30% test data for each classifier. We found that the NB ratios were almost constant even when the training set increased, The SVM was high at first, but when the training set increased, the ratios were significantly lower. But the KNN was better than the NB and SVM, the accuracy increases even when the training set is increased as shown in Figure 4. So, we used KNN to categorize important data to be encrypted using block cipher, the less important data is encrypted using the stream cipher.

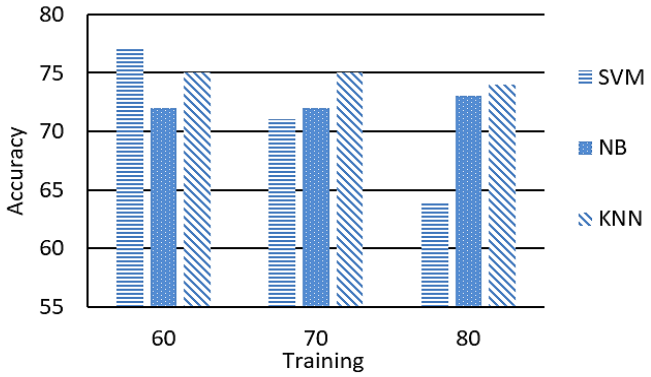

Figure 4. Comparison between NB, SVM, and KNN classifiers

2.3. Proposed hybrid system architecture

The hybrid system consists of two ciphers: SC and BC. First, we added some improvements to the BS, where we divided the data into a variable block size to get rid of the padding. We used a different key to encrypt each block to increase protection on the data, we used CBC mode and combined AES algorithm with it. As far as SC is concerned, we have reduced the size of the data by almost half, so they will not need much time to encrypt it, and we used RC4 algorithm with SC.

Our system passing the data (plaintext) to the KNN classifier to classify it into two parts: important and more important. Then more important data encrypted using block cipher that use AES. AES has a fixed block size of 128 bits, key size of 128, 192, or 256 bits. AES runs on a 4×4 column-main order array of bytes, called the state. Most AES accounts are made in a limited selected field. Each round consists of several processing steps, including: SubBytes where each byte is replaced with another according to a search table, ShiftRows where the last three rows of the state are periodically converted a certain number of steps, MixColumns it works on its state columns, combining the four bytes in each column, AddRoundKey. Each byte of the state is combined with a block of round key using XOR and finally KeyExpansion where encryption key produced the round keys [28], [29]. While less important data encrypted using stream cipher that use RC4. RC4 creates a key stream. Any current ciphers can be used by combining it with plain text using exclusive XOR. To create a key stream, encryption use the secret internal state that consists of two parts: a permutation of all 256 possible bytes which is configured using a variable length key, usually between 40 and 2048 bits, using the key scheduling algorithm (KSA), and two 8-bit index pointers which is generated using the pseudo-random generation algorithm (PRGA) [30], to finally get our encrypted data (ciphertext) as shown in Figure 5. The previous technique is used in the same way for decryption.

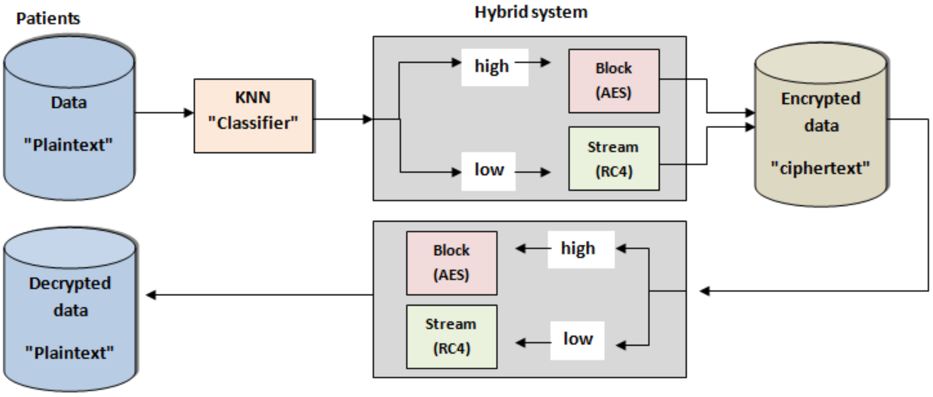

Figure 5. Hybrid system encryption and decryption

3. SIMULATION AND RESULTS

3.1. Simulation parameter

Table 2 presents the features of stream cipher (RC4) and block cipher (AES) which will be used and compared with the proposed method. The main goal of comparison is the CPU processing time and the impact of the proposed method in increasing the security when we use important data as well as reducing the central processing unit (CPU) time.

