Inspiring the
Leading
Teachnologies

ELYSIUMPRO
INSPIRING THE LEADING EDGE TECHNOLOGIES

ElysiumPRO

Final Year Projects

Cloud Computing

Titles & Abstract

2023-2024

elysiumpro.in

CLOUD COMPUTING

ELYSIUMPRO
INSPIRING THE LEADING EDGE TECHNOLOGIES

EPRO_CLD_001

Enabling Balanced Data Deduplication in Mobile Edge Computing

In the mobile edge computing (MEC) environment, edge servers with storage and computing resources are deployed at base stations within users' geographic proximity to extend the capabilities of cloud computing to the network edge. 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. It also offers a promising solution to reducing data redundancy in ESSs. However, the unique characteristics of MEC, such as edge servers' geographic distribution and coverage, render cloud data deduplication mechanisms obsolete.

EPRO_CLD_002

Key Reduction in Multi-Key and Threshold Multi-Key Homomorphic Encryptions by Reusing Error

As cloud computing and AI as a Service are provided, it is increasingly necessary to deal with privacy sensitive data. To deal with the sensitive data, there are two cases of outsourcing process: i) many clients participate dynamically ii) many clients are pre-determined. The solutions for protecting sensitive data in both cases are the multi-key homomorphic encryption (MKHE) scheme and the threshold multi-key homomorphic encryption (TMKHE) scheme. However, these schemes may be difficult for clients with limited resources to perform MKHE and TMKHE. In addition, due to the large size of the evaluation keys, in particular multiplication and rotation keys, the communication between the clients and server that provide outsourcing service increases. Also, the size of the evaluation keys that the server must hold is tremendous, in particular, for the multiplication and rotation keys, which are essential for bootstrapping operation.

CLOUD COMPUTING

ELYSIUMPRO
INSPIRING THE LEADING EDGE TECHNOLOGIES

EPRO_CLD_003

Data Lake Architecture for Storing and Transforming Web Server Access Log Files

Web server access log files are text files containing important data about server activities, client requests addressed to a server, server responses, etc. Large-scale analysis of these data can contribute to various improvements in different areas of interest. The main problem lies in storing these files in their raw form, over long time, to allow analysis processes to be run at any time enabling information to be extracted as foundation for high quality decisions. Our research focuses on offering an economical, secure, and high-performance solution for the storage of large amount of raw log files. Proposed system implements a Data Lake (DL) architecture in cloud using Azure Data Lake Storage Gen2 (ADLS Gen2) for extract–load–transform (ELT) pipelines. This architecture allows large volumes of data to be stored in their raw form. Afterwards they can be subjected to transformation and advanced analysis processes without the need of a structured writing scheme. The main contribution of this paper is to provide a solution that is affordable and more accessible to perform web server access log data ingestion, storage and transformation over the newest technology, Data Lake.

EPRO_CLD_004

A Robust Selective Encryption Scheme for H.265/HEVC Video

To protect the information of video stream, many selective video encryption schemes have been proposed based on the H.265/HEVC video. However, most of the existing algorithms are not robust, thus failing to decrypt under packet loss. To further improve the robustness capability of video protection, a robust selective encryption scheme is proposed in this paper. In H.265/HEVC standard, video is encoded into multiple slices, and the slices are decoded independently. Inspired by the feature, each slice is individually encrypted using RC4 stream cipher. The pseudorandom binary sequence (PRBS) for one slice is related to encoding parameters and the SHA-256 hash value of the corresponding slice header, thus ensuring the real-time update of the PRBS and increasing the resistance to chosen-plaintext attack. Two-rounds shifting algorithm is designed to scramble non□zero coefficients of the transform units (TUs) and then motion vector difference (MVD) parameters, quantized transform coefficients (QTCs) and intra prediction modes (IPMs) are selected for encryption

CLOUD COMPUTING

ELYSIUMPRO
INSPIRING THE LEADING EDGE TECHNOLOGIES

EPRO_CLD_005

VeriDedup: A Verifiable Cloud Data Deduplication Scheme With Integrity and Duplication Proof

Data deduplication is a technique to eliminate duplicate data in order to save storage space and enlarge upload bandwidth, which has been applied by cloud storage systems. However, a cloud storage provider (CSP) may tamper user data or cheat users to pay unused storage for duplicate data that are only stored once. 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. In this paper, we propose a verifiable deduplication scheme called VeriDedup to address the above problems. It can guarantee the correctness of duplication check and support flexible tag generation for integrity check over encrypted data deduplication in an integrative way.

