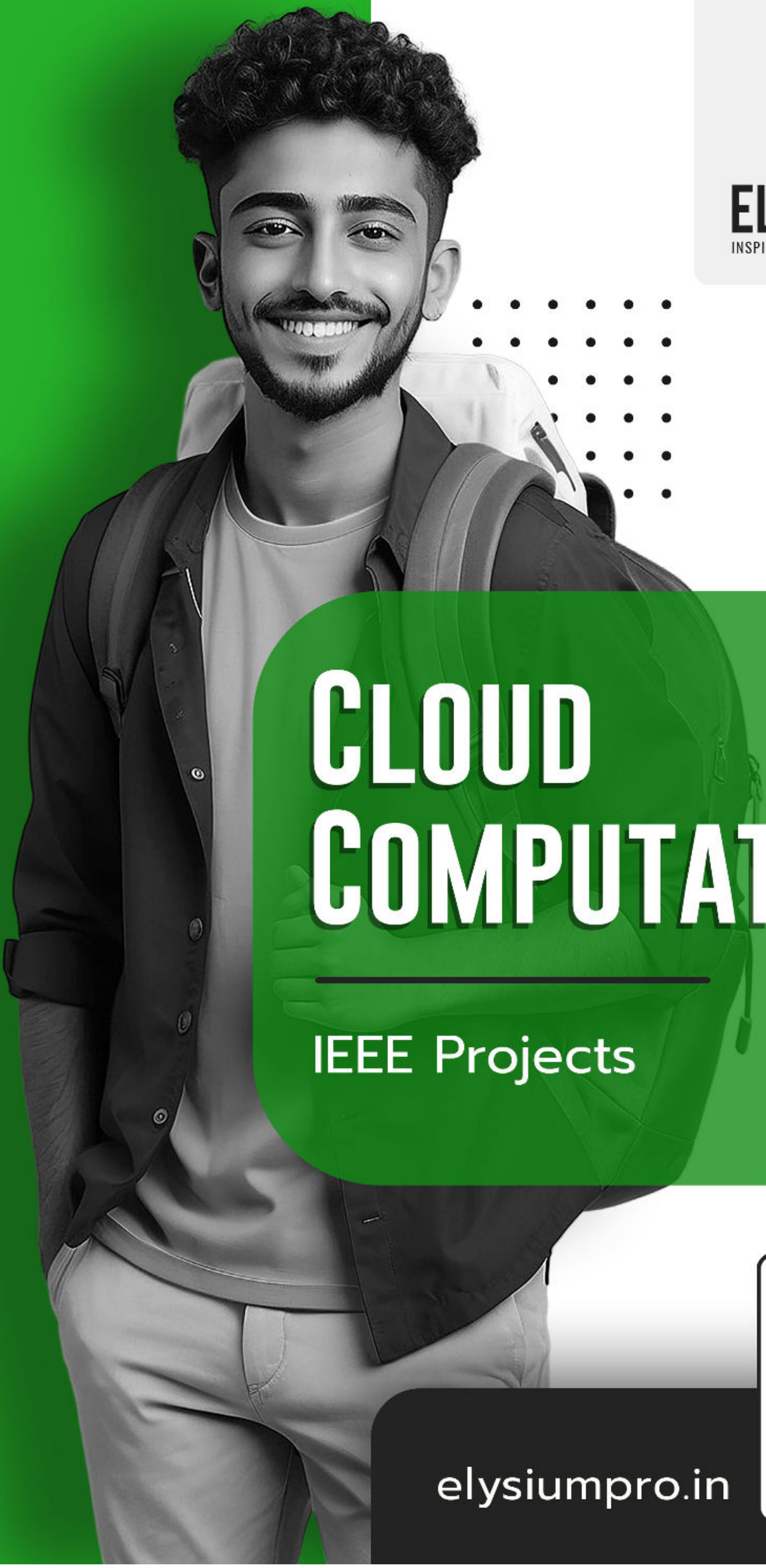
Titles & Abstract 2024- 2025

ELYSIUMPRO

INSPIRING THE LEADING EDGE TECHNOLOGIES



Advanced Academic Final Year Projects

CLOUD COMPUTATING

IEEE Projects

elysiumpro.in

EPRO-CLD-001

Multi-Dimensional Flat Indexing for Encrypted Data

We address the problem of indexing encrypted data outsourced to an external cloud server to support server-side execution of multi-attribute queries. Our approach partitions the dataset in groups with the same number of tuples, and associates all tuples in a group with the same combination of index values, so to guarantee protection against static inferences. Our indexing approach does not require any modifications to the server-side software stack, and requires limited storage at the client for query support. The experimental evaluation considers, for the storage of the encrypted and indexed dataset, both a relational database (PostgreSQL) and a key-value database (Redis). We carried out extensive experiments evaluating client-storage requirements and query performance. The experimental results confirm the efficiency of our solution. The proposal is supported by an open source implementation.

