ISSN 2303-4521
Periodicals of Engineering and Natural Sciences *Original Research*
Vol. 11, No. 3, May 2023, pp.148-154

Exploring the potential of offline cryptography techniques for securing ECG signals in healthcare

Azmi Shawkat Abdulbaqi [1], Hussein Ali Hussein Al Naffakh [2], Sura Abdulmunem Mohammed Al-Juboori [3] , Ahmed Dheyaa Radhi [4], Jamal Fadhil Tawfeq [5], Poh Soon JosephNg [*, 6]

[1]Renewable Energy Research Center, University of Anbar, Ramadi, Iraq
[2] College of Health and Medical Techniques, University of Alkafeel, AlNajaf, Iraq
[3] Ministry of Higher Education and Scientific Research, Baghdad, Iraq
[4] College of Pharmacy, University of Al-Ameed, Karbala PO Box 198, Iraq
[5] Department of Medical Instrumentation Technical Engineering, Medical Technical College, Al-Farahidi University, Baghdad, Iraq
[6] Faculty of Data Science & Information Technology, INTI International University, Persiaran Perdana BBN, 71800 Nilai, Negeri Sembilan, Malaysia

ABSTRACT

In the research, a software for ECG signal based on Chaos encryption based on C#-programmed and Kit o Microsoft Visual Studio Development was implemented. A chaos logic map (ChLMp) and its initial value are utilized to create Level-1 ECG signal based on Chaos encryption bit streams. A ChLMp, an initial value, a ChLMp bifurcation parameter, and two encryption level parameters are utilized to create level-2 ECG signa based on Chaos encryption bit streams. The level-3 ECG signal based on Chaos encryption software utilizes two parameters for the level of encryption, a permutation mechanism, an initial value, a bifurcation parameter of the level of encryption, and a ChLMp. We assess 16-channel ECG signals with great resolution utilizing encryption software. The level-3 ECG signal based on Chaos encryption program has the slowest and most reliable encryption speed. The encryption effect is superior, according to test findings, and when the right decoding parameter is utilized, the ECG signals may be completely recovered. The high resolution 16-channel ECG signals (HRMCECG) won't be recovered if an invalid input parameter occurred, such as a 0.00001% initial poin error, which will result in chaotic encryption bit streams.

Keywords: Chaos Logic Map (ChLMp); High Resolution Multi-Channel ECG Signal (HRMCECG); Chaos-based Encryption; (Chaotic Encryption) ; computer science

Corresponding Author:

Poh Soon JosephNg
Faculty of Data Science and Information Technology, INTI International University
Persiaran Perdana BBN Putra Nilai, 71800 Nilai, Negeri Sembilan, Malaysia
Email: joseph.ng@newinti.edu.my

1. Introduction

A mechanism of chaotic encryption is an interesting research topic. This encryption method is suitable for encrypting audio, images, video, and clinical ECG signals with large block files. Generate various beginning points and chaotic logistics maps utilizing various coding methods. A chaotic sequence is continuous and sensitive to the kind of chaotic logistic map and the beginning point. As contrast to block encryption approaches like Rivest, Shamir, and Adleman (RSA) and the Advanced Encryption Standard (AES) algorithm[1]. It is commonly required to transmit patient records from specialist to specialist across foreign nations. Furthermore, patients are recording their own ECGs and keeping records with portable devices. Afterward, reports of these recordings are typically forwarded to a medical institution for evaluation. Recently, networks have been utilized to transfer electronic medical records from laboratories to hospitals or to specialist offices in an attempt to save costs and enhance services[2]. Consequently, a kind of remote assistance might emerge between worldwide cardiac specialists and nations without specialists, such as poor nations. In each of these cases, the ECG signal must be encrypted to preserve confidentiality[3]. Many patients subscribe to wireless telecardiology applications for rapidly diagnosis of cardiovascular disease (CVD), rescue services of emergency, events based on on-site cardiologist attendance, etc. The patient is connected to portable electrocardiography (ECG) acquisition equipment that transmits ECG packets to his phone via Bluetooth[4]. Wireless telecardiology apps need patients to visit a hospital or surveillance center for fast cardiovascular disease diagnosis. (CVD), emergency rescue services, and events requiring presence of a cardiologist on-site. ECGs transmitted in plain text, as shown in Figure 1, can compromise the patient's privacy and be spoofable[5][6]. A patient's ECG signal contains sensitive cardiovascular information. Hence, If these ECG segments are not encrypted get mishandled and endanger the sensitive health information about the patient, it would violate HIPAA. Insurance companies, in particular, may profit from the disclosure of this private health information. Fraudsters can exploit the recorded ECG segment to gain unauthorized access to sensitive areas, such as medical services since ECG is utilized for biometric identification. To protect patients' privacy and prevent potential spoof attacks, ECG segments must be encrypted (as are medical photos). The wavelet-based [6] approach, the noised smearing technique, and the permutation cipher were previously utilized. Even though all of these approaches are computationally expensive, they are still suitable for the embedded systems and mobile devices with limited capacity of the computational[7]. This paper builds a chaotic multi-scroll ECG encryption system. For many different cryptographic keys, a chaos system may generate an extremely lengthy random sequence. It will be feasible to create a pseudo-one-time pad method as a result. The chaos cryptographic session key has been distributed via the Diffie–Hellman key exchange protocol[8][9]. The suggested encryption for ECG effectively hides the identity of the patient utilizing 12 publicly accessible ECG segments utilizing spectrum analysis. Furthermore, HIPAA law is protected by upholding patients' sensitive health information[10].

