Smart manufacturing integrates operational technology (OT) with information technology (IT) to form highly interconnected cyber-physical systems (CPS). These systems rely on devices, sensors, actuators, and control systems that interact across multiple layers, emphasizing real-time monitoring and feedback loops for production efficiency [1]. This layered approach provides a foundation for implementing multi-layer security models, enabling protection at the device, control, and enterprise layers.

**IEEE Citation:**  
[1] A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems, Manufacturing Letters, vol. 3, pp. 18–23, 2015.

**Literature Review – Step 2**

With the rapid growth of digital communication and data sharing, securing sensitive information has become increasingly critical, particularly when data traverse public networks. Single-layer security mechanisms, such as traditional encryption alone, are vulnerable to evolving cyber threats. A multi-layered security framework that integrates **cryptography with steganography** has been proposed to enhance data protection in these environments [2]. This approach embeds encrypted data within images using advanced techniques like DNA sequence coding, QR codes, and least significant bit (LSB) steganography. Security evaluations using metrics such as **PSNR, MSE, SNR, NPCR, and UACI** demonstrate strong diffusion, confusion, and resilience against differential cryptanalysis. The framework highlights how multi-layered protection mechanisms can reliably safeguard **data integrity and confidentiality**, providing a practical model that aligns with the need for layered security in cyber-physical and industrial systems [2].

**IEEE Citation:**  
[2] *Multi-Layered Security Framework Combining Steganography and DNA Coding*, Systems, vol. 13, no. 341, 2025. [Online]. Available: <https://doi.org/10.3390/systems13050341>

## ****Literature Review – Step 3****

Cloud-connected autonomous systems face significant cybersecurity challenges, including protection of telemetry data, endpoint security, and Electronic Control Units (ECUs). Multi-layer security frameworks have been proposed to ensure **data integrity, operational safety, and prevention of unauthorized access**. These frameworks integrate encryption, authentication, and real-time monitoring mechanisms across cloud, network, and device layers. Evaluations based on autonomous vehicle deployments demonstrate that such integrated approaches maintain system performance while significantly reducing vulnerabilities, highlighting the critical role of layered security in autonomous and cyber-physical systems [3].

**IEEE Citation:**  
[3] Multi-Layer Security Architecture for Cloud-Connected Autonomous Systems, Journal of Computer Science and Technology Studies, vol. 7, no. 3, pp. 798–803, 2025. [Online]. Available: <https://doi.org/10.32996/jcsts.2025.7.3.87>

## ****Literature Review – Step 4****

Hybrid security frameworks combining **quantum key distribution (QKD) and classical cryptography** have been proposed to secure steganographic data transmission. By leveraging QKD protocols such as E91, a shared secret key is generated with provable security against eavesdropping, which is then hashed and used in symmetric encryption schemes like AES to encrypt steganographic images. This multi-layer approach integrates **quantum-based key generation, classical encryption, hashing, and steganography** to enhance both confidentiality and integrity of transmitted data. Experimental results demonstrate that such frameworks maintain high key generation rates, efficient encryption/decryption, and low computational overhead while being resilient against both quantum and classical attacks, offering a robust solution for applications requiring stringent security [4].

**IEEE Citation:**  
[4] Multi-Layered Security System: Integrating Quantum Key Distribution with Classical Cryptography to Enhance Steganographic Security, Alexandria Engineering Journal, 2025. [Online]. Available: <https://doi.org/10.1016/j.aej.2025.02.056>

## ****Literature Review – Step 5****

Smart grid applications are particularly vulnerable to **denial-of-service (DoS) attacks**, which can disrupt communication networks, sensor nodes, and overall grid functionality. Multi-layer security mechanisms integrating **dynamic authentication, cryptographic puzzles, and secure key generation** have been proposed to mitigate such threats. The Multiuser Threshold–based Dynamic Cipher Puzzle (MT-DCP) system dynamically adjusts puzzle complexity per user and integrates Improved Secure Key Generation using Enhanced Identity-Based Encryption (ISKG-EIBE). Experimental implementations demonstrate minimal computational overhead (0.0091 ms), high key sensitivity (99.32%), and efficient resource usage in terms of memory, execution time, and energy. These results indicate that threshold-based, multi-layered security frameworks provide robust protection against DoS attacks while maintaining operational efficiency in smart grid environments [5].

