CODE	TITLE	APPLICATION / DESCRIPTION
VTJCC01	Privacy-Preserving and Trusted Keyword Search for Multi-Tenancy Cloud	**Description**: We provide a privacy-preserving, verifiable, accountable, and parallelizable solution for "privacy-preserving keyword search problem" among multiple independent data owners. We consider a scenario in which each tenant is a data owner and a user's goal is to efficiently search for granted documents that contain the target keyword among all the data owners.
VTJCC02	Attribute-Based Searchable Encryption with Forward Security for Cloud-Assisted IoT	**Description:** The data owner punctures the trapdoor to accomplish the data deletion. Then, the deletion process does not need to communicate with a trusted third party and can guarantee forward security.
VTJCC03	PoEDDP-A Fast RSA-Based Proof of Possession Accumulator of Dynamic Data on the Cloud	**Description:** However, the most critical factor is the efficiency of integrity checks, which must prioritize restricted-resource data owners without affecting the performance of the Cloud Service Provider.
VTJCC04	EDASVIC: Enabling Efficient and Dynamic Storage Verification for Clouds of Industrial Internet Platforms	**Description:** We propose an efficient and dynamic storage verification scheme Edasvic for cloud storage in the IIP. We adopt the polynomial commitment to build an efficient homomorphic authenticator, and further design an authenticator accumulator, which can be efficiently generated with limited computational overheads.
VTJCC05	Group Key Management and Sharing Protocol in Cloud Computing Environment	**Description :** As data on cloud is beyond the control area of authentic participants, shared data should be made usable on demand of authentic users. Shared data are vulnerable to misplaced or erroneously altered by Cloud Service Provider (CSP) or attackers.
VTJCC06	Achieving Secure, Verifiable, and Efficient Boolean Keyword Searchable Encryption for Cloud Data Warehouse	**Description:** The Searchable Encryption (SE) technique is palpable for supporting the keyword searches over the encrypted data. Although many SE schemes have introduced their own unique searching methods based on indexing structure on top of searchable encryption techniques, there are no schemes that support Boolean expression queries essential for the search conditions over the DW schema
VTJCC07	Optimal Resource Allocation Using Genetic Algorithm in Container-Based Heterogeneous Cloud	**Description :** The proposed framework simplifies the deployment of cloud services and streamlines workload monitoring and analysis within a diverse cloud system
VTJCC08	Attribute-Based Management of Secure Kubernetes Cloud Bursting	**Description:** Our model addresses the challenges of complexity, cost, and data protection compliance by leveraging both Kubernetes and ABE. We introduce an attribute-based bursting component that uses Kubernetes labels for orchestration, and an encryption component that employs ABE for data protection
VTJCC09	PRBFPT: A Practical Redactable Blockchain Framework With a Public Trapdoor	**Description:** Hence, this paper proposes a practical, redactable blockchain framework with a public trapdoor (hereafter referred to as PRBFPT). PRBFPT comprises an editing scheme for adding blocks using a new type of blockchain with a chameleon hash. Specifically, PRBFPT is able to involve all nodes in the blockchain in the editing operations by means of a public trapdoor, without requiring additional trapdoor management by predefined nodes or organizations

CODE	TITLE	APPLICATION / DESCRIPTION	
VTJCC10	I/O Causality Based In-Line Data Deduplication for Non-Volatile Memory Enabled Storage Systems	**Description**:We propose I/O Causality based In-line Deduplication (ICID) to maximize the deduplication ratio for NVM-based storage systems. Unlike previous inline deduplication schemes that use hash indexes to identify duplicate data slices, ICID records memory-copy operations in a B-tree structure to achieve causality-based inline deduplication.	IEEE 2024 - CLOUD COMPUTING
VTJCC11	Scalable Data Partitioning Techniques for Distributed Data Processing in Cloud Environments	**Description:** Cloud computing is a technology that shows great promise owing to its ability to provide unlimited resources for computing and data storage services. These services are crucial for effectively managing the data according to specific requirements. In the current system, data is saved in the cloud using dynamic data operations and computations	
VTJCC12	Dynamic AES Encryption and Blockchain Key Management: A Novel Solution for Cloud Data Security	**Description:** Traditional methods usually fall short in mitigating risks associated with compromised encryption keys and centralized key storage. To combat these challenges, our proposed solution encompasses a two-phase approach. In the first phase, dynamic Advanced Encryption Standard (AES) keys are generated, ensuring each file's encryption with a unique and ever-changing key	
VTJCC13	Heterogeneous Reconfigurable Accelerator for Homomorphic Evaluation on Encrypted Data	**Description:** We propose a homomorphic evaluation accelerator with heterogeneous reconfigurable modular computing units (RCUs) for the Brakerski/Fan-Vercauteren (BFV) scheme. RCUs leverage operator abstraction to efficiently perform basic sub-operations of homomorphic evaluation such as residue number system (RNS) conversion, number theoretic transform (NTT), and other modular computations.	
