Cloud Computing

1. Attribute Based Encryption with Privacy Preserving In Clouds

Abstract

Security and privacy are very important issues in cloud computing. In existing system access control in clouds are centralize d in nature. The scheme uses a symmetric key approach and does not support authentication. Symmetric key algorithm uses same key for both encryption and decryption. The authors take a centralized approach where a single key distribution center (KDC) distributes secret keys and attributes to all users. A new decentralized access control scheme for secure data storage in clouds that supports anonymous authentication. The validity of the user who stores the data is also verified. The proposed scheme is resilient to replay attacks. In this scheme using Secure Hash algorithm for authentication purpose, SHA is the one of several cryptographic hash functions, most often used to verify that a file has been unaltered. The Pailliercryptosystem is a probabilistic asymmetric algorithm for public key cryptography. Pailier algorithm use for Creation of access policy, file accessing and file restoring process.

2. 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 authorization 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 authorization. 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 approaches presented using both analytical evaluation of the overheads and simulations to guide the decision makers to which approach to use.

3. Building Confidential and Efficient Query Services in the Cloud with RASP Data Perturbation

Abstract

With the wide deployment of public cloud computing infrastructures, 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. On the other hand, a secured query service should still provide efficient query processing and significantly reduce the in-house workload to fully realize the benefits of cloud computing. We propose the RASP data perturbation method to provide secure and efficient 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 indexing techniques to be applied to speedup range query processing. The kNN-R algorithm is designed to work with the RASP range query algorithm to process the kNN queries. We have carefully analyzed the attacks on data and queries under a precisely defined threat model and realistic security assumptions. Extensive experiments have been conducted to show the advantages of this approach on efficiency and security.

4. Consistency as a Service: Auditing Cloud Consistency

Abstract

Cloud storage services have become commercially popular due to their overwhelming advantages. To provide ubiquitous always-on access, a cloud service provider (CSP) maintains multiple replicas for each piece of data on geographically distributed servers. A key problem of using the replication technique in clouds is that it is very expensive to achieve strong consistency on a worldwide scale. In this paper, we first present a novel consistency as a service (CaaS) model, which consists of a large data cloud and multiple small audit clouds. In the CaaS model, a data cloud is maintained by a CSP, and a group of users that constitute an audit cloud can verify whether the data cloud provides the promised level of consistency or not. We propose a two-level auditing architecture, which only requires a loosely synchronized clock in the audit cloud. Then, we design algorithms to quantify the severity of violations with two metrics: the commonality of violations, and the staleness of the value of a read. Finally, we devise a heuristic auditing strategy (HAS) to reveal as many violations as possible. Extensive experiments were performed using a combination of simulations and a real cloud deployment to validate HAS.

5. Decentralized Access Control Of Data Stored In Cloud Using Key Policy Attribute Based Encryption

Abstract

Cloud computing is a rising computing standard in which assets of the computing framework are given as a service over the Internet. As guaranteeing as it may be, this standard additionally delivers a lot of people new challenges for data security and access control when clients outsource sensitive data for offering on cloud servers, which are not inside the same trusted dominion as data possessors. In any case, in completing thus, these results unavoidably present a substantial processing overhead on the data possessor for key distribution and data administration when finegrained data access control is in demand, and subsequently don't scale well. The issue of at the same time accomplishing fine-grainedness, scalability, and data confidentiality of access control really still remains uncertain. This paper addresses this open issue by, on one hand, characterizing and implementing access policies based on data qualities, and, then again, permitting the data owner to representative the majority of the calculation undertakings included in fine-grained data access control to un-trusted cloud servers without unveiling the underlying data substance. We accomplish this goal by exploiting and combining techniques of decentralized key policy Attribute Based Encryption (KP-ABE) . Extensive investigation shows that the proposed approach is highly efficient and secure.

6. 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.

7. 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 finetuned 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.

8. Identity-Based Distributed Provable Data Possession in Multi-Cloud Storage

Abstract

Remote data integrity checking is of crucial importance in cloud storage. It can make the clients verify whether their outsourced data is kept intact without downloading the whole data. In some application scenarios, the clients have to store their data on multi-cloud servers. At the same time, the integrity checking protocol must be efficient in order to save the verifier's cost. From the two points, we propose a novel remote data integrity checking model: ID-DPDP (identity-based distributed provable data possession) in multi-cloud storage. Theformal system model and security model are given. Based onthe bilinear pairings, a concrete ID-DPDP protocol is designed.The proposed ID-DPDP protocol is provably secure under thehardness assumption of the standard CDH (computational DiffieHellman) problem. In addition to the structural advantage ofelimination of certificate management, our ID-DPDP protocol isalso efficient and flexible. Based on the client's authorization,the proposed ID-DPDP protocol can realize private verification,delegated verification and public verification.