EPRO-CLD-002

Automating VPN Configuration in Computer Networks

The configuration of security systems for communication protection, such as VPNs, is traditionally performed manually by human beings. However, because the complexity of this task becomes soon difficult to manage when its size increases, critical errors that may open the door to cyberattacks may be introduced. Moreover, even when a solution is computed correctly, sub-optimizations that may afflict the performance of the configured VPNs may be introduced. Unfortunately, the possible solution that consists in automating the definition of VPN configurations has been scarcely studied in literature so far. Therefore, this paper proposes an automatic approach to compute the configuration of VPN systems. Both the allocation scheme of VPN systems in the network and their protection rules are computed automatically. This result is achieved through the formulation of a Maximum Satisfiability Modulo Theories problem, which provides both formal correctness-by-construction and optimization of the result. A framework implementing this approach has been developed, and its experimental validation showed that it is a valid alternative for replacing time-consuming and error-prone human operations for significant problem sizes.

EPRO-CLD-003

Quantized Distributed Economic Dispatch for Microgrids: Paillier Encryption-Decryption Scheme

designed to optimally coordinate the power outputs of a collection of distributed generators (DGs) in order to meet the total load demand at the lowest generation cost under the DG capacity limits while ensuring communication efficiency and security. First, to facilitate data encryption and reduce data release, a novel dynamic quantization scheme is integrated into the DED algorithm, through which the effects of quantization errors can be eliminated. Next, utilizing matrix norm analysis and mathematical induction, a sufficient condition is provided to demonstrate that the developed DED algorithm converges precisely to the optimal solution under finite quantization levels (and even the three-level quantization using sign transmissions). Moreover, an encryption–decryption scheme is developed based on quantized outputs, which ensures confidential communication by leveraging the homomorphic property of the Paillier cryptosystem. Finally, the effectiveness and superiority of the implemented secure distributed algorithm are confirmed through a simulated example.

EPRO-CLD-004

Joint Task Offloading, Resource Allocation, and Trajectory Design for Multi-UAV

Mobile edge computing (MEC) has emerged as a solution to address the demands of computation-intensive network services by providing computational capabilities at the network edge, thus reducing service delays. Due to the flexible deployment, wide coverage and reliable wireless communication, unmanned aerial vehicles (UAVs) have been employed to assist MEC. This paper investigates the task offloading problem in a UAV-assisted MEC system with collaboration of multiple UAVs, highlighting task priorities and binary offloading mode. We defined the system gain based on energy consumption and task delay. The joint optimization of UAVs' trajectory design, binary offloading decision, computation resources allocation, and communication resources management is formulated as a mixed integer programming problem with the goal of maximizing the long-term average system gain. Considering the discrete-continuous hybrid action space of this problem, we propose a novel deep reinforcement learning (DRL) algorithm based on the latent space to solve it. The evaluation results demonstrate that our proposed algorithm outperforms three state-of-the-art alternative solutions in terms of task delay and system gain.

EPRO-CLD-005

Hybrid Optimization Algorithm for Detection ofSecurity Attacks in IoT-Enabled CyberPhysical Systems

The Internet of Things (IoT) is being prominently used in smart cities and a wide range of applications in society. The benefits of IoT are evident, but cyber terrorism and security concerns inhibit many organizations and users from deploying it. Cyber-physical systems that are IoT-enabled might be difficult to secure since security solutions designed for general information/operational technology systems may not work as well in an environment. Thus, deep learning (DL) can assist as a powerful tool for building IoT-enabled cyber-physical systems with automatic anomaly detection. In this paper, two distinct DL models have been employed i.e., Deep Belief Network (DBN) and Convolutional Neural Network (CNN), considered hybrid classifiers, to create a framework for detecting attacks in IoT-enabled cyber-physical systems. However, DL models need to be trained in such a way that will increase their classification accuracy. Therefore, this paper also aims to present a new hybrid optimization algorithm called "Seagull Adapted Elephant Herding Optimization" (SAEHO) to tune the weights of the hybrid classifier. The "Hybrid Classifier + SAEHO" framework takes the feature extracted

EPRO-CLD-006

Towards Safe Load Balancing based on Control Barrier Functions and Deep Reinforcement Learning

In the context of commercial solutions, reliable and safe-to-operate systems are of paramount importance. Taking this problem into account, we propose a safe learning-based load balancing algorithm for Software Defined-Wide Area Network (SD-WAN), which is empowered by Deep Reinforcement Learning (DRL) combined with a Control Barrier Function (CBF). It safely projects unsafe actions into feasible ones during both training and testing, and it guides learning towards safe policies. We successfully implemented the solution on GPU to accelerate training by approximately 110x times and achieve model updates for on-policy methods within a few seconds, making the solution practical. We show that our approach delivers near-optimal Quality-of-Service (QoS performance in terms of end-to-end delay while respecting safety requirements related to link capacity constraints. We also demonstrated that on-policy learning based on Proximal Policy Optimization (PPO) performs better than off-policy learning with Deep Deterministic Policy Gradient (DDPG) when both are combined with a CBF for safe load balancing.