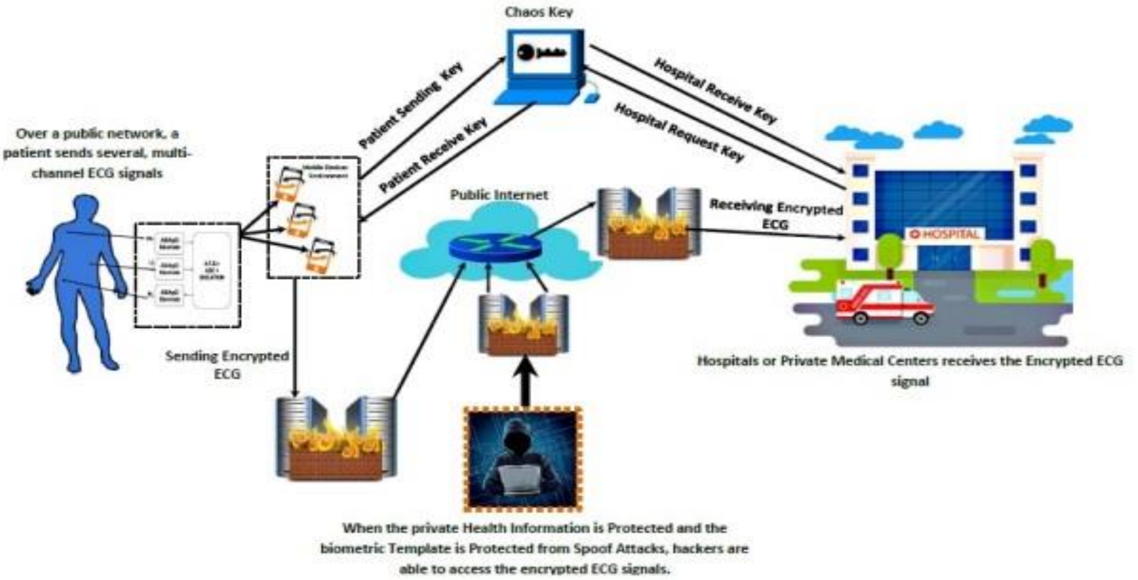

Chaos Key
Patient Sending Key
Patient Receive Key
Hospital Receive Key
Hospital Request Key
Over a public network, a patient sends several, multi-channel ECG signals
Public Internet
Receiving Encrypted ECG
HOSPITAL
Sending Encrypted ECG
Hospitals or Private Medical Centers receives the Encrypted ECG signal
When the private Health Information is Protected and the biometric Template is Protected from Spoof Attacks, hackers are able to access the encrypted ECG signals.

