JAVA/J2EE PROJECT ABSTRACTS

(Big Data, Cloud Computing, Networking, Network-Security, Mobile Computing, Wireless Sensor Network, Datamining, Webmining, Artificial Intelligence, Vanet, Ad-Hoc Network)

VIJAYANAGAR

NETWORKING

1. **Implementation of DNA cryptography in cloud computing and using socket programming**
   Cloud computing is the latest technology in the field of distributed computing. It provides various online and on-demand services for data storage, network services, platform services and etc. Many organizations are unenthusiastic to use cloud services due to data security issues as the data resides on the cloud services provider's servers. To address this issue, there have been several approaches applied by various researchers worldwide to strengthen security of the stored data on cloud computing. The Bi-directional DNA Encryption Algorithm (BDEA) is one such data security techniques. However, the existing technique focuses only on the ASCII character set, ignoring the non-English user of the cloud computing. Thus, this proposed work focuses on enhancing the BDEA to use with the Unicode characters

2. **Cost-Effective Authentic and Anonymous Data Sharing with Forward Security**
   Data sharing has never been easier with the advances of cloud computing, and an accurate analysis on the shared data provides an array of benefits to both the society and individuals. Data sharing with a large number of participants must take into account several issues, including efficiency, data integrity and privacy of data owner. Ring signature is a promising candidate to construct an anonymous and authentic data sharing system. It allows a data owner to anonymously authenticate his data which can be put into the cloud for storage or analysis purpose. Yet the costly certificate verification in the traditional public key infrastructure (PKI) setting becomes a bottleneck for this solution to be scalable. Identity-based (ID-based) ring signature, which eliminates the process of certificate verification, can be used instead. In this paper, we further enhance the security of ID-based ring signature by providing forward security: If a secret key of any user has been compromised, all previous generated signatures that include this user still remain valid. This property is especially important to any large scale data sharing system, as it is impossible to ask all data owners to reauthenticate their data even if a secret key of one single user has been compromised. We provide a concrete and efficient instantiation of our scheme, prove its security and provide an implementation to show its practicality.

3. **Dual-Server Public-Key Encryption With Keyword Search for Secure Cloud Storage**
   Searchable encryption is of increasing interest for protecting the data privacy in secure searchable cloud storage. In this paper, we investigate the security of a well-known cryptographic primitive, namely, public key encryption with keyword search (PEKS) which is very useful in many applications of cloud storage. Unfortunately, it has been shown that the traditional PEKS framework suffers from an inherent insecurity called inside keyword guessing attack (KGA) launched by the malicious server. To address this security vulnerability, we propose a new PEKS framework named dual-server PEKS (DS-PEKS). As another main contribution, we define a new variant of the smooth projective hash functions (SPHFs) referred to as linear and homomorphic SPHF (LH-SPHF). We then show a generic construction of secure DS-PEKS from LH-SPHF. To illustrate the feasibility of our new framework, we provide an efficient instantiation of the general framework from a Decision Diffie–Hellman-based LH-SPHF and show that it can achieve the strong security against inside the KGA.

4. **An Effective Re Deployment of Cooperative Network(S) to Transmit in Incremental Clusters Approach**
   Scheduling and broadcasting of data through network tunnels is always a big challenge in closed network topologies. Each and individual tunnel or part of network will be having its own capacity to transmit and receive the packets. Adoptive and open networks are easy to transmit the data

but the challenges will occur in synchronization of data transmission among them. So clustering, tracking, log maintenance of the data transmission among the channels or tunnels and retransmission with respect energy levels and synchronization can be achieved by incremental tracking retransmission (ITR[1]) approach. Energy levels will be monitored by network monitor and assigns scheduling depends on the network capacity of the available methodologies. Here the three methodologies are 1.Memory less channels[2] , 2. Modulated channel[3], 3.Joint and uniform scheduling[4] for data transmission with respect to scheduling. Considerable throughput criteria is framed with incremental flow with our work to end up fair and best accuracy levels. This ITR method is totally unique in open networks. Here open networks means which can adopt with legacy and other adoptive open networks in tunnelling or bridge level transmission. The packet buffering and delivery is always depends on previous cluster or next cluster and chance of losing the packets. So to overcome our work is practically implemented in chunks mechanism. Totally 3 or more chunks will be framed as clusters which acts as incremental growth in transmission with respect to losing of the packets. The central frame work which works as auto deployment methodology to track the tunnels. The loss of frequency is traceable using this frame work and adopts the lost and non lost packets addresses and flushes to next level to fulfil ITR method. The practical implementation depends on asynchronous services to roll back to any level/cluster. The feasible transmission is achieved in incremental level of clusters which will get the log or track information about the data from central frame work.

