Asian Journal of Convergence in Technology *Volume III, Issue III*
ISSN No.:2350-1146, I.F-2.71

Enhanced Data Leakage Detection in IoT Network Backup with Cloud Using Paillier Homomorphic Cryptosystem

Anand R. Dargad
Department of Computer Science and Engineering
ADCET, Ashta, India
ananddargad05@gmail.com

Sandeep G. Sutar
Department of Computer Science and Engineering
ADCET, Ashta, India
sutarsandeep07@gmail.com

***Abstract*—The simplicity of sharing data through the Web furthermore, Distributed computing accidentally presents a developing issue of Data leakage. In the meantime, numerous end-clients are unconscious that their information was leaked or stolen following most information is leaked by operations running out of sight. This paper presents a novel client driven, mantrap-propelled Data Leakage Prevention (DLP) approach that can find, present any sending of information – both approved and unapproved – to end-clients and along these lines give them the capacity to stop the sending process. Our proposed system introduces mechanism to design an algorithm which communicates Internet of Things devices with the corresponding privileges and present a novel approach to support stronger security by encrypting the data with differential privilege keys also reduce the storage size of the authenticated information to increase the security of the data while sending to agent.**

Keywords—Internet of Things (IoT), Data Leakage Detection, Cloud Computing.

I. INTRODUCTION

Internet of Things (IoT) is becoming one of the important concepts in the day to day life. The Internet of Things means the interconnection between the two physical entities which can be connected by the internet. The Internet of Things also called Internet of Everything, is the network of "things" which are combination of electronics, software, sensors and connectivity to enable objects to exchange data with the connected devices which are in the same network. It is the smart way to access the information which is gathered through some sort of sensors. Such information can be controlled remotely across network and provides opportunities for more direct integration between the physical world and computer-based systems and the result of this is improved efficiency, accuracy and economic benefits.

Cloud computing is an adaptable, intense and financially savvy system in giving ongoing information to clients whenever with incomprehensible scope and quality. The cloud comprises of equipment, systems, administrations and interfaces that empower the conveyance of processing as an administration. Cloud computing has a huge effect on the IT industry and research groups. Cloud computing gives High calculation power and capacity limit by means of using countless PCs together, empowering clients to convey applications with the low cost. Capacity cost for cloud client is computed as pay per requirement.

Data Leakage is characterized as the inadvertent or purposeful circulation of private or delicate information to an unapproved user. Confidential information of organizations or associations contains protected innovation (IP), money related data, individual Mastercard information and other data relying upon that organization's work. There are three conditions of information as "data in rest", "data in movement" and "data being used". At each of these three conditions, data can be leaked. To avoid such leakage we provide Data Leakage Prevention (DLP) technique which provides set of operations.

II. RELATED WORK

A. Literature Survey

In this work, the author focuses on an existing U2IoT architecture (i.e., unit IoT and ubiquitous IoT), to design an aggregated-proof based hierarchical authentication scheme (APHA) for the layered networks. Solidly, 1) the totaled evidences are built up for numerous objectives to accomplish in reverse and forward mysterious information transmission; 2) the coordinated way descriptors, homomorphism capacities and Chebyshev disorderly maps are together connected for shared confirmation; 3) distinctive get to powers are doled out to accomplish various leveled get to control [1].

In this paper, survey is planned to serve as a rule and a theoretical system for setting mindful item improvement and research in the Internet of Things worldview. It likewise gives a precise investigation of existing Internet of Things items in the commercial view and highlights various possibly noteworthy research headings and patterns. Here considering a rule and a calculated system for setting mindful item improvement [2].

The author analyses particular Internet of Things security and protection issues, including security necessities, risk models and assault scientific classifications from the human

services point of view. Additionally author proposes an insightful communitarian security model to minimize security hazard; talks about how diverse advancements, for example, enormous information, surrounding knowledge and wearable gadgets can be utilized in a human services setting; addresses different e-Health arrangements and controls over the world to decide how they can encourage economies and social orders as far as economic improvement; and gives a few roads to future research on Internet of Things to construct medicinal services situated in light of an arrangement of open issues and difficulties. This work is used to create Internet of Things security and protection highlights [3].

This article reports the ebb and flow condition of research on the Internet of Things by looking at the writing, distinguishing trends and flow patterns, portraying challenges that undermine Internet of Things dispersion, exhibiting open research inquiries, future headings and accumulating a far reaching reference rundown to help scientists. This paper gives idea related with Ubiquitous IoT [4].

