CODE	TITLE	DESCRIPTION
VTJCC01	Toward Automated Security Analysis and Enforcement for Cloud Computing Using Graphical Models for Security	We proposed a novel framework Cloud Safe that extends its features to deploy optimal security countermeasures in the cloud.
VTJCC02	Data Integrity Audit Based on Data Blinding for Cloud and Fog Environment	This paper proposes a data integrity audit scheme based on data blinding. This scheme uses the edge devices in the transmission node to establish a fog computing layer between the cloud service provider and the data owner to reduce transmission delay. The subordinate distribution relationship and weight between fog nodes. dynamically allocate the optimal path and transmit the data to reduce transmission delay.
VTJCC03	Secure Data Storage and Sharing Techniques for Data Protection in Cloud Environments	Typically, data protection is achieved through leakage prevention and leaker detection and this article concentrates on achieving efficient protection by preventing leakage and detecting the malicious entity responsible for leakage as Depicted. The major approaches for preventing data leakage are tailored by utilizing cryptography, access control mechanisms, and differential privacy with machine learning techniques while leaker detection is mainly achieved
VTJCC04	An Encrypted Cloud Email Searching and Filtering Scheme Based on Hidden Policy Ciphertext-Policy Attribute-Based Encryption with Keyword Search.	Innovatively applies the ABKS design to the encrypted cloud email scenario. The sender creates an additional list of recipients for searching and filtering and adds the recipient filtering server to this list of recipients. The user' attributes in this recipient list are used as the access control policy of the encrypted keyword index. Therefore, the recipients can search keywords by their attributes, and, in turn, the recipient filtering server can filter keywords by its own attributes
VTJCC05	Privacy Preserving Data Mining Framework for Negative Association Rules: An Application to Healthcare Informatics	Data mining in healthcare must be done in a way that protects the identity of patients, especially when dealing with sensitive information. However, revealing this information puts it at risk of attack. Healthcare data privacy protection has lately been addressed by technologies that disrupt data (data sanitization) and reconstruct aggregate distributions in the interest of doing research in data mining
VTJCC06	A Fair Dynamic Load Balanced Task Distribution Strategy for Heterogeneous Cloud Platforms Based on Markov Process Modeling	In such a scenario, the VM is unable to handle a percentage of these tasks, which remain unprocessed and unaccomplished. Thus, proper VM selection is required during task distribution, which is usually based on the current workload. However, the current workload alone may not be a good criterion. This is because the workload on different machines may vary because of differences in their computing capacities
VTJCC07	Privacy-Preserving Public Auditing for Shared Cloud Data with Secure Group Management	When data is stored in the cloud, there is a risk of data loss because users lose direct control over their data. To solve this problem, many cloud storage auditing techniques have been studied. proposed a public auditing scheme for shared data that supports data privacy, identity traceability, and group dynamics
VTJCC08	Utilizing Microservices Architecture for Enhanced Service Sharing in IoT Edge Environments.	As a result, edge computing (also known as fog computing) has been proposed to overcome the two limitations of utilizing cloud resources [1]. Fog nodes (also known as edge servers) [2] are defined as virtualized platforms placed at the edge of the network to bring cloud services closer to IoT nodes. The local processing introduced by the resultant Cloud-Fog-IoT architecture provides great benefits such as supporting latency-sensitive applications, enhanced privacy, and reduced workloads reaching the backbone of the network
VTJCC09	A Particle Swarm Optimization with Lévy Flight for Service Caching and Task Offloading in Edge-Cloud Computing	Given the service caching solution, LMPSO uses a heuristic method with three stages for task offloading, where the first stage tries to make full use of cloud resources, the second stage uses edge resources for satisfying requirements of latency-sensitive tasks, and the last stage improves the overall performance of task executions by re-offloaded some tasks from the cloud to edges

CODE	TITLE	DESCRIPTION	
VTJCC10	An Efficient Hybrid Ranking Method for Cloud Computing Services Based on User Requirements	Analytical hierarchy process (AHP) and fuzzy logic are used to rank cloud services. Furthermore, a fuzzy Delphi filtering method is proposed to decrease the execution time of ranking cloud services	IEEE 2022 - CLOUD COMPUTING
