Scientific Research Publishing

Journal of Information Security, 2026, 17(1), 19-24
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

To Preserve Privacy for Smart Home Security System in Cloud Computing

Depeng Li

Department of Information and Computer Sciences, University of Hawaii at Manoa, Honolulu, HI, USA
Email: depengli@hawaii.edu

How to cite this paper: Li, D.P. (2026) To Preserve Privacy for Smart Home Security System in Cloud Computing. *Journal of Information Security*, **17**, 19-24.
https://doi.org/10.4236/jis.2026.171002

Received: October 7, 2024
Accepted: January 11, 2026
Published: January 14, 2026

Abstract

In smart home security system, privacy preservation is highly demanded. Nowadays, security methods such as cryptographical schemes are deployed to protect privacy. However, current systems do not provide any formal privacy model. Therefore, neither a privacy guarantee nor quantification for the privacy loss can be offered. In this paper, a few privacy-related questions have been raised. A novel privacy framework has been proposed that partially answers these questions by utilizing a set of theoretical models, e.g., the hidden Markov model, differential privacy, and information flow. Finally, the e-Lock state changes in the smart home are used as a case study. This paper intends to construct a framework which mainly focuses on theoretical analyses. The development of this system is out of the scope.

Keywords

Electronic Lock, Privacy Model, Privacy Preservation

1. Introduction

Nowadays, smart devices such as sensors and actuators have been extensively deployed in the smart home system. These devices have communication capability, which lets the house user remotely control automated electronic devices by entering a single command or a PIN number [1]. To save time or energy, sometimes, house users prefer to hire third parties, such as home security companies that provide 24/7 security protection services. However, the participation of the sensing application and the security company could potentially leak the privacy of the house users. Actually, without well-designed privacy preservation solutions, it is possible that private data is misused.

The privacy leakage for smart home [2]—even for very simple appliances such as electronic locks (e-Lock) [3]—is a potential challenge. It increasingly affects all

house users, given the fact that captured private data can be misused to infer personal activities. The insight is based on the observation that some intermittent activities, such as e-Lock switched on/off, could possibly infer personal absence/presence at the smart home.

A false alarm attack system in [3] is studied, which is launched against the most popular and commercially endorsed electronic lock. However, in the context of smart home security monitoring system, privacy preservation and privacy analyses (e.g., [4]) for e-Lock have not been presented. More importantly, it lacks a formal model of privacy analysis—privacy guarantee and quantitative evaluation are desirable. The pertinent privacy-related questions should be addressed regarding time-series e-Lock state data:

1) How much privacy is lost, and to what extent if all e-Lock states in smart home are open for access?

2) If perturbation methods which introduce uncertain noise to true personal data are deployed, could aggregator still query the leakage of privacy?

3) If the aggregator (e.g., server or the cloud of the security company) is not trusted, could we protect the privacy by an access control scheme based on information flow?

Our contributions: we propose a theoretical privacy framework to analyze the privacy leakage through accommodating fundamental functionality, e.g., sharing/hiding, perturbation and access control for aggregated time-series e-Lock state dataset for smart home system stored in cloud computing. We not only carefully study potential privacy inference but also try to address corresponding concerns about privacy loss in the case of the true dataset, of the distorted dataset and of the dataset under information flow protection:

1) To offer privacy protection, noisy perturbing of real data is assumed. We then invoke the differential privacy method to analyze the significant difference between specific residences' absences from the smart home.

2) When the switching on/off operations of e-Locks are open to access, they are treated as the input and, in turn, could be modeled as a real-valued correlated Gaussian random variable. Based on that, a hidden Markov Chain model is provided to measure the absence of occupancies in correlation with the e-Lock's switching on/off operations.

3) Turning on/off operations of e-Locks are transmitted to the security companies' servers or even their cloud. They may be borrowed by a third party for investigation in future. It is possible that the aggregator is untrusted. An attempt to utilize cyber property information flow is taken to shield privacy.

2. Architecture of E-Lock in Smart Home

Currently, there are different ways of integrating smart homes into the broader context of smart services, smart grids, and even smart cities, considering that our world is growing smarter than ever.

This ongoing trend has come up with interesting and useful applications. How-

ever, in the light of a majority of consumers being lack of technology and not necessarily trained in security in computer system, cloud computing system, or control systems, this paper has extensively studied the security of privacy needs. When certain sensory data is leaked or the communication data pattern is revealed in the current smart home system, consumers or network managers should be notified or be aware of the privacy leakage.

