JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

An improvement of security for AES implementations

M.Prasanna Kumar1*, Umma Aashritha Reddy[2], Ayesha Siddiqua[3], Kothapalli Aasritha sai[4], Jangala Suneetha[5]
1*Assistant Professor: Vignan's Nirula Institute of Technology and Science for Women.
2,3,4,5 B.Tech Scholar: Vignan's Nirula Institute of Technology and Science for Women.

During the last couple of years, cyber security has been of immense concern. Encryption is a process used for the protection of data. Symmetric as well as asymmetric encryption techniques are widely used in information security. The most commonly used safe symmetric encryption currently available is Advanced Encryption Standard (AES). However, AES encryption is slow in computation. Our test shows that the use of both techniques takes 3.045 milliseconds for 1024 bytes of data Every 2048 bytes of data its value increases by 3–4 milliseconds and so on. Cryptographic circuits, because they involve sensitive data, become easy subjects for fraudulent manipulations also known as attacks by malicious individuals. Many attacks have already been found and studied. One of the most powerful methods is called DFA (Differential Fault Analysis) cryptanalysis, by introducing faults on purpose into the calculations-for example, using a laser. Then, countermeasures are designed and validated to protect the hardware implementation of cryptographic methods such as the AES algorithm.

Keywords: Cybersecurity, Encryption, Symmetric encryption, Asymmetric encryption, Advanced Encryption Standard (AES), AES encryption, Differential Fault Analysis (DFA), Cryptanalysis

1. Introduction

The National Institute of Standards and Technology (NIST) held [1-5] a competition in 2001 that resulted in the selection of the Advanced Encryption Standard (AES) as the current symmetric encryption standard. As of 2001, the National Institute of Standards and Technology (NIST) DES (Data Encryption Standard) should be replaced. Additionally, its broad [6-8] widespread use in a range of contemporary applications, like online payments mobile phones, smart cards, ment systems, electronic purses, and pay television, which accounts for the considerable interest it has ignited. Moreover, their application is highly advantageous since they have less memory, less complexity, and less difficulty The implementation of ware is made simpler.

The operations of addition, subtraction, multiplication, [9-16] and division in finite field arithmetic are explained by Stalling.AES operation performance is dependent on key length 3.Four distinct transformations are performed on each round: [17-21] AddRoundKey, MixColumn, SubBytes, and Shift Rows.The simulation is explained in the next section. AES process using straightforward examples to make the optimization part understandable. Most recent AES improvements have been made to domain hardwareSatoheet.optimize AES through circuit National logic is used by CMOSstandardcell library4.Ahmadet.aluse, which is implemented using a truth table on a Vertex IIFPGAchip5, Daemenet, and Aluse 32-bit data as the foundational unit of AES transformation to enhance the execution. Using AES-NI extended instruction set to significantly improve the AES algorithm7. There are lots of additional hardware [22-27] implementation for optimized AES.

Any corporate or academic entity's security assessment has to include analysis related to the strength of the cipher. Cipher analysts have shown that, on current hardware platforms, effectively around eight out of ten AES rounds can be brute-forced. The attacker cannot make the attack on the system significant to them if the remaining 2 rounds are not disrupted timely (Bogdanov et al., 2011). The current trend is that computing power is upsurging, and within a very short time, it would be fully deciphered in the allocated time, jeopardizing the system that is being tested. Many researches are being conducted presently to find ways [28] of ameliorating the security of the AES algorithm.

These algorithms are found in an interacting part that takes cues from its environment. Smart cards, as most electronic components, use energy; hence they also emit radiation. The other influencing factors include temperature and even [29-30] magnetic fields. The nature of these communications enables an attacker to notice and capture them in order to perform a secret channel attack, which is also known as Side-Channel Analysis, or SCA (Standaert et al., 2006; Brier et

al., 2004; Le et al., 2006; Katashita et al., 2008; Standaert et al., 2008; Prouff and Rivain, 2003; Ng et al., 2020). [31-32] For the past two decades, several concepts of side-channel attacks have been developed.

2. Literature survey

Integrated circuit [33-35] designers have tried to design several countermeasures for the implementation of AES toward the goal of eliminating the possibility of a fault injection attack demonstrated to be able to inject exploitable [36] flaws to fraudulently extract confidential data.

