Journal of Intelligent Systems and Internet of Things (JISIoT)
Vol. 11, No. 01, PP. 21-28, 2024
DOI: https://doi.org/10.54216/JISIoT.110103

Security and Privacy Protection for Online Electronic Documents Based on Novel Encryption Techniques

Amer Ibrahim[1], Ravi Sekhar[2]*, Jamal Fadhil Tawfeq[3], Sinan Q. Salih[4]*, Pritesh Shah[2], Ahmed Dheyaa Radhi[5]

[1]College of Computer and Information Technology, American University in the Emirates, Dubai, United Arab Emirates, [2]Symbiosis Institute of Technology (SIT) Pune Campus, Symbiosis International (Deemed University) (SIU), Pune, 412115, Maharashtra, India, [3]Department of Medical Instrumentation Technical Engineering, Medical Technical College, Al-Farahidi University, Baghdad, Iraq, [4]Department of Medical Instrumentation, Technical College of Engineering, Al-Bayan University, Baghdad, Iraq, [5]College of Pharmacy, University of Al-Ameed, Karbala PO Box 198, Iraq
Email: amer.ibrahim@aue.ae; ravi.sekhar@sitpune.edu.in; pritesh.shah@sitpune.edu.in; jamaltawfeq55@gmail.com; Sinan.salih@albayan.edu.iq; ahmosawi@alameed.edu.iq

Abstract

Corporate strategies have employed techniques that enter the domain of shadow and espionage in this rapidly developing, technologically competitive business environment. Supporting a security strategy is a way to counter these possible dangers. To preserve corporate success in the marketplace, network security needs to be crucial to the protection of electronic documents. Encryption technology has become more important in recent years for protecting online digital documents. This research was motivated by the fact that document verification has become quite time-consuming and difficult due to a variety of challenging and laborious processes. Existing technologies often malfunction when a single kind of encryption, such as AES, Data Encryption Standard (DES), or Rivest, Shamir, Adleman (RSA), is utilized at the request of the customer. Therefore, this study proposes hybrid cryptography, which integrates two novel algorithms into existing encryption protocols. A digital signature is generated for the data when a user uploads a data. The data are encrypted in parallel using the suggested Secured Hash Function-256 (SHA-256) method with improved DES and RSA (SHA-256+Enhanced DES+RSA). The proposed encryption method was shown to be more accurate than previous studies in experimental evaluations of data encryption.

Received: July 20, 2023 Revised: November 20, 2023 Accepted: December 02, 2023

Keywords: Online Electronic Document; Digital Signatures; Encryption, and SHA-256 with Enhanced DES and RSA algorithm (SHA-256+Enhanced DES+RSA)

1. Introduction

All tiers of government in our nation use documents as a working tool and offer crucial job material. Transmission efficiency will be impacted by speed limits and distance when the primary form of conventional document interchange is the manual service and mail technique. Traditional methods of transmitting documents have their own drawbacks, however, including slower speeds, more susceptibility to leaks and losses, and higher costs [1]. The proliferation of computer technology and the establishment of a national e-government led to the elimination of the use of paper documents in an increasing number of government agencies [2]. In an e-government context, electronic documents (ED) overcome paper's drawbacks by having a fast retrieval, compact storage, long-distance distribution, and multi-user sharing [3]. This has changed the "Document travel" phenomena of conventional document processing, broken time and space limits in material transmission, and resulted in prompt, electricized document delivery, considerably improving business efficiency. However, the intergovernmental transmission of ED must contend with

new vulnerabilities and new methods of attack. These include concerns regarding the security of the documents, the transfer and detection of ED across computer viruses, and various industries. These problems are associated with the implementation and spread of ED in China. Since the internet is a publicly accessible network, anybody, anywhere, and using any method may establish a connection to it [4]. This presents a difficulty for the security of ED since anybody can access to the Internet. The most common threats to the safety of electronic document delivery include unauthorized access to the data, tampering with the data, impersonation, the introduction of viruses, and so on. For instance, the incidence of infection with computer viruses in China reached 91 percentage in 2007, and 85.5% in 2008, according to a study on the technical analysis of the 2008 computer virus situation investigation [5]. New computer viruses in 2008 were 49% higher than in 2007, according to a study on computer viruses and Internet security in China. The internet is the significant cause for spreading the virus; if the virus in the ED system is not quickly identified, it will cause the system to become dysfunctional, potentially leading to the loss of vital records or significant delays in their transmission, and ultimately rendering the entire electronic government system useless [6]. Hence, we should encourage the use of ED, support security research, and enhance the distribution of electronic papers in a secure manner. This study suggested using Secured Hash Function-256 (SHA-256)+DSA to encrypt online ED to increase the EDs security. The study is structured in such a manner that Part 2 provides literature review, Part 3 outlines the recommended approach, Part 4 depicts findings and discussion, and Part 5 draws a conclusion to the research.

