Optimized Data Collection and Computation using Internet of Things (IoT)

Bharath Kumara, S. Anantha Padmanabhan

Abstract: IOT is one of the standard data transfer technique used in day today applications like health monitoring, industrial data collection and in home security system. Security in data transmission is one of the major concerned research area in IOT. The existing methodologies is secure data transmission is not provided full fledge privacy for data collection and transmission. Hence, this paper proposed a new methodology to compute and secure the valuable data. The methodology to optimize the data collection is achieved in two different steps. The noise is added to original data in the first step to secure the original data. In second step different nodes in the network/clustered average data will be computed. Later the research methods is implementing to minimize the data loss. To show the performance of the optimal data collection and secure transmission we simulate different constraints of the network parameters and compared with existing methods. The developed algorithm proved that it is one of the better data collection technique.

Index Terms: IoT, Security, Data Collection, Throughput.

I. INTRODUCTION

As internet technology evolution, IOT is also trending the technology and market. Through the internet any devices can be controlled in real time. IoT can be able to connect smart phones, Wearable Devices etc. IoT is capable of interconnecting the world wide objects to collect the data and sends the data too. Architecture of the IoT mainly divided into four blocks.

Sensors: Sensors are used to sense the data for the required applications.

IoT Gateways: An intermediate component work between internal and external to the network. Gateway collects the information from network and forward the same to global.

Cloud server/storage: During large data collection huge amount of storage required. Storing the data physically is more economic. Hence cloud storage is used.

End User: User can able to access and retrieve the data at any place using electronic devices like mobiles, personal computers etc. the accessed information is in the form of pie chart and bar graph.

IoT makes the data collection as more convenient. Sensor sense the data and process the data to next level. IoT having a feature to provide data tracking and monitoring. In several application like military and national issues IoT efficiently secure the data. Figure 1 shows the architecture of IOT.

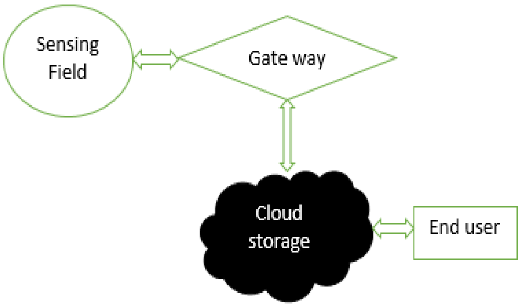

Figure 1: Architecture of IOT.

The cloud reserves the data for future use, and it will be utilized through the internetwork.

The methodologies in the past research have not an algorithm to secure the data efficiently and effectively. A privacy algorithm is require to secure the data at end- to- end. The authorization of channel is need to develop in future in this algorithm development.

II. LITERATURE

The IoT challenges and framework for industrial issues are discussed in [14]. The legal enforcement, privacy, trust and confidential issues are discussed in [15]. Many of the existing methodologies focused to detect the network layer and application factors [5] [4]. The clustering and statistics trust management is achieved through event of interest mechanism [8, 9].

The proposed algorithm in [13] explains the methods for analyze the malicious nodes and its performance. The spatial pattern is designed with the help of linear aggregation and distribution of non-homogenous measurements. The method is not efficiently work for multiple event attacks. RCDA method proposed a method to collect the data in multi event, but the communication cost is too high. The data encoding is very complex task.

Differential fast transfer method proposed a method to overcome RCDA issues. Instead of sending raw data different data is sent to the cluster head [16].

a. Contribution of this research:

The aim of the research is to develop a methodology for sharing the data among the user using IOT.

The proposed methodology working on two phase calculation and aggregation.

1. Addition of noise to secure the data.
2. Data computation using average of all the data in the field.

Manuscript published on 30 August 2019.
***Correspondence Author(s)**

Mr.Bharath Kumara, Resarch scholor and Assistant professor Dept. of ECE, VTU Belgaum / Ramaiah University of applied science/ Bangalore, India.

Dr. S. Anantha Padmanabhan, Dept. of ECE, VTU Belgum/Gopalan College of Engineering/ Bangalore, India.