VTJCC14	Optimized Encryption-Integrated Strategy for Containers Scheduling and Secure Migration in Multi-Cloud Data Centers	**Description :** This paper presents a novel two-stage container scheduling solution that addresses node imbalances and efficiently deploys containers. The proposed solution formulates the scheduling process as an optimization problem, integrating various objective functions and constraints to enhance server consolidation and minimize energy	
VTJCC15	DEDUCT: A Secure Deduplication of Textual Data in Cloud Environments	**Description:** This paper introduces DEDUCT, an innovative data deduplication method for textual data. DEDUCT employs a hybrid approach that combines cloud-side and client-side deduplication mechanisms to achieve high compression rates while maintaining data security	
VTJCC16	Cloud-assisted Privacy-Preserving Spectral Clustering Algorithm within a Multi-User Setting	**Description :** In response to this challenge, we explore the outsourcing dilemma of spectral clustering in a cloud and multi-user environment and propose a quantum-secure and efficient solution. Specifically, by employing the CKKS homomorphic encryption algorithm within a dual non-collusive server model, we formulate a comprehensive and multi-user spectral clustering outsourcing scheme	
VTJCC17	Efficient Privacy-Friendly and Flexible Wearable Data Processing With User-Centric Access Control	**Description:** In addition, they almost exclusively focus on data aggregation operations, neglecting multiplication and division operations on encrypted data, which are fundamental operations with significant importance in various application scenarios. In this paper, we present efficient and privacy-preserving schemes for multiplication and division operations with fine-grain data-sharing and user-centric access control capabilities, called SAMM and SAMD, respectively	
VTJDM01	Dynamic Searchable Symmetric Encryption With Strong Security and Robustness	**Description:** Dynamic Searchable Symmetric Encryption (DSSE) is a prospective technique in the field of cloud storage for secure search over encrypted data. A DSSE client can issue update queries to an honest-but-curious server for adding or deleting his ciphertexts to or from the server and delegate keyword search over those ciphertexts to the server. Numerous investigations focus on achieving strong security	IEEE 2024 DATA MINING

CODE	TITLE	APPLICATION / DESCRIPTION
VTJDM02	A Novel Proxy Re-Encryption Technique for Secure Data Sharing in Cloud Environment	**Description**: Due to the data owners' lack of trust, they save their data in an encrypted format that is inaccessible to outsiders. The phrase "proxy re-encryption" (PRE) refers to a popular way of delivering encrypted data stored in the cloud
VTJDM03	Comment on "Expressive Public-Key Encryption with Keyword Search: Generic Construction from KP-ABE and an Efficient Scheme Over Prime-Order Groups"	**Description:** An expressive PEKS scheme is a variant of the PEKS scheme that supports conjunctive and disjunctive searches (expressive search).
VTJDM04	An Implementation for Secure Data Deduplication on End-to-End Encrypted Documents	**Description:** Reconciling client-side encryption with cross-user deduplication is an active research topic. We present the first secure cross-user deduplication scheme that supports client-side.
