CODE	TITLE	APPLICATION / DESCRIPTION
VTJCC01	Enhanced Key Exchange and Lightweight Encryption for IoT Security Using Timestamp-Based OTP and SIT	**Description**: We propose an end-to-end secured IoT system that ensures the system's integrity is never compromised using lightweight cryptographic algorithms. We propose a three-module system, where the first module handles user authentication using a time-based one-time password, the second secures communication using lightweight enhanced RSA
VTJCC02	Verifiable And Secure Data Deduplication With A Real-Time Data Integrity Checking With a Cloud	**Description:** VERDUP, a verifiable and secure deduplication scheme with the support of real-time data integrity checking and fine-grained access control specifically designed for IIoT environments. VERDUP utilizes a two-stage deduplication approach based on a dynamic tree model in a fog-assisted cloud architecture, integrated with blockchain technology to enhance deduplication efficiency and data integrity verification
VTJCC03	Enhancing Edge Data Deduplication with Robust Optimization Amidst Uncertainties	**Description:** This project proposes a robust optimization-based framework for efficient data deduplication in Mobile Edge Computing (MEC) environments. It introduces two algorithms—uEDDE-C and the lightweight uEDDE-A—to handle uncertainties like data demand fluctuations and edge server failures. The solution effectively reduces storage costs and retrieval latency, ensuring reliable performance in dynamic edge networks
VTJCC04	A Secure Property-Based Token Attestation Framework Using Homomorphic Encryption for Mobile Cloud Systems	**Description:** This project introduces PTA-HE, a secure Property-Based Token Attestation framework that integrates Homomorphic Encryption to protect sensitive data during processing in mobile cloud environments. It enables computations on encrypted data while ensuring only authorized tokens are validated through Trusted Third Parties (TTPs). Experimental results confirm that PTA-HE offers strong privacy with acceptable performance trade-offs, making it suitable for confidentiality-critical cloud applications
VTJCC05	Privacy Preserving Data Collaborative Searchable Encryption for Group Cloud Data Sharing in Cloud Computing	**Description :** This scheme introduces a dedicated keyword server to export server-derived keywords, thereby withstanding KGA attempts. Based on this, PCSE deploys cryptographic reverse firewalls to thwart subversion attacks. To overcome the single point of failure inherent in a single keyword server, the export of server-derived keywords is collaboratively performed by multiple keyword servers
VTJCC06	Ripple: A Decentralized Edge-Based Data Deduplication Framework	**Description:** This project introduces Ripple, a decentralized data deduplication framework for edge computing environments. By enabling each edge server to maintain a local data index, Ripple efficiently detects and eliminates redundant data without centralized coordination, significantly reducing data retrieval latency and improving storage utilization.
VTJCC07	A Security Analysis of Website-Enabled Direct File Uploads to Cloud Storage Services	**Description :** This project conducts the first comprehensive security evaluation of direct file uploads from websites to cloud storage services, identifying six major vulnerability categories. Through large-scale testing, it uncovers 79 previously unknown security flaws across popular platforms like Google and Reddit. The study provides mitigation strategies and offers critical insights for securing cloud-based file upload mechanisms in web applications
VTJCC08	Secure Keyword Search and Key Management Scheme in Cloud Environments	**Description:** Key-aggregate, keyword retrieval, privacy, practicability, An SE enables a cloud server to securely perform a keyword retrieval over the encrypted data without exposing any information of data content and search queries
VTJCC09	An Medical Data A User Authentication Of A Cloud Data	**Description:** The proposed protocol utilizes a post-quantum fuzzy commitment (PQFC) scheme to enhance security and is rigorously analyzed under the random oracle model and ProVerif tool. Its functionality and security are thoroughly assessed, demonstrating adherence to key requirements such as memoryless operation

CODE	TITLE	APPLICATION / DESCRIPTION
VTJCC10	Secure Multi-Authority Key-Policy Attribute-Based Encryption with ECC Integration	**Description**: This project proposes a secure and efficient data protection framework for IoT systems by combining Key-Policy Attribute-Based Encryption (KP-ABE) with Elliptic Curve Cryptography (ECC). The approach aims to reduce encryption overhead while ensuring fine-grained access control and strong data security
VTJCC11	Information-Theoretic Secure User Authentication via Secret Sharing Computation	**Description:** This project proposes a lightweight user authentication and secure communication system using a (k, n)-threshold secret sharing scheme to achieve information-theoretic security. It prevents replay attacks through dynamic authentication data and eliminates the need for heavy cryptographic computation. The approach is ideal for IoT environments, offering strong security with minimal resource usage
VTJCC12	A Scalable Key-Splitting Protocol for Secure Data Sharing in IoT Devices	**Description:** This project introduces a lightweight, privacy-preserving computation system for Gmail-connected devices using threshold cryptography and efficient encryption techniques like ECC or NTRU. It avoids the overhead of multi-share or FHE-based methods, enabling secure and scalable data sharing through encrypted communication linked to Gmail accounts
VTJCC13	Quality of Service-Aware Scheduling in Cloud Platforms Using a Hybrid Approach	**Description:** The main contribution of this paper is to calculate the maximum cost for each transaction flow which has not been addressed in previous studies. This new multipurpose function includes flow load amount, load amount on makespan, capacity of Virtual Machines (VMs) and execution speed parameter.
