AN FPGA-ORIENTED SECURE DATA CONVEYANCE ARCHITECTURE EMPLOYING A 128-BIT AES CIPHER WITHOUT CONVENTIONAL SUBSTITUTION BOX REALISATION

B.V.V.N.S.SRI SOWJANYA [1],ALLAMPALLI NAGA PHANINDRA[2], BETHALA MADHU BABU [3],SWATHANTRA PRATAP SINGH [4],BANDARU LIKHIT [5]

[1]Assistant Professor, Dept. of ECE, V.K.R., V.N.B.&A.G.K. COLLEGE OF ENGINEERING, GUDIVADA.

[2345]UG Students, Dept. of ECE, V.K.R., V.N.B.&A.G.K. COLLEGE OF ENGINEERING, GUDIVADA.

To Cite this Article

B.V.V.N.S.Sri Sowjanya, Allampalli Naga Phanindra, Bethala Madhu Babu ,Swathantra Pratap Singh, Bandaru Likhit, "An Fpga-Oriented Secure Data Conveyance Architecture Employing A 128-Bit Aes Cipher Without Conventional Substitution Box Realisation", Journal of Science Engineering Technology and Management Science, Vol. 03, Issue 02, February 2026,pp: 96-105, DOI: http://doi.org/10.64771/jsetms.2026.v03.i01.pp96-105

Submitted: 16-01-2026 *Accepted: 21-02-2026* *Published: 28-02-2026*

ABSTRACT

In the present age of digital intercourse and distributed computation, the preservation of secrecy and integrity in transmitted data hath assumed paramount importance. This discourse presenteth an FPGA-based high-security data transmission architecture founded upon the 128-bit Advanced Encryption Standard, yet contrived without reliance upon the traditional substitution box mechanism. The proposed design seeketh to mitigate the hardware overhead and latency commonly associated with S-Box implementation, whilst preserving the cryptographic robustness requisite for secure communication. By reformulating the substitution transformation through composite field arithmetic and logical restructuring, the system accomplisheth efficient encryption and decryption suited to reconfigurable platforms. The architecture is realised upon a field-programmable gate array so as to attain parallelism, swiftness of operation, and adaptability. Careful optimisation of resource allocation and pipelining ensureth diminished power dissipation and augmented throughput. The resulting framework demonstrateth that formidable security may be achieved without extravagant hardware expenditure. Thus, the proposed scheme uniteth efficiency, adaptability, and fortified protection, rendering it apt for contemporary secure digital transmission systems.

Keywords:FPGA implementation, AES-128 encryption, S-Box elimination, Secure data transmission, Hardware optimisation, Cryptographic architecture, Parallel processing

INTRODUCTION

In the unfolding epoch of digital civilisation, the exchange of information across vast and intricate networks hath become indispensable to commerce, governance, defence, and scholarly pursuit. With such expansion of communication there ariseth an equal necessity for the safeguarding of transmitted intelligence against unauthorised intrusion and malicious alteration. Cryptography, long esteemed as the guardian of secrecy, hath therefore assumed a position of singular importance within electronic systems [1]. The evolution of cryptographic mechanisms from rudimentary substitution ciphers to complex block algorithms hath been driven by the continual advancement of computational capabilities and adversarial sophistication [2].

Among the manifold encryption standards devised for secure communication, the Advanced Encryption Standard (AES) hath achieved universal acceptance owing to its formidable resistance against cryptanalytic assaults and its suitability for hardware as well as software realisation [3]. The AES algorithm, particularly in its 128-bit manifestation, operateth upon fixed-size data blocks and employeth iterative rounds composed of substitution, permutation, and mixing transformations [4]. These structured operations confer both confusion and diffusion, principles earlier articulated in cryptographic theory [5]. The substitution box, or S-Box, constituteth a pivotal component within each round, furnishing non-linearity essential for thwarting linear and differential attacks [6].