Figure 1. Architecture of suggested ECG based on Chaos encryption system

2. Related literature review

Secure communications offer a wide range of utilizes that many researchers have developed and suggested. Basically, the writers who employ synchronization and the authors who do not may be loosely split into two groups in terms of how they approach this significant issue in writing. The process of two (or more) chaotic systems coming together to exhibit a shared dynamical behavior after a transient duration is known as synchronization of chaos, as suggested by the name. Here, the common behavior might be a simple phase locking or a full coincidence of the chaotic trajectories. Numerous ideas of synchronization for chaotic systems have been put out from the work of Kolumban et al. [11], the most effective and frequent is identically synchronized when the state of the transmitter and the receiving system asymptotically converge [12]. Two less reliable synchronization ideas, generalized synchronization [13], and synchronization of the phase [14], have also been introduced more recently. Signal recovery is highly challenging since the chaotic synchronization methods that have been reported so far are very sensitive to channel distortion and noise. Because synchronization is so sensitive to noise, several writers have experimented with a variety of strategies that do not need synchronization. Chaos shift keying (CSK) is the first of this kind [15]. A kind of digital modulation is CSK. Depending on message symbol's current value, one of the N chaos generators with a variety of properties, signal xi(t), I = 1, N), is transmitted. The CSK's primary flaw is that the decision circuit's necessary threshold level is dependent on the signal-to-noise ratio (SNR). The chaotic on-off keying (COOK) is a specific instance of CSK [16]. One chaotic oscillator, utilized by COOK, is turned on/ off according on the binary message's transmission symbol. The primary flaw of the CSK system, which is that the threshold value of the decision circuit depends on the amount of noise, also exists in COOK.. The maximum distance between the signal set's components can be achieved via COOK, however the decision circuit's necessary level of threshold depends on the SNR (Signal on Noise Ratio). Nevertheless, by utilizing the differential CSK, the threshold value may be maintained while the distance is doubled (DCSK).

In DCSK, time division creates the two channels. The modulated reference carrying the message symbol is transmitted after the reference signal for every message symbol. Every bit of information is transmitted via functions of the two sample due to the bit rate being halved, which is the main disadvantage of DCSK. To address this issue, authors [17] suggested frequency modulation DCSK (FM-DCSK) in the literature. This system's peculiarity is that it maintains a consistent amount of transmitted energy for per bit that belongs to a single symbol. The sole difference between DCSK and FM modulator is that the DCSK modulator's input is an FM modulated signal rather than a chaotic one. In the FM-DCSK standard system, just one information bearing is sent after the reference signal, which is a drawback[18]. The quadratic chaos shift keying (QCSK) scheme is one of the most effective ones among the many techniques that have been suggested in the literature to boost the data rate of DCSK. The QCSK scheme's fundamental premise is the chaotic signals generation that are orthogonal over a predetermined time period. As a result, it is arbitrary to build any kind of chaotic signal constellation from a base of chaotic functions. For instance, the QCSK encoding of four symbols utilizes two chaotic basis functions in a linear fashion[19]. The essential need for utilizing this concept in a communication system is the ability of the chaotic basis functions generation beginning with a single chaotic signal. The same idea applies to common digital communication protocols like QPSK, where a conventional phase shifter may be utilized to extract the quadrature component from phase one. Its high level of complexity is this method's principal drawback[20].

3. Data collection (dataset)

Utilizing a select few entries from the Normal Sinus Rhythm Database (NSRDB), we validated our suggested model of ECG-based person identification. Every submission included four ECG segments that were randomly selected for utilize in our experimentations. At a rate of 128 Hz, the obtained ECG signals were sampled. The duration of every ECG segment was 5 s, which translates to 5 × 128 or 640 samples per segment. The resolution of the ECG was 10 bits. As a result, every ECG segment resembled like a vector with 640 elements and a accuracy of around three digits after the decimal[21][22].

4. Chaotic encryption mechanisms

Utilizing a limited sample of data from the Normal Sinus Rhythm Database, our suggested person identification model of ECG-based was validated (NSRDB). For our experimentations, from each entry, four ECG segments were chosen randomly [23]. The ECG signals that were recorded were sampled at a rate of 128 Hz. The length of each ECG segment was 5s, which translates 5 128 or 640 samples in a single segment. The ECG resolution had an 10 bits. Each ECG segment thus resembled a vector with 640 elements and about 3-digit accuracy after the decimal [24].

