International Journal of Current Research in Multidisciplinary (IJCRM) *ISSN: 2456-0979*
Vol. 3, No. 4, (April'18), pp. 01-05

PRIVACY-PRESERVING DATA ANALYTICS IN CLOUD-BASED SMART HOME WITH COMMUNITY HIERARCHY

G. Srividhya[1], Sughan Richardson. S[2]
[1]*Assistant Professor, Dept. of ECE, Panimalar Engineering College, Chennai, India,*
[2]*UG Scholar, Dept. of ECE, Panimalar Engineering College, Chennai, India*

ABSTRACT
The prominence of the Internet of Things (IoT) has led to increasing data volumes, which are expected to grow exponentially. The IoT has great potential to positively change society but also presents challenges regarding privacy. In practice, Smart community public housing projects involving tens of thousands of households have recently been implemented. This study proposed a privacy-preserving intelligent home system, which connects a single home controller with data-hiding capabilities through community networking and integrates the data to hierarchical architecture on a cloud platform for a data analytical access control mechanism. In addition, this paper outlines a variety of smart home data applications through data collected from a smart community environment with the developed privacy protection mechanism. The monitoring and protecting mechanism combines privacy-enhancing technologies with a privacy-preserving strategy from the initial system-designing stage through to full data lifecycle management. The types of smart home data that can be obtained from a community hierarchy, such as identification values, sensitive data, and non-sensitive data, were collected and classified. Through a combination of empirical application and sophisticated exploration of theoretical knowledge, this paper substantially contributes to the home automation field. The proposed system architecture is expected to enable both easy understanding for users and compliance for analytical service providers regarding the operation, procedure, limitation, and benefits of smart home data analysis, thereby providing a solution that ensures both privacy and data availability.
KEYWORDS: *Smart Home, Community Hierarchy,Privacy-Preserving, Data Analytics.*

INTRODUCTION

This study proposed privacy-preserving data analytics as a solution for optimizing the performance of cloud-based smart homes with community hierarchy. The home controller performed data hiding and minimization by de-identifying source raw data and delivering them as aggregated data.
Subsequently, the community broker achieved data aggregation and separation by further transferring the aggregated data after fusing the de-identified information with surrounding information. Finally, the cloud platform provided predefined public data for analyses, inquiries, and management while preserving privacy. The process mechanism of the cloud platform provided the enforcement process and access control mechanism at home and community levels. In addition, the platform obtained users' consent through an inform process scenario and demonstration, and provided comprehensive value-added and extensive data analytics services by importing other public data. Therefore, the platform enables controlling the privacy protection process and satisfies the requirements of advanced data analytics and applications. This study performed empirical data collection in smart communities, in which the aforementioned privacy-protecting mechanisms were applied and diversified applications of smart home data analytics were demonstrated, including community profile and feature analyses and operation, maintenance, and obstacle alerts. This study also investigated temporal, spatial, and between-household interactions within a community in smart home scenarios regarding privacy-preserving analytics. Notably, the inclusion of the community level added more flexibility than did previous systems. However, future research should further examine how to determine stakeholders at the community level to facilitate data authorization. Through a combination of empirical application and sophisticated exploration of theoretical knowledge, this paper substantially contributes to the home automation field. This study recommends that follow-up studies employ more precise temporal division of public and private periods to enhance the flexibility of the settings. For personalized service, family member authorization should be expanded from households to individuals. The proposed system architecture is expected to enable easy understanding (for the users) and compliance (for the analytic service providers) regarding the operation, procedure, limitation, and benefits of smart home data analytics, thereby providing a solution that retains both privacy and availability.

LITERATURE SURVEY

[1] Data Privacy
1) Personal data must be minimized as much as possible. The data from environmental or wearable sensors in a smart home system are identified by applying a sharing degree to evaluate the privacy levels of identifiers and sensitive data.

Filtering data,defining control parameters, and deleting unnecessary information should be done before implementing the smart home system. An intuitive method to do so is to hide the interaction between personal data and other data should be hidden from the clear text. For example, information about family members or household can be masked through re-encoding or encrypting to avoid directly identifying personal information, thereby achieving anti-tracking. Data segmentation is an advanced method of data protection; this involves partitioning data, such as personal health care information, home security status, and energy management, to implement distributed processing through decentralized archiving and analysis.

