**Elysium Technologies Private Limited**

**IEEE FINAL YEAR PROJECTS**

**CLOUD COMPUTING’ 2013 - 14**

---

**Why Choose Us?**

- 13 Years of Experience
- Automated Services
- 24/7 Help Desk Support
- Experience & Expertise Developers
- Advanced Technologies & Tools
- Legitimate Member of all Journals
- Having 1,50,000 Successive records in all Languages
- More than 12 Branches in Tamilnadu, Kerala & Karnataka.
- Ticketing & Appointment Systems.
- Individual Care for every Student.
- Around 250 Developers & 20 Researchers
Elysium Technologies Private Limited
Singapore | Madurai | Chennai | Trichy | Coimbatore | Cochin | Ramnad | Pondicherry | Trivandrum | Salem | Erode | Tirunelveli
http://www.elysiumtechnologies.com, info@elysiumtechnologies.com

Corporate Office: Madurai
227-230 Church Road, Anna Nagar, Madurai – 625020.
0452-4390702, 4392702, +91-9944793398.
info@elysiumtechnologies.com, elysiumtechnologies@gmail.com

Branch Office: Chennai
S.P.Towers, No.81 Valluvar Kottam High Road, Nungambakkam,
Chennai - 600034. 044-42072702, +91-9600354638,
chennai@elysiumtechnologies.com

Branch Office: Trichy
15, III Floor, SI Towers, Melapudur main Road, Trichy – 620001.
0431-4002234, +91-9790464324.
trichy@elysiumtechnologies.com

Branch Office: Coimbatore
577/4, DB Road, RS Puram, Opp to KFC, Coimbatore – 641002
0422- 4377758, +91-9677751577.
coimbatore@elysiumtechnologies.com
Branch Office: Ramnad
1st Floor, A.R.IT Park, Rasi Color Scan Building, Ramanathapuram
- 623501. 04567-223225,
+919677704922.ramnad@elysiumtechnologies.com

Branch Office: Tirunelveli
Plot No: 4, C Colony, P&T Extension, Perumal puram, Tirunelveli-
627007. 0462-2532104, +919677733255,
tirunelveli@elysiumtechnologies.com

Branch Office: Erode
74, 2nd floor, K.V.K Complex,Upstairs Krishna Sweets, Mettur Road, Opp. Bus stand, Erode-638 011. 0424-4030055, +91-
9677748477 eroode@elysiumtechnologies.com

Branch Office: Pondicherry
No: 88, First Floor, S.V.Patel Salai, Pondicherry – 605 001. 0413–
4200640 +91-9677704822
pondy@elysiumtechnologies.com

Branch Office: Salem
TNHB A-Block, D.no.10, Opp: Hotel Ganesh Near Busstand. Salem
– 636007, 0427-4042220, +91-989444716.
salem@elysiumtechnologies.com
**ETPL CLD-001**

Using Cloud Computing to Implement a Security Overlay Network

Abstract: This article proposes and analyzes a general cloud-based security overlay network that can be used as a transparent overlay network to provide services such as intrusion detection systems, antivirus and antispam software, and distributed denial-of-service prevention. The authors analyze each of these cloud security services in terms of resiliency, effectiveness, performance, flexibility, control, and cost.

---

**ETPL CLD-002**

Cloud computing-based forensic analysis for collaborative network security management system

Abstract: Internet security problems remain a major challenge with many security concerns such as Internet worms, spam, and phishing attacks. Botnets, well-organized distributed network attacks, consist of a large number of bots that generate huge volumes of spam or launch Distributed Denial of Service (DDoS) attacks on victim hosts. New emerging botnet attacks degrade the status of Internet security further. To address these problems, a practical collaborative network security management system is proposed with an effective collaborative Unified Threat Management (UTM) and traffic probers. A distributed security overlay network with a centralized security center leverages a peer-to-peer communication protocol used in the UTMs collaborative module and connects them virtually to exchange network events and security rules. Security functions for the UTM are retrofitted to share security rules. In this paper, we propose a design and implementation of a cloud-based security center for network security forensic analysis. We propose using cloud storage to keep collected traffic data and then processing it with cloud computing platforms to find the malicious attacks. As a practical example, phishing attack forensic analysis is presented and the required computing and storage resources are evaluated based on real trace data. The cloud-based security center can instruct each collaborative UTM and prober to collect events and raw traffic, send them back for deep analysis, and generate new security rules. These new security rules are enforced by collaborative UTM and the feedback events of such rules are returned to the security center. By this type of close-loop control, the collaborative network security management system can identify and address new distributed attacks more quickly and effectively.

