Title of the Research Paper Goes Here

Author Name
Department, Institution
City, Country
Email / ORCID

***Abstract*—Word Count: 180–190 words (strict IEEE rule).**

Pedagogical Purpose of Abstract: The abstract is not an introduction. It is a **compressed scientific argument summarizing the *entire paper*.**

A reviewer often decides whether to read the paper **only from the abstract.**

Mandatory Abstract Flow (do NOT change order):

Sentence 1 – Context / Hook State why the general problem matters (industry, society, scalability, security, efficiency).

Sentence 2–3 – Problem Gap Identify exactly what is missing, inefficient, insecure, or poorly handled in existing work.

Sentence 4–6 – Proposed Approach Describe what you propose at a conceptual level (no implementation details).

Sentence 7–8 – Results State quantitative improvements (percentage, latency, accuracy, cost).

Sentence 9 – Conclusion / Future Scope Mention one logical extension.

Common Rejection Triggers: No numbers, vague claims, buzzwords, citations, equations, or undefined acronyms.

***Index Terms*—Provide 4–6 keywords aligned with IEEE taxonomy and indexing systems.**

I. Introduction

Length: 500–600 words

Teaching Insight: The introduction answers ONE reviewer question: *"Why should I care about this paper?"*

Required Logical Structure (Paragraph-by-Paragraph):

Paragraph 1 – Big Picture Introduce the broader domain and why it is important today.

Paragraph 2 – Technical Background Explain only the concepts needed to understand the problem (assume a technical reader).

Paragraph 3 – Existing Approaches Summarize how the problem is currently addressed (without deep critique yet).

Paragraph 4 – Problem Gap Clearly state 2–3 concrete limitations of existing solutions.

Paragraph 5 – Motivation Explain why these limitations matter in practice or theory.

Paragraph 6 – Proposed Direction Briefly explain what your paper does to address these gaps.

Paragraph 7 – Paper Organization Describe what each section contains.

DO NOT include: Results, equations, tables, implementation details.

A. Main Contributions and Novelty

Exactly 5 bullet points (IEEE expectation).

Each bullet must:

- Start with a strong verb (Propose, Design, Develop, Analyze)
- Describe ONE contribution
- Clearly state novelty (what was not done before)

Weak bullets = guaranteed rejection.

II. Literature Review

Length: 600–800 words

Teaching Insight: This section proves you understand the research landscape better than the reviewer.

Correct Writing Strategy:

- Group studies by methodology, not by author
- Compare ideas, not papers
- Highlight limitations related to YOUR problem

Mandatory Elements:

- At least one literature summary table
- At least one comparative feature table

Common Mistake: Describing papers without synthesis or critical analysis.

III. Problem Statement

Length: 150 words

Teaching Insight: This section converts motivation into a **formal research problem**.

Must Explicitly State:

- System assumptions
- Constraints
- Threats / failure cases
- One clear problem definition sentence

No solutions allowed here.

IV. Proposed Methodology / Model

4–5 subsections, 60–100 words each

Teaching Insight: This is where reviewers decide if your idea is real or hand-wavy.

Each Subsection Must Answer:

- What is this component?
- Why is it needed?
- How does it interact with others?

Equations: Use equations to formalize logic, not to show mathematical skill.

$$y^* = \arg\max_y P(y|x) \tag{1}$$

Figures:

- One architecture diagram
- One workflow/flowchart

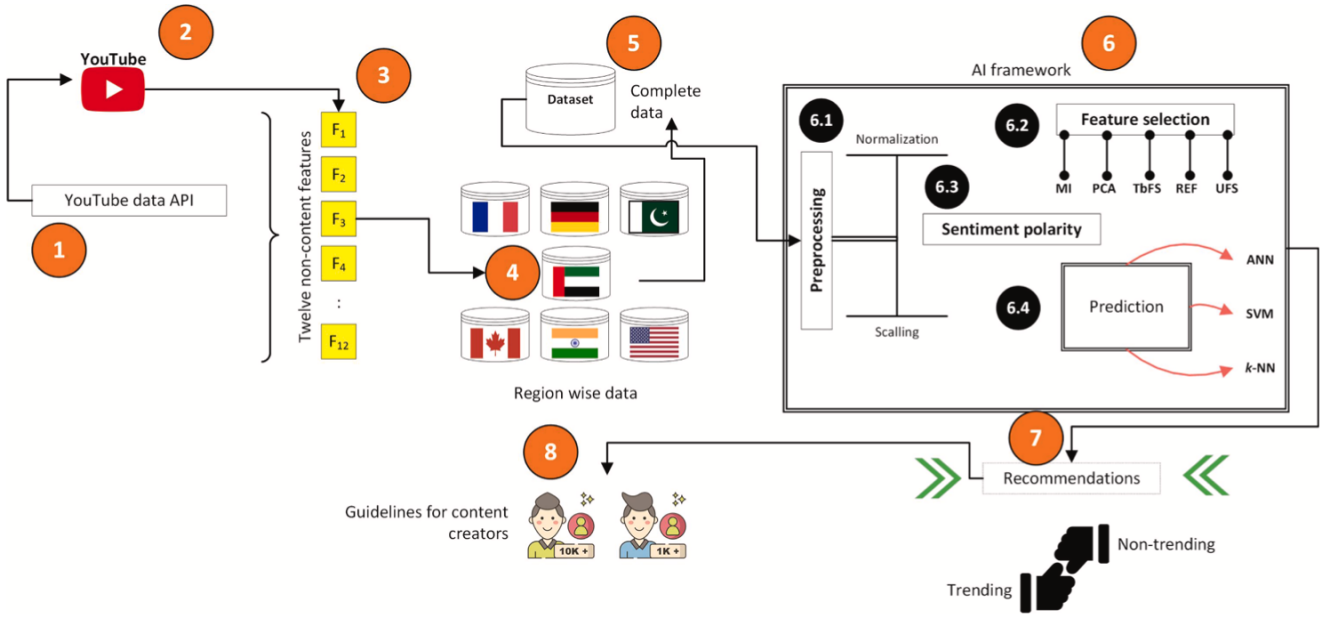

Fig. 1. The overall working of the proposed solution.

Fig. 1. Figure showing the flowchart proposed for FCN-8 quantization and the comparison pipeline followed (for quantization technqiues, i.e., Direct Quantization, Llyod's Quantizer and L_2 error minimization) in the current study based on pixel accuracy, mean IOU, and mean accuracy.

V. Implementation Details

Length: 50 words
Purpose: Enable reproducibility without clutter.
Include ONLY: OS, CPU, RAM, tools, libraries, datasets.

VI. Results and Discussion

Highest-weight section for acceptance.
Must Contain:

- Quantitative metrics
- Baseline comparison
- Interpretation of results

Teaching Rule: Never present a graph without explaining WHY it looks that way.

VII. Complexity / Security / Privacy Analysis

Domain-dependent but highly recommended.
Explain computational cost, attack resistance, or scalability.

VIII. Limitations

Mandatory for strong papers.
Teaching Insight: Acknowledging limitations increases reviewer trust.

IX. Conclusion

Length: 200–250 words
Required Flow:

- Restate problem
- Summarize contributions
- Highlight quantitative outcomes
- Mention future work (30 words)

Acknowledgment

Optional institutional or funding support.

References

Minimum 11–12 references, mostly from last 5 years.

TABLE I
RECENT PROPOSED MODELS IN LITERATURE WITH POSSIBLE LIMITATIONS

Ref No.	Proposed Model	Tools/Technology	Experimentation	Contributions	Limitations
[?]	Privacy-Enhanced Revocable DID Scheme	BLS/ECC Signatures, Blockchain, Threshold Cryptography	Theoretical and comparative analysis of credential unlinkability	Enables revocable and unlinkable DIDs with privacy guarantees	No real deployment or runtime benchmarking
[?]	ZKP-Based Identity System	zk-SNARKs, Ethereum, Verifiable Credentials	Prototype-based identity verification with selective disclosure	Demonstrates privacy-preserving identity using blockchain	Limited performance testing; access control logic not detailed
[?]	IoT Identity Privacy via ZKP and Secret Sharing	ZKPs, Shamir Secret Sharing, Blockchain	Security analysis for IoT identity in decentralized setups	Combines ZKPs with threshold sharing for IoT DID protection	No prototype or real-world validation
[?]	Universal Blockchain Identity Framework (BlockSafe)	ZKPs, DID, Trust Anchors	Conceptual model with architecture design	Proposes scalable blockchain-based identity for smart cities	Lacks empirical testing or performance data
[?]	zk-creds: Issuer-Agnostic ZKP Credential Toolkit	Merkle Trees, ZKPs, Multi-Issuer VC Model	Toolkit tested for credential flexibility and interoperability	Enables ZKP-based VC proofs without issuer lock-in	Performance evaluation is preliminary
[?]	BADIMAC: Decentralized Access Control with DID	Blockchain, VCs, Smart Contracts, DID	Prototype workflow for access decisions in decentralized apps	Integrates DID and VC with on-chain access enforcement	Limited scalability and real-world evaluation

