International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 07
March 2018

Privacy Preserving IoT Applications in Smart Homes: A Generic Framework

N. Nirmalajyothi & M.Venkataeswara Rao
[1]Associate Professor, Dept. of CSE, Aurora's Techonological& Research Institute, Hyderabad, Telangana, India
[2]Associate Professor, Dept. of IT, ViganaanaBharathi Institute of Technology, Hyderabad, Telangana, India

Abstract:*In this paper, the brief overview of existing frameworks for development of IoTapplications, techniques to develop smart home applications using existing IoT frameworks, and a new generic framework for the developmentof IoTbasedsmart home system is presented. The proposed generic framework comprises various modules such as Auto-Configuration andManagement, Communication Protocol, Auto-Monitoring and Control, and Objects Access Control. The architecture of the new genericframework and the functionality of various modules in the framework are also presented. The proposed generic framework is helpful for makingevery house as smart house to increase the comfort of inhabitants. Each of the components of generic framework is robust in nature in providingservices at any time. The components of smart home system are designed to take care of various issues such as scalability, interoperability,device adaptability, security and privacy.*

Keywords-Internet of Things (IoT); Smart Home System; Sensor Networks; Security; Auto-Configuration; Communication Protocol; AccessControl; Device Managementis

I. INTRODUCTION

The term "Internet of Things" was first used by Kevin Ashton at Procter & Gamble in 1999, to describe an Internet-basedinformation service architecture [3]. Generally the term refersto Internet-enabled objects interacting with each other andcooperating to achieve specific goals. These objects could beRFID, sensors, actuators or mobile phones [21]. The Internetof Things claims to improve peoples' lives. For instance, atool could measure heart rate and body temperature, and thencommunicate with the energy management system to adjustroom temperature depending on the individual's physiological status. Other tools activate smart streetlights, monitorsurveillance cameras and control traffic lights. Collected information can be shared with different stakeholders to improve business intelligence.

The IoT makes life less effortful and more convenient. Onthe other hand, the invisibility of the data collection, usageand sharing processes raise concerns. The privacy of IoTusers could easily be sacrificed [17]. On the one hand, weaccept the fact that the service providers need to access ourinformation in order to deliver tailored services.

The concept of privacy varies from countries, cultures andjurisdiction. However in general, privacy is associated withcollection, storage, use, processing, sharing or destruction ofpersonally identifiable data. Chen et al. [4] surveys datasecurity & privacy issues around the complete data lifecyclefor cloud computing. Based on their framework, we derivefour areas to ensure security & privacy for a smart homeanalytic solution. The areas of data ownership, transfer,storage & processing and access are discussed bellow.

A. Data Ownership: Data generated at smart homes are sensitive, and ownershipissues are not always clear. Although a community center,healthcare provider or service providers could own the sensorand network devices, yet the data pertain to the residents ofthe homes. They should know what kind of data are collected,stored and shared. They should be able to stop the collectionas well as ask for destruction of any stored records.

B. Data Transfer: Transmission of the sensor data through unsecure networksshould be protected. Confidentiality and integrity should beensured for

any data transfer. Confidentiality is securingsensitive data against a malicious user and integrity ispreserving the truthfulness of the data. Cryptography or VPNtechniques [5], [6] are some of the commonly used approachesfor securely transferring data.

C. Data Storage & Processing: Data stored with personally identifiable information (oridentifiers) in an external cluster is a serious threat to dataprivacy. Personal and quasi identifiers [22] describepersonally identifiable information. These attributes candirectly or in-directly reveal personal information. Steps toprotect privacy are to replace any personally identifiableinformation with randomized placeholders, introduce noise orswapping values while ensuring that statistical properties anddata consistency are maintained [7], [8]. Another alternativeapproach is using generalization and suppression methods [9],[10], [11]. The processing of smart home data should beindependent of sensitive information. Storing the data used foranalysis/mining as mentioned above can achieve this.However, the use of transformation challenge is to find theright trade-off between amount of privacy and informationloss [9], [10], [11], [12].

D. Data Access: Access to the system should be ensured through properauthentication and authorization. The system should beconfigurable to assign rights to execute analysis/mining jobsto appropriate users and access the generated results. Amongmany methods the role base access control (RBAC) has beenwidely accepted because of its simplicity, flexibility incapturing dynamic requirements and support for the principleof least privilege and efficient privilege management [13],[14], [15].