EPRO-CLD-007

HashVFL: Defending Against Data Reconstruction Attacks in Vertical Federated Learning

Vertical Federated Learning (VFL) is a trending collaborative machine learning model training solution. Existing industrial frameworks employ secure multi-party computation techniques such as homomorphic encryption to ensure data security and privacy. Despite these efforts, studies have revealed that data leakage remains a risk in VFL due to the correlations between intermediate representations and raw data. Neural networks can accurately capture these correlations, allowing an adversary to reconstruct the data. This emphasizes the need for continued research into securing VFL systems.

Our work shows that hashing is a promising solution to counter data reconstruction attacks. The one-way nature of hashing makes it difficult for an adversary to recover data from hash codes. However, implementing hashing in VFL presents new challenges, including vanishing gradients and information loss. To address these issues, we propose HashVFL, which integrates hashing and simultaneously achieves learnability, bit balance, and consistency.

Experimental results indicate that HashVFL effectively maintains task performance while defending against data reconstruction attacks. It also brings additional benefits in reducing the degree of label leakage, mitigating adversarial attacks, and detecting abnormal inputs. We hope our work will inspire further research into the potential applications of HashVFL

EPRO-CLD-008

DiffMDD: A Diffusion-Based Deep LearningFramework for MDD Diagnosis Using EEG

Major Depression Disorder (MDD) is a common yet destructive mental disorder that affects millions of people worldwide. Making early and accurate diagnosis of it is very meaningful. Recently, EEG, a non-invasive technique of recording spontaneous electrical activity of brains, has been widely used for MDD diagnosis. However, there are still some challenges in data quality and data size of EEG: (1) A large amount of noise is inevitable during EEG collection, making it difficult to extract discriminative features from raw EEG; (2) It is difficult to recruit a large number of subjects to collect sufficient and diverse data for model training. Both of the challenges cause the overfitting problem, especially for deep learning methods. In this paper, we propose DiffMDD, a diffusion-based deep learning framework for MDD diagnosis using EEG. Specifically, we extract more noise-irrelevant features to improve the model's robustness by designing the Forward Diffusion Noisy Training Module. Then we increase the size and diversity of data to help the model learn more generalized features by designing the Reverse Diffusion Data Augmentation Module.

EPRO-CLD-009

On the Privacy Effect of Data Enhancement via the Lens of Memorization

Machine learning poses severe privacy concerns as it has been shown that the learned models can reveal sensitive information about their training data. Many works have investigated the effect of widely adopted data augmentation and adversarial training techniques, termed data enhancement in the paper, on the privacy leakage of machine learning models. Such privacy effects are often measured by membership inference attacks (MIAs), which aim to identify whether a particular example belongs to the training set or not. We propose to investigate privacy from a new perspective called memorization. Through the lens of memorization, we find that previously deployed MIAs produce misleading results as they are less likely to identify samples with higher privacy risks as members compared to samples with low privacy risks. To solve this problem, we deploy a recent attack that can capture individual samples' memorization degrees for evaluation. Through extensive experiments, we unveil several findings about the connections between three essential properties of machine learning models, including privacy, generalization gap, and adversarial robustness. We demonstrate that the generalization gap and privacy leakage are less correlated than those of the previous results. Moreover, there is not necessarily a trade-off between adversarial robustness and privacy as stronger adversarial robustness does not make the model more susceptible to privacy attacks.

EPRO-CLD-010

Towards Automated Attack Discovery in SDN Controllers Through Formal Verification

Software-defined Network (SDN), presented to be a novel architecture of network because of its separation of data plane and control plane, brings centralization and extensibility to network management as well as new attacks that exploit the flexibility of SDN. OpenFlow, which is the protocol that is applied by the majority of SDN, leads to the widely used definition of the communication between the controller and the switch resulting in similar implementations regardless of different vendors. In this paper, we focus on the mechanisms of packet processing and topology discovery and their fundamental weaknesses caused by general implementations or device limitations. Despite the common vulnerabilities, the universal standard mechanisms of basic function in SDN also enlighten us to present an automated attack discovery method based on the formal verification with a generic model of SDN system. We describe the abstraction of the SDN components, their key functions, and communications along with the malicious operations that could be executed by malicious hosts and malicious switches and translate them into a formal model of the SDN system.