2) Data aggregation is another common method for data privacy protection. Aggregated statistics can be compiled per family unit by time division, which is a meaningful unit specifically for energy billing.Notably, personal information should be handled with the highest level of aggregation and the least number of details to inhibit usability trade-off. The phases of value chain analysis, including data collection, curation, storage, and data use, are continually examined through key privacy-by-design strategies. Meanwhile, the in-depth analysis of key principles and technologies required for information and communication technology and IoT environments are conducted during the implementation of smart home management systems.

[2]Privacy-Enhancing Technologies

1) Conventional techniques for data privacy processing consist of encryption and data hiding. However, because of the emergence of data mining research, various other techniques have been developed to improve conventional resource-limited IoT devices and optimize smart home systems and smart meters. Anonymity technologies achieve de-identification of identifiers through random replacement or pseudonymization; furthermore, when other sensitive data are involved, anonymity technologies also apply a series of k-anonymity technologies to protect complete data sets by reducing column precision or releasing merely a portion of sampled data. As discussed previously, the accuracy of smart home data should be considered when smart home system users perceive that the benefits of the IoT services exceed the risk of privacy loss.

2) During the evolution of privacy-preserving data mining and publishing methods, data with noise addition frequently reflected poor distributions of the initial data, leading to poor prediction efficiency. Later, differential privacy was developed to preserve the statistical properties of the protected data and minimize the effect of predictability. Conventionally, statistical disclosure controls (SDC) are commonly used by government agencies to aggregate industrial and demographic statistics; however, advanced SDC applications in smart home systems must consider granular solutions suitable for various scenarios without disrupting the data.

[3]Process Mechanism

1) As noted, privacy by design must be integrated in the initial designing phase of smart home systems. When the data privacy classification is completed, privacy-enhancing technologies are applied at various stages of the chain analysis. Consequently, those who control the data obtain the smart home system users' confidence by fulfilling their obligations regarding data protection, which is an essential element for popularizing IoT smart home services.

2) During the system design and construction stage, smart home systems must not only provide a transparent mechanism to properly notice users, but also enable the users to express consent and withdraw (the necessary basis of personal privacy protection). In addition, to ensure accountability and compliance, the overall system must possess enforcement and display tools such as automation policies. Current smart home systems lack simple mechanisms for users to understand and adopt the services. Thus, recent studies on building privacy protection into consumer electronics have comprehensively examined the life cycles of data security from network environments and hosting devices to applications and services related to business logic middleware, particularly the need of multilevel queries for smart home data analytics. At the application level, the fine-grained access control of privacy protection is required to provide end-to-end monitoring mechanisms of integrated data privacy protection.

PROPOSED SYSTEM

A. OVERALL SYSTEM ARCHITECTURE (THREE-LAYERED HIERARCHICAL ARCHITECTURE)

This study proposed a privacy-preserving smart home system, which connected a single home controller with data-hiding capabilities through community networking and integrated the data to a hierarchical architecture on a cloud platform for data analytics access control mechanism. The community broker not only performed home- and community-level data separation and aggregation but also supported the functions of the surrounding environmental data being imported to enrich data analytics. Moreover, the cloud platform provided public access to data analytics, queries, and management. Privacy preservation was then achieved by integrating informing, enforcement and a fine-grained access control mechanism of the communities and homes. By integrating its global services and open data, the

platform provided overall value-added and extended data analytics services.

B. PROPOSED SYSTEM ARCHITECTURE

The main privacy-protecting functions of the home controller comprise predefining source data format, data hiding, and data minimization. By de-identifying data at the home level, the home controller protects personal data in the household and forms the basis of overall privacy protection. The community broker provides privacy protection in community and home levels through data separation, aggregation, and fusion. Furthermore, by integrating the environmental and geographical attributes of the vicinity, including the subsystems of buildings and community surroundings (e.g., central monitor and control, surveillance, vehicle charging, and digital signage systems), the community broker enriches the implications of data analytics and achieves community profile and feature analysis, operation and maintenance, and obstacle alarming. The cloud platform integrates the enforcement process, access control mechanism, informing process scenario, and demonstrations at the community and home level to process privacy protection. In addition, the platform provides access to predefined public information for analysis and management services. Other globally public information (e.g., characteristics of administrative areas, traffic and police information, energy contract management, weather, and air quality) are also introduced to achieve extended data analytics services such as comparison of traffic information.

