K-Anonymity based storage for IoT-enabled devices in distributed Cloud Computing environment

[1]Nancy Grover,[2]Er. Dinesh Kumar

[1]Student,Giani Zial Singh,MRSPTU,BATHINDA,PUNJAB,INDIA.

[2]Associate Professor,Giani Zial Singh,MRSPTU,BATHINDA,PUNJAB,INDIA.

Abstract: The things in IoT can be divided into coarse and fine resources as indicated by the size of resources. The granularity of the resources ought to be based on the complexity of the structure and function. The fine grain resources more often than not have basic structure and single function, which can be further divided into sensors, controllers and RFID equipment as indicated by the resource type. The IoT is a broad term alluding to applications as various as Internet-connected vehicles, consumer gadgets and smart phones. Adding power to RF devices with relatively short range enables more functionality, for example, sensing, mesh networking and automated control. Sharing data secured and hided using K-Anonymity based scheme is more efficient compared to the light weight authentification using username and password.

Keywords:IOT, RFID, K-Anonymity.

I. INTRODUCTION

Internet of Things or IoT) is the internetworking of physical devices, vehicles (also referred to as "connected devices" and "smart devices"), buildings, and other items embedded with electronics, software, sensors, actuators, and network connectivity that enable these objects to collect and exchange data. The IoT allows objects to be sensed and/or controlled remotely across existing network infrastructure, creating opportunities for more direct integration of the physical world into computer-based systems, and resulting in improved efficiency, accuracy and economic benefit in addition to reduced human intervention.

1.2 AUTHENTICATION PROTOCOL

It involves three types of entities one is user second is control server and third is the provider server. Control server will provides the authentification and data server provides the data services and user is the end part which request the services from the database server.

Registration Phase: in this phase user register itself to the control system. Once user register to the control system control system allocates the username and password to the user. So that system can be controlled to have secured access.

Login Phase: Any user who is allocated with username and password will access the contents in authentified way. So that any user can access and retrieve the contents in secured environment.

Authentication and Key agreement Phase: It is the mutual understanding between user system and control system. User generates the time stamp value. And system first checks the time stamp value. User will be listened only when the time stamp value matches. Later on control system checks the time stamp value. Stop the connection if the condition is false.

1.3 APPLICATIONS AND THINS IN IOT

With the development of technologies under the IoT, the IoT applications become quickly in fields of smart home, forestry monitoring, intelligent transportation, wisdom medical, industrial automation et cetera. For various applications, the system accesses distinctive appropriate device resources which are called "things" in IoT. Typical applications and things in IoT are broke down as follows [3]:

1) Smart Home: Mainly for home environment monitoring and electrical equipment control. The system consists with control center, various sorts of electrical equipment and agent devices, and has the functions of agent management, data transmission, access authentication and environment monitoring. The system adopts RFID technology for device identification and Bluetooth and GSM modules for data transmission. The things involved in the system

incorporate various kinds of electrical equipment with control function (TV, washing machine and ventilate), RFID devices for device authentication, and Bluetooth and GSM modules for network communication.

2) Forestry Monitoring: Mainly to monitor forest resources and the environment. The authors designed an IoT forest environmental factors collection platform based on ZigBee for measuring the forest environmental factors (light intensity, temperature, humidity and so forth.). The collected GPS and clock information is transmitted to the server for processing, accomplishing the effective monitoring for forest resources. The things involved in the system incorporate the various sorts of sensors for environmental information collection (temperature sensors, humidity sensors, and light sensors and GPS sensors) and ZigBee wireless LAN for data transmission.

3) Intelligent transportation: Mainly to monitor the traffic conditions and providing data for traffic management or reference recommendations for drivers. The system designed in research consists with fixed roadside detection units, on-board units located in the vehicles, backend server and the client terminals. The system obtains the road picture information through the cameras on roadside keeping in mind the end goal to decide the weather and road conditions, and obtains the temperature, speed and position information of every vehicle through on-board units. The system advance transfers the collected and aggregated data to the backend server database through the 3G network, and gives traffic data information to users with portable terminal. The things involved in the system incorporate cameras for gaining the picture information, the roadside units utilized for calculations to decide traffic condition and weather, various kinds of sensors used to obtain environmental information and 3G modules utilized for communications

1.4 K-ANONYMITY

In the case of anonymity, it is usually publicly available data on which linking is to be prohibited and so attributes which appear in private data and also appear in public data are candidates for linking; therefore, these attributes constitute the quasi-identifier and the disclosure of these attributes must be controlled. It is believed that these attributes can be easily identified by the data holder.