Retrieval Number: J90470881019/19©BEIESP
DOI: 10.35940/ijitee.J9047.0881019
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

3. Proposing the improvised method to optimized the clusters issues.
4. Minimize the computation cost.

The paper is organized in such a way as follows: first discussion on background of IoT, data collection and its security. Secondly, discussion on literature on the existing methodologies. In third section we are discussing the proposed methodology and its related expressions. Further, the performance analysis of the proposed method. Lastly, the summary of the paper, future work of the project is explained. Then, it followed by the references.

III. PROPOSED METHODOLOGY

a. Network Model:

Consider the network which is connected as well as undirected graph, these graph are mainly composed of $x \in X$ various clusters $\{Cl_1, Cl_{2,} \dots \dots, Cl_x\}$, $[x]$ is denoted using the digit variable such as $1,2,3 \dots .x$. Let's assume that any graph $P = \{D, E\}$.Moreover in order to describe the network, here D= $\{cl_r, r = [x]\}$ and all the network are described through $E \subseteq DXD$. Moreover in case there exist any CE (Connection edge) in the given network between cl_r and cl_s then cl_s is the neighbor of $c\,l_r$. The neighbor is denoted by

X_r= $\{x_r \mid (x_r, x_s) \in E, \forall\, cl_s \in D\}$.

The average value computed in all the nodes is $\bigcup_{r=1}^{x} D_x$.Computation process is parted into two steps as Data collection and Average Computation. In first step the clusters gathers the data from D_x and Data Node is represented as: Z_u^r ∈ Real number,

$$Z_{DA}^r = \sum_{u \in D_x} Z_u^r \tag{1}$$

Z= $[Z_1^r, z_2^k, \dots \dots \dots, x_{n_k}^k]^T \in R^n$ is used as a vector for representing the data from D_r and the equation represented as:

$$Z_{DA}^r = 1^{Time} D^r \tag{2}$$

Let's assume that all these clusters have finished data collection before the equation 2 and equation 3 is Initial time of second steps.

$$time = IniT_0 \tag{3}$$

$$B_r(INIT_0) = \frac{x}{\sum_{i=1}^{x} x_i} Z_{DA}^r = \frac{x}{\sum_{i=1}^{x} x_i} 1^{Time} Z^r \tag{4}$$

Equation 3 depicts the start of second steps the equation 4 shows the initial value of the set cl_r at$INIT_0$.

$$B_r(time + 1) = M_{rr} B_r(time) + \sum_{cl_u \in X_r} M_{ru} B_u(time), t \geq INIT_{0,} \tag{5}$$

The equation 5 presents the updated states of the equation at the $time > INIT_0$. M_{ru} And M_{ru} are the weights.

Let's assume the weightsM_{ru} ,$1 <= r$, $u <= x$ which satisfies the below criteria such that there exist any positive constant $\delta \in (0,1)$ so that below three condition are satisfied.

- $\forall r, M_{rr}$
- M_{ru} is greater than 0 and it implies greater than δ
- $\forall u$, $\sum_{r=1}^{x} M_{ru} = 1$, $\forall r$, $\sum_{u=1}^{r} M_{ru} = 1$

b. Secure data reporting:

Due to the security concern, nodes refuses to send the raw data to the Clusters. Hence the intention is to provide the security by preserving the information. The noise is added with original information/data even soon after transmitting information to the cluster:

$$\tilde{Z}_u^r = Z_u^r + \zeta_u^r, \tag{6}$$

ζ_u^r is the Gaussian noise whose mean value is zero variance is σ^2.

$$\tilde{Z}_u^r = Z^r + \zeta^r \tag{7}$$

c. Security analysis:

When the data collection takes place the node collects and process the noisy data to the clusters. The Gaussian noise is used for creating the noisy data. In case if any outer body tries to interfere the data privacy of D_k^i the information regarding the noisy data can be determined through the Gaussian noise. In order to analyze the noisy process random function $f_1(.) : H \rightarrow H\ to$ to the data Z_r^u of node D_u^r

$$\tilde{Z}_i^r = f_1(Z_i^r) = Z_i^r + \zeta_i^r. \tag{8}$$

$M_1(D_u^r)$ is randomized function.

d. Improvised methodology:

The improvised data computation and security is signified with the expression. The method provide better accuracy with minimum radius.