RESULTS & DISCUSSION

This section describes the applications of the proposed statistical management service, which organizes public information (predefined at various levels) and conducts data analytics and application upon authorization. The public information available on the cloud platform includes aggregated statistical reports and the percentage of usage of each function. In addition, based on the comparison of profile features in various communities, applications such as traffic police patrol scheduling can be developed. User interfaces can be optimized accordingly to enhance the convenience and applicability of smart home services in individual communities. Later, upon user consent, the data collected from homes and communities can be used to develop and implement new applications, such as global cross-region tracking of registration plates, early detection and prevention of obstacles, and personalized recommendations for households. The analytical results of various data as well as the temporal and spatial privacy interaction between community households are described as follows.

[1] Public Information Inquiry and Management Services and Advanced Applications of Authorized Data

According to the characteristics of smart home applications, the top three items are Homepage (default option for standby mode), Community Information Data processing in the community broker. Data transformation and access control on the cloud platform and Video Intercommunion (essential module in community life). These observations inspire the addition of announcement marquees to the Homepage, and development of online-to-offline community commerce in the future.. In order to emphasize the different habits, the most common items were discarded from the graph. Notably, among older communities, more space is accompanied by more devices that must be controlled, especially the combinations of Single Controls and Scenario Control. By contrast, in newer communities with undeveloped nearby environments, people are more concerned about security for the Community Video item.. In particular, the grouping result recommends a mix of the Scenario/Control and Environment/Energy categories to simplify user interfaces; the Gas Meter Report item is also moved to the top of the Constructor Area. These authorized insights can be useful for providing personalized recommendations or schedule services for user experience optimization.

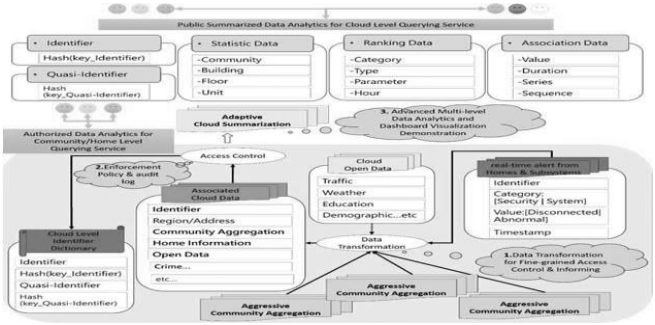
[2] Interaction between the Temporal and Spatial Aspects of Privacy Management in Community Households

In a smart home environment, time is fixed and finite for every household, whereas the space is dynamic (e.g., spatial deployment varies by household). However, data analytics requires user interaction to generate value, thereby generating privacy protection. In other words, the basic privacy of personal activities must be protected by clustering the activities into larger units (e.g., hour, day, and week) while the seemingly public and consistent time tracks user

activity by exact seconds. Conversely, the fixed spatial settings of the originally private space standardize the analytical aspects of every household, thereby maintaining the basic spatial privacy of each household. However, when the smart home environment was extended to community operations, space became the fixed and public component (e.g., community activity room), whereas the seemingly stable schedules of regular working hours needed privacy protection for security considerations (e.g., security guard patrol hours). Although the actual spatial configuration and various operating time of diverse communities exhibited relatively low considerations of personal privacy, the overall application could still prevent information leaks from critical security areas (e.g., front and rare entrances and the power system space).

Moreover, the system could achieve effective scheduling of the security patrol or optimization of the power supply system according to the community attributes. The cloud platform provided the predefined and public statistical and analytical information together. This heterogeneous combination of open data may generate unexpected analytical results with serendipity. In addition, with user consent, advanced private data can be analyzed using numerous existing study results, thereby providing households additionally in-depth data analyzing services.

This study had some limitations. First, in addition to the annual, seasonal, and monthly statistical analyses on the cloud platform, the weekly, daily, and hourly scales could have been further divided for the default scale. For example, time fragmentation can provide information for a detailed analysis by dividing days of week into weekdays and holidays, and hours into public and private periods (e.g., early morning hours when every family member is present before leaving for work and school; morning hours with few family members in presence, except housewives, older people, and young people; evening hours when family members return home; and the inactive night hours of sleep periods). Similarly, in addition to interface recommendations.



APPLICATION DEVELOPMENT

The primary motive for the application development is that to provide encryption for the host as their URL can be accessed by any other third party host so in this case an application is developed for different operating systems. Creating application allows the user to use their appliances in a more secure way as the host will not be provided with any URL instead the application will be provided so that their corresponding loads can be controlled under their supervision.