(Yen and Wu, 2006) uses the Cyclic Redundancy Check (CRC) (n + 1,n) to detect faults, where n = {4,8,16} is the byte count of the message. ((5,4) It is easy to use CRC), ((9,8) CRC), or ((17,16) CRC) structures to Implement the proposed countermeasure. The CRC technique has specialized for the targeted S-Box system and the One limitation of this paper is that the results make use of inverse S-Box. The proposed as a countermeasure [37] composite field-based S-Box was applied in the suggested as a countermeasure. For dealing with this problem, the method proposed in Reyhani-Masoleh and Mozaffari-Kermani (2010) rely on a numerical report of S-Box's input and output, in addition to the inverse SubByte for fault detection and the inverse S-Box for SubByte.

Two categories of implementations [38-40] exist for both software and hardware, with hardware implementation posing to be more attractive compared to the former due to providing better security, faster execution, and improved power efficiency ([1]Karthigai Kumar and Baskaran, 2010).Gaj and Chodowiec The authors demonstrated ASIC realization of cryptography algorithm 2009's (et al., Chih-Pin (2003), [41] Luke and Liu (2003)ASICs are integrated circuits which have very few flexibilities and are focused towards single use. In addition small-scale production is now not possible with rising Non Recurring Engineering cost.

In [2], Lu et al. presented a new architecture technique [42-47] to reduce the complexity architecture of the AES algorithm when it is implemented in hardware, including smartphones, PDAS and card, etc. It has been linked to the combining of the AES was both encrypted and decoded. provides an unconditionally working AES crypto-engine. To do so, they focused on a few key points. of Particularly, AES (Inv)Sub Bytes and Module for (Inv) Mix column. In [3], a number of secret key algorithms were performed to see which one may provide the best performance for encrypting and decoding information. The choice for this was based on four popular algorithms: Blowfish, DES, 3DES, and AES. To analyse these encryption [48-50] size and algorithm contents input files were edited, with two distinct These algorithms were tested on platforms such as P-4 2.4 GHz and P-II 266 MHz. According to the results Blowfish is the one that can provide the most effectiveness compared to other algorithms and AES outperforms 3DES and DES. The designed TMRrp&TTRke32 and TMRrp&TTRke64 are immune to all single-bit and single-byte transient and permanent faults that occur in the core components of the round-path unit, whereas only transient faults in the key expansion unit.

In the suggested architecture, [51-55] TMRrp&TTRke64 suffers from a 52.29% throughput degradation and 55.4% area overhead. Sheikhpour et al. (2019) designed an efficient and cost-effective fault robust architecture for the AES block cipher that varies with key size and pipeline levels.

Chu and Benaissa (2013) applied polynomial residue number systems (PRNS) to protect AES against fault attacks. The PRNS architecture restyles and reconsiders the design approach for the AES implementation. High error coverage [56] is possible with the implementation of the proposed fault detection system. However, the technique is not so easy to adopt because of the complex and technical applicability challenges of the given complexity. Using Add Round Key parity prediction, Mix Columns, Shift Rows, and the relationship between Sub Bytes input and output, Mestiri et al., (2013) defend the AES algorithm against fault attacks. [57] This proposed fault detection approach can detect 99.998% of injected flaws based on information redundancy. However, its throughput is less compared to that of the original approach.

3. Proposed methodology

This framework checks for security, privacy, load balancing, and trust in the following contexts. The cloud benefactor goes through framework gateways in response to the requests from the user and the transferring of data whenever the user directs them. The following elements are included in the suggested framework:

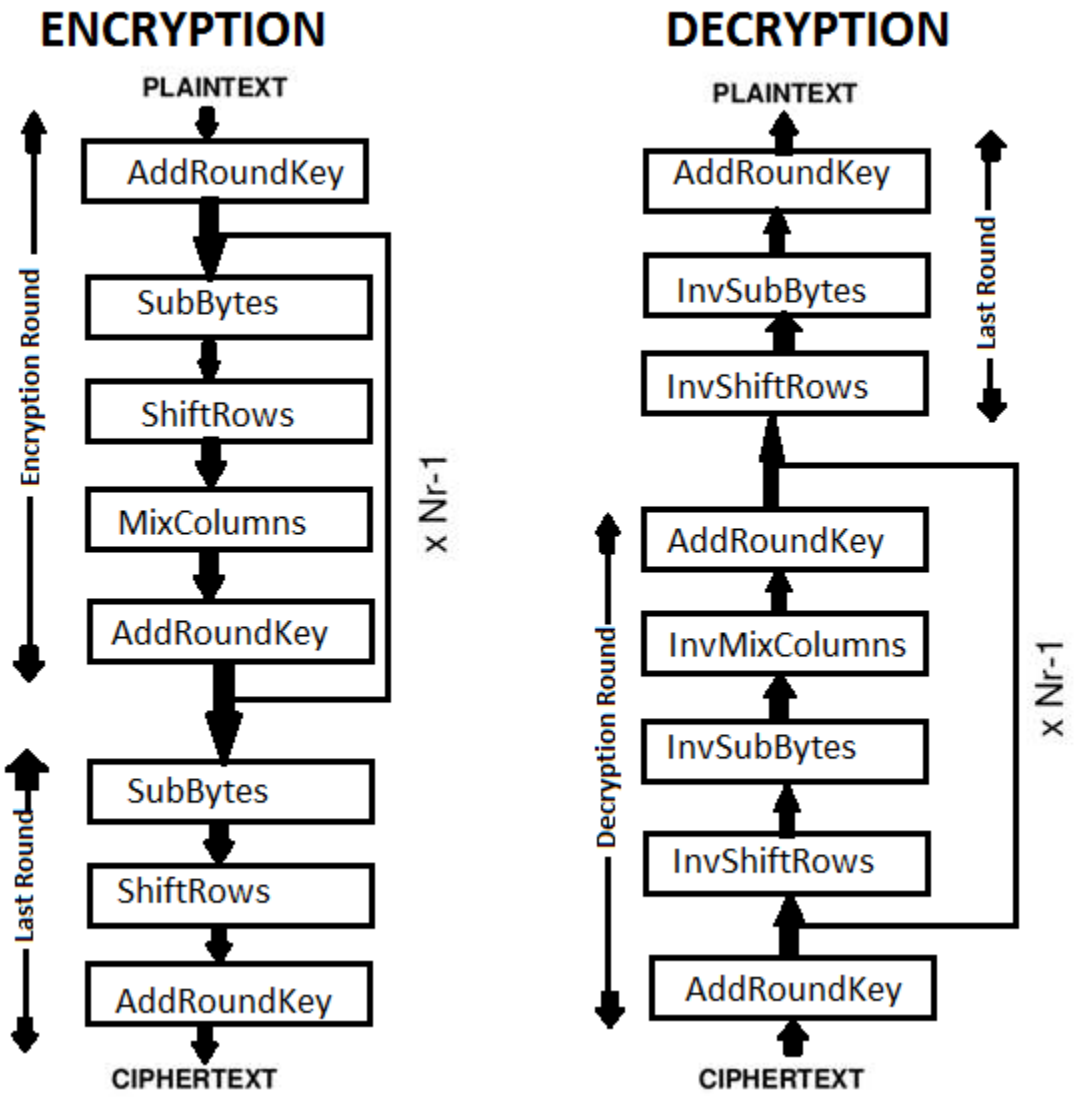
It manages the CSP layer which includes major resources and expertise in the building process. It also computes the operations of the distributed cloud storage servers and controls the live, obscure work-out technique. Software as a service is its primary component, a model that offers software applications as a service to the end users. Platform as a service (PaaS): This concept suggested a request-handling environment. The development tools incorporated in this paradigm also come in handy when it comes to complex applications. Infrastructure as a service is a platform providing the necessary resources from virtual and physical computers down to virtual storage.

Trust Management Unit for Security Services: Security Services Trust management gateways, however, regulate the service configuration trust management controls every unit, including security management. The following illustrates all the units further. Security management layer: This is the layer that provides implementation functionality as well as security and privacy details.

The modules below, along with their description, constitute the security service. Availability, as measured by a security control unit, is the proportion of time a client can utilize the service.

It ensures that whatever is stored on cloud storage is protected from access that is unintended or undesirable. Authenticating users generally memorize their usernames and passwords quite well once they have accessed the cloud using a web browser.

Attack detection unit: after all, fairly mundane tasks that err on the side of satisfying the needs of cloud security. Data protection unit: shows use of the AES algorithm to make data safer in cryptography techniques using AES ciphers so that they can effectively control network resources, balance loads, and have lower power consumption while encrypting 128-bit data blocks at 1000 blocks per second with the possibility of the double round key.