$$\min_{\epsilon_u^r} \frac{\delta}{\sum_{r=1}^{x} x_r} \sqrt{\frac{1}{2c} \sum\nolimits_{r=1}^{Z} \sum\nolimits_{u=1}^{Z_r} \frac{1}{\epsilon_u^r}} . \tag{9}$$

c , δ and $\sum_{r=1}^{x}$ are the positive constant, hence the optimization problem gets transferred to finding the

Optimal solution i.e. minimization of $\sum_{r=1}^{x} \sum_{u=1}^{x_r} \frac{1}{\epsilon_u^r}$. Improvised methodology is given as

$$\min_{\epsilon_u^r} \sum\nolimits_{u=1}^{x_r} \frac{1}{\epsilon_u^r} . \tag{10}$$

IV. PERFORMANCE EVALUATION

The working of algorithm is verified with various network parameters and constrains to simulate the desired result. Malicious nodes are introduced from 10 to 40 with the simulated nodes of 100. Figure 2 shows the energy consumption versus simulation time graph.

Figure 3 shows the average number of dead nodes present when we introduce the malicious nodes. We can clearly observe from the graph if more quantity of malicious node in the network which will improves the energy consumption.

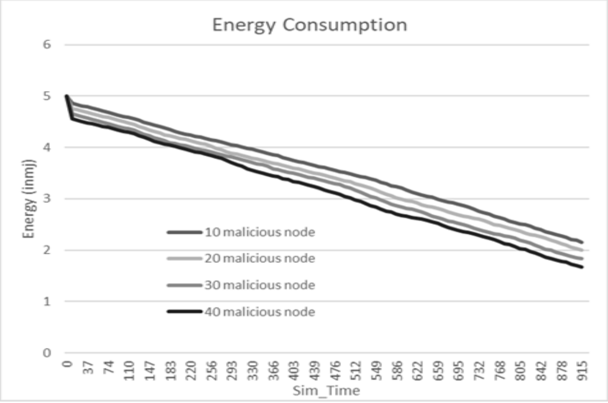

Figure 2: Energy consumption.

The analysis is the reflection of betterment in proposed methodology.

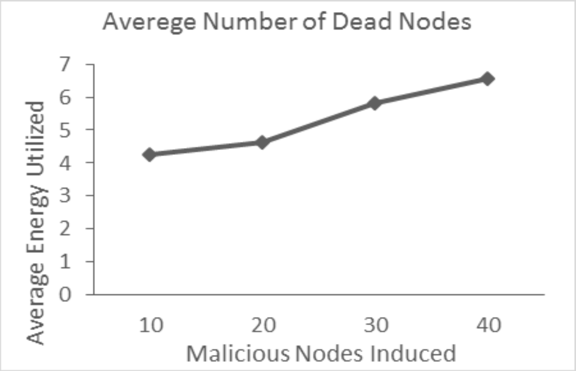

Figure 3: Average number of dead nodes.

i. **Comparative analysis:**

The comparison of existing method with the proposed method is analyzed in figure 4 and in figure 5. We can observe the packet identified by the earlier methods for 10 to 40 malicious nodes. In the proposed method 60 to 70 malicious nodes respectively.

The comparison is done based throughput, the rate of successful message delivered over the communication channel is high. The throughput is measured in bit per second. In proposed method the throughput is 0.555, to 0.1672. These values proved our suggested technique provides better performance.

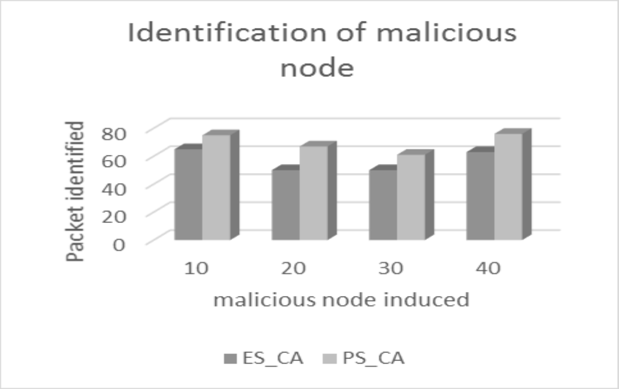

Figure 4: Comparison of malicious nodes.