Table 2. Comparing AES and RC4 [30]

Algorithm	AES	RC4
Block size	64 bits and more	8 bits
Key size	128/192/256 bits	1-256 bits
Key Schedule	Complex	Simple
Complexity	Simple design	Complex comparatively

3.2. Experiment setting and challenges

In this study, a desktop computer 2.00 GHz processer, with 16.00 GB RAM operating under Windows was used and Java integrated development tool is used. It also supports various programming languages such as Python, Scala, and Java. As mentioned earlier the main goal of this work is to compare the performance of stream, block, and hybrid algorithms. In order to carry out the following tasks: i) use KNN algorithm to classify the data set that we used it in this work; ii) calculate the encryption/decryption time of each algorithm using input files of different sizes; and iii) calculate the encryption/decryption time (CPU processing time) of each algorithm using input files of different sizes.

One of the challenges we encountered in this study is that the amount of data collected takes a long time and finding large and comfortable data is not easy. Also, the data has to be visualized in graphs which take a long time to do manually. So, we used Microsoft Excel to speed it up. Also, one of the problems we encountered was that when writing code using Scala, we had no knowledge of it and had to attend courses to be able to reach the quality of the code we aspire to.

3.3. Results

By applying an extensive performance evaluation for the proposed method by injecting the emulator with different datasets size and then evaluate the CPU time as a performance measure. In Figure 6, we show the efficiency of security algorithms in terms of encryption time in different data size. You can see that time to encrypt files using proposed hybrid algorithm is less than the other two algorithms used in this study this improvement is because the proposed approach classifies the data according to importance and use the appropriate encryption algorithm which at the end reflect the time and performance of proposed algorithm against other algorithms. Regarding the efficiency of security algorithms in terms of decryption time in different data size, the time to encrypt files using proposed hybrid algorithm is less than the other two algorithms going closer to the SC algorithm which comes from the way the proposed approach decrypts the data according to the way back of encryption by using the best algorithm which at the end gives the proposed approach a step better than other algorithms.

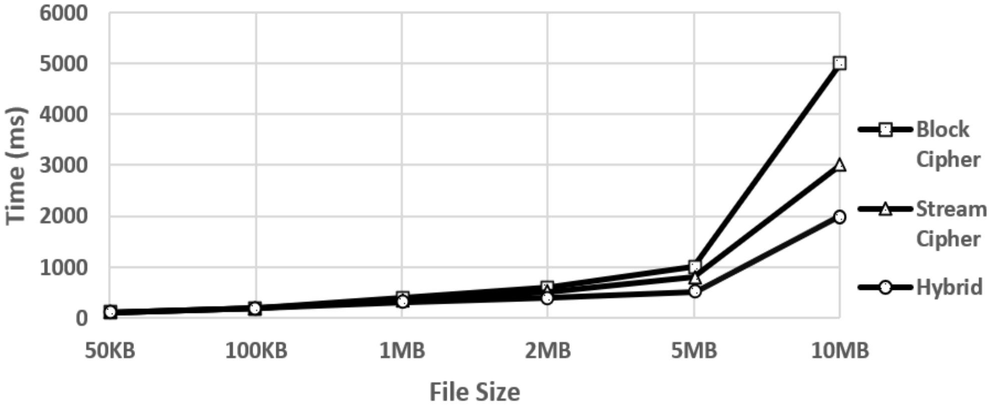

Figure 6. Encryption time of RC4, AES and hybrid

4. CONCLUSION

In this dynamic method, different encryption algorithms have been tested and their efficiency has been compared in term of encryption/decryption time. Block cipher showed the worst results compared to the algorithms that were implemented in this article. There is also good evident that the stream cipher generally takes less time than the block cipher for encryption/decryption. So, we develop a hybrid system that take advantages from both SC and BC to decrease encryption/decryption time and processing time and increase data security. We use ML classifiers: NB, SVM, and KNN to classify data into important and more important parts. KNN give us the best results 76.34%. Then hybrid system encrypt/decrypt important data using SC, and more important data using BC; to ensure that the size of data cut to a half. To get the best results from hybrid system with regard to encryption/decryption time and CPU time.

The use of block cipher and stream cipher is not limited to text-only. Since image encryption eliminates an important role in hiding information. Therefore, it is important to protect image data from unauthorized access. They proposed a new method based on the stream cipher for selective encryption for 256 colors and gray color images based on encryption discrete cosine transform (DCT) transactions. Another method based on the block cipher called RDH-EI method. As a future work, it is expected that the proposed approach will be tested and improved to be used with images to classify and encrypt especially for health platform with patient images.