9. Privacy-Preserving Multi-keyword Ranked Search over Encrypted Cloud Data

Abstract

With the advent of cloud computing, data owners are motivated to outsource their complex data management systems from local sites to the commercial public cloud for great Flexibility and economic savings. But for protecting data privacy, sensitive data has to be encrypted before outsourcing, which obsoletes traditional data utilization based on plaintext keyword search. Thus, enabling an encrypted cloud data search service is of paramount importance. Considering the large number of data users and documents in the cloud, it is necessary to allow multiple keywords in the search request and return documents in the orderof their relevance to these keywords. Related works on searchable encryption focus on single keyword search or Boolean keyword search, and rarely sort the search results. In this paper, for the first time, we define and solve the challenging problem of privacypreserving multi-keyword ranked search over encrypted cloud data (MRSE). We establish a set of strict privacy requirements for such a secure cloud data utilization system. Among various multikeyword semantics, we choose the efficient similarity measure of “coordinate matching”, i.e., as many matches as possible, to capture the relevance of data documents to the search query. Wefurther use “inner product similarity” to quantitatively evaluate such similarity measure. We first propose a basic idea for the MRSE based on secure inner product computation, and then givetwo significantly improved MRSE schemes to achieve various stringent privacy requirements in two different threat models. Thorough analysis investigating privacy and efficiency guaranteesof proposed schemes is given. Experiments on the real-world dataset further show proposed schemes indeed introduce low overhead on computation and communication.

Mobile Computing

1. Cloud-Assisted Mobile-Access of Health Data With Privacy and Auditability

Abstract

Motivated by the privacy issues, curbing the adoption of electronic healthcare systems and the wild success of cloud service models, we propose to build privacy into mobile healthcare systems with the help of the private cloud. Our system offers salient features including efficient key management, privacy-preserving data storage, and retrieval, especially for retrieval at emergencies, and auditability for misusing health data. Specifically, we propose to integrate key management from pseudo random number generator for unlinkability, a secure indexing method for privacy preserving keyword search which hides both search and access patterns based on redundancy, and integrate the concept of attribute based encryption with threshold signing for providing role-based access control with auditability to prevent potential misbehavior, in both normal and emergency cases.

2. Efficient Authentication for Mobile and Pervasive Computing

Abstract

With today's technology, many applications rely on the existence of small devices that can exchange information and form communication networks. In a significant portion of such applications, the confidentiality and integrity of the communicated messages are of particular interest. In this work, we propose two novel techniques for authenticating short encrypted messages that are directed to meet the requirements of mobile and pervasive applications. By taking advantage of the fact that the message to be authenticated must also be encrypted, we propose provably secure authentication codes that are more efficient than any message authentication code in the literature. The key idea behind the proposed techniques is to utilize the security that the encryption algorithm can provide to design more efficient authentication mechanisms, as opposed to using standalone authentication primitives.

3. Preserving Location Privacy in Geo-Social Applications

Abstract

Using geo-social applications, such as FourSquare, millions of people interact with their surroundings through their friends and their recommendations. Without adequate privacy protection, however, these systems can be easily misused, e.g., to track users or target them for home invasion. In this paper, we introduce LocX a novel alternative that provides significantly-improved location privacy without adding uncertainty into query results or relying on strong assumptions about server security. Our key insight is to apply secure user-specific, distance-preserving Coordinate transformations to all location data shared with the server. The friends of a user share this user's secrets so they can apply the same transformation. This allows all location queries to be evaluated correctly by the server, but our privacy mechanisms guarantee that servers are unable to see or infer the actual location data from the transformed data or from the data access. We show that LocX provides privacy even against a powerful adversary model, and we use prototype measurements to show that it provides privacy with very little performance overhead, making it suitable for today's mobile devices.

