

CODE	TITLE	APPLICATION / DESCRIPTION
VTJCC01	An Effective Privacy-Preserving Blockchain-Assisted Security Protocol for Cloud-Based Digital Twin Environment	Description: In this article, we first review a recently proposed two-factor authentication protocol for DT environments that utilizes the blockchain technology. Trace authority This entity is the trusted third party that is accountable for the generation of the system parameters and the partial private keys for the entities along with the participant's registration
VTJCC02	Accelerating Finite Field Arithmetic for Homomorphic Encryption on GPUs	Description: Fully Homomorphic Encryption (FHE) is a rapidly developing technology that enables computation directly on encrypted data, making it a compelling solution for security in cloud-based systems. In addition, modern FHE schemes are believed to be resistant to quantum attacks
VTJCC03	Achieving Decentralized and Dynamic SSO-Identity Access Management System for Multi-Application Outsourced in Cloud	Description: As the growing demand in outsourcing system resources such as data and applications to the cloud platform, implementing traditional SSO models to support efficient and fine-grained access control for multi-user and multi-application environment is not practical
VTJCC04	Defense Against Software-Defined Network Topology Poisoning Attacks	Description: The controller learns network topologies and makes traffic forwarding decisions. However, some serious vulnerabilities are gradually exposed in the topology management services of current SDN controller designs
VTJCC05	Attribute-Based Approaches for Secure Data Sharing in Industrial Contexts	Description : Access control, NGAC, fine-grained, attribute-based, encryption, attribute-based access control (ABAC), secure data sharing: The paper concludes by identifying knowledge gaps to provide direction to future research on attribute-based approaches for secure data sharing in industrial contexts.
VTJCC06	Authenticated Distributed Group Key Agreement Protocol Using Elliptic Curve Secret Sharing Scheme	Description: Secret sharing scheme (SSS), key agreement protocol (KAP), group key agreement protocol (GKAP), elliptic curve (EC), elliptic curve discrete logarithm (ECDLP): Elliptic curves are quite popular in resource-constrained environments to produce enough security with smaller key sizes.
VTJCC07	Resource Scheduling in Edge Computing: Architecture, Taxonomy, Open Issues and Future Research Directions	Description : This procedure may completely exploit the edge server's computational and storage capabilities and efficiently execute computing operations. However, transferring all the overflowing computing tasks to an edge server leads to long processing delays and surprisingly high energy consumption for numerous computing tasks.
VTJCC08	A Secure Cloud-Edge Collaborative Fault-Tolerant Storage Scheme and Its Data Writing Optimization	Description: Designing a secure and efficient fault-tolerant storage scheme is urgent and indispensable. Unfortunately, existing fault-tolerant schemes for ESS still retain various drawbacks, including: high edge storage overhead, hard to protect the edge data privacy and low data writing performance.
VTJCC09	A Pairing-Free Certificateless Searchable Public Key Encryption Scheme for Industrial Internet of Things	Description: IIoT data is stored on the cloud service provider's server, the data must be encrypted to protect the user's privacy. However, the encrypted data faces the search problem, which is usually solved by Public Key Encryption with Keyword Search (PEKS).

CODE	TITLE	APPLICATION / DESCRIPTION	
VTJCC10	Key Reduction in Multi-Key and Threshold Multi-Key Homomorphic Encryptions by Reusing ErrorKey Reduction in Multi-Key and Threshold Multi-Key Homomorphic	Description: However, there are several problems for MKHE. First, the ciphertext of MKHE is expanded during homomorphic operations and this expansion is proportional to the number of clients. Second, each client needs to generate the evaluation keys and the outsourcing server must have the evaluation keys of all clients to support homomorphic operations.	IEEE 2023 - CLOUD COMPUTING
VTJCC11	CACPA: Credible Alliance-Chain-Based Public Auditing Scheme for Cloud Storage	Description: Blockchain, cloud storage, public auditing, third-party auditor. Smart contracts to deal with transactions related issues, such as dispute resolution: Any behavior of a TPA node will be inspected by other nodes to maintain good reputation of the group, and malicious behaviors will bring severe punishments.	
