Key Management Scheme for Secure Channel Establishment in Fog Computing

G.RANI
Assistant Professor
Department of CSE
Teegala Krishna Reddy Engineering College,Hyderabad

AMBATI SRINIVAS GOUD
Department of CSE
Teegala Krishna Reddy Engineering College, Hyderabad
ambatisrinivas2000@gmail.com
ranicse@tkrec.ac.in

NENAVATHU GOPAL
Department of CSE
Teegala Krishna Reddy Engineering College,Hyderabad
nenavathgopal77@gmail.com

DHEERAJ RAO
Department of CSE
Teegala Krishna Reddy Engineering College,Hyderabad
Dheerajrao780@icloud.com

BODA MOHAN KRISHNA GOUD
Department of CSE
Teegala Krishna Reddy Engineering College,Hyderabad
crazymohan2001@gmail.com

Abstract - Fog computing is a promising extension of cloud computing, and enables computing directly at the edge of the network. Due to the decentralized and distributed nature of fog nodes, secure communication channels have to be supported in fog computing, which are generally realized through secure keys. Key management schemes are usually employed to generate, distribute and maintain the secret keys. In this paper, we propose a key management scheme called dynamic contributory broadcast encryption (DConBE) for secure channel establishment in fog computing. It allows a group of fog nodes that want to establish a fog system to negotiate a public encryption key and each node's decryption key in one round without a trusted dealer. Any end user may encrypt messages under the public encryption key with short ciphertexts to any subset of the fog nodes in the system. Only selected fog nodes in the system can decrypt the encrypted messages using their respective decryption key. Our new key management scheme also achieves the properties of fog node dynamics, fully collusion-resistant and stateless.

I. INTRODUCTION

In the past few years, cloud computing has attracted widespread concerns from both commercial circles and academia. It provides flexible and on-demand resources (e.g., storage, computing, networking) to the end users according to their demands at the moment. However, as the fast growth of IoT devices, traditional cloud based methods will be unable to provide adequate services to end users in the near future. Further, for latency-sensitive applications, current cloud computing paradigm can hardly meet their demands for low latency due to limited network bandwidth, long geographic distance between traditional cloud and an end user. In order to guarantee the quality of service (QoS) for above application trends, a new cloud computing architecture has to be developed.

Fog computing is a promising extension of cloud computing, and has been shown to be an effective solution for above issues in traditional cloud. This new architecture enables computing directly at the edge of the network. As fog computing is implemented at the edge of the network, it provides applications that offer better QoS and user experience. In fog computing, fog nodes, e.g., access points, intelligent vehicles, edge routers and cellular base stations, can be distributed geographically and support mobility. End users, fog and cloud are forming a three tier layered network, supporting a series of application scenarios, e.g., intelligent transportation, industrial automation, smart grid, and wireless sensor networks.

II. LITERATURE SURVEY

TITLE : Privacy-Preserving Public Auditing Protocol for Low Performance End Devices in Cloud [1]
AUTHOR : J. Li, L. Zhang, K. Liu, H. Qian, and Z. Dong,
YEAR : 2016

DESCRIPTION

Cloud storage provides tremendous storage resources for both individual and enterprise users. In a cloud storage system, the data owned by a user are no longer possessed locally. Hence, it is not competent to ensure the integrity of the outsourced data using traditional data integrity checking methods. A privacy-preserving public auditing protocol allows a third party auditor to check the integrity of the outsourced data on behalf of the users without violating the privacy of the data. However, existing privacy-preserving public auditing protocols assume that the end devices of users are powerful enough to compute all costly operations in real time when the data to be outsourced are given. In fact, the end devices may also be those with low computation capabilities. In this paper, we propose two lightweight privacy-preserving public auditing protocols. Our protocols are based on online/offline signatures, by which an end device only needs to perform lightweight computations when a file to be outsourced is available. Besides, our proposals support batch auditing and data dynamics. Experiments show that our protocols are hundreds of times more efficient than a recent proposal regarding to the computational overhead on user side.

TITLE : Enabling Robust and Privacy-Preserving Resource Allocation in Fog Computing **[2]**
AUTHOR : L. Zhang, and J. Li
YEAR : 2018

DESCRIPTION

Fog computing is an extension of cloud computing and enables computing directly at the edge of the network. In fog computing paradigm, the fog nodes reside between smart end devices and the cloud. Benefiting from the structure of fog computing, fog computing can provide services with low latency, location awareness, and mobility. Since the fog nodes are not as powerful as the cloud, resource allocation techniques are usually adapted to optimize the utilization of the resources of fog nodes. However, the current resource allocation techniques are not privacy-preserving, i.e., an attacker can easily find end devices' sensitive information. In this paper, we propose a privacy-preserving resource allocation scheme for fog computing. The new proposal has constant message expansion, and it is secure against both an eavesdropper and a smart gateway that is employed to perform the resource allocation algorithm. Our scheme is also robust, since it achieves a full key compromise resistance which guarantees that even if the private keys of all the fog nodes in a fog system are corrupted the scheme remains secure.