---

**ETPL CLD-003**

Workload-Based Software Rejuvenation in Cloud Systems

Cloud computing is a promising paradigm able to rationalize the use of hardware resources by means of virtualization. Virtualization allows to instantiate one or more virtual machines (VMs) on top of a single physical machine managed by a virtual machine monitor (VMM). Similarly to any other software, a VMM experiences aging and failures. Software rejuvenation is a proactive fault management technique that involves terminating an application, cleaning up the system internal state, and restarting it to prevent the occurrence of future failures. In this work, we propose a technique to model and evaluate the VMM aging process and to investigate the optimal rejuvenation policy that maximizes the VMM availability under variable workload conditions. Starting from dynamic reliability theory and adopting symbolic algebraic techniques, we investigate and compare existing time-based VMM rejuvenation policies. We also propose a time-based policy that adapts the rejuvenation timer to the VMM workload condition improving the system availability. The effectiveness of the proposed modeling technique is demonstrated through a numerical example based on a case study taken from the literature.
<table>
<thead>
<tr>
<th>ETPL CLD-004</th>
<th>Security Challenges in Vehicular Cloud Computing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abstract: In a series of recent papers, Prof. Olariu and his co-workers have promoted the vision of vehicular clouds (VCs), a nontrivial extension, along several dimensions, of conventional cloud computing. In a VC, underutilized vehicular resources including computing power, storage, and Internet connectivity can be shared between drivers or rented out over the Internet to various customers. Clearly, if the VC concept is to see a wide adoption and to have significant societal impact, security and privacy issues need to be addressed. The main contribution of this work is to identify and analyze a number of security challenges and potential privacy threats in VCs. Although security issues have received attention in cloud computing and vehicular networks, we identify security challenges that are specific to VCs, e.g., challenges of authentication of high-mobility vehicles, scalability and single interface, tangled identities and locations, and the complexity of establishing trust relationships among multiple players caused by intermittent short-range communications. Additionally, we provide a security scheme that addresses several of the challenges discussed.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ETPL CLD-005</th>
<th>Security and Privacy in Cloud Computing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abstract: Recent advances have given rise to the popularity and success of cloud computing. However, when outsourcing the data and business application to a third party causes the security and privacy issues to become a critical concern. Throughout the study at hand, the authors obtain a common goal to provide a comprehensive review of the existing security and privacy issues in cloud environments. We have identified five most representative security and privacy attributes (i.e., confidentiality, integrity, availability, accountability, and privacy-preservability). Beginning with these attributes, we present the relationships among them, the vulnerabilities that may be exploited by attackers, the threat models, as well as existing defense strategies in a cloud scenario. Future research directions are previously determined for each attribute.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ETPL CLD-006</th>
<th>Performance of Virtual Machines Under Networked Denial of Service Attacks: Experiments and Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abstract: The use of virtual machines (VMs) to provide computational infrastructure and services to organizations is increasingly prevalent in the modern IT industry. The growing use of this technology has been driven by a desire to increase utilization of resources through server consolidation. Virtualization has also made the dream of such utility computing platforms as cloud computing a reality. Today, virtualization technologies can be found in almost every data center. However, it remains unknown whether the VMs are more vulnerable on external malicious attacks. If so, to what extent their performance degrades, and which virtualization technique has the closest to native performance? To this end, we devised a representative set of experiments to examine the performance of most typical virtualization techniques under typical denial-of-service (DoS) attacks. We show that, on a DoS attack, the performance of a web server hosted in a VM can degrade by up to 23%, while that of a nonvirtualized server hosted on the same hardware degrades by only 8%. Even with relatively light attacks, the file system and memory access performance of hypervisor-based virtualization degrades at a much higher rate.</td>
<td></td>
</tr>
</tbody>
</table>
than their nonvirtualized counterparts. We further examine the root causes of such degradation and our results shed new lights in enhancing the robustness and security of modern virtualization systems.

### NICE: Network Intrusion Detection and Countermeasure Selection in Virtual Network Systems

**Abstract:** Cloud security is one of the most important issues that has attracted a lot of research and development effort in recent years. Particularly, attackers can exploit vulnerabilities of a cloud system and compromise virtual machines to deploy further large-scale Distributed Denial-of-Service (DDoS). DDoS attacks usually involve early stage actions such as multistep exploitation, low-frequency vulnerability scanning, and compromising identified vulnerable virtual machines as zombies, and finally DDoS attacks through the compromised zombies. Within the cloud system, especially the Infrastructure-as-a-Service (IaaS) clouds, the detection of zombie exploration attacks is extremely difficult. This is because cloud users may install vulnerable applications on their virtual machines. To prevent vulnerable virtual machines from being compromised in the cloud, we propose a multiphase distributed vulnerability detection, measurement, and countermeasure selection mechanism called NICE, which is built on attack graph-based analytical models and reconfigurable virtual network-based countermeasures. The proposed framework leverages OpenFlow network programming APIs to build a monitor and control plane over distributed programmable virtual switches to significantly improve attack detection and mitigate attack consequences. The system and security evaluations demonstrate the efficiency and effectiveness of the proposed solution.

### CloudAC: a cloud-oriented multilayer access control system for logic virtual domain

**Abstract:** The security issue has been a challenging concern for cloud computing because of the multitenant usage model. In cloud, each application normally runs on a dynamic coalition that is composed by multiple virtual machines (VMs) running on different virtualised service nodes, which the authors called logic virtual domain (LVD). Moreover, the owners of cloud applications, who are also the tenants of cloud, would specify some security policies to control the access to those resources that they have paid for. Therefore the owners of cloud infrastructures have to provide the tenants with the mechanism to correctly configure and enforce the access control policies on resources that are from multiple service nodes, to meet the security requirements from cloud applications. To address the above challenge, this study presents the design and implementation about a multilayer access control architecture for LVD, named CloudAC, aiming to provide isolation control, information flow control and resource-sharing control among multiple VMs on Xen virtualisation platforms in cloud computing environment. The theory and technology this research formed will provide reliable security guarantee for resource configuration and application deployment on LVDs.

### Towards Trustworthy Resource Scheduling in Clouds

**Abstract:** Managing the allocation of cloud virtual machines at physical resources is a key requirement for the success of clouds. Current implementations of cloud schedulers do not consider the entire cloud infrastructure neither do they consider the overall user and infrastructure properties. This results in major security, privacy, and resilience concerns. In this paper, we propose a novel cloud scheduler which considers both user requirements and infrastructure properties. We focus on assuring users that their
virtual resources are hosted using physical resources that match their requirements without getting users involved with understanding the details of the cloud infrastructure. As a proof-of-concept, we present our prototype which is built on OpenStack. The provided prototype implements the proposed cloud scheduler. It also provides an implementation of our previous work on cloud trust management which provides the scheduler with input about the trust status of the cloud infrastructure.

**ETPL CLD-010**

**Gearing resource-poor mobile devices with powerful clouds: architectures, challenges, and applications**

Abstract: Mobile cloud computing, with its promise to meet the urgent need for richer applications and services of resource-constrained mobile devices, is emerging as a new computing paradigm and has recently attracted significant attention. However, there is no clear definition and no well-defined scope for mobile cloud computing due to commercial hype, and diverse ways of combining cloud computing and mobile applications. This article makes the first attempt to present a survey of mobile cloud computing from the perspective of its intended usages. Specifically, we introduce three common mobile cloud architectures and classify comprehensive existing work into two fundamental categories: computation offloading and capability extending. Considering the energy bottleneck and user context of mobile devices, we discuss the research challenges and opportunities of introducing cloud computing to assist mobile devices, including energy-efficient interactions, virtual machine migration overhead, privacy, and security. Moreover, we demonstrate three real-world applications enabled by mobile cloud computing, in order to stimulate further discussion and development of this emerging field.

**ETPL CLD-011**

**uCloud: a user-centric key management scheme for cloud data protection**

Abstract: One of the most challenging problems of cloud service solicitation is to persuade users to trust the security of cloud service and upload their sensitive data. Although cloud service providers can claim that their services are well-protected by elaborate encryption mechanisms, traditional cloud systems still cannot persuade the users that even if the cloud servers are compromised, the data are still securely protected. This study proposes uCloud, a user-centric key management scheme for cloud data protection, to solve this problem. uCloud utilizes RSA and indirectly encrypts users’ data by users’ public keys, but stores the users’ private keys on neither servers nor users’ PCs; instead, the private keys are stored on users’ mobile devices and presented via two-dimensional (2D) barcode images when they are utilized to decrypt users’ sensitive data. In this manner, users’ data are safely protected even if the cloud servers are compromised. Also, uCloud provides users with the experience of managing visible private keys by storing the keys into mobile phones and displaying them via 2D barcodes. Moreover, three scenarios: personal storage, home surveillance and enterprise storage scenarios are proposed to present the practicability of uCloud. In addition, a hierarchical structure is designed for basic key backup and data sharing in the proposed scheme.