REFERENCES

[1] E. de Matos *et al.*, “Context information sharing for the internet of things: a survey,” *Computer Networks*, vol. 166, Jan. 2020, Art. no. 106988, doi: 10.1016/j.comnet.2019.106988.

[2] P. Dixit, A. K. Gupta, M. C. Trivedi, and V. K. Yadav, “Traditional and hybrid encryption techniques: A survey,” in *Lecture Notes on Data Engineering and Communications Technologies*, vol. 4, 2018, pp. 239–248.

[3] C. Manifavas, G. Hatzivasilis, K. Fysarakis, and Y. Papaefstathiou, “A survey of lightweight stream ciphers for embedded systems,” *Security and Communication Networks*, vol. 9, no. 10, pp. 1226–1246, Dec. 2016, doi: 10.1002/sec.1399.

[4] V. K. Quy, V. H. Nam, D. M. Linh, N. T. Ban, and N. D. Han, “A survey of QoS-aware routing protocols for the MANET-WSN convergence scenarios in IoT networks,” *Wireless Personal Communications*, vol. 120, no. 1, pp. 49–62, Apr. 2021, doi: 10.1007/s11277-021-08433-z.

[5] Y. Hussain *et al.*, “Context-aware trust and reputation model for fog-based IoT,” *IEEE Access*, vol. 8, pp. 31622–31632, 2020, doi: 10.1109/ACCESS.2020.2972968.

[6] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, and E. K. Markakis, “A survey on the internet of things (IoT) forensics: challenges, approaches, and open issues,” *IEEE Communications Surveys and Tutorials*, vol. 22, no. 2, pp. 1191–1221, 2020, doi: 10.1109/COMST.2019.2962586.

[7] C. S. Park, “Security architecture for secure multicast CoAP applications,” *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 3441–3452, Apr. 2020, doi: 10.1109/JIOT.2020.2970175.

[8] A. Chopra, “Paradigm shift and challenges in IoT security,” *Journal of Physics: Conference Series*, vol. 1432, no. 1, Jan. 2020, Art. no. 12083, doi: 10.1088/1742-6596/1432/1/012083.

[9] Sangeeta Sangeeta and Er. Arpneek Kaur, “A review on symmetric key cryptography algorithms,” *International Journal of Advanced Research in Computer Science*, vol. 8, no. 4, pp. 358 – 361, 2017, doi: 10.26483/ijarcs.v8i4.3777.

[10] A. Pandya and P. Pandey, “Comparative analysis of encryption technique,” *International Research Journal of Engineering and Technology*, vol. 5, no. 3, pp. 2010–2012, 2018.

[11] M. A. Al-Shabi, “A survey on symmetric and asymmetric cryptography algorithms in information security,” *International Journal of Scientific and Research Publications (IJSRP)*, vol. 9, no. 3, Mar. 2019, Art, no. 8779, doi: 10.29322/ijsrp.9.03.2019.p8779.

[12] M. N. Alenezi, H. K. Alabdulrazzaq, and N. Q. Mohammad, “Symmetric encryption algorithms: review and evaluation study,” *International Journal of Communication Networks and Information Security (IJCNIS)*, vol. 12, no. 2, Aug. 2020, doi: 10.54039/IJCNIS.V12I2.4698.

[13] A. Alwarafy, K. A. Al-Thelaya, M. Abdallah, J. Schneider, and M. Hamdi, “A survey on security and privacy issues in edge-computing-assisted internet of things,” *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4004–4022, Mar. 2021, doi: 10.1109/JIOT.2020.3015432.

[14] S. Deb and B. Bhuyan, “Performance analysis of current lightweight stream ciphers for constrained environments,” *Sadhana - Academy Proceedings in Engineering Sciences*, vol. 45, no. 1, Oct. 2020, doi: 10.1007/s12046-020-01489-w.

[15] S. M., “Analysis and implementation of the ultra-lightweight block cipher: PRESENT,” *Journal of VLSI Design and its Advancement*, Mar. 2020, doi: 10.5281/ZENODO.3706620.

[16] P. Freyre, O. Cuellar, N. Díaz, and A. Alfonso, “Block ciphers with matrices operating alternately over columns and rows,” *Journal of Science and Technology on Information security*, vol. 2, no. 12, pp. 18–29, 2020, doi: 10.54654/ISJ.V2I12.84.