Asymmetric 128-bit data encryption is used in the AES data encryption algorithm. A set of 16 bytes are fed into the algorithm. Before this, each of these input bytes is first permuted using a predetermined table called S.

Non-linear operation: Box(Substitution-Box). Then, the bytes arekept in a 4 by 4 matrix known as "state," with its rows rotatedAccording to the line number determines the rotation increment to the right.This is because theS-boxapproacheasiertoconstructandfasterthanthecomWith a politeness field approach, the above proposed detection strategiesbox approach using LUT. We make use of the following to determine the 256 entries.

Look-uptable S-box (LUT). The transformation of Mix Columns is the binary multiplication of polynomials from another matrix for every element of the matrix.This method makes a "mixture" in each column. Themodulo X4+1, polynomial(X)=3X3+X2+X+2, is multiplied each byte in the column by the inpolynomial form.Following that,theare reduced modulo 2 and we indicate the correct formthe ofamatrix

4. Result

The AES algorithm with and without the fault detection approach was implemented on an FPGA using a Vertex 5 XC5VFX70T package FF1136 speed-2 and Xilinx ISE 13.4 as the synthesis tool and ModelSim (PE Student Edition 6.6d) for simulation. VHDL was used to program the design. Table 4 summarizes the out ¬ comes of the implementation.

The AES took up 429 slicesin its original form. The implemented frequency is 250.412 MHz. Thus, the total throughputis 2671.06 Mbits/s. In the AES encryption process,a new fault detection technique consumes 11.65% more Slices thanthe original implementation. The frequency of AES encryption withfault detection improves by 48.4% against the original insince the number of cycles increases. Therefore, the maximum frequency is improved due to the pipeline registers incorporated in the round in AES. Since the processing architecture utilized in the system is pipelined, latcy is not found

to be generated as a problem in the system. That is, encryption and re-encryption is done in the same clock cycle. So, the system is capable of reaching a this produces an encryption result and error checking against fault attacks at each clock cycle, thus having a maximum frequency higher than that of AES. The data is processed and fault detected simultaneously, meaning data processing is fastened.

The protected AES requires 31 clock cycles, while the unprotected AES takes 12 clock cycles. This reduces the throughput being much lower compared to the original AES since the throughput is inversely proportional to the number of cycles. In the process of encryption, our proposed detection technique decreases the throughput by 42.55 %. Our fault detection technique can achieve good balance between security and performancesafety and low implementation costs.

Performance of different hardware implementations offault detection algorithms is summarized in Table 5. Notethat the results obtained are comparable to previous implementations about fault coverage (FC), area, frequency, throughputand efficiency overhead. It should be added that, sincemost similar studies split faulty outputs into undetected andDetected error categories, we categorized the silent fault and falsepositive as detected error.

Table 1

Fault detection capability for AES encryption.

Faults types		Fault coverage (%)			
		Silent fault	Undetected error	False positive	Detected error
Single-bit (N = 1)		2.952	0.092	8.375	88.581
Multiple bit	N = 2	1.476	0.012	4.087	94.425
	N = 3	0.803	0.0003	2.371	96.8257
	N = 4	0.223	≈0	0.971	98.806
	N = 5	0.168	≈0	0.589	99.246
	N = 6	0.089	≈0	0.286	99.625
	N = 7	0.039	≈0	0.127	99.834
	Random faults	0.357	0.009	0.095	99.539

Table 2

Synthesis results.

AES-128	Encryption					Decryption		
	Area (Slice) (Overhead)	Freq. (MHz) (Overhead)	Thro. (Mbps) (Degradation)	Slice LUTs (Overhead)	Flip-Flops (Overhead)	Area (Slice) (Overhead)	Freq. (MHz) (Overhead)	Thro. (Mbps) (Degradation)
Original	429	250.412	2671.06	1290	269	524	224.45	2394.13
Protected	479 (11.65%)	371.614 (48.4%)	1534.4 (42.55%)	1604 (24.34%)	318 (18.21%)	630 (20.23%)	300.89 (34.05%)	1242.38 (45.6%)