**ETPL CLD-012**

**Toward Secure Multikeyword Top-k Retrieval over Encrypted Cloud Data**

Abstract: Cloud computing has emerging as a promising pattern for data outsourcing and high-quality data services. However, concerns of sensitive information on cloud potentially causes privacy problems. Data encryption protects data security to some extent, but at the cost of compromised efficiency. Searchable symmetric encryption (SSE) allows retrieval of encrypted data over cloud. In this paper, we
focus on addressing data privacy issues using SSE. For the first time, we formulate the privacy issue from the aspect of similarity relevance and scheme robustness. We observe that server-side ranking based on order-preserving encryption (OPE) inevitably leaks data privacy. To eliminate the leakage, we propose a two-round searchable encryption (TRSE) scheme that supports top-$k$ multikeyword retrieval. In TRSE, we employ a vector space model and homomorphic encryption. The vector space model helps to provide sufficient search accuracy, and the homomorphic encryption enables users to involve in the ranking while the majority of computing work is done on the server side by operations only on ciphertext. As a result, information leakage can be eliminated and data security is ensured. Thorough security and performance analysis show that the proposed scheme guarantees high security and practical efficiency.

### ETPL CLD-013  
**Attribute-Based Encryption With Verifiable Outsourced Decryption**

Abstract: Attribute-based encryption (ABE) is a public-key-based one-to-many encryption that allows users to encrypt and decrypt data based on user attributes. A promising application of ABE is flexible access control of encrypted data stored in the cloud, using access polices and ascribed attributes associated with private keys and ciphertexts. One of the main efficiency drawbacks of the existing ABE schemes is that decryption involves expensive pairing operations and the number of such operations grows with the complexity of the access policy. Recently, Green proposed an ABE system with outsourced decryption that largely eliminates the decryption overhead for users. In such a system, a user provides an untrusted server, say a cloud service provider, with a transformation key that allows the cloud to translate any ABE ciphertext satisfied by that user's attributes or access policy into a simple ciphertext, and it only incurs a small computational overhead for the user to recover the plaintext from the transformed ciphertext. Security of an ABE system with outsourced decryption ensures that an adversary (including a malicious cloud) will not be able to learn anything about the encrypted message; however, it does not guarantee the correctness of the transformation done by the cloud. In this paper, we consider a new requirement of ABE with outsourced decryption: verifiability. Informally, verifiability guarantees that a user can efficiently check if the transformation is done correctly. We give the formal model of ABE with verifiable outsourced decryption and propose a concrete scheme. We prove that our new scheme is both secure and verifiable, without relying on random oracles. Finally, we show an implementation of our scheme and result of performance measurements, which indicates a significant reduction on computing resources imposed on users.

### ETPL CLD-014  
**Harnessing the Cloud for Securely Outsourcing Large-Scale Systems of Linear Equations**

Abstract: Cloud computing economically enables customers with limited computational resources to outsource large-scale computations to the cloud. However, how to protect customers' confidential data involved in the computations then becomes a major security concern. In this paper, we present a secure outsourcing mechanism for solving large-scale systems of linear equations (LE) in cloud. Because applying traditional approaches like Gaussian elimination or LU decomposition (aka. direct method) to such large-scale LEs would be prohibitively expensive, we build the secure LE outsourcing mechanism via a completely different approach-iterative method, which is much easier to implement in practice and only demands relatively simpler matrix-vector operations. Specifically, our mechanism enables a customer to securely harness the cloud for iteratively finding successive approximations to the LE
solution, while keeping both the sensitive input and output of the computation private. For robust cheating
detection, we further explore the algebraic property of matrix-vector operations and propose an efficient
result verification mechanism, which allows the customer to verify all answers received from previous
iterative approximations in one batch with high probability. Thorough security analysis and prototype
experiments on Amazon EC2 demonstrate the validity and practicality of our proposed design.

ETPL
CLD-015  Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud

Abstract: With the character of low maintenance, cloud computing provides an economical and efficient
solution for sharing group resource among cloud users. Unfortunately, sharing data in a multi-owner
manner while preserving data and identity privacy from an untrusted cloud is still a challenging issue, due
to the frequent change of the membership. In this paper, we propose a secure multi-owner data sharing
scheme, named Mona, for dynamic groups in the cloud. By leveraging group signature and dynamic
broadcast encryption techniques, any cloud user can anonymously share data with others. Meanwhile, the
storage overhead and encryption computation cost of our scheme are independent with the number of
revoked users. In addition, we analyze the security of our scheme with rigorous proofs, and demonstrate
the efficiency of our scheme in experiments.

ETPL
CLD-016  Key Challenges in Cloud Computing: Enabling the Future Internet of Services

Abstract: Cloud computing will play a major role in the future Internet of Services, enabling on-demand
provisioning of applications, platforms, and computing infrastructures. However, the cloud community
must address several technology challenges to turn this vision into reality. Specific issues relate to
deploying future infrastructure-as-a-service clouds and include efficiently managing such clouds to
deliver scalable and elastic service platforms on demand, developing cloud aggregation architectures and
technologies that let cloud providers collaborate and interoperate, and improving cloud infrastructures'
security, reliability, and energy efficiency.