4. Privacy-Preserving Optimal Meeting Location Determination on Mobile Devices

Abstract

Equipped with state-of-the-art smartphones and mobile devices, today's highly interconnected urban population is increasingly dependent on these gadgets to organize and plan their daily lives. These applications often rely on current (or preferred) locations of individual users or a group of users to provide the desired service, which jeopardizes their privacy; users do not necessarily want to reveal their current (or preferred) locations to the service provider or to other, possibly untrusted, users. In this paper, we propose privacy-preserving algorithms for determining an optimal meeting location for a group of users. We perform a thorough privacy evaluation by formally quantifying privacy-loss of the proposed approaches. In order to study the performance of our algorithms in a real deployment, we implement and test their execution efficiency on Nokia smartphones. By means of a targeted user-study, we attempt to get an insight into the privacy-awareness of users in location based services and the usability of the proposed solutions.

5. Leveraging Social Networks for P2P Content-Based File Sharing in Disconnected MANETs

Abstract

Current peer-to-peer (P2P) file sharing methods in mobile ad hoc networks (MANETs) can be classified into three groups: flooding-based, advertisement-based, and social contact-based. The first two groups of methods can easily have high overhead and low scalability. They are mainly developed for connected MANETs, in which end-to-end connectivity among nodes is ensured. The third group of methods adapts to the opportunistic nature of disconnected MANETs but fails to consider the social interests (i.e., contents) of mobile nodes, which can be exploited to improve the file searching efficiency. In this paper, we propose a P2P content based file sharing system, namely SPOON, for disconnected MANETs.

The system uses an interest extraction algorithm to derive a node's interests from its files for content-based file searching. For efficient file searching, SPOON groups common-interest nodes that frequently meet with each other as communities. It takes advantage of node mobility by designating stable nodes, which have the most frequent contact with community members, as community coordinators for intracommunity searching, and highly mobile nodes that visit other communities frequently as community ambassadors for intercommunity searching. An interest-oriented file searching scheme is proposed for high file searching efficiency. Additional strategies for file prefetching, querying-completion, and loop prevention, and node churn consideration are discussed to further enhance the file searching efficiency. We first tested our system on the GENI Orbit testbed with a real trace and then conducted event-driven experiment with two real traces and NS2 simulation with simulated disconnected and connected MANET scenarios. The test results show that our system significantly lowers transmission cost and improves file searching success rate compared to current methods.

Data Mining

1. Anomaly Detection on User Browsing Behaviors Using Hidden Semi-Markov Model

Abstract

CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) is widespread security on the World Wide Web to prevent Application layer DDOS attacks and abusing online services. Generating of CAPTCHA statically to WebPages in the website might annoy users and introduce additional service delays for legitimate users."Puzzle" also has the effect of denying web crawlers access to the site. That causes denying the search engines indexing the content of the websites. In this paper, we introduce a new scheme to achieve early attack detection and countering the attack by generating CAPTCHA dynamically for abnormal HTTP requests of the website, on a popular event generation in the corresponding WebPages. A Hidden semi-Markov model used to describe the browsing behaviors of different users. A novel P-algorithm is introduced for serving the CAPTCHA to attacker to a specific WebPages, based on entropy of the users' HTTP request rate, page viewing time, Page request sequence. If users are requesting for service from proxy servers, any user fall in to the deviated behavior category we generate CAPTCHA dynamically instead of dropping all the requests from behind the proxy server.

2. Attribute Based Encryption with Privacy Preserving In Clouds

Abstract

Security and privacy are very important issues in cloud computing. In existing system access control in clouds are centralized in nature. The scheme uses a symmetric key approach and does not support authentication. Symmetric key algorithm uses same key for both encryption and decryption. The authors take a centralized approach where a single key distribution center (KDC) distributes secret keys and attributes to all users. A new decentralized access *control* scheme for secure data storage in clouds that supports anonymous authentication. The validity of the user who stores the data is also verified. The proposed scheme is resilient to replay attacks. In this scheme using Secure Hash algorithm for authentication purpose. SHA is the one of several cryptographic hash functions, most often used to verify that a file has been unaltered. The Paillier crypto system is a probabilistic asymmetric algorithm for public key cryptography. Pailier algorithm use for Creation of access policy, file accessing and file restoring process.

3. 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 authorization 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 authorization. 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 approaches presented using both analytical evaluation of the overheads and simulations to guide the decision makers to which approach to use.

