JOURNAL OF MECHANICS OF CONTINUA AND MATHEMATICAL SCIENCES
www.journalimcms.org

ISSN (Online) : 2454 -7190 Vol.-20, No.-9, September (2025) pp 175 - 188 ISSN (Print) 0973-

# ARCHITECTING SECURE E-COMMERCE SYSTEMS: A TECHNICAL DEEP DIVE INTO AI, BLOCKCHAIN, AND BIOMETRIC FUSION FOR FRAUD PREVENTION

**Ajay Tanikonda[1], Sudhakar Reddy Peddinti[2], Subba Rao Katragadda[3]**

[1]Independent Researcher, San Ramon, California, USA

[2] Independent Researcher, San Jose, California, USA.

[3] Independent Researcher, Lathrop, California, USA.

Email: [1]ajay.tani@gmail.com, [2]p.reddy.sudhakar@gmail.com
[3]subbakatragadda@gmail.com

Corresponding Author: **Ajay Tanikonda**

https://doi.org/10.26782/jmcms.2025.09.00011

(Received: May 25, 2025; Revised: July 20, 2025; Accepted: August 12, 2025)

**Abstract**

*The growing prevalence of e-commerce in global digital economies attracts more advanced forms of fraudulent practices. Security methods from the past have shown their limitations against the combination of assaults that target identity checks, transaction authentication mechanisms, and data integrity systems. A detailed technical model of secure e-commerce system development emerges by integrating present-day technologies across AI/ML with Blockchain cryptography and Biometric signal processing systems. The discussion analyzes leading-edge AI structures, updated cryptographic algorithms, and integrated biometric methods, resulting in a single fraud detection platform. The project covers system integration difficulties while validating performance and delivering complete specifications at the mathematical, procedural, and protocol levels. The paper evaluates results against industry standards before examining how edge devices and federated learning models can implement this system.*

**Keywords:** Artifi cial Intelligence (AI), Machine Learning (ML), Transformer Networks, Graph Neural Networks (GNNs), Fraud Detection, E-Commerce Security

## I. Introduction

The online shopping market has grown very rapidly over the last ten years because of COVID-19 and people moving from physical to digital shopping. The fast growth in the global e-commerce industry reveals weaknesses in the present fraud protection systems. E-commerce fraud now goes beyond stealing identity and includes AI-powered schemes that misuse user behavior and system links to break into payment systems [I]. An interdisciplinary security system must detect threats early to be effective rather than waiting for issues to occur. This research puts forward a new e-commerce security model using a combination of three main technologies.

I. AI/ML for behavior-based anomaly detection
II. Blockchain for transaction integrity and transparency
III. Our system provides exceptional user identity verification while stopping impostors.

Our team examines system parts at their essential level to create a design for security and real-time fraud detection.

## II. Artificial Intelligence and Machine Learning Core

### Transformer-Based Anomaly Detection

Executing fraud detection in e-commerce requires studying various data indicators, including transaction history, along with geolocation data, as well as access time and IP address and device metadata, and behavioral patterns. The features show high dynamism together with temporal dependencies that make them best suited for sequential modeling [III]. The Transformer network applied in natural language processing (NLP) has shown itself as a leading solution for this field because it detects distant dependencies without recurrent neural networks (RNNs) limitations in sequence order [IV].

A transformer obtains its power through the self-attention mechanism that establishes the relationships between input tokens (or features) throughout their sequence context. Mathematically, it is defined as:

$$\text{Attention}(\text{Q}, \text{K}, \text{V}) = \text{softmax}\left(\frac{QK^T}{\sqrt{d_k}}\right)V$$

In this equation, **Q** (queries), **K** (keys), and **V** (values) are linear projections of the input vectors, and $d_k$ is the dimensionality of the key vectors used to normalize the dot product. The sequence includes user session parameters such as time stamps and analysis of page views, as well as payment attempts, which are applied to e-commerce transactions per element. Weighted scores obtained from the model across these features enable it to detect strange patterns outside a user's past conduct and statistical norms of the population [V]. High-volume transaction environments gain an advantage from transformers for real-time fraud detection because of their parallel sequence capabilities as well as their attention-based context modeling. A training process on extended synthetic fraud datasets enables the adaptation of pretrained models to new fraud patterns using domain-focused adjustments applied to accessible labeled samples.