(F. K. Santosoet. Al, 2015) offers a technique for securing smart home system. The technique contains robust protectionbased on AllJoyn framework the usage of uneven Elliptic curvecryptography for authentication. It makes use of a WiFi-based totally IoTgateway to allow cozy communication among IoT devicesthat allows us to permit customers to setup, get right of access to and manage the device.The translation is likewise accomplished between one of a kind IoTrequirements via a handy interface thru android device.The machine has been tested on WiFi-enabled STM32F4 ARMCortex M4F microprocessor, Raspberry Pi Linux laptopand Galaxy Note GT N7000 Android smartphone. However,the gadget needs guide configuration of every IoT toolwith ID (identifier), pre-shared mystery key, and access factorcall.

(O. BeratSezeret. Al, 2015) proposed a smart domesticontology for six appliances inside the home consisting of fridge,washing system, dishwasher, tv, oven, andlaptop.The smart domestic machine is developed using RDF andSesame Framework. It is determined that scaling of sensorgadgets at run-time isn't always taken care by way of the smart homeontology.

(V. H. Bhide, et. Al, 2015) affords ansmart self-gaining knowledge of system for home automation the use of loT. The approachself-learns to manipulate and display environmental conditions inhomes. The machine is examined for mild, temperature, degree, andhumidity sensor devices to understand the environmentalconditions and additionally to stumble on the faults in devices. It is locatedthat the machine makes use of device-to-cloud communique versionand it wishes manual fault correction by means of technicians.

(S. K. Dattaet. Al, 2015) defined for customizedhealthcare in smart homes. It uses Machine-to-MachineMeasurement (M3M) framework for discovering, managingand interacting with heterogeneous devices deployed in cleverhome and eHealth domain names. The gadget plays complexfacts processing, the discovery of necessary assets,maintenance of the records of information and car-secured control. Italso combines sensor data from exclusive domain names (createspass-domain knowledge) and generates actionable intelligenceusing semantic reasoning engine. The device calls for lessthan 3.5MB of memory, much less than 2% of CPU load, strengthintake of 259mW-298mW in Samsung galaxy S3running android KitKat.

(M. Zehnderet. Al, 2015) gives a way for powersaving in clever homes based on client

conduct. Themachine uses deterministic finite nation device (FSM) methodfor mining frequent and periodic patterns within the event information.The extracted patterns are converted to association rules andmodern behavior of population is used to hit upon theopportunities to store energy and additionally to sendaadvice to the population. The approach achieves the useful recommendation of approximately 10% the use of frequent andperiodic styles. The effects may be improved via the usage of differentdevice gaining knowledge of algorithms and thinking about other criteriawhich includes pattern period, the time among events, weekday andseason when the pattern occur maximum and comments ofinhabitants.

(MayurBholeet. Al, 2015) added analytics offerings forclever homes. The technique addresses diverse issues associated withquit-user revel in and recommends appropriate toolsettings based totally on usage records of devices of clever homemachine. It additionally employs an appliance usage-prediction engineto are expecting the fame of a tool at any time.The gadget isdiscovered to be scalable and has executed recommendationaccuracy of 90%. Further the device can be prolonged tooptimize the strength utilization.

(I. Papp et. Al, 2015) evolved a method for uniformillustration and manipulate of Bluetooth Low Energy gadgets indomestic automation software program. It contains a ordinary gateway thatcontrols any logo tool. The method ensures scalability andsmooth plug-n-play logo unfastened integration of latest gadgets.It additionallysupports guide mode and plug-n-play operational modes.

The manual mode allows addition of profiles, services anddevice position in configuration record. Plug-n-play mode assignsprofiles and services to the newly detected gadgetsrobotically.

(G. V. Vivek et.Al, 2015) proposesIoT offerings using WiFiZigBee gateway for a domestic automation machine. The gatewayestablishes communication amongst extraordinary protocols andoffers get admission to to the sensors and actuators. It allows to lessenelectricity intake. The machine has been tested the use ofcubietruck board as gateway and Xbee module with doorsensor, temperature sensor and light sensor. Sensors have beenlinked to unique strength resources and accomplished reductionof 20mA.

(Ming Wang, et. Al, 2013) proposed an IoT basedappliance manage gadget for clever houses. The vitalcontroller units up a radio frequency 433 MHz wi-fi sensorand actuator network (WSAN) to control and display domesticappliances. The WSAN includes switch module and RFmanipulate module to at once manage all home equipment. The systemobserved to be scalable, smooth to reconfigure and reorganize.However, it needs automation and optimizing the applianceoperations.