VTJCC12	An Efficient Post-Quantum Attribute-Based Encryption Scheme Based on Rank Metric Codes for Cloud Computing	Description: Attribute-based encryption is a valuable technique for ensuring data privacy and confidentiality in the realm of cloud computing. Using this cryptographic primitive, the data owner can securely store and share data within the cloud environment	
VTJCC13	A User-Priorities-Based Strategy for Three-Phase Intelligent Recommendation and Negotiating Agents for Cloud Services	Description: The Recommender system recommends CSP as per users' priorities, which eases the filtration process. The negotiation process provided by IRNAM ensures that users' choices are prioritized with maximum jobs to CSP. IRNAM keeps track of the most critical metrics and can reach decisions quickly and for the best possible deal	
VTJCC14	Secure Cloud-Aided Approximate Nearest Neighbor Search on High-Dimensional Data	Description : One way to handle this problem is to outsource the heavy computing of high-dimensional large-scale data to cloud servers. However, when a cloud server responsible for computing tasks is untrustworthy, some security issues may arise. In this study, we proposed a cloud server-aided LSH scheme and the application model	
VTJCC15	Enabling Balanced Data Deduplication in Mobile Edge Computing	Description: Edge storage system (ESS), is comprised by connected edge servers in a specific area, which ensures low-latency services for users. However, high data storage overheads incurred by edge servers' limited storage capacities is a key challenge in ensuring the performance of applications deployed on an ESS. Data deduplication, as a classic data reduction technology, has been widely applied in cloud storage systems.	
VTJCC16	Solving Task Scheduling Problem in Mobile Cloud Computing Using the Hybrid Multi-Objective Harris Hawks Optimization Algorithm	Description : Mobile devices can run a wide range of programs, and they all require more and more processing power. Due to their limited resources, mobile devices often make use of cloud computing's offloading features to do more complex tasks. The offloading problem in Mobile Cloud Computing (MCC) is the task scheduling problem, which entails deciding where to dump work to maximize its value	IEEE 2023 - DATA MINING
VTJDM01	Delegate and Verify the Update Keys of Revocable Identity-Based Encryption	Description: In this paper, we newly introduce the concept of delegated RIBE (DRIBE) that can delegate the generation of update keys to the semi-trusted cloud server and define the security models of DRIBE. Next, we propose a DRIBE scheme by generically combining a hierarchical IBE (HIBE) scheme, an identity based broadcast encryption (IBBE).	
VTJDM02	A Novel Construction of Updatable Identity Based Hash Proof System and Its Applications	Description: In the previous works, to further provide the continuous leakage resilience for the identity-based encryption scheme, a new cryptography primitive, called updatable identity-based hash proof system (U-IB-HPS), was proposed. perfect key update function or the corresponding security with tight reduction relies on a non-static complexity assumption	

CODE	TITLE	APPLICATION / DESCRIPTION
VTJDM03	Early Predicting of Students Performance in Higher Education	Description: Students learning performance is one of the core components for assessing any educational systems. Student's performance is very crucial in tackling issues of learning process and one of the important matters to measure learning outcomes
VTJDM04	A Diabetes Monitoring System and Health-Medical Service Composition Model in Cloud Environment	Description: Diabetes is a common chronic illness or absence of sugar in the blood. The early detection of this disease decreases the serious risk factor. Nowadays, Machine Learning based cloud environment acts as a vital role in disease detection
VTJDM05	A Rankable Boolean Searchable Encryption Scheme Supporting Dynamic Updates in a Cloud Environment	Description: Searchable encryption, Boolean search, rankable search, dynamic updating, privacy preserving, cryptography: Security analysis proofs that our scheme can ensure security in the known ciphertext model and the known background model.