5. **An adjunct hash neighbor in 4way MANETS to share data efficiently**

To share the data in between neighbor nodes in established or fixed MANET is a big challenge. Always displaced movements MANET nodes are unpredictable with respect to their moving places in case of sharing data. And data sharing is late and sometimes hard in between deferent networks. And also compromised nodes may take advantage to take and hide the data. So to overcome these scenario we propose a new approach called SMN (Smart movement notice), EDT (Efficient data Transfer). And to transfer the data in encoded format we propose a new algorithm ROTA (Rotation orient transfer analog). All these techniques can be used across the MANETs in deferent networks. The data can be shared via non compromised hash technique in ROTA technique. All the techniques are inter related with one approach of data transfer in efficient manner. The neibour nodes displacements are available all the times to all current network nodes and also root or master node. The master node is the key node to transfer the data to other networks in encoded formats. The data can be large and also feasible formats to transfer to legacy networks.

6. **Secure Distributed Deduplication Systems with Improved Reliability**

Data deduplication is a technique for eliminating duplicate copies of data, and has been widely used in cloud storage to reduce storage space and upload bandwidth. However, there is only one copy for each file stored in cloud even if such a file is owned by a huge number of users. As a result, deduplication system improves storage utilization while reducing reliability. Furthermore, the challenge of privacy for sensitive data also arises when they are outsourced by users to cloud. Aiming to address the above security challenges, this paper makes the first attempt to formalize the notion of distributed reliable deduplication system. We propose new distributed deduplication systems with higher reliability in which the data chunks are distributed across multiple cloud servers. The security requirements of data confidentiality and tag consistency are also achieved by introducing a deterministic secret sharing scheme in distributed storage systems, instead of using convergent encryption as in previous deduplication systems. Security analysis

demonstrates that our deduplication systems are secure in terms of the definitions specified in the proposed security model. As a proof of concept, we implement the proposed systems and demonstrate that the incurred overhead is very limited in realistic environments.

7. **Honeywords: Making Password-Cracking Detectable**

We propose a simple method for improving the security of hashed passwords: the maintenance of additional "honey- words" (false passwords) associated with each user's account. An adversary who steals a file of hashed passwords and in- verts the hash function cannot tell if he has found the password or a honeyword. The attempted use of a honeyword for login sets off an alarm. An auxiliary server (the "hon- eychecker") can distinguish the user password from honey- words for the login routine, and will set off an alarm if a honeyword is submitted.

8. **A Secure Group Key Management Scheme for Sensor Networks**

Security is an important issue in sensor networks. Manyapplications in military, distributed information gatheringetc., demand for Secure Group Communication (SGC) insensor networks. The SGC requires common network-widegroup key for confidentiality of control messages and datareports. The group key should be updated when a node iscompromised. In this paper we propose a new key management. scheme for group key computation and distributionwhich is based on tree structure. The proposed scheme minimizesstorage as well as communication and computationcost of end user (i.e., sensor nodes). The complex encryption/decryption operations used to distribute new group keywhenever a node is compromised are replaced by one wayhash functions and simple XOR operations.Keywords: Secure Group Communication, SensorNode, Hash Function, Group Key.

9. **Maximizing P2P File Access Availability in mobile Ad Hoc Networks though Replication for Efficient File Sharing**

File sharing applications in mobile ad hoc networks (MANETs) have attracted more and more attention in recent years. The efficiency of file querying suffers from the distinctive properties of such networks including node mobility and limited communication range and resource. An intuitive method to alleviate this problem is to create file replicas in the network. However, despite the efforts on file replication, no research has focused on the global optimal replica creation with minimum average querying delay. Specifically, current file replication protocols in mobile ad hoc networks have two shortcomings. First, they lack a rule to allocate limited resources to different files in order to minimize the average querying delay. Second, they simply consider storage as available resources for replicas, but neglect the fact that the file holders' frequency of meeting other nodes also plays an important role in determining file availability. Actually, a node that has a higher meeting frequency with others provides higher availability to its files. This becomes even more evident in sparsely distributed MANETs, in which nodes meet disruptively. In this paper, we introduce a new concept of resource for file replication, which considers both node storage and meeting frequency. We theoretically study the influence of resource allocation on the average querying delay and derive a resource allocation rule to minimize the average querying delay. We further propose a distributed file replication protocol to realize the proposed rule. Extensive trace-driven experiments with synthesized traces and real traces show that our protocol can achieve shorter average querying delay at a lower cost than current replication protocols.