**IEEE Citation:**  
[5] An Efficient Multiuser Threshold–Based Dynamic Cipher Puzzle With Secure Key Generation for DoS Attacks in Smart Grid Applications, Transactions on Emerging Telecommunications Technologies, vol. 36, no. 7, July 2025. [Online]. Available: https://doi.org/10.1002/ett.70204

## ****Literature Review – Step 6****

Time-based cryptography has emerged as a key approach for enforcing **timed access, verifiable delays, and secure computations**. Techniques such as **Time-Lock Puzzles (TLPs) and Verifiable Delay Functions (VDFs)** allow cryptographic operations to be executed with predictable delays, providing resistance against parallel attacks and ensuring verifiable timing guarantees. Analytical evaluations show that TLPs are simple to implement but can introduce computation delays, whereas VDFs are more computationally intensive yet allow efficient verification. These approaches are particularly relevant in multi-layer security frameworks for cyber-physical systems, where timed access and delay verification can strengthen authentication, secure communication, and resilience against certain classes of attacks [6].

**IEEE Citation:**  
[6] Analytical Evaluation of Time-Based Cryptography, Institute of Automation and Applied Informatics (IAI), KASTEL Security Research Labs, Karlsruhe Institute of Technology (KIT), 2025.

## ****Literature Review – Step 7****

Emerging cybersecurity challenges require frameworks that integrate both **Multi-Level Security (MLS)** and **Zero Trust (ZT)** principles to secure sensitive data in isolated or high-risk environments. The proposed model classifies data into three sensitivity levels—Classified, Sensitive, and Open—and applies **dynamic, level-specific security controls**. By combining MLS with Zero Trust’s automated dynamic access capabilities, the framework enhances responsiveness to anomalous behaviors and mitigates limitations of traditional static access controls. Such multi-layered security approaches are crucial for protecting critical systems in military, governmental, and enterprise environments, ensuring secure data utilization without compromising usability [7].

**IEEE Citation:**  
[7] A Proposal for a Zero-Trust-Based Multi-Level Security Model and Its Security Controls, Applied Sciences, vol. 15, no. 2, p. 785, 2025. [Online]. Available: <https://doi.org/10.3390/app15020785>

## ****Literature Review – Step 8****

Ensuring **data privacy in cloud storage** is a major challenge due to evolving cyber threats and privacy vulnerabilities. Multi-layered security mechanisms, such as **multi-layer encoding frameworks combined with one-time password (OTP) authorization**, have been proposed to enhance the confidentiality, integrity, and accessibility of cloud-stored data. This approach organizes data storage across multiple encoded layers while providing flexible authentication, improving both efficiency and robustness against unauthorized access. The framework demonstrates how **layered security architectures** can mitigate privacy risks in cloud environments, highlighting the need for adaptable and comprehensive strategies for data protection [8].

**IEEE Citation:**  
[8] Advancing Data Privacy in Cloud Storage: A Novel Multi-Layer Encoding Framework, Applied Sciences, vol. 15, no. 13, p. 7485, 2025. [Online]. Available: <https://doi.org/10.3390/app15137485>

## ****Literature Review – Step 9****

IoT-Cloud systems require lightweight and scalable security solutions due to the resource constraints of IoT devices and the complexity of cloud infrastructures. Multi-layered hybrid security frameworks have been proposed to address these challenges by integrating technologies such as **Blockchain, improved ECDSA-ZSS encryption, credential management, and auditing layers**. These frameworks optimize encryption speed, computational efficiency, and system responsiveness while ensuring data integrity and authenticity across heterogeneous environments. Evaluations show that such multi-stage, layered approaches not only strengthen security but also improve execution time, communication efficiency, and adaptability for dynamic IoT-Cloud workloads, making them suitable for next-generation secure cloud-connected IoT applications [9].

**IEEE Citation:**  
[9] Designing a Layered Framework to Secure Data via Improved Multi Stage Lightweight Cryptography in IoT Cloud Systems, arXiv preprint arXiv:2509.01717, 2025. [Online]. Available: <https://doi.org/10.48550/arXiv.2509.01717>

## ****Literature Review – Step 10****

The heterogeneous and interconnected architecture of IoT systems exposes them to a wide range of cyber threats. **Moving Target Defence (MTD)** has emerged as a promising paradigm to enhance IoT security by continuously shifting attack surfaces, thereby increasing the difficulty, cost, and risk for attackers. Hybrid MTD approaches, such as those using a **three-layer Temporal Hierarchical Attack Representation Model (3-layer-THARM)**, evaluate network states, security metrics, and accessibility of nodes and edges to identify potential attack paths. Analyses indicate that combining multiple MTD techniques (e.g., shuffle and diversity strategies) reduces the probability of attack success, lowers overall attack risk, and increases attack costs, providing an effective multi-layered defensive strategy for IoT infrastructures [10].