VTJDM06	Improving Shopping Mall Revenue by Real-Time Customized Digital Coupon Issuance	Description: With the development of bigdata and deep learning technology, bigdata and deep learning technology have also been applied to the marketing field, which was a part of business administration. Customer churn management is one of the most important areas of marketing
VTJDM07	Accountable Clouds Through Blockchain	Description : We show that, through smart contracts, it is possible to create an unforgeable log that can be used for auditing and automatic Service Level Agreement (SLA) verification. As a practical case study, we consider Cloud storage services and define interaction protocols.
VTJDM08	A Consent-Based Privacy-Compliant Personal Data-Sharing System	Description: Personal data is becoming increasingly valuable in business, as the insights that can be obtained from data processing continue to improve. However, it also can cause adverse effects on individuals. To improve data quality while satisfying privacy compliance, companies
VTJDM09	Private Web Search Using Proxy-Query Based Query Obfuscation Scheme	Description : Private web search, web search privacy, query obfuscation, proxy-queries based web search, and information retrieval: we present a novel PWS scheme that uses a proxy-query-based query obfuscation approach. Proxy-query-based query obfuscation is a new study topic in PWS research
VTJDM10	False-Bottom Encryption: Deniable Encryption from Secret Sharing	Description: We show how to implement a deniable encryption method from secret sharing. Unlike the related concept of honey encryption, which employs a preprocessing step in symmetric encryption to re-shape the distribution of a plaintext towards making the real plaintext indistinguishable from a ciphertext for a fake message
VTJDM11	Mining Insights from Esports Game Reviews with an Aspect-Based Sentiment Analysis Framework	Description: To ensure the quality of Esports game services and establish a balanced gaming environment, it is essential to consider the opinions of unprofessional players and comprehensively analyze their reviews. This study proposes a new framework for analyzing Esports reviews of players

CODE	TITLE	APPLICATION / DESCRIPTION	
VTJDM12	PRUS: Product Recommender System Based on User Specifications and Customers Reviews	Description: The main contribution of this research is the inclusion of negative polarity in the analysis of product rankings alongside positive polarity. To account for reviews that contain many sentiments and different elements, the suggested method first breaks them down into sentences	IEEE 2023 - DATA MINING
VTJDM13	Privacy Preserving and Serverless Homomorphic-Based Searchable Encryption as a Service (SEaaS)	Description: This investigates the Accessible Encryption as a Help (SEaaS) and presents a creative protection safeguarding Various Watchword Accessible Encryption (MKSE) plot inside a serverless cloud climate, tending to already neglected security objectives. The proposed plot utilizes probabilistic encryption and influences completely homomorphic encryption to empower procedure on ciphertext, working with look through on scrambled information.	
VTJDM14	Security-Aware Provenance for Transparency in IoT Data Propagation	Description: This paper tackles the challenge of ensuring accurate and secure data delivery in Internet of Things (IoT) systems, where end-users often lack transparency about potential data manipulation risks.	
