Architecting the Neural Network for CVS Health

February 12, 2025

PRESENTED BY: TEAM 17

Daryn Imashev, Gillis Wang, Isabella Chen, Nikita Suryawanshi, Jackson Sui

Agenda

Intro of the connectionist approach

Well-suited source of value

Architect the neural network

Challenges

CONNECTIONISM MODELS

Artificial neural networks inspired by biological brain structure.

Distributed Parallel Processing

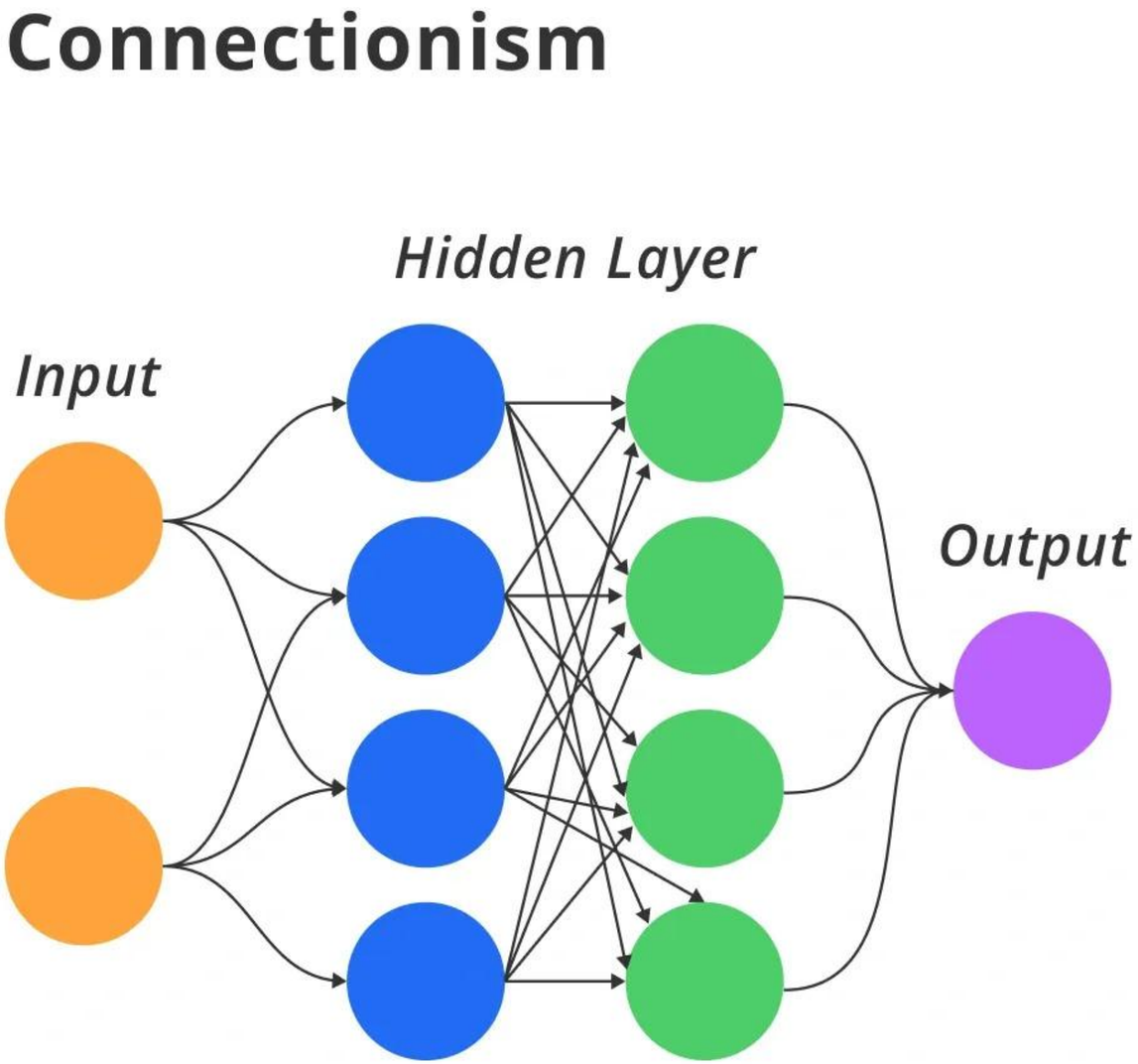
Information flows through interconnected nodes(artificial neurons)

Adaptive Learning

Modifies connection weights through exposure to data

Emergent Behavior

Complex capabilities arise from simple unit interactions



FRAUD DETECTION SYSTEM IN CVS

Financial Protection and Risk Mitigation
Briefly elaborate on the proposed recommendation