10. Privacy-Preserving and Truthful Detection of Packet Dropping Attacks in Wireless Ad Hoc Networks

Link error and malicious packet dropping are two sources for packet losses in multi-hop wireless ad hoc network. In this paper, while observing a sequence of packet losses in the network, we are interested in determining whether the losses are caused by link errors only, or by the combined effect of link errors and malicious drop. We are especially interested in the insider-attack case, whereby malicious nodes that are part of the route exploit their knowledge of the communication context to selectively drop a small amount of packets critical to the network performance. Because the packet dropping rate in this case is comparable to the channel error rate, conventional algorithms that are based on detecting the packet loss rate cannot achieve satisfactory detection accuracy. To improve the detection accuracy, we propose to exploit the correlations between lost packets. Furthermore, to ensure truthful calculation of these correlations, we develop a homomorphic linear authenticator (HLA) based public auditing architecture that allows the detector to verify the truthfulness of the packet loss information reported by nodes. This construction is privacy preserving, collusion proof, and incurs low communication and storage overheads. To reduce the computation overhead of the baseline scheme, a packet-block-based mechanism is also proposed, which allows one to trade detection accuracy for lower computation complexity. Through extensive simulations, we verify that the proposed mechanisms achieve significantly better detection accuracy than conventional methods such as a maximum-likelihood based detection.

11. Routing in Wireless Sensor Network using Fuzzy based Trust Model

Wireless sensor network is a collection of large number of sensor nodes that are deployed in large number to monitor the environment. There is a great technological advancement in wireless sensor network during last few years. Due to low-cost, small-size, nature of Wireless Sensor Networks (WSNs), it allows them to sense the information in various hostile environments (e.g. military surveillance, battlefield). So, to fully achieve the capacity of WSNs, sensor nodes need to cooperate in the collection and must disseminate topology information. These sensor nodes specifically operate in a multihop routing. Sensor network in muiltihop routing faces a variety of risks which is also due to the harsh operating environments. In this paper a fuzzy based approach is introduced which will enhance the routing security and reliability in WSNs.

12. Privacy Preserving Cloud-based Computing Platform (PPCCP) for using Location Based Services

Mobile cloud computing (MCC) is an emerging trend which combines the benefits of cloud computing with the mobile devices. This new technology not only offers tremendous computing power and storage to the mobile devices with limited processing and storage capabilities but also increases the affordability and reliability. Despite providing various benefits, MCC is still in its early stages in providing trust guarantees to a user. Location-Based Services (LBS), on the other hand, are those services which operate on a users location to provide him/her services such as finding nearby restaurants, hospitals, bus terminal and ATMs, to name a few. While a users location is mandatory for LBS to work, it imposes serious threats to the users privacy. In this paper we propose a privacy preserving cloud-based computing architecture for using

location-based services. On one hand, our architecture provides a secure mechanism for using LBS services anonymously while on the other hand it utilizes untrusted but fast and reliable cloud services for its implementation in an efficient and effective manner. Moreover, we provide various attack scenarios and show that how our architecture preserves the privacy of the user and is difficult to compromise.

13. **NICE: Network Intrusion Detection and Countermeasure Selection in Virtual Network Systems**

Cloud security is one of most important issues that has attracted a lot of research and development effort in past few years. Particularly, attackers can explore 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.

14. **EMAP: Expedite Message Authentication Protocol for Vehicular Ad Hoc Networks**

Vehicular ad hoc networks (VANETs) adopt the Public Key Infrastructure (PKI) and Certificate Revocation Lists (CRLs) for their security. In any PKI system, the authentication of a received message is performed by checking if the certificate of the sender is included in the current CRL, and verifying the authenticity of the certificate and signature of the sender. In this paper, we propose an Expedite Message Authentication Protocol (EMAP) for VANETs, which replaces the time-consuming CRL checking process by an efficient revocation checking process. The revocation check process in EMAP uses a keyed Hash Message Authentication Code ðHMACÞ, where the key used in calculating theHMAC is shared only between nonrevoked On-Board Units (OBUs). In addition, EMAP uses a novel probabilistic key distribution, which enables nonrevoked OBUs to securely share and update a secret key. EMAP can significantly decrease the message loss ratio due to the message verification delay compared with the conventional authentication methods employing CRL. By conducting security analysis and performance evaluation,EMAP is demonstrated to be secure and efficient.