EPRO-CLD-011

Federated-Reinforcement Learning-Assisted IoT Consumers System for Kidney Disease Images

The number of people with kidney disease rises every day for many reasons. Many existing machine-learning-enabled mechanisms for processing kidney disease suffer from long delays and consume much more resources during processing. In this paper, the study shows how federated and reinforcement learning schemes can be used to develop the best delay scheme. The scheme must optimize both the internal and external states of reinforcement learning and the federated learning fog cloud network. This work presents the Adaptive Federated Reinforcement Learning-Enabled System (AFRLS) for Internet of Things (IoT) consumers' kidney disease image processing. The main relationship between IoT consumers and kidney image is that the data is collected from different IoT consumer sources, such as ultrasound and X-rays in healthcare clinics. In healthcare applications, kidney urinary tasks reduce the time it takes to preprocess federated learning datasets for training and testing and run them on different fog and cloud nodes. AFRLS decides the scheduling on other nodes and improves constraints based on the decision tree. Based on the simulation results, AFRLS is a new strategy that reduces the time tasks need to be delayed compared to other machine learning methods used in fog cloud networks. The AFRLS improved the delay among nodes by 55%, the delay among internal states by 40%, and the training and testing delay by 51%

EPRO-CLD-012

Multi-agent Reinforcement Learning based Distributed Channel Access for Industrial

resources to meet the high requirements for communication rate and reliability in high-performance manufacturing processes. Therefore, this paper proposes a task-aware distributed channel access scheme for multiantenna smart mobile resources in a factory. First, this paper introduces an edge-cloud collaboration framework for smart factories to support autonomous wireless access point selection for mobile resources. Second, a user-centric active wireless channel access scheme is proposed and a channel resource allocation optimization problem is formulated for mobile resources to leverage multiple antennas and movement direction to address the unstable connection problem. Third, a centralized-training-and-distributed-execution multiagent reinforcement learning (MARL) model with a specially designed neural network architecture is built for smart mobile resources, effectively using important input information of the next interaction objects for mobile resources. Simulation results show that the proposed MARL scheme outperforms common schemes of 3GPP LTE, traditional reinforcement learning schemes, and random selection schemes in improving communication rate and stability.

EPRO-CLD-013

Application of Machine LearningOptimizationinCloud Computing Resource SchedulingandManagement

users through the access to the centralized resources to complete the calculation, the cloud computing center will return the results of the program processing to the user. Cloud computing is not only for individual users, but also for enterprise users. By purchasing a cloud server, users do not have to buy a large number of computers, saving computing costs. According to a report by China Economic News Network, the scale of cloud computing in China has reached 209.1 billion yuan. At present, the more mature cloud service providers in China are Ali Cloud, Baidu Cloud, Huawei Cloud and so on. Therefore, this paper proposes an innovative approach to solve complex problems in cloud computing resource scheduling and management using machine learning optimization techniques. Through in-depth study of challenges such as low resource utilization and unbalanced load in the cloud environment, this study proposes a comprehensive solution, including optimization methods such as deep learning and genetic algorithm, to improve system performance and efficiency, and thus bring new breakthroughs and progress in the field of cloud computing resource management.Rational allocation of resources plays a crucial role in cloud computing. In the resource allocation of cloud computing, the cloud computing center has limited cloud resources, and users arrive in sequence. Each user requests the cloud computing center to use a certain number of cloud resources at a specific time.

EPRO-CLD-014

Multi-agent Reinforcement Learning based Distributed Channel Access for Industrial

processing capacity which leads to delay in executing workflows and it results in increase of makespan, cost, energy consumption. In order to effectively schedule complex workflows i.e. with more task dependencies, we propose a novel multi objective workflow scheduling algorithm using Deep reinforcement Learning. Initially, priorities of all workflows calculated based on their dependencies and then calculated priorities of VMs based on electricity cost at datacenters to map workflows onto precise VMs. These priorities are fed to scheduler which uses Deep Q-Network model to dynamically schedule tasks by considering both priorities of tasks and VMs. Extensive simulations carried out on workflowsim by considering realtime scientific workflows (Montage, cybershake, Epigenomics, LIGO). Our proposed MOPWSDRL compared against existing state of art approaches i.e. Heterogeneous Earliest First Deadline, Cat Swarm Optimization, Ant Colony Optimization. Results revealed that our proposed MOPDSWRL outperforms existing state of art algorithms by minimizing makespan, energy consumption.

EPRO-CLD-015

Optimal Finite Horizon Scheduling of Wireless Networked Control Systems

We address the problem of indexing encrypted data outsourced to an external cloud server to support server-side execution of multi-attribute queries. Our approach partitions the dataset in groups with the same number of tuples, and associates all tuples in a group with the same combination of index values, so to guarantee protection against static inferences. Our indexing approach does not require any modifications to the server-side software stack, and requires limited storage at the client for query support. The experimental evaluation considers, for the storage of the encrypted and indexed dataset, both a relational database (PostgreSQL) and a key-value database (Redis). We carried out extensive experiments evaluating client-storage requirements and query performance. The experimental results confirm the efficiency of our solution. The proposal is supported by an open source implementation.