Our proposed method has the highest frequency and theleast area overhead compared to (Mozaffari-Kermaniand Reyhani-Masoleh, 2010; Chu and Benaissa, 2013; Mestiriet al., 2013; Mestiri et al., 2019; Sheikhpour et al., 2021). The fault detection structure in (Chu and Benaissa, 2013) does not affect theoperating frequency, but it contributes to around 81% of the original AESimplementation's area overhead. In comparison with our system, theapproach described in Mestiri et al., 2013 has a higher fault detection rate Higherfaultcoveragewhilealsohavingaveryhighareaoverheadof25.38%. Moreover, witha frequencydegradationof 11.53% TheproposedimplementationinZhangetal.,2019necessitates a largerareaoverheadthanourapproach.Althoughthemethodprovidedin(Bedouietal.,2017)providessignificantlyhigherfaultcoveragethanour system, it isaccompaniedwithalargeariaload (34.73%) anda 59.99%downturninthethroughput. Incomparisontoourwork, theproposed implementation in (Benhadjyoussef et al., 2020)coveredmorefaults thanourmethod, althoughrequiringa 14%areaoverhead.

5. Conclusion

We have presented in this paper a low-cost counter measure for theAES encryption and decryption process. The AES round architecture is modified with incorporation of temporal redundancy in our approach. The round is divided into three stages and two pipeline registers are added in between in the proposed design toenhance fault coverage. The concurrent

fault detection method based on time redundancy applies well to blocks in the criticalpath. We used fault injection simulations written in the VHDLanguage to verify that the suggested schema can detect problems.
As we have seen, the created approach can detect 99.539% of injected random errors. The overhead in area is quite low, the overhead in speed and power consumption are low. The overhead is limited to the memorization of the first result and to the comparison logic,the power consumed increases little. To ensure the accuracy of our results, we compare our implementation results to those found in the literature. It is important to note that the results obtained are comparable to those of other implementations. Our fault detection approach can strike a balance between high safety and inexpensive implementation costs.

6.References

[1].Karthigai Kumar and Baskaran, 2010P. Karthigai Kumar, K. Baskaran
An ASIC implementation of low power and high throughput blowfish crypto algorithm
[2] Lu, C. C., & Tseng, S. Y. (2002). Integrated design of AES (Advanced Encryption Standard) encrypter and decrypter. In Application-Specific Systems, Architectures and Processors, 2002. Proceedings. The IEEE International Conference on (pp. 277-285).
[3] Nadeem, H (2006). A performance comparison of data encryption algorithms," IEEE Information and Communication Technologies, (pp. 84-89).
[4] Dia, S., E, Hatem M. A. K., &Mohiy M. H. (2010, May) Evaluating the Performance of Symmetric Encryption Algorithms. International Journal of Network Security, Vol.10, No.3, (pp.213-219).
[5]Yen, C., Wu, B., 2006. Simple error detection methods for hardware implementation of advanced encryption standard. IEEE Trans. Compute. 55 (6), 720–731. Zhang J., Wu N., Zhou F., Ge F., Zhang X., 2019. Securing the AES cryptography
[6] Mozaffari-Kermani, M., Reyhani-Masoleh, A., 2010. Concurrent structureindependent fault detection schemes for the advanced encryption standard. IEEE Trans. Compute. 59 (5), 608–622.
[7] Sheikhpour, S., Mahani, A., Bagheri, N., 2021. Reliable advanced encryption standard hardware implementation: 32-bit and 64-bit data-paths. Microprocess. Microsystem. J., Elsevier 81, 103740.
[8]Chu, J., Benaissa, M., 2013. Error detecting AES using polynomial residue number systems. Microprocess. Microsystem. J. Elsevier 37 (2), 228–234.
[9] Mestiri, H., Kahri, F., Bouallegue, B., Machhout, M., 2016. A high-speed AES design resistant to fault injection attacks. Microprocess. Microsystem. J., Elsevier 41, 47– 55.

[10] Patibandla, R. S. M. L., Rao, B. T., Narayana, V. L., & Srinivas, V. S. (2021). An overview of ontology-based artificial intelligence services in health care systems. In *Proceedings of the International Conference on Health Care Systems* (pp. 47–63).

[11] Maddumala, V. R., Maha Lakshmi, K., Anusha, P., & Lakshman Narayana, V. (2020). Enhanced morphological operations for improving the pixel intensity level. *Journal of Computational and Theoretical Nanoscience*, 29(3), 9191–9201.