VTJDM15	Supporting Schema References in Keyword Queries Over Relational Databases	Description: This paper introduces Lathe, a novel Relational Keyword Search (R-KwS) system designed to empower naive or informal users in exploring and retrieving information from relational databases without requiring knowledge of schema details or query languages	
VTJDM16	Leakage-Resilient Anonymous Multi-Receiver Certificate-Based Key Encapsulation Scheme	Description : This refers to the scheme's ability to withstand information leakage. In the context of cryptography, leakage typically refers to unintended disclosure of secret information	
VTJDM17	Normalized Storage Model Construction and Query Optimization of Book Multi-Source Heterogeneous Massive Data	Description: Systematic research and implementation were conducted to solve the problem of how to process, manage, and query multi-source heterogeneous massive book data in the metaverse, improving the utilization value and query efficiency of the data. This study utilized the semi-structured features of book text data to construct an extraction rule model for heterogeneous book data, and effectively extracted massive heterogeneous book information	
VTJNS01	Data Secure De-Duplication and Recovery Based on Public Key Encryption with Keyword Search	Description : In this paper, we focus on how to achieve secure de-duplication and recover data in ciphertext for different users, and determine whether the indexes of public key searchable encryption and the matching relationship of trapdoor are equal in ciphertext to achieve secure de-duplication	IEEE 2023 - NETWORK SECURITY
VTJNS02	Analysis and Design of Secure Sampled-Data Control Subject to Denial-of-Service Attacks	Description: DoS attacks impose constraints on the CPS, where packets may be jammed between the sensor and controller by a malicious entity, potentially resulting in system instability and performance degradation	
VTJNS03	A Data-Driven Smart Evaluation Framework for Teaching Effect Based on Fuzzy Comprehensive Analysis	Description: As consequence, this paper utilizes fuzzy comprehensive analysis to deal with this problem from the perspective of big data mining. In particular, it proposes a data-driven smart evaluation framework for teaching effect based on fuzzy comprehensive analysis	

CODE	TITLE	APPLICATION / DESCRIPTION	IEEE 2023 - NETWORK SECURITY
VTJNS04	Offloading Mechanisms Based on Reinforcement Learning and Deep Learning Algorithms in the Fog Computing Environment	Description: Offloading can be utilized to transfer resource-intensive tasks from resource-limited end devices to a resource-rich fog or cloud layer to reduce end-to-end latency and enhance the performance of the system	
VTJNS05	Automated Firewall Configuration in Virtual Networks	Description: This article focuses on packet filters, i.e., the most common firewall technology used in computer networks, and it proposes a new methodology to automatically define the allocation scheme and configuration of packet filters in the logical topology of a virtual network	
VTJNS06	Privacy-Preserving Searchable Encryption Scheme Based on Public and Private Blockchains	Description: Private blockchain, public blockchain, access control, forward privacy, backward privacy, Privacy-Preserving Searchable Encryption (PPSE) : First, we store an encrypted index in a private blockchain while outsourcing corresponding encrypted documents to a public blockchain	
VTJNS07	A Data Deduplication Scheme Based on DBSCAN With Tolerable Clustering Deviation	Description: To protect data privacy, users prefer to store encrypted data in cloud servers. Cloud servers reduce the cost of storage and network bandwidth by eliminating duplicate copies. To address the potential internal data leakage problem, the concept of clustering deviation is proposed for the first time. We improve the DBSCAN algorithm to tolerate clustering deviation	
VTJNS08	Multiuser Computation Offloading for Long-Term Sequential Tasks in Mobile Edge Computing Environments	Description : Dependencies among computational tasks, resource competition among multiple users, and diverse long-term objectives. Mobile applications typically consist of several functionalities, and one huge category of the applications can be viewed as a series of sequential tasks	IEEE 2023 - IMAGE PROCESSING
VTJIM01	Blockchain-Assisted Verifiable and Secure Remote Sensing Image Retrieval in Cloud Environment	Description: Secure retrieval of remote sensing images in an outsourced cloud environment garners considerable attention. Since the cloud service provider (CSP) is considered as a semi trusted third party that may return incorrect retrieval results to save computational resources or defraud retrieval fees for profit	
