IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Special Issue || Dec. 2019 || PP 01-05
International Conference on Management Practices, Innovations & Research 2019

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

Ms. Geeta Nikude, Prof.Pravin Kulurkar
PG Student: Dept. of Computer Science Engineering Vidarbha Institute of Technology Nagpur, India
Prof: Dept. of Computer Science Engineering Vidarbha Institute of Technology Nagpur, India

Abstract— *In Information-Centric Internet of Things (ICIoT), Internet of Things (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 DPD-ICIoT, newly introduced attribute manifest 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 efficient cryptographic operations, and an automatic attribute self- update mechanism 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 CP-ABE scheme.*

Keywords— *IoT, ICN, Encryption, NICT, Cryptography, DPD-ICIoT, NFD, Information retrieval, Internet of things, Authorization, Cache storage.*

I. Introduction

IoT (Internet of Things) is likely to have a major impact on human lives as new services and applications are devel-oped through integration of the physical and digital worlds . It is predicted that
50 billion devices will be connect-ed through IoT by 2020, and vast amounts of data will be generated from those devices
. Today, most IoT services are designed based on Internet technology, which was originally conceived for end-to-end communications. Based on such technology, IoT data sharing applications have been developed on the basis of centralized servers/clouds, which produce redundant and duplicate traffic and bring out large latencies. Such a considerable volume of redundant traffic hinders efficient data flows and impose limitations on providing highly available services as is required by IoT applications With regard to the use of IoT applications, users are usually concerned only about the IoT data that they retrieve rather than where the data are stored or cached . Information- Centric Networking (ICN) is an emerging tech-nology that enables users to retrieve data from close caches without the need to access distant servers or clouds each time . Reducing the redundant traffic overhead and data retrieval latency by moving data from clouds to caches close to users is a promising approach. It integrates computing power and storage to alleviate the bottleneck of network bandwidth resources . Among the existing IC-Ns, Content-Centric Network (CCN)/Named Data Network (NDN) is one of the most promising architectures; therefore, in this paper, we focus on CCN/NDN.

Compared to Internet-based IoT designs, ICN-based IoT designs have several salient and distinctive features with regard to security, heterogeneity, fast configuration, and diverse communication paradigms , besides a reduction in traffic and latency. ICN is expected to be one of the fundamental technologies that will support IoT applications and services in the future, and for simplicity, hereafter, we refer to the IoT designs using ICN as ICIoT. ICIoTs have recently been widely discussed for use in IoT applications, such as smart cities , smart grid , smart home , IoT data sharing , service-oriented architectures , and data collection in IoT

The design requirements and challenges as well as the applicability of ICIoT have also been discussed in IRTF ICNRG . ICIoT has emerged as a promising solution to provide viable IoT services to users . To realize a true IoT vision, ensuring security is a key issue. Along these lines, some of the primary security threats that IoT data sharing tends to face include unauthorized access, illegal modification, and impersonated publication and retrieval. It is necessary to design a flexible and secure IoT data sharing scheme, wherein IoT data are securely published, cached in the network, and retrieved by only authorized users. However, because of unpredictable caching of IoT data on untrusted devices as is typical in ICIoTs, it is challenging to provide fine-grained data access control in a distributed caching environment to future IoT services.

the lowest performance situation with at most one cached copy in one domain and the bandwidth cost for CP-ABE. The bandwidth cost is defined as the bandwidth consumption for communications.

II. Objectives

These systems would allow the users to get the personalized services intelligently by using their context and profile information to improve users' experience (see Fig. 1). However, in such user-centric networks, security becomes a key issue as several devices involve in information sharing in a volatile environment [4]. The security issues that might arise during information transfer can be categorized into two types: application security, and user security

The IoT system shall support event-based and periodical IoT streaming data sharing among devices as well. As the typical IoT scenario, we consider the following transporta-tion data sharing. The car sensor detects an event that the road segment X, street Y is frozen and slippery at 9 am on Dec. 11, 2016. It wants to provide this data to drivers, and as a further restriction, only to the drivers who, given their current location, are expected to reach Street Y in 10 minutes, or to residents of buildings with more than 50 people along road segment X.

- Compared with the existing CP-ABE scheme, the total bandwidth cost in packet transmissions consumed for attribute retrievals can be greatly reduced.
- To the best of our knowledge, this is the first work to investigate publisher-driven fine-grained access control in a ubiquitously distributed caching scenario for ICIoT.
- We integrate CP-ABE with the typical ICN, CCN/NDN and propose a novel DPD-ICIoT scheme for providing distributed, secure, and flexible data sharing for ICIoT.
- We employ a key chain mechanism for efficient data encryption and decryption.