[12] Narayana, V. L., Malleswari, K. S. N., Divyanjali, M., Nandini, S., & Purnima, G. (2023). Video frame based prompt compression model with steganography for secure data transmission. In *Proceedings of the International Conference on Advanced Intelligent Systems* (pp. 373–377). https://doi.org/10.1109/ICAIS56108.2023.10073883

[13] Naresh, A., Pavani, V., Meghana Chowdary, M., & Lakshman Narayana, V. (2020). Energy consumption reduction in cloud environment by balancing cloud user load. *Journal of Critical Reviews*, 7(7), 1003–1010. https://doi.org/10.31838/jcr.07.07.184

[14] Patibandla, R. S. M. L., & Vejendla, L. N. (2022). Significance of blockchain technologies in industry. In *Advances in Blockchain Technologies* (pp. 19–31). https://doi.org/10.1007/978-3-030-70501-5_2

[15] Pasala, S., Pavani, V., Lakshmi, G. V., & Narayana, V. L. (2020). Identification of attackers using blockchain transactions using cryptography methods. *Journal of Critical Reviews*, 7(6), 368–375. https://doi.org/10.31838/jcr.07.06.65

[16] Mounika, B., Anusha, P., Narayana, V. L., & Lakshmi, G. V. (2020). Use of blockchain technology in providing security during data sharing. *Journal of Critical Reviews*, 7(6), 338–343. https://doi.org/10.31838/jcr.07.06.59

[17] Narayana, V. L., Vinayaki, K. V., Swetha, P. A., Sri, K. D., & Chaithanya, G. (2024). Superior attribute weighted set for object skeleton detection using ResNet50 with edge-based segmentation model. In *Proceedings of the International*

Conference on Smart Computing and Systems (pp. 1132–1139). IEEE. https://doi.org/10.1109/ICSCSS60660.2024.10624879

[18] Gopi, A. P., & Naik, K. J. (2022). An IoT model for fish breeding analysis with water quality data of pond using modified multilayer perceptron model. *2022 International Conference on Data Analytics for Business and Industry (ICDABI)*, 448-453. https://doi.org/10.1109/ICDABI56818.2022.10041617

[19] Arepalli, P. G., & Naik, K. J. (2024). A deep learning-enabled IoT framework for early hypoxia detection in aqua water using lightweight spatially shared attention-LSTM network. *Journal of Supercomputing, 80*(2), 2718-2747. https://doi.org/10.1007/s11227-023-05580-x

[20] Arepalli, P. G., & Naik, K. J. (2023). An IoT-based water contamination analysis for aquaculture using lightweight multi-headed GRU model. *Environmental Monitoring and Assessment, 195*(12), Article 1516. https://doi.org/10.1007/s10661-023-12126-4

[21] Gopi, A. P., Gowthami, M., Srujana, T., Gnana Padmini, S., & Durga Malleswari, M. (2023). Classification of denial-of-service attacks in IoT networks using AlexNet. In *Smart Innovation, Systems and Technologies* (Vol. 316, pp. 349-357). https://doi.org/10.1007/978-981-19-5403-0_30

[22] Bikku, T., Gopi, A. P., & Prasanna, R. L. (2019). Swarming the high-dimensional datasets using ensemble classification algorithm. In *Advances in Intelligent Systems and Computing* (Vol. 815, pp. 583-591). https://doi.org/10.1007/978-981-13-1580-0_56

[23] Arepalli, P. G., & Khetavath, J. N. (2024). Water quality classification using multi-cell RNN in aquaculture ponds for Catla fish. In *Lecture Notes in Networks and Systems* (Vol. 897, pp. 363-370). https://doi.org/10.1007/978-981-99-9704-6_34

[24] Arepalli, P. G., & Naik, K. J. (2024). Water contamination analysis in IoT-enabled aquaculture using deep learning-based AODEGRU. *Ecological Informatics, 79*, Article 102405. https://doi.org/10.1016/j.ecoinf.2023.102405

[25] Arepalli, P. G., & Naik, K. J. (2024). An IoT-based smart water quality assessment framework for aqua-ponds management using Dilated Spatial-temporal Convolution Neural Network (DSTCNN). Aquacultural Engineering, 104, Article 102373. https://doi.org/10.1016/j.aquaeng.2023.102373

[26] Gopi, A. P., Narayana, V. L., & Kumar, N. A. (2018). Dynamic load balancing for client-server assignment in distributed systems using genetic algorithm. Ingenierie des Systemes d'Information, 23(6), 87-98. https://doi.org/10.3166/ISI.23.6.87-98