VTJDM01	Achieve Privacy-Preserving Priority Classification on Patient Health Data in Remote e-Healthcare System	Specifically, to reduce the system latency, we design a non-interactive privacy-preserving priority classification algorithm, which allows the WBAN gateway to conduct the privacy-preserving priority classification for the received users' medical packets by itself and relay these packets according to their priorities (criticalities)	IEEE 2022 - DATA MINING
VTJDM02	Mining Transactional Databases for Frequent and High Utility Fuzzy Sequential Patterns with Time Intervals	The application of fuzzy theory in sequential pattern mining has also been favored leading to more natural linguistic representation. Researchers have proposed various hybrid algorithms with fuzzy of any one parameter, such as time or quantity	
VTJDM03	Trapdoor Privacy in Public Key Encryption with Keyword Search	Keyword privacy prevents any information leaked from the keyword itself, and similarly trapdoor privacy prevents any information leaked from the trapdoor side	
VTJDM04	Privacy Preserving Attribute-Focused Anonymization Scheme for Healthcare Data Publishing	According to privacy regulations and ethical requirements, it is essential to preserve the privacy of patients before sharing data for medical research. State-of-the-art literature on privacy preserving studies either uses cryptographic approaches to protect the privacy or uses anonymizing techniques regardless of the type of attributes, this results in poor protection and data utility	
VTJDM05	Optimized Re-linearization Algorithm of the Multi-key Homomorphic Encryption Scheme	First, we reduce the scale of the evaluation key by increasing its modulus instead of using a gadget vector to decompose the user's public key and extend the cipher text of homomorphic multiplication. Second, we use rescaling technology to optimize the re-linearization algorithm; thus, the error bound of the cipher text is reduced, and the homomorphic operation efficiency is improved	
VTJDM06	Analysis and Prediction of Students Academic Performance Based on Educational Data Mining	In order to avoid unreasonable evaluation results and monitor the students' future performance in advance, this paper comprehensively uses the relevant theories of clustering, discrimination and convolution neural network to analyze and predict students' academic performance	
VTJDM07	An Efficient Search Method Using Features to Match Joint Keywords on Encrypted Cloud Data	It proposes an efficient search method using features to match joint keywords (FMJK) on encrypted cloud data. This method proposes that each *d* keywords are randomly selected from the non-duplicated keywords, which are extracted from the documents of the data owner, to generate a joint keyword, and all joint keywords form a keyword dictionary	
VTJDM08	Can We Predict Student Performance Based on Tabular and Textual Data?	We first collect a dataset that included student behavior data and course comments textual data. Then we fuse the student behavior data with course comments textual data to predict student performance, using a Transformer-based framework with a uniform vector representation	

CODE	TITLE	DESCRIPTION	
VTJDM09	A Systematic Review Towards Big Data Analytics in social media	People are open to sharing opinions, views, and ideas on any topic in different formats out loud. This creates the opportunity to make the "Big Social Data" handy by implementing machine learning approaches and social data analytics. This study offers an overview of recent works in social media, data science, and machine learning to gain a wide perspective on social media big data analytics	IEEE 2022 - DATA MINING
VTJDM10	Enhanced Search Engine Using Proposed Framework and Ranking Algorithm Based on Semantic Relations	A novel of ranking algorithm and mathematical model of calculating semantic score is developed to order and classify the relevant results of unclear query based on semantic relations	
VTJDM11	ESVSSE: Enabling Efficient, Secure, Verifiable Searchable Symmetric Encryption	Symmetric Searchable Encryption (SSE) is deemed to tackle the privacy issue as well as the operability and confidentiality in data outsourcing. However, most SSE schemes assume that the cloud is honest but curious. This assumption is not always applicable. And even if some schemes supported verification, integrity or freshness checking in a malicious cloud, but the performance and security functionalities are not fully exploited	
VTJDM12	Extremely Randomized Trees with Privacy Preservation for Distributed Structured Health Data.	One main difficulty lies in analyzing such data without compromising patients' privacy and personal data, which is a primary concern in healthcare applications	
VTJDM13	DSAS: A Secure Data Sharing and Authorized Searchable Framework for e-Healthcare System	In e-healthcare system, an increasing number of patients enjoy high-quality medical services by sharing encrypted personal healthcare records (PHRs) with doctors or medical research institutions. However, one of the important issues is that the encrypted PHRs prevent effective search of information, resulting in the decrease of data usage	