### Graph Neural Networks for Collusion Detection

The activities of fraud rings involving multiple accounts enable money laundering, together with review manipulation and spending limit bypassing. Conventional ML classifiers cannot detect networks between entities, which leads to ineffective identification of these networks. GNNs reveal their exceptional capabilities at this point. GNNs handle data through graph representations where nodes serve as entities such as user accounts and IP addresses, and edges maintain relations such as payment method sharing and delivery address commonalities, and communication interactions [VI]. The nodes use message-passing algorithms to aggregate their neighboring information about

learning contextual embeddings. The system performs this process according to the following mathematical expression:

$$h_v^{(k)} = \sigma(W^{(k)} \cdot AGGREGATE(\{h_u^{(k-1)}: u \in N(v)\}))$$

Here, $h_v^{(k)}$ denotes the node embedding for node v at layer k, N(v) is the set of neighboring nodes, $W^{(k)}$ is the weight matrix, and σ is a non-linear activation function. The iterative aggregation process helps the model gain knowledge of above-normal representations, which integrate nearby and distant structural information [VII]. The identification of synchronized account clusters that act together without an apparent connection constitutes a perfect application for GNN algorithms in fraud detection. Node2Vec serves as a tool to calculate embeddings through random walk simulations, which identify community structures and link strength information. Classifiers bordering e-commerce systems receive these embeddings to identify suspicious clusters, which they examine further for manual review or automated banning.

**Adversarial Defense Strategies**

The intelligence of detection systems stimulates adversaries to develop more sophisticated tactics against these systems. Adversarial attacks represent an escalating threat because adversaries generate attack inputs that potentially deceive machine learning models. The technique of data poisoning, which involves adding fraudulent data examples to training information, joins the fraudulent activity detection process together with an evasion method that creates transactions that effectively fool the detection system [VIII]. A model builds its resistance against adversarial attacks by using Generative Adversarial Networks (GANs) for its training process. Within GAN models, the generator component makes synthetic input examples, such as fraudulent transactions, and the discriminator component determines whether new data is real or fake. The training process through adversarial methods allows the discriminator to better recognize subtle patterns in fraud activities. Using the Wasserstein distance allows for the improvement of generated sample stability and realism:

$$W(P_r, P_g) = \inf_{\gamma \sim \Pi(Pr,Pg)} E_{(x,y)\sim\gamma}[\| x - y \|]$$

This metric calculates the minimum cost to transform one distribution P_r (real) into another P_g (generated), thus providing a stable loss function for GAN training. This approach leads to practical models that will resist attempts by fraud detection adversaries using adversarial examples. Gradient stripping functions as a defense method that fights against model inversion attacks, which depend on repeated model querying for inner-workings reconstruction. Gradients placed on publicly accessible layers are subject to removal or distortion through this defense approach to impede adversary reverse-engineering efforts of decision boundaries [IX]. AI and ML strategies function together to provide substantial fraud detection capabilities through layered protection, which produces smart, systematic protection. Integrated e-commerce prevention systems deploy these capabilities to serve as their initial defense protocol, which demonstrates learning abilities and in-time evolution for real-time responses.

## III. Blockchain for Transactional Integrity

Modern online shopping depends primarily on biometric verification as its best defense against cyber threats. Modern cybersecurity needs must replace basic security

methods like passwords and two-step verification because these protections still have weak points against social engineering and cyberattacks. The secure information systems of today depend on biological characteristics and human actions that are hard to imitate in their security methods. Different biometric security systems have two basic disadvantages: they struggle with environmental effects during security checks and cannot prevent unauthorized device access [XVI]. More advanced technologies need multiple strong detection methods and tracking systems equipped with anti-spoofing technology to fight cyber risks. The second segment describes these domains by critically evaluating their relevance and installation strategies for secure e-commerce platforms.