VTJCC14	Securing Cloud Systems with Smart Authentication and Adaptive Encryption	**Description :** The framework exhibited strong resilience against brute force, spoofing, phishing, guessing, and impersonation attacks. Implementing this framework in a cloud authentication environment significantly enhances data confidentiality and protects against unauthorized access.
VTJCC15	Homomorphic Encryption-Based Privacy Preservation Using Data Sharing in cloud Environments	**Description:** Computational modeling, Security, Computational efficiency, Biological system modeling, Protection, Data models, Cryptography, Data privacy, the proposed method is more efficient in communication and computational overheads than other PPFL-HE methods
VTJCC16	Secure Fine-Grained Access Control with Policy Protection for Smart Grids	**Description :** This project proposes a privacy-preserving access control scheme for smart grid data sharing using cuckoo filters for attribute hiding and blockchain for secure data revocation, ensuring fine-grained access control with low computational overhead
VTJCC17	EVDSE: Efficient and Verify Data Search With Encryption In a Cloud Logs	**Description:** We propose EVSEB-an efficient and verifiable searchable encryption framework for encrypted cloud-hosted logs. EVSEB supports fine-grained multi-keyword Boolean search, privacy-preserving access control, and per-file integrity verification with minimal overhead. At its core, EVSEB introduces a hybrid indexing model that integrates a hierarchical log-type classification tree, Bloom filters, and inverted indexes to reduce search space
VTJCC18	Quantum Secret Sharing Protocol Security In Cloud Environment	**Description:** To address these gaps, in this article, we introduce a new concept of QSS, which leans on a generic distributed quantum network, based on a threshold scheme, where all the players collaborate also to the routing of quantum information among them. The dealer, by exploiting a custom flexible weighting system, takes advantage of a newly defined quantum Dijkstra algorithm

CODE	TITLE	APPLICATION / DESCRIPTION	
VTJCC19	EBMD: Efficient Based Medical Data Share In Database	**Description**: However, this shift introduces critical security and privacy risks, as sensitive patient information is stored on untrusted third-party servers To address these limitations in medical data outsourcing, we present ECMO, a novel protocol that combines an ordered additive secret sharing algorithm with a unique index permutation method	IEEE 2025 - CLOUD COMPUTING
VTJCC20	Toward a Publicly Verifiable Confidential Cloud Data Security in Blockchain	**Description:** We also provide a technical solution to embed secure multi-party computations within smart contracts by using the Promise programming pattern. Finally, a cost analysis is provided to justify the feasibility of the framework compared to other solutions	
VTJCC21	Multi-key Homomorphic Encryption With an secure in a Cloud Data in Automorphism Data	**Description:** Multi-key homomorphic encryption (MKHE) allows computations to be performed on ciphertexts encrypted with different keys, thus expanding the application scenarios of homomorphic encryption to more fields. We improved the automorphism-based blind rotation by using the hybrid product, making it suitable for the multi-key schemes	
VTJCC22	Secure and Private Analytics of Healthcare Records in Multi-Tenant Cloud Environments Using Blockchain	**Description:** Medical services, Blockchains, Data privacy, Engines, Privacy, Cryptography, Scalability, Computational efficiency, Transforms, Computer architecture, This approach is privacy in healthcare analytics, providing a scalable and secure solution to a pressing problem	
VTJCC23	A Lightweight Hashing-Based Approach for Privacy-Preserving IoT Service Recommendation	**Description :** Data privacy, Privacy, Accuracy, Aggregates, Distributed databases, Internet of Things, Recommender systems, our proposal surpasses other approaches in terms of recommendation accuracy and efficiency while protecting user privacy	
VTJCC24	Multiple Attribute Features and Mashup Requirement Attention using cloud computing	**Description:** Cloud computing, Transformers The performance of the proposed optimization configuration model in different scenarios is compared and the influence of model parameters on the optimization results is analyzed	
VTJCC25	A Robust Image Encryption with a Dynamic Data for secure Data With a Cloud	**Description :** Deficient cloud security can lead to privacy breaches, data theft, and unauthorized access, making robust security solutions indispensable for protecting against cyber-threats and providing data privacy	
VTJDM01	Secure Keyword Search with Access Control Using Secret Sharing for Cloud Data Outsourcing	**Description:** This project presents a secure keyword search system using secret sharing with built-in user access control for cloud-based environments. It ensures that only authorized users can search encrypted data, protecting privacy even against semi-honest adversaries. The enhanced secret sharing technique improves efficiency, making the solution ideal for scalable, privacy-preserving data outsourcing	IEEE 2024 - DATA MINING
VTJDM02	Secure and Transparent E-Voting System Using Blockchain, Smart Contracts, Differential Privacy, and Email-Based Voter Authentication	**Description:** This project aims to develop a secure and transparent e-voting system using blockchain technology. It integrates smart contracts for reliability and differential privacy for vote anonymity, while utilizing email verification for voter authentication instead of complex digital identity frameworks	