EPRO_CLD_006

Task Scheduling Mechanisms for Fog Computing: A Systematic Survey

In the Internet of Things (IoT) ecosystem, some processing is done near data production sites at higher speeds without the need for high bandwidth by combining Fog Computing (FC) and cloud computing. Fog computing offers advantages for real-time systems that require high speed internet connectivity. Due to the limited resources of fog nodes, one of the most important challenges of FC is to meet dynamic needs in real-time. Therefore, one of the issues in the fog environment is the optimal assignment of tasks to fog nodes. An efficient scheduling algorithm should reduce various qualitative parameters such as cost and energy consumption, taking into account the heterogeneity of fog nodes and the commitment to perform tasks within their deadlines. This study provides a detailed taxonomy to gain a better understanding of the research issues and distinguishes important challenges in existing work.

CLOUD COMPUTING

ELYSIUMPRO
INSPIRING THE LEADING EDGE TECHNOLOGIES

EPRO_CLD_007

Data Secure De-Duplication and Recovery Based on Public Key Encryption With Keyword Search

In the current era of information explosion, users' demand for data storage is increasing, and data on the cloud has become the first choice of users and enterprises. Cloud storage facilitates users to backup and share data, effectively reducing users' storage expenses. As the duplicate data of different users are stored multiple times, leading to a sudden decrease in storage utilization of cloud servers. Data stored in plaintext form can directly remove duplicate data, while cloud servers are semi-trusted and usually need to store data after encryption to protect user privacy. 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. For the duplicate file, the data user's re- encryption key about the file is appended to the ciphertext chain table of the stored copy.

EPRO_CLD_008

Enhancing Security and Privacy Preservation of Sensitive Information in e-Health Datasets Using FCA Approach

Advances in data collection, storage, and processing in e-Health systems have recently increased the importance and popularity of data mining in the health care field. However, the high sensitivity of the handled and shared data, brings a high risk of information disclosure and exposure. It is therefore important to hide sensitive relationships by modifying the shared data. This major information security threat has, therefore, mandated the requirement of hiding/securing sensitive relationships of shared data. As a large number of data mining activities that attempt to identify interesting patterns from databases depend on locating frequent item sets, further investigation of frequent item sets requires privacy-preserving techniques. To solve many difficult combinatorial problems, such as data distribution problem, exact and heuristic algorithms have been used. Exact algorithms are studied and considered optimal for such problems, however they suffer scalability bottleneck, as they are limited to medium-sized instances only. Heuristic algorithms, on the other hand, are scalable, however, they perform poor on security and privacy preservation

CLOUD COMPUTING

ELYSIUMPRO
INSPIRING THE LEADING EDGE TECHNOLOGIES

EPRO_CLD_009

Real-Time Detection Schemes for Memory DoS (M-DoS) Attacks on Cloud Computing Applications

Memory Denial of Service (M-DoS) attacks refer to a class of cyber-attacks that aim to exhaust the memory resources of a system, rendering it unavailable to legitimate users. This type of attack is particularly dangerous in cloud computing environments, where multiple users share the same resources. Detection and mitigation of M-DoS attacks in real-time is a challenging task, as they often involve a large number of low-rate requests, making it difficult to distinguish them from legitimate traffic. Several real-time detection schemes have been proposed to identify and mitigate M-DoS attacks in cloud computing environments. These schemes can be broadly classified into two categories: signature-based and anomaly-based detection. Signature-based detection methods rely on the identification of specific patterns or characteristics of known M-DoS attack techniques, while anomaly-based detection methods identify abnormal behaviour that deviates from the normal pattern of usage

EPRO_CLD_010

A Review on Protection and Cancelable Techniques in Biometric Systems

An essential part of cloud computing, IoT, and in general the broad field of digital systems, is constituted by the mechanisms which provide access to a number of services or applications. Biometric techniques aim to manage the access to such systems based on personal data; however, some biometric traits are openly exposed in the daily life, and in consequence, they are not secret, e.g., voice or face in social networks. In many cases, biometric data are non-cancelable and non-renewable when compromised. This document examines the vulnerabilities and proposes hardware and software countermeasures for the protection and confidentiality of biometric information using randomly created supplementary information. Consequently, a taxonomy is proposed according to the operating principle and the type of supplementary information supported by protection techniques, analyzing the security, privacy, revocability, renewability, computational complexity, and distribution of biometric information.