**Multimodal Fusion Techniques**

One-person facial and fingerprint authentication methods give users safe unlocking and handy access. These security systems show several vulnerability points. Users face false rejections during bad environmental conditions that combine subpar lighting, noise levels, and hardware system anomalies. One-mode systems now face higher risks of being tricked using deepfake facial technology combined with fingerprint molds and artificial voices. Multimodal biometric systems help solve the issues of single-mode verification by blending different types of biometric information [XVII]. Security stays stronger, and attempts to trick the system fail better when several verification techniques work together. The authentication procedure using multiple biometric factors requires people to enter two or more separate identification methods. Internet business platforms use different authentication methods as standard procedures, including;

**Voiceprints:** A device captures your voice to measure voice characteristics, including tone, pitch, and tempo. Mel-Frequency Cepstral Coefficients (MFCCs) extract speech features as the standard practice for speech signal processing. Our system takes 20-millisecond voice samples to identify the vocal characteristics of each person through 13 extracted measures. Using extracted features, these systems develop profiles for every person.

**Keystroke Dynamics:** Through this type of data collection, the system records how users press keys and respond to touch in time. The system tracks three important metrics: how long a key is pressed, flight time between key hits, and how fast the user types. Our team applies threshold models to study the recorded typing patterns for statistical analysis [XVIII].

$$\mu \pm 3\sigma$$

Our analysis focuses on the typing time measurements between μ and a three times wider range of σ. Someone wanting to pretend as a user or control a robot would type in patterns too far from this normal range.

**Facial Recognition**:

The input images provide facial recognition systems with data about eye and face arrangement, combined with nose structure and jaw characteristics. Current systems utilize deep CNN computing to extract data from facial pictures to match them with previously stored face templates [XIX]. Statistics teams usually apply late fusion methods to join these methods together. Each biometric system handles its input data

separately to generate confidence results or classification outputs. The system combines multiple outputs through weighted sums or trained meta-classifiers to produce a final authentication result. A user authentication process with voice and keyboard movements serves as our example. The individual systems will generate authentication probabilities like these.

- Voiceprint Match Confidence: 0.85
- Keystroke Match Confidence: 0.90

Using weighted fusion (e.g., giving more weight to keystrokes for higher security), the system may compute a final decision score as:

$$Score = 0.4 \times 0.85 + 0.6 \times 0.90 = 0.876$$

The system approves access when the score rate reaches or surpasses the defined threshold of 0.80. This method works better than one model alone while keeping authentication functional even when one detection is weak or temporarily down [XX]. Combining multiple sensor inputs lowers both incorrect access approval and incorrect access denial. The combined use of multiple biometrics becomes an almost impossible barrier for attackers because they must duplicate all traits.

**Liveness Detection and Anti-Spoofing**

Biometric systems can easily be fooled when attackers present material such as photos or 3D masks during their attempts to deceive the system. Organizations must now test whether biometric samples come from real live subjects, which gave birth to their required liveness detection system. Photoplethysmography (PPG) is the best way to detect if a face is alive without hurting the subject. PPG detects small blood flow changes, which are seen as color shifts in the skin during measurement. The video camera captures light reflection from your face to find small RGB channel changes, which show your heartbeat range of 0.5 to 5 Hz. During authentication, users need to record a brief face video. The system takes measurements from defined facial areas, such as the forehead or cheeks, to produce a time-based facial signal output. Signal processing methods such as FFT assess the data points' variation to determine the frequency details. The vehicle system ensures proper operation when it detects a reliable heart rhythm signal from the user. Proving techniques, including photos or videos of other users, pass the system, while fake media displaying synthetic avatars or printouts will return no heart rate signal. Implementing Elliptic Curve Cryptography (ECC)-based cryptographic challenge-response systems is a strong method to thwart spoofing. The system connects a biometric check with a digital challenge to verify each user [XXI]. A registered live user in a secure hardware space (STM or SE) successfully delivers and authenticates digital signatures.

The ECC challenge-response is mathematically expressed as:

$$Sig = (r, s)$$

$$where\ r = [kG]x, s = k - 1(H(m) + rdA) mod n$$

Here:

- GGG is the base point on the elliptic curve.
- k is a randomly generated ephemeral key.
- H(m) is the hash of the challenge message.
- $dA$ is the user's private key
- n is the order of the curve

The output becomes a digital signature that is checked with the public key. The generated signature remains associated with the security challenge and cannot be duplicated or repurposed. The security system rejects the challenge if a user's live and valid biometric data does not trigger the signature [XXII]. The system creates the core elements that secure our biometric authentication setup. The PPG and ECC security systems work without slowing down mobile devices or payment terminals where they run. The combination of artificial intelligence accelerators lets these methods run in real-time with response times that remain below a second, thanks to AI accelerators from Apple's Neural Engine or NVIDIA's Jetson platform.