	Race	Birth	Gender	ZIP	Problem
t1	Black	1965	m	0214*	short breath
t2	Black	1965	m	0214*	chest pain
t3	Black	1965	f	0213*	hypertension
t4	Black	1965	f	0213*	hypertension
t5	Black	1964	f	0213*	obesity
t6	Black	1964	f	0213*	chest pain
t7	White	1964	m	0213*	chest pain
t8	White	1964	m	0213*	obesity
t9	White	1964	m	0213*	short breath
t10	White	1967	m	0213*	chest pain
t11	White	1967	m	0213*	chest pain

Fig. 1 Data with K-anonymity[2]

II. LITERATURE SURVEY

[1] Meng-Shiuan Pan(2016) et al: In many Internet of Things (IoT) applications, messages may need to be disseminated to some specific objects or nodes using multicast transmissions. In the literature, the multicast routing protocol can be divided into non-geographic-based and geographic-based. In this work, they proposed a lightweight and distributed geographic multicast routing protocol to solve the above problems. Our scheme contains three phases. First, the first phase selects intermediate nodes to reach multicast destinations. Then, the second phase removes loops and trims routes constructed in the first phase[3].

[2] Renato F. Fernandes (2016) et al: IoT for urban networks, network technologies depends on the application requirements such as reliability, delivery rate, safety, consumption, and others. The Open WSN group from Berkeley University build an IoT development platform under the most IoT networks standards. However, it uses synchronous mechanisms for media access. Therefore, this paper proposes an asynchronous multichannel MAC protocol based in RIT mechanism using Open WSN platform for use in applications with low power consumption and high scalability requirements[4].

[3] Biplob R. Ray (2016) et al: In this paper, they address the problem of ownership transfer of RFID tagged objects in Internet of Things (IoT) in a secure manner. They analysed the proposed object ownership transfer protocol both qualitatively and quantitatively to evaluate its effectiveness. The analysis shows that the proposed protocol is more secure and requires less computation as compared to existing similar protocols[5].

[4] Ruhul Amin(2016) et al: They propose an architecture which is applicable for distributed cloud environment and based on it, an authentication protocol using smartcard has been proposed, where the registered user can access all private information securely from all the private cloud servers. To proof security strength of their protocol, they have used AVISPA tool and BAN logic model in this article. In addition, informal cryptanalysis confirms that the protocol is protected against all possible security threats. The performance analysis and comparison confirm that the proposed protocol is superior than its counterparts[6].

[5] Benjamin Aziz(2016) et al: They present a formal model of the MQ Telemetry Transport version 3.1 protocol based on a timed message-passing process algebra. We explain the modeling choices that we made, including pointing out ambiguities in the original protocol specification, and we carry out a static analysis of the formal protocol model, which is based on an approximation of a name-substitution semantics for algebra. The analysis reveals that the protocol behaves correctly as specified against the rst two quality of service modes of operation providing at most once and at least once delivery semantics to the subscribers. However, we and that the third and highest quality of service semantics is prone to error and at best ambiguous in certain aspects of its specification. Finally, we suggest an enhancement of this level of QoS for the protocol[7].

R. Giuliano(2012) et.al To give advanced services to natives, Smart City services are enabled by a huge utilization of Internet of Things (IoT) technologies. The issue of coexistence amongst ALOHA and non-persistent CSMA devices transmitting in a similar area, and in a similar band, has been investigated by reproductions. Data obtained from reproduction can be utilized to survey the maximum number of ALOHA-, and CSMA-based devices that can be served in the area for the predetermined performance target.

III. ALGORITHM

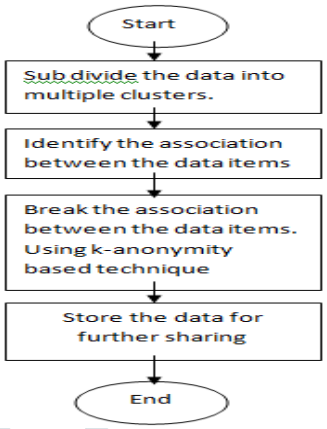
Step1 input the data from outsource to be shared on the network.

Step2 segment the data in rows and columns.

Step3 based on the features and similarity with k-anonymity technique replace the values with special symbols.

Step4 It will break the association between the multiple values and will break the knowingness amongst the data items.