CODE	TITLE	APPLICATION / DESCRIPTION
VTJDM03	An Efficient Data with a Generic Construction in a Public Key with a Random Data in a SQL	**Description**: The proposed method leverages only fundamental cryptographic building blocks, relying exclusively on a standard public key encryption (PKE) scheme along with cryptographic hash functions, without requiring additional complex primitives. More concretely, the proposed construction leverages a PKE scheme that ensures one-wayness against chosen plaintext attacks (OW-CPA)
VTJDM04	Blockchain-Enabled Comprehensive Security Framework for Industrial IoT	**Description:** This project introduces a blockchain-based end-to-end security model for IIoT systems, ensuring decentralized authentication, data integrity, and access control. It combines smart contracts and SHA-256 encryption to dynamically enforce security without relying on central authorities. The hybrid blockchain approach offers scalability, performance, and confidentiality for secure industrial operations
VTJDM05	Secure and Decentralized Health Data Management Using IoMT and Blockchain	**Description:** This project presents a blockchain-enabled framework using Hyperledger Fabric to ensure secure, interoperable, and privacy-preserving management of IoMT data across healthcare systems. By integrating edge computing, it enables real-time data processing, reduces latency, and maintains device-level privacy. The solution supports efficient remote monitoring and clinical decision-making, promoting a unified and trustworthy digital healthcare ecosystem
VTJDM06	A Verifiable Data With Symmetric Searchable Encryption With Dynamic Data Store With Database In Security	**Description:** We present two novel approaches, Hexie and Jianding. Hexie implements secret sharing to conceal index entries, enabling dynamic updates, non-interactive interactions, and lightweight clients. To enhance the reliability of search results and address the problem of empty, incomplete, or inaccurate outcomes, we introduce the Jianding scheme as an extension of Hexie.
VTJDM07	An Advance Data Sharing with Quantum Secret Sharing Scheme with Cloud Data	**Description :** We propose procedures to distribute some shares before a secret is given in those schemes. The new procedures enhance the applicability of the secret sharing schemes to wider scenarios as some participants can be unavailable when the dealer obtains the quantum secret.
VTJDM08	Enhanced Privacy Preservation in Mixed Data Sharing Using Correlation-Aware Differential Privacy and Data Balancing	**Description:** This project develops a servlet-based web application that enables privacy-preserving data sharing using a correlation-aware differential privacy approach. It balances and enhances unbalanced datasets by generating synthetic records and applying noise within correlated attribute groups. The system ensures strong privacy protection while maintaining data truthfulness and utility, making it suitable for sensitive domains like healthcare and finance
VTJDM09	An Open-source Web application Data Management	**Description :** This paper introduces 'BeyondLife', a cross-platform, open-source, and privacy-enhancing digital will management solution designed to securely handle and distribute digital assets after death. At the core of this solution is a customized Ciphertext-Policy Attribute-Based Encryption (CP-ABE) scheme, referred to as PD-CP-ABE
VTJDM10	Adaptive Task Scheduling and Load Optimization in Fog Networks for Healthcare	**Description:** Processor scheduling, Edge computing, Costs, Computational modeling, Cloud computing, Resource management. The foundation of this approach is the DRL model, which is designed to dynamically optimize the partition of computational tasks across fog nodes to improve both data throughput and operational response times
VTJDM11	Privacy Preserving Health Care Data Sharing With Data Mining	**Description:** This study examined current perspectives on data sharing, investigating the trust level in privacy preserving data sharing tools and techniques among healthcare professionals and organization's, and their openness to adopting technology for secure data sharing. We incorporated participants from various healthcare professions across Australia. We aimed to uncover prevalent attitudes toward data sharing in the healthcare sector by employing a mix of descriptive statistics and knowledge

CODE	TITLE	APPLICATION / DESCRIPTION
VTJDM12	Decentralized Authentication and Secure Data Sharing Using IOTA-Based Self-Sovereign Identity	**Description**: This project presents ISIF, a decentralized identity and data-sharing framework for IoT devices using IOTA, enabling secure, scalable, and trustless authentication without centralized authorities
VTJDM13	Cross-Border Data Sharing: A Trust-Enabled Framework Using TTDS	**Description:** The paper introduces a general framework called Trans-Border Trusted Data Spaces (TTDS) that enables secure, traceable, and policy-compliant international data exchange. It leverages technologies like smart contracts, zero-trust identity models, and IP-layer traffic monitoring to enforce data governance and accountability across borders. The framework ensures interoperability with global standards and addresses legal, technical, and trust challenges in cross-border data circulation.