ETPL
CLD-017  Privacy-Preserving Public Auditing for Secure Cloud Storage

Abstract: Using cloud storage, users can remotely store their data and enjoy the on-demand high-quality
applications and services from a shared pool of configurable computing resources, without the burden of
local data storage and maintenance. However, the fact that users no longer have physical possession of the
outsourced data makes the data integrity protection in cloud computing a formidable task, especially for
users with constrained computing resources. Moreover, users should be able to just use the cloud storage
as if it is local, without worrying about the need to verify its integrity. Thus, enabling public auditability
for cloud storage is of critical importance so that users can resort to a third-party auditor (TPA) to check
the integrity of outsourced data and be worry free. To securely introduce an effective TPA, the auditing
process should bring in no new vulnerabilities toward user data privacy, and introduce no additional
online burden to user. In this paper, we propose a secure cloud storage system supporting privacy-
preserving public auditing. We further extend our result to enable the TPA to perform audits for multiple
users simultaneously and efficiently. Extensive security and performance analysis show the proposed
schemes are provably secure and highly efficient. Our preliminary experiment conducted on Amazon EC2
instance further demonstrates the fast performance of the design.
### CAM: Cloud-Assisted Privacy Preserving Mobile Health Monitoring

**Abstract:** Cloud-assisted mobile health (mHealth) monitoring, which applies the prevailing mobile communications and cloud computing technologies to provide feedback decision support, has been considered as a revolutionary approach to improving the quality of healthcare service while lowering the healthcare cost. Unfortunately, it also poses a serious risk on both clients' privacy and intellectual property of monitoring service providers, which could deter the wide adoption of mHealth technology. This paper is to address this important problem and design a cloud-assisted privacy preserving mobile health monitoring system to protect the privacy of the involved parties and their data. Moreover, the outsourcing decryption technique and a newly proposed key private proxy reencryption are adapted to shift the computational complexity of the involved parties to the cloud without compromising clients' privacy and service providers' intellectual property. Finally, our security and performance analysis demonstrates the effectiveness of our proposed design.

### Visualization framework for inter-domain access control policy integration

**Abstract:** The rapid increase in resource sharing across domains in the cloud computing environment makes the task of managing inter-domain access control policy integration difficult for the security administrators. Although a number of policy integration and security analysis mechanisms have been developed, few focus on enabling the average administrator by providing an intuitive cognitive sense about the integrated policies, which considerably undermines the usability factor. In this paper we propose a visualization framework for inter-domain access control policy integration, which integrates Role Based Access Control (RBAC) policies on the basis of role-mapping and then visualizes the integrated result. The role mapping algorithm in the framework considers the hybrid role hierarchy. It can not only satisfy the security constraints of non-cyclic inheritance and separation of duty but also make visualization easier. The framework uses role-permission trees and semantic substrates to visualize the integrated policies. Through the interactive policy query visualization, the average administrator can gain an intuitive understanding of the policy integration result.

### SeDas: A Self-Destructing Data System Based on Active Storage Framework

**Abstract:** Personal data stored in the Cloud may contain account numbers, passwords, notes, and other important information that could be used and misused by a miscreant, a competitor, or a court of law. These data are cached, copied, and archived by Cloud Service Providers (CSPs), often without users' authorization and control. Self-destructing data mainly aims at protecting the user data's privacy. All the data and their copies become destructed or unreadable after a user-specified time, without any user intervention. In addition, the decryption key is destructed after the user-specified time. In this paper, we present SeDas, a system that meets this challenge through a novel integration of cryptographic techniques with active storage techniques based on T10 OSD standard. We implemented a proof-of-concept SeDas prototype. Through functionality and security properties evaluations of the SeDas prototype, the results demonstrate that SeDas is practical to use and meets all the privacy-preserving goals described. Compared to the system without self-destructing data mechanism, throughput for uploading and downloading with the proposed SeDas acceptably decreases by less than 72%, while latency for
upload/download operations with self-destructing data mechanism increases by less than 60%.

### ETPL CLD-021 Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption

**Abstract:** Personal health record (PHR) is an emerging patient-centric model of health information exchange, which is often outsourced to be stored at a third party, such as cloud providers. However, there have been wide privacy concerns as personal health information could be exposed to those third party servers and to unauthorized parties. To assure the patients’ control over access to their own PHRs, it is a promising method to encrypt the PHRs before outsourcing. Yet, issues such as risks of privacy exposure, scalability in key management, flexible access, and efficient user revocation, have remained the most important challenges toward achieving fine-grained, cryptographically enforced data access control. In this paper, we propose a novel patient-centric framework and a suite of mechanisms for data access control to PHRs stored in semitrusted servers. To achieve fine-grained and scalable data access control for PHRs, we leverage attribute-based encryption (ABE) techniques to encrypt each patient's PHR file. Different from previous works in secure data outsourcing, we focus on the multiple data owner scenario, and divide the users in the PHR system into multiple security domains that greatly reduces the key management complexity for owners and users. A high degree of patient privacy is guaranteed simultaneously by exploiting multiauthority ABE. Our scheme also enables dynamic modification of access policies or file attributes, supports efficient on-demand user/attribute revocation and break-glass access under emergency scenarios. Extensive analytical and experimental results are presented which show the security, scalability, and efficiency of our proposed scheme.

### ETPL CLD-022 An Effective Network Traffic Classification Method with Unknown Flow Detection

**Abstract:** Traffic classification technique is an essential tool for network and system security in the complex environments such as cloud computing based environment. The state-of-the-art traffic classification methods aim to take the advantages of flow statistical features and machine learning techniques, however the classification performance is severely affected by limited supervised information and unknown applications. To achieve effective network traffic classification, we propose a new method to tackle the problem of unknown applications in the crucial situation of a small supervised training set. The proposed method possesses the superior capability of detecting unknown flows generated by unknown applications and utilizing the correlation information among real-world network traffic to boost the classification performance. A theoretical analysis is provided to confirm performance benefit of the proposed method. Moreover, the comprehensive performance evaluation conducted on two real-world network traffic datasets shows that the proposed scheme outperforms the existing methods in the critical network environment.

### ETPL CLD-023 A Novel Privacy Preserving Location-Based Service Protocol With Secret Circular Shift for k-NN Search

**Abstract:** Location-based service (LBS) is booming up in recent years with the rapid growth of mobile devices and the emerging of cloud computing paradigm. Among the challenges to establish LBS, the user privacy issue becomes the most important concern. A successful privacy-preserving LBS must be secure and provide accurate query [e.g., -nearest neighbor (NN)] results. In this work, we propose a private
circular query protocol (PCQP) to deal with the privacy and the accuracy issues of privacy-preserving LBS. The protocol consists of a space filling curve and a public-key homomorphic cryptosystem. First, we connect the points of interest (POIs) on a map to form a circular structure with the aid of a Moore curve. And then the homomorphism of Paillier cryptosystem is used to perform secret circular shifts of POI-related information (POI-info), stored on the server side. Since the POI-info after shifting and the amount of shifts are encrypted, LBS providers (e.g., servers) have no knowledge about the user's location during the query process. The protocol can resist correlation attack and support a multiuser scenario as long as the predescribed secret circular shift is performed before each query; in other words, the robustness of the proposed protocol is the same as that of a one-time pad encryption scheme. As a result, the security level of the proposed protocol is close to perfect secrecy without the aid of a trusted third party and simulation results show that the k-NN query accuracy rate of the proposed protocol is higher than 90% even when is large.