EPRO-CLD-016

The Least Increasing Aversion (LIA) Protocol: Illustration on Identifying Individual Susceptibility to

We address the problem of indexing encrypted data outsourced to an external cloud server to support server-side execution of multi-attribute queries. Our approach partitions the dataset in groups with the same number of tuples, and associates all tuples in a group with the same combination of index values, so to guarantee protection against static inferences. Our indexing approach does not require any modifications to the server-side software stack, and requires limited storage at the client for query support. The experimental evaluation considers, for the storage of the encrypted and indexed dataset, both a relational database (PostgreSQL) and a key-value database (Redis). We carried out extensive experiments evaluating client-storage requirements and query performance. The experimental results confirm the efficiency of our solution. The proposal is supported by an open source implementation.

EPRO-CLD-017

Temporal Characterization and Prediction of VR Traffic: A Network Slicing Use Case

We address the problem of indexing encrypted data outsourced to an external cloud server to support server-side execution of multi-attribute queries. Our approach partitions the dataset in groups with the same number of tuples, and associates all tuples in a group with the same combination of index values, so to guarantee protection against static inferences. Our indexing approach does not require any modifications to the server-side software stack, and requires limited storage at the client for query support. The experimental evaluation considers, for the storage of the encrypted and indexed dataset, both a relational database (PostgreSQL) and a key-value database (Redis). We carried out extensive experiments evaluating client-storage requirements and query performance. The experimental results confirm the efficiency of our solution. The proposal is supported by an open source implementation.

EPRO-CLD-018

Gotham Testbed: A Reproducible IoT Testbed for Security Experiments and Dataset Generation

We address the problem of indexing encrypted data outsourced to an external cloud server to support server-side execution of multi-attribute queries. Our approach partitions the dataset in groups with the same number of tuples, and associates all tuples in a group with the same combination of index values, so to guarantee protection against static inferences. Our indexing approach does not require any modifications to the server-side software stack, and requires limited storage at the client for query support. The experimental evaluation considers, for the storage of the encrypted and indexed dataset, both a relational database (PostgreSQL) and a key-value database (Redis). We carried out extensive experiments evaluating client-storage requirements and query performance. The experimental results confirm the efficiency of our solution. The proposal is supported by an open source implementation.

EPRO-CLD-019

A Situation Based Predictive Approach for Cybersecurity Intrusion Detection and Prevention Using Machine

We address the problem of indexing encrypted data outsourced to an external cloud server to support server-side execution of multi-attribute queries. Our approach partitions the dataset in groups with the same number of tuples, and associates all tuples in a group with the same combination of index values, so to guarantee protection against static inferences. Our indexing approach does not require any modifications to the server-side software stack, and requires limited storage at the client for query support. The experimental evaluation considers, for the storage of the encrypted and indexed dataset, both a relational database (PostgreSQL) and a key-value database (Redis). We carried out extensive experiments evaluating client-storage requirements and query performance. The experimental results confirm the efficiency of our solution. The proposal is supported by an open source implementation.

EPRO-CLD-020

Deep Learning in the Fast Lane: A Survey on Advanced Intrusion Detection Systems forIntelligent Vehicle Networks

We address the problem of indexing encrypted data outsourced to an external cloud server to support server-side execution of multi-attribute queries. Our approach partitions the dataset in groups with the same number of tuples, and associates all tuples in a group with the same combination of index values, so to guarantee protection against static inferences. Our indexing approach does not require any modifications to the server-side software stack, and requires limited storage at the client for query support. The experimental evaluation considers, for the storage of the encrypted and indexed dataset, both a relational database (PostgreSQL) and a key-value database (Redis). We carried out extensive experiments evaluating client-storage requirements and query performance. The experimental results confirm the efficiency of our solution. The proposal is supported by an open source implementation.

EPRO-CLD-021

Semantic Deep Hiding for Robust Unlearnable Examples

We address the problem of indexing encrypted data outsourced to an external cloud server to support server-side execution of multi-attribute queries. Our approach partitions the dataset in groups with the same number of tuples, and associates all tuples in a group with the same combination of index values, so to guarantee protection against static inferences. Our indexing approach does not require any modifications to the server-side software stack, and requires limited storage at the client for query support. The experimental evaluation considers, for the storage of the encrypted and indexed dataset, both a relational database (PostgreSQL) and a key-value database (Redis). We carried out extensive experiments evaluating client-storage requirements and query performance. The experimental results confirm the efficiency of our solution. The proposal is supported by an open source implementation.

EPRO-CLD-022

Secure Distributed Control for Demand Response in Power Systems AgainstDeception Cyber-Attacks With Arbitrary Patterns

We address the problem of indexing encrypted data outsourced to an external cloud server to support server-side execution of multi-attribute queries. Our approach partitions the dataset in groups with the same number of tuples, and associates all tuples in a group with the same combination of index values, so to guarantee protection against static inferences. Our indexing approach does not require any modifications to the server-side software stack, and requires limited storage at the client for query support. The experimental evaluation considers, for the storage of the encrypted and indexed dataset, both a relational database (PostgreSQL) and a key-value database (Redis). We carried out extensive experiments evaluating client-storage requirements and query performance. The experimental results confirm the efficiency of our solution. The proposal is supported by an open source implementation.