**IEEE Citation:**  
[10] Vulnerability Defence Using Hybrid Moving Target Defence in Internet of Things Systems, Computers & Security, 2025. [Online]. Available: <https://doi.org/10.1016/j.cose.2025.104380>

## ****Literature Review – Step 11****

Modern computing systems face increasingly sophisticated cyberattacks that threaten critical operations and personal data. **Moving Target Defense (MTD)** strategies actively shift attack surfaces to enhance system resilience, but configuring systematic MTD strategies requires careful analysis of attack patterns and system components. The **MTD-Diorama visualization engine** provides a framework to correlate cyberattack information with MTD components, enabling researchers to systematically design and implement multi-layer defense strategies. This approach facilitates the identification of vulnerable attack surfaces, improves orchestration of MTD strategies, and enhances overall cybersecurity posture across diverse computing environments [11].

**IEEE Citation:**  
[11] MTD-Diorama: Moving Target Defense Visualization Engine for Systematic Cybersecurity Strategy Orchestration, Sensors, vol. 24, no. 13, p. 4369, 2024. [Online]. Available: <https://doi.org/10.3390/s24134369>

## ****Literature Review – Step 12****

Interactive platforms such as **Capture The Flag (CTF) challenges** are increasingly used to enhance cybersecurity skills by integrating **cryptography and steganography** in multi-level problem-solving exercises. These platforms provide progressive tasks involving AES and RSA encryption, data hiding and retrieval techniques, reverse engineering, file analysis, and web security vulnerabilities. By combining **web-based interfaces with terminal/SSH access**, participants can engage in realistic scenarios that reinforce both theoretical knowledge and practical skills. Such educational frameworks exemplify how **layered cryptographic and steganographic challenges** can foster critical thinking, problem-solving, and practical cybersecurity awareness in a controlled, multi-layered learning environment [12].

**IEEE Citation:**  
[12] Design and Develop CTF Challenge Using Cryptography and Steganography, International Research Journal of Modern Engineering and Technology Science, 2025. [Online]. Available: <https://www.doi.org/10.56726/IRJMETS66523>

## ****Literature Review – Step 13****

Hybrid cryptographic frameworks combining **Quantum Key Distribution (QKD) with classical encryption techniques** enhance security for steganographic applications by leveraging the principles of quantum mechanics. The proposed system uses the **E91 QKD protocol** to generate a high-entropy shared secret key, which is then hashed and applied in symmetric encryption (AES) for steganographic images. This multi-layered approach strengthens **confidentiality and integrity**, offering resistance against both quantum and classical attacks. Experimental results demonstrate practical feasibility, including efficient key generation, encryption/decryption performance, and manageable computational overhead. Such hybrid systems provide a robust model for secure data transmission in scenarios demanding stringent security measures [13].

**IEEE Citation:**  
[13] Multi-Layered Security System: Integrating Quantum Key Distribution with Classical Cryptography to Enhance Steganographic Security, Alexandria Engineering Journal, 2025. [Online]. Available: <https://doi.org/10.48550/arXiv.2408.06964>

## ****Literature Review – Step 14****

Recent advances in **quantum key distribution (QKD)** demonstrate practical, high-performance encryption even with imperfect hardware. By employing **quantum dot-based sub-Poissonian photon sources** and advanced protocols such as the **truncated decoy state** and **heralded purification**, secure keys can be transmitted over longer distances while mitigating risks from multi-photon events. Real-world experiments show compatibility with room-temperature quantum dot sources and improvements over conventional laser-based QKD, significantly reducing technical and cost barriers. These breakthroughs make **quantum-secure communication more accessible and scalable**, paving the way for practical deployment in real-world networks [14].

**IEEE Citation:**  
[14] Decoy-State and Purification Protocols for Superior Quantum Key Distribution with Imperfect Quantum-Dot-Based Single-Photon Sources: Theory and Experiment, PRX Quantum, 2025. [Online]. Available: https://doi.org/10.1103/7fdd-m92n

## ****Literature Review – Step 15****

Recent research at CRYPTO 2025 highlights multiple breakthroughs in **advanced cryptographic primitives, proofs, and protocols**. Basso et al. [15] presented a **complete security proof of SQIsign**, a leading isogeny-based digital signature, introducing the **Fiat–Shamir with hints framework** to achieve EUF-CMA security in the ROM. Garg et al. [16] developed a **modular framework for special-purpose witness encryption (WE)**, enabling constructions of registered attribute-based and threshold encryption schemes with linear-size common reference strings. Baecker et al. [17] proposed a **fully-adaptive, partially-oblivious threshold pseudorandom function (PRF)**, resolving key refresh and non-verifiability issues in prior OPRF models.