VTJDM14	Public Key Authenticated Encryption with Searched in Encrypted Data in Data Mining	**Description:** The complexity of all algorithms in PEWS increases linearly with the keyword length, while remaining almost constant or even decreasing linearly with the number of wildcards. To resist against (insider) KGA, we further extend PEWS into the first Public-key Authenticated Encryption with Wildcard Search (PAEWS) scheme. Our PEWS and PAEWS schemes are highly flexible, supporting searches for any number of wildcards positioned anywhere within the keyword
VTJDM15	Secure Data Exchange Techniques for Industrial Environments: A New Approach	**Description:** This project introduces an enhanced SALT-based security framework for Industrial Control Systems, using analog related data to securely exchange symmetric keys. It enables real-time encryption and key rotation without major system changes, ensuring cost-effective and robust protection.
VTJDM16	Privacy-Focused Certificateless Encryption with User Revocation for Healthcare Systems	**Description :** This project proposes a pairing-free, revocable certificateless encryption scheme with ciphertext evolution for secure healthcare data sharing. It enables efficient revocation of unauthorized users while preserving data privacy and reducing computational overhead. The scheme is proven secure against adaptive chosen ciphertext attacks, making it practical for real-world healthcare systems
VTJDM17	A Hybrid Recommendation Model Using Multi-Level Sentiment and Rating Interactions	**Description:** Reviews, Feature extraction, Recommender systems, Sentiment analysis, Data mining, Representation learning, Transformers, Sentiment dictionaries and attention mechanisms are then applied to assign appropriate weights to the review features of users and items, respectively
VTJDM18	Secure and Real-Time 1-to-N Face Recognition System for Web-Based User Authentication	**Description:** This system enhances user authentication by integrating live face capture and identification through OpenCV, replacing static image storage with real-time facial recognition, ensuring secure access to sensitive data with dynamic user information retrieval
VTJDM19	Secure Multi-Keyword Encrypted Search with Access Control for IoT Systems	**Description:** Cloud computing, Privacy, Simulation, Scalability, Collaboration, Public key cryptography, User experience, Encryption. Model is constructed, seamlessly embedding entity private keys and public keys into encryption, search, decryption, and other steps, ensuring high privacy and security of this scheme.
VTJDM20	Privacy-Preserving Autonomous System Routing via Intelligent Graph Filtering	**Description:** Routing, Privacy, Peer-to-peer computing, Decision trees, Costs, Scalability, Routing protocols, Computer architecture, Computational complexity. These protocols are based on Multi-Party Computation (MPC) schemes, which guarantee privacy at the cost of high computational

CODE	TITLE	APPLICATION / DESCRIPTION	
VTJDM21	Controlled Service Scheduling Strategy for Intelligent IoT Resource Management	**Description**: Resource management, Processor scheduling, Computational modeling, Dynamic scheduling, Quality of service, Software defined networking. the scheme can enhance performance in ever-changing Internet of Things settings by optimizing the allocation of resources.	IEEE 2025 - DATA MINING
VTJDM22	Secure Key Agreement and Authentication Mechanism with IDS for Fog Computing	**Description:** Servers, Security, Authentication, Passwords, Computational modeling, Cloud computing, Neural networks, Edge computing, Protocols. The proposed lightweight authentication protocol to enhance the overall security framework in the fog environment	
VTJNS01	A Network Security Protocols For The Quantum key and Cryptography Data Distribution	**Description:** we present our novel solution for integrating three different cryptographic assumptions (two of them quantum resistant) into hybrid network security protocols, ensuring that three different cryptographic assumptions must be broken before the protocol becomes vulnerable. Our solution allows for a seamless integration of classical and post-quantum (PQ) cryptography, and quantum key distribution (QKD) into existing network security protocols (e.g., TLS, IPsec).	IEEE 2025 - NETWORK SECURITY
VTJNS02	Optimization of RSA-Based Encryption Performance and Resource Allocation in Networks	**Description:** Firstly, optimize the encryption performance by optimizing the parameter selection of the RSA algorithm, selecting appropriate public and private key lengths, and reducing unnecessary computational overhead. At the same time, introducing fast power algorithm optimization accelerates the encryption and decryption. At the same time, a load-aware resource allocation algorithm is designed to monitor the real-time load situation of network nodes	
VTJNS03	A Blockchain-Based Zero Trust Model for Privacy-Centric IoT Cybersecurity	**Description :** This research presents the "Unified Quantum-Resilient Blockchain-Zero Knowledge Proofs Privacy Authentication Framework (QBC-ZKPAF)," a novel approach to enhance IoT security by integrating blockchain, Zero Trust Architecture, and post-quantum cryptography for privacy-preserving authentication, access control, and secure communication	