VTJIM02	An Efficient Decentralized Identity Management System Based on Range Proof for Social Networks	Description : Decentralized identity, range proofs, blockchain, social network, privacy protection, Online social networks (OSNs): The security analysis shows that our protocol provides stronger privacy protection. We implement a system prototype on the blockchain for evaluation	
VTJIM03	Applicable Image Security Based on Computational Genetic Approach and Self-Adaptive Substitution	Description: Image security, chaotic systems, computational methods, and genetic algorithm, Cryptographic Algorithms: This paper suggests a novel image encryption and decryption technique based on a computational genetic approach and self-adaptive chaotic substitution	
VTJIM04	Reversible data hiding in encrypted images with secret sharing and hybrid coding	Description: Reversible image hiding, iterative encryption, image sharing, high payload and hybrid coding: the encrypted image is shared by a block based CRTSS strategy to generate multiple encrypted shares and the multiple encrypted shares are distributed to multiple data-hider	

CODE	TITLE	APPLICATION / DESCRIPTION
VTJBC01	Data Integrity Audit Scheme Based on Quad Merkle Tree and Blockchain	Description: Meanwhile, our scheme is based on the audit method of the quad Merkle hash tree, using the root of the quad Merkle hash tree to verify the integrity of data, which significantly improves computing and storage efficiency. Automated verification of auditing activities by deploying smart contracts on the blockchain
VTJBC02	Sec-Health: A Blockchain-Based Protocol for Securing Health Records	Description: We propose Sec-Health, a blockchain-based protocol that secures health records, addressing all of the main security and complementary properties defined in current regulations. We show that Sec-Health is a suitable solution by analyzing it under several attack scenarios and describing how it overcomes the problems of existing solutions
VTJBC03	A Comprehensive Survey on Blockchain-Based Decentralized Storage Networks	Description: A decentralized network utilizing end-to-end encryption eliminates the risk of data loss associated with centralized data control by enabling clients to transmit their files securely. The storage providers must prove that they have kept unaltered files in this network for this time
VTJBC04	Secure and Lightweight Blockchain-Enabled Access Control for Fog-Assisted IoT Cloud Based Electronic Medical Records Sharing	Description: As for the advancement of IoT and cloud computing in healthcare, outsourcing encrypted Electronic medical records (EMRs) created by the aggregation of medical treatment applications and health data collected from IoT devices enables high accessibility, effective collaboration, and zero computational operation cost
VTJBC05	Blockchain for Healthcare Management Systems	Description : Blockchain, DSL, health, interoperability, MDE, model, security, smart contracts, software architecture, Health Management Systems: This paper focuses on architectural mechanisms used to support the interoperability and security of Blockchain-based Health Management Systems.
VTJBC06	Blockchain-Based Service-Oriented Architecture for Consent Management, Access Control, and Auditing	Description: Blockchain, consent management, fast healthcare information resources (FHIR), general data protection regulation (GDPR), service-oriented architecture (SOA), business process management (BPM): The experimental results show that blockchain can effectively support sharing consent and audit events among healthcare organizations, supervisory authorities, and individuals
VTJBC07	Dynamic Secure Access Control and Data Sharing Through Trusted Delegation and Revocation in a Blockchain-Enabled Cloud-IoT Environment	Description : Access delegation, blockchain, edge computing, practical Byzantine fault tolerance (PBFT) consensus, revocation, secure data sharing: this research proposes dynamic secure access control using the blockchain (DSA-Block) model, which performs secure access control and data sharing. The data are secured using a differential privacy mechanism
VTJBC08	EFPB: Efficient Fair Payment Based on Blockchain for Outsourcing Services in Cloud Computing	Description: Despite the maturity of cloud services a number of operational challenges remain. For example, how do we ensure trust between outsourcers and workers in a zero-trust environment? While a number of blockchain-based solutions that eliminate the reliance on trusted third parties have been presented, many of these existing approaches do not achieve robust fairness and/or support compatibility with other systems
VTJBC09	Blockchain-Based Process Quality Data Sharing Platform for Aviation Suppliers	Description: A detailed method for the implementation of quality and data security sharing is proposed to support the sharing platform's real-time and orderly operation. Build critical technologies such as manufacturing quality data block packaging models, data storage security sharing.