IV. FLOWCHART



V. RESULTS AND ANALYSIS

5.1 NETWORK CONFIGURATION

Table 1 Network Configuration

SIMULATION PARAMETERS	
COVERAGE AREA	1000m x 1000m
PROTOCOLS	AODV
NUMBER OF NODES	20
SIMULATION TIME	50 seconds
TRANSMISSION RANGE	250m
MOBILITY MODEL	RANDOM WAY POINT MODEL
LOAD	5 Kb-UDP Packets
MOBILITY SPEED(variable)	(4,8,0.5,1)Seconds
TRAFFIC TYPE	CBR,UDP,FTP,TCP
PACKET SIZE	512 Kbps
PAUSE TIME	10,20,30,40,50

5.2 PARAMETERS TAKEN

1. **Time.** It means Total time taken for the sharing of the data between two remote devices connected through internet.
2. **Energy.** It is the Total energy required for the total communication.

5.3 COMPARISON FOR TIME TO ACCESS

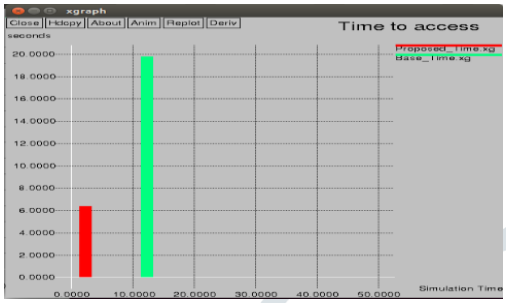


Fig. 2 Comparison of Time of Access

Fig. 2 shows the comparison of time of access for base and proposed algorithm. Because proposed scheme uses the K-Anonymity based scheme. Whole data will be stored with kth level anonymization. So while sharing the data less time will be required for sending and receiving the data. Each data item owner is hidden using k-anonymity based scheme. But in the existing scheme the username and password is asked from the user. That type of scheme is time consuming and also can be attacked at various levels.

5.4 COMPARISON FOR ENERGY

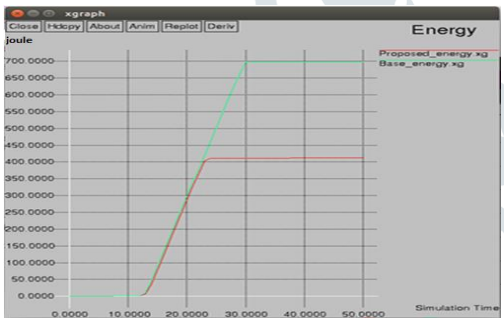


Fig. 3 Energy Comparison

Fig. 3 shows the Energy comparison between the base and proposed scheme. The Energy in terms of battery in case of proposed scheme is less. Because for every time data access there is no requirement to ask username and password. Which will save large energy. In result less cost for the sharing of the data. K-anonymity based scheme is better scheme in making data more secured to access

VI. CONCLUSION

Society is experiencing exponential growth in the number and variety of data collections containing person-specific information as computer technology, network connectivity and disk storage space become increasingly affordable. Data holders, operating autonomously and with limited knowledge, are left with the difficulty of releasing information that does not compromise privacy, confidentiality or national interests. In many cases the survival of the database itself depends on the data holder's ability to produce anonymous data because not releasing such information at all may diminish the need for the data, while on the other hand, failing to provide proper protection within a release may create circumstances that harm the public or others. Work in this area ensures that the recipient of information has the authority to receive that information. While access control and authentication protections can safeguard against direct disclosures, they do not address disclosures based on inferences that can be drawn from released data.

The more insidious problem in the work that is the subject of this paper is not so much whether the recipient can get access or not to the information as much as what values will constitute the information the recipient will receive.

VII. FUTURE WORK

Current research work includes the security to the data being shed on the network. Various nodes inter changing the data will be secured from users identity disclosure. In future another authentification mechanism for real time application can be performed using k level anonymization .

REFERENCES

[1] Meng-Shiuan Pan and Shu-Wei Yang," A Lightweight and Distributed Geographic Multicast Routing Protocol for IoT Applications", 7 November 2016, COMPNW 6048

[2]Renato F. Fernandes Jr. *, Dennis Brandão," Proposal of Receiver Initiated MAC Protocol for WSN in urban environment using IoT ",IFAC-PapersOnLine 49-30 (2016) 102–107.

[3] Biplob R. Ray, Jemal Abawajy, Morshed Chowdhury, Abdulhameed A Alelaiwi," Universal and secure object ownership transfer protocol for the Internet of Things", FUTURE 3338.