2. Literature Review

An "Improved Identity-Based Encryption" technique is suggested, which may efficiently easier the process of key generation, minimize the network traffic, and enhance the WSN security by considering its unique features and building on the notion of identity-based encryption (IBE) [7]. For this study [8], researchers looked at the safety features of four distinct encryption systems. The author presented the study and use of a single homomorphic encryption method in a cloud setting and based his comparison of the effectiveness of four such algorithms on experimental data. The study [9] offers a novel cryptographic approach to ensuring the safety of digital audio. Inspired by classic symmetric models, this encryption scheme relies on a chaotic circle map and revised rotation equations to produce truly random data. Using asymmetric scalar-product-preserving encryptions and Hadamard product operations, article [10] offers a "Searchable Encryption that enables Privacy-Preserving Fuzzy Multi keyword search" on cloud-based infrastructures. The author uses the machine learning primitive "Word2vec" to get a fuzzy correlation score for encrypted data and query predicates, allowing us to implement the usefulness of fuzzy searches. The performance is broken down and analyzed in several different ways, including multi keyword token analysis, file retrieval and matching accuracy analysis, and so on.

The article [11] analyzes the efficiency of the SIMON cryptographic algorithm and suggests a lightweight-cryptography method based on SIMON for usage in an IoT-driven environment. While most previous research has focused on hardware implementations, this one takes a software perspective to performance optimization. The contribution investigates the features of the SIMON cypher with an eye on using it in IoT health-care systems for improved performance. The study [12] suggests a method of encrypting digital images inside ED. The primary notion is that by adding digital watermarks to the images in this document, the authorship of the electronic document may be safeguarded. The paper considers three cases utilizing the suggested methodology: Complete copies of ED, copies of images within the document, and copies of text. It is shown that authorship confirmation can be effectively done in all three scenarios. The study [13] suggests a safe electronic health record program based on essential element crypto algorithm and smart contract innovation to ensure privacy, verification, authenticity of medical information, and allow fine-grained security controls. In this system, we secure data using attribute-based encryption and IBE, and we implement digital signatures using identity-based signatures. The article [14] introduces a new approach to dual watermarking by combining the "Discrete Wavelet Transform (DWT)," "Singular Value Decomposition (SVD)," and "Set Partitioning In Hierarchical Tree" structure. The approach employs a second-level DWT to decompose the host image into a variety of frequency components. Then, we apply the SVD transformation to the selected wavelet subcomponent. Both the logo watermark and the signature watermark are encrypted using Arnold transform and hamming code, respectively, before embedding. As a last step, we use an embedding technique to include both encoded watermarks into the host image after its transformation [15-23].

3. Proposed Methodology

This section discusses in detail about the security and privacy protection for online ED. Figure 1 depicts the flow of the proposed methodology. When a sender "A" uploads a document digitally, digital signature is generated for the document using SHA-256 integrated digital signature algorithm. In parallel, data are encrypted by the

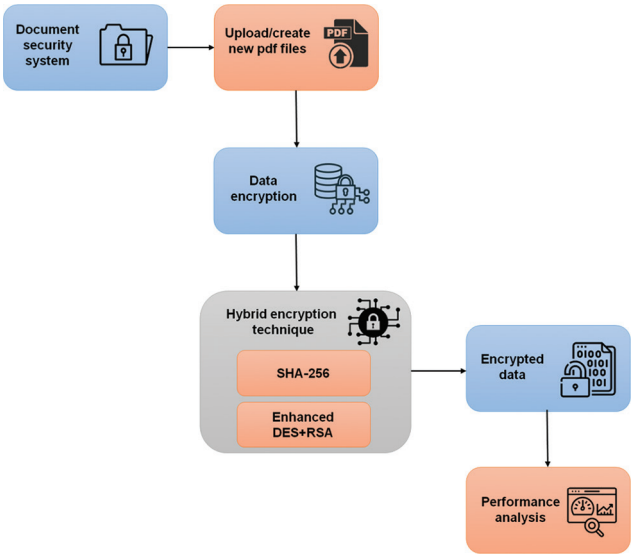

Figure 1: Flow of the proposed methodology.

proposed hybrid encryption technique Enhanced Data Encryption Standard (DES) + Rivest, Shamir, Adleman (RSA) algorithm.