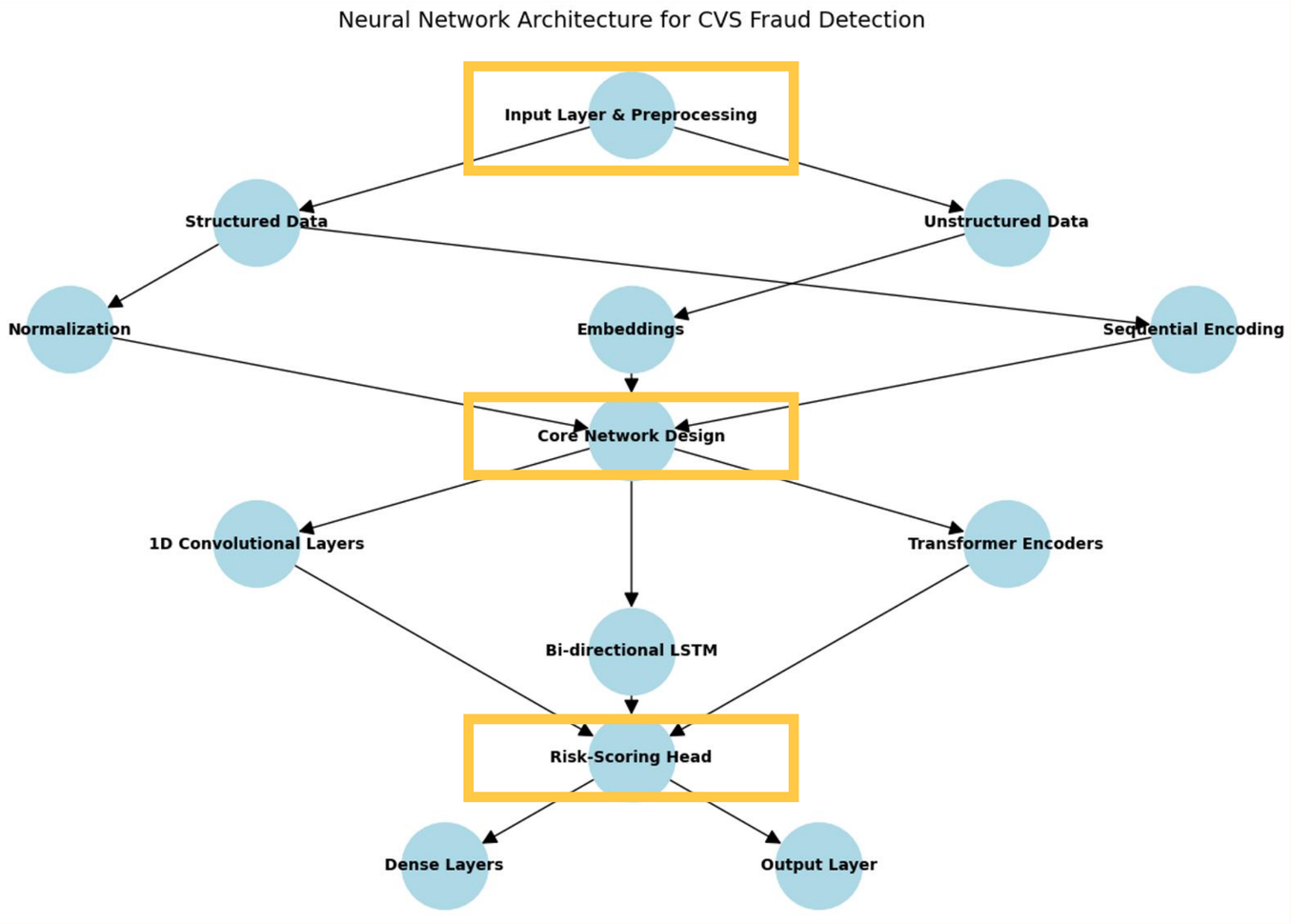
Customer Trust and Data Security
Briefly elaborate on the proposed recommendation

Adaptive and Intelligent Fraud Prevention
Briefly elaborate on the proposed recommendation

OPTIMIZING FRAUD PREVENTION THROUGH NEURAL NETWORK DYNAMICS

Pattern Recognition	Adaptive Learning	Data Rich Environment
• **Core Detection Capability:** Fraud detection systems require identification of complex patterns and anomalies across massive transactional datasets. • **Architectural Advantage:** Connectionist approaches demonstrate superior performance to traditional method.	• **Evolving Threat Challenge:** Fraud patterns demonstrate constant mutation, requiring detection system to continuously update their recognition parameters. • **Dynamic Learning Response:** Connectionist architectures automatically retrain on emerging fraud signatures, maintaining detection efficacy where rigid rule-based systems fail.	• **Scalability Imperative:** Fraud detection systems must process exponentially growing transactional data streams with increasing dimensionality. • **Architectural Optimization:** Connectionist frameworks inherently scale with data volume, leveraging distributed representations to extract predictive signals from noise-dense environments.

NEURAL NETWORK ARCHITECTURE FOR CVS FRAUD DETECTION



Phase 1: Input data and preprocess

Preprocessing standardizes structured and unstructured data (prescription records, purchase histories, staff annotations) through normalization, embeddings, and sequential encoding.

Phase 2: Processing

Analyzes temporal anomalies in structured data, flags suspicious language patterns in unstructured text, and tracks sequential behaviors across multiple locations to identify potential fraud.

Phase 3: Output

Identify the likelihood of fraud and combine all the data to produce a fraud risk score.

MITIGATE THE KEY CHALLENGES

Class Imbalance	Focal Loss for Hard-to-Classify Cases	Weight fraud instances higher than legitimate transactions, aligning with CVS's historical fraud rates.
Evolving Fraud Tactics	Online Learning with Memory Replay	Retrain the neural network weekly using CVS's centralized fraud database, incorporating new attack patterns.
Real Time Constraints	Training a Smaller, Faster Model (Model Distillation)	CVS runs a faster, optimized version that can quickly analyze transactions and detect frauds.
Regulatory Compliance	Add a Layer of Privacy During Training	Add some noise during training to obscure individual patient data while retaining fraud detection capabilities.

Thank you for listening!

Do you have any questions?