4. Building Confidential and Efficient Query Services in the Cloud with RASP Data Perturbation

Abstract

With the wide deployment of public cloud computing infrastructures, 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. On the other hand, a secured query service should still provide efficient query processing and significantly reduce the in-

house workload to fully realize the benefits of cloud computing. We propose the RASP data perturbation method to provide secure and efficient range query and kNN query services for protected data in the cloud. The RASP data perturbation method combines orderpreserving encryption, dimensionality expansion, random noise injection, and random projection, to provide strong resilience to attacks on the perturbed data and queries. It also preserves ultidimensional ranges, which allows existing indexing techniques to be applied to speedup range query processing. The kNN-R algorithm is designed to work with the RASP range query algorithm to process the kNN queries. We have carefully analyzed the attacks on data and queries under a precisely defined threat model and realistic security assumptions. Extensive experiments have been conducted to show the advantages of this approach on efficiency and security.

5. Dealing With Concept Drifts in Process Mining

Abstract

Although most business processes change over time, contem-porary process mining techniques tend to analyze these processes as if they are in steady-state. Processes may change suddenly or gradually. The drift may be periodic (e.g. due to seasonal in_uences) or one-of-a-kind (e.g., the e_ects of new legislation). For process management it is crucial to discover and understand such concept drifts in processes. In this paper, we present a case study of analyzing concept drifts in three di_erent processes within a large Dutch municipality.

6. Decentralized Access Control Of Data Stored In Cloud Using Key Policy Attribute Based Encryption

Abstract

Cloud computing is a rising computing standard in which assets of the computing framework are given as a service over the Internet. As guaranteeing as it may be, this standard additionally delivers a lot of people new challenges for data security and access control when clients outsource sensitive data for offering on cloud servers, which are not inside the same trusted dominion as data possessors. In any case, in completing thus, these results unavoidably present a substantial processing overhead on the data possessor for key distribution and data administration when fine-grained data access control is in demand, and subsequently don't scale well. The issue of at the same time accomplishing fine-grandness, scalability, and data confidentiality of access control really still remains uncertain. This paper addresses this open issue by, on one hand, characterizing and implementing access policies based on data qualities, and, then again, permitting the data owner to representative the majority of the calculation undertakings included in fine-grained data access control to un-trusted cloud servers without unveiling the underlying data substance. We accomplish this goal by exploiting and combining techniques of decentralized key policy Attribute Based Encryption (KP-ABE) . Extensive investigation shows that the proposed approach is highly efficient and secure.

7. Discovering Emerging Topics in Social Streams via Link-Anomaly Detection

Abstract

Detection of emerging topics is now receiving renewed interest motivated by the rapid growth of social networks.Conventional-term-frequency-based approaches may not be appropriate in this context, because the information exchanged in socialnetwork posts include not only text but also images, URLs, and videos. We focus on emergence of topics signaled by social aspects of theses networks. Specifically, we focus on mentions of users—links between users that are generated dynamically (intentionally or unintentionally) through replies, mentions, and retweets. We propose a probability model of the mentioning behavior of a social network user, and propose to detect the emergence of a new topic from the anomalies measured through the model. Aggregating anomaly scores from hundreds of users, we show that we can detect emerging topics only based on the reply/mention relationships in social-network posts. We demonstrate our technique in several real data sets we gathered from Twitter. The experiments show that the proposed mention-anomaly-based approaches can detect new topics at least as early as text-anomaly-based approaches, and in some cases much earlier when the topic is poorly identified by the textual contents in posts.

8. Keyword Query Routing

Abstract

Keyword search is an intuitive paradigm for searching linked data sources on the web. We propose to route keywords onlyto relevant sources to reduce the high cost of processing keyword search queries over all sources. We propose a novel method for computingtop-k routing plans based on their potentials to contain results for a given keyword query. We employ akeyword-elementrelationshipsummary that compactly represents relationships between keywords and the data elements mentioning them. Amultilevelscoring mechanismis proposed for computing the relevance of routing plans based on scores at the level of keywords, data elements,element sets, and subgraphs that connect these elements. Experiments carried out using 150 publicly available sources on the webshowed that valid plans (precision@1 of 0.92) that are highly relevant (mean reciprocal rank of 0.89) can be computed in 1 second onaverage on a single PC. Further, we show routing greatly helps to improve the performance of keyword search, without compromisingits result quality.