3.1. E-document encryption using SHA-256 with enhanced DES and RSA algorithm

To secure the context of E-document, we employed SHA-256+Enhanced DES+RSA for E-document encryption. The E-document is double encrypted by this approach. In the first stage, E-document is encrypted by SHA-256 encryption algorithm. In the second stage, encrypted E-document is again encrypted by enhanced DES+RSA algorithm.

3.1.1. SHA-256 encryption algorithm

A one-way hash function, SHA-256 takes a string of arbitrary length and returns a string of the same length. It is a part of the SHA-2 family and is one of six different functions that make up SHA-2. To provide more effective encryption, it produces keys with a greater key space and sensitivity. It utilizes a modified SHA-0 hash algorithm. To create the initial secret key for protecting online ED, SHA-256 has been employed. A text string of 360 characters is given as input to the SHA-256 algorithm, which converts it into a secret key of 256 characters. SHA-256 is used to create three distinct chaotic sequences, one for each of the input image's three color components (Red, Green, and Blue).

3.1.2. DES

After more than three decades of service, the DES, commonly known as the Data Encryption Algorithm, is still widely used. The DES is the best-known symmetric cryptosystem. The DES encrypts and decrypts using the same algorithm. It uses a 56-bit key to encrypt a 64-bit data block.

- It creates cypher text (P) by encrypting plain text (C) with key (l1), where P = Il1 (C)
- Plain text (C) is created by decrypting encrypted text (P) using key (l1), where C = Dk1 (C)

Plaintext is first encrypted using one key, then again using a different key, and finally using a third key in triple DES.

$$P = I_{l3}\left(I_{l2}(I_{l1}(P))\right) \quad (1)$$

$$C = J_{l3}\left(J_{l2}(J_{l1}(C))\right) \quad (2)$$

The key length of 3DES is 168 bits, which is 3 times as large as the key length of DES, which is 56 bits. As a result, the complexity of the key has grown by a factor of 2^{112}. The key length that is used is 112 bits, although this is primarily because of the risk of an attack known as a meet-in-the-middle attack: If the adversary is in possession of both the plain text and the cypher, then he is in a position to attack the encryption on both ends. The plain text represents all the potential encryption keys (256 possibilities). The encrypted documents that are produced by this process also include all potential keys for each level 2 encryption (2^{112} possibilities). Their findings are contrasted with those obtained when the encrypted text was decrypted using each key individually (2^{56} possibilities). Therefore,

in all, just $2^{112} + 2^{56}$ encrypting and decryption operations are carried out, but the brute force approach requires 2^{168} of each operation.

3.1.3. RSA approach

RSA has crucial characteristics that affect its speed and security. When the modulus is made longer, it becomes more difficult to break down into its component parts. It will be more challenging to decrypt without knowing the private key because of the increased length. Changes to the message length have a corresponding effect on the length of encrypted messages in a digital document. Therefore, greater size chunks are chosen to strengthen the security of the data in use, allowing for the encipherment of a larger message. The time-dependent performance of the RSA method was examined by adjusting such values. The values of I, j, and q may be calculated in the subsequent stages.

- Select the prime integers c and n that are both extremely huge (100+digits).
- Set q=c*n.
- Select an enormous integer I such that

GCD (i, (i, (c–1))*(n–1))=1

- Find j such that i*j mod ((c–1)*(n–1))=1

In cryptography, the "public key" refers to a certain numeric (q, i). In spite of the fact that these numbers are available to the public, computing j from q is computationally impossible for sufficiently big values of p and q. After obtaining the public key, R uses it to generate the cypher P, which is then used to encrypt the message.

$$P = Me\ mood\ q\ i: Public\ key \tag{3}$$

The encryption is then deciphered by the recipient using the private key and the following equation:

$$R = Pj\ mod\ q\ j: Private\ Key \tag{4}$$

Now, this might look a little complicated, and the math does require a lot of computational power because the numbers are so big. Both c and n could have more than 100 decimal digits, j and i will be about the same size, and n could have more than 200 digits. Still, a simple example might be helpful. In this instance, the values of c, n, I, and j are chosen