[17] A. A. Pammu, W. G. Ho, N. K. Z. Lwin, K. S. Chong, and B. H. Gwee, “A high throughput and secure authentication-encryption AES-CCM algorithm on asynchronous multicore processor,” *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 4, pp. 1023–1036, Apr. 2019, doi: 10.1109/TIFS.2018.2869344.

[18] G. Hatzivasilis, K. Fysarakis, I. Papaefstathiou, and C. Manifavas, “A review of lightweight block ciphers,” *Journal of Cryptographic Engineering*, vol. 8, no. 2, pp. 141–184, Apr. 2018, doi: 10.1007/s13389-017-0160-y.

[19] V. Mohindru, Y. Singh, and R. Bhatt, “Hybrid cryptography algorithm for securing wireless sensor networks from node clone attack,” *Recent Advances in Electrical & Electronic Engineering (Formerly Recent Patents on Electrical & Electronic Engineering)*, vol. 13, no. 2, pp. 251–259, Apr. 2019, doi: 10.2174/2352096512666190215125026.

[20] T. Cura, “Use of support vector machines with a parallel local search algorithm for data classification and feature selection,” *Expert Systems with Applications*, vol. 145, May 2020, Art. no. 113133, doi: 10.1016/j.eswa.2019.113133.

[21] M. Usman and S. M. Awan, “A data specific comparative study for choosing best cryptographic technique,” *VAWKUM Transactions on Computer Sciences*, vol. 15, no. 1, Mar. 2018, doi: 10.21015/vtcs.v15i1.480.

[22] M. Ahmad and S. Aftab and S. Muhammad and S. Ahmad, “Machine learning techniques for sentiment analysis: a review,” *Int. J. Multidiscip. Sci. Eng*, vol. 8, no. 3, pp. 27–32, 2017.

[23] and J. P. S. R. Singhal, Nidhi, "Comparative analysis of AES and RC4 algorithms for better utilization," *International Journal of Computer Trends and Technology*, vol. 1, no. 3, pp. 177–181, 2011.

[24] M. E. Hameed, M. M. Ibrahim, N. A. Manap, and M. L. Attiah, "Comparative study of several operation modes of AES algorithm for encryption ECG biomedical signal," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 9, no. 6, pp. 4850–4859, Dec. 2019, doi: 10.11591/ijece.v9i6.pp4850-4859.

[25] W. Bhaya, "Review of data preprocessing techniques in data mining," *Journal of Engineering and Applied Sciences*, vol. 12, pp. 4102–4107, 2017, doi: 10.3923/jeasci.2017.4102.4107.

[26] V. Khadse, P. N. Mahalle, and S. V. Biraris, "An empirical comparison of supervised machine learning algorithms for internet of things data," in *Proceedings - 2018 4th International Conference on Computing, Communication Control and Automation, ICCUBEA 2018*, 2018, doi: 10.1109/ICCUBEA.2018.8697476.

[27] V. Bijalwan, V. Kumar, P. Kumari, and J. Pascual, "KNN based machine learning approach for text and document mining," *International Journal of Database Theory and Application*, vol. 7, no. 1, pp. 61–70, Feb. 2014, doi: 10.14257/ijdta.2014.7.1.06.

[28] S. Chaudhary, F. Suthar, and N. K. Joshi, "Comparative study between cryptographic and hybrid techniques for implementation of security in cloud computing," *Performance Management of Integrated Systems and its Applications in Software Engineering*, 2020, pp. 127–135.

[29] U. Gupta, and S. Saluja, and T. Tiwari, "Enhancement of cloud security and removal of anti-patterns using multilevel encryption algorithms," *International Journal of Recent Research Aspects*, vol. 5, no. 1, pp. 55–61, 2018.

[30] S. Sriadhi, R. Rahim, and A. S. Ahmar, "RC4 algorithm visualization for cryptography education," *Journal of Physics: Conference Series*, vol. 1028, no. 1, , Jun. 2018, Art, no. 12057, doi: 10.1088/1742-6596/1028/1/012057.

BIOGRAPHIES OF AUTHORS

Dana Khwailleh is a master degree holder in computer science from Jordan University of Science and Technology, Irbid, Jordan in 8/2020. Now she is working as a Quality Assurance engineer at Nadsoft company. Her research interest is in security over internet of thing and wireless networks. She can be contacted at email: danarkh95@gmail.com.

Firas Albalas is an Associate Professor in the Department of Computer Science, Jordan University of Science and Technology, Irbid, Jordan. He received his PhD in Computer Science from Glamorgan (South Wales) University, Cardiff, UK in 2009. His current research interests include mobile computing, IoT and wireless sensor networks. He can be contacted at email: faalbalas@just.edu.jo.