VTJDM05	Prediction of Chronic Kidney Disease - A Machine Learning Perspective	**Description:** Chronic Kidney Disease dataset has been taken from the UCI repository. Seven classifier algorithms have been applied in this research such as artificial neural network, C5.0, Chi-square Automatic interaction detector, logistic regression, linear support vector machine with penalty L1 & with penalty L2 and random tree
VTJDM06	Enhancing the prediction of employee turnover with knowledge graphs and explainable AI	**Description :** The proposed methodology extends beyond prediction and incorporates explainable artificial intelligence (XAI) techniques to unearth the pivotal factors influencing an employee's decision to either remain with or depart from a particular organization. The empirical analysis was conducted using a comprehensive dataset from IBM that includes the records of 1,470 employees
VTJDM07	A Reinforcement Learning Based Recommendation System to Improve Performance of Students in Outcome Based Education Model	**Description:** A single course may contain one or more CLOs. These CLOs are then mapped to PLOs and PLOs are then mapped to PEOs. Therefore, our objective in this work is to improve deficient/weak CLOs of students by suggesting online resources. Whereas, in the absence of this proposed system, students have to find out these resources by themselves or course teacher recommends relevant online resources
VTJDM09	A Secure Medical Data Sharing Framework for Fight Against Pandemics Like Covid-19 by Using Public Blockchain	**Description:** However, they still have flaws in granting full authorization to individuals, ensuring the security of personal information, speed, and scalability. They mostly use private or consortium blockchains. However, in a public blockchain, a system that everyone can participate in and follow provides more reliable information
VTJDM10	Secure Sharing Architecture of Personal Healthcare Data Using Private Permissioned Blockchain for Telemedicine	**Description:** Telemedicine primarily aims to facilitate the transmission of healthcare data through electronic channels, enabling users to access medical services. It supports healthcare services around the globe, aids in early diagnosis and treatment, and assists with remote care by provisioning effective healthcare that is safe, secure, and reliable
VTJDM11	Investigating Gender and Age Variability in Diabetes Prediction: A Multi-Model Ensemble Learning Approach	**Description:** Leveraging the capabilities of ensemble learning, an advanced technique that combines multiple models, the predictive model's efficiency is substantially enhanced, resulting in precise and reliable predictions of individuals' diabetic status. Addressing the challenge of diabetes prediction, a novel ensemble learning model was proposed.

CODE	TITLE	APPLICATION / DESCRIPTION	
VTJDM12	Blockchain-Enabled Framework for Transparent Land Lease and Mortgage Management	**Description:** We present a Blockchain driven system that not only tackles alteration and double-spending issues in traditional systems but also implements distributed data management. Current state-of-the-art solutions do not fully incorporate crucial features of Blockchain, such as transparency, prevention of double-spending, auditability, immutability, and user participation	IEEE 2024 - DATA MINING
VTJDM13	Enhancing Gun detections with transfer learning and YAMNet Audio classification	**Description:** The Mel spectrograms created from the collected features are used for multi-class audio classification, which makes it possible to identify different types of guns. 1174 audio samples from 12 distinct weapons make up the study's extensive dataset, which offers a varied and representative collection for training and evaluation	
VTJDM14	A Novel Early Detection and Prevention of Coronary Heart Disease Framework Using Hybrid Deep Learning Model and Neural Fuzzy Inference System	**Description:** This work proposed an Optimal Scrutiny Boosted Graph Convolutional LSTM (O-SBGC-LSTM), SBGC-LSTM enhanced by Eurygaster Optimization Algorithm (EOA) to tune hyper-parameters for early prevention and detection of diabetes disease	
VTJDM15	Scalable and Popularity-Based Secure Deduplication Schemes With Fully Random Tags	**Description :** Our scheme uses homomorphic encryption (HE) to generate comparable random tags to record data popularity and then uses the binary search in the AVL tree to accelerate the tag comparisons. Besides, we find the popularity tamper attacks in existing schemes and design a proof of ownership (PoW) protocol against it	
VTJDM16	IPO-PEKS: Effective Inner Product Outsourcing Public Key Searchable Encryption From Lattice in the IoT	**Description:** Public-key Encryption with Keyword Search (PEKS) allows customers to search for target encrypted files using keywords. However, the majority of PEKS implementations are unable to repel malicious quantum-capable attackers	
VTJDM17	Enhancing IoT Security and Efficiency: A Blockchain Assisted Multi-Keyword Searchable Encryption Scheme	**Description:** The attribute-based searchable encryption (ABSE) as been used within IoT to maintain data privacy and integrity. However, existing ABSE approaches often rely on centralized systems that are susceptible to single-point failures and are inefficient in terms of decryption and data retrieval	
VTJDM18	Medical Image Encryption through Chaotic Asymmetric Cryptosystem	**Description:** The encryption process initiates with a secure key exchange mechanism using elliptic curves and the Blum-Goldwasser Cryptosystem. Pixel randomization is achieved through a chaotic map, followed by encryption using ECC and BGC, which integrates the discrete logarithmic problem, probabilistic encryption, and the quadratic residuosity problem.	
