PhD Research Proposal

Title: An Efficient Access Control and Tracking Method for Internet of Things (IoT) Data and Services

Applicant: Fahmida Hossain (fahmidacsedu@gmail.com)

Supervisor: Professor Joarder Kamruzzaman (joarder.kamruzzaman@federation.edu.au)

Abstract: In recent years, IoT device deployment and usage have been increased exponentially. These devices produce a vast amount of data every moment. However, the data owners (users) have limited control over accessing and tracking these data, especially future usages. Hence, an efficient method is needed to monitor the IoT-generated data. The method should be secure enough that maintain user's privacy and track data usage to avoid outrageous cyber threats, traffic analysis, online data thefts, and eavesdropping. This research proposes a secure and efficient access control and tracking technique for IoT data and services. In the proposed mechanism, users will have more control over their data and can abstractly track how their data is being used. The security constraints are met by integrating a lightweight encryption technique in the middleware of the proposed model. The model will also maintain a secure channel among the participating entities, e.g., manufacturers, users, cloud servers and related authorities such as the key generator. The proposed method will be examined by developing Android, iOS, Linux, and Windows applications. The performance of the proposed scheme will be evaluated in terms of scalability, power consumption, memory usage, space requirement, acquisition, time variance dependency, data processing cost, services for its users and embeddedness into physical systems. All these together will result in more sustainability, reliability and efficiency for IoT service and generated data.

Introduction: In the last few years, IoT device usages for different purposes are increasing exponentially [1]. The approximate structure of an IoT system consists of three sub-steps: (i) Hardware for sensing and communication; (ii) Middleware process for computing, analysis and data storage (iii) Application/tools for interpretation and visualization of service [2]. Overall, each IoT sub-process transferred a massive amount of data [3] which introduce several new technological challenges for the researchers, including connectivity, compatibility, standard, maintenance, efficiency and analysis. Although a significant portion of IoT-generated data is private, confidential, valuable and personal, the current IoT system provides limited control over accessing and tracking these data, especially their future usages [4, 5]. In addition, involvement of third parties in IoT systems creates an opportunity for attackers to eavesdrop, modify, and hack these valuable personal data [6]. Thus, this research proposes an efficient secured access control and tracking method for IoT data and service, where users have more control over their data and can abstractly track down data usages.

Research Description: The proposed research methodology is divided into the following five sub-stages (shown in Fig.1):

(i) *Collaboration, Processes and Application:* It includes business processes, individual process/action, reporting, analytic, and controlling.

(ii) *Abstraction:* This stage aggregate data and its access.

(iii) *Data Accumulation and Edge Computing:* This consists of the storage unit, encryption, data element, analysis and transformation.

(iv) *Communication and processing units:* Includes hardware and software for communication and processing.

(v) *Physical Devices:* It consists of the "Things" of IoT such as sensors, wearables and other intelligent devices.

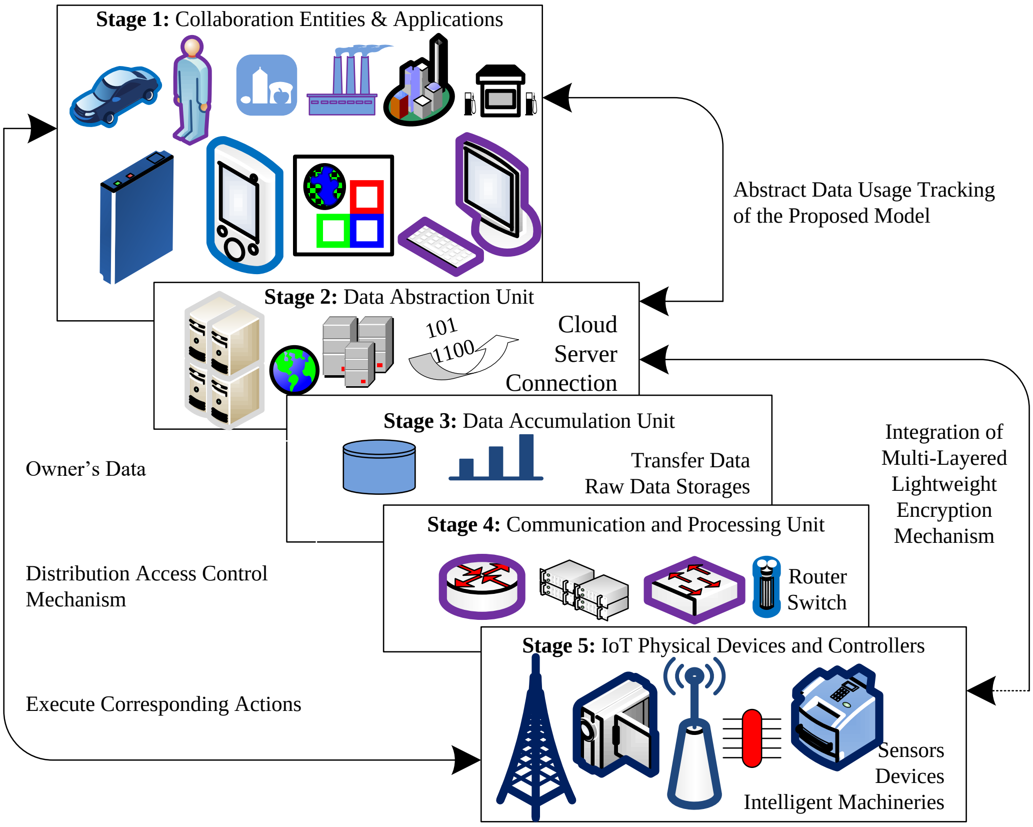
Stage 1: Collaboration Entities & Applications
Abstract Data Usage Tracking of the Proposed Model
Stage 2: Data Abstraction Unit
101
1100
Cloud
Server
Connection
Stage 3: Data Accumulation Unit
Transfer Data
Raw Data Storages
Owner's Data
Integration of Multi-Layered Lightweight Encryption Mechanism
Stage 4: Communication and Processing Unit
Router
Switch
Distribution Access Control Mechanism
Stage 5: IoT Physical Devices and Controllers
Execute Corresponding Actions
Sensors
Devices
Intelligent Machineries