Meanwhile, due to its limited computing capacity, a single smart home cannot process all data in time. Therefore, taking advantage of cloud computing becomes a reasonable choice. However, privacy leakage that occurs during the data transmission between the smart home system and the cloud environment becomes a big concern. Due to this potential issue, a framework is proposed in this paper to integrate smart homes into the platform clouds or service clouds. In the proposed framework, to simply use the privacy protection solution, we only think about the e-lock, which is relatively simple. Although other smart devices, e.g., refrigerator, oven, etc., are more complicated devices, they can be protected in a similar way.

E-Locks in a smart home include three components—keypad, central processing unit and solenoid (actuator). If the credential inputted at keypad is valid, a signal is sent to solenoid to change the e-Lock's state from off to on. The application generates time-series categorical data, which is aggregated to the server/cloud of the security company through secure communication channel. The admin or even authority staff (e.g., policeman) may be able to query or even access the anonymized dataset from now on.

Note that the framework proposed in this paper only focuses on theoretical analyses by using some privacy preservation methodologies. How to implement them in real-world smart home system (e.g., e-lock) is out of the scope of this paper.

3. Privacy Loss and Threat Model

3.1. Privacy Loss Scenario

Untrusted third party: The collected dataset could be borrowed by a third party to accomplish research duties such as optimization or investigation tasks such as criminal inquiry. Unveiling time-series true/raw data may violate householder's privacy.

Untrusted third-party aggregator that peeks for privacy: An adversary queries the collected data set to steal privacy by taking advantage of the strong correlation among successive values in the series.

Example I: Eve observes that Alice left the community. Eve can query the number of e-Lock state changes in the community at two successive time slots to guess which house Alice left.

Privacy for residence occupancy: An e-Lock state change C_i can let an adversary infer that the resident is present or absent with the support of a temporal correlation of participatory sensing data.

Example II: Alice is the only one at home, and then, e-Lock's state changes. Eve

can probably infer that Alice may open the door and leave or Alice has accompanied. If it is the former, Eve can take the risk to break in.

3.2. Threat Models

Like other research [5] in areas of privacy preservations, we assume that smart devices (e.g., e-Lock, etc.) in the smart home and the cloud/server obey network communication schemes. However, both users and the aggregators could be untruthful since they can lie, and they also have the intention to combine the information if possible. However, we need at least a fraction of them (e.g., a majority) to be honest. Comparing with other privacy-related research, this paper provides more theoretical analyses.

4. Proposed Privacy Framework

4.1. Utilize Markov Chain

We assume that the state of an e-Lock L_i (where $L_i \in L = \{L_1, L_2, \cdots, L_n\}$, n is the number of e-Locks in households) is sampled when there is an unlock/lock action. $L_i \in \{0,1\}$ where 0 denotes unlocked and 1 locked. Let array L_t^n denote the state of all e-Lock at time t. There are 2^n possible states of all e-Locks.

Assume there are m family members. The presence of each person in the household is also monitored as $P_i \in \{0,1\}$ where 0 denotes absence and 1 presence. At the time instant t, the presence of all members $\{P_1, P_2, \cdots, P_m\}$ is denoted as an array P_t^m. There are 2^m possible states of the presence of all m family members.

Thus, we model the joint probability distribution of the e-Lock states and the presence state over x time instants:

$$P\left(L_t^n, P_t^m\right) = \prod_{t=1}^{x} P\left(L_t^n \middle| L_{t-1}^n\right) P\left(P_t^m \middle| L_t^n\right) \tag{1}$$

Based on (1), we can deduce a hidden Markov model for the presence of persons, which can be characterized by three parameters: 1) the initial presence, 2) a state distribution and 3) a conditional distribution. After defining the 3 inputs with concrete details, our hidden Markov model should assess the interrelated association between the pair (*L*, *P*) in which array *P* with all elements being 0 is what both the burglar and the security company are interested in.

4.2. Identify Differential Privacy

Let I_i denote all e-Lock state change data related to one smart home or even a community. Denote $I = \sum_i^n I_i$ which is the collected dataset related with n persons $\{I_1, I_2, \cdots, I_n\}$. We demand the following holds

$$\Pr\left[A(I) = x\right] \le \mathrm{e}^{\epsilon} \Pr\left[A(I') = x\right] \tag{2}$$

where Pr is a probability distribution over the randomness of algorithm $A(I)$ where I is the input, I' is the addition or removing of one single user, and x

is an any value output. Let $\boldsymbol{Q}=\{Q_1,Q_2,\cdots,Q_n\}$ be any query sequence, we demand the following holds:

$$\left|Q(I)-Q(I')\right|_p \le \Delta_p(Q) \tag{3}$$

where $p\in\{1,2\}$, $Q(I)$ and $Q(I')$ are each vectors, $\Delta_p(Q)$ measures Manhattan distance $\sum_i\left|Q_i(I)-Q_i(I')\right|$ and $\Delta_2(Q)$ Euclidean distance $(\sqrt{\sum_i\left(Q_i(I)-Q_i(I')\right)^2})$.