TABLE II
COMPARISON - PROPOSED MODEL VS PREVIOUS MODELS

Ref.	**Data Processing**	**Verification**	**Pattern Analysis**	**Security**	**Decentralized**	**Dynamic Routing**	**Decision Making**	**Adaptive Network**
[?]	✓	✓	✓	X	X	X	✓	X
[?]	✓	✓	✓	X	X	X	✓	X
[?]	✓	✓	✓	X	X	X	✓	X
[?]	✓	✓	✓	✓	X	X	✓	X
[?]	✓	✓	✓	✓	X	X	✓	X
Proposed Model	✓	✓	✓	✓	✓	✓	✓	✓

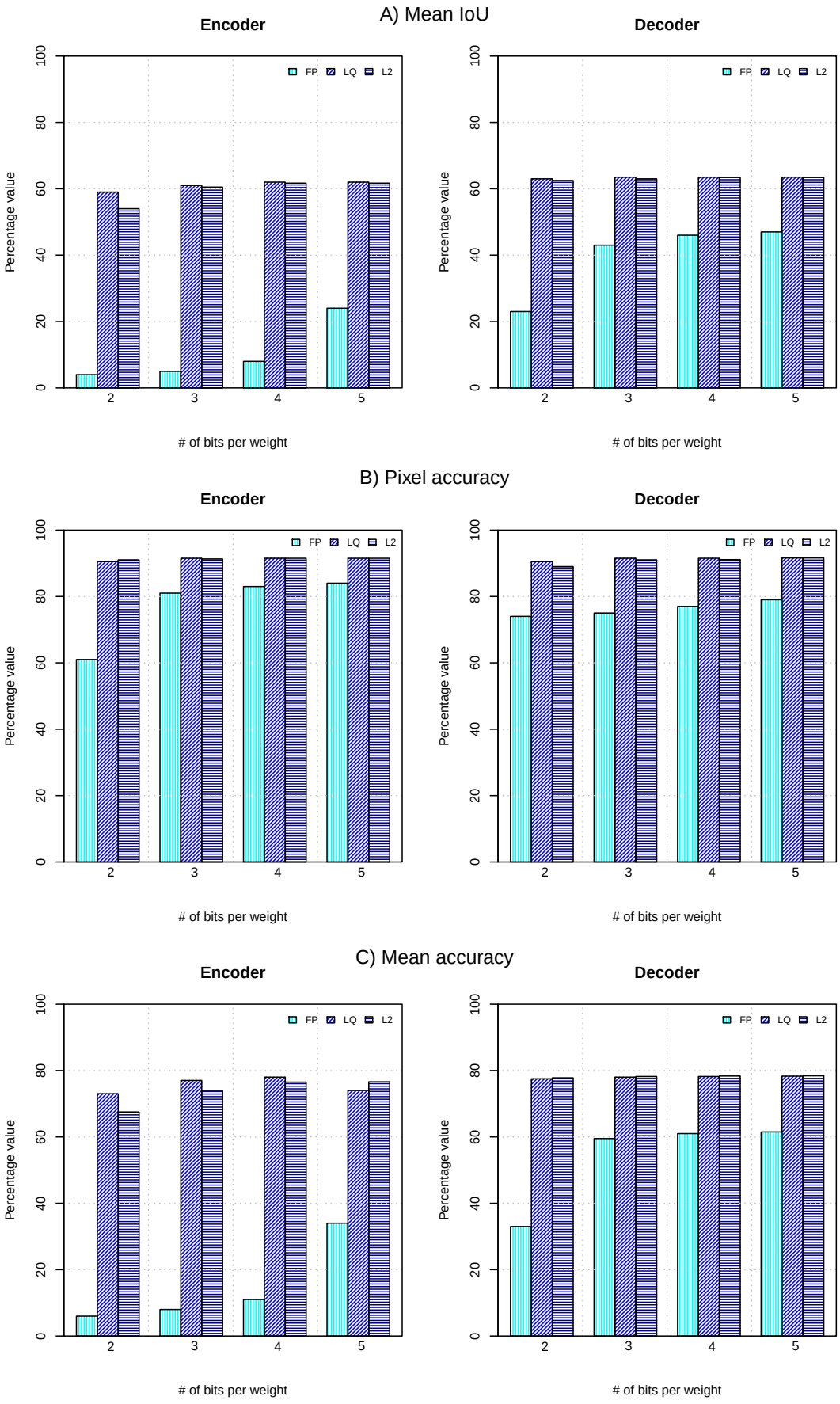

Fig. 2. Results