[4] Ruhul Amin, Neeraj Kumar, G.P. Biswas, R. Iqbal, Victor Chang "A light weight authentication protocol for IoT-enabled devices in distributed Cloud Computing environment", 20 December 2016.
[5] Benjamin Aziz," A Formal Model and Analysis of an IoT Protocol",2016 Vol 4 ,120-134
[6] Tian D.,Dr.S.P.Setty,"Artificial Neural Network Based Decision on Parameter Values in AODV to Enhance the Performance of Mobile Ad Hoc Networks", Vol. 6(5),pp 375-4377, 2003.
[7] Zhenqiang Y. ," Mobility prediction in mobile ad hoc networks using neural learning machines", Simulation Modelling Practice and Theory vol. 66 pp. 104–121,2003.
[8] Abolhasan M. , Thomas Fevens," Neighborhood-based interference minimization for stable position-based routing in mobile ad hoc networks", Vol. 4,pp. 234-40,2003.
[9] Ulas C. Kozat, Jong-hwan Kim," Efficient content delivery in mobile ad-hoc networks using CCN", vol. 3,pp.1–19,2003.
[10] Lin guolong ," MSAR: A metric self-adaptive routing model for Mobile Ad Hoc Networks", Journal ofNetworkandComputerApplications , vol. 68,pp. 114–125,2004.
[11] D.P.F. Mo¨ller," Introduction to the Internet of Things", 2016, Springer International Publishing Switzerland, 978-3-319-25178-3_4
[12] Deepak Mishra and Swades De," Energy Harvesting and Sustainable M2M Communication in 5G Mobile Technologies", 2016, Springer International Publishing Switzerland, 978-3-319-30913-2_6
[13] Shulong Wang, Yibin Hou, Fang Gao1 and Xinrong Ji," Access Features Analysis of Things in the Internet of Things", 2016, IEEE, 978-1-5090-2534-3
[14] Archudha Arjunasamy, Thangarajan Ramasamy," A Proficient Heuristic for Selecting Friends in Social Internet of Things", 2016, ISCO, 3294794
[15] Minchul Shin, Inwhee Joe," Energy management algorithm for solar-powered energy harvesting wireless sensor node for Internet of Things", 2016, IET Commun., Vol. 10, Iss. 12, pp. 1508–1521
[16] Kun Wang, Xin Qi, Lei Shu, Der-Jiunn Deng, and Joel J. P. C. Rodrigues," Toward Trustworthy Crowdsourcing in the Social Internet of Things", 2016, IEEE, 1536-1284
[17] Dongsik Jo and Gerard Jounghyun Kim," ARIoT: Scalable Augmented Reality Framework for Interacting with Internet of Things Appliances Everywhere", 2016, IEEE Transactions on Consumer Electronics, Vol. 62, No. 3
[18] David Linthicum," Responsive Data Architecture for the Internet of Things", 2016, IEEE, 0018-91 62
[19] Jun Qi, Po Yang, Martin Hanneghan, Dina Fan, Zhikun Deng, Feng Dong," Ellipse fitting model for improving the effectiveness of life-logging physical activity measures in an Internet of Things environment", 2016, IET Netw., Vol. 5, Iss. 5, pp. 107–113
[20] Haojun Huang, Jianguo Zhou, Wei Li, Juanbao Zhang, Xu Zhang, Guolin Hou," Wearable indoor localisation approach in Internet of Things", 2016, IET Netw., pp. 1–5
[21] Zhaoyang Zhang, Xianbin Wang, Yu Zhang, and Yan Chen," Grant-Free Rateless Multiple Access: A Novel Massive Access Scheme for Internet of Things", 2016, IEEE COMMUNICATIONS LETTERS, VOL. 20, NO. 10
[22] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the Internet of Things: A Review," 2012, in Proc. of Intl. Conf. on Computer Science and Electronics Engineering (ICCSEE), vol. 3, no., pp. 648-651
[23] J. Granjal, E. Monteiro, and J. S´a Silva, "Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues," 2015, IEEE Communications Surveys & Tutorials Volume: 17, Issue: 3, pp. 1294-1312
[24] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey", Computer Networks, Vol.54, 2010, p. 2787-2805
[25] O. Novo, N. Beijar, M. Ocak, J. Kjallman, M. Komu, and T. Kauppinen," Capillary Networks – Bridging the Cellular and IoT Worlds," 2015, IEEE 2nd World Forum on Internet of Things