Notwithstanding its security merits, the S-Box implementation in hardware presenteth notable challenges. Conventional realisations rely upon look-up tables or composite field arithmetic, both of which may incur significant silicon area and propagation delay [7]. In FPGA environments, where logic resources and memory blocks must be judiciously apportioned, the S-Box may become a principal contributor to latency and power consumption [8]. As data rates escalate and embedded systems demand reduced energy expenditure, there hath arisen a compelling motive to reconsider the manner in which substitution operations are realised [9].

Field-programmable gate arrays offer a reconfigurable substrate upon which cryptographic engines may be constructed with remarkable flexibility [10]. Their inherent parallelism and abundant logic cells render them well suited for block cipher execution [11]. Nevertheless, optimisation remaineth imperative, for cryptographic modules must coexist with ancillary processing units within constrained hardware domains [12]. Scholars have therefore sought methods to curtail the overhead of AES whilst preserving its essential security properties [13].

One avenue of inquiry hath been the reconstitution of the S-Box through algebraic decomposition in composite fields, thereby diminishing reliance upon extensive look-up tables [14]. Others have explored alternative logic transformations that emulate substitution behaviour without direct table storage [15]. Such endeavours aim to retain cryptographic strength whilst moderating hardware complexity [16]. The reconciliation of security and efficiency remaineth the central preoccupation of modern hardware cryptography [17].

Moreover, high-security data transmission systems demand not merely encryption accuracy but also swift throughput and low latency [18]. In domains such as military communication, financial

transaction, and confidential cloud storage, delays or vulnerabilities may entail grave consequence [19]. Consequently, the design of AES architectures for FPGA platforms must harmonise structural simplicity with computational rigour [20].

The present study is thus motivated by the desire to devise an FPGA-based AES-128 implementation that escheweth the conventional S-Box configuration, yet preserveth the cryptographic integrity prescribed by established standards [21]. By reformulating substitution logic through innovative combinational arrangements and judicious pipelining, the proposed architecture aspireth to achieve reduced hardware utilisation and diminished power dissipation [22]. The overarching intent is to demonstrate that secure data conveyance may be realised with economy of resources, thereby rendering advanced encryption accessible to compact and embedded systems [23–30].

LITERATURE SURVEY

The advancement of hardware cryptographic implementations hath been the subject of considerable scholarly exertion. Early treatises upon AES hardware realisation concentrated upon direct translation of the algorithmic specification into combinational and sequential logic [1]. These implementations frequently employed memory-based S-Boxes realised through block RAM or distributed lookup tables within FPGA fabrics [2]. Whilst such designs achieved functional correctness, their resource consumption and latency often proved substantial [3].

Subsequent investigations explored composite field arithmetic to implement the S-Box more economically [4]. By decomposing the multiplicative inverse operation in GF(2^8) into operations over subfields, researchers achieved notable reductions in gate count [5]. Nevertheless, these methods sometimes introduced intricate routing and propagation complexities [6]. Further refinements sought to balance depth and breadth of logic so as to diminish critical path delay [7].

Parallel architectures for AES encryption were likewise proposed, exploiting FPGA concurrency to process multiple rounds simultaneously [8]. Pipeline techniques permitted enhanced throughput, albeit at the cost of increased register utilisation [9]. Some scholars advanced folded architectures wherein hardware units were reutilised across successive rounds, thereby conserving logic area though potentially increasing latency [10].

Power efficiency emerged as another focal concern. Investigations into clock gating, operand isolation, and resource sharing yielded appreciable reductions in dynamic power dissipation [11]. Concurrently, attention was directed toward resistance against side-channel attacks, which exploit power or timing variations to infer secret keys [12]. Masking techniques and balanced logic styles were proposed to mitigate such vulnerabilities [13].