Fig. 1: Architectural block diagram of the proposed model

The abstract data tracking of the proposed method will be involved stages 1 and 2; whereas, stages 3 to 5 will ensure secure collection, storage, and transfer of the data applying a lightweight encryption protocol. In the proposed model, control information and action are passed from stage 1 to 5 downward, data in both directions and policy in the upward direction. The working of the proposed model follows the reference structured provided for IoT by CISCO [7] that also includes a preference for tracking possibility, usages and related security issues.

Aims and Objectives: Aims and principal objectives of the proposed research are given below:

(a) Investigate enhancement possibilities of existing IoT paradigm through a systematic literature review targeting data access control, tracking and usages.

(b) Develop a lightweight encryption technique that hides data meaning from all IoT authorized entities, including service providers, key exchange authorities, cloud managers and eavesdroppers.

(c) Proposed a model to intergrade the developed encryption method with the IoT system.

(d) Evaluate the performance of the proposed approach and prove its significance concerning existing works.

Research Methodology and Timetable: The overall research work can be divided into six months long seven subparts. In the following table, a brief timeline-based research plan is provided:

Time Period	**Research Project Methodology**
Year One, 1st half (Months 1-to-6)	**i.** Review the literature and evaluate the performance of the existing IoT data and services control mechanisms, encryption techniques, modeling and measurement techniques. **ii.** Develop the protocol for **S**ystematic **L**iterature **R**eview (SLR).
Year One, 2nd half (Months 7-to-12)	**iii.** Automatic literature search, study filtration, data extraction and analysis for SLR. **iv.** Identify gaps in this domain and prepare a CORE A*/A journal paper based on SLR. **v.** Prepare for confirmation review, write report and confront seminar on it.
Year Two, 1st half (Months 13-to-18)	**vi.** Develop the proposed access control and tracking model.
Year Two, 2nd half (Months 19-to-24)	**vii.** Develop several cross platform applications to test the model prepare in (iv). **viii.** Prepare two research papers for publication based on (vi) and (vii).
Year Three, 1st half (Months 25-to-30)	**ix.** Develop the secure encryption protocols and integrate it with the model developed in sub-step-(vii).
Year Three, 2nd half (Months 30-to-36)	**x.** Evaluate the performance of the integrated proposed method (ix) **xi.** Prepare two CORE A*/A journal papers for publication based on (ix) and (x).
Year Four, 1sthalf (Months 37-to-42)	**xii.** Prepare for final review, write report and confront seminar on it. **xiii.** Write up and submission of Thesis for PhD degree.

Conclusion: This research proposes an efficient access controlling and tracking system for IoT data and services. The security and scalability of the proposed method are accomplished through the integration of a lightweight encryption technique. The research also aims to implement the proposed methods in cross-platform applications. Finally, we evaluate the performance of the proposed approach to prove its significance and supremacy over the existing approaches and point out its overall future impact.

References

[1] A. Chowdhury, G. Karmakar and J. Kamruzzaman, “The co-evolution of cloud and IoT applications: Recent and future trends”, Handbook of Research on the IoT, Cloud Computing, and Wireless Network Optimization, Edited by S. Singh and R.M. Sharma, IGI Global, 213-234, 2019, DOI: http://dx.doi.org/10.4018/978-1-5225-7335-7.ch011

[2] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of Things (IoT): A vision, architectural elements, and future directions”, In Future Gener. Comput. Syst., 29(7), 1645-1660, 2013, DOI: http://dx.doi.org/10.1016/j.future.2013.01.010

[3] M. M. Rashid, J. Kamruzzaman, M. M. Hassan, S. S. Shafin and Z.A. Bhuiyan, “Survey on Behavioral Pattern Mining from Sensor Data in Internet of Things,” IEEE Access, 8, 333.18-41, 2020, DOI: http://dx.doi.org/10.1109/ACCESS.2020.2974035

[4] Ahmed Banafa, “Three Major Challenges Facing IoT”, In IEEE Newsletters, 2017, Available at: https://iot.ieee.org/newsletter/march-2017/three-major-challenges-facing-iot.html (Last accessed: 22th May 2021).

[5] S. Seneviratne, Y. Hu, T. Nguyen, G. Lan, S. Khalifa, K. Thilakarathna, M. Hassan, and A. Seneviratne, “A Survey of Wearable Devices and Challenges”, In IEEE Communications Surveys Tutorials, 19 (4), 2573-2620, 2017, DOI: https://doi.org/10.1109/COMST.2017.2731979

[6] A. Khraisat, I. Gondal, P. Vamplew, J. Kamruzzaman, and A. Alazab, “A Novel Ensemble of Hybrid Intrusion Detection Systems for Detecting Internet of Things Attacks,” Electronics, 8(11), 1210, 2019, DOI: https://doi.org/10.3390/electronics8111210

[7] CISCO, “Building the Internet of Things”, 2018 Available at: https://www.cisco.com/c/dam/global/en_ph/assets/ciscoconnect/pdf/bigdata/jim_green_cisco_connect.pdf (Last accessed: 22th May 2021).