Goyal et al. [18] designed the first **adaptively secure hierarchical identity-based encryption (HIBE)** from standard assumptions without relying on bilinear pairings or random oracles. Crites and Stewart [19] analyzed **adaptive security weaknesses in threshold Schnorr signatures**, identifying practical attacks and generalizations. Waters and Wu [20] introduced a **pure indistinguishability obfuscation approach to adaptively-sound SNARGs** for NP, eliminating the need for additional algebraic assumptions. Bai et al. [21] proposed a **quasi-polynomial time quantum algorithm for the extrapolated dihedral coset problem (EDCP)** relevant to LWE reductions.

Ishai et al. [22] developed a **succinct garbling framework from homomorphic secret sharing**, drastically reducing garbled circuit sizes and improving efficiency. Lee et al. [23] combined FHE and LSSS-based MPC to achieve **actively secure multiparty computation in the dishonest majority setting** with constant complexity. Cheng and Jaeger [24] formalized **adaptive security for constrained PRFs**, while Bacho et al. [25] proposed **three-round adaptively secure threshold Schnorr signatures** under DDH. Bitansky et al. [26] constructed **additive randomized encodings from public-key encryption**, and Carnemolla et al. [27] introduced **anamorphic-resistant encryption schemes** resistant to subversion attacks.

Additional works include Dodis and Goldin [28] analyzing **technical implications of anamorphic encryption**, Bunz et al. [29] presenting **hash-based accumulation for Reed–Solomon codes**, Carrier et al. [30] assessing **dual-lattice attacks on Kyber**, Feng and Tang [31] on **optimal asynchronous common coin protocols**, Khovratovich et al. [32] improving **hash-based signature trade-offs**, Liu et al. [33] enhancing **actively secure 2-party computation with BitGC**, and Xu et al. [34] analyzing **bitwise garbling schemes and optimal ciphertext sizes**.

These contributions collectively advance **security proofs, practical efficiency, adaptive and quantum-safe constructions, and resistance against novel attack vectors**, illustrating the growing breadth of contemporary cryptography research.

**IEEE Citations:**  
[15] A. Basso et al., “A Complete Security Proof of SQIsign,” CRYPTO, 2025.  
[16] S. Garg et al., “A Framework for Witness Encryption from Linearly Verifiable SNARKs and Applications,” CRYPTO, 2025.  
[17] R. Baecker et al., “A Fully-Adaptive Threshold Partially-Oblivious PRF,” CRYPTO, 2025.  
[18] R. Goyal et al., “A Note on Adaptive Security in Hierarchical Identity-Based Encryption,” CRYPTO, 2025.  
[19] E. Crites, A. Stewart, “A Plausible Attack on the Adaptive Security of Threshold Schnorr Signatures,” CRYPTO, 2025.  
[20] B. Waters, D. J. Wu, “A Pure Indistinguishability Obfuscation Approach to Adaptively-Sound SNARGs for NP,” CRYPTO, 2025.  
[21] S. Bai et al., “A Quasi-polynomial Time Algorithm for the Extrapolated Dihedral Coset Problem over Power-of-Two Moduli,” CRYPTO, 2025.  
[22] Y. Ishai et al., “A Unified Framework for Succinct Garbling from Homomorphic Secret Sharing,” CRYPTO, 2025.  
[23] S. Lee et al., “Actively Secure MPC in the Dishonest Majority Setting,” CRYPTO, 2025.  
[24] K. Cheng, J. Jaeger, “Adaptive Security for Constrained PRFs,” CRYPTO, 2025.  
[25] R. Bacho et al., “Adaptively Secure Three-Round Threshold Schnorr Signatures from DDH,” CRYPTO, 2025.  
[26] N. Bitansky et al., “Additive Randomized Encodings from Public Key Encryption,” CRYPTO, 2025.  
[27] D. Carnemolla et al., “Anamorphic Resistant Encryption: the Good, the Bad and the Ugly,” CRYPTO, 2025.  
[28] Y. Dodis, E. Goldin, “Anamorphic-Resistant Encryption; Or Why the Encryption Debate is Still Alive,” CRYPTO, 2025.  
[29] B. Bünz et al., “Arc: Accumulation for Reed–Solomon Codes,” CRYPTO, 2025.  
[30] K. Carrier et al., “Assessing the Impact of a Variant of MATZOV's Dual Attack on Kyber,” CRYPTO, 2025.  
[31] H. Feng, Q. Tang, “Asymptotically Optimal Adaptive Asynchronous Common Coin and DKG with Silent Setup,” CRYPTO, 2025.  
[32] D. Khovratovich et al., “At the Top of the Hypercube -- Better Size-Time Tradeoffs for Hash-Based Signatures,” CRYPTO, 2025.  
[33] H. Liu et al., “Authenticated BitGC for Actively Secure Rate-One 2PC,” CRYPTO, 2025.  
[34] F. Xu et al., “Bitwise Garbling Schemes: A Model with 3/2κ-bit Lower Bound of Ciphertexts,” CRYPTO, 2025.