VTJNS01	Leakage-Resilient Anonymous Heterogeneous Multi-Receiver Hybrid Encryption in Heterogeneous Public-Key System Settings	**Description:** Very recently, several leakage-resilient anonymous multi-receiver encryption (LR-AMRE) schemes based on various public-key systems were also proposed. However, these LR-AMRE schemes are not suitable for a heterogeneous public-key environment under which an authorized receiver group includes heterogeneous receivers under various PKS settings and these receivers have various types of secret/public key pairs	IEEE 2024 - NETWORK SECURITY
VTJNS02	Formal Verification of Data Modifications in Cloud Block Storage Based on Separation Logic	**Description:** Formal verification of these operations can improve the reliability of CBS to some extent. Although separation logic is a mainstream approach to verifying program correctness, the complex architecture of CBS creates some challenges for verifications	

CODE	TITLE	APPLICATION / DESCRIPTION
VTJNS03	An Efficient IoT-Fog-Cloud Resource Allocation Framework Based on Two-Stage Approach	**Description**: One common feature of the fog paradigm is its limitations in capabilities, which make it unsuitable for processing large volumes of data. To ensure the smooth execution of delay-sensitive application tasks and the large volume of data generated, there is a need for the fog paradigm to collaborate with the cloud paradigm to achieve a common goal
VTJNS04	Multi-Smart Meter Data Encryption Scheme Based on Distributed Differential Privacy	**Description:** We use an improved homomorphic encryption method to realize the encryption aggregation of users' data. Second, we propose a double-blind noise addition protocol to generate distributed noise through interaction between users and a cloud platform to prevent semi-honest participants from stealing data by colluding with one another
VTJNS06	AES Security Improvement by Utilizing New Key-Dependent XOR Tables	**Description:** In this article, we propose an algorithm to create new, key-dependent XOR tables from an initial secret key. At the same time, we prove that in the ciphertext the new XOR operation can preserve the independent, co-probability distribution of the random key
VTJNS07	Ethereum Blockchain Framework Enabling Banks to Know Their Customers	**Description:** The potential of blockchain technology in revolutionizing the KYC process has been acknowledged globally. Blockchain technology provides a decentralized platform for storing customer data, enabling financial institutions to access the information seamlessly.
VTJNS08	An Efficient Task Scheduling for Cloud Computing Platforms Using Energy Management Algorithm: A Comparative Analysis of Workflow Execution Time	**Description :** To facilitate comparison, the number of virtual machines in the Visual Studio.Net framework environment is used for the implementation. The experimental findings indicate that increasing the number of virtual machines reduces Makespan. Moreover, the Energy Management Algorithm (EMA) outperforms
VTJNS09	AASSI: A Self-Sovereign Identity Protocol With Anonymity and Accountability	**Description:** In this paper, we bridge this gap by introducing AASSI, a pioneering SSI protocol meticulously designed to balance the twin imperatives of privacy and accountability. Specifically, AASSI extends support for anonymity, self-derivation, fine-grained tracing and selective revocation
VTJNS10	A Comparative Analysis of Metaheuristic Techniques for High Availability Systems	**Description :** In cloud environments, dynamic management of load balancing is crucial. This study explores how virtual machines can effectively remap resources in response to fluctuating loads dynamically, optimizing overall network performance. The core of this research involves an in-depth analysis of several metaheuristic algorithms applied to load balancing in cloud computing