III. System Specification

With the existing CP-ABE scheme, all the attribute values and attribute updates need to be provided through centralized servers, such as attribute server and DSAs. In contrast, the attribute values are described in AMs and retrieved from close caches. Herein, we perform system evaluations to compare the existing CP-ABE scheme with the proposed DPD-ICIoT scheme. We consider that the metric for comparison is the ratio between the bandwidth cost of the DPD-ICIoT scheme at

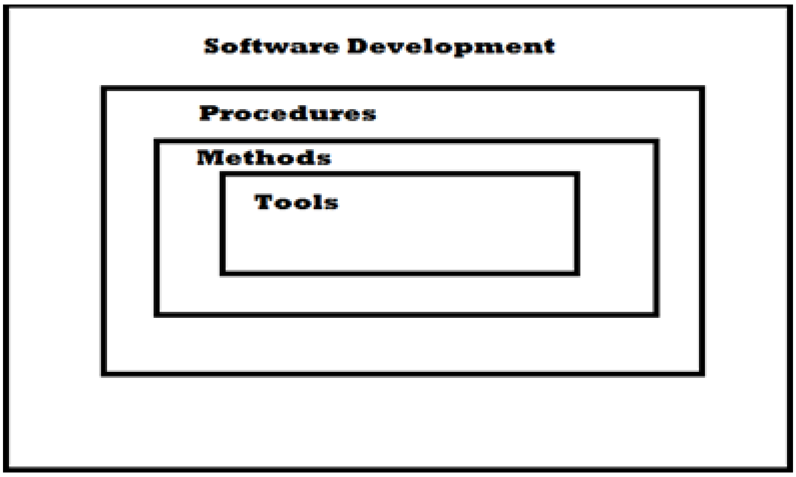


Fig1. Schemantic of System Specification Assume that the network is divided into many domains. Ineach domain, one piece of AM or DM or data chunk can only be cached at most once, which is the lowest performance for CCN. If more AMs are cached, the cost for AM retrieval will be reduced further. CCN is utilized as the method for dataretrieval. Based on the above assumptions, a proposed network can be modeled as a undirected, connected graph G = (V ; E), where V is a finite set of vertices (network nodes), and E is the set of edges (network links) representing connection of those vertices. N denotes the total number of nodes in V . It is assume

IV. System Evaluation

We also have plan to improve NovaGenesis performance by:

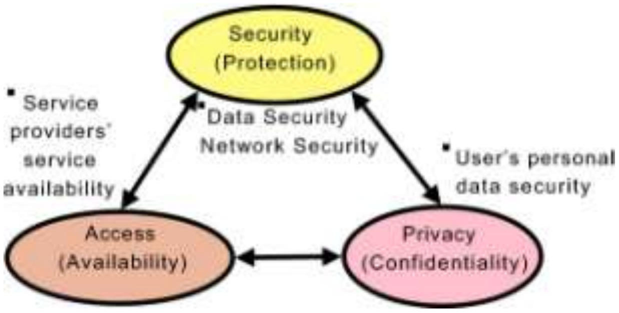
(i) adding source coding to NG messages; (ii) exploring load balancing and multi-path routing; (iii) elasticity of NovaGenesis services; (iv) refinement of the prototype; (v) employ different hash code sizes to reduce overhead in NG messages; (vi) implement hierarchical multi-domain/level name resolution, network caching and name-based routing. These improvements promise a better performance when compared to the current solutions. For this reason, they will be the target of future work.

This section returns to the design dimensions presented in Table 1, giving a summary of NovaGenesis benefits to the problem of trustable unlicensed spectrum management for IoT/Wi-Fi. Moreover, it points out open challenges for future developments. Table 5 summarizes our contributions for the control plane of new generation WSANs and IoT:

- D3—NovaGenesis made possible name-based access and routing of spectrum sensing data, including network caching for efficient, distributed and coherent software-control (control plane) of smart environments.
- D4—Integration of software-defined control and operation [37,49]. The current SDN model (based on the OpenFlow protocol) is limited to configure forwarding tables at link layer switches. NG allowed broader configuration and management of physical devices via their software representatives (e.g., DSM services). Therefore, NG extends software-defined paradigm towards exposing hardware capabilities to spectrum management services, enabling "richer" orchestration of resources.

D5—NovaGenesis includes support for the dynamic composition of control plane services based on semantic and context-awareness. It provides mechanisms for the complete service life-cycling. Quality of service (QoS) can be measured from the established contracts, enabling estimation of services reputation..