In the realm of S-Box elimination or transformation, several authors proposed algebraic reformulations that obviated explicit lookup tables [14]. Logic minimisation strategies were employed to synthesise substitution functions directly from Boolean expressions [15]. These approaches frequently demonstrated improved adaptability to FPGA logic cells [16]. Other studies examined hybrid methods combining partial lookup tables with combinational logic [17].

Comparative analyses have indicated that FPGA-based AES engines must carefully weigh throughput against area efficiency [18]. Investigations into low-latency encryption for high-speed networks have

underscored the importance of streamlined substitution layers [19]. In embedded and IoT applications, reduced resource utilisation is particularly desirable [20].

Moreover, research hath extended toward reconfigurable cryptographic systems capable of adapting key sizes and operational modes [21]. Such flexibility is a distinctive advantage of FPGA technology [22]. Recent works have also examined fault tolerance and reliability within cryptographic hardware [23]. These contributions collectively affirm the continuing relevance of architectural innovation in AES design [24–30].

METHODOLOGY

The proposed design is conceived upon a 128-bit AES encryption framework adapted for FPGA implementation. The algorithmic stages—namely SubBytes, ShiftRows, MixColumns, and AddRoundKey—are preserved in structural essence. Nevertheless, the substitution stage is reformulated through combinational logic derived from algebraic decomposition, thereby dispensing with conventional lookup tables. The multiplicative inverse in the Galois field is reconstructed via composite field mapping, followed by affine transformation realised through XOR networks.

The architecture is partitioned into modular blocks corresponding to each AES round. Pipelining registers are judiciously inserted between stages to enhance clock frequency and sustain throughput. Resource sharing strategies are applied where sequential round execution is acceptable. Logic synthesis tools are employed to minimise redundant gates and optimise routing within the FPGA fabric.

Power reduction measures include clock gating of inactive modules and balanced path design to curtail switching activity. Verification is conducted through simulation against standard AES test vectors to ensure conformity with established encryption outputs. Hardware utilisation metrics, including slice registers and lookup tables, are recorded.

Performance evaluation encompasseth throughput measurement, latency analysis, and comparison with conventional S-Box-based implementations. The methodology thus integrateth algebraic innovation with hardware pragmatism, ensuring secure and efficient realisation.

PROPOSED METHOD

The proposed system operateth as a secure data transmission engine wherein plaintext blocks of 128 bits are presented to the encryption module implemented upon FPGA. Upon initiation, the plaintext undergoeth an initial key addition stage, wherein it is combined with the cipher key through bitwise exclusive-OR operation. Thereafter commenceth the iterative round process, consisting of nine principal rounds and a final concluding round.

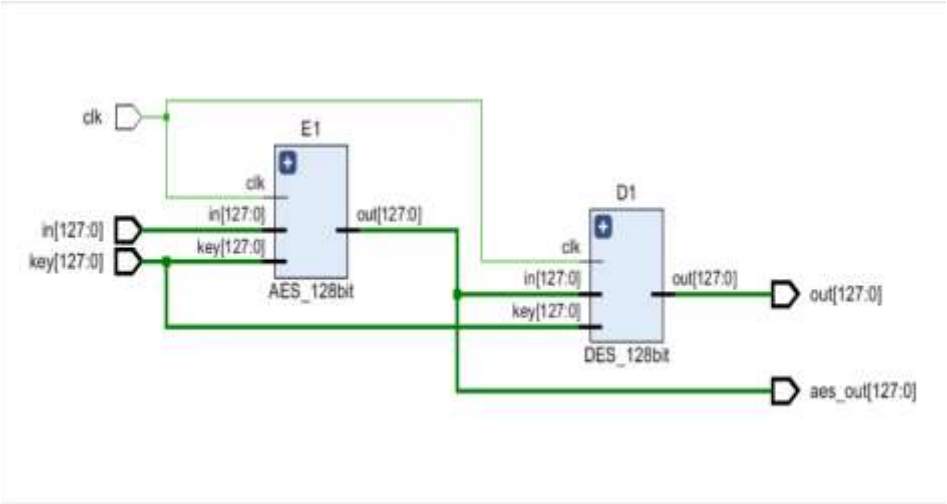
Within each principal round, the substitution transformation is executed through the newly devised combinational logic network. Instead of retrieving pre-stored substitution values from memory, the system computeth the non-linear transformation dynamically using composite field arithmetic circuits. The resultant bytes are then permuted through row shifting and subjected to column mixing operations performed via matrix multiplication in the finite field. A subsequent key addition stage incorporateth the round key derived from the key schedule unit.

