**🔹 1. Problem Background**

* **Software-Defined Networking (SDN):**  
  SDN separates the control plane (controller) from the data plane (switches/routers).  
  → This flexibility comes with **new security risks**, especially because the centralized controller is a single point of attack.
* **Weakness of traditional models:**  
  Perimeter-based defenses (firewalls, VPNs) can’t stop insider threats or lateral movements inside the network.
* **Zero Trust Architecture (ZTA):**  
  Principle of *“never trust, always verify”*. Every request must be authenticated and authorized dynamically.

**🔹 2. Proposed Solution: ZSDN-Guard**

The paper proposes a **zero-trust security framework for SDN**, integrating:

* Zero Trust principles
* Deep learning anomaly detection
* Fine-grained, dynamic trust evaluation

**Core Components:**

1. **Data Collection Module** – gathers logs, configs, and access requests.
2. **Dynamic Trust Evaluation** – computes trust scores per user (with decay over time).
   * Example thresholds: 0.55 (browse), 0.75 (download), 0.85 (upload), 0.90 (admin).
3. **Anomaly Detection Engine (NetSeqDL)** – CNN + Attention + LSTM sequence model for traffic analysis.
4. **Adaptive Access Control** – grants/denies resources based on trust score & anomaly results.
5. **Secure Communication Module** – establishes cryptographic, two-way authenticated channels.

**🔹 3. Novel Contributions**

* **ZSDN-Guard framework:** End-to-end Zero Trust for SDN.
* **NetSeqDL model:** A deep learning anomaly detector (CNN + Attention + LSTM).
  + Accuracy: ~99.65%
  + False alarm rate: ~1.18%
  + Outperforms classical ML (SVM, RF, CNN) and prior DL models.
* **ZeroSimNet platform:** A Mininet-based testbed to simulate attacks (DDoS, port scans) and defenses.

**🔹 4. Experiments & Results**

* **Simulation setup:**
  + Mininet + Ryu SDN controller
  + Attack tools: Nmap (port scanning), hping3 (DDoS floods)
* **Key Findings:**
  + Without protection: throughput collapsed (<1% under DDoS).
  + With ZSDN-Guard: maintained ~80–85% throughput (~3.1 Gbps).
  + Port scanning attempts returned *“filtered”* (blocked before verification).
* **Traffic anomaly detection:**
  + Accuracy = 99.65%
  + Higher than RF (97.5%), CNN (98.8%), LSTM (≈98%)
  + Superior ROC curve (higher TPR, lower FPR).

**🔹 5. Takeaways**

* **Zero Trust + Deep Learning** works well for SDN, addressing insider threats and dynamic traffic anomalies.
* **ZSDN-Guard** successfully:
  + Mitigates DDoS and scanning attacks.
  + Provides dynamic trust-based access control.
  + Keeps high throughput and low false positives.
* **Future Work:** Apply to larger/more complex real-world networks, further optimize models.

**🔹 6. Why This Matters**

* In real SDN deployments (cloud, 5G, IoT), traditional perimeter defenses fail.
* This framework shows how AI + Zero Trust principles can **practically harden SDN** without huge performance loss.
* Provides a roadmap for **intelligent, adaptive, software-defined security** in next-gen networks.