CODE	TITLE	APPLICATION / DESCRIPTION	
VTJBC10	Heart Disease Prediction Using Novel Quine McCluskey Binary Classifier (QMBC)	Description: Cardiovascular disease is the primary reason for mortality worldwide, responsible for around a third of all deaths. To assist medical professionals in quickly identifying and diagnosing patients, numerous machine learning and data mining techniques are utilized to predict the disease	IEEE 2023 - BLOCK CHAIN
VTJBC11	A Novel Secure and Privacy-Preserving Model for OpenID Connect Based on Blockchain	Description: Open ID Connect (OIDC) is one of the most widely used delegated authentication protocols in web and mobile applications providing a single sign-on experience. It allows third-party applications, called Relying Parties (RP), to securely request and receive information about authenticated sessions and end-users from an identity provider.	
VTJBC12	A Secure Big Data Storage Framework Based on Blockchain Consensus Mechanism with Flexible Finality	Description: Data security and integrity are becoming increasingly important as the volume of data being created and stored grows. A controlled third party that provides most of the existing big data security systems makes them susceptible to several security risks. By resolving current technology challenges, including scalability, non-tampering, trustworthiness, data governance, and transparency, blockchain technology plays a vital role and has a significant potential to safeguard personal information.	
VTJBC13	Blockchain-Enabled Technique for Privacy Preserved Medical Recommender System	Description: The study introduces a Secure Recommendation and Training Technique (SERTT) to address privacy concerns related to the Internet of Medical Things (IoMT) recommender system data. This approach combines federated learning and blockchain methodologies to enhance the security and privacy of IoMT data	
VTJBC14	A Data Integrity Verification Scheme for Centralized Database Using Smart Contract and Game Theory	Description : Currently, many companies and institutions use centralized or distributed databases to store massive amounts of data. However, the use of untrusted centralized third-party auditors can result in security issues because these auditors may be malicious and tamper with or delete user data. This poses a significant challenge for ensuring the reliability of the	
VTJNW01	Task Scheduling in Cloud Computing: A Priority-Based Heuristic Approach	Description : The performance of the proposed model is compared in terms of overall waiting time and CPU time against some existing techniques like BATS, IDEA, and BATS+BAR to determine the efficacy of our proposed algorithms. Additionally, three distinct scenarios have been considered to demonstrate the competency	IEEE 2023 - NETWORKING
VTJNW02	EN - L A K P : L i g h t w e i g h t Authentication and Key Agreement Protocol for Emerging Networks	Description: Software Defined Networking (SDN) and Wireless Sensor Networks (WSNs) will be developed and deployed to improve computing facilities. Micro-electromechanical system (MEMS) technologies advance, and WSNs gain in popularity because they provide real-time monitoring solutions that are both economically and practically viable	
VTJNW03	Threat Model and Defense Scheme for Side-Channel Attacks in Client-Side De-duplication	Description: In client-side de-duplication, if the cloud server detects that the user's outsourced data have been stored, then clients will not need to re-upload the data. However, the information on whether data need to be uploaded can be used as a side-channel, which can consequently be exploited by adversaries to compromise data privacy	

CODE	TITLE	APPLICATION / DESCRIPTION	IEEE 2023 - NETWORKING
VTJNW04	Dynamic Resource Allocation Using an Adaptive Multi-Objective Teaching-Learning Based Optimization Algorithm in Cloud	Description: To bridge the gap between frequently changing customer requirement and available infrastructure for the services, we propose a dynamic resource allocation strategy using an adaptive multi-objective teaching-learning based optimization (AMO-TLBO) algorithm in Cloud computing	
VTJNW05	Intelligent Segment Routing: Toward Load Balancing with Limited Control Overheads	Description: The overheads can greatly reduce the forwarding efficiency for a large network, when segment headers become too long. To achieve the better of two targets, we propose the intelligent routing scheme for traffic engineering (IRTE), which can achieve load balancing with limited control overheads.	
VTJNW06	A Fast Converging and Globally Optimized Approach for Load Balancing in Cloud Computing	Description: Cloud computing, load balancing, swarm intelligence, particle swarm optimization, greywolf optimization: A combined approach of GWO-PSO that capitalizes on the benefits of fast convergence and global optimization is proposed in this paper	