Multipurpose control of UPFC; it may control the power at the same time and compensation is carried out with respect to terminal voltage and line series compensation change or alteration in phase-shift angle. The power circuit of UPFC is shown below



F**ig2**.Event Driven Data Management

NovaGenesis adopts temporary caches in every domain to improve named-content distribution. This approach is founded in ICN, in which contents are accessed by their names and popular information is made available to future access in local cache. NG name resolution approach is integrated to a network caching to form a name resolution and network caching service (NRNCS). By integrating name resolution to content caching, NG facilitates content delivery by their names.

The current implementation of NRNCS adopts a publish/subscribe communication model, in which services publish and/or subscribe name bindings (NBs) and associated contents (if any) from the local domain cache. Therefore, NRNCS provides a rendezvous point analogous to message queuing telemetry transport (MQTT) brokers.

NRNCS is implemented by three services: (i) publish/subscribe service (PSS) to which services can publish or subscribe NBs/contents; (ii) generic indirection resolution service (GIRS) that selects appropriate hash tables to store named data; (iii) a hash table service (HTS), which in fact stores NBs and associated contents. Every NG domain must have at least one instance of each of these core services.

However, elasticity is provided by increasing the numbers of PSS/GIRS/HTS.

V. Simulation Model Of System

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 efficient 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.

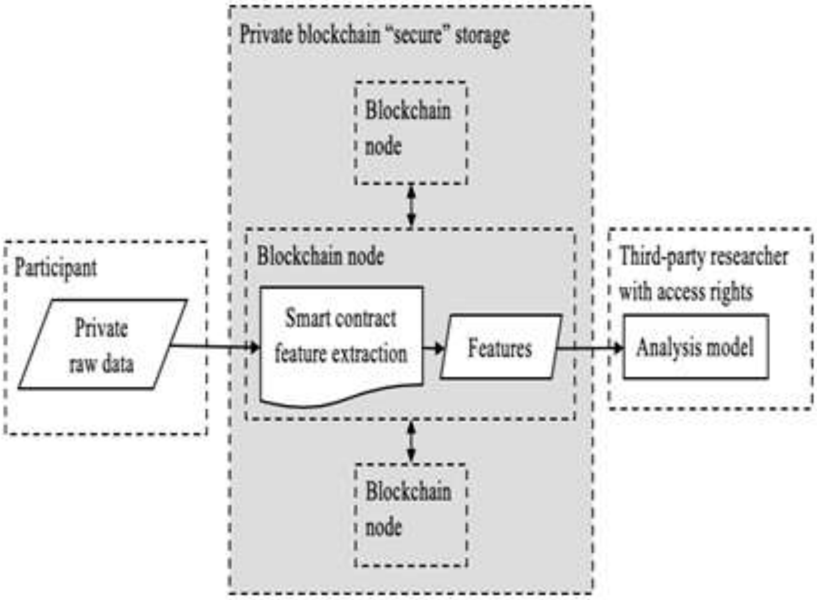

Private blockchain "secure" storage
Blockchain node
Participant
Private raw data
Blockchain node
Smart contract feature extraction
Features
Third-party researcher with access rights
Analysis model
Blockchain node

Fig3. Privacy Preserving Method

NOA (Network Operator and Authority): The en-tity who operates a network consisting of routers, gateways, and access points, which are potentially equipped with caches. It provides security policies and functions for the devices in the network, such as functions for identity management and authentication services for entities. • DSA (Data Sharing Authority): The entity that assists Publishers to provide access privileges to Users for securely providing their IoT data.

ta, can be published by Publishers, such as mobiles, sensors, actuators, and RFIDs. They are distributedly cached or stored throughout network. In Fig. 1, IoT data published by P1 are cached at access points, routers, and BSs, and stored in the cloud and servers, which is depicted with the yellow circle. It is assumed that the nearby cache or storage points for the targeted data of the Users is the cloud at Domaina
, BS and access point at Domainb , and router at Domainc . The Users can retrieve data from these cache or storage poin