VTJNS04	An Efficient Bi-Encoder-Based Skill Classification and Employer Notification Model for Smart Job Market Analysis	**Description:** This research proposes a lightweight, scalable AI-driven Job Portal System that integrates skill extraction and employer-employee interaction modules, providing real-time updates via Gmail notifications to enhance the recruitment process and improve job matching efficiency	
VTJNS05	A Decision-Making Model for Uncertainty-Aware Evaluation of Blockchain Traceability Systems	**Description :** Blockchains, Reliability, Decision making, Supply chains. Moreover, to verify the validity and reliability of the proposed approach, a comparison analysis was performed to show the efficacy of the proposed model. Finally, concluding remarks are discussed	
VTJNS06	A Secure and Optimized Framework for Controller Selection and Resource Management in SDN	**Description:** By establishing a blockchain-centric secure resource allocation with controller selection, the proposed technique addresses challenges in SDN. Here, user registration, load balancing, attack detection, controller selection, and resource allocation phases are included	
VTJNS07	Unrestricted File Upload Vulnerabilities: Security Challenges and Future Directions in Modern Communication Systems	**Description:** This project presents an in-depth analysis of Unrestricted File Upload (UFU) vulnerabilities in applications used across IoT, smart homes, and smart city systems. It highlights how easily exploitable UFUs can compromise system confidentiality, integrity, and availability. The study emphasizes the need for stronger security mechanisms and outlines future directions to enhance file upload safety in modern communication systems	

CODE	TITLE	APPLICATION / DESCRIPTION	
VTJNS08	Hierarchical Synchronization Strategies for Robust and Scalable SDN Networks	**Description**:Software defined networking, Servers, Scalability. This paper presents a hybrid synchronization model combining a hierarchical design with established resilient cluster mechanisms	IEEE 2024 - NETWORK SECURITY
VTJNS09	Energy-Efficient Cloud Task Management Using a Multi-Objective Optimization Model	**Description:** EMO-TS dynamically adjusts task scheduling based on real-time workloads and operational conditions, effectively minimizing power consumption without sacrificing system performance	
VTJBC01	Efficient Blockchain Mechanisms for Ensuring Data Integrity in IoT Systems	**Description:** This project integrates a lightweight blockchain module into a LoRa network, where data is encrypted and stored in blocks. The system uses a cyclic process to encrypt, transmit, and decrypt the blockchain every 20 seconds, ensuring secure data exchange between devices and servers	IEEE 2025 - BLOCK CHAIN
VTJBC02	Blockchain-Enabled Healthcare: Ensuring Secure and Scalable Data with MySQL Integration	**Description:** The project presents a robust and secure architecture for healthcare data management by integrating MySQL with blockchain technology, forming the MySQL-Blockchain Healthcare Architecture (MBHA). This system combines the structured querying and efficiency of traditional relational databases with the tamper-proof, decentralized nature of blockchain	
VTJBC03	A Cryptographic Reputation System for Fair and Private Performance Evaluation	**Description :** This project presents ARSPA, a secure and anonymous performance appraisal system using blockchain and cryptographic techniques. It ensures honest feedback by protecting reviewer identity, preventing multiple submissions, and storing reviews transparently and immutably on a public blockchain	
VTJBC04	A Blockchain-Enabled Secure Data Sharing Framework for Edge Computing Networks	**Description:** The Blockchain-based Secure Data Sharing Framework (BSDSF) enhances security and efficiency in edge-cloud computing by integrating blockchain with Byzantine Fault Tolerant (BFT) consensus and smart contracts. It ensures low-latency, tamper-resistant data sharing through a two-tier consensus system and real-time node validation. The framework significantly reduces transaction delays and improves throughput, making edge data exchange more reliable and secure	
VTJBC05	TM-Chain: Trusted Computing Base Measurement and Management for IoT Using Blockchain and Cloud	**Description :** TM-Chain is a blockchain-based architecture designed to securely and efficiently manage Trusted Computing Base (TCB) measurements in large-scale IoT environments. It addresses the limitations of traditional remote attestation systems—such as scalability issues and centralized vulnerabilities—by using distributed, tamper-resistant storage. TM-Chain introduces custom protocols for encrypted TCB data transfer, identity-linked storage, and verifier access, enabling secure and traceable	
VTJBC06	A Secure Blockchain Technique For Integration Knowledge Discovery in Cloud	**Description:** Blockchain integration is one of the suggested applications of technology that could help secure the data during transmission, storage, and knowledge discovery. Moreover, by integrating smart contracts, a secure architecture could also assimilate accountability during data exchange	
VTJBC07	Optimized Data Exchange and Storage in Blockchain-Enabled Edge Computing Environments	**Description:** This project proposes a blockchain-based data relay and trading model for edge devices, enabling secure and transparent data sharing. It introduces a novel Proof-of-Data-Trading (PoDT) consensus to balance trust and efficiency. The system ensures tamper-proof transactions and optimizes storage and resource use in edge computing	

CODE	TITLE	APPLICATION / DESCRIPTION	