15. **Cluster-Based Certificate Revocation with Vindication Capability for Mobile Ad Hoc Networks**
16. **Using Identity and Trust with Key Management for achieving security in Ad hoc Networks**

Communication in Mobile Ad hoc network is done over a shared wireless channel with no Central Authority (CA) to monitor. Responsibility of maintaining the integrity and secrecy of data, nodes in the network are held responsible. To attain the goal of trusted communication in MANET (Mobile Ad hoc Network) lot of approaches using key management has been implemented. This work proposes a composite identity and trust based model (CIDT) which depends on public key, physical identity, and trust of a node which helps in secure data transfer over wireless channels. CIDT is a modified DSR routing protocol for achieving security. Trust Factor of a node along with its key pair and identity is used to authenticate a node in the network. Experience based trust factor (TF) of a node is used to decide the authenticity of a node. A valid certificate is generated for authentic node to carry out the communication in the network. Proposed method works well for self certification scheme of a node in the network.

17. Search Me If You Can: Privacy-preserving Location Query Service

Location-Based Service (LBS) becomes increasingly popular with the dramatic growth of smartphones and social network services (SNS), and its context-rich functionalities attract considerable users. Many LBS providers use users' location information to offer them convenience and useful functions. However, the LBS could greatly breach personal privacy because location itself contains much information. Hence, preserving location privacy while achieving utility from it is still an challenging question now. This paper tackles this non-trivial challenge by designing a suite of novel fine-grained Privacy-preserving Location Query Protocol (PLQP). Our protocol allows different levels of location query on encrypted location information for different users, and it is efficient enough to be applied in mobile platforms.

18. Fast Transmission to Remote Cooperative Groups: A New Key Management Paradigm

The problem of efficiently and securely broadcasting to a remote cooperative group occurs in many newly emerging networks. A major challenge in devising such systems is to overcome the obstacles of the potentially limited communication from the group to the sender, the unavailability of a fully trusted key generation center, and the dynamics of the sender. The existing key management paradigms cannot deal with these challenges effectively. In this paper, we circumvent these obstacles and close this gap by proposing a novel key management paradigm. The new paradigm is a hybrid of traditional broadcast encryption and group key agreement. In such a system, each member maintains a single public/secret key pair. Upon seeing the public keys of the members, a remote sender can securely broadcast to any intended subgroup chosen in an ad hoc way. Following this model, we instantiate a scheme that is proven secure in the standard model. Even if all the nonintended members collude, they cannot extract any useful information from the transmitted messages. After the public group encryption key is extracted, both the computation overhead and the communication cost are independent of the group size. Furthermore, our scheme facilitates simple yet efficient member deletion/addition and flexible rekeying strategies. Its strong security against collusion, its constant overhead, and its implementation friendliness without relying on a fully trusted authority render our protocol a very promising solution to many applications.

19. Back-Pressure-Based Packet-by-Packet Adaptive Routing in Communication Networks

Back-pressure-based adaptive routing algorithms where each packet is routed along a possibly different path have been extensively studied in the literature. However, such algorithms typically

result in poor delay performance and involve high implementation complexity. In this paper, we develop a new adaptive routing algorithm built upon the widely studied back-pressure algorithm. We decouple the routing and scheduling components of the algorithm by designing a probabilistic routing table that is used to route packets to per-destination queues. The scheduling decisions in the case of wireless networks are made using counters called shadow queues. The results are also extended to the case of networks that employ simple forms of network coding. In that case, our algorithm provides a low-complexity solution to optimally exploit the routing-coding tradeoff.

20. AMPLE: An Adaptive Traffic Engineering System Based on Virtual Routing Topologies

Handling traffic dynamics in order to avoid network congestion and subsequent service disruptions is one of the key tasks performed by contemporary network management systems. Given the simple but rigid routing and forwarding functionalities in IP base environments, efficient resource management and control solutions against dynamic traffic conditions is still yet to be obtained. In this article, we introduce AMPLE — an efficient traffic engineering and routing topologies for long term operation through the optimized setting of link weights. Based on these diverse paths, adaptive traffic control performs intelligent traffic splitting across individual routing topologies in reaction to the monitored network dynamics at short timescale. According to our evaluation with real network topologies and traffic traces, the proposed system is able to cope almost optimally with unpredicted traffic dynamics and, as such, it constitutes a new proposal for achieving better quality of service and overall network performance in IP networks. Management system that performs adaptive traffic control by using multiple virtualized routing topologies. The proposed system consists of two complementary components: offline link weight optimization that takes as input the physical network topology and tries to produce maximum routing path diversity across multiple virtual