**Literature Review – CRYPTO 2025 Advances**

Recent works in CRYPTO 2025 cover a broad spectrum of cryptographic primitives, highlighting improvements in efficiency, security proofs, and novel constructions.

**Blind Signatures and Lattice Signatures:** Klooß and Reichle [35] propose **pairing-free blind signatures from proofs of inequality**, achieving communication and signature sizes of 608 B and 192 B, respectively, under the DDH assumption in the random oracle model. This advances prior AGM-based blind signature constructions by reducing overhead while also achieving one-more strong unforgeability. Complementing this, Gärtner [36] introduces **compact lattice signatures via iterative rejection sampling**, reducing rejection probability and allowing narrower output distributions for more compact signatures, achieving size improvements comparable to schemes like Falcon while preserving security.

**Cryptanalysis and Attacks:** Bhati and Andreeva [37] present the **first plaintext recovery attack on XCB-AES**, a tweakable block cipher mode from the IEEE 1619.2 standard. Their “shared difference attack” exploits the separability property of polynomial hash functions, demonstrating that XCB-AES and related TEM designs are fundamentally insecure. Similarly, Haidar et al. [38] show that Falcon’s lattice-based signatures are vulnerable to **Rowhammer-based single-bit fault attacks**, enabling full key recovery from a single targeted bit flip.

**Protocols and Multi-Party Computation:** Bandarupalli et al. [39] and Li & Song [40] develop **asynchronous MPC protocols with linear communication** and low additive overhead, relying on computationally efficient primitives in the random oracle model. These works achieve post-quantum security while optimizing both communication and computation. Haitner et al. [41] demonstrate that **computationally differentially private inner-product protocols imply oblivious transfer**, establishing equivalence for constant additive error regimes.

**Functional Encryption and Correlation Generation:** Bhushan et al. [42] construct **dynamic bounded-collusion streaming functional encryption** from minimal assumptions, improving prior sFE constructions by avoiding indistinguishability obfuscation. Li et al. [43] present **pseudorandom correlation generators over arbitrary Galois rings**, enabling efficient offline correlation generation for MPC protocols over rings like Z2k\mathbb{Z}\_{2^k}Z2k​, significantly outperforming prior homomorphic encryption-based approaches.

**Quantum and Nonlocal Computation:** Bacho et al. [44] develop a **compiler for nonlocal games into single-prover protocols**, enabling classical verification of quantum computations based on trapdoor claw-free functions. This builds on prior works on blind quantum computation and expands applications to more general quantum cryptographic protocols.

**Randomness Extraction and Differential Privacy:** Aggarwal et al. [45] construct a **strong two-source non-malleable extractor** requiring only linear min-entropy, avoiding computational assumptions such as DDH. Haitner et al. [41] further link computational differential privacy to cryptographic primitives like oblivious transfer, bridging privacy-preserving protocols with secure multi-party computation.

**Polynomial Commitment and Key Control Security:** Bünz et al. [46] introduce **DewTwo**, a transparent polynomial commitment scheme with quasi-linear prover time, logarithmic verifier time, and 4.5 KB proofs, improving on prior transparent PCS constructions. Bhaumik et al. [47] formalize **key control (KC) security** in key derivation functions, analyzing constructions from NIST SP 800-108 and demonstrating achievable security margins for XOF- and hash-based KDFs, while highlighting limitations in block-cipher-based modes.

**Verifiable Delay Functions and Deterministic Algorithms:** Guan et al. [48] show the **impossibility of VDFs in the random oracle model**, ruling out black-box constructions from standard primitives and inspiring the study of proof-of-work functions. Houben [49] presents **deterministic constant-time algorithms for class group actions**, enabling CSIDH-style key exchanges without dummy operations or conditional branching.