VTJBC08	Leveraging Blockchain to Transition Social Media from Centralized to Decentralized Models	**Description**: Blockchain, Blockchain-Based Social Media, Consensus Mechanisms, Cryptography, Decentralization, Distributed Ledger, Monetization, Non-Fungible Tokens, Peer-to-Peer, Social Media	IEEE 2024 - NETWORK SECURITY
VTJBC09	A Decentralized Approach to Certificate Authentication and Issuer Trust Using Blockchain	**Description:** This project proposes a blockchain-based system for educational certificate verification, ensuring tamper-proof storage and fast, secure validation through Ethereum. It improves efficiency, reduces costs, and provides a decentralized solution for verifying the authenticity of certificates	IEEE 2025 - BLOCK CHAIN
VTJBC10	End-to-End Security in Smart Homes Using a Consortium Blockchain Approach	**Description:** This project proposes a blockchain-based security framework for IoT smart homes, using a consortium blockchain to enhance data confidentiality, integrity, and access control while minimizing the burden on resource-constrained devices. It integrates with fog computing to ensure secure and efficient data transmission to the cloud	
VTJBC11	Enhancing Data Security with Attribute-Based Encryption and Blockchain Integration	**Description:** This project presents a secure end-to-end IoT communication architecture by combining blockchain with Attribute-Based Encryption (ABE) for decentralized key management and fine-grained access control. It ensures lightweight, tamper-proof, and flexible data sharing in resource-constrained environments. Simulation results show the system achieves fast consensus and reliable performance, making it ideal for scalable IoT deployments	
VTJBC12	Blockchain-Enabled Audit Trail System (BEATS) for Tamper-Proof Data Logging	**Description :** This project introduces BEATS, a blockchain-based efficient audit trail system that ensures secure, tamper-proof, and real-time activity tracking. By using an RSA-based Cryptographic Accumulator, BEATS enables instant transaction verification with constant time and space complexity. It significantly enhances the scalability and practicality of audit systems for large-scale, security-critical applications	
VTJBC13	A Blockchain-Based Secure Data Sharing Architecture for IoT-Fog Environments	**Description:** Technological innovation, Data privacy, Accuracy, Computational modeling, Smart contracts, Throughput, Consensus protocol , Internet of Things, Resource management, Edge computing	
VTJBC14	Application of Blockchain for Securing Confidential Data in Digital Information Infrastructures	**Description :** This project proposes a blockchain-based system to secure sensitive customer data in financial institutions, using SHA-256 encryption and smart contracts for encrypted data sharing, access control, and real-time auditability. It enhances data confidentiality, integrity, and security against unauthorized access and tampering	
VTJBC15	Privacy-Enhanced Redactable Blockchain with Controlled Access in Decentralized Environments	**Description:** This project introduces PriChain, a privacy-preserving redactable blockchain framework that enables fine-grained, authorized data modification while maintaining data confidentiality. It uses multi-authority attribute-based encryption to enforce strict access control and prevent unauthorized redactions	
VTJBC16	A Secure and Scalable Blockchain Model for Data Management Using Attribute-Based Cryptography	**Description:** Blockchains, Security, Hash functions, Data privacy. Experimental results indicate that our blockchain infrastructure achieves enhanced security while maintaining high efficiency.	

CODE	TITLE	APPLICATION / DESCRIPTION
VTJBC17	Privacy-Preserving and Secure Content Sharing in Decentralized Security Systems	**Description**: Security, Servers, Routing, Protocols, Authentication, Access control. The security analysis and performance evaluation shows that the proposed integration scheme is a viable solution to realize our content dissemination model
VTJBC18	A Methodology for Replicating Data in EVM compatible in a Blockchain	**Description:** This paper introduces a methodology for replicating exploit transactions across EVM-compatible blockchains, enabling testing of new security measures. By addressing key challenges in address mapping, contract deployment and storage configuration
VTJBC19	Fort2BCK: Hybrid Cryptographic Validation for Robust Healthcare Data Protection	**Description:** Fort2BCK is a secure blockchain framework designed for healthcare systems, addressing data tampering, unauthorized access, and consensus vulnerabilities. It employs dual-layer verification with RSA, ECDSA, and Zero-Knowledge Proofs to enhance authentication and block integrity. The framework improves resistance to attacks, ensures regulatory compliance, and supports secure, scalable clinical data management
VTJBC20	A Novel Data for Authority Access Data Delegation by Utilizing Self Data sovereign in a identity and verifiable credentials	**Description:** SSI focuses predominantly on direct interactions between two independent entities. It enables direct identification, authentication, authorization, and access to resources and services where the identity holders are the authenticated bearers of their credentials. On the other hand, it does not address primarily indirect identity control, such as delegation, which is an essential part of life situations and natural human relationships.