VTJNW01	NDPsec: Neighbor Discovery Protocol Security Mechanism	The performance is measured in terms of processing time, traffic overhead, and resilience against network-based attacks. The results obtained from the experiments showed that NDPsec successfully prevented cyberattacks, with approximately 144% less processing time and over 50% less traffic overhead compared to SeND (the default security mechanism for NDP protocol)	IEEE 2022 - NETWORKING
VTJNW02	Efficient Multi-Client Functional Encryption for Conjunctive Equality and Range Queries	The decryption algorithm on the multiple cipher texts of the same time period. MC-FE for predicates can be used for a network event or medical data monitoring system based on time series data gathered by multiple clients	
VTJNW03	VeriDedup: A Verifiable Cloud Data Deduplication Scheme with Integrity and Duplication Proof	Although previous solutions adopt message-locked encryption along with Proof of Retrievability (PoR) to check the integrity of deduplicated encrypted data, they ignore proving the correctness of duplication check during data upload and require the same file to be derived into same verification tags, which suffers from brute-force attacks and restricts users from flexibly creating their own individual verification tags	
VTJNW04	Secret Key Generation by Continuous Encryption Before Quantization	The first transformed by a continuous encryption function into a pair of sequences of quasi-continuous pseudo-random numbers (QCPRNs) of any desired length, and then these QCPRNs are quantized into keys. We show that CEbQ can yield a much lower key error rate than direct quantization subject to standardized randomness tests	

CODE	TITLE	DESCRIPTION	
VTJNW05	Efficient Anonymous Authentication for Wireless Body Area Networks	Anonymous authentication schemes were proposed to resolve this challenge, and latest schemes ensure that even if a WBAN client's private key is exposed, previous session keys generated by this client cannot be compromised (known as forward security).	IEEE 2022 - NETWORKING
VTJNW06	Research on Data Routing Strategy of Deduplication in Cloud Environment	However, the cluster data duplication technology also brings new issues on de-duplication rate reduction and load balancing of storage nodes. The application of data routing strategy can well balance the problem of de-duplication rate and load balancing	
VTJNW07	PRMS: Design and Development of Patients' E-Healthcare Records Management System for Privacy Preservation in Third	Block chain technology rescues the CSPs by providing the robust security to the underlying data by encrypting data using the unique and secret keys. Each network user in Block chain has its own unique and secret keys linked directly to the transaction keys as a digital signature to protect the data	
VTJNW08	Surgical DDoS Filtering With Fast LPM	The potential of longest prefix matching (LPM) for enforcing precise DDoS scrubbing policies seems to be overlooked in contemporary packet filtering data paths	
VTJNW09	Localization Of Data Injection Attacks on Distributed M-Estimation	We begin with a novel data injection attack scheme, and its effects on decentralized optimization algorithms, and primarily DPG	
VTJNW10	Cross-Platform Reputation Generation System Based on Aspect-Based Sentiment Analysis	This system aims at generating a reputation value toward online entities (movies, hotels, restaurants, services, etc.) and computing a satisfaction score toward each aspect of the target entity by processing textual and numerical data collected from multiple platforms	
VTJNW11	Detecting and Mitigating Collusive Interest Flooding Attacks in Named Data Networking	Named Data Networking (NDN) has recently appeared as a new paradigm to solve many shortcomings in the current TCP/IP architecture. Its main characteristics like stateful forwarding and in-network caching made NDN networks an efficient environment for data delivery where the data is	
VTJNS01	A Method for Endpoint Aware Inspection in a Network Security Solution	The method utilizes a subset of the protected network to gather hash fingerprints from the endpoint application network traffic patterns. The information gathered from this subset is then utilized for gaining endpoint awareness for the rest of the protected network	IEEE 2022 - NETWORK SECURITY
VTJNS02	Privacy Preserving Image Watermark Embedding Method Based on Edge Computing	We had proposed a perturbing encryption method with homomorphism to ensure the information security and the correctness of discrete wavelet transformation in the encrypted domain. In addition, the framework was designed to guarantee the safety of singular value decomposition that edge server could not recover the original image matrix	

CODE	TITLE	DESCRIPTION	
VTJNS03	Autonomous Path Identity-Based Broadcast Proxy Re-Encryption for Data Sharing in Clouds	Cloud computing with massive storage and computing capabilities has become widespread in actual applications. It is critical to ensure secure data sharing in cloud-based applications	
