Journal of ISMAC (2019)
Vol.01/ No. 02, June 2019, pp: 81-91 ISSN: 2582-1369 (online)
DOI: https://doi.org/10.36548/jismac.2019.2.001

# SECURITY AND PRIVACY PRESERVING OF SENSOR DATA LOCALIZATION BASED ON INTERNET OF THINGS

**Dr. S. R. Mugunthan,**
Associate Professor,
Department of Computer Science and Engineering,
Sriindu college of Engineering and Technology,
Sheriguda, Hyderabad, India.
Email: srmugunth@gmail.com

**Abstract:** The internet of thing which is a prominent network for the transmission of valuable information over the internet, by tracking, computing and refining handles large scale of information as it being engaged in a wide range of application, ranging from the home to industries and government concerns. It provides with the capability of the transmitting information's over internet without the interference of the humans. Despite its potentials, the internet of the things suffer from limited storage facilities and seek the services of the cloud to assist with the storage provisions for the data that are being sensed. Though cloud is facilitated with the enormous resources of storage, the placing of the sensed data into the cloud would be energy consuming and prone to the security threats causing illegal access. So the paper proposes the multi-objective optimization technique based on the NDSGA-II to present with the optimal solutions for the energy and the security issues involved in the locating of the data into the cloud. The proposed method is validated using the network simulator-II to detail its efficiency, in terms of energy consumption, security, network longevity, and resource utilization.

**Keywords:** Internet of Things, Sensed data, cloud-data centers, energy consumption, security, NDSGA-II

## 1. Introduction

The internet of things strives for the creating a world that is fully connected enabling even the tangible object that are connected with the internet to communicate. It is the incorporation of smart objects of differing types, with the ability to gather information from the physical environment around, compute it, filter it and transmit it over the internetwork [2]. This makes the internet of things to cause dramatic alterations in the everyday life of the people almost in all fields from home, transportation, industries, hospitals, military, entertainment, media, to government conversations etc. [9]. This swift progress of the internet of things has caused collection and transmission of the data in the large scale [4] helping in the tracking, devising, operating, controlling and smart decision making [5] has made it a promising paradigm in wide range of the applications. The data collection of the internet of things is supported by the wireless sensor networks that act as the back bone of the IOT helping in sensing the enormous data

Journal of ISMAC (2019)
Vol.01/ No. 02, June 2019, pp: 81-91 ISSN: 2582-1369 (online)
DOI: https://doi.org/10.36548/jismac.2019.2.001

from the internet connected tangible objects around. The limitations of the internet of things devices in terms of storage, pushes them for an external storage device to help them in storing the sensed data for the future use. The cloud seems to provide with the improved and the scalable pay as you go storage service for the internet of things as they are equipped with more resources that facilitate computing and communication along with the storage facilities. Despite the promising nature of the cloud storage services for the internet of things, the cloud data centers that assist in the storage of the internet of things suffer from the major issues that is the energy consumption that causes more carbon emission and the security provisioning that maintains the secrecy of the particulars of the persons preventing the illegal access. The researches proceeded with the aim of providing frame work that is efficient in the conserving the energy results with the demerit of improper resource usage along with the security issues. The researches with the concept of privacy provisioning for the data located in the cloud causes enormous energy consumption that results with the reduce in the longevity of the network [3]

So the placing or locating the data from IOT to the data centers of the cloud requires, procedures that are proficient in terms of energy enhancing the network longevity and secured preventing illegal access against the sensed data that stored in the data centers of the cloud.

The paper proposes a multi-objective optimization based on the usage of the resource, energy meeting all the privacy constraints of the data centers in the location of the sensed data into cloud utilizing the non-dominated sorting genetic algorithm –II and validates the same with the network simulator-II to detail the efficiency and the QOS of the proposed method.