EPRO-CLD-023

Modeling Load Redistribution Attacks in Integrated Electricity-Gas Systems

We address the problem of indexing encrypted data outsourced to an external cloud server to support server-side execution of multi-attribute queries. Our approach partitions the dataset in groups with the same number of tuples, and associates all tuples in a group with the same combination of index values, so to guarantee protection against static inferences. Our indexing approach does not require any modifications to the server-side software stack, and requires limited storage at the client for query support. The experimental evaluation considers, for the storage of the encrypted and indexed dataset, both a relational database (PostgreSQL) and a key-value database (Redis). We carried out extensive experiments evaluating client-storage requirements and query performance. The experimental results confirm the efficiency of our solution. The proposal is supported by an open source implementation.

EPRO-CLD-024

An Unsupervised Adversarial Autoencoder forCyber Attack Detection in Power Distribution Grids

We address the problem of indexing encrypted data outsourced to an external cloud server to support server-side execution of multi-attribute queries. Our approach partitions the dataset in groups with the same number of tuples, and associates all tuples in a group with the same combination of index values, so to guarantee protection against static inferences. Our indexing approach does not require any modifications to the server-side software stack, and requires limited storage at the client for query support. The experimental evaluation considers, for the storage of the encrypted and indexed dataset, both a relational database (PostgreSQL) and a key-value database (Redis). We carried out extensive experiments evaluating client-storage requirements and query performance. The experimental results confirm the efficiency of our solution. The proposal is supported by an open source implementation.

EPRO-CLD-025

The Role of Deep Learning in Advancing Proactive Cybersecurity Measures for Smart Grid Networks

We address the problem of indexing encrypted data outsourced to an external cloud server to support server-side execution of multi-attribute queries. Our approach partitions the dataset in groups with the same number of tuples, and associates all tuples in a group with the same combination of index values, so to guarantee protection against static inferences. Our indexing approach does not require any modifications to the server-side software stack, and requires limited storage at the client for query support. The experimental evaluation considers, for the storage of the encrypted and indexed dataset, both a relational database (PostgreSQL) and a key-value database (Redis). We carried out extensive experiments evaluating client-storage requirements and query performance. The experimental results confirm the efficiency of our solution. The proposal is supported by an open source implementation.

EPRO-CLD-026

Quantized Distributed Economic Dispatch for Microgrids: Paillier Encryption-Decryption Scheme

We address the problem of indexing encrypted data outsourced to an external cloud server to support server-side execution of multi-attribute queries. Our approach partitions the dataset in groups with the same number of tuples, and associates all tuples in a group with the same combination of index values, so to guarantee protection against static inferences. Our indexing approach does not require any modifications to the server-side software stack, and requires limited storage at the client for query support. The experimental evaluation considers, for the storage of the encrypted and indexed dataset, both a relational database (PostgreSQL) and a key-value database (Redis). We carried out extensive experiments evaluating client-storage requirements and query performance. The experimental results confirm the efficiency of our solution. The proposal is supported by an open source implementation.

EPRO-CLD-027

Automated Knowledge-Based Cybersecurity Risk Assessment of Cyber-Physical Systems

We address the problem of indexing encrypted data outsourced to an external cloud server to support server-side execution of multi-attribute queries. Our approach partitions the dataset in groups with the same number of tuples, and associates all tuples in a group with the same combination of index values, so to guarantee protection against static inferences. Our indexing approach does not require any modifications to the server-side software stack, and requires limited storage at the client for query support. The experimental evaluation considers, for the storage of the encrypted and indexed dataset, both a relational database (PostgreSQL) and a key-value database (Redis). We carried out extensive experiments evaluating client-storage requirements and query performance. The experimental results confirm the efficiency of our solution. The proposal is supported by an open source implementation.

EPRO-CLD-028

Attribute-hiding fuzzy encryption for privacy-preserving data evaluation

We address the problem of indexing encrypted data outsourced to an external cloud server to support server-side execution of multi-attribute queries. Our approach partitions the dataset in groups with the same number of tuples, and associates all tuples in a group with the same combination of index values, so to guarantee protection against static inferences. Our indexing approach does not require any modifications to the server-side software stack, and requires limited storage at the client for query support. The experimental evaluation considers, for the storage of the encrypted and indexed dataset, both a relational database (PostgreSQL) and a key-value database (Redis). We carried out extensive experiments evaluating client-storage requirements and query performance. The experimental results confirm the efficiency of our solution. The proposal is supported by an open source implementation.