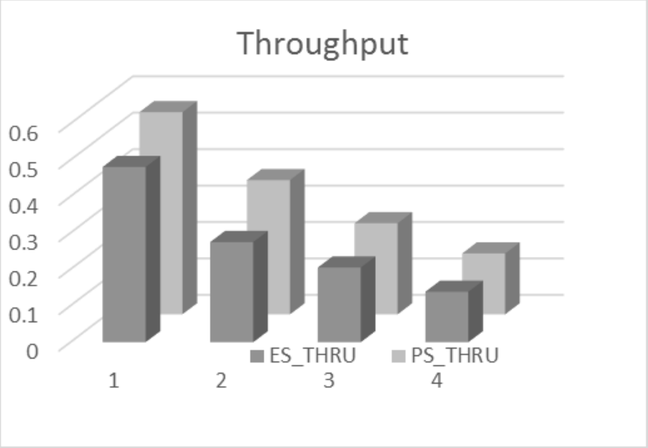

Figure 5: Throughput comparison.

IV. CONCLUSION

The suggested method in the paper for security and data collection in optimized way using IoT is a different technique compared to traditional techniques. The method is performed in two steps, in the primary steps addition of noise with average computed data in the cluster, secondly it transfer the data to the neighbored using the proposed algorithm securely. The performance is evaluated with consideration of malicious nodes and dead nodes. The throughput also compared with existing methodology and the proposed methodology performed better in it. All the performance parameters are plotted in graph. Though our algorithm performs very well when the malicious nodes are induced still it is interesting to observe that how it performs when more number of nodes are considered and how it performs with the other constraints.

REFERENCES

1. B. Dorsemain, J. Gaulier "Internet of Things: A Definition & Taxonomy" 9th, International conference on NGMAST, Cambridge, 2015, pp: 72-77.
2. G. Davis, "2020: life with 50 billion connected devices", ICCE, las vegas, NV-2018, pp: 1-2.
3. A. A. Abed, "Internet of Things (IoT): Architecture and design," *Al-Sadeq AIC-MITCSA*, Baghdad, 2016, pp: 1-3.
4. P. V. Dudhe, N. V. Kadam, R. M. Hushangabade and M. S. Deshmukh, "Internet of Things (IOT): An overview and its applications," ICECDS, *Chennai*, *2017*, pp: 2650-2653.
5. L. Krishnamachari, D. Estrin and S. Wicker, "The impact of data aggregation in wireless sensor networks," *Proceedings 22nd International Conference on Distributed Computing Systems Workshops*, Vienna, Austria, 2002, pp. 575-578.
6. R. Neisse, G. Steri and G. Baldini, "Enforcement of security policy rules for the Internet of Things," *2014 IEEE 10th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, Larnaca, 2014, pp. 165-172.
7. Z. Ling, K. Liu, Y. Xu, Y. Jin and X. Fu, "An End-to-End View of IoT Security and Privacy," *GLOBECOM 2017*, Singapore, 2017, pp: 1-7.
8. B. Yu, J. Wright, S. Nepal, L. Zhu, J. Liu and R. Ranjan, "IoT Chain: Establishing Trust in the Internet of Things Ecosystem Using Block chain," in *IEEE Cloud Computing*, vol. 5, pp. 12-23, Jul./Aug. 2018.
9. M. Alramadhan and K. Sha, "An Overview of Access Control Mechanisms for Internet of Things," 2017 26th ICCCN, Vancouver, BC, 2017, pp: 1-6.
10. Y. Sharaf-Dabbagh and W. Saad, "On the authentication of devices in the Internet of things," *2016 IEEE 17th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, Coimbra, 2016, pp. 1-3.