The remaining paper, explains the related works based on the locating of the sensed data into the cloud and the privacy preserving methods available in section. 2 and the proposed work that achieves the optimal solution in terms of energy and security for the locating of the sensed data into the cloud is explained in the section.3, the validation of the proposed method to evince its proficiency is proceeded in the section 4 and the conclusion detailing the summary of the work done is presented in the section.5

## 2. Related Works

Ding et al [1], the paper proposes the survey on the internet of things its data fusion methodologies and the security privacy issues for the data fusion in IOT and includes the future enhancement to be proceeded with along with the research challenge involved in it. Wazid, et al [2] the paper presents the authentication schemes that are necessary for the cloud driven IOT services, with the challenges incurred for the research enhancement in the future involving the authentication scheme along with the available security protocols. Xu et al [3] the block chain scheme for data

Journal of ISMAC (2019)
Vol.01/ No. 02, June 2019, pp: 81-91 ISSN: 2582-1369 (online)
DOI: https://doi.org/10.36548/jismac.2019.2.001

protection of the large-scale medical industry is proposed to avoid, the leakage in the private information reserved in the cloud computing that works for the internet of things. , Liu, et al [4], the paper proposes the privacy of the data accumulated for an individual by maintaining in its raw state and making it unclear with the other data accumulated, to provide complete protection by making the client naïve on the information gathered. He et al [5] the paper propose the sector based random routing for the wireless-sensor networks that takes the essential part in the internet of things to put an end to the problem of the privacy in the source localization. Wang et al [6] the paper proposes the privacy scheme using the CTD and BRP method to secure the location of the source thereby reducing the energy consumption and prolonging of the network longevity in the wireless sensor networks that work for the IOT. Luceri, et al [7] the enormous data gathered in the internet of things is provided with the security model inside the network by proposing the model that is the enrolled crowd sensing model. Conti et al [8] the paper involves the discussion of the internet of things and challenges present in them and later address the available research's to tackle with the present challenges in the internet of things. Sarwar, et al [9] the paper present the survey on the IOT privacy considering including the analysis on the privacy issues in the IOT, the Challenges , the countermeasures and the deep analysis of the privacy preserving. Shen et al [10] the paper proposes a secure data uploading method for the smart home networks, since the privacy and the security are the major hindrance in the smart home systems along with the surety of the integrity of the data monitored eluding the malicious attacks that alter the data. Sastry, et al [11] the paper introduces the echo protocol for the purpose of secure location verification that never needs the synchronization, encryption/decryption and precise clocks, but can be installed only in the cheap mobile devices. Zhou et al [12] the paper proposes the security of the wireless body networks with the efficient biometric based key agreement

## 3. Proposed Work

The data sensed by the internet of things using wireless sensor network for various wide range of application, faces inadequacy in storage due to the huge inflow of data. This could be managing by shifting the data gathered to the cloud resource that provides a substantial storage area on the on- demand basis on pay per use. But the privacy and the energy consumed in the data centers of the cloud still remains as an issue. The paper address the issue of energy consuming and privacy in the locating of the sensed data in the cloud and reducing the same using the non-dominated sorting genetic algorithm. The Fig. 1 below details the process of the proposed method.

### 3.1. Problem Formulation

The huge data sensed using the wireless sensor networks requires a perfect place to store with for the future use. So the problem of storing the data meeting the privacy constraint ($P_c$) is along with the energy efficiency is addressed in the paper.

Journal of ISMAC (2019)
Vol.01/ No. 02, June 2019, pp: 81-91 ISSN: 2582-1369 (online)
DOI: https://doi.org/10.36548/jismac.2019.2.001

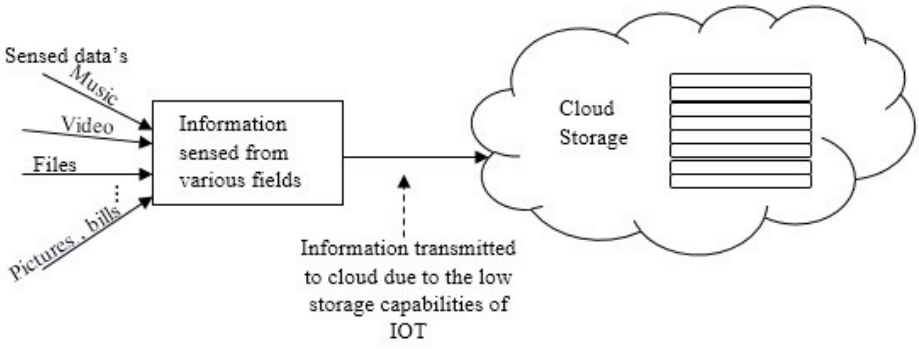


Fig.1 Placing Sensed Data into Cloud

The frame work to meet the multiple –objectives of the privacy constraint and the energy consumption of the placing the data into the data centers of the cloud is modelled as the graph $G(A, E)$ where $A = \{a_1, a_2, \ \dots \ a_n\}$ is the collection of the sensed data and the $E$ is the edge defining the multi-objective problem for all the sensed data that is the energy consumption ($E_c$) and the privacy conflicts ($P_c$) of the data sets.