9. Privacy-Preserving Multi-keyword Ranked Search Over Encrypted Cloud Data

Abstract

with the advent of cloud computing, data owners are motivated to outsource their complex data management systems from local sites to the commercial public cloud for great flexibility and economic savings. But for protecting data privacy, sensitive data has to be encrypted before outsourcing, which obsoletes traditional data utilization based on plaintext keyword search. Thus, enabling an encrypted cloud data search service is of paramount importance. Considering the large number of data users and documents in the cloud, it is necessary to allow multiple keywords in the search request and return documents in the order of their relevance to these keywords. Related works on searchable encryption focus on single keyword search or Boolean keyword search, and rarely sort the search results. In this paper, for the first time, we define and solve the challenging problem of privacy preserving multi-keyword ranked search over encrypted cloud data (MRSE).We establish a set of strict privacy requirements for such a secure cloud data utilization system. Among various multi keyword semantics, we choose the efficient similarity measure of “coordinate matching”, i.e., as many matches as possible, to capture the relevance of data documents to the search query. We further use “inner product similarity” to quantitatively evaluate such similarity measure. We first propose a basic idea for the MRSE based on secure inner product computation, and then give two significantly improved MRSE schemes to achieve various stringent privacy requirements in two different threat models. Thorough analysis investigating privacy and efficiency guarantees of proposed schemes is given. Experiments on the real-world dataset further show proposed schemes indeed introduce low overhead on computation and communication.

10. Supporting Privacy Protection in Personalized Web Search

Abstract

Personalized web search (PWS) has demonstrated its effectiveness in improving the quality of various search services on the Internet. However, evidences show that users' reluctance to disclose their private information during search has become a major barrier for the wide proliferation of PWS. We study privacy protection in PWS applications that model user preferences as hierarchical user profiles. We propose a PWS framework called UPS that can adaptively generalize profiles by queries while respecting userspecified privacy requirements. Our runtime generalization aims at striking a balance between two predictive metrics that evaluate the utility of personalization and the privacy risk of exposing the generalized profile. We present two greedy algorithms, namely GreedyDPand GreedyIL, for runtimegeneralization. We also provide an online prediction mechanism for deciding whether personalizing a query is beneficial. Extensive experiments demonstrate the effectiveness of our framework. The experimental results also reveal that GreedyIL significantly outperforms GreedyDP in terms of efficiency.

11. Web Image Re-Ranking Using Query-Specific Semantic Signatures

Abstract

Image re-ranking, as an effective way to improve the results of web-based image search, has been adopted by current commercial search engines. Given a query keyword, pools of images are first retrieved by the search engine based on textual information. By asking the user to select a query image from the pool, the remaining images are re-ranked based on their visual similarities with the query image. A major challenge is that the similarities of visual features do not well correlate with images' semantic meanings which interpret users' search intention. On the other hand, learning a universal visual semantic space to characterize highly A diverse image from the web is difficult and inefficient. In this paper, we propose a novel image re-ranking framework, which automatically offline learns different visual semantic spaces for different query keywords through keyword expansions. The visual features of images are projected into their related visual semantic spaces to get semantic signatures. At the online stage, images are re-ranked by comparing their semantic signatures obtained from the visual semantic space specified by the query keyword. The new approach significantly improves both the accuracy and efficiency of image re-ranking. The original visual features of thousands of dimensions can be projected to the semantic signatures as short as 25 dimensions. Experimental results show that 20% ⍰ 35% relative improvement has been achieved on re-ranking precisions compared with the state of-the-art methods.

SECURE COMPUTING

1. Hop-by-Hop Message Authentication and Source Privacy in Wireless Sensor Networks

Abstract:

Message authentication is one of the most effective ways to thwart unauthorized and corrupted messages from being forwarded in wireless sensor networks (WSNs). For this reason, many message authentication schemes have been developed, based on either symmetric-key cryptosystems or public-key cryptosystems. Most of them, however, have the limitations of high computational and communication overhead in addition to lack of scalability and resilience to node compromise attacks. To address these issues, a polynomial-based scheme was recently introduced. However, this scheme and its extensions all have the weakness of a built-in threshold determined by the degree of the polynomial: when the number of messages transmitted is larger than this threshold, the adversary can fully recover the polynomial. In this paper, we propose a scalable authentication scheme based on elliptic curve cryptography (ECC). While enabling intermediate nodes authentication, our proposed scheme allows any node to transmit an unlimited number of messages without suffering the threshold problem. In addition, our scheme can also provide message source privacy. Both theoretical analysis and simulation results demonstrate that our proposed scheme is more efficient than the polynomial-based approach in terms of computational and communication overhead under comparable security levels while providing message source privacy.