EPRO-CLD-029

Privacy-Preserving Naïve Bayesian Classification for Health Monitoring Systems

In recent years, issues of privacy preservation in data mining and machine learning have received more and more attention from the research community. Privacy-preserving data mining and machine learning solutions enable data holders to jointly discover knowledge and valuable information, as well as construct machine learning models without privacy concerns. In this paper, we address the distressing problem of privacy-preservation for a novel data model called the semi-fully distributed setting. Differently from the existing scenarios, each record of the dataset in this data model is composed of three parts, in which the first part is privately kept by a data user, the second one is securely stored by the miner, and the rest is publicly known by both the miner and the data user. For this new data model, we propose a privacy-preserving Naive Bayes classification solution based on secure multi-party computation.

EPRO-CLD-030

Dynamic User Clustering for Efficient and Privacy-Preserving Federated Learning

With the wider adoption of machine learning and increasing concern about data privacy, federated learning (FL) has received tremendous attention. FL schemes typically enable a set of participants, i.e., data owners, to individually train a machine learning model using their local data, which are then aggregated with the coordination of a central server to construct a global FL model. Improvements upon standard FL include (i) reducing the communication overheads of gradient transmission by utilizing gradient sparsification and (ii) enhancing the security of aggregation by adopting privacy-preserving aggregation (PPAgg) protocols. However, state-of-the-art PPAgg protocols do not interoperate easily with gradient sparsification due to the heterogeneity of users' sparsified gradient vectors. To resolve this issue, we propose a Dynamic User Clustering (DUC) approach with a set of supporting protocols to partition users into clusters based on the nature of the PPAgg protocol and gradient sparsification technique, providing both security guarantees and communication efficiency. Experimental results show that DUC-FL significantly reduces communication overheads and achieves similar model accuracy compared to the baselines. The simplicity of the proposed protocol makes it attractive for both implementation and further improvements

EPRO-CLD-031

The Role of Cyber-Physical-Social Systems in Smart Energy Future

Future energy systems (FESs) require greater interaction, integration, and cooperation between physical infrastructure, cyber technologies, and human participants from prosumers to communities and governments. Cyber-Physical-Social Systems (CPSSs) will be the enabling technology to ensure the efficiency, effectiveness, sustainability, security and safety of energy generation and use. In this paper, we will first present an overview of the challenges in CPSSs. We will then outline potential contributions that CPSSs can make to FESs, as well as the opportunities that FESs present to CPSSs.

EPRO-CLD-032

Systematically Assessing the Security Risks of AI/ML-enabled Connected Healthcare Systems

cyber-space. A smart city is defined as a connectable, sensible, accessible, ubiquitous, sharable, and visible closed-loop system that supports the technology-based infrastructure, usually consisting of sensors and actuators embedded throughout the urban topography. These networks interconnect with wireless mobile devices such as smart phones with an Internet-based backbone with cloud service. A smart city is a highly stochastic hybrid structure that solves issues successfully with the help of an interdisciplinary approach and captures the overall vision outline. The CPSS collects data and flows it from the human physical systems such as the condition of traffic, bridges, parking space, roads or buildings, quality of air or water information, and status of resources of cities. Enabling a smart city setting involves a cyber–physical infrastructure combined with a new platform of software and strict requirements for security, privacy, safety, mobility, and the processing of huge amounts of information called big data. In addition, endeavors to deploy smart city applications have provided invaluable feedback from the city officials responsible for adopting such deployments and the end operators themselves. Transportation and energy networks are important arteries for the urban environment, and citywide systems should be functioning efficiently, and user and environmentally friendly. To ensure the operation of systems, a real-time view of the operating system of

EPRO-CLD-033

Cyber-Physical Testbed Co-Simulation Real-Time:Normal and Abnormal System Frequency Response

throughout the urban topography. These networks interconnect with wireless mobile devices such as smart phones with an Internet-based backbone with cloud service. A smart city is a highly stochastic hybrid structure that solves issues successfully with the help of an interdisciplinary approach and captures the overall vision outline. The CPSS collects data and flows it from the human physical systems such as the condition of traffic, bridges, parking space, roads or buildings, quality of air or water information, and status of resources of cities. Enabling a smart city setting involves a cyber–physical infrastructure combined with a new platform of software and strict requirements for security, privacy, safety, mobility, and the processing of huge amounts of information called big data. In addition, endeavors to deploy smart city applications have provided invaluable feedback from the city officials responsible for adopting such deployments and the end operators themselves. Transportation and energy networks are important arteries for the urban environment, and citywide systems should be functioning efficiently, and user and environmentally friendly.