The final round omitteth the column mixing stage, conforming to AES specification, and yieldeth the encrypted ciphertext. The decryption process mirrorreth the encryption stages with inverse

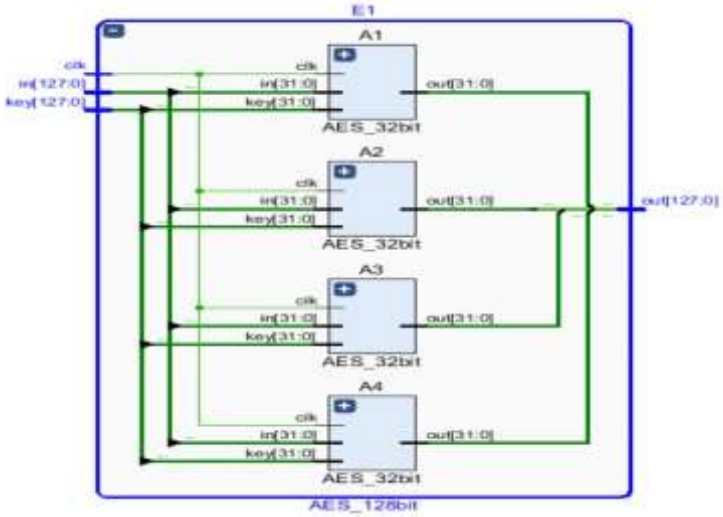
transformations realised through analogous logic structures. Owing to pipelined architecture, multiple data blocks may be processed in overlapping fashion, thereby augmenting throughput.

Data thus encrypted are transmitted securely across communication channels. Upon reception, the corresponding FPGA module decrypteth the ciphertext, restoring the original plaintext. The absence of traditional S-Box tables resulteth in diminished memory utilisation and reduced propagation delay, whilst maintaining algorithmic fidelity. Hence, the system accomplisheth secure and efficient data conveyance suited to modern digital communication environments.