TITLE : Fog and IoT: An Overview of Research Opportunities [3]
AUTHOR : M. Chiang, and T. Zhang
YEAR : 2016

DESCRIPTION

Fog is an emergent architecture for computing, storage, control, and networking that distributes these services closer to end users along the cloud-to-things continuum. It covers both mobile and wireline scenarios, traverses across hardware and software, resides on network edge but also over access networks and among end users, and includes both data plane and control plane. As an architecture, it supports a growing variety of applications, including those in the Internet of Things (IoT), fifth-generation (5G) wireless systems, and embedded artificial intelligence (AI). This survey paper summarizes the opportunities and challenges of fog, focusing primarily in the networking context of IoT.

Fog is an architecture that distributes computation, communication, control and storage closer to the end users along the cloud-to-things continuum. Sometimes the term "fog" is used interchangeably with the term "edge," although fog is broader than the typical notion of edge. The relevance of fog/edge is rooted in both the inadequacy of the traditional cloud and the emergence of new opportunities for the Internet of Things, 5G and embedded artificial intelligence.

TITLE : Distributed Aggregate Privacy-Preserving Authentication in VANETs [4]
AUTHOR : L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin, and C. Hu
YEAR : 2017

DESCRIPTION

Existing secure and privacy-preserving vehicular communication protocols in vehicular ad hoc networks face the challenges of being fast and not depending on ideal tamper-proof devices (TPDs) embedded in vehicles. To address these challenges, we propose a vehicular authentication protocol referred to as distributed aggregate privacy-preserving authentication. The proposed protocol is based on our new multiple trusted authority one-time identity-based aggregate signature technique. With this technique a vehicle can verify many messages simultaneously and their signatures can be compressed into a single one that greatly reduces the storage space needed by a vehicle or a data collector (e.g., the traffic management authority). Instead of ideal TPDs, our protocol only requires realistic TPDs and hence is more practical.

Vehicular ad hoc networks (VANETs) have attracted substantial attention in both ndustry and academia. A VANET typically consists of vehicles and properly distributed roadside units (RSUs). A vehicle can send/receive safety-related messages (e.g., speed, location, dangerous road conditions) to/from nearby vehicles and RSUs. These messages reduce the drivers' risk of having an accident and help them manage small emergencies.

TITLE : Secure Intelligent Traffic Light Control Using Fog Computing [5]
AUTHOR : J. Liu, J. Li, L. Zhang, F. Dai, Y. Zhang, X. Meng, and J. Shen
YEAR : 2018

DESCRIPTION

As the number of vehicles grows, traffic efficiency is becoming a worldwide problem. Intelligent transportation system aims to improve the traffic efficiency, where intelligent traffic light control is an important component. Existing intelligent traffic light control systems face some challenges, e.g., avoiding heavy roadside sensors, resisting malicious vehicles and avoiding single-point failure. To cope with those challenges, we propose two secure intelligent traffic light control schemes using fog computing whose security are based on the hardness of the computational DiffieHellman puzzle and the hash collision puzzle respectively. The two schemes assume the traffic lights are fog devices. The first scheme is a simple extension of a recent scheme for defending denial-of-service attacks. We show this simple extension is not efficient when the vehicle density is high. The second scheme is much more efficient and is fog device friendly. Even the vehicle density is high, the traffic light may verify the validity of the vehicles efficiently. Our schemes may resist the attacks from malicious vehicles. Our schemes can avoid the problem of single-point failure. Our improved scheme is fog device friendly.