VTJBC21	Towards Scalable and Trustworthy Indexing in Blockchain: The FlexIM Approach	**Description :** This project introduces FlexIM, an efficient and verifiable index management system for dynamic blockchain queries. Using reinforcement learning and data distribution insights, FlexIM significantly speeds up queries while reducing storage requirements compared to existing systems like vChain+.
VTJBC22	Blockchain-Enabled Framework for Privacy-Preserving Mobile Healthcare Systems	**Description:** This project proposes a blockchain-based framework for secure and scalable mobile healthcare (mHealth) data management, addressing privacy and centralization issues in existing systems. It integrates mobile computing with IPFS and Ethereum blockchain for decentralized, tamper-proof storage and access
VTJBC23	Process Modeling Techniques for Developing Blockchain Applications	**Description :** Blockchains, Decentralized applications, Business, Smart contracts, Authorization, Stakeholders, Software, Finance, Supply chains, Process mining
VTJBC24	Secure Cross-Domain Authentication in IIoT Using Blockchain Technology	**Description:** This project presents a blockchain-assisted cross-domain authentication and key negotiation scheme for IIoT systems, addressing the limitations of traditional centralized methods. By introducing a session token mechanism and leveraging blockchain for secure key updates, it reduces authentication overhead and enhances security.
VTJBC25	PhishDetectPro: A Servlet-Based Smart Wallet Simulation and Approval Phishing Detection Framework Using Intent Validation	**Description:** This project explores approval phishing, a deceptive blockchain scam where users unknowingly grant token access to malicious smart contracts. These contracts, controlled by attackers, are later triggered to steal funds. The attack is made worse by weak wallet UIs that fail to warn users properly. The scam setup includes a sophisticated backend hidden behind CDN layers, managing fake investment sites, fund tracking, and dynamic content

CODE	TITLE	APPLICATION / DESCRIPTION
VTJNW01	Adaptive Clustering for Improved Byzantine Fault Tolerance in Blockchain Systems	**Description**: This project enhances the PBFT-based hybrid blockchain by adding a dynamic clustering layer that monitors node behavior, classifies them into trustworthy, neutral, or suspicious clusters, and adjusts consensus accordingly. This improves resilience against Byzantine faults, even when malicious nodes approach the one-third limit
VTJNW02	Decentralized Genomic Data Sharing and Monetization Using Blockchain and NFTs	**Description:** This project proposes a blockchain and NFT-based solution for genomic data management, allowing individuals to control, secure, and monetize their Raw and Sequenced Genomic Data (RGD and SGD). Using NFTs and smart contracts, the system ensures traceability, secure sharing, and user-controlled access, addressing ownership and privacy challenges in genomic data handling
VTJNW03	Resilient Edge Data Caching: Balancing Popularity Awareness and Server Failures	**Description:** This project introduces the Uncertainty-aware Edge Data Caching (uEDC) framework, which adapts caching strategies to dynamic environments and server reliability issues. It incorporates robust optimization, lightweight encryption, and integrity validation to improve data retrieval latency, reduce costs, and enhance security in Mobile Edge Computing (MEC) systems
VTJNW04	Cross-Chain Ethereum Architecture for Secure and Dynamic Access Management	**Description:** This paper presents an access control architecture that separates access management from data storage, enhancing security and scalability. Using smart contracts and Hyperledger YUI, the system enables dynamic permission verification and secure inter-chain communication, offering a flexible solution for applications requiring strong data governance and compliance
VTJNW05	Asymmetric Updatable Encryption Using ElGamal for Infinite Ciphertext Revisions	**Description :** This article presents an ElGamal-based asymmetric updatable encryption scheme designed to address secure key rotation challenges in cryptographic systems. The scheme allows efficient, secure key updates without decryption, ensuring data confidentiality and integrity.
VTJNW06	Fault-Tolerant Data Distribution in Edge Computing via Erasure Coding: The EdgeHydra Approach	**Description:** EdgeHydra is a fault-tolerant data distribution scheme for edge computing that uses erasure coding to improve file delivery efficiency. By encoding data into both data and parity blocks, it allows edge servers to reconstruct files even with missing blocks, enhancing robustness against delays and failures while reducing distribution times by up to 50.54%.
VTJNW07	A Homomorphic Encryption Method Based on Crowd Networks	**Description :** This method leverages fully homomorphic encryption technology, thereby eliminating the use of plaintext throughout the sensing process and enhancing security compared to traditional encryption methods. Initially, a sensing model is constructed based on the classic crowd sensing architecture. Subsequently, fully homomorphic encryption technology is employed for plaintext-free data transmission
VTJNW08	Cloud-Network-End Security Integration for Smart Wireless Environments	**Description:** Security, Collaboration, Information services, Cloud computing, Semantics, Data communication. Wireless networks review the current research on end system security, network connection security, and cloud services security, respectively.