VTJNS11	MS-FL: A Federated Learning Framework Based on Multiple Security Strategies	**Description:** To address these issues, this paper proposes a novel federated learning framework MS-FL based on multiple security strategies. The framework's algorithms guarantee that data providers need not worry about data privacy leakage. At the same time, it can defend against poisoning attack from malicious nodes
VTJBC01	PASSP: A Private Authorization Scheme Oriented Service Providers	**Description:** We propose a private authorization scheme oriented service providers. A decentralized publicly-verifiable re-encryption method based on IPFS is proposed to minimize the reliance on service providers, by shifting to a distributed storage and computation model

CODE	TITLE	APPLICATION / DESCRIPTION
VTJBC02	PEEV: Parse Encrypt Execute Verify—A Verifiable FHE Framework	**Description**: Homomorphic encryption can be used to allow processing directly on encrypted data, but a dishonest cloud provider can alter the computations performed, thus violating the integrity of the results. To overcome these issues, we propose PEEV (Parse, Encrypt, Execute, Verify), a framework that allows a developer with no background in cryptography to write programs operating on encrypted data
VTJBC05	Blockchain-Assisted Hierarchical Attribute-Based Encryption Scheme for Secure Information Sharing in Industrial Internet of Things	**Description:** To address the need to exchange data between logistics networks, we proposed a novel decentralized hierarchical attribute-based encryption (HABE) scheme combining edge computing and blockchain. To begin, we offer an IoT data encryption strategy in which edge devices can send data to a nearby cloud network for data processing while maintaining privacy
VTJBC06	Secure Reviewing and Data Sharing in Scientific Collaboration: Leveraging Blockchain and Zero Trust Architecture	**Description:** Under this mechanism, only the assigned reviewer would have access to the confidential manuscript, ensuring the integrity of the review process. In scientific collaborations, the imperative for confidential data sharing extends beyond reproducibility to encompass vital collaborative endeavors such as publications, Memorandums of Understanding (MoUs), grants, and funding
VTJBC07	Blockchain-Based KYC Model for Credit Allocation in Banking	**Description:** Furthermore, a centralized system permits collaboration and operation execution by multiple financial institutions. Aside from these two scenarios, KYC processes can also be executed via a blockchain-based system
VTJBC08	Public Edu Chain: A Framework for Sharing Student-Owned Educational Data on Public Blockchain Network	**Description :** PublicEduChain allows students to store their data in smart contracts created on the public Ethereum network, making it possible to share this information with any educational institution and administrative units. Educational institutions can access student data stored in smart contracts on the public Ethereum network through Learning Management System (LMS) applications and can add data to these contracts. PublicEduChain ensures that data is managed under student ownership within a fully decentralized infrastructure
VTJBC09	Blockchain Based Logging to Defeat Malicious Insiders: The Case of Remote Health Monitoring Systems	**Description**: Malicious insiders may tamper, steal or change patients' health data, which results in a loss of patient trust in these systems. Audit logs in the cloud, which may point to illegal data access, may also be erased or forged by malicious insiders as they tend to have technical knowledge and privileged access to the system. Thus, in this work, we propose a Cloud Access Security Broker (CASB) model that (a) logs every action performed on user data and (b) secures those logs by placing them in a private blockchain that is viewable by the data owners.