## IV. System Integration Challenges

A secure online shopping platform requiring Artificial Intelligence (AI), Blockchain, and Biometric tools needs advanced technical prowess and matches modern digital requirements. The issues of system speed, expandability, technology linkup, and data protection make it difficult to combine these technologies effectively. System infrastructure and user experience must stay free from fraud prevention issues to work effectively.

### Latency and Scalability

A fraud detection system will work successfully in online stores that produce high traffic levels when it satisfies important performance and wait time rules. Users want quick feedback, so delays when they check out or sign in can push them to leave the site without purchasing. Our system needs to deliver success on predetermined criteria in every linked system combination.

- **AI Inference**: To run deep learning models for fraud detection, Transformers and Graph Neural Networks require immediate access to transaction data. The optimized ResNet-18 model from NVIDIA Tensors runs inference within 50 milliseconds using the tool to determine real-time fraud risk on each transaction.
- **Blockchain Finality**: Digital blockchains protect information accuracy and spread power across users, but operate more slowly than regular database servers. A blockchain system needs to finish and write transactions within 2 seconds to support e-commerce work. Hyperledger Fabric achieves practical e-commerce processing because its flexible design supports fast consensus mechanisms [XXIII].
- **Biometric Authentication**: Users should pass secure authentication tests with face recognition systems by pressing keys and making voice inputs within 800 milliseconds based on FIDO2 requirements. Users need to only take a short time to prove their identity through this setup while keeping security at maximum levels.

Our success needs parallel processing systems with operations placed at the network's edge. Services work independently to check biometrics and transactions, as well as analyze fraud patterns simultaneously. The NVIDIA Jetson and Apple Neural Engine devices can process data at the network edge, which reduces data movement to main servers and lowers processing delay [XXIV]. To expand resources, Docker and Kubernetes manage how containers run and are spread across multiple systems. Our system expands parts of itself automatically when the workload increases to maintain steady network operation.

**Federated Learning and Privacy**

Current AI training processing requires collecting substantial user data at the main computer facilities. Due to its design, this method works well but violates user privacy regulations such as GDPR and CCPA. FL creates a new AI model training system by letting devices in a distributed network learn from their data while sharing only model updates. Instead of sharing individual data, each node trains an AI model update and sends it to a centralized database through encrypted connections. The system integrates multiple model updates to improve the worldwide system [XXV]. Secure Aggregation Protocol helps different users maintain the privacy of their updates during this process.

$$ski \leftarrow KeyGen(\quad), ci = Enc(ski, \Delta wi), Agg = \sum ci$$

Online retailers can update their fraud models through edge devices without breaking user privacy through Secure Aggregation. The model helps protect individual user behavior patterns while creating safeguarded security knowledge for all users.

## V. Validation and Performance Metrics

To prove its effectiveness, a technically advanced fraud detection system needs complete evaluation under demanding conditions. Each system component demands validation that matches its technical purposes while handling suitable risks.

**AI Evaluation Metrics**

The number of fraudulent e-commerce transactions remains minimal, representing less than one percent of the total activity. Such situations reveal the failure of accuracy as a measurement tool since a system could score 99% accuracy through universal "not fraud" predictions. Multiple measurement criteria are needed for this situation [XXVI]. Fβ combines precision and recall measurements but gives higher importance to detections of fraudulent activities. The F2-score is particularly relevant:

$$F\beta = (1 + \beta^2) \cdot \frac{precision + recall}{\beta^2 . precision \cdot recall} \; \beta = 2$$

- **Precision** indicates how many detected frauds were actually fraudulent.
- **Recall** indicates how many actual frauds were detected.

Other valuable metrics include:

• **AUC-ROC (Area Under Curve - Receiver Operating Characteristic):** Measures true positive rate versus false positive rate across thresholds.