[27] Sarada, K., Narayana, V. L., Gopi, A. P., & Pavani, V. (2020). An iterative group based anomaly detection method for secure data communication in networks. Journal of Critical Reviews, 7(6), 208-212. https://doi.org/10.31838/jcr.07.06.39

[28] Narayana, V. L., Gopi, A. P., & Chaitanya, K. (2019). Avoiding interoperability and delay in healthcare monitoring system using blockchain technology. Revue d'Intelligence Artificielle, 33(1), 45-48. https://doi.org/10.18280/ria.330108

[29] Gopi, A. P., Jyothi, R. N. S., Narayana, V. L., & Sandeep, K. S. (2023). Classification of tweets data based on polarity using improved RBF kernel of SVM. International Journal of Information Technology, 15(2), 965-980. https://doi.org/10.1007/s41870-019-00409-4

[30] Narayana, V. L., Gopi, A. P., Khadherbhi, S. R., & Pavani, V. (2020). Accurate identification and detection of outliers in networks using group random forest methodology. Journal of Critical Reviews, 7(6), 381-384. https://doi.org/10.31838/jcr.07.06.67

[31] Rao, B. T., Patibandla, R. S. M. L., Narayana, V. L., & Gopi, A. P. (2021). Medical data supervised learning ontologies for accurate data analysis. In Semantic Web for Effective Healthcare Systems (pp. 249-267). https://doi.org/10.1002/9781119764175.ch11

[32] Patibandla, R. S. M. L., Gopi, A. P., Narayana, V. L., & Rao, B. T. (2023). Decentralized smart healthcare systems using blockchain and AI. In Blockchain applications in healthcare: Innovations and practices (Vol. 1, pp. 139-154). DOI: 10.1002/9781394229512.ch8

[33] Lakshman Narayana, V., & Gopi, A. P. (2020). Enterotoxigenic Escherichia coli detection using the design of a biosensor. Journal of New Materials for Electrochemical Systems, 23(3), 164-166. DOI: 10.14447/jnmes.v23i3.a02

[34] Rani, B. M. S., Majety, V. D., Pittala, C. S., Vijay, V., Sandeep, K. S., & Kiran, S. (2021). Road Identification Through Efficient Edge Segmentation Based on Morphological Operations. *Traitement du Signal*, *38*(5).
[35] Kanumalli, S. S., Ch, A., & Murty, P. S. R. C. (2020). Secure V2V Communication in IOV using IBE and PKI based Hybrid Approach. *International Journal of Advanced Computer Science and Applications*, *11*(1).
[36] Kiran, S., Kanumalli, S. S., Krishna, K. V. S. S. R., & Chandra, N. (2021). WITHDRAWN: internet of things integrated smart agriculture for weather predictions and preventive mechanism.
[37] Prathipati, Silpa Chaitanya, and Susanta Kumar Satpathy. "A Multilevel De-Noising Approach for Precision Edge-Based Fragmentation in MRI Brain Tumor Segmentation." *Traitement du Signal* 40.4 (2023): 1715.

[38] Krishna, Komanduri Venkata Sesha Sai Rama, et al. "Classification of Glaucoma Optical Coherence Tomography (OCT) Images Based on Blood Vessel Identification Using .CNN and Firefly Optimization." Traitement du Signal 38.1 (2021).
[39] Prathipati, Silpa Chaitanya, and Susanta Kumar Satpathy. "Transforming 3D Brain Tumour Image Segmentation: An Enhanced V-Net Approach for Precise Diagnosis and Treatment Planning." *2024 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI)*. IEEE, 2024.

[40] Ekkurthi, A., Sujatha, V., Kumar, K.V.,"**Effective Moving Object Tracking Using Adaptive Background Subtraction with Advanced Probability Evolutionary Algorithm",*International Journal on Recent and Innovation Trends in Computing and Communication***, 2023, 11, pp. 1–3

[41] Sujatha, V., Yaddala, M., Kollipara, V., Shaik, K., Burri, R.K(23),"Movie reviews data classification using convolution neural networks",***AIP Conference Proceedings***. 2023, 2724, 030009

[42] Godavarthi, B., Majety, V. D., Mrudula, Y., & Nalajala, P. (2019). Fault identification in power lines using GSM and IoT technology. *Advances in Intelligent Systems and Computing*, *815*, 647–655. https://doi.org/10.1007/978-3-319-91117-2_70

[43] Majety, V. D., & Murali, G. (2018). A remote epileptic patient supervising system. *Advances in Modelling and Analysis B*, *61*(4), 207–210. https://doi.org/10.18280/ama_b.610402
[44] Naresh, A., TSLP, H., Ch, G., & Kumari, G. R. P. (2023, July). Early Prophecy of Low-Birth-Weight Babies Using BM Error Rate Classifier. In *2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT)* (pp. 1-6). IEEE.