As per the Internet of Things (IoT) vision, regular questions, for example, any sort of household machines, actuators and installed frameworks will be associated with each other and with the internet in the near future. This will shape a conveyed connect with detecting abilities that will permit phenomenal market openings, impelling new administrations, including vitality observing and control of homes, structures, mechanical procedures et cetera. Web administrations are utilized for correspondence as a part of Internet of Things [5].

Outsourcing the information in cloud computing is exponentially creating to scale up the equipment and programming assets. So the protection of outsourced sensitive data is becoming a major data security challenge in cloud computing. To address these information security challenges, author proposes a proficient information encryption to encode delicate information before sending to the cloud server [6].

The author presents novel clients driven, mantrap-enlivened Data Leakage Prevention (DLP) approach that can find, show any sending of information – both approved and unapproved – to end-clients and in this way give them the capacity to stop the sending procedure. Here own kernel module executed to cooperate with the client space program in getting clients endorsement for each sending procedure – giving the client full control over every single outbound data sending process in their gadgets. With this, the end-client can simply choose which information sending procedure ought to be permitted or blocked. This beats the restrictions of frequently inflexible and erroneous DLP arrangements relying upon pre-set principles and substance discovery [7].

III. Proposed System

To design a data leakage prevention mechanism, it is challenging task to provide strong security by encrypting the data with differential privilege keys in Internet of Things network. The present work is focused on how to design an algorithm to communicate Internet of Things devices with the corresponding privileges and how to use cryptographic algorithm to provide stronger security by encrypting the data. The objectives of our proposed system are:

Design an algorithm to communicate Internet of Things devices with the corresponding privileges.

Present an advanced scheme to support stronger security of the data.

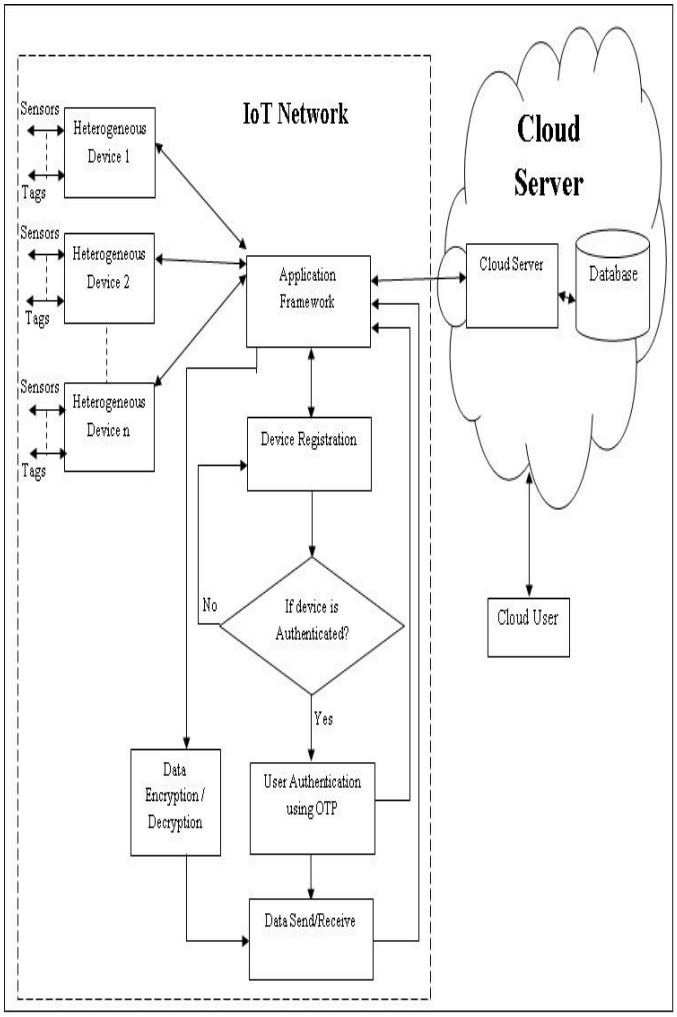

Fig. 1 System Architecture

In above figure, there are various heterogeneous devices connected to the application framework. Such heterogeneous devices have some sort of sensors. In the application framework the basic information regarding the devices is stored. For heterogeneous device's authentication OTP method is used. While storing data, it will be converted into encrypted format and for sending data to heterogeneous device it will be converted into plain text. The cloud service is used to store the data of the devices in cloud database server. The cloud database server managed by the cloud user.