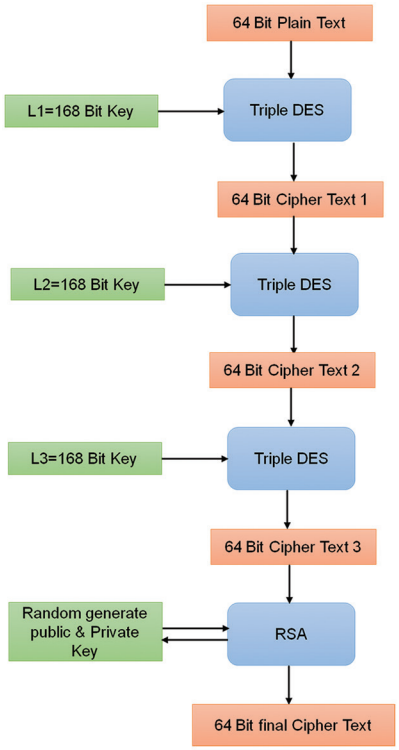

Figure 2: Encryption process.

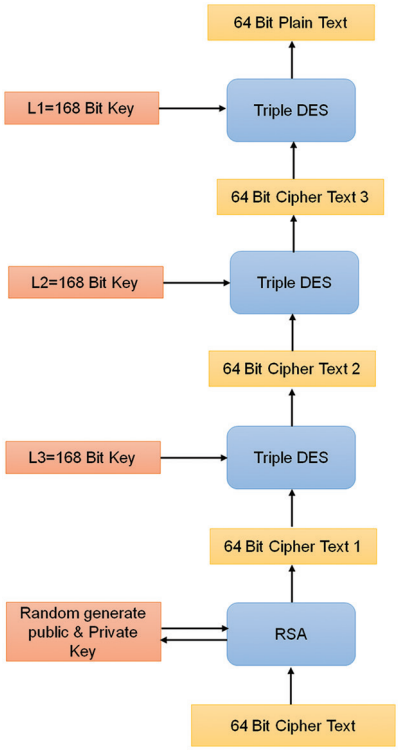

Figure 3: Decryption process.

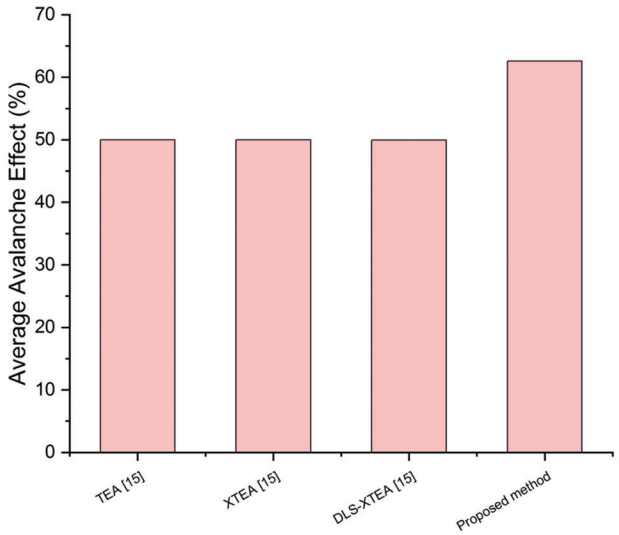

Figure 4: Average avalanche effect.

to be very small on purpose so that the reader can see how badly these values work, but hopefully, the algorithm will be shown well enough.

3.1.4. Enhanced DES and RSA algorithm

To further strengthen DES's protections, we have implemented a novel method. As such, we have decided to employ a Three-Time DES with RSA Algorithm. The key length is 504 bits. The keys are being used autonomously. Public and private key pairs are generated at random in the RSA algorithm. Figures 2 and 3 show the encryption and decryption procedure.

$$Triple\ DES = \ 3J^{I} = I_{l3}\left(I_{l2}\left(I_{l1}\left(P\right)\right)\right); P = (3J^{I}{}_{L3}\left(3J^{I}{}_{L2}\left(3J^{I}{}_{Li}\left(C\right)\right)\right) \quad (5)$$

$$C = \left(3J^{J}{}_{L3}\left(3J^{J}{}_{L2}\left(3J^{J}{}_{Li}P\right)\right)\right) \quad (6)$$