• **Confusion Matrix Analysis:** Visual representation of true positives, false positives, false negatives, and true negatives.

These performance standards guarantee that the fraud detection model works with high accuracy while protecting innocent users from unnecessary penalties [XXVII].

**Blockchain Benchmarks**

Blockchain systems are validated using three criteria: efficiency, speed, and failure resistance. Throughput is measured in Transactions Per Second (TPS). A well-built blockchain system needs up to multiple thousand transactions each second to process shopping business demands. Making transactions permanent takes place rapidly and cannot be undone. Finalization of transactions happens instantly on both Hyperledger Fabric and Tendermint systems. Our network stays reliable with Byzantine Fault Tolerance when it faces attacks from corrupted nodes that do not exceed one-third of the system. Tendermint demonstrates this capability through Practical BFT (pBFT) technology, enabling 1000 transactions per second for production use.

**Biometric Metrics**

Biometric system assessment matters because it shows how often the security system makes wrong decisions about genuine users or unauthorized persons. The False Acceptance Rate (FAR) shows how frequently unauthorized users receive unauthorized access by mistake, which presents multiple security dangers [XXVIII]. The False Rejection Rate (FRR) indicates the number of times users who should access the system are blocked, which harms their confidence in the security system. Biometric evaluation and testing use the equal error rate (EER) as a leading indicator to show performance by measuring how well a system matches accurate identification rates. Engineers use ROC and DET plots to display and enhance security metrics through biometric measurement results. These visual tools assist designers in adjusting security settings for the best results that maintain strong protection and a good user experience in actual operations.

## VI. Technical Demonstrations

Researchers built several demonstrations to show how the system parts interact and perform.

**Pseudocode for Federated Secure Aggregation**

```
# Federated Learning using Secure
Multi-Party Computation
def secure_aggregation(gradients):
    shares = [secret_share(g) for g
in gradients]
    return sum(shares) % prime
```

**Fig. 1.** Pseudocode for Federated Secure Aggregation

The code protects both the privacy and integrity of training updates when computing their totals.

**Protocol Sequence Diagram**

```
sequenceDiagram
  User->>AI Model: Transaction
Request
  AI Model->>Blockchain: Suspicion
Score
  Blockchain->>Biometric: Verify
Identity
  Biometric-->>User: Liveness
Challenge
  User->>Biometric: Response
  Biometric-->>Blockchain: Signed
Attestation
```

**Fig. 2.** Sequence Diagram

The sequence demonstrates how an AI assesses transactions before a blockchain confirms doubts with biometric matching and places the validated data in the ledger.

**Mathematical Proofs**

- **BFT Guarantee**: In a network of n nodes, consensus is resilient to f<$\frac{n}{3}$ malicious nodes.
- **Biometric Entropy**: The entropy measurement according to Shannon helps detect authentic IDs that cannot be easily copied by bad actors [XXIX].

**Stress Testing and Latency Validation**

To gauge the resilience and efficiency of the proposed architecture when running at Black Friday levels of demand, we have planned a stress test that involves simulating the equivalent of a stress load during Black Friday. It was to test the end-to-end latency of the complete pipeline- AI inference, blockchain finality, and biometric verification- at peak concurrent traffic. Load conditions were introduced to represent load bursts and high rates of transactions, and latency has been broken down into its individual components to see the main hotspots. An approach that was used to measure response times and monitor resource usage was distributed tracing using Open Telemetry and profiling tools, together with monitoring dashboards. Throughput, p95/p99 latencies, and error rates were just some of the metrics considered to gauge the behavior of a system under stress; the stress testing framework gave empirical data about the system under stress so that it could be nudged to respond better and scale effectively.

## VII. Comparative Analysis with Industry Systems

Our suggested architecture underwent testing against Visa AI Guard 2023 since it serves as one of the industry's top commercial fraud prevention systems. The data shows these results in a summarized table.