REFERENCES

[1] Turner, J. F. Gantz, D. Reinsel, and S. Minton, "The digital universe of opportunities: Rich data and the increasing value of the internet of things," Apr. 2014. [Online]. Available: https://www.emc.com/leadership/digital-universe/ 2014iview/index.htm

[2] G. Ramamoorthy, "IoT Drives Innovation in the Semiconductor Industry," Jul. 2015. [Online]. Available: https://www.gartner.com/webinar/3071623

[3] S. Kong, Y. Kim, R. Ko, and S. K. Joo, "Home appliance load disaggregation using cepstrum-smoothing-based method," *IEEE Trans. Consumer Electron.*, vol. 61, no. 1, pp. 24–30, Feb. 2015.

[4] J. Han, C. S. Choi, W. K. Park, I. Lee, and S. H. Kim, "Smart home energy management system including renewable energy based on ZigBee and PLC," *IEEE Trans. Consumer Electron.*, vol. 60, no. 2, pp.198–202, May. 2014.

[5] J. Han, C. S. Choi, W. K. Park, I. Lee, and S. H. Kim, "PLC-based photovoltaic system management for smart home energy management system," *IEEE Trans. Consumer Electron.*, vol. 60, no. 2, pp. 184– 189, May. 2014.

[6] T. Kim, H. Park, S. H. Hong, and Y. Chung, "Integrated system of face recognition and sound localization for a smart door phone," *IEEE Trans. Consumer Electron.*, vol. 59, no. 3, pp. 598–603, Aug. 2013.

[7] J. Wang, Z. Zhang, B. Li, S. Lee, and R. Sherratt, "An enhanced fall detection system for elderly person monitoring using consumer homenetworks," *IEEE Trans. Consumer Electron.*, vol. 60, no. 1, pp. 23–29, Feb. 2014.

[8] H. Y. Tung, K. F. Tsang, H. C. Tung, K. T. Chui, and H. R. Chi, "The design of dual radio ZigBee homecare gateway for remote patient monitoring," *IEEE Trans. Consumer Electron.*, vol. 59, no. 4, pp. 756– 764, Nov. 2013.

[9] K. Rose, S. Eldridge, and L. Chapin, "The Internet of Things: An Overview," Oct. 2015. [Online]. Available: https://www.internetsociety. org/doc/iot-overview

[10] B. Lee, J. Byun, M. I. Choi, B. Kang, and S. Park, "Degradation diagnosis system of photovoltaic panels with mobile application," *IEEE Trans. Consumer Electron.*, vol. 60, no. 3, pp. 338–346, Aug. 2014.

[11] C. H. Tsai, Y. W. Bai, M. B. Lin, J. Rong, and Y. W. Lin, "Design and implementation of a PIR luminaire with zero standby power using a photovoltaic array in enough daylight," *IEEE Trans. Consumer Electron.*, vol. 59, no. 3, pp. 499–506, Aug. 2013.

[12] Y. M. Wi, J. U. Lee, and S. K. Joo, "Electric vehicle charging method for smart homes/buildings with a photovoltaic system," *IEEE Trans. Consumer Electron.*, vol. 59, no. 2, pp. 323–328, May. 2013.

[13] J. Byun, S. Park, B. Kang, I. Hong, and S. Park, "Design and implementation of an intelligent energy saving system based on standby power reduction for a future zero-energy home environment," *IEEE*

[14] *Trans. Consumer Electron.*, vol. 59, no. 3, pp. 507– 514, Aug. 2013.

[15] H. C. Jo, S. Kim, and S. K. Joo, "Smart heating and air conditioning scheduling method incorporating customer convenience for home energy management system," *IEEE Trans. Consumer Electron.*, vol. 59, no. 2, pp. 316–322, May. 2013.

[16] Q. Liu, G. Cooper, N. Linge, H. Takruri, and R. Sowden, "DEHEMS: Creating a digital environment for large-scale energy management at homes," *IEEE Trans. Consumer Electron.*, vol. 59, no. 1, pp. 62–69, Feb. 2013.

[17] Y. T. Lee, W. H. Hsiao, C. M. Huang and S.C.T. Chou, "An integrated cloud-based smart home management system with community hierarchy," *IEEE Trans. Consumer Electron.*, vol. 62, no. 1, pp.1–9, Feb. 2016.

[18] D. Cook and N. Krishnan, "Mining the home environment," *J. Intell. Inf. Syst*., vol. 43, no. 3, pp. 503–519, Dec. 2014.

[19] S.D. Warren and L.D. Brandeis, "The right to privacy," *Harv. Law Rev.*, vol. 4, no. 5, pp. 193–220, Dec. 1890.

[20] W. Wilkowska, M. Ziefle, and S. Himmel, "Perceptions of personal privacy in smart home technologies: Do user assessments vary depending on the research method?" in *Proc. Int. Conf. Hum. Asp. Inf. Secur. Priv.Trust*, 2015, pp. 592–603.