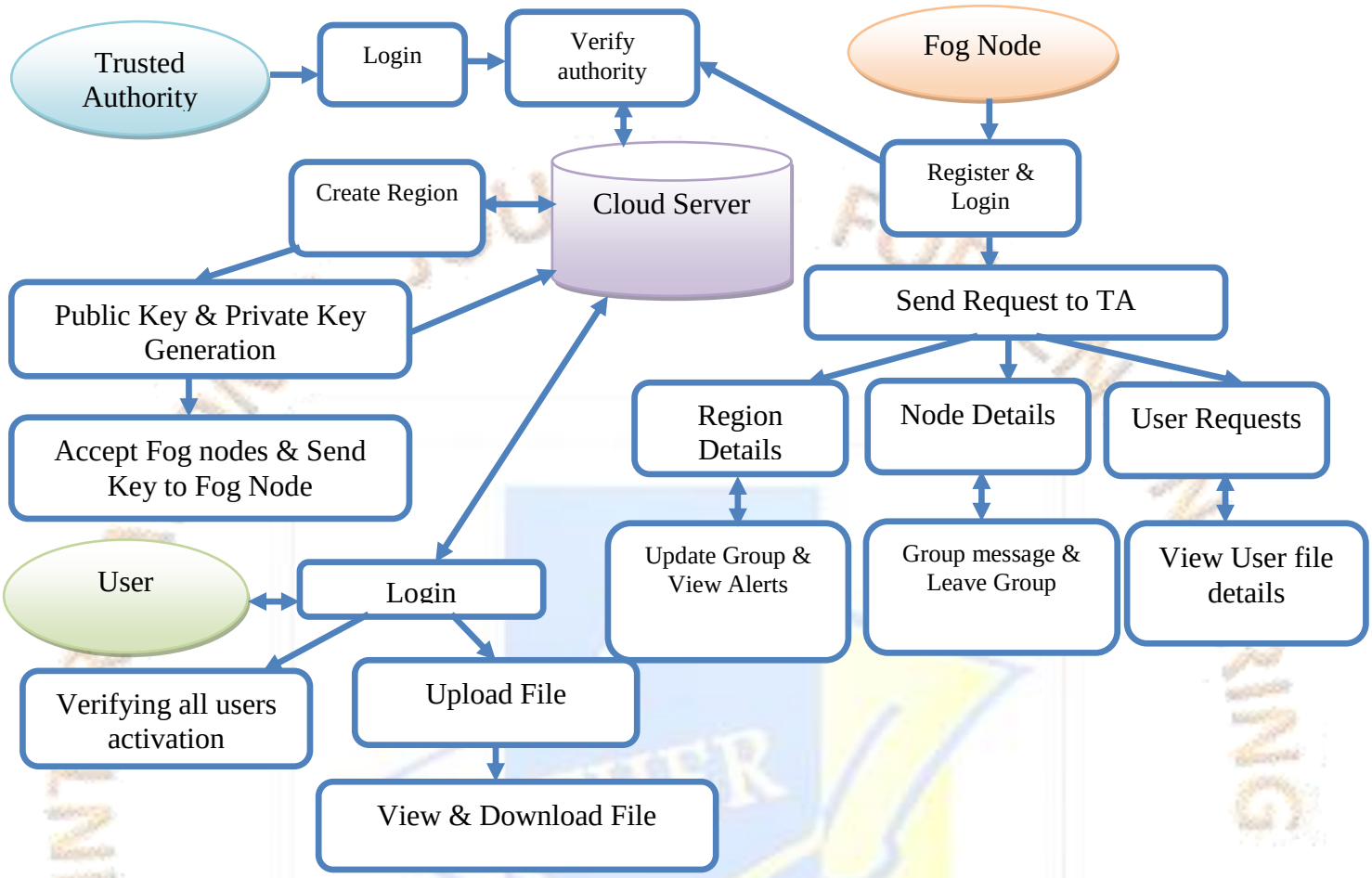
III. EXISTING SYSTEM

- For latency-sensitive applications, current cloud computing paradigm can hardly meet their demands for low latency due to limited network bandwidth, long geographic distance between traditional cloud and an end user.
- However, they still face many technical challenges when they are applied to fog computing, in which the key challenge identified with most of the existing schemes is communication and computation complexity.

IV. PROPOSED SYSTEM

- We propose a key management scheme called dynamic contributory broadcast encryption (DConBE) for secure channel establishment in fog computing.
- It allows a group of fog nodes that want to establish a fog system to negotiate a public encryption key and each node's decryption key in one round without a trusted dealer

V. SYSTEM ARCHITECTURE



VI. CONCLUSION

We have defined the notion of DConBE and proposed a concrete DConBE scheme for key management in fog computing. In DConBE, any end user can send encrypted messages to any subset of fog nodes in a fog system without requiring a trusted dealer. The new DConBE scheme allows a fog node to join or leave the fog system efficiently. The security of the proposed scheme is proven under the decision.

VII. REFERENCES

[1] J. Li, L. Zhang, K. Liu, H. Qian, and Z. Dong, "Privacy-Preserving Public Auditing Protocol for Low Performance End Devices in Cloud," IEEE Transactions on Information Forensics and Security, vol. 11, no. 11, pp. 2572–2583, 2016.
[2] L. Zhang, and J. Li, "Enabling Robust and Privacy-Preserving Resource Allocation in Fog Computing," IEEE Access, vol. 6, pp. 50384–50393, 2018.
[3] M. Chiang, and T. Zhang, "Fog and IoT: An Overview of Research Opportunities," IEEE Internet of Things Journal, vol. 3, no. 6, pp. 854–864, 2016.
[4] L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin, and C. Hu, "Distributed Aggregate Privacy-Preserving Authentication in VANETs," IEEE Transactions on Intelligent Transportation Systems, vol. 18, no. 3, pp. 516–526, 2017.
[5] J. Liu, J. Li, L. Zhang, F. Dai, Y. Zhang, X. Meng, and J. Shen, "Secure Intelligent Traffic Light Control Using Fog Computing," Future Generation Computer Systems, vol. 78, part 2, pp. 817-824, 2018.