11. O. Arias, J. Wurm, K. Hoang and Y. Jin, "Privacy and Security in Internet of Things and Wearable Devices," in *IEEE Transactions on Multi-Scale Computing Systems*, vol. 1, no. 2, pp. 99-109, 1 April-June 2015.
12. D. Díaz-Sánchez, R. S. Sherratt, F. Almenarez, P. Arias and A. Marín, "Secure store and forward proxy for dynamic IoT applications over M2M networks," in IEEE Transactions on Consumer Electronics, vol. 62, no. 4, pp. 389-397.
13. N. Li, D. Liu and S. Nepal, "Lightweight Mutual Authentication for IoT and Its Applications," in *IEEE Transactions on Sustainable Computing*, vol. 2, no. 4, pp. 359-370, 1 Oct.-Dec. 2017.
14. L. Zhang, Y. Zhang, S. Tang and H. Luo, "Privacy Protection for E-Health Systems by Means of Dynamic Authentication and Three-Factor Key Agreement," in *IEEE Transactions on Industrial Electronics*, vol. 65, no. 3, pp. 2795-2805, March 2018.
15. Fan Wu, Lili Xu, Saru Kumari, Xiong Li, Jian Shen, Kim-Kwang Raymond Choo, Mohammad Wazid, Ashok Kumar Das, An efficient authentication and key agreement scheme for multi-gateway wireless sensor networks in IoT deployment, Journal of Network and Computer Applications, Volume 89, 2017, Pages 72-85,ISSN 1084-8045.
16. C. Liu *et al*., "Authorized Public Auditing of Dynamic Big Data Storage on Cloud with Efficient Verifiable Fine-Grained Updates," in *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 9, pp. 2234-2244, Sept. 2014.
17. J. Baek, Q. H. Vu, J. K. Liu, X. Huang and Y. Xiang, "A Secure Cloud Computing Based Framework for Big Data Information Management of Smart Grid," in *IEEE Transactions on Cloud Computing*, vol. 3, no. 2, pp. 233-244, 1 April-June 2015.
18. C. Liu, R. Ranjan, C. Yang, X. Zhang, L. Wang and J. Chen, "MuR-DPA: Top-Down Levelled Multi-Replica Merkle Hash Tree Based Secure Public Auditing for Dynamic Big Data Storage on Cloud," in *IEEE Transactions on Computers*, vol. 64, no. 9, pp. 2609-2622, 1 Sept. 2015.
19. Z. Yan, W. Ding, X. Yu, H. Zhu and R. H. Deng, "Deduplication on Encrypted Big Data in Cloud," in *IEEE Transactions on Big Data*, vol. 2, no. 2, pp. 138-150, 1 June 2016.
20. Goyal, Vipul & Pandey, Omkant & Sahai, Amit & Waters, Brent. (2006). Attribute-based encryption for fine-grained access control of encrypted data. Proceedings of the ACM Conference on Computer and Communications Security. 89-98. 89-98. 10.1145/1180405.1180418.
21. Y. Yang, X. Liu and R. H. Deng, "Lightweight Break-Glass Access Control System for Healthcare Internet-of-Things," in *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3610-3617, Aug. 2018.
22. K. Yang, X. Jia and K. Ren, "Secure and Verifiable Policy Update Outsourcing for Big Data Access Control in the Cloud," in *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 12, pp. 3461-3470, 1 Dec. 2015.
23. Y. Miao, J. Ma, X. Liu, X. Li, Q. Jiang and J. Zhang, "Attribute-Based Keyword Search over Hierarchical Data in Cloud Computing," in *IEEE Transactions on Services Computing*.
24. P. Xu, H. Jin, Q. Wu and W. Wang, "Public-Key Encryption with Fuzzy Keyword Search: A Provably Secure Scheme under Keyword Guessing Attack," in *IEEE Transactions on Computers*, vol. 62, no. 11, pp. 2266-2277, Nov. 2013.
25. Keshav, S. padmanabhan “An overview of IoT, and services” national conference on IoT technologies, 2019, Hassan, PP: 20-24.

AUTHORS PROFILE

Mr. Bharath Kumara, B.E in ECE, M.Tech in DECS, PGDHRM, E-MBA, pursuing Ph.D, in Electronics and Communication Engineering at VTU, Belgaum. Currently working as an Assistant Professor in the dept. of Electronic and Communication Engineering, RUAS, Bangalore. Many paper is published in standard international journals, on the research area of Wireless sensor networks. Life member of ISTE, Delhi. I am a writer of kannada novel, artist, director, and producer kannada film industry. My email- bharathkumara87@gmail.com.

Dr. S. Anantha Padmanabhan Working as a Professor in the Department of ECE at Gopalan College of Engineering and Management, Bangalore. He also published many articles in reputed journals and International Conference. He obtained Ph.d from Anna university chennai in the field of Digital Signal Processing and his area of research are signal processing, control systems, field theory and electrical machines.