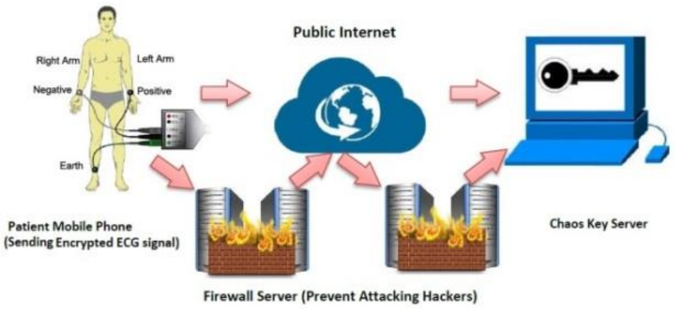


Figure 2. Chaos server and the mobile for the patient with the 3-step key exchange utilization

5. System description of encryption /decryption

Figure 1, illustrates the EDS's overall organization. The generator unit of ECG signal, unit of encryption , and unit of decryption make up the device.

5.1. ECG Generator unit

A MICROCHIP 16F84A microcontroller (MC) serves as the foundation of the generator. The following is how the ECG is generated: ECG period that was sampled at 255 Hz and digitalized at 8 bits is preserved in the MC's Flash memory[25]. The DAC0808 digital-to-analog converter receives this data from the MC repeatedly at a rate of 255 Hz, and our system utilizes its output after passing it through a voltage divider across resistor R6 to increase the produced signal voltage level to 3 mV peak-to-peak. The circuitry representation is shown in Figure 2[26].

5.2. Encrypting unit

As its primary two sub-units, this unit is structured around the generator of the chaotic and the multiplexing and encryption subunit[27].

5.3. Generator of the chaotic

A Colpitts oscillator serves as the chaotic generator. The LC circuit is positioned at the NPN bipolar junction's collector transistor and consists of a voltage divider with components of dual capacitors (capacitor(C1) and capacitor(C2) coupled to output transistor of a bipolar junction (BJT). The BJT Q2N2222 is the circuit's nonlinear component in this oscillator[28]. Figure 3 shows a representation of the circuit we utilized. Any of the two capacitors' voltages displays erratic behavior. The ECG in the EDS is encrypted utilizing this signal[29].

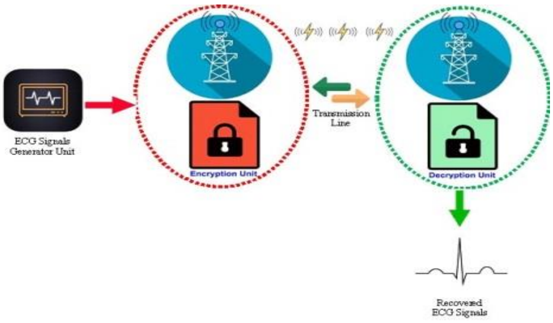


Figure 3. General organization of the EDS

A Colpitts oscillator serves as the chaotic generator. The LC circuit is positioned at the NPN bipolar junction's collector transistor and consists of a voltage divider with components of dual capacitors (capacitor(C1) and capacitor(C2) coupled to output transistor of a bipolar junction (BJT). The BJT Q2N2222 is the circuit's nonlinear component in this oscillator [28]. Figure 3 shows a representation of the circuit we utilized. Any of the two capacitors' voltages displays erratic behavior. The ECG in the EDS is encrypted utilizing this signal [29].

5.4. Unit of decrypting

The signal to this device is entered into a One-to-Two DE-Multiplexer (DMX), which gets the encrypted ECG. The substractor receives the two DMX outputs, which then transfers its output to a Low_Pass_Filter for hidden ECG signal retrieving [30][31].

5.5. Software application and performance testing

Figure HRMCECGs prior to encryption, which was observed utilizing ECG software for enabling medical observation of heartrate developed by the Nicolet Company. This encryption software can be applied utilizing the following steps [32]:

First, load the HRMCECGs into the "Chaos Encryption2" software for testing chaotic encryption and decryption.

Second: Enter the location and file name of the encrypted file and save them.