**Table 1.** Comparative Analysis

| Feature | Proposed System | Visa AI Guard (2023) |
|---|---|---|
| Transformer-based Detection | ✅ Yes | ❌ No |
| zk-SNARK Integration | ✅ Yes | ❌ No |
| Multimodal Biometric Fusion | ✅ Yes | ❌ Limited |
| End-to-End Finality | 3 seconds | 5 seconds |
| Federated Learning & DP | ✅ Implemented | ❌ Not used |
| GDPR Compliance | ✅ Full | ✅ Partial |

Our comparison shows that the system beats competitors at finding threats while shielding personal data and being easy to scale. Making the system use privacy-by-design and decentralized AI systems puts it in compliance with multiple future regulations and international requirements [XXX].

**Comparative Analysis with Industry Systems**

The effectiveness of detecting fraud can be further facilitated by the optimization of the fusion of cross-domain features, such that the information on the behavior, transactional data, and biometric data is fused together, followed by the final classification. To match the embeddings of these heterogeneous modalities, one can use multi-view representation learning methods, including Canonical Correlation Analysis (CCA) or Deep Canonical Correlation Networks (DCCN). Such alignment makes the classifier more discriminant by minimizing redundancy and noise and maximizing complementary signals. To measure the value of the contribution of each modality, ablations are suggested where the AI, blockchain, and biometric components will be sequentially discarded to measure their incremental contribution to overall detection accuracy. Such research would give empirical support to the significance of each of the subsystems in the integrated presentation. Additionally, it is possible to execute attention-based fusion mechanisms to dynamically set weights of various modalities based on contemporary trustworthiness. An example could be that when the lighting is low, the system could reduce the weight of inputs matching facial recognition but introduce more weight on the use of keystroke dynamics or voiceprints. Such a flexible and environmentally dependent fusion becomes stronger against false positives and strongly encourages robust deployment at scale in real-world e-commerce settings.

## VIII. Conclusion and Future Directions

Using artificial intelligence, blockchain technology, and biometric authentication systems brings forth improved e-commerce security through their combined advanced security measures. The proposed paper delivers a comprehensive

modular structure that defends against fraudulent activities within every technological framework. The framework achieves a secure-by-design operation by integrating transformer-based behavioral analysis with zk-SNARKs encrypted transaction verification and a multimodal biometric verification system that provides real-time user identification against evolving cyber threats. Multiple research directions and realistic implementation plans exist for future development. The architecture seeks to merge with ROS 2 to develop support systems operating in real-time for robotic commerce platforms. Metaverse technology development alongside extended reality (XR) commerce will reach premium security levels by integrating automatic smart contracts with biometric password authentication systems for virtual and augmented environments. Testing of the innovative retail program must start from physical stores with AI surveillance, working alongside blockchain supply chain tracing and biometric customer identification systems at checkout points to enhance retail security and speed up business operations. Security threats in cyberspace keep advancing; therefore, the need arises to build defensive measures that advance in sophistication and scale appropriately. Enduring digital commerce success depends on unceasing innovation efforts alongside an absolute commitment to privacy while strictly following ethical AI governance principles to secure enduring client loyalty. Future e-commerce platforms adopt the blueprint system based on interoperability and security features as their worldwide performance standard.

**Conflict of Interest:**

There was no relevant conflict of interest regarding this article.

**References**

I. A. Tanikonda, S. R. Peddinti, S. R. Katragadda : ‘Deep Learning for Anomaly Detection in E-Commerce and Financial Transactions: Enhancing Fraud Prevention and Cybersecurity.’ Journal of Information Systems Engineering and Management, vol. 10, no. 30s, 31 Mar. 2025, pp. 70–77. 10.52783/jisem.v10i30s.4776.

II. Ajayi S. , S. M. C. Loureiro, & D. Langaro: ‘Internet of things and consumer engagement on retail: state-of-the-art and future directions. EuroMed journal of business’. EuroMed Journal of Business. Vol. 18(3), pp: 397-423, 2023. https://www.emerald.com/emjb/article/18/3/397/83898/Internet-of-things-and-consumer-engagement-on

III. A. A. Alkuwaiti, & M. Al Mubarak: ‘Internet of Things in Water Distribution Systems. In Social Responsibility, Technology and AI’. Internet of Things in Water Distribution Systems. Vol. 23 pp: 143-159, 2024 https://www.emerald.com/books/edited-volume/17277/chapter-abstract/94250831/Internet-of-Things-in-Water-Distribution-Systems?redirectedFrom=fulltext