### ETPL CLD-024 From the Enterprise Perimeter to a Mobility-Enabled Secure Cloud

Abstract: The enterprise perimeter has exhibited gradual trust degradation owing to a succession of connectivity decisions involving Web, email, virtual private networking, exceptions, and mobile networks as well as a succession of threats including malware and advanced persistent threats (APTs). The author proposes restoring trust to the enterprise by focusing protection strategies on a set of prioritized assets. The protections center on three zones: a client zone, a network zone with network-based carrier protection services, and a cloud zone with third-party attested security heavily indexed toward identity and access management services. The resultant enterprise network is more resilient to leakage attacks such as APTs.

### ETPL CLD-025 Dynamic Audit Services for Outsourced Storages in Clouds

Abstract: In this paper, we propose a dynamic audit service for verifying the integrity of an untrusted and outsourced storage. Our audit service is constructed based on the techniques, fragment structure, random sampling, and index-hash table, supporting provable updates to outsourced data and timely anomaly detection. In addition, we propose a method based on probabilistic query and periodic verification for improving the performance of audit services. Our experimental results not only validate the effectiveness of our approaches, but also show our audit system verifies the integrity with lower computation overhead and requiring less extra storage for audit metadata.

### ETPL CLD-026 Collaboration in multicloud computing environments: Framework and security issues

Abstract: A proposed proxy-based multicloud computing framework allows dynamic, on-the-fly collaborations and resource sharing among cloud-based services, addressing trust, policy, and privacy issues without preestablished collaboration agreements or standardized interfaces.

### ETPL CLD-027 Privacy Preserving Data Sharing With Anonymous ID Assignment

Abstract: An algorithm for anonymous sharing of private data among N parties is developed. This technique is used iteratively to assign these nodes ID numbers ranging from 1 to N. This assignment is anonymous in that the identities received are unknown to the other members of the group. Resistance to
collusion among other members is verified in an information theoretic sense when private communication channels are used. This assignment of serial numbers allows more complex data to be shared and has applications to other problems in privacy preserving data mining, collision avoidance in communications and distributed database access. The required computations are distributed without using a trusted central authority. Existing and new algorithms for assigning anonymous IDs are examined with respect to trade-offs between communication and computational requirements. The new algorithms are built on top of a secure sum data mining operation using Newton's identities and Sturm's theorem. An algorithm for distributed solution of certain polynomials over finite fields enhances the scalability of the algorithms. Markov chain representations are used to find statistics on the number of iterations required, and computer algebra gives closed form results for the completion rates.

**ETPL CLD-028**  
**Adaptive and attribute-based trust model for service level agreement guarantee in cloud computing**

Abstract: In cloud computing, trust management is more important than ever before in the use of information and communication technologies. Owing to the dynamic nature of the cloud, continuous monitoring on trust attributes is necessary to enforce service-level agreements. This study presents Cloud-Trust, an adaptive trust management model for efficiently evaluating the competence of a cloud service based on its multiple trust attributes. In Cloud-Trust, two kinds of adaptive modelling tools (rough set and induced ordered weighted averaging (IOWA) operator) are organically integrated and successfully applied to trust data mining and knowledge discovery. Using rough set to discover knowledge from trust attributes makes the model surpass the limitations of traditional models, in which weights are assigned subjectively. Moreover, Cloud-Trust uses the IOWA operator to aggregate the global trust degree based on time series, thereby enabling better real-time performance. Experimental results show that Cloud-Trust converges more rapidly and accurately than do existing approaches, thereby verifying that it can effectively take on trust measurement tasks in cloud computing.

**ETPL CLD-029**  
**Using Mussel-Inspired Self-Organization and Account Proxies to Obfuscate Workload Ownership and Placement in Clouds**

Abstract: Recent research has provided evidence indicating how a malicious user could perform coresidence profiling and public-to-private IP mapping to target and exploit customers which share physical resources. The attacks rely on two steps: resource placement on the target's physical machine and extraction. Our proposed solution, in part inspired by mussel self-organization, relies on user account and workload clustering to mitigate coresidence profiling. Users with similar preferences and workload characteristics are mapped to the same cluster. To obfuscate the public-to-private IP map, each cluster is managed and accessed by an account proxy. Each proxy uses one public IP address, which is shared by all clustered users when accessing their instances, and maintains the mapping to private IP addresses. We describe a set of capabilities and attack paths an attacker needs to execute for targeted coresidence, and present arguments to show how our approach disrupts the critical steps in the attack path for most cases. We then perform a risk assessment to determine the likelihood an individual user will be victimized, given that a successful nondirected exploit has occurred. Our results suggest that while possible, this event is highly unlikely.
**ETPL CLD-030  Performance Analysis of Network I/O Workloads in Virtualized Data Centers**

Abstract: Server consolidation and application consolidation through virtualization are key performance optimizations in cloud-based service delivery industry. In this paper, we argue that it is important for both cloud consumers and cloud providers to understand the various factors that may have significant impact on the performance of applications running in a virtualized cloud. This paper presents an extensive performance study of network I/O workloads in a virtualized cloud environment. We first show that current implementation of virtual machine monitor (VMM) does not provide sufficient performance isolation to guarantee the effectiveness of resource sharing across multiple virtual machine instances (VMs) running on a single physical host machine, especially when applications running on neighboring VMs are competing for computing and communication resources. Then we study a set of representative workloads in cloud-based data centers, which compete for either CPU or network I/O resources, and present the detailed analysis on different factors that can impact the throughput performance and resource sharing effectiveness. For example, we analyze the cost and the benefit of running idle VM instances on a physical host where some applications are hosted concurrently. We also present an in-depth discussion on the performance impact of colocating applications that compete for either CPU or network I/O resources. Finally, we analyze the impact of different CPU resource scheduling strategies and different workload rates on the performance of applications running on different VMs hosted by the same physical machine.

**ETPL CLD-031  Attribute-Based Access to Scalable Media in Cloud-Assisted Content Sharing Networks**

Abstract: This paper presents a novel Multi-message Ciphertext Policy Attribute-Based Encryption (MCP-ABE) technique, and employs the MCP-ABE to design an access control scheme for sharing scalable media based on data consumers' attributes (e.g., age, nationality, or gender) rather than an explicit list of the consumers' names. The scheme is efficient and flexible because MCP-ABE allows a content provider to specify an access policy and encrypt multiple messages within one ciphertext such that only the users whose attributes satisfy the access policy can decrypt the ciphertext. Moreover, the paper shows how to support resource-limited mobile devices by offloading computational intensive operations to cloud servers while without compromising data privacy.