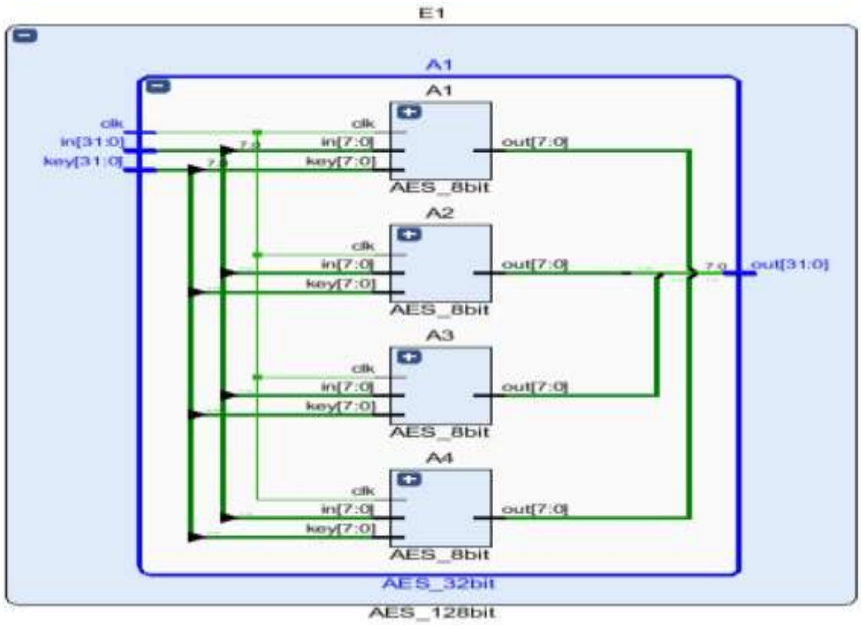
RESULTS&ANALYSIS



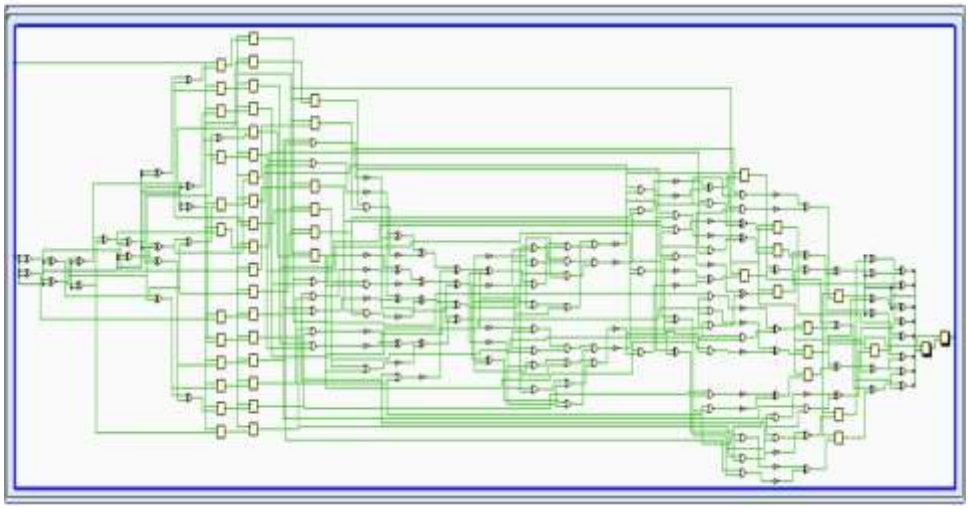
AES FUNCTIONAL DIAGRM



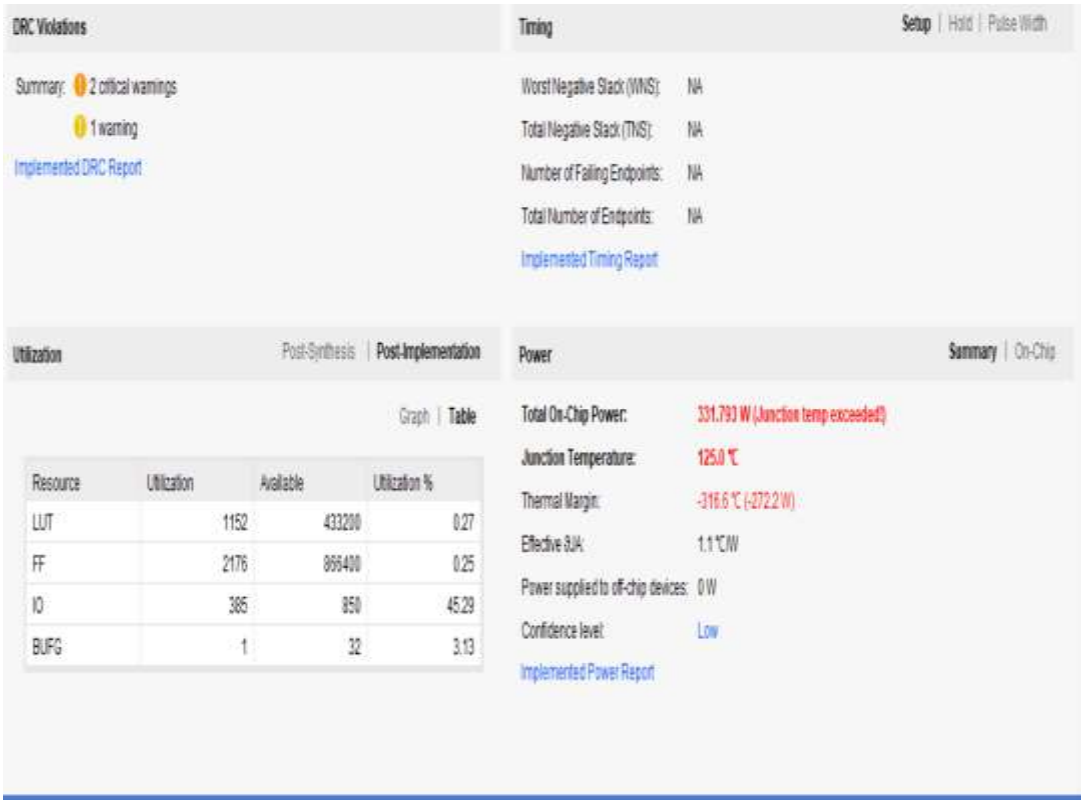
AES-32 BIT Representation



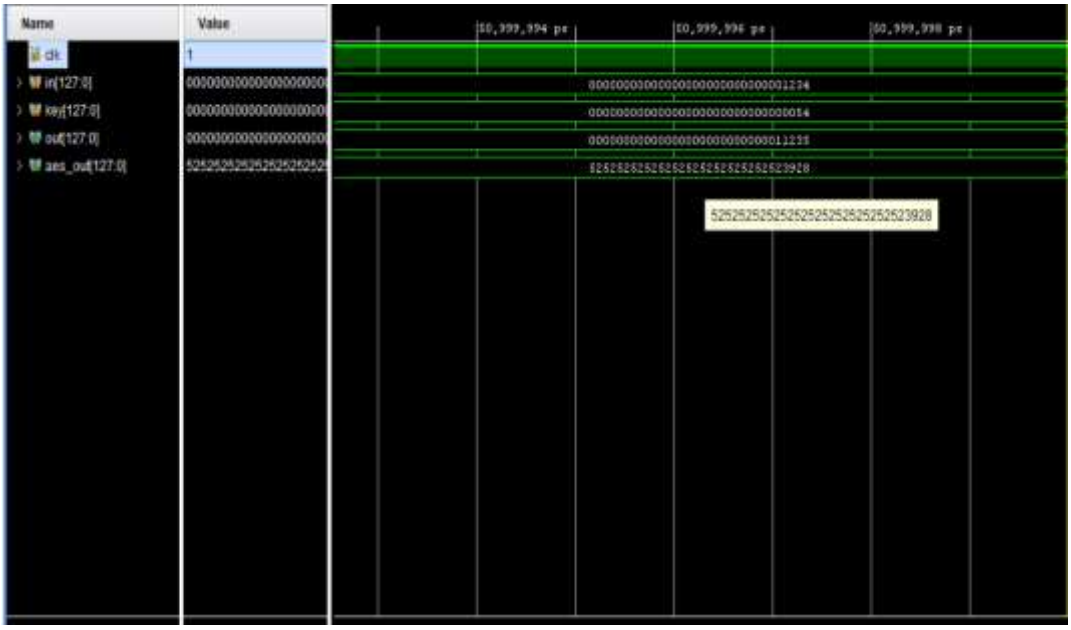
Aes 8-Bit Representation



Each Aes Function Representation


DRC Violations
Summary: 2 critical warnings
1 warning
Implemented DRC Report
Timing
Setup | Hold | Pulse Width
Worst Negative Slack (WNS): NA
Total Negative Slack (TNS): NA
Number of Failing Endpoints: NA
Total Number of Endpoints: NA
Implemented Timing Report
Utilization
Post-Synthesis | Post-Implementation
Graph | Table
Resource Utilization Available Utilization %
LUT 1152 433200 0.27
FF 2176 866400 0.25
IO 385 850 45.29
BUFG 1 32 3.13
Power
Summary | On-Chip
Total On-Chip Power: 331.793 W (Junction temp exceeded!)
Junction Temperature: 125.0 °C
Thermal Margin: -316.6 °C (-272.2 W)
Effective θJA: 1.1 °C/W
Power supplied to off-chip devices: 0 W
Confidence level: Low
Implemented Power Report