VTJNW09	Analysis and Optimization of Robust Packet Detection Mechanisms in Random Access Networks	**Description:** Autocorrelation, Receivers, Decoding, Benchmark testing, Wireless sensor networks, Optimization. This study holds considerable implications for the design and deployment of packet-detection schemes networks

CODE	TITLE	APPLICATION / DESCRIPTION	
VTJNW10	Blockchain-Assisted Privacy and Security Enhancement in Federated Learning	**Description**: To effectively address such privacy and security attack issues, this work proposes a Blockchain-based Privacy-preserving and Secure Federated Learning (BPS-FL) scheme, which employs the threshold homomorphic encryption to protect the local gradients of clients	IEEE 2025 - NETWORKING
VTJNW11	Improved Quantum Cryptography: Multi-Qubit BB84 and Entanglement-Based E91 Protocols for Reliable Key Distribution and Data Security	**Description:** This project enhances BB84 and E91 quantum key distribution protocols by increasing qubit counts, adding measurement bases, and integrating error mitigation, enabling secure and reliable communication even in noisy quantum environments	
VTJNW12	Blockchain-Powered Platform for Secure Management and Verification of Educational Credentials	**Description:** This project introduces ElimuChain, a blockchain-based framework for unified academic certificate issuance and verification across all educational levels and institutions. Built on Binance Smart Chain with IPFS integration, it ensures secure, tamper-proof, and decentralized credential management. The system offers a scalable, transparent, and efficient solution to combat certificate fraud and streamline verification for stakeholders	
VTJNW13	Securing IIoT Environments with Blockchain-Enabled End-to-End Protection	**Description:** The main aim of this research is to propose a blockchain-based security framework for the Industrial Internet of Things (IIoT), addressing the challenges of scalability, data integrity, and security. The framework eliminates the need for a centralized authority by utilizing smart contracts for authentication, authorization, and data management, while incorporating lightweight cryptographic schemes and hybrid blockchain implementation for enhanced efficiency and adaptability	
VTJNW14	Secure Multi-Signature Protocol to Counter Transaction Malleability in DeFi	**Description :** This project introduces a robust multi-signature scheme (MSS) designed to protect blockchain-based DeFi protocols from transaction malleability attacks. By enabling joint signatures between users and block producers, and incorporating unmalleable transaction techniques using cryptographic hash functions, the scheme ensures enhanced security and transaction integrity.	
VTJIM01	Smart Reversible Data Hiding for Encrypted Images with Secret Sharing	**Description:** Secret sharing, high embedding, capacity reversible data hiding in encrypted images. This paper innovatively proposes a high capacity RDH-EI scheme that combines adaptive most significant bit (MSB) prediction with secret sharing technology	IEEE 2025 - IMAGE PROCESSING
VTJIM02	Secure Medical Image Sharing With Watermarking In Image Processing	**Description :** This study analyzes various methods for safe medical data sharing, highlighting their advantages and limitations We categorize these approaches into centralized techniques, such as encryption and watermarking, and distributed methods, such as blockchain and federated learning. Additionally, this research examines the evolution of medical image watermarking techniques	
VTJIM03	Enhanced Image Security via Two-Layer Encryption with Switched System Dynamics	**Description:** This research introduces a two-layer image encryption scheme combining control theory and dynamic system modeling to enhance security, addressing vulnerabilities in traditional methods by increasing resistance to cryptanalytic attacks while maintaining computational efficiency	
VTJIM04	Secure And Efficient Encrypted Image Retrieval With Private Share Data	**Description:** We propose SEEIR, a secure and efficient encrypted image retrieval scheme based on ASS. First, SEEIR enhances retrieval security through secure kNN-ASS, a novel method that encrypts index shares across twin clouds to enforce access control. Only users with keys authorized by the data owner can generate valid query vectors	

CODE	TITLE	APPLICATION / DESCRIPTION
VTJIM05	A Grayscale-Guided Approach for RGB Reconstruction from Near-Infrared Images	**Description**: Steganography is utilized in a wide range of practical applications, such as secure communication between individuals or organizations, copyright protection of digital content, and embedding personal details into photographs for smart identity cards. It also plays a role in areas like video-audio synchronization, secure internal data exchange within companies, and improving the reliability of image
VTJIM06	Comprehensive Review and Analysis of a Image processing encryption Techniques	**Description:** This paper provides a comprehensive review of advanced image encryption techniques aimed at preserving the confidentiality and integrity of visual information. The analysis includes traditional cryptographic methods, such as AES, RSA, and Blowfish, as well as quantum encryption, chaos-based encryption, DNA encryption, frequency domain techniques, neural network-based methods, and compressive sensing
VTJIM07	Secure and Reversible Data Hiding Using Edge-Aware and Multi-MSB Self-Prediction	**Description:** Reversible Data Hiding (RDH) allows extra data like timestamps to be embedded into encrypted images without revealing the original image. Traditional methods struggle with encrypted images due to reduced redundancy. This new approach solves that issue, ensuring both data privacy and full image recovery