**ETPL CLD-032  Secure Logging as a Service—Delegating Log Management to the Cloud**

Abstract: Securely maintaining log records over extended periods of time is very important to the proper functioning of any organization. Integrity of the log files and that of the logging process need to be ensured at all times. In addition, as log files often contain sensitive information, confidentiality and privacy of log records are equally important. However, deploying a secure logging infrastructure involves substantial capital expenses that many organizations may find overwhelming. Delegating log management to the cloud appears to be a viable cost saving measure. In this paper, we identify the challenges for a
secure cloud-based log management service and propose a framework for doing the same.

**ETPL CLD-033 Enabling Data Integrity Protection in Regenerating-Coding-Based Cloud Storage: Theory and Implementation**

Abstract: To protect outsourced data in cloud storage against corruptions, adding fault tolerance to cloud storage, along with efficient data integrity checking and recovery procedures, becomes critical. Regenerating codes provide fault tolerance by striping data across multiple servers, while using less repair traffic than traditional erasure codes during failure recovery. Therefore, we study the problem of remotely checking the integrity of regenerating-coded data against corruptions under a real-life cloud storage setting. We design and implement a practical data integrity protection (DIP) scheme for a specific regenerating code, while preserving its intrinsic properties of fault tolerance and repair traffic saving. Our DIP scheme is designed under a mobile Byzantine adversarial model, and enables a client to feasibly verify the integrity of random subsets of outsourced data against general or malicious corruptions. It works under the simple assumption of thin-cloud storage and allows different parameters to be fine-tuned for a performance-security trade-off. We implement and evaluate the overhead of our DIP scheme in a real cloud storage testbed under different parameter choices. We further analyze the security strengths of our DIP scheme via mathematical models. We demonstrate that remote integrity checking can be feasibly integrated into regenerating codes in practical deployment.

**ETPL CLD-034 A Cloud-Based Approach to Interoperable EHRs**

Abstract: We present a cloud-based approach for the design of interoperable Electronic Health Record (EHR) systems. Cloud computing environments provide several benefits to all the stakeholders in the healthcare ecosystem (patients, providers, payers, etc.). Lack of data interoperability standards and solutions has been a major obstacle in the exchange of healthcare data between different stakeholders. We propose an EHR system - Cloud Health Information Systems Technology Architecture (CHISTAR), that achieves semantic interoperability through the use of a generic design methodology which uses a reference model that defines a general purpose set of data structures and an archetype model that defines the clinical data attributes. CHISTAR application components are designed using the Cloud Component Model approach that comprises of loosely coupled components that communicate asynchronously. In this paper we describe the high level design of CHISTAR and the approaches for semantic interoperability, data integration and security.

**ETPL CLD-035 Enabling Dynamic Data and Indirect Mutual Trust for Cloud Computing Storage Systems**

Abstract: Storage-as-a-Service (SaaS) offered by cloud service providers (CSPs) is a paid facility that enables organizations to outsource their sensitive data to be stored on remote servers. Thus, SaaS reduces the maintenance cost and mitigates the burden of large local data storage at the organization's end. A data owner pays for a desired level of security and must get some compensation in case of any misbehavior committed by the CSP. On the other hand, the CSP needs a protection from any false accusation that may be claimed by the owner to get illegal compensations. In this paper, we propose a cloud-based storage...
scheme that allows the data owner to benefit from the facilities offered by the CSP and enables indirect mutual trust between them. The proposed scheme has four important features: (i) it allows the owner to outsource sensitive data to a CSP, and perform full block-level dynamic operations on the outsourced data, i.e., block modification, insertion, deletion, and append, (ii) it ensures that authorized users (i.e., those who have the right to access the owner's file) receive the latest version of the outsourced data, (iii) it enables indirect mutual trust between the owner and the CSP, and (iv) it allows the owner to grant or revoke access to the outsourced data. We discuss the security issues of the proposed scheme. Besides, we justify its performance through theoretical analysis and a prototype implementation on Amazon cloud platform to evaluate storage, communication, and computation overheads.

**ETPL CLD-036**
**Distributed, Concurrent, and Independent Access to Encrypted Cloud Databases**

Abstract: Placing critical data in the hands of a cloud provider should come with the guarantee of security and availability for data at rest, in motion, and in use. Several alternatives exist for storage services, while data confidentiality solutions for the Database as a Service paradigm are still immature. We propose a novel architecture that integrates cloud database services with data confidentiality and the possibility of executing concurrent operations on encrypted data. This is the first solution supporting geographically distributed clients to connect directly to an encrypted cloud database, and to execute concurrent and independent operations including those modifying the database structure. The proposed architecture has the further advantage of eliminating intermediate proxies that limit the elasticity, availability and scalability properties that are intrinsic in cloud-based solutions. The efficacy of the proposed architecture is evaluated through theoretical analyses and extensive experimental results based on a prototype implementation subject to the TPC-C standard benchmark for different numbers of clients and network latencies.

**ETPL CLD-037**
**On the Knowledge Soundness of a Cooperative Provable Data Possession Scheme in Multicloud Storage**

Abstract: Provable data possession (PDP) is a probabilistic proof technique for cloud service providers (CSPs) to prove the clients' data integrity without downloading the whole data. In 2012, Zhu (em et al.) proposed the construction of an efficient PDP scheme for multicloud storage. They studied the existence of multiple CSPs to cooperatively store and maintain the clients' data. Then, based on homomorphic verifiable response and hash index hierarchy, they presented a cooperative PDP (CPDP) scheme from the bilinear pairings. They claimed that their scheme satisfied the security property of knowledge soundness. It is regretful that this comment shows that any malicious cloud service provider (CSP) or the malicious organizer (O) can generate the valid response which can pass the verification even if they have deleted all the stored data, {em i.e.}, Zhu (em et al.)'s CPDP scheme can not satisfy the property of knowledge soundness. Then, we discuss the origin and severity of the security flaws. It implies that the attacker can get the pay without storing the clients' data. It is important to clarify the scientific fact in order to design more secure and practical CPDP scheme in Zhu (em et al.)'s system architecture and security model.