VTJBC10	Blockchain Based an Efficient and Secure Privacy Preserved Framework for Smart Cities	**Description :** The centralized repository that is currently in place made the majority of hacks possible. The sharing of sensitive data and authentication are essential stages in guaranteeing the security of applications associated with IoT. Blockchain and IoT are two widely used technologies, with IoT focusing on data collection via various devices and blockchain enabling data integrity
VTJBC11	Research on the privacy protection technology of Blockchain spatiotemporal big data	**Description:** In this context, data holders often opt for cloud storage of their data to mitigate the pressure of local storage and computing overhead. However, this centralized storage mode renders the data susceptible to risks of tampering and leakage due to the absence of physical control over spatiotemporal big data
VTJBC12	A New Identity Authentication and Key Agreement Protocol Based on Multi-Layer Blockchain in Edge Computing	**Description:** In the edge computing environment, with the frequent cross-domain authentication and data sharing of IoT devices in different security domains, identity authentication faces a series of challenges and security issues. Most of the traditional identity authentication methods are based on public key infrastructure

CODE	TITLE	APPLICATION / DESCRIPTION	
VTJBC13	Stub Signature-Based Efficient Public Data Auditing System Using Dynamic Procedures in Cloud Computing.	**Description :** we suggest proposing a partial signature-based data auditing system so that both privacy and accuracy can be fortified while reducing the computational cost associated with auditing processes significantly. This system would involve using cryptographic techniques such as homomorphic encryption and hash functions, which would enable secure sharing between multiple parties while ensuring integrity checks on stored files at regular intervals for any potential tampering attempts made by external attackers or malicious insiders who may try to gain unauthorized access into confidential user information stored within cloud sites.	IEEE 2024 - BLOCK CHAIN
VTJBC14	Effective Identity Authentication Based on Multi-attribute Centers for Secure Government Data Sharing	**Description:** To address these issues, we suggest proposing a partial signature-based data auditing system so that both privacy and accuracy can be fortified while reducing the computational cost associated with auditing processes significantly. This system would involve using cryptographic techniques such as homomorphic encryption and hash functions	
VTJNW01	Intelligent SLA Selection Through the Validation Cloud Broker System	**Description:** Cloud computing has transformed digital service delivery by providing scalable, flexible access to computing resources, including servers, storage, and applications, under a pay-per-use model	IEEE 2024 - NETWORKING
VTJNW05	Incentive-Vacation Queueing for Edge Crowd Computing	**Description:** We analyze an orchestrated ECC where devices rent resources in exchange for incentives. Our incentive-vacation queueing (IVQ) model associates performance with incentive payments using vacation queueing, considering the multitenancy of devices through a server vacation dependent on incentives received	
VTJNW06	Concise and Efficient Multi-Identity Fully Homomorphic Encryption Scheme	**Description :** However, MKFHE schemes used to construct MIBFHE usually have complex construction and large computational complexity, which also causes the same problem for MIBFHE schemes	
VTJNW07	Digitalized and Decentralized Open-Cry Auctioning: Key Properties, Solution Design, and Implementation	**Description:** In this paper, we identify the key properties for the development of decentralized open-cry auctioning systems, including verifiability, transaction immutability, ordering, and time synchronization. Three prominent blockchain platforms, namely, Ethereum, Hyperledger Fabric, and R3 Corda were analyzed in terms of their capabilities to ensure these properties for gap identification	
VTJNW08	ACO-Based Scheme in Edge Learning NOMA Networks for Task-Oriented Communications	**Description :** In this paper, we propose efficient communications under a task-oriented principle by optimizing power allocation and edge learning-error prediction in an edge-aided non-orthogonal multiple access (NOMA) network. Furthermore, we propose a novel approach based on the ant colony optimization (ACO) algorithm to jointly minimize the learning error and optimize the power allocation variables	
VTJNW09	Non-Fungible Token Enhanced Blockchain Based Online Social Network	**Description:** One of the reasons for such a growth is their features such as ubiquitous access, on-demand service, friendship networks, user engagement strategies like recommendation engines, etc. However, there are various limitations to the current approach, such as the centralization of control, lack of data ownership, poor access control, fake news, bot accounts, censorship, digital rights management issues, etc	
VTJNW10	REHREC: Review Effected Heterogeneous Information Network Recommendation System	**Description:** Although user and business nodes have been used in HINs, review contents have not been used. In this work, we use review nodes in HINs in addition to user and business nodes. Since written reviews provide valuable insights into points of interest within recommendation systems, integrating review nodes into HINs allows us to assess their impact on recommendation systems.	

CODE	TITLE	APPLICATION / DESCRIPTION
VTJNW11	Federated Learning for Decentralized DDoS Attack Detection in IoT Networks.	**Description**: This study introduces a Federated Learning-based approach, named Federated Learning for Decentralized DDoS Attack Detection (FL-DAD), which utilizes Convolutional Neural Networks (CNN) to efficiently identify DDoS attacks at the source.
VTJNW12	Innovative Energy-Efficient Proxy Re-Encryption for Secure Data Exchange in Wireless Sensor Networks.	**Description:** The proposed PRE scheme optimizes efficiency by integrating lightweight symmetric and asymmetric cryptographic techniques, thereby minimizing computational costs during PRE operations and conserving energy for resource-constrained nodes. In addition, the scheme incorporates sophisticated key management and digital certificates to ensure secure key generation and distribution