CLOUD COMPUTING

ELYSIUMPRO
INSPIRING THE LEADING EDGE TECHNOLOGIES

EPRO_CLD_011

A Novel Hybrid Multikey Cryptography Technique for Video Communication

Online video streaming is becoming more widespread in people's everyday entertainment routines. Protecting copyright and piracy has become a key concern in real-time video streaming systems. This research provides a revolutionary multi-key and hybrid cryptography approach to offer security. This work describes the software implementation of video encryption and decryption employing continuous systems based on the Elliptic Curve Cryptography approach as pseudorandom encryption key generators. This approach creates several keys to encrypt and decode small chunks of video files that are produced dynamically based on the video data. The suggested approach was implemented on the Android platform, where applications for sender and recipients had been created to enable streaming. The security and performance of the proposed system have been examined by implementing it on devices and streaming videos. The outcomes demonstrate superiority in terms of performance and security

EPRO_CLD_012

CloudpredNet: An Ultra-Short-Term Movement Prediction Model for Ground- Based Cloud Image

Ground-based cloud images can provide information on weather and cloud conditions, which are important for cloud monitoring and PV power generation forecasting. Prediction of short-time cloud movement from images is a major means of intra-hourly irradiation forecasting for solar power generation and is also important for precipitation forecasting. However, there is a lack of advanced and complete methods for cloud movement prediction from ground-based cloud images, and traditional techniques based on image processing and motion vector calculations have difficulty in predicting cloud morphological changes, which makes accurate prediction of cloud motion (especially nonlinear motion) very challenging. Therefore, this paper proposes CloudpredNet, a ground-based cloud ultra-short-term movement prediction model based on an "encoder-generator" architecture.

CLOUD COMPUTING

ELYSIUMPRO
INSPIRING THE LEADING EDGE TECHNOLOGIES

EPRO_CLD_013

A Rankable Boolean Searchable Encryption Scheme Supporting Dynamic Updates in a Cloud Environment

At present, three problems exist in searchable encryption in cloud storage services: firstly, most traditional searchable encryption schemes only support single-keyword search while fail to perform Boolean searches; even if a few schemes support Boolean searching, the storage efficiency is also unsatisfactory. Secondly, most existing schemes do not support dynamic keyword updates, so the update efficiency is low. Thirdly, most existing schemes cannot meet all demands of users, to perform rankable searching over search files according to the importance of keywords. To solve these problems, a rankable Boolean searchable encryption scheme supporting dynamic updates in a cloud environment (RBDC) is proposed. By using Paillier and GM encryption algorithms, secure indices supporting dynamic updating are established. Based on applicable knowledge gleaned from cryptography and set theory, the indices of keyword intersections and the intersection search trapdoors are constructed to achieve multi-keyword Boolean search

EPRO_CLD_014

Efficacy of Bluetooth-Based Data Collection for Road Traffic Analysis and Visualization Using Big Data Analytics

Ground-based cloud images can provide information on weather and cloud conditions, which play an important role in cloud cover monitoring and photovoltaic power generation forecasting. However, the cloud motion prediction of ground-based cloud images still lacks advanced and complete methods, and traditional technologies based on image processing and motion vector calculation are difficult to predict cloud morphological changes. In this paper, we propose a cloud motion prediction method based on Cascade Causal Long Short-Term Memory (CCLSTM) and SuperResolution Network (SR-Net). Firstly, CCLSTM is used to estimate the shape and speed of cloud motion. Secondly, the Super-Resolution Network is built based on perceptual losses to reconstruct the result of CCLSTM and, finally, make it clearer. We tested our method on Atmospheric Radiation Measurement (ARM) Climate Research Facility TSI (total sky imager) images. The experiments showed that the method is able to predict the sky cloud changes in the next few steps.

CLOUD COMPUTING

ELYSIUMPRO
INSPIRING THE LEADING EDGE TECHNOLOGIES

EPRO_CLD_015

RFSE-GRU: Data Balanced Classification Model for Mobile Encrypted Traffic in Big Data Environment

With the widespread use of mobile technologies and the Internet, traffic in mobile networks is increasing. This situation has made the classification of traffic an important element for data security and network management. However, encryption of traffic in modern networks makes it difficult to classify traffic with traditional methods. In this study, a unique deep learning-based classification model is proposed for the classification of encrypted mobile traffic data. The proposed model is a classification model called RFSE-GRU, which combines the Gated Recurrent Units (GRU) algorithm, feature selection and data balancing. The features that are more meaningful in the classification process are determined by selecting the features with the Random Forest algorithm. In addition, Synthetic Minority Oversampling Technique (SMOTE) oversampling algorithm and Edited Nearest Neighbor (ENN) undersampling algorithm were used together to reduce the negative impact of data imbalance on classification performance

EPRO_CLD_016

Secure Scheme for Locating Disease-Causing Genes Based on Multi-Key Homomorphic Encryption

Genes have great significance for the prevention and treatment of some diseases. A vital consideration is the need to find a way to locate pathogenic genes by analyzing the genetic data obtained from different medical institutions while protecting the privacy of patients' genetic data. In this paper, we present a secure scheme for locating disease-causing genes based on Multi-Key Homomorphic Encryption (MKHE), which reduces the risk of leaking genetic data. First, we combine MKHE with a frequency-based pathogenic gene location function. The medical institutions use MKHE to encrypt their genetic data. The cloud then homomorphically evaluates specific gene-locating circuits on the encrypted genetic data. Second, whereas most location circuits are designed only for locating monogenic diseases, we propose two location circuits (TH-intersection and Top-q) that can locate the disease-causing genes of polygenic diseases. Third, we construct a directed decryption protocol in which the users involved in the homomorphic evaluation can appoint a target user who can obtain the final decryption result.