Third: Choose on the encryption level and set the rl, r2, xl, x2, nf, and df encryption parameters. Within the following ranges, actual values may be utilized to fill in the encryption parameters: rl, r2: 3.6 to 4.0. xl, x2, df: zero to one, nf: ten thousand to ten million. The following is a list of the proper encryption settings for this experiment: the degree of encryption Level-3: nf=10000; df=0.2; rl=3.965; xl=0.321; r2=3.811; x2=0.124.
Fourth: The encryption process takes 127 seconds; just click the ENC button to begin. Step 5: As indicated in Fig. 4, utilize ECG software to see the encrypted HRMCECG heartrate.
Sixth: Upload the encrypted ECG signals to the software "Chaos Encryption2. 0" for chaotic encryption and decryption.
Seven: Set the location and file name of the decrypted file and save them.
Eight: Enter the decryption parameters rl, r2, xl, x2, nf, and df after choosing the appropriate degree of decryption.
Nine: Utilize the ECG software to see the HRMCECGs that have been properly encrypted.
Ten: With the proper decryption parameters r2, xl, x2, nf, and df entered and the incorrect decryption parameter r1 with a 0.00001% starting mistake, choose the right degree of decryption.
Eleven: Check the incorrectly decrypted HRMCECGs with the ECG software. The testing HRMCECGs had data sizes of 28.538 Kbytes, 14.493 Kbytes, and 17.277 Kbytes, respectively, and their heartrates were timed at 42 min 42 s, 13 min 18 s, and 11 min 11 s, respectively. The encryption process employed level-3 encryption, taking 127, 97, and 103 seconds, respectively [33].

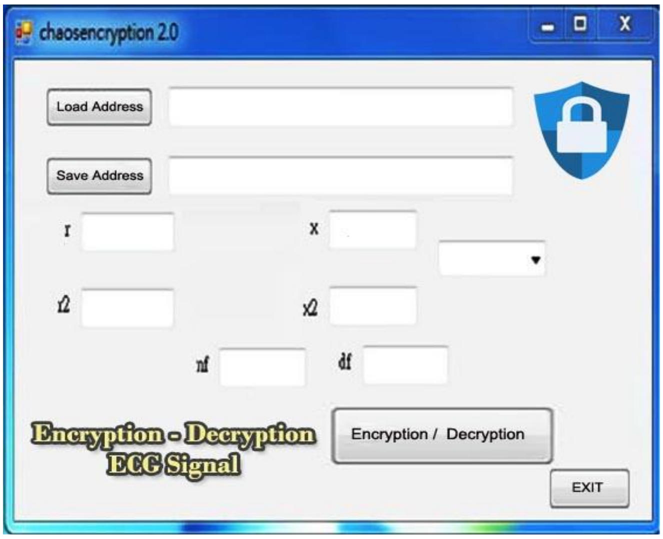
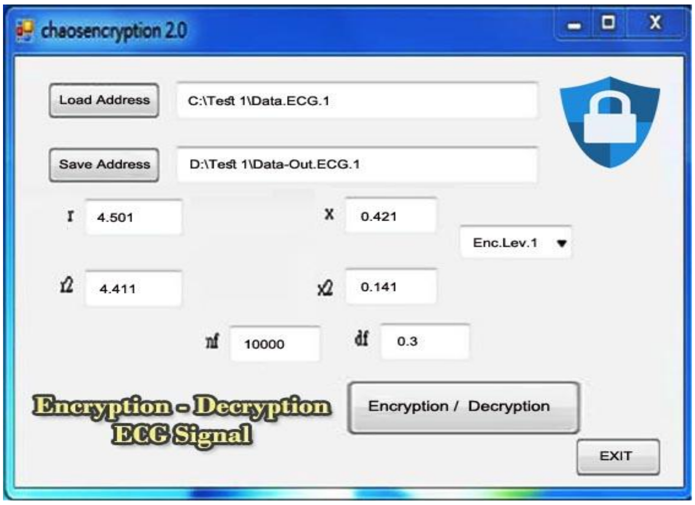


Figure 4. The offline ECG was suggested based on Chaos encryption software



Load Address C:\Test 1\Data.ECG.1

Save Address D:\Test 1\Data-Out.ECG.1

r 4.501
x 0.421
Enc.Lev.1
r2 4.411
x2 0.141
nf 10000
df 0.3

Figure 5. shows a working window of the offline ECG based on Chaos encryption software