IV. Keith Bonawitz, Vladimir Ivanov, Ben Kreuter, Antonio Marcedone, H. Brendan McMahan, Sarvar Patel, Daniel Ramage, Aaron Segal, and Karn Seth : 'Practical Secure Aggregation for Privacy-Preserving Machine Learning.' Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS '17), Association for Computing Machinery, 2017, pp. 1175–1191. 10.1145/3133956.3133982

V. Hannah Davis, Christopher Patton, Mike Rosulek, and Phillipp Schoppmann. : 'Verifiable Distributed Aggregation Functions.' IACR Cryptology ePrint Archive, Paper 2023/130, 2023. https://eprint.iacr.org/2023/130

VI. FIDO Alliance. : 'Passkeys: Passwordless Authentication.' FIDO Alliance, 24 July 2025. https://fidoalliance.org/fido2/

VII. Ian J. Goodfellow, Jean Pouget-Abadie, Mehdi Mirza, Bing Xu, David Warde-Farley, Sherjil Ozair, Aaron Courville, and Yoshua Bengio.: 'Generative Adversarial Nets.' Advances in Neural Information Processing Systems 27 (NeurIPS 2014), 2014, https://proceedings.neurips.cc/paper_files/paper/2014/hash/f033ed80deb0234979a61f95710dbe25-Abstract.html

VIII. M. Gupta, M. V. Baisoya, & M. K. Rathore : 'Review of Internet of Things (IoT) Networks using Edge Computing Techniques.' SSRN, 4 Sep. 2024 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4946684

IX. Will Hamilton, Zhitao Ying, and Jure Leskovec. : 'Inductive Representation Learning on Large Graphs.' Advances in Neural Information Processing Systems 30 (NeurIPS 2017), 2017, https://proceedings.neurips.cc/paper/2017/hash/5dd9db5e033da9c6fb5ba83c7a7ebea9-Abstract.html

X. Y. N. Imamverdiyev, & F. I. Musayeva: 'ANALYSIS OF GENERATIVE ADVERSARIAL NETWORKS.' Problems of Information Technology, no. 1, 2022, pp. 20-27. https://jpit.az/ru/journals/297

XI. Khoshraftar, Shima, and Aijun An. : 'A Survey on Graph Representation Learning Methods.' ACM Transactions on Intelligent Systems and Technology, vol. 15, no. 1, Feb. 2024, Article 19, 55 pages. 10.1145/3633518.

XII. R. Kiss, and G. Szűcs. : 'Unsupervised Graph Representation Learning with Inductive Shallow Node Embedding.' Complex & Intelligent Systems, vol. 10, 2024, pp. 7333–7348. https://link.springer.com/article/10.1007/s40747-024-01545-6

XIII. Z. Liu, J. Guo, K. Y. Lam, & J. Zhao : (2022). : Efficient dropout-resilient aggregation for privacy-preserving machine learning. IEEE Transactions on Information Forensics and Security, vol. 18, 2022, 1839-1854. https://ieeexplore.ieee.org/abstract/document/9757847

XIV. Liu, Z., J. Guo, K.-Y. Lam, and J. Zhao. : 'Efficient Dropout-Resilient Aggregation for Privacy-Preserving Machine Learning.' IEEE Transactions on Information Forensics and Security, vol. 18, 2023, pp. 1839–1854. https://ieeexplore.ieee.org/abstract/document/9830997

XV. S. Madakam, R. Ramaswamy, and S. Tripathi. : 'Internet of Things (IoT): A Literature Review.' Journal of Computer and Communications, vol. 3, 2015, pp. 164–173, https://www.scirp.org/journal/paperinformation?paperid=56616

XVI. Y. More, P. Ramachandran, P. Panda, A. Mondal, H. Virk, & D. Gupta.: An Efficient Secure Computation Framework for Secure Aggregation.' arXiv, 15 Feb. 2022. https://arxiv.org/abs/2201.07730