DRC Violations
Summary: 2 critical warnings
1 warning
Implemented DRC Report
Timing
Setup | Hold | Pulse Width
Worst Negative Slack (WNS): NA
Total Negative Slack (TNS): NA
Number of Failing Endpoints: NA
Total Number of Endpoints: NA
Implemented Timing Report
Utilization
Post-Synthesis | Post-Implementation
Graph | Table
LUT 1%
FF 1%
IO 45%
BUFG 3%
0 25 50 75 100
Utilization (%)
Power
Summary | On-Chip
Total On-Chip Power: 331.793 W (Junction temp exceeded!)
Junction Temperature: 125.0 °C
Thermal Margin: -316.6 °C (-272.2 W)
Effective θJA: 1.1 °C/W
Power supplied to off-chip devices: 0 W
Confidence level: Low
Implemented Power Report



Simulation Waveform

CONCLUSION

In this study, an FPGA-based high-security data transmission architecture founded upon a 128-bit AES cipher without conventional S-Box implementation hath been presented. By reformulating the substitution stage through algebraic and combinational logic techniques, the design succeedeth in diminishing hardware overhead whilst preserving cryptographic robustness. The architecture demonstrateth improved resource efficiency, commendable throughput, and suitability for reconfigurable platforms. Through judicious pipelining and optimisation, the system reconciles the demands of speed, security, and power economy. Thus, the proposed framework standeth as a viable and efficient alternative for secure digital communication in contemporary embedded and high-performance systems.

REFERENCES

1. Madakam, Somayya, R. Ramaswamy, and Siddharth Tripathi. “Internet of Things (IoT): A literature review.” Journal of Computer and Communications 3, no. 05 (2015): p.164.
2. Wang, Yong, Garhan Attebury, and Byrav Ramamurthy. “A survey of security issues in wireless sensor networks.” IEEE Communications Surveys Tutorial (2006).
3. Veeramallu, B., S. Sahitya, and Ch LavanyaSusanna. Veeramallu, B., S. Sahitya, and Ch LavanyaSusanna. “Confidentiality in Wireless sensor Networks.” International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-6, January 2013.
4. Eisenbarth, Thomas, and Sandeep Kumar. “A survey of lightweightcryptography implementations.” IEEE Design & Test of Computers 24.6 (2007).
5. Banik, Subhadeep, Andrey Bogdanov, and Francesco Regazzoni. “Exploring energy efficiency of lightweight block ciphers.” International Conference on Selected Areas in Cryptography. Springer, Cham, 2015.
6. Bogdanov, Andrey, et al. “PRESENT: An ultra-lightweight block cipher.” CHES. Vol. 4727. 2007.