The working of our proposed system is, first any device tries to connect with the application framework. Then application framework checks whether that device is registered or not. If that device is not registered then application framework will register that device. If that device is already registered then application framework will send OTP for the authentication. If the match of OTP found to be correct then application framework will provide data to the particular device/ user.

While sending the requested data cloud user or admin of system will send data in two types as, explicitly i.e. in this case admin add some fake data set in original data set and in second type simple, data can be sent as it is i.e. original data.

A. *Methodology*

Cloud User

In the cloud environment, cloud user works as cloud admin to handle database server.

Cloud Database Server

A database is accessible to clients from the cloud and delivered to resource on demand via the internet from a cloud database provider's servers. Cloud databases can use cloud computing to achieve optimized scaling, high availability and multi-tenancy and effective resource allocation.

Application Framework

Application frameworks in Internet of Things, where devices are seamlessly connect and share information securely with each other. With this primary requirement, one cannot overemphasize the role of software technology as an enabler for Internet of Things devices. Internet of Things application framework integrates any number and type of smart things. In this module the application framework interfaces with user authentication using OTP, data encryption decryption systems and cloud database server.

User Authentication using OTP

Secure OTP Authentication uses One-Time-Password (OTP) technology to provide strong authentication. An OTP is a password that is valid for only ONE login session and after that it becomes obsolete. It is also known as a dynamic password. There are two approaches to generate an OTP: Time based OTP – the OTP changes at frequent intervals (for example every 30 or 60 seconds).Event-based OTP – the OTP is generated by pressing a button on the OTP device or token [9].

Data Encryption /Decryption

During the communication in Internet of Things devices, there is need to prevent data leakage. So data encryption technique is used to encrypt data and decrypt data while transmission. For the encryption and decryption operation we are using paillier homomorphic cryptosystem.

The Paillier cryptosystem is a probabilistic asymmetric algorithm for public key cryptography. The issue of registering n^{th} deposit classes is accepted to be computationally troublesome. The decisional composite residuosity presumption is the obstinacy theory whereupon this cryptography is based. The scheme is an addictive homomorphic cryptosystem; this implies, given just public key and the encryption of message1 (m_1) and message2 (m_2), one can register the encryption of m_1+m_2 [8].

IV. Experimental Setup

The experiment is carried out on Raspberry Pi 2 along with a system having processor I3 and 4GB RAM. An application is implemented using ASP.NET 4.0. Ultrasonic sensor is used for measuring the distance.

V. Results

Analysis of Proposed System

Strength of proposed system analyzed by considering following factors,

A. *Explicit Request [10]*

We concentrate on situations with a few objects that are shared among various users. These are the most interesting situations, since object sharing makes it hard to recognize a liable from non-liable users. Situations with more objects to share and situations with objects shared among fewer users are clearly easy to handle.

In our situations we considered set of |T|=50 objects and online requests of clients got one by one with a similar condition. Assume 8 objects fulfill this condition, so that every one of the users will get same 8 data sets.

The fake and unique data sets are chosen arbitrarily using e-random algorithm. By apportioning 10% to 15% fake objects; the administrator can identify a liable user even in worst scenario leakage situation, while without fake data set he will be unsuccessful in the worst scenario as well as in the normal case.

TABLE I

Dependence of Guilt Probability on Number of Fake Data Set

Table Head	**Pr {G_i | S}**
10	0.1
15	0.18
20	0.23
25	0.32
30	0.4
35	0.48

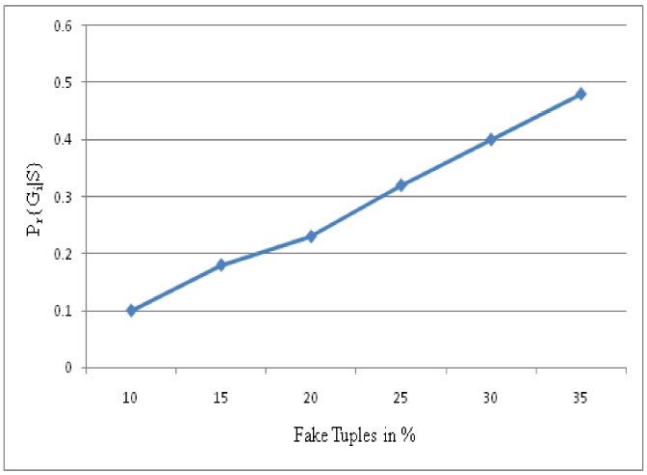

Fig. 2 Graphical representations of results shown in Table I

Above table and graph shows that as addition of fake data sets increases to the user's dataset, the probability of guilt detection also increases.