4. Results and Discussion

This section discusses in detail about the findings of the security and privacy protection for online ED. The parameters are average avalanche effect, execution time, resource consumption, and energy consumption (EC). The existing methods utilized in this research to evaluate the performance of the proposed method are Tiny Encryption Algorithm (TEA), eXtended Tiny Encryption Algorithm (XTEA), Dynamic Light-weight Symmetric XTEA (DLS-XTEA). The Avalanche effect may be used to assess the efficiency of proposed and traditional algorithms in ensuring the security of online electronic data. Based on the approach's resistance to threats and real-time attacks during data transfer, it is calculated. The ratio of modified bits to the sum of bits in the cypher text is called as the avalanche effect in encryption techniques. Figure 4 depicts Avalanche effect comparison. Compared to conventional methods, the proposed method exhibits more significance.

When estimating the execution time of a task, run-time or system actions that the system does on its behalf are also taken into consideration. Figure 5 depicts the execution time comparison. Compared to conventional methods, the proposed method has a lower execution time to execute its task.

The term "memory consumption (MC)" refers to the total amount of memory that an application uses while running Figure 6 shows MC comparison (RAM and code size) during the encryption process. Figure clearly shows that the proposed method has a low MC when compared to other methods.

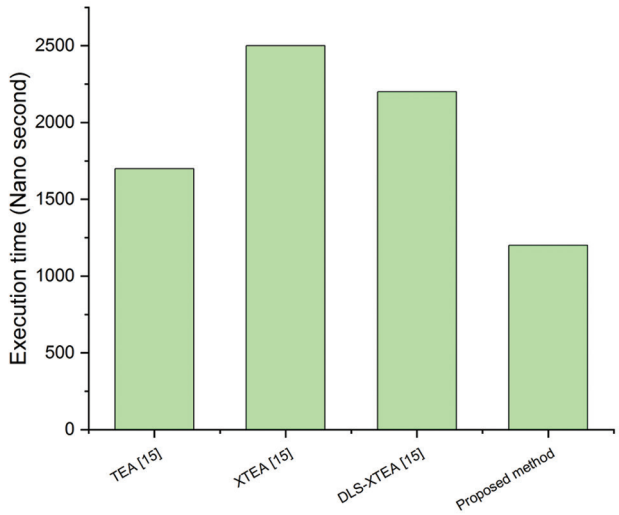

Figure 5: Execution time.

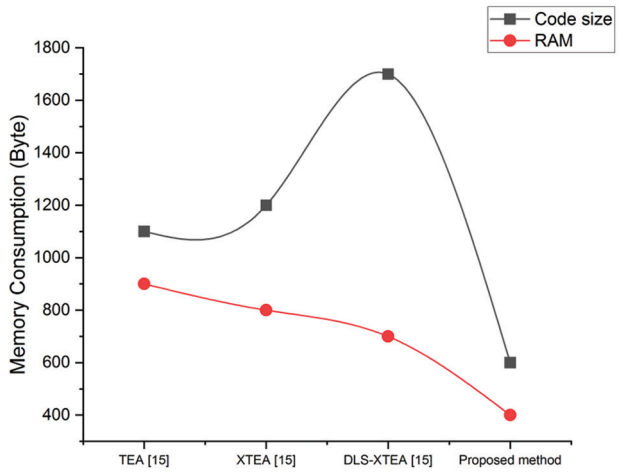

Figure 6: Memory consumption.

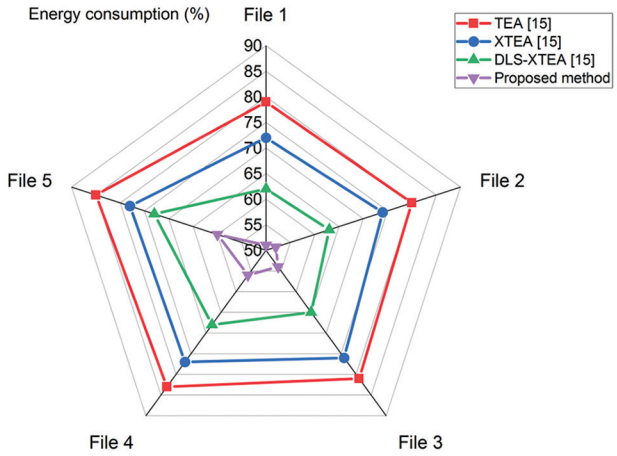

Figure 7: Energy consumption.

The amount of energy that must be used to encrypt data is referred to as the EC. Figure 7 depicts EC comparison. Figure clearly shows that the proposed method has a low EC when compared to other methods.