CLOUD COMPUTING

ELYSIUMPRO
INSPIRING THE LEADING EDGE TECHNOLOGIES

EPRO_CLD_017

A MapReduce Based Approach for Secure Batch Satellite Image Encryption

The overarching goal of this research was to examine the state of satellite imagery security in relation to its deteriorating form due to rising demand. The most common approaches to safeguarding satellite images during transmission across transmission networks, which are not protected by standard encryption, are the focus of this investigation. Since satellite imagery can be encrypted both in transit and while stored on a computer's hard drive, we put the suggested Image Encryption System to the test by applying it to a collection of satellite photos. Concurrently encrypting data and running MapReduce jobs is key to the study methodology employed. This will be carried out in the Hadoop ecosystem, where an innovative method of analysing random numbers for use in Image encryption will be put to the test. The encryption was processed using MapReduce in the Hadoop ecosystem. Images were saved as BMP files with added security metadata. The evaluation of experiments was based on four (4) indicators. It was found that the processing time for batch encryption calculations grew in proportion to the amount of computations. All cluster, map, and reduction processes were put to the test using encrypted images, exposing load balancing difficulties and inefficiencies.

EPRO_CLD_018

Multimedia Security Using Encryption: A Survey

Considering the current dependency on digital technology in modern society, the protection of multimedia is highly important. Encryption is vital in modern digital communication, ensuring data confidentiality, authentication, integrity, and non-repudiation. Multimedia encryption-based security techniques are becoming increasingly important as they allow for the secure sharing of multimedia content on digital platforms. This survey aims to review the state of secure and privacy-preserving encryption schemes applicable to digital multimedia, such as digital images, digital video, and digital audio. An extensive analysis of the existing cryptography schemes and multimedia encryption algorithms will be conducted to give an extensive overview of the current state of security encryption schemes specifically designed for digital multimedia technology. The survey results will be used to understand better the effectiveness and reliability of secure multimedia encryption schemes and contribute to developing efficient and secure encryption schemes in the future.

CLOUD COMPUTING

ELYSIUMPRO
INSPIRING THE LEADING EDGE TECHNOLOGIES

EPRO_CLD_019

SDTP: Accelerating Wide-Area Data Analytics With Simultaneous Data Transfer and Processing

For the efficient analysis of geo-distributed datasets, cloud providers implement data-parallel jobs across geo-distributed sites (e.g., datacenters and edge clusters), which are generally interconnected by wide-area network links. However, current state-of-the-art geo-distributed data analytic methods fail to make full use of the available network and computing resources. The main reason is that such geo-distributed methods must wait for bottleneck sites to complete the corresponding transmission and computation in each phase. Furthermore, such geo-distributed methods may be impractical to the network bandwidth dynamicity and diverse job parallelism. To this end, we propose a Simultaneous Data Transfer and Processing (SDTP) mechanism to accelerate wide-area data analytics, with the joint consideration of network bandwidth dynamics and job parallelism. In the SDTP, a site can execute the computation, provided that it obtains the required input data.

EPRO_CLD_020

Deadline-Constrained Cost Minimisation for Cloud Computing Environments

The interest in performing scientific computations using commercially available cloud computing resources has grown rapidly in the last decade. However, scheduling multiple workflows in cloud computing is challenging due to its non-functional constraints and multi-dimensional resource requirements. Scheduling algorithms proposed in literature use search-based approaches which often result in very high computational overhead and long execution time. In this paper, a Deadline-Constrained Cost Minimisation (DCCM) algorithm is proposed for resource scheduling in cloud computing. In the proposed scheme, tasks were grouped based on their scheduling deadline constraints and data dependencies. Compared to other approaches, DCCM focuses on meeting the user-defined deadline by sub-dividing tasks into different levels based on their priorities. Simulation results showed that DCCM achieved higher success rates when compared to the state-of-the-art approaches.

ELYSIUMPRO
INSPIRING THE LEADING EDGE TECHNOLOGIES

50K+
Projects Reached

25+
Years of Experience

24/7
Desk Support

25+ Years of Experience | Automated Services | 24/7 Desk Support
Advanced Technologies and Tools | Legitimate Members of all Journals
Quality Product Training | Industry Exposure

(+91) 99447 93398

#229, First Floor, A Block, Elysium Campus,
Church Rd, Anna Nagar, Madurai,
Tamil Nadu 625020

elysiumpro.in