XVII. G. Mwansa, and N. Mabanza. : 'Review of Internet of Things Security Protocols – A Bibliometric Analysis.' 2023 25th International Conference on Advanced Communication Technology (ICACT), Pyeongchang, Korea, Republic of, 2023, pp. 394–400. IEEE. https://ieeexplore.ieee.org/abstract/document/10079641

XVIII. F. Qaswar, M. Rahmah, M. A. Raza, A. Noraziah, B. Alkazemi, Z. Fauziah, M. K. A. Hassan, and A. Sharaf. : 'Applications of Ontology in the Internet of Things: A Systematic Analysis.' Electronics, vol. 12, no. 1, 2023, Article 111. 10.3390/electronics12010111

XIX. S. R. Katragadda, A. Tanikonda, S. R. Peddinti : 'Deep Learning for Autonomous Data Quality Enhancement: A Paradigm Shift in Machine Learning Pipelines'. Journal of Information Systems and Education Management, vol. 10 no. 30s, 2025 pp. 602–609. 10.52783/jisem.v10i19s.3102

XX. Kunal Yogen Sevak, and Babu George. : "The Evolution of Internet of Things (IoT) Research in Business Management: A Systematic Review of the Literature." Journal of Internet and Digital Economics, vol. 4, no. 3, 6 Nov. 2024, pp. 242–265. https://www.emerald.com/jide/article/4/3/242/1212329/The-evolution-of-Internet-of-Things-IoT-research

XXI. J. So, R. E. Ali, B. Güler, J. Jiao, and A. S. Avestimehr. : 'Securing Secure Aggregation: Mitigating Multi-Round Privacy Leakage in Federated Learning'. Proceedings of the AAAI Conference on Artificial Intelligence, vol. 37, no. 8, June 2023, pp. 9864-73. 10.1609/aaai.v37i8.26177.

XXII. Hua Sun. : 'Secure aggregation with an oblivious server'. arXiv, 2023. https://arxiv.org/abs/2307.13474

XXIII. S. B. Verma. : (2022). Emerging Trends in IoT and Computing Technologies. https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=%5B33%5D%09Verma%2C+S.+B.+%282022%29.+Emerging+Trends+in+IoT+and+Comp

XXIV. L. Wang, M. Polato, A. Brighente, M. Conti, L. Zhang, and L. Xu. : 'PriVeriFL: Privacy-Preserving and Aggregation-Verifiable Federated Learning.' *IEEE Transactions on Services Computing*, vol. 18, no. 2, Mar.-Apr. 2025, pp. 998–1011. 10.1109/TSC.2024.3451183

XXV. L. Wang, S. Shi, F. Ma, F. R. Yu, P. Li, and Y. T. He. : 'Subgraph Invariant Learning Towards Large-Scale Graph Node Classification'. *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 39, no. 20, Apr. 2025, pp. 21144-52. 10.1609/aaai.v39i20.35412.

XXVI. Y. Wang, Y. Y. Chang, Y. Liu, J. Leskovec, & P. Li. : 'Inductive representation learning in temporal networks via causal anonymous walks'. *arXiv,* arXiv:2101.05974. https://arxiv.org/abs/2101.05974

XXVII. L. Yang, C. Chatelain, and S. Adam. : 'Dynamic Graph Representation Learning With Neural Networks: A Survey.' *IEEE Access*, vol. 12, 2024, pp. 43460–43484. https://ieeexplore.ieee.org/abstract/document/10473053

XXVIII. Hong-Yu Yao, Chun-Yang Zhang, Zhi-Liang Yao, C. L. Philip Chen, and Junfeng Hu. : 'A Recurrent Graph Neural Network for Inductive Representation Learning on Dynamic Graphs.' *Pattern Recognition*, vol. 154, 2024, Article 110577. 10.1016/j.patcog.2024.110577

XXIX. Ying, Rex, Tianyu Fu, Andrew Wang, Jiaxuan You, Yu Wang, and Jure Leskovec. : 'Representation Learning for Frequent Subgraph Mining.' *arXiv*, 2024. arxiv.org/abs/2402.14367

XXX. Zhang, Chaoyu, and Shaoyu Li. : 'State-of-the-Art Approaches to Enhancing Privacy Preservation of Machine Learning Datasets: A Survey.' *arXiv*, 2024. arxiv.org/abs/2404.16847.