**ETPL CLD-038**
**Cross-Layer Dynamic Admission Control for Cloud-Based Multimedia Sensor Networks**

Abstract: Cloud-based communications system is now widely used in many application fields such as medicine, security, environment protection, etc. Its use is being extended to the most demanding services
like multimedia delivery. However, there are a lot of constraints when cloud-based sensor networks use the standard IEEE 802.15.3 or IEEE 802.15.4 technologies. This paper proposes a channel characterization scheme combined to a cross-layer admission control in dynamic cloud-based multimedia sensor networks to share the network resources among any two nodes. The analysis shows the behavior of two nodes using different network access technologies and the channel effects for each technology. Moreover, the existence of optimal node arrival rates in order to improve the usage of dynamic admission control when network resources are used is also shown. An extensive simulation study was performed to evaluate and validate the efficiency of the proposed dynamic admission control for cloud-based multimedia sensor networks.

<table>
<thead>
<tr>
<th>ETPL CLD-039</th>
<th>Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abstract: Data sharing is an important functionality in cloud storage. In this article, we show how to securely, efficiently, and flexibly share data with others in cloud storage. We describe new public-key cryptosystems which produce constant-size ciphertexts such that efficient delegation of decryption rights for any set of ciphertexts are possible. The novelty is that one can aggregate any set of secret keys and make them as compact as a single key, but encompassing the power of all the keys being aggregated. In other words, the secret key holder can release a constant-size aggregate key for flexible choices of ciphertext set in cloud storage, but the other encrypted files outside the set remain confidential. This compact aggregate key can be conveniently sent to others or be stored in a smart card with very limited secure storage. We provide formal security analysis of our schemes in the standard model. We also describe other application of our schemes. In particular, our schemes give the first public-key patient-controlled encryption for flexible hierarchy, which was yet to be known.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ETPL CLD-040</th>
<th>Building Confidential and Efficient Query Services in the Cloud with RASP Data Perturbation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abstract: Using clouds to host data query services has become an appealing solution for the advantages on scalability and cost-saving. However, some data might be sensitive that the data owner does not want to move to the cloud unless the data confidentiality and query privacy are guaranteed. In addition, a secured query service should still provide efficient query processing and significantly reduce the in-house workload for the purpose of cloud computing. Bearing these criteria in mind, we propose the RASP data perturbation method to provide secure range query and kNN query services for protected data in the cloud. The RASP data perturbation method combines order preserving encryption, dimensionality expansion, random noise injection, and random projection, to provide strong resilience to attacks on the perturbed data and queries. It also preserves multidimensional ranges, which allows existing multidimensional indexing techniques to be applied in range query processing. The kNN-R algorithm is designed to work with the RASP range query algorithm to process the kNN queries. We carefully analyze the attacks on data and queries under a precisely defined threat model and realistic assumptions. Extensive experiments have been conducted to show the advantages of this approach on the balance of performance and security.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ETPL CLD-041</th>
<th>Discovery and Resolution of Anomalies in Web Access Control Policies</th>
</tr>
</thead>
</table>
Abstract: Emerging computing technologies such as Web services, service-oriented architecture, and cloud computing has enabled us to perform business services more efficiently and effectively. However, we still suffer from unintended security leakages by unauthorized actions in business services while providing more convenient services to Internet users through such a cutting-edge technological growth. Furthermore, designing and managing Web access control policies are often error-prone due to the lack of effective analysis mechanisms and tools. In this paper, we represent an innovative policy anomaly analysis approach for Web access control policies, focusing on XACML (eXtensible Access Control Markup Language) policy. We introduce a policy-based segmentation technique to accurately identify policy anomalies and derive effective anomaly resolutions, along with an intuitive visualization representation of analysis results. We also discuss a proof-of-concept implementation of our method called XAnalyzer and demonstrate how our approach can efficiently discover and resolve policy anomalies.

ETPL CLD-042  Balancing Performance, Accuracy, and Precision for Secure Cloud Transactions

Abstract: In distributed transactional database systems deployed over cloud servers, entities cooperate to form proofs of authorizations that are justified by collections of certified credentials. These proofs and credentials may be evaluated and collected over extended time periods under the risk of having the underlying authorization policies or the user credentials being in inconsistent states. It therefore becomes possible for policy-based authorization systems to make unsafe decisions that might threaten sensitive resources. In this paper, we highlight the criticality of the problem. We then define the notion of trusted transactions when dealing with proofs of authorizations. Accordingly, we propose several increasingly-stringent levels of policy consistency constraints, and present different enforcement approaches to guarantee the trustworthiness of transactions executing on cloud servers. We propose a Two-Phase Validation Commit protocol as a solution, which is a modified version of the basic Two-Phase Commit protocols. We finally analyze the different presented approaches using both analytical evaluation of the overheads and simulations to guide the decision makers to which approach to use.

ETPL CLD-043  Scalable Distributed Service Integrity Attestation for Software-as-a-Service Clouds