The energy consumption of the cloud data center is modelled based on the energy consumption of the host ($H_{Ec}$) along with the energy consumption of the virtual machines ($V_{Ec}$) that are used or unused ($VM_{used}$ $or$ $VM_{unused}$ ) and the energy consumption of the switches ($S_{Ec}$). So the energy model for the storing of the data into the cloud is given as shown in the equation (1)

$$Total_{E_c} = H_{Ec} + S_{Ec} + V_{Ec} \quad (1)$$

The Privacy constraint based on the conflicts between the data set is modelled such that the conflicting or the incompatible data sets are provided with the separate location of storage (host) from the other dataset. The normal data set ($N_{DS}$) and incompatible data set ($IN_{Ds}$) stored in different location. The location of the incompatible data ($L_{IN_{Ds}}$) provided is computed using the following equation (2)

$$L_{IN_{Ds}} = \{d_x \mid d_x, \epsilon \, IN_{Ds}, x = \{\, 1,2, \dots \dots \dots, \mid IN_{Ds} \mid \}\} \quad (2)$$

So the non-dominated sorting genetic algorithm is utilized in identifying the optimal solution for locating of the data set with minimum energy consumption reducing and improving the security. Such that in a sensed data set with $\{d_1, d_2, d_3 d_{4,\dots\dots\dots\dots} d_n\}$ any set of sensed data conflict might be the $d_x$ or $d_{x-n}$ conflicting with the other data set is

Journal of ISMAC (2019)
Vol.01/ No. 02, June 2019, pp: 81-91 ISSN: 2582-1369 (online)
DOI: https://doi.org/10.36548/jismac.2019.2.001

assigned with the separate location (host) in order to reduce the conflicting increasing the privacy as shown in the Fig.2

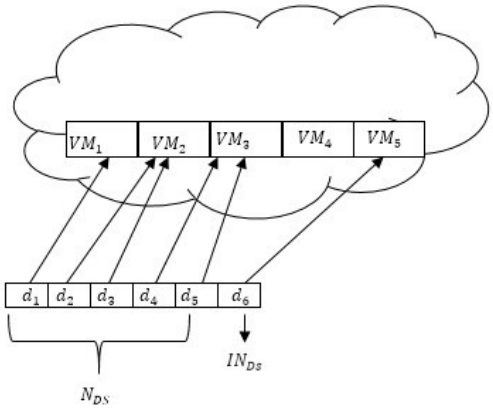


Fig .2 Storage Provision of Conflicting Data set

### 3.2. Non- Dominated Sorting Genetic Algorithm for Data locating of Sensed Data

The NDSGA-II is a searching algorithm that presents the non-dominated optimal solutions for the multi- objective optimization problem of the sensed data localization into the cloud. The process beginning with the initialization of the population, in this paper recommended to be the data location strategies, selection cross over and the mutation is done to identify the elite location strategy reducing the energy consumption and avoiding the privacy conflict by separating the conflicting data set into different host.

The steps involved in the process of selecting the elite data placement strategy reducing the energy and the privacy conflict is as follows.

Step 1: Initialize population with, each individual in the population representing the location scheme for the sensed data of the internet of devices.

Step 2: Evaluates for the fitness of the objectives with $Min(Total_{E_c})$ and $Min\ (P_c)$

Step 3: Sorts out the placement strategies based on the Non-dominated Sorting.

Step 4: The individuals sorted with the extreme values are assigned with larger distance to set them aside for the next evaluation using $\sum_{ob=1}^{2} \frac{\gamma_{ob}^{s+1} - \gamma_{ob}^{s-1}}{\gamma_{ob}^{max} - \gamma_{ob}^{min}}$ , Where the S is the optimal solution with the function value $\gamma$ and $l$ is the solution set, and 'ob' is target of the solution.

Step 5: Select the appropriate individuals in forming the new population.

Step 6: perform cross over and Mutation with the$Cross\ over\ rate = 7$, and the $Mutation\ Rate = .5$

Step 7: Evaluate Fitness $Min\ (H_{Ec} + S_{Ec} + V_{Ec})$ and $Min\ (P_c)$

Journal of ISMAC (2019)
Vol.01/ No. 02, June 2019, pp: 81-91 ISSN: 2582-1369 (online)
DOI: https://doi.org/10.36548/jismac.2019.2.001

Step 8: Integrate the new and the parent population and sort the population based on the elitism.