5.6. Difference in percentage-root mean (PRD)

The Percentage Root means difference specifies the fidelity by wise comparison with the raw data. In spite of their extensive utilization, the accurate quality of signal reconstructions is not shown by PRD, and the evaluation via visual examination has to be executed onto the decompressed signals. PRD is signified as[34]:

$$\mathrm{PRD} = \sqrt{\frac{\sum_{n=1}^{N}(x(n)-x\prime(n))^2}{\sum_{n=1}^{N} x^2(n)}}\, x\, 100 \qquad (1)$$

where x(n) and x'(n) x n equates the original and reconstructed the values of the sample accordingly, and N is the size of the window utilized to determine the PRD. The PRD low value signifies a preferably less error among the original signal and signal reconstructed. The below table 4.3, illustrates the PRD measurement of the ECG signal rec. 134 taken from MIT-BIH Arrhythmia dataset[35].

5.7. Quality Score (QS)

QS is the CR-ration and PRD which quantifies the performance overall of the Encryption/Decryption technique. A high quality score denotes great performance with little mistake. QS is defined as follows[36]:

$$\mathrm{QS} = \frac{\mathrm{CR}}{\mathrm{PRD}} \qquad (2)$$

6. Conclusion

Based on the results of our previous studies on chaotic encryption, we developed offline chaos-based HRMCECG heartrate encryption and decryption software utilizing C# programming and the development kit of Microsoft Visual Studio. Additionally, a recommendations and advice regarding its application and encryption and decryption performance was also provided. The results of tests on the actual files indicate that the offline chaos-based HRMCECG heartrate encryption and decryption software developed in this study performs outstandingly. In future studies, we will devote greater effort to developing more robust ECG signal based on Chaos encryption software and a simpler interface for encryption parameter input.

Declaration of competing interest

The authors declare that they have no known financial or non-financial competing interests in any material discussed in this paper.

Funding information

No funding was received from any financial organization to conduct this research.

References

[1] I. Al-Barazanchi et al., “Remote Monitoring of COVID-19 Patients Using Multisensor Body Area Network Innovative System,” Comput. Intell. Neurosci., vol. 2022, pp. 1–14, Sep. 2022, doi: 10.1155/2022/9879259.

[2] G. Nguyen et al., “Machine Learning and Deep Learning frameworks and libraries for large-scale data mining: a survey,” Artif. Intell. Rev., vol. 52, no. 1, pp. 77–124, 2019, doi: 10.1007/s10462-018-09679-z.

[3] C. Shorten and T. M. Khoshgoftaar, “A survey on Image Data Augmentation for Deep Learning,” J. Big Data, vol. 6, no. 1, 2019, doi: 10.1186/s40537-019-0197-0.

[4] R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, A. Al-Nemrat, and S. Venkatraman, “Deep Learning Approach for Intelligent Intrusion Detection System,” IEEE Access, vol. 7, pp. 41525–41550, 2019, doi: 10.1109/ACCESS.2019.2895334.

[5] K. Sivaraman, R. M. V. Krishnan, B. Sundarraj, and S. Sri Gowthem, “Network failure detection and diagnosis by analyzing syslog and SNS data: Applying big data analysis to network operations,” Int. J. Innov. Technol. Explor. Eng., vol. 8, no. 9 Special Issue 3, pp. 883–887, 2019, doi: 10.35940/ijitee.I3187.0789S319.

[6] A. D. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, “A decentralized privacy-preserving healthcare blockchain for IoT,” Sensors (Switzerland), vol. 19, no. 2, pp. 1–17, 2019, doi: 10.3390/s19020326.

[7] F. Al-Turjman, H. Zahmatkesh, and L. Mostarda, “Quantifying uncertainty in internet of medical things and big-data services using intelligence and deep learning,” IEEE Access, vol. 7, pp. 115749–115759, 2019, doi: 10.1109/ACCESS.2019.2931637.

[8] S. Kumar and M. Singh, “Big data analytics for healthcare industry: Impact, applications, and tools,” Big Data Min. Anal., vol. 2, no. 1, pp. 48–57, 2019, doi: 10.26599/BDMA.2018.9020031.