VI. Self Update Mechanism

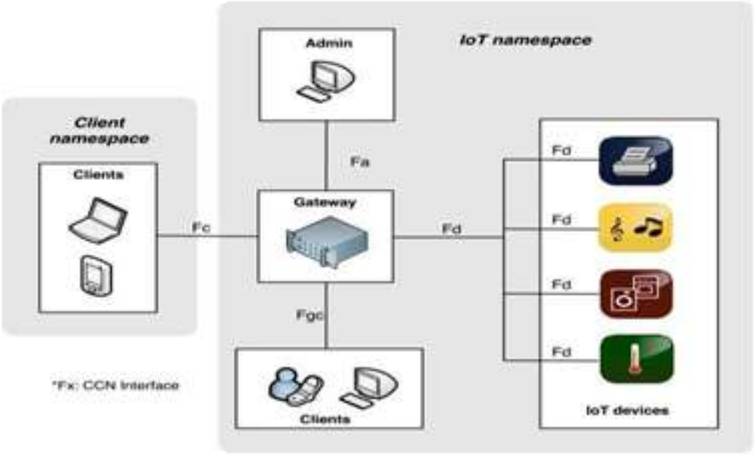


Fig4. IoT Namespace

These systems would allow the users to get the personalized services intelligently by using their context and profile information to improve users' experience (see Fig. 1). However, in such user-centric networks, security becomes a key issue as several devices involve in information sharing in a volatile environment [4]. The security issues that might arise during information transfer can be categorized into two types: application security, and user security

The IoT system shall support event-based and periodical IoT streaming data sharing among devices as well. As the typical IoT scenario, we consider the following transporta-tion data sharing. The car sensor detects an event that the road segment X, street Y is frozen and slippery at 9 am on Dec. 11, 2016. It wants to provide this data to drivers, and as a further restriction, only to the drivers who, given their current location, are expected to reach Street Y in 10 minutes, or to residents of buildings with more than 50 people along road segment X. These data are sent to the network and distributedly cached, and the drivers on the street or the people living in the building retrieve these

VII. Conclusion

In this world of growing technologies everything has been computerized. With large number of work opportunities the Human workforce has increased. Thus there is a need of a system which can handle the data of such a large number of Employees in an organization. This project simplifies the task of maintain records and provide security of that record because of its user friendly natureUPFC is one of the index tools of AC transfer system having promising capabilities for controlling the parameters of utilizing the transfer system in the steady state and the transient state of system.

References

[1]. United Nation. (2014). World Urbanization Prospect. [Online].Available

[2]. http://dl.acm.org/citation.cfm?id=308574.308676

[3]. M. S. Hossain, ``Cloud-supported cyber-physical localization framework for patients monitoring,'' IEEE Syst. J., vol. 11, no. 1, pp. 118 127, Mar. 2017.

[4]. M. S. Hossain, G. Muhammad, W. Abdul, B. Song, and B.

[5]. B. Gupta, ``Cloud-assisted secure video transmission and sharing framework for smart cities,'' Future Generat. Comput. Syst. J., Elsevier 2017, to be pub- lished. [Online].

[6]. J. Liao, L. Stankovic, and V. Stankovic, ``Detecting household activity

[7]. patterns from smart meter data,'' in Proc. Int. Conf. Intell. Environ. (IE), vol. 6. Jul. 2014, pp. 71 78.

[8]. A. Yassine, A. A. N. Shirehjini, and S. Shirmohammadi,

[9]. ``Smart meters big data: Game theoretic model for fair data sharing in deregulated smart grids,'' IEEE Access, vol. 3, pp. 2743 2754, 2015.

[10]. A. Yassine and S. Shirmohammadi, ``Measuring users' privacy payoff using intelligent agents,'' in Proc. IEEE Int. Conf. Comput. Intell. Meas. Syst. Appl., May 2009, pp. 169 174.

[11]. A. Yassine and S. Shirmohammadi, ``A business privacy model for virtual communities,'' Int. J. Web Based Commun., vol. 5, no. 2, Mar. 2009.

[12]. Y. C. Chen, H. C. Hung, B. Y. Chiang, S. Y. Peng, and P.

[13]. J. Chen, ``Incre- mentally mining usage correlations among appliances in smart homes,'' in Proc. 18th Int. Conf. Netw.- Based Inf. Syst. (NBiS), 2015, pp. 273 279.

[14]. K. Jack and K.William, ``The UK-DALE dataset, domestic appliance-level

[15]. electricity demand and whole-house demand from ve UK homes,'' Sci. Data, vol. 2, p. 150007, Sep. 2015.

[16]. J. Clement, J. Ploennigs, and K. Kabitzsch, ``Detecting activities of daily living with smart meters,'' in Advance Technology and Societal Change. Heidelberg, Germany:

[17]. Springer,2014,pp.143160.[Online].Available:https://link.springer.com/chapter/10.1007/978-3-642-37988- 8_10

[18]. Q. Ni, A. B. G. Hernando, and I. P. de la Cruz, ``The Elderly's independent living in smart homes: A characterization of activities and sensing infrastructure survey to facilitate services development,'' Sensors, vol. 15, no. 5, pp. 11312 11362, 2015. [Online]. Available: http://www.mdpi.com/