B. Simple Request [10]

With the sample data request, users are keen on specific data. Consequently, data sharing is not explicitly defined by their requests. The administrator is "constrained" to allot certain data to various users. In the event that same data is shared among numerous users, then it will be difficult to recognize a liable user.

In our experimental situation, consider set T has 30 articles and the quantity of data sets given to clients is in the range of [10, 25].

Here we take the sample from 6 users. The value in the figure 2 demonstrates that, as overlap of the user's request with the leaked dataset increases the guilt probability increments.

The guessing probability of data sets is considered as p=0.3.

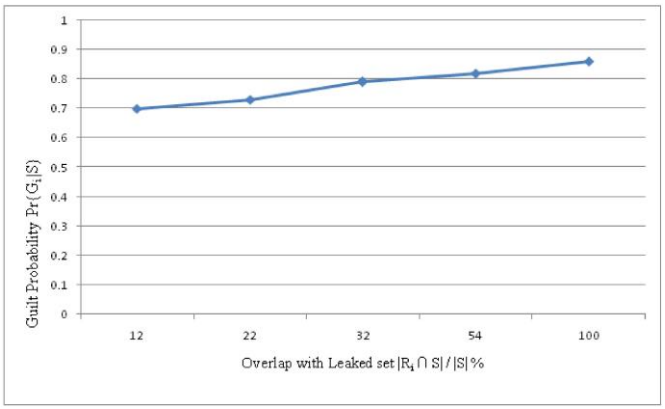

Fig. 3 Guilt probabilities for sample request from users

V. Conclusion

We identified few issues related to data leakage in Internet of Things network through literature survey. Then proposed and implemented solution for these issues by making use of homomorphic cryptosystem.

Acknowledgment

We are thankful to the authorities of A.D.C.E.T, the reviewer for their valuable suggestions, the college authorities for providing the required infrastructure and support. Finally, we would like to extend a heartfelt gratitude to friends and family members.

References

[1] "Aggregated-Proof Based Hierarchical Authentication Scheme for the Internet of Things" Huansheng Ning, Senior Member, IEEE, Hong Liu, Student Member, IEEE, and Laurence T. Yang, Member IEEE, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 26, NO. 3, MARCH 2015.

[2] "A Survey on Internet of Things from Industrial Market Perspective" CHARITH PERERA, (Member, IEEE), CHI HAROLD LIU, (Member, IEEE), SRIMAL JAYAWARDENA, (Member, IEEE), AND MIN CHEN, (Senior Member, IEEE) January 8, 2015.

[3] "The Internet of Things for Health Care: A Comprehensive Survey" S. M. RIAZUL ISLAM1, (Member, IEEE), DAEHAN KWAK, MD. HUMAUN KABIR, MAHMUD HOSSAIN, AND KYUNG-SUP KWAK, (Member, IEEE) April 4, 2015, accepted May 8, 2015.

[4] "The Internet of Things—A survey of topics and trends" Andrew Whitmore & Anurag Agarwal & Li Da Xu Inf Syst Front DOI 10.1007/s10796-014-9489-2.

[5] "Web Services for the Internet of Things through CoAP and EXI "Angelo P. Castellani, Mattia Gheda, Nicola Bui, Michele Rossi, Michele Zorzi, Oct 2011.

[6] "Data Encryption and Decryption Algorithms using Key Rotations for Data Security in Cloud System", by Prakash G L, Dr. Manish Prateek, 2014 IEEE.

[7] Ryan K L Ko, Alan Y S Tan, Ting Gao "A Mantrap-Inspired, User-Centric Data Leakage Prevention (DLP) Approach" 2014 IEEE 6th International Conference on Cloud Computing Technology and Science.

[8] https://en.wikipedia.org/wiki/Paillier_cryptosystem

[9] "GENERATION OF SECURE ONE-TIME PASSWORD BASED ON IMAGE AUTHENTICATION" Himika Parmar, Nancy Nainan and Sumaiya Thaseen CS & IT-CSCP 2012.

[10] "Data Leakage Detection" Panagiotis Papadimitriou, Student Member, IEEE, and Hector Garcia-Molina, Member, IEEE, IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL. 23, NO. 1, JANUARY 2011.