VTJNS04	An Improvement of Security Scheme for Radio Environment Map Under Massive Attacking	However, an open characteristic environment always leads to a security problem; for example, when malicious terminals exist in the environment and data falsification attacks occur, the accuracy of the REM is affected by the malicious action. In this study, we improve the double-layer monitor algorithm by optimizing the reward penalty function using a similarity comparison and sustainable monitor	
VTJNS05	A Secure Optimization Routing Algorithm for Mobile Ad Hoc Networks	The fuzzy clustering algorithm is activated first, and the Cluster Heads (CHs) are selected depending on the value of indirect, direct, and recent trust that each CH has. In addition, value nodes were discovered based on trust levels. Moreover, the CHs are engaged in multi hop routing, and the selection of the ideal route is based on the projected protocol, which selects the best routes based on latency, throughput, and connection within the course's boundaries	
VTJNS06	Privacy Enhanced and Verifiable Compressed Sensing Reconstruction for Medical Image Processing on the Cloud	Our design is privacy-enhanced. Our design cannot only protect the privacy of the original image, but also blind the sampled signal, the sensing matrix and the solution vector of the convex optimization problem. We argue the one-way privacy of the above information under the chosen-plaintext attack with rigorous theoretical analysis	
VTJNS07	A Robust Chaos-Based Technique for Medical Image Encryption	This paper recommends a novel hybrid encryption/decryption scheme that can be applied in e-healthcare, or IoHS, for the protection of medical images	
VTJNS08	Dynamic Virtual Machine Consolidation Algorithm Based on Balancing Energy Consumption and Quality of Service	The physical host; second, the resource-demand scaling of physical hosts is not considered during virtual machine (VM) placement, which results in the lack of accuracy in selecting suitable hosts. In view of the above problems	
VTJNS09	Emotion Analysis Using Multilayered Networks for Graphical Representation of Tweets	The current paper proposes a novel algorithm referred to as the Multi-Layered Tweet Analyzer (MLTA) that graphically models social media text using multi-layered networks (MLNs) in order to better encode relationships across independent sets of tweets	
VTJNS10	An Efficient Key Management and Multi-Layered Security Framework for SCADA Systems	This makes the deployment of sophisticated security features challenging. As a result, effective lightweight cryptography solutions are needed to strengthen the security of industrial plants against cyber threats	
VTJBC01	Enabling Trust and Privacy Preserving eKYC System Using Blockchain	Essentially, the security and privacy of e-KYC related documents stored in the cloud becomes the crucial issue. Existing e-KYC platforms generally rely on strong authentication and apply traditional encryption to support their security and privacy requirement	

CODE	TITLE	DESCRIPTION
VTJBC02	Blockchain Technology for Secure Supply Chain Management	Blockchain (BC) emerges as a technology that can manage the data and build trust efficiently and transparently. It can also aid in transaction authorization and verification in the supply chain or payments without a third party
VTJBC03	Identity-Based Privacy Preserving Remote Data Integrity Checking with a Designated Verifier	To overcome these shortcomings, we propose an identity-based remote data possession checking scheme that satisfies the data owner's requirement to specify a unique verifier. Moreover, in this scheme, we use a random integer to blind data integrity proof to protect data privacy and use Merkle hash tree structure to achieve dynamic update of data
VTJBC04	Systematic Review of Security Vulnerabilities in Ethereum Blockchain Smart Contract	It is a distributed ledger technology based on a decentralized peer-to-peer (P2P) network. It enables users to store data globally on thousands of computers in an immutable format and empowers users to deploy small pieces of programs known as smart contracts
VTJBC05	Electronic Health Records Sharing Model Based on Blockchain With Checkable State PBFT Consensus Algorithm	The medical abstract and the access strategy are stored in the block chain to avoid being tampered with. To achieve the fine-grained access control, we propose the attribute-based encryption scheme and multi-keyword encryption scheme to encrypt EHRs
VTJBC06	Data Integrity Audit Scheme Based on Blockchain Expansion Technology	Users and cloud service providers (CSP) deploy smart contracts on the main chain and sub-chains. Intensive and frequent computing work is transferred to the sub-chain for completion, and the computation results of the sub-chain are submitted to the main chain periodically or when needed to ensure its finality

IEEE 2022 - BLOCK CHAIN