A Distributed Publisher-Driven Secure Data Sharing Scheme for Information-Centric IoT

ABSTRACT

IoT (Internet of Things) is likely to have a major impact on human lives as new services and applications are developed through integration of the physical and digital worlds. In Information-Centric Internet of Things (ICIoT), IoT data can be cached throughout a network for close data copy retrievals. Such a distributed data caching environment, however, poses a challenge to flexible authorization in the network. To address this challenge, Ciphertext-Policy Attribute-Based Encryption (CP-ABE) has been identified as a promising approach. However in the existing CP-ABE scheme, publishers need to retrieve attributes from a centralized server for encrypting data, which leads to high communication overhead. To solve this problem, we incorporate CP-ABE and propose a novel Distributed Publisher-driven secure Data sharing for ICIoT (DPD-ICIoT) to enable only authorized users to retrieve IoT data from distributed cache. In DPDICIoT, newly introduced Attribute Manifest (AM) is cached in the network, through which publishers can retrieve the attributes from nearby copy holders instead of a centralized attribute server. In addition, a key chain mechanism is utilized for e_cient cryptographic operations, and an Automatic Attribute Self-update Mechanism (AASM) is proposed to enable fast updates of attributes without querying centralized servers. According to the performance evaluation, DPD-ICIoT achieves lower bandwidth cost compared to the existing CPABE scheme.

EXISTING SYSTEM

In existing the ciphertext-policy attribute-based encryption (CP-ABE) a user's private-key is associated with a set of attributes and a ciphertext specifies an access policy over a defined universe of attributes within the system. A user will be ale to decrypt a ciphertext, if and only if his attributes satisfy the policy of the respective ciphertext. Policies may be defined over

attributes using conjunctions, disjunctions and (k,n)-threshold gates. CP-ABE thus allows to realize implicit authorization, i.e., authorization is included into the encrypted data and only people who satisfy the associated policy can decrypt data. Another nice features is, that users can obtain their private keys after data has been encrypted with respect to policies. So data can be encrypted without knowledge of the actual set of users that will be able to decrypt, but only specifying the policy which allows to decrypt. Any future users that will be given a key with respect to attributes such that the policy can be satisfied will then be able to decrypt the data.

DRAWBACKS

- CP-ABE scheme does not consider a ubiquitous distributed caching environment and completely relies on centralized servers/clouds.
- It restricts scalability of IoT systems.

PROPOSED SYSTEM

In this paper, we propose a novel Distributed Publisher-driven secure Data sharing for ICIoT (DPD-ICIoT) to enable only authorized users to retrieve IoT data from distributed cache. In DPDICIoT, newly introduced Attribute Manifest (AM) is cached in the network, through which publishers can retrieve the attributes from nearby copy holders instead of a centralized attribute server. In addition, a key chain mechanism is utilized for e_cient cryptographic operations, and an Automatic Attribute Self-update Mechanism (AASM) is proposed to enable fast updates of attributes without querying centralized servers. According to the performance evaluation, DPD-ICIoT achieves lower bandwidth cost compared to the existing CPABE scheme. Ciphertext Policy Attribute-Based Encryption (CPABE) with centralized server(s), wherein all attribute values and access policies are retrieved from the servers. The existing CP-ABE scheme does not consider a ubiquitous distributed caching environment and completely relies on centralized servers/clouds, which restricts the scalability of IoT systems.

ADVANTAGES

- It achieves lower bandwidth cost.

- It provides efficient cryptographic operations.

SYSTEM REQUIREMENTS

H/W System Configuration:-

- Processor - Pentium –IV
- RAM - 4 GB (min)
- Hard Disk - 20 GB
- Key Board - Standard Windows Keyboard
- Mouse - Two or Three Button Mouse
- Monitor - SVGA

S/W System Configuration:-

- Operating System : Windows 7 or 8 32 bit
- Application Server : Tomcat5.0/6.X
- Programming Language : Java
- Java Version : JDK 1.6 and above