5. Conclusion

As a result of the rapid expansion of network and Internet applications, there is an increasing need to tighten security measures across these platforms. Therefore, the significance and value of the online electronic document data exchanged through the internet and other media are growing. Data security for sensitive information and multimedia is becoming more crucial. Encryption is a key technique for safe electronic data transfer across open networks. For safe electronic data transfer, we suggested a SHA-256+Enhanced DES+RSA encryption technique in this study. The performance of the suggested technique is shown by comparison with well-known methods such as TEA, XTEA, and DLS-XTEA. The suggested strategy outperforms traditional strategies, according to simulation findings.

References

[1] N. A, Azeez, and C. Van der Vyver, "Security and Privacy Issues in E-Health Cloud-Based System: A Comprehensive Content Analysis," *Egyptian Informatics Journal*, vol. 20, no. 2, p. 97-108, 2019, doi: 10.1016/j.eij.2018.12.001

[2] M. Sharma, and R. Sehrawat, "A Hybrid Multi-Criteria Decision-Making Method for Cloud Adoption: Evidence from the Healthcare Sector," *Technology in Society*, vol. 61, p. 101258, 2020, doi: 10.1016/j.techsoc.2020.101258

[3] S. Shi, D. He, L. Li, N. Kumar, M. K. Khan, and K. K. R. Choo, "Applications of Blockchain in Ensuring the Security and Privacy of Electronic Health Record Systems: A Survey," *Computers and security*, vol. 97, p. 101966, 2020, doi: 10.1016/j.cose.2020.101966

[4] I. Yaqoob, I. A. T. Hashem, A. Ahmed, S. M. A. Kazmi, and C. S. Hong, "Internet of Things Forensics: Recent Advances, Taxonomy, Requirements, and Open Challenges," *Future Generation Computer Systems*, vol. 92, pp. 265-275, 2019, doi: 10.1016/j.future.2018.09.058

[5] X. Hu, and L. Ma, "A Study on the Hybrid Encryption Technology in the Security Transmission of Electronic Documents," in: *2010 International Conference of Information Science and Management Engineering*. vol. 1, IEEE, Shaanxi, China, pp. 60-63, Aug. 2010, doi: 10.1109/isme.2010.100

[6] S. Tanwar, K. Parekh, and R. Evans, "Blockchain-based Electronic Healthcare Record System for Healthcare 4.0 Applications," *Journal of Information Security and Applications*, vol. 50, p. 102407, 2020, doi: 10.1016/j.jisa.2019.102407

[7] C. Cao, Y. Tang, D. Huang, W. Gan, and C. Zhang, "IIBE: An Improved Identity-based Encryption Algorithm for WSN Security," *Security and Communication Networks*, vol. 2021, p. 8527068, 2021, doi: 10.1155/2021/8527068

[8] E. M. Zhao, and Y. Geng, "Homomorphic Encryption Technology for Cloud Computing," *Procedia Computer Science*, vol. 154, pp.73-83, 2019, doi: 10.1016/j.procs.2019.06.012

[9] A. Anand, S. Rani, D. Anand, H. M. Aljahdali, and D. Kerr, "An Efficient CNN-based Deep Learning Model to Detect Malware Attacks (CNN-DMA) in 5G-IoT Healthcare Applications," *Sensors*, vol. 21,

no. 19, p. 6346, 2021, doi: 10.3390/s21196346

[10] K. Kordov, "A Novel Audio Encryption Algorithm with Permutation-Substitution Architecture", *Electronics*, vol. 8, no. 5, p. 530, 2019, doi: 10.3390/electronics8050530

[11] M. Zhang, Y. Chen, and J. Huang, "SE-PPFM: A Searchable Encryption Scheme Supporting Privacy-Preserving Fuzzy Multikeyword in Cloud Systems", *IEEE Systems Journal*, vol, 15, no. 2, pp. 2980-2988, 2020, doi: 10.1109/jsyst.2020.2997932

[12] A. M. Ali, M. A. Ngadi, I. I. Al Barazanchi, and P. S. JosephNg, "Intelligent Traffic Model for Unmanned Ground Vehicles Based on DSDV-AODV Protocol," *Sensors* (*Basel*), vol. 23, no. 14, p. 6426, 2023, doi: 10.3390/s23146426