Step 9: Select Elite individuals.

Step10: Terminate if termination criteria met.

Step11: Else GOTO Step 5

The above steps in NDSGA-II is utilized in identifying the locating schemes with minimum energy and segregating the elite location for the sensed data, reducing the conflicting between the sensed data that are gathered. Thus improving the energy consumption for the locating of the data and making it privacy aware by segregating the location of $N_{DS}$ and $L_{IN_{Ds}}$ , enhancing the security for the sensed data located in the data centers for the cloud. The fig.3 gives the flow chart of the proposed method of locating .

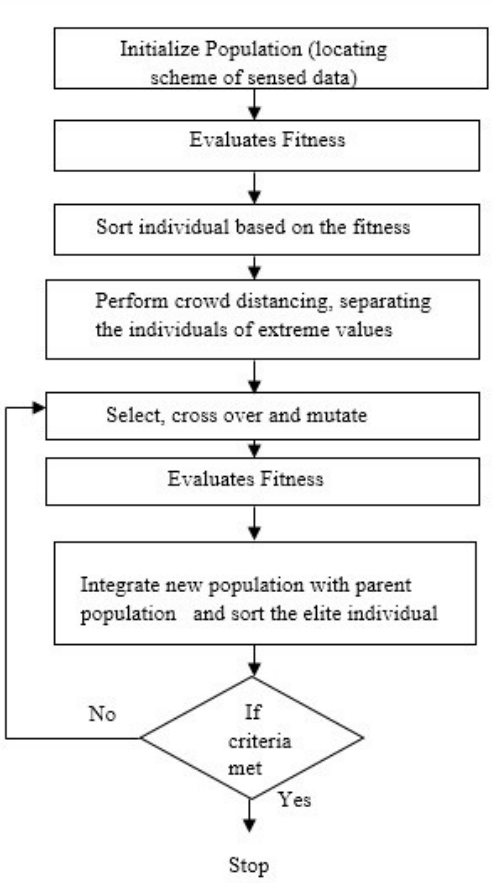


Fig .3 Proposed Flow Diagram

## 4. Result Evaluation

Journal of ISMAC (2019)
Vol.01/ No. 02, June 2019, pp: 81-91 ISSN: 2582-1369 (online)
DOI: https://doi.org/10.36548/jismac.2019.2.001

The proposed method of data locating with the NDSGA-II following the fat-tree topology is simulated in the network simulator-II, for varying number of data sets, that are sensed were the sensed data sets vary from 100 to 500, in the simulation area of 1000 *1000 sq. units, and the simulation time with the 100 seconds, the proposed method utilizing the non-dominated sorting genetic algorithm is compared with the previous methods of used in locating , to identify the efficiency of the proposed method. The table.1 below gives the parameters involved in the simulation.

Table. 1 Simulation Parameters

| Parameter | Value |
|---|---|
| Total number of data set | 100-500 |
| Simulation Area | 1000*1000 sq. units |
| Simulation time | 1000 seconds |
| Topology | Fat –tree topology |
| Initial Energy | 100 Joules |
| Cross over rate | 7 |
| Mutation rate | .5 |
| No.of population | 5 |

The Fig.4 below shows the energy consumption of the data centers of the cloud when engaged with the proposed method of non-dominated sorting genetic algorithm and the comparison with the previous method for varying number of data sets. The energy consumption of the proposed method in comparison with the other methods of genetic and PSO to arrive at an optimal solution is very much improved.