**Group Key Agreement:** Auerbach et al. [50] improve **continuous group-key agreement protocols**, addressing inefficiencies in TreeKEM’s propose-and-commit approach and reducing update costs to Θ(log⁡N)\Theta(\log N)Θ(logN) in expectation for large groups, enabling concurrent updates while maintaining tree structure.

These works collectively advance **efficiency, post-quantum security, and foundational cryptographic constructions**, while also addressing vulnerabilities in widely deployed standards and algorithms.

**IEEE References (CRYPTO 2025 subset):**  
[35] M. Klooß, M. Reichle, “Blind Signatures from Proofs of Inequality,” CRYPTO, 2025.  
[36] J. Gärtner, “Compact Lattice Signatures via Iterative Rejection Sampling,” CRYPTO, 2025.  
[37] A. S. Bhati, E. Andreeva, “Breaking the IEEE Encryption Standard – XCB-AES in Two Queries,” CRYPTO, 2025.  
[38] C. Abou Haidar, Q. Payet, M. Tibouchi, “Crowhammer: Full Key Recovery Attack on Falcon with a Single Rowhammer Bit Flip,” CRYPTO, 2025.  
[39] A. Bandarupalli et al., “Computationally Efficient Asynchronous MPC with Linear Communication and Low Additive Overhead,” CRYPTO, 2025.  
[40] J. Li, Y. Song, “Constant-Round Asynchronous MPC with Optimal Resilience and Linear Communication,” CRYPTO, 2025.  
[41] I. Haitner, N. Mazor, J. Silbak, E. Tsfadia, C. Yan, “Computationally Differentially Private Inner Product Protocols Imply Oblivious Transfer,” CRYPTO, 2025.  
[42] K. Bhushan, A. Korb, A. Sahai, “Dynamic Bounded-Collusion Streaming Functional Encryption from Minimal Assumptions,” CRYPTO, 2025.  
[43] Z. Li, C. Xing, Y. Yao, C. Yuan, “Efficient Pseudorandom Correlation Generators over Z/p^k Z,” CRYPTO, 2025.  
[44] K. Bacho, A. Kulpe, G. Malavolta, S. Schmidt, M. Walter, “Compiled Nonlocal Games from any Trapdoor Claw-Free Function,” CRYPTO, 2025.  
[45] D. Aggarwal, P. Dutta, S. Mukherjee, S. Nagargoje, M. Obremski, “Efficient Strong 2-Source Non-Malleable Extractor for Any Linear Min-Entropy,” CRYPTO, 2025.  
[46] B. Bünz, T. Mopuri, A. Shirzad, S. Sridhar, “DewTwo: a Transparent PCS with Quasi-Linear Prover, Logarithmic Verifier and 4.5 KB Proofs from Falsifiable Assumptions,” CRYPTO, 2025.  
[47] R. Bhaumik et al., “Cryptographic Treatment of Key Control Security – In Light of NIST SP 800-108,” CRYPTO, 2025.  
[48] Z. Guan, A. Riazanov, W. Yuan, “Breaking Verifiable Delay Functions in the Random Oracle Model,” CRYPTO, 2025.  
[49] M. Houben, “Deterministic Algorithms for Class Group Actions,” CRYPTO, 2025.  
[50] B. Auerbach, M. C. Noval, B. Erol, K. Pietrzak, “Continuous Group-Key Agreement: Concurrent Updates without Pruning,” CRYPTO, 2025.

Recent work presents a **Java-based blockchain framework for securing cloud storage** by integrating **RSA encryption** to protect sensitive data in collaborative environments. The proposed system leverages **blockchain’s immutability** alongside strong cryptographic mechanisms to ensure **data confidentiality, integrity, and availability**. Experimental evaluations highlight efficient **block creation, encryption/decryption, and data retrieval**, demonstrating its practicality for real-world cloud storage applications. The architecture provides a solid foundation for further advancements in **secure, decentralized cloud storage systems** [51].

IEEE Citation:  
[51] S. K. Rana and K. Kumar, "A Java-Based Blockchain Framework for Cloud Storage Security Using RSA in Collaborative Environment," in Proc. Int. Conf. on Artificial Intelligence and Networks (ICAIN 2024), LNNS, vol. 1269, 2025, pp. 387–402. [Online]. Available: https://doi.org/10.1007/978-3-031-XXXX-X\_27