[13] I. Al-Barazanchi, W. Hashim, A. Ahmed Alkahtani, H. Rasheed Abdulshaheed, H. Muwafaq Gheni, A. Murthy, E. Daghighi, SA. Shawkat, and ZA. Jaaz, "Remote Monitoring of COVID-19 Patients Using Multisensor Body Area Network Innovative System," *Computational Intelligence and Neuroscience*, vol. 2022, p. 9879259, 2022, doi: 10.1155/2022/9879259

[14] Y. Niu, S. I. Kadhem, I. A. M. Al Sayed, Z. A. Jaaz, H. M. Gheni, and I. Al Barazanchi, "Energy-Saving Analysis of Wireless Body Area Network Based on Structural Analysis," in: *2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*. IEEE, Ankara, Turkey, pp. 1-6, 2022, doi: 10.1109/hora55278.2022.9799972. Available from: https://ieeexplore.ieee.org/document/9799972 [Last accessed on 2023 Nov 15].

[15] R. Al-Amri, R. K. Murugesan, E. M. Alshari, and H. S. Alhadawi, "Toward a Full Exploitation of IoT in Smart Cities: A Review of IoT Anomaly Detection Techniques," pp. 193-214, 2022. Available from: https://link.springer.com/10.1007/978-3-030-85990-9_17 [Last accessed on 2023 Nov 15].

[16] Z. M. Yaseen, T. T. Zigale, Tiyasha, D. Ravi Kumar, S. Q. Salih, S. Awasthi, T. M. Tung, N. Al-Ansari, and S. K. Bhagat, "Laundry Wastewater Treatment Using a Combination of Sand Filter, Bio-Char and Teff Straw Media," *Scientific Reports*, vol. 9, no. 1, p. 18709, 2019, doi: 10.1038/s41598-019-54888-3

[17] S. Q. Salih, A. Sharafati, I. Ebtehaj, H. Sanikhani, R. Siddique, R. C. Deo, H. Bonakdari, S. Shahid, and Z. M. Yaseen, "Integrative Stochastic Model Standardization with Genetic Algorithm for Rainfall Pattern Forecasting in Tropical and Semi-Arid Environments," *Hydrological Sciences Journal*, vol. 65, no. 7, pp. 1145-57, 2020, doi: 10.1080/02626667.2020.1734813

[18] H. Tao, S. Q. Salih, M. K. Saggi, E. Dodangeh, C. Voyant, N. Al-Ansari, Z. M. Yaseen, and S. Shahid, "A Newly Developed Integrative Bio-Inspired Artificial Intelligence Model for Wind Speed Prediction," *IEEE Access*, vol. 8, pp. 83347-8358, 2020, doi: 10.1109/access.2020.2990439

[19] U. Beyaztas, S. Q Salih, K. W. Chau, N. Al-Ansari, and Z. M. Yaseen, "Construction of Functional Data Analysis Modeling Strategy for Global Solar Radiation Prediction: Application of Cross-Station Paradigm," *Engineering Applications of Computational Fluid Mechanic*, vol. 13, no. 1, pp. 1165-1181, 2019, doi: 10.1080/19942060.2019.1676314

[20] S. Abdullah, J. Arshad, M. M. Khan, M. Alazab, and K. Salah, "PRISED Tangle: A Privacy-Aware Framework for Smart Healthcare Data Sharing Using IOTA Tangle," *Complex and Intelligent Systems*, vol, 9, no. 3, pp. 3023-3041, 2023, doi: 10.1007/s40747-021-00610-8

[21] I. Al Barazanchi et al., "WBAN System Organization, Network Performance and Access Control: A Review," 7th Int. Conf. Eng. Emerg. Technol. ICEET 2021, no. October, pp. 27–28, 2021, doi: 10.1109/ICEET53442.2021.9659564.

[22] H. H. Abbas, Z. A. Jaaz, I. Al_Barazanchi, and H. R. Abdulshaheed, "Survey on Enhanced Security Control measures in Cloud Computing systems," J. Phys. Conf. Ser., vol. 1878, no. 1, p. 012004, 2021, doi: 10.1088/1742-6596/1878/1/012004.

[23] H. H. A. and H. R. A. I. Al-Barazanchi, Z. A. Jaaz, "Practical application of IOT and its implications on the existing software," 2020 7th Int. Conf. Electr. Eng. Comput. Sci. Informatics (EECSI), Yogyakarta, Indones., no. October, pp. 10–14, 2020, doi: 10.23919/EECSI50503.2020.9251302.