2. Human Effects of Enhanced Privacy Management Models

ABSTRACT:

We enhance existing and introduce new social network privacy management models and we measure their human effects. First, we introduce a mechanism using proven clustering techniques that assists users in grouping their friends for traditional group based policy management approaches. We found measurable agreement between clusters and user-defined relationship groups. Second, we introduce a new privacy management model that leverages users' memory and opinion of their friends (called example friends) to set policies for other similar friends. Finally, we explore different techniques that aid users in selecting example friends. We found that by associating policy temples with example friends (versus group labels), users author policies more efficiently and have improved perceptions over traditional group-based policy management approaches. In addition, our results show that privacy management models can be further enhanced by utilizing user privacy sentiment for mass customization. By detecting user privacy sentiment (i.e., an unconcerned user, a pragmatist or a fundamentalist), privacy management models can be automatically tailored specific to the privacy sentiment and needs of the user.

3. Secure Ordered Bucketization

ABSTRACT:

This study examines the ordered bucketization (OB) as a cryptographic object. In OB, plaintext space is divided into p disjoint buckets, numbered from 1 to p, based on the order of the ranges that they cover. OB is quite useful in that a range query can be performed over encrypted data without the need to decrypt by attaching a bucket number to each ciphertext. Unfortunately, no research has been carried out on the security of OB in a cryptographic sense. This paper defines an encryption scheme with OB (EOB) and suggests a new security model for EOB, IND-OCPA-P, which assumes an adversary has reasonable power. Previous constructions proposed for efficient range queries [5], [6], [14] were not secure in this model. Finally, an OB construction, in which the EOB implementation is secure on the IND-OCPA-P model, is proposed. In the proposed OB, p-1 points are selected on the uniform distribution in the plaintext-space and the plaintext-space is divided based on the selected points. A bucket number is assigned to each divided range in ascending range order. With regard to the efficiency of a range query, the proposed OB guarantees reasonably good efficiency on range queries by showing that the distribution of a bucket size is not skewed.

4. Tradeoff between Reliability and Security in Multiple Access Relay Networks under Falsified Data Injection Attack

Abstract:

We consider a multiple access relay network where multiple sources send independent data to a single destination through multiple relays, which may inject falsified data into the network. To detect the malicious relays and discard (erase) data from them, tracing bits are embedded in the information data at each source node. In addition, parity bits are added to correct the errors caused by fading and noise. When the total amount of redundancy, tracing bits plus parity bits, is fixed, an increase in parity bits to increase the reliability requires a decrease in tracing bits, which leads to a less accurate detection of malicious behavior of relays, and vice versa. We investigate the tradeoff between the tracing bits and the parity bits in minimizing the probability of decoding error and maximizing the throughput in multisource, multi relay networks under falsified data injection attacks. The energy and throughput gains provided by the optimal allocation of redundancy and the tradeoff between reliability and security are analyzed.

PARALLEL AND DISTRIBUTED SYSTEMS

1. **A Probabilistic Misbehavior Detection Scheme toward Efficient Trust Establishment in Delay-Tolerant Networks**

Abstract

Malicious and selfish behaviors represent a serious threat against routing in delay/disruption tolerant networks (DTNs). Due to the unique network characteristics, designing a misbehavior detection scheme in DTN is regarded as a great challenge. In this paper, we propose iTrust, a probabilistic misbehavior detection scheme, for secure DTN routing toward efficient trust establishment. The basic idea of iTrust is introducing a periodically available Trusted Authority (TA) to judge the node's behavior based on the collected routing evidences and probabilistically checking. We model iTrust as the inspection game and use game theoretical analysis to demonstrate that, by setting an appropriate investigation probability, TA could ensure the security of DTN routing at a reduced cost. To further improve the efficiency of the proposed scheme, we correlate detection probability with a node's reputation, which allows a dynamic detection probability determined by the trust of the users. The extensive analysis and simulation results demonstrate the effectiveness and efficiency of the proposed scheme.