Abstract: Software-as-a-Service (SaaS) cloud systems enable application service providers to deliver their applications via massive cloud computing infrastructures. However, due to their sharing nature, SaaS clouds are vulnerable to malicious attacks. In this paper, we present IntTest, a scalable and effective service integrity attestation framework for SaaS clouds. IntTest provides a novel integrated attestation graph analysis scheme that can provide stronger attacker pinpointing power than previous schemes. Moreover, IntTest can automatically enhance result quality by replacing bad results produced by malicious attackers with good results produced by benign service providers. We have implemented a prototype of the IntTest system and tested it on a production cloud computing infrastructure using IBM System S stream processing applications. Our experimental results show that IntTest can achieve higher attacker pinpointing accuracy than existing approaches. IntTest does not require any special hardware or secure kernel support and imposes little performance impact to the application, which makes it practical for largescale cloud systems.
<table>
<thead>
<tr>
<th>ETPL CLD-044</th>
<th>Privacy-Preserving Enhanced Collaborative Tagging</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abstract: Collaborative tagging is one of the most popular services available online, and it allows end user to loosely classify either online or offline resources based on their feedback, expressed in the form of free-text labels (i.e., tags). Although tags are not per se sensitive information, the wide use of collaborative tagging services increases the risk of cross referencing, thereby seriously compromising user privacy. In this paper, we make a first contribution in this direction by showing how a specific privacy-enhancing technology, namely tag suppression, can be used to protect end-user privacy. Moreover, we analyze how our approach can affect the effectiveness of a policy-based collaborative tagging system which supports enhanced Web access functionalities, like content filtering and discovery, based on preferences specified by end users.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ETPL CLD-045</th>
<th>A UCONabc Resilient Authorization Evaluation for Cloud Computing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abstract: The Business-driven access control used in cloud computing is not well suited for tracking fine-grained user service consumption. UCONABC applies continuous authorization reevaluation, which requires usage accounting that enables fine-grained access control for cloud computing. However, it was not designed to work in distributed and dynamic authorization environments like those required in cloud computing. During a continuous (periodical) reevaluation an authorization exception condition may occur. This proposal aims to provide resilience to the UCONabc continuous authorization reevaluation, by dealing with individual exception conditions while maintaining a suitable access control in the cloud environment. The experiments made with a proof-of-concept prototype show a set of measurements for an application scenario (e-commerce) and allows for the identification of exception conditions in the authorization reevaluation.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ETPL CLD-046</th>
<th>Decentralized Access Control with Anonymous Authentication for Securing Data in Clouds</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abstract: In this paper, we propose a new privacy preserving authenticated access control scheme for securing data in clouds. In the proposed scheme, the cloud verifies the authenticity of the user without knowing the user's identity before storing information. Our scheme also has the added feature of access control in which only valid users are able to decrypt the stored information. The scheme prevents replay attacks and supports creation, modification, and reading data stored in the cloud. Moreover, our authentication and access control scheme is decentralized and robust, unlike other access control schemes designed for clouds which are centralized. The communication, computation, and storage overheads are comparable to centralized approaches.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ETPL CLD-047</th>
<th>Privacy Preserving Back-Propagation Neural Network Learning Made Practical with Cloud Computing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abstract: To improve the accuracy of learning result, in practice multiple parties may collaborate through conducting joint Back-propagation neural network learning on the union of their respective data sets. During this process no party wants to disclose her/his private data to others. Existing schemes supporting this kind of collaborative learning are either limited in the way of data partition or just consider two parties. There lacks a solution that allows two or more parties, each with an arbitrarily partitioned data set,</td>
<td></td>
</tr>
</tbody>
</table>
to collaboratively conduct the learning. This paper solves this open problem by utilizing the power of cloud computing. In our proposed scheme, each party encrypts his/her private data locally and uploads the ciphertexts into the cloud. The cloud then executes most of the operations pertaining to the learning algorithms over ciphertexts without knowing the original private data. By securely offloading the expensive operations to the cloud, we keep the computation and communication costs on each party minimal and independent to the number of participants. To support flexible operations over ciphertexts, we adopt and tailor the BGN 'doubly homomorphic' encryption algorithm for the multi-party setting. Numerical analysis and experiments on commodity cloud show that our scheme is secure, efficient and accurate.

**ETPL CLD-048**  
**Privacy Preserving Delegated Access Control in Public Clouds**  
Abstract: Current approaches to enforce fine-grained access control on confidential data hosted in the cloud are based on fine-grained encryption of the data. Under such approaches, data owners are in charge of encrypting the data before uploading them on the cloud and re-encrypting the data whenever user credentials change. Data owners thus incur high communication and computation costs. A better approach should delegate the enforcement of fine-grained access control to the cloud, so to minimize the overhead at the data owners, while assuring data confidentiality from the cloud. We propose an approach, based on two layers of encryption, that addresses such requirement. Under our approach, the data owner performs a coarse-grained encryption, whereas the cloud performs a fine-grained encryption on top of the owner encrypted data. A challenging issue is how to decompose access control policies (ACPs) such that the two layer encryption can be performed. We show that this problem is NP-complete and propose novel optimization algorithms. We utilize an efficient group key management scheme that supports expressive ACPs. Our system assures the confidentiality of the data and preserves the privacy of users from the cloud while delegating most of the access control enforcement to the cloud.

**ETPL CLD-049**  
**Cloud video as a Service [VaaS] with storage, streaming, security and Quality of service: Approaches and directions**  
Video as a Service (VaaS) is the cloud service that is gaining momentum in the modern world. With a lot of online web service providers shifting their products to video based services, for enhancing their business, VaaS will take a vital part in the developing cloud computing scenario. Video Streaming depends on storage, Streaming protocols and variations, Security and Quality of Service. A review of the analogies like storage, streaming protocols and variations, security and quality of service has been made in this paper. Also we have arrived at a perception of which technology may be suitable for cloud video as a service scheme. Finally we analyze the future direction.

**ETPL CLD-050**  
**Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing**  
Cloud computing is the apt technology for the decade. It allows user to store large amount of data in cloud storage and use as and when required, from any part of the world, via any terminal equipment. Since cloud computing is rest on internet, security issues like privacy, data security, confidentiality, and authentication is encountered. In order to get rid of the same, a variety of encryption algorithms and mechanisms are used. Many researchers choose the best they found and use it in different combination to provide security to the data in cloud. On the similar terms, we have chosen to make use of a combination
of authentication technique and key exchange algorithm blended with an encryption algorithm. This combination is referred to as "Three way mechanism" because it ensures all the three protection scheme of authentication, data security and verification, at the same time. In this paper, we have proposed to make use of digital signature and Diffie Hellman key exchange blended with (AES) Advanced Encryption Standard encryption algorithm to protect confidentiality of data stored in cloud. Even if the key in transmission is hacked, the facility of Diffie Hellman key exchange render it useless, since key in transit is of no use without user's private key, which is confined only to the legitimate user. This proposed architecture of three way mechanism makes it tough for hackers to crack the security system, thereby protecting data stored in cloud.

<table>
<thead>
<tr>
<th>ETPL</th>
<th>A Trust Based Approach for Increasing Security in Cloud Computing Infrastructure</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLD-051</td>
<td>Users of cloud computing do not have currently appropriate tools for their verification of confidentiality, privacy policy, computing accuracy, and data integrity. To deal with this problem, a new approach called Trusted Cloud Computing Infrastructure is proposed inspired by Trusted Cloud Computing Platform. Through presenting a User Trusted Entity (UTE) the proposed approach is supposed to make cloud computing infrastructures reliable in order to enable infrastructure service developers to provide a closed execution environment. One advantage of the proposed UTE is that managers of Infrastructure as a Service (IaaS) systems have no privilege within UTE. Therefore cloud computing managers cannot interfere in Trusted Coordinator functionality. It has been assumed UTE should be kept by a third agent without any incentives to collude with IaaS services and highly trusted to ensure confidential execution of guest virtual machines. In addition, UTE allows users to authenticate IaaS server and determine the security of cloud service before startup of virtual machine</td>
</tr>
</tbody>
</table>