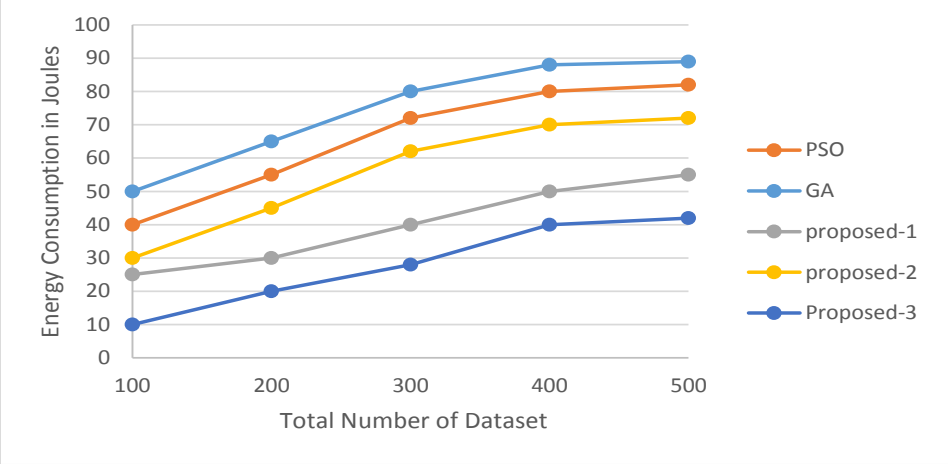


Fig. 4 Energy Consumption

Journal of ISMAC (2019)
Vol.01/ No. 02, June 2019, pp: 81-91 ISSN: 2582-1369 (online)
DOI: https://doi.org/10.36548/jismac.2019.2.001

The Fig. 5 below shows the simulation results for the enhanced lifetime of the network, the data placement scheme that enhances the energy consumption, improves the longevity of the network. The figure shows the longevity of the network achieved by the proposed system in comparison with the other methods of data locating schemes based on the genetic algorithm and the particle swarm optimization. The proposed shows 37.2% improvement compared to the genetic algorithm and 27.8% improvement compared to the particle swarm optimization.


Fig. 5 Network Lifetime

The data placement scheme using the non-dominated genetic algorithm-II, provides with the optimized method of resource utilization, as the utilization of the resources are the key to manage the resource provision of the cloud based on the proposed method provides with the maximum resource utilization ($R_U$), with the average resource utilization as shown in the equation (3)

$$R_U = \frac{1}{S_o} \sum_{N=1}^{n} R_{U_N} \tag{3}$$

Where, $S_o$ the space occupied by the physical hosts and the $N$ is the total number of physical hosts available, the Fig. 6 below shows the simulation results obtained for the resource utilization based on the proposed method of non-dominated sorting algorithm-II. The comparison with the other methods of data locating schemes with the genetic and the particle swarm evinces the efficiency of the proposed method in terms of the resource utilization.

Journal of ISMAC (2019)
Vol.01/ No. 02, June 2019, pp: 81-91 ISSN: 2582-1369 (online)
DOI: https://doi.org/10.36548/jismac.2019.2.001


Fig. 6. Resource Utilization

The data locating separating the$IN_{DS}$ and placing them on a different VM and placing the rest of the dataset that are normal $N_{DS}$ into a separate host, ensures the privacy of the data being stored into the cloud, improving the security of the cloud, so the proposed method shows enhanced security by preventing the private data's from being accessed by the unauthorized persons. The Fig.7 below shows the simulation results for the security provision of the private data's from being affected by the unauthorized access by placing the conflicting data sets into a separate host. The comparison of the proposed method over the other prevailing method of data locating shows the proficiency of the proposed NDSGA-II based data locating.

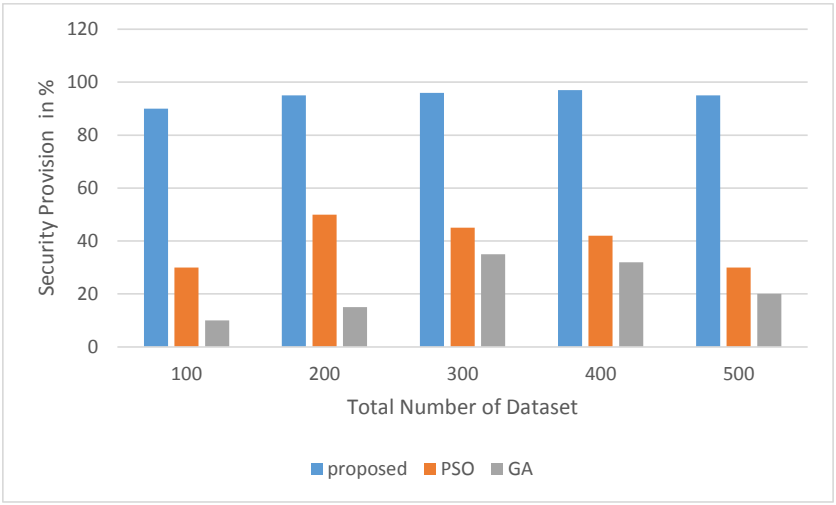


Fig. 7 Security Provisioning

Journal of ISMAC (2019)
Vol.01/ No. 02, June 2019, pp: 81-91 ISSN: 2582-1369 (online)
DOI: https://doi.org/10.36548/jismac.2019.2.001

Thus the proposed method using the, non-dominated sorting genetic algorithm for the data locating scheme of the sensed data, shows much improved energy and resources utilization with the security provision , by placing the $IN_{Ds}$ and the $N_{DS}$ in different hosts. The results obtained for the proposed data locating schemes based on the non-dominating sorting genetic algorithm, and the other methods of data locating based on the genetic and the particle swarm optimization show that the proposed method based on the, non-dominated sorting genetic algorithm provides a better quality of service in terms of$E_C$, $P_C$ , $R_U$ and network lifetime than the other methods for varying number of data sets.