2. An Error-Minimizing Framework for Localizing Jammers in Wireless Networks

Abstract

Jammers can severely disrupt the communications in wireless networks, and jammers' position information allows the defender to actively eliminate the jamming attacks. Thus, in this paper, we aim to design a framework that can localize one or multiple jammers with a high accuracy. Most of existing jammer-localization schemes utilize indirect measurements (e.g., hearing ranges) affected by jamming attacks, which makes it difficult to localize jammers accurately. Instead, we exploit a direct measurement—the strength of jamming signals (JSS). Estimating JSS is challenging as jamming signals may be embedded in other signals. As such, we devise an estimation scheme based on ambient noise floor and validate it with real-world experiments. To further reduce estimation errors, we define an evaluation feedback metric to quantify the estimation errors and formulate jammer localization as a nonlinear optimization problem, whose global optimal solution is close to jammers’ true positions. We explore several heuristic search algorithms for approaching the global optimal solution, and our simulation results show that our error-minimizing-based framework achieves better performance than the existing schemes. In addition, our error-minimizing framework can utilize indirect measurements to obtain a better location estimation compared with prior work.

3. Efficient Data Query in Intermittently-Connected Mobile Ad Hoc Social Networks

Abstract

This work addresses the problem of how to enable efficient data query in a Mobile Ad-hoc SOcial Network (MASON), formed by mobile users who share similar interests and connect with one another by exploiting Bluetooth and/or WiFi connections. The data query in MASONs faces several unique challenges including opportunistic link connectivity, autonomous computing and storage, and unknown or inaccurate data providers. Our goal is to determine an optimal transmission strategy that supports the desired query rate within a delay budget and at the same time minimizes the total communication cost. To this end, we propose a centralized optimization model that offers useful theoretic insights and develop a distributed data query protocol for practical applications. To demonstrate the feasibility and efficiency of the proposed scheme and to gain useful empirical insights, we carry out a testbed experiment by using 25 off-the-shelf Dell Streak tablets for a period of 15 days. Moreover, extensive simulations are carried out to learn the performance trend under various network settings, which are not practical to build and evaluate in laboratories.

4. A System for Denial-of-Service Attack Detection Based on Multivariate Correlation Analysis

Abstract

Interconnected systems, such as Web servers, database servers, cloud computing servers etc, are now under threads from network attackers. As one of most common and aggressive means, Denial-of-Service (DoS) attacks cause serious impact on these computing systems. In this paper, we present a DoS attack detection system that uses Multivariate Correlation Analysis (MCA) for accurate network traffic characterization by extracting the geometrical correlations between network traffic features. Our MCA-based DoS attack detection system employs the principle of anomaly-based detection in attack recognition. This makes our solution capable of detecting known and unknown DoS attacks effectively by learning the patterns of legitimate network traffic only. Furthermore, a triangle-area-based technique is proposed to enhance and to speed up the process of MCA. The effectiveness of our proposed detection system is evaluated using KDD Cup 99 dataset, and the influences of both non-normalized data and normalized data on the performance of the proposed detection system are examined. The results show that our system outperforms two other previously developed state-of-the-art approaches in terms of detection accuracy.

5. A Two-stage Deanonymization Attack Against Anonymized Social Networks

Abstract

Digital traces left by users of online social networking services, even after anonymization, are susceptible to privacy breaches. This is exacerbated by the increasing overlap in user-bases among various services. To alert fellow researchers in both the academia and the industry to the feasibility of such an attack, we propose an algorithm, Seed-and-Grow, to identify users from an anonymized social graph, based solely on graph structure. The algorithm first

identifies a seed sub-graph, either planted by an attacker or divulged by a collusion of a small group of users, and then grows the seed larger based on the attacker's existing knowledge of the users' social relations. Our work identifies and relaxes implicit assumptions taken by previous works, eliminates arbitrary parameters, and improves identification effectiveness and accuracy. Simulations on real-world collected datasets verify our claim.