[45] Kumari, G. R. P., Reddy, A. H., Lakshmi, K., Abhinaya, B., Sanjana, S., & Naresh, A. (2024, March). Time-Frame-Based Drowsiness Detection System Using CNN. In *2024 2nd International Conference on Disruptive Technologies (ICDT)* (pp. 711-716). IEEE.
[46] V. Pavani, K. Divya, V. V. Likhitha, G. S. Mounika and K. S. Harshitha, "Image Segmentation based Imperative Feature Subset Model for Detection of Vehicle Number Plate using K Nearest Neighbor Model," *2023 Third International Conference on Artificial Intelligence and Smart Energy (ICAIS)*, Coimbatore, India, 2023, pp. 704-709, doi: 10.1109/ICAIS56108.2023.10073848.
[47] V. Pavani, M. N. Swetha, Y. Prasanthi, K. Kavya and M. Pavithra, "Drowsy Driver Monitoring Using Machine Learning and Visible Actions," *2022 International Conference on Electronics and Renewable Systems (ICEARS)*, Tuticorin, India, 2022, pp. 1269-1279, doi: 10.1109/ICEARS53579.2022.9751890.
[48] Sri, Kurra Santhi, et al. "Advanced system control with traffic handling for secure communication in IoT routing protocol." *Journal Européen des Systèmes Automatisés* 54.2 (2021): 229-233.
[49] Arumugham, Vinothini, et al. "An explainable deep learning model for prediction of early-stage chronic kidney disease." *Computational Intelligence* 39.6 (2023): 1022-1038.
[50] Majety, Vasumathi Devi, et al. "Enhanced secure communication AODV routing protocol using SVM in MANETS." *AIP Conference Proceedings*. Vol. 2724. No. 1. AIP Publishing, 2023.
[51] Krisha, P.S., Peram, S.R. (2023). CT image precise denoising model with edge based segmentation with labeled pixel extraction using CNN based feature extraction for oral cancer detection. Traitement du Signal, Vol. 40, No. 3, pp. 1297-1304. https://doi.org/10.18280/ts.400349
[52] P. S. Krishna, V. R. Aparna, V. Priyanka, P. T. Niharika and T. Shivangi, "Convolution Neural Network Model with Feature Linked Vector for Oral Cancer Detection," *2023 IEEE 12th International Conference on Communication Systems and Network Technologies (CSNT)*, Bhopal, India, 2023, pp. 304-308, doi: 10.1109/CSNT57126.2023.10134660.

[53] Rayachoti, Eswaraiah, Sudhir Tirumalasetty, and Silpa Chaitanya Prathipati. "SLT based watermarking system for secure telemedicine." *Cluster Computing* 23.4 (2020): 3175-3184.
[54] Eswaraiah, Rayachoti, Tirumalasetty Sudhir, and Prathipati Silpa Chaitanya. "Curvelet transform based watermarking for telemedicine." *Wireless Personal Communications* 122.1 (2022): 309-329.
[55] Varshini, Y., Mounika, T., Kumari, G. R. P., Sirisha, G., & Deepthi, Y. (2023, March). Crop Yield Forecast Using Machine Learning. In *2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS)* (Vol. 1, pp. 2310-2315). IEEE.
[56] B. Aruna Kumari "**Time Series Data Classification for Precise Stock Market Price Prediction using ML" ICICACS International Conference on Integrated Circuits and Communication Systems, Scopus indexed, ISBN:**979-8-3503-1755-8/ **https://ieeexplore.ieee.org/document/10498248,18 April 2024**
[57] B.Aruna Kumari "HumanvAction Recognition From Video Frames Using Recurrent Neural Networks" ICDT 2nd International Conference on Disruptive Technologies (ICDT),Scopis indexed , ISBN:979-8-3503-7105-5/ https://ieeexplore.ieee.org/document/10489658, 11 April 2024