Differential privacy is a mathematical framework that can release statistical outcomes and protect private data against privacy leakage. In this paper, although differential privacy can be used to partially identify the quantitative nature of privacy leakage, this is just a tiny circumstance for each complicated scenario of the whole smart home case study. How to precisely measure the privacy leakage in real life for a smart home is too complicated to be provided by our solution.

4.3. Integrate Hyberproperty

The malicious third party may query the true data and revise its belief from the keep-going interaction thereafter [6]. An experiment $£=\langle S,b_H,\sigma_H,\sigma_L\rangle$ is processed where S is the query system, b_H denotes prebelief about high state, σ_H denotes high state and σ_L denotes low state. The third-party/agent predicts the output distribution p'_A and S produces a state $\sigma'\in \mathrm{p}'=[\![S]\!](\dot{\sigma}_L\oplus\dot{b}_H)$. The agent can infer a postbelief: $b'_H=(\mathrm{p}'_A|o)\,\dot{\downarrow}\,H$ where o is the low projection of the output state. With $£$, we, instantiating Bayes' rule on these probabilities, get Bayesian inference:

$$BI(£,o)=\frac{b_H(\sigma_H)\bullet([\![S]\!]\dot{\sigma_L}\oplus\dot{\sigma_H}\,\dot{\downarrow}\,H)(o)}{(\sum\sigma'_H\colon b_H(\sigma'_H)\bullet([\![S]\!]\dot{\sigma_L}\oplus\dot{\sigma_H}\,\dot{\downarrow}\,H))(o)} \tag{4}$$

5. Case Study and Discussions

Let us take an electronic lock (e-lock) as an example: at the time point t_i, a few controllers, O_h, O_p, and O_c representing the resident, physical automation control device in the smart room and the cyber remote control program, respectively, issue their own control command $\{c_{O_h},c_{O_p},c_{O_c}\}_{t_i}$. In the proposed framework, since each of O_h, O_p, and O_c could be malicious, we will choose the right control command O_r for the e-lock P based on the current context set $\varphi(t_i)$ and the e-lock statuses, $S_k=[M]_{i\times j}$. The context set $\varphi(t_i)$ could include different kinds of residents such as host, guests, and so on. Note that the privacy-related issues can include many more factors and therefore could be more complicated than the scenario we are discussing in this paper. For example, the security company may also hire different kinds of security guards, full-time, contract, substitution, etc. They all have been granted different levels of access control privilege based on their priority. This paper only thinks about a very simple case study and will count them in for our future research. In other words, the context, together with the current status of the e-lock, decides whether privacy is leaked or

not. In future, our work may also include simulation or even real-world experiments. Comparing with other privacy-related research, this paper provides more theoretical analyses. Furthermore, our works will centrally focus on privacy preservation via perturbing distributed noisy information to time-series e-Lock state change data to minimize the privacy loss with a lower utility-privacy tradeoff. In addition, how to extend the hidden Markov Chain method to precisely quantify privacy loss and corresponding counter-measures via differentially private protection will be studied.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] Cook, D.J. (2012) How Smart Is Your Home? *Science*, **335**, 1579-1581. https://doi.org/10.1126/science.1217640

[2] Kim, T.H., Bauer, L., Newsome, J., Perrig, A. and Walker, J. (2011) Access Right Assignment Mechanisms for Secure Home Networks. *Journal of Communications and Networks*, **13**, 175-186. https://doi.org/10.1109/jcn.2011.6157417

[3] Oh, S., Yang, J., Bianchi, A. and Kim, H. (2014) Poster: Power Replay Attack in Electronic Door Locks. *IEEE Symposium on Security and Privacy*, San Jose, 2014, 1-2.

[4] Dwork, C. (2008) Differential Privacy: A Survey of Results. In: Agrawal, M., Du, D., Duan, Z. and Li, A., Eds., *Lecture Notes in Computer Science*, Springer Berlin Heidelberg, Springer, 1-19. https://doi.org/10.1007/978-3-540-79228-4_1

[5] Rastogi, V. and Nath, S. (2010). Differentially Private Aggregation of Distributed Time-Series with Transformation and Encryption. *Proceedings of the* 2010 *ACM SIGMOD International Conference on Management of Data*, Indianapolis, 6-10 June 2010, 735-746. https://doi.org/10.1145/1807167.1807247

[6] Clarkson, M.R., Myers, A.C. and Schneider, F.B. (2009) Quantifying Information Flow with Beliefs. *Journal of Computer Security*, **17**, 655-701. https://doi.org/10.3233/jcs-2009-0353