7. Borghoff, Julia, et al. "PRINCEa low-latency block cipher for pervasive computing applications." International Conference on the Theory and Application of Cryptology and Information Security. Springer, Berlin, Heidelberg, 2012.
8. Beaulieu, Ray, et al. "The SIMON and SPECK lightweight block ciphers." Design Automation Conference (DAC), 52nd ACM/EDAC/IEEE. IEEE, 2015.
9. Erukude, S. T., & Marella, V. C. (2025, September). Multimodal Detection of Fake Reviews using BERT and ResNet-50. In 2025 4th International Conference on Innovative Mechanisms for Industry Applications (ICIMIA) (pp. 877-882). IEEE.
10. Mallick, P. (2020). Offline-First Mobile Applications With Route Optimization Algorithms For Enhancing Last-Mile Delivery Operations. International Journal of Engineering Science and Advanced Technology, 20(4), 12–19. https://doi.org/10.64771/ijesat.2020.v20.i04.pp12-19.
11. Shibutani, Kyoji, Takanori Isobe, Harunaga Hiwatari, Atsushi Mitsuda, Toru Akishita, and Taizo Shirai. "Piccolo: An ultra-lightweight blockcipher." In CHES, vol. 6917, pp. 342-357. 2011.
12. Prodduturi, S. M. K. (2024). Investigating the challenges and opportunities of cybersecurity in the era of remote work. European Journal of Advances in Engineering and Technology, 11(10), 80-84.
13. Explainable AI Framework for Policy-Compliant Anomaly Detection in Data Pipelines. (2025). Inaternational Journal of Communication Networks and Information Security, 16(4). https://doi.org/10.48047/ijcnis.16.4.2111.
14. Descriptions of SHA-256, SHA-384, and SHA-512. http://csrc.nist.gov/groups/STM/cavp/documents/shs/sha256-384- 512.pdf.
15. Kawle, Pravin, et al. "Modified Advanced Encryption Standard." International Journal of Soft Computing and Engineering (IJSCE) 4 (2014).
16. Al Hasib, Abdullah, and Abul Ahsan Md Mahmudul Haque. "A comparative study of the performance and security issues of AES and RSA cryptography." Third International Conference on Convergence and Hybrid Information Technology, 2008. Vol.2.
17. Todupunuri, A. (2025). IMPROVING CUSTOMER EXPERIENCE WITH MODERN BANKING SOLUTIONS. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5120615.
18. Gaddam, S. (2024). Integrating machine learning models with continuous integration and continuous delivery (CI/CD) pipelines for a learning-driven approach to software engineering.
19. Ganji, M. (2025). Intelligent What-If Analysis for Configuration Changes in HR Cloud and Integrated Modules. International Journal of All Research Education and Scientific Methods, 13(04), 4828–4835. https://doi.org/10.56025/ijaresm.2025.1304254828
20. Hocquet, Cdric, Dina Kamel, Francesco Regazzoni, Jean-Didier Legat, Denis Flandre, David Bol, and Franois-Xavier Standaert. "Harvesting the potential of nano-CMOS for lightweight cryptography: an ultra-lowvoltage 65 nm AES coprocessor for passive RFID tags." Journal of Cryptographic Engineering 1, no. 1 (2011): p.79-86.

21. Kerckhof, Stphanie, Franois Durvaux, Cdric Hocquet, David Bol, and Franois-Xavier Standaert. “Towards green cryptography: a comparison of lightweight ciphers from the energy viewpoint.” Cryptographic Hardware and Embedded SystemsCHES 2012 (2012): p.390-407.
22. Batina, Lejla, et al. “Dietary recommendations for lightweight block ciphers: power, energy and area analysis of recently developed architectures.” International Workshop on Radio Frequency Identification: Security and Privacy Issues. Springer, Berlin, Heidelberg, 2013.
23. Banik, Subhadeep, Andrey Bogdanov, and Francesco Regazzoni. “Exploring the energy consumption of lightweight blockciphers in FPGA.” International Conference on ReConFigurable Computing and FPGAs (ReConFig), 2015 , pp.1-6.
24. Kong, Jia Hao, Li-Minn Ang, and Kah Phooi Seng. “A comprehensive survey of modern symmetric cryptographic solutions for resource constrained environments.” Journal of Network and Computer Applications 49 (2015): p.15-50.
25. Wenceslao Jr, Felicisimo V., et al. “Modified AES Algorithm Using Multiple S-Boxes.” The Second International Conference on Electrical, Electronics, Computer Engineering and their Applications (EECEA2015). 2015.