[21] E. Waltz, "How I quantified myself," *IEEE Spectrum*, vol. 49, no. 9, pp. 42–47, Sep. 2012.

[22] D. Townsend, F. Knoefel, and R. Goubran, "Privacy versus autonomy: A tradeoff model for smart home monitoring technologies," in *Proc. IEEE EMBC'16*, Boston, MA, 2011, pp. 4749–4752.

[23] A. Chakravorty, T. Wlodarczyk, and C. Rong, "Privacy Preserving Data Analytics for Smart Homes," in *IEEE SPW*, San Francisco, CA, 2013, pp. 23–27. 206 IEEE Transactions on Consumer Electronics, Vol. 63, No. 2, May 2017

[24] G. D'Acquisto, J. Domingo-Ferrer, P. Kikiras, V. Torra, Y.A. de Montjoye, A. Bourka, "Privacy by design in big data: an overview of privacy enhancing technologies in the era of big data analytics," *ENISA Tech. Rep.*, Dec. 2015.

[25] A. Cavoukian, "Privacy by design [leading edge]," *IEEE Tech. Soc. Mag.*, vol. 31, no. 4, pp. 18– 19, Dec. 2012.

[26] A. Cavoukian, "International council on global privacy and security, by design," *IEEE Potentials*, vol. 35, no. 5, pp. 43–46, Sept.-Oct. 2016.

[27] M. H. Davis, U. Lang, and S. Shetye, "A Cybermodel for Privacy by Design: Building privacy protection into consumer electronics," *IEEE Consumer Electron. Mag.*, vol. 4, no. 1, pp. 41–49, Jan. 2015.

[28] L. Sweeney, "k-anonymity: A model for protecting privacy." *Int. J. Uncertainty Fuzziness Knowledge Based Syst.*, vol. 10, no. 5, pp. 557– 570, May. 2002.

[29] Machanavajjhala, A., Kifer, D., Gehrke, J., and Venkitasubramaniam, M. (2007). l-diversity: Privacy beyond k-anonymity. *ACM Trans. Knowl. Discov. Data*, vol. 1, no. 1, p. 3, Mar. 2007.

[30] N. Li, T. Li and S. Venkatasubramanian, "t-Closeness: Privacy Beyond k-Anonymity and l-Diversity," in *2007 IEEE 23rd ICDE*, Istanbul, 2007, pp. 106–115.

[31] A. Cavoukian and K. Kursawe, "Implementing privacy by design: The smart meter case," in *2012 SGE*, Oshawa, ON, 2012, pp. 1–8.

[32] R. Agrawal and R. Srikant. "Privacy-preserving data mining." *ACM Sigmod Record*., vol. 29, no. 2, pp. 439–450, May. 2000.

[33] C. Dwork, "Differential privacy: A survey of results," in *Proc. TMAC 2008*, Hong Kong, 2008, pp. 1–19.

[34] J. Domingo-Ferrer and J. Mateo-Sanz, "Practical data-oriented microaggregation for statistical disclosure control," *IEEE Trans. Knowl. Data Eng.*, vol. 14, no. 1, pp. 189–201, Jan. 2002.

[35] D. He, N. Kumar, and J. H. Lee, "Secure pseudonym-based near field communication protocol for the consumer internet of things," *IEEE Trans. Consumer Electron.*, vol. 61, no. 1, pp. 56–62, Feb. 2015.

[36] G. Song, S. Kim, and D. Seo, "Saveme: client-side aggregation of cloud storage," *IEEE Trans. Consumer Electron.*, vol. 61, no. 3, pp. 302–310, Aug. 2015.

[37] J. Yun, I. Y. Ahn, N. M. Sung, and J. Kim, "A device software platform for consumer electronics based on the internet of things," *IEEE Trans. Consumer Electron.*, vol. 61, no. 4, pp. 564–571, Nov. 2015.

[38] Y. Jeong, H. Joo, G. Hong, D. Shin, and S. Lee, "AVIoT: web-based interactive authoring and visualization of indoor internet of things," *IEEE Trans. Consumer Electron.*, vol. 61, no. 3, pp. 295–301, Aug. 2015.

[39] G. Ohtake, K. Ogawa, and R. Safavi-Naini, "Privacy preserving system for integrated broadcast-broadband services using attribute-based encryption," *IEEE Trans. Consumer Electron.*, vol. 61, no. 3, pp. 328– 335, Aug. 2015.