[9] L. M. Ang, K. P. Seng, G. K. Ijemaru, and A. M. Zungeru, “Deployment of IoV for Smart Cities: Applications, Architecture, and Challenges,” IEEE Access, vol. 7, pp. 6473–6492, 2019, doi: 10.1109/ACCESS.2018.2887076.

[10] B. P. L. Lau et al., “A survey of data fusion in smart city applications,” Inf. Fusion, vol. 52, no. January, pp. 357–374, 2019, doi: 10.1016/j.inffus.2019.05.004.

[11] Y. Wu et al., “Large scale incremental learning,” Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit., vol. 2019-June, pp. 374–382, 2019, doi: 10.1109/CVPR.2019.00046.

[12] A. Mosavi, S. Shamshirband, E. Salwana, K. wing Chau, and J. H. M. Tah, “Prediction of multi-inputs bubble column reactor using a novel hybrid model of computational fluid dynamics and machine learning,” Eng. Appl. Comput. Fluid Mech., vol. 13, no. 1, pp. 482–492, 2019, doi: 10.1080/19942060.2019.1613448.

[13] V. Palanisamy and R. Thirunavukarasu, “Implications of big data analytics in developing healthcare frameworks – A review,” J. King Saud Univ. - Comput. Inf. Sci., vol. 31, no. 4, pp. 415–425, 2019, doi: 10.1016/j.jksuci.2017.12.007.

[14] J. Sadowski, “When data is capital: Datafication, accumulation, and extraction,” Big Data Soc., vol. 6, no. 1, pp. 1–12, 2019, doi: 10.1177/2053951718820549.

[15] J. R. Saura, B. R. Herraez, and A. Reyes-Menendez, “Comparing a traditional approach for financial brand communication analysis with a big data analytics technique,” IEEE Access, vol. 7, pp. 37100–37108, 2019, doi: 10.1109/ACCESS.2019.2905301.

[16] D. Nallaperuma et al., “Online Incremental Machine Learning Platform for Big Data-Driven Smart Traffic Management,” IEEE Trans. Intell. Transp. Syst., vol. 20, no. 12, pp. 4679–4690, 2019, doi: 10.1109/TITS.2019.2924883.

[17] S. Schulz, M. Becker, M. R. Groseclose, S. Schadt, and C. Hopf, “Advanced MALDI mass spectrometry imaging in pharmaceutical research and drug development,” Curr. Opin. Biotechnol., vol. 55, pp. 51–59, 2019, doi: 10.1016/j.copbio.2018.08.003.

[18] C. Shang and F. You, “Data Analytics and Machine Learning for Smart Process Manufacturing: Recent Advances and Perspectives in the Big Data Era,” Engineering, vol. 5, no. 6, pp. 1010–1016, 2019, doi: 10.1016/j.eng.2019.01.019.

[19] Y. Yu, M. Li, L. Liu, Y. Li, and J. Wang, “Clinical big data and deep learning: Applications, challenges, and future outlooks,” Big Data Min. Anal., vol. 2, no. 4, pp. 288–305, 2019, doi: 10.26599/BDMA.2019.9020007.

[20] M. Huang, W. Liu, T. Wang, H. Song, X. Li, and A.Liu,"A queuing delay utilization scheme for on-path service aggregation in services-oriented computing networks," IEEE Access , vol .7 , pp .23816-23833 ,2019 ,doi :10 .1109/ACCESS .2019 .2899402.

[21]G.Xu,Y.Shi,X.Sun,andW.Shen,"Internetofthingsinmarineenvironmentmonitoring:A review," Sensors (Switzerland), vol .19 ,no .7 ,pp .1-21 ,2019 ,doi :10 .3390/s19071711

[22] M. Aqib, R. Mehmood, A. Alzahrani, I. Katib, A. Albeshri, and S. M. Altowaijri, "Smarter traffic prediction using big data, in-memory computing, deep learning and gpus," vol. 19, no. 9, 2019. DOI: 10.1109/MIS.2019.2947728.

[23] S. Leonelli and N. Tempini, "Data Journeys in the Sciences," 2020. DOI: 10.7551/mitpr