EPRO-CLD-034

A Game-Theoretical Scheme in the Smart Grid With Demand-Side Management:Towards a Smart Cyber-Physical Power Infrastructure

The smart grid is becoming one of the fundamental cyber-physical systems due to the employment of information and communication technology. In the smart grid, demand-side management (DSM) based on real-time pricing is an important mechanism for improving the reliability of the grid. Electricity retailers in the smart grid can procure electricity from various supply sources, and then sell it to the customers. Therefore, it is critical for retailers to make effective procurement and price decisions. In this paper, we propose a novel game-theoretical decision-making scheme for electricity retailers in the smart grid using real-time pricing DSM. We model and analyze the interactions between the retailer and electricity customers as a four-stage Stackelberg game. In the first three stages, the electricity retailer, as the Stackelberg leader, makes decisions on which electricity sources to procure electricity from, how much electricity to procure, and the optimal retail price to offer to the customers, to maximize its profit. In the fourth stage, the customers, who are the followers in the Stackelberg game, adjust their individual electricity demand to maximize their individual utility.

EPRO-CLD-035

Secure Relay Selection With Outdated CSI in Cooperative Wireless Vehicular Networks: A DQN Approach

provide a certain degree of fading mitigation and to improve spectral efficiency. In a cooperative scenario, the intercept probability of the system can be reduced by optimizing the relay selection scheme in order to select the optimal relay from a set of available relays for data transmission. However, due to the mobility of WVNs, the best relay is often selected in practice based on outdated channel state information (CSI), which in turn affects the overall system performance. Therefore, there is a need for a robust relay selection scheme (RSS) that guarantees a satisfactory overall achievable performance in the presence of an outdated CSI. Motivated by this and considering the advantageous features of autoregressive moving average (ARMA), the present contribution models a cooperative vehicular communication scenario with relay selection as a Markov decision process (MDP) and proposes two deep Q-networks (DQNs), namely DQN-RSS and DQN-RSS-ARMA.

EPRO-CLD-036

Depriving the Survival Space of Adversaries Against Poisoned Gradients in Federated Learning

they all fall short of securing practical FL scenarios with heterogeneous and unbalanced data distribution. Moreover, the cutting-edge defenses currently at our disposal demand access to a proprietary dataset that closely mirrors the distribution of clients' data, which runs counter to the fundamental principle of privacy protection in FL. It is still challenging to devise an effective defense approach that applies to practical FL. In this work, we strive to narrow the divide between FL defense and its practical use. We first present a general framework to comprehend the effect of poisoning attacks in FL when the training data is not independent and identically distributed (non-IID). We then present HeteroFL, a novel FL scheme that incorporates four complementary defensive strategies. These tactics are implemented in succession to refine the aggregated model toward approaching the global optimum. Ultimately, we devise an adaptive attack specifically for HeteroFL, aimed at offering a more thorough evaluation of its robustness.

EPRO-CLD-037

Learning Near-Optimal Intrusion Responses Against Dynamic Attackers

We study automated intrusion response and formulate the interaction between an attacker and a defender as an optimal stopping game where attack and defense strategies evolve through reinforcement learning and self-play. The game-theoretic modeling enables us to find defender strategies that are effective against a dynamic attacker, i.e. an attacker that adapts its strategy in response to the defender strategy. Further, the optimal stopping formulation allows us to prove that optimal strategies have threshold properties. To obtain near-optimal defender strategies, we develop Threshold Fictitious Self-Play (T-FP), a fictitious self-play algorithm that learns Nash equilibria through stochastic approximation.

EPRO-CLD-038

Trusted Operations of a Military Ground Robot in the Face of Man-in-the-Middle Cyberattacks Using Deep

on the concepts of deep learning Convolutional Neural Network (CNN). The proposed algorithm is specifically designed to reduce the cyber vulnerability of the Robot Operating System (ROS), a well-known middleware platform, widely used in both civilian and military domains. To demonstrate the efficacy of the proposed algorithm, we conduct penetration testing (real-time man-in-the-middle cyberattacks) on the GVR-BOT ground vehicle, a replicate of a military ground robot, developed by the United States Army Combat Capabilities Development Command (CCDC), Ground Vehicle Systems Center. The cyberattacks also exploit the vulnerability of the Robot Operating System employed on its onboard computer. We collect experimental data and train our CNN based on two different operating conditions, namely, legitimate and malicious. We normalize and convert the network traffic data in the form of RGB or grayscale images.

EPRO-CLD-039

Optimal Finite Horizon Scheduling of Wireless Networked Control Systems

scheduler located at the central node, i.e., base station (BS), determines the transmission schedule of sensor-to-BS and BS-to-controller communication links. We assume that each link can accommodate a single transmission at a time and is prone to data losses with time-varying probability. Moreover, each controller estimates the system state remotely based on available information. In such a setting, we formulate an optimization problem to minimize the network-induced estimation error at the controller. In particular, we determine the optimal transmission schedule on each link that leads to the minimum normalized mean squared error (nMSE) in a given finite horizon (FH). We compare the performance of our proposed FH scheduler to various schedulers from the existing literature. Our simulation results show that by solving the finite horizon problem optimally, we are able to reduce the nMSE by 10% when compared to the best performing scheduling policy among the selected policies from the state-of-the-art. Moreover, the linear-quadratic Gaussian (LQG) cost is reduced by more than 13% indicating a control performance improvement in the network.