## 5. Conclusion

The paper address the problem of locating the data sensed from the various application into the cloud, optimizing the energy consumption of storing the data into the cloud and elude the illegal access by, proper placement of the conflicting and the non-conflicting in the separate hosts. This process of data locating is based on the non-dominant sorting genetic algorithm-II to arrive at an optimal solution to maximize the quality of service by minimizing the energy consumption, maximizing the resource utilization and enhancing the security by protecting the privacy of the data set by storing the $IN_{Ds}$ and the $N_{DS}$ in different hosts. The further evaluation using the network simulator-II, provides with the efficiency of the proposed method of data locating compared to the prevailing methods. In future the paper is proceed with the optimization providing the optimal solution reducing the access time of the virtual machines.

## References

[1] Ding, Wenxiu, Xuyang Jing, Zheng Yan, and Laurence T. Yang. "A survey on data fusion in internet of things: Towards secure and privacy-preserving fusion." *Information Fusion* 51 (2019): 129-144.

[2] Wazid, Mohammad, Ashok Kumar Das, Rasheed Hussain, Giancarlo Succi, and Joel JPC Rodrigues. "Authentication in cloud-driven IoT-based big data environment: Survey and outlook." *Journal of Systems Architecture* 97 (2019): 185-196.

[3] Xu, Jie, Kaiping Xue, Shaohua Li, Hangyu Tian, Jianan Hong, Peilin Hong, and Nenghai Yu. "Healthchain: A Blockchain-based Privacy Preserving Scheme for Large-scale Health Data." *IEEE Internet of Things Journal* (2019).

[4] Liu, Yi-Ning, Yan-Ping Wang, Xiao-Fen Wang, Zhe Xia, and Jing-Fang Xu. "Privacy-preserving raw data collection without a trusted authority for IoT." *Computer Networks* 148 (2019): 340-348.

[5] He, Yu, Guangjie Han, Hao Wang, James Adu Ansere, and Whenbo Zhang. "A sector-based random routing scheme for protecting the source location privacy in WSNs for the Internet of Things." *Future Generation Computer Systems* 96 (2019): 438-448.

[6] Wang, Hao, Guangjie Han, Lina Zhou, James Adu Ansere, and Wenbo Zhang. "A source location privacy protection scheme based on ring-loop routing for the IoT." *Computer Networks* 148 (2019): 142-150.

[7] Luceri, Luca, Felipe Cardoso, Michela Papandrea, Silvia Giordano, Julia Buwaya, Stephane Kundig, Constantinos Marios Angelopoulos et al. "VIVO: A secure, privacy-preserving, and real-time crowd-sensing framework for the Internet of Things." *Pervasive and Mobile Computing* 49 (2018): 126-138.

[8] Conti, Mauro, Ali Dehghantanha, Katrin Franke, and Steve Watson. "Internet of Things security and forensics: Challenges and opportunities." (2018): 544-546.

[9] Sarwar, Kinza, Sira Yongchareon, and Jian Yu. "A Brief Survey on IoT Privacy: Taxonomy, Issues and Future Trends." In *International Conference on Service-Oriented Computing*, pp. 208-219. Springer, Cham, 2018.

[10] Shen, Jian, Chen Wang, Tong Li, Xiaofeng Chen, Xinyi Huang, and Zhi-Hui Zhan. "Secure data uploading scheme for a smart home system." *Information Sciences* 453 (2018): 186-197.

[11] Sastry, Naveen, Umesh Shankar, and David Wagner. "Secure verification of location claims." In *Proceedings of the 2nd ACM workshop on Wireless security*, pp. 1-10. ACM, 2003.

[12] Zhou, Jun, Zhenfu Cao, and Xiaolei Dong. "BDK: secure and efficient biometric based deterministic key agreement in wireless body area networks." In *Proceedings of the 8th international conference on body area networks*, pp. 488-494. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2013.