6. Securing Broker-Less Publish/Subscribe Systems Using Identity-Based Encryption

Abstract

The provisioning of basic security mechanisms such as authentication and confidentiality is highly challenging in a contentbased publish/subscribe system. Authentication of publishers and subscribers is difficult to achieve due to the loose coupling of publishers and subscribers. Likewise, confidentiality of events and subscriptions conflicts with content-based routing. This paper presents a novel approach to provide confidentiality and authentication in a broker-less content-based publish/subscribe system. The authentication of publishers and subscribers as well as confidentiality of events is ensured, by adapting the pairing-based cryptography mechanisms, to the needs of a publish/subscribe system. Furthermore, an algorithm to cluster subscribers according to their subscriptions preserves a weak notion of subscription confidentiality. In addition to our previous work [23], this paper contributes 1) use of searchable encryption to enable efficient routing of encrypted events, 2) multicredential routing a new event dissemination strategy to strengthen the weak subscription confidentiality, and 3) thorough analysis of different attacks on subscription confidentiality. The overall approach provides fine-grained key management and the cost for encryption, decryption, and routing is in the order of subscribed attributes. Moreover, the evaluations show that providing security is affordable w.r.t. 1) throughput of the proposed cryptographic primitives, and 2) elays incurred during the construction of the publish/subscribe overlay and the event dissemination.

7. Shared Authority Based Privacy-preserving Authentication Protocol in Cloud Computing

Abstract

Cloud computing is emerging as a prevalent data interactive paradigm to realize users' data remotely stored in an online cloud server. Cloud services provide great conveniences for the users to enjoy the on-demand cloud applications without considering the local infrastructure limitations. During the data accessing, different users may be in a collaborative relationship, and thus data sharing becomes significant to achieve productive benefits. The existing security solutions mainly focus on the authentication to realize that a user's privative data cannot be unauthorized accessed, but neglect a subtle privacy issue during a user challenging the cloud server to request other users for data sharing. The challenged access request itself may reveal the user's privacy no matter whether or not it can obtain the data access permissions. In this paper, we propose a shared authority based privacy-preserving authentication protocol (SAPA) to address above privacy issue for cloud storage. In the SAPA, 1) shared access authority is achieved by anonymous access request matching mechanism with security and privacy considerations (e.g., authentication, data anonymity, user privacy, and forward security);

2) attribute based access control is adopted to realize that the user can only access its own data fields;

3) proxy re-encryption is applied by the cloud server to provide data sharing among the multiple users. Meanwhile, universal composability (UC) model is established to prove that the SAPA theoretically has the design correctness. It indicates that the proposed protocol realizingprivacy-preserving data access authority sharing, is attractive for multi-user collaborative cloud applications.

8. Secure and Efficient Data Transmission for Cluster-Based Wireless Sensor Networks

Abstract

Secure data transmission is a critical issue for wireless sensor networks (WSNs). Clustering is an effective and practical way to enhance the system performance of WSNs. In this paper, we study a secure data transmission for cluster-based WSNs (CWSNs), where the clusters are formed dynamically and periodically. We propose two secure and efficient data transmission (SET) protocols for CWSNs, called SET-IBS and SET-IBOOS, by using the identity-based digital signature (IBS) scheme and the identity-based online/offline digital signature (IBOOS) scheme, respectively. In SET-IBS, security relies on the hardness of the Diffie-Hellman problem in the pairing domain. SET-IBOOS further reduces the computational overhead for protocol security, which is crucial for WSNs, while its security relies on the hardness of the discrete logarithm problem. We show the feasibility of the SET-IBS and SET-IBOOS protocols with respect to the security requirements and security analysis against various attacks. The calculations and simulations are provided to illustrate the efficiency of the proposed protocols. The results show that the proposed protocols have better performance than the existing secure protocols for CWSNs, in terms of security overhead and energy consumption.

9. Transmission-Efficient Clustering Method for Wireless Sensor Networks Using Compressive Sensing

Abstract

Compressive sensing (CS) can reduce the number of data transmissions and balance the traffic load throughout networks. However, the total number of transmissions for data collection by using pure CS is still large. The hybrid method of using CS was proposed to reduce the number of transmissions in sensor networks. However, the previous works use the CS method on routing trees. In this paper, we propose a clustering method that uses hybrid CS for sensor networks. The sensor nodes are organized into clusters. Within a cluster, nodes transmit data to cluster head (CH) without using CS. CHs use CS to transmit data to sink. We first propose an analytical model that studies the relationship between the size of clusters and number of transmissions in the hybrid CS method, aiming at finding the optimal size of clusters that can lead to minimum number of transmissions. Then, we propose a centralized clustering algorithm based on the results obtained from the analytical model. Finally, we present a distributed implementation of the clustering method. Extensive simulations confirm that our method can reduce the number of transmissions significantly.