(A. Chakravorty, et. Al, 2013) designed a framework forprivateness retaining statistics analytics for smart houses. Theframework has deliberate to obtain records security at each levelof facts life cycle which include: records era, data switch, factsgarage, facts processing and records sharing. The performance,uncertainty level and performance of different facts safetystrategies could need to be measured.

(S. D. T. Kelly, 2013) proposesIoT for environmentalcondition monitoring in houses. It plays circumstancetracking and electricity control of domestic devices suchas electric lamp, water heater, battery charging units, washingmachines and refrigerators. The machine consists of cleversensing devices, IoT software gateway and net server.

II. METHODS AND SCHEMES

The generic framework for smart home system consists ofvarious components such as auto configuration and devicemanagement, auto-monitoring & control, cross-platformcommunication protocol, object access control, user interface,context aware adaption scheme, and data analysis andvisualization.The architecture of proposed generic framework is depictedin fig. 1. The core components of smart home system aredetailed in the following sub sections.

A. Auto-Configuration and DeviceManagement:

The auto configuration and management component ofsmart home system self-configures/self-organizes objects andmakes the objects ready for communication. It also addressesthe scalability problem. This component provides plug n playconnectivity to objects for achieving device compatibility. Thecomponent communicates with objects in visible range ofWiFi network and enrolls them with authentication. Theenrolled objects will be configured automatically to makethem ready for further operation.

B. Communication Protocol:

This component of smart home system will send/receive dataand control information to and from connected objects. Theprotocol also takes care of interoperability issues.

C. Auto Monitoring and Control: This component/module monitors status and health of allobjects and controls automatically based on context. Theobjects will also be controlled based on commands issued bythe user.

D. Objects Access Control: This component of smart home system prevents andprotects data and control information transmitted to and fromobjects from unauthorized access.

E. User Interface (UI): The user interface module of thesmart home systemenables users to interact with the smart home system to accessthat status of devices and control them with commands givenmanually. The user interface component of smart home systemis remotely accessible by the computers/mobile phonesconnected to the internet.

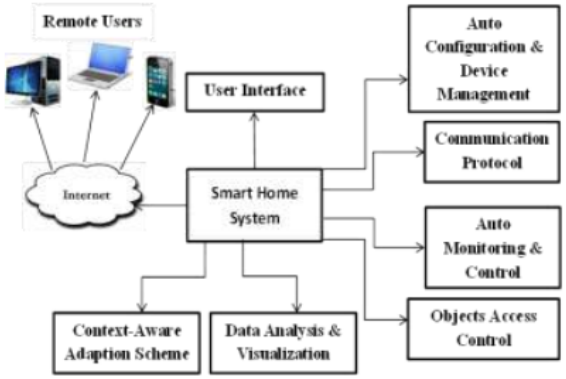

Figure 1. Generic Framework for Smart Home System

F. Context Aware Adaption Scheme: The context aware adaption scheme of smart home systemcontrols the operation of devices based on the history of usageand current situation. It uses machine learning algorithms tolearn the usage history and predicts the operation of devicesbased on the context. The inhabitant's behavior and emotionswill also be considered for determining the context andprediction of device operation.

G. Data Analysis and Visualization: The smart home system also provides data analysis andvisualization service. The usage reports of devices,consumption of energy and other statistical details will beanalyzed and visualized.The proposed generic framework is helpful for makingevery house as smart house to increase the comfort ofinhabitants. Each of the components of generic framework isrobust in nature in providing services at any time.

III. CONCLUSIONS

In this paper, a generic framework for smart home system ispresented. The generic framework is unique in nature andaddresses all the issues associated with making a house smart.It comprises various components such as auto-configurationand device management, auto-monitoring & control, crossplatform communication protocol, object access control, userinterface, context aware adaption scheme, and data analysis andvisualization.

REFERENCES

[1] Chetana Sharma (16 March 2016), [Online]. "Correcting the IoTHistory", Avilable:.http://www.chetansharma.com/IoT_History.htm

[2] Brown Eric (13 September 2016). [Online]. "Who Needs theInternet of Things?". Available:https://www.linux.com/news/who-needs-internet-things

[3] Brown Eric (20 September 2016). [Online]."21 Open SourceProjects for IoT". Available:

https://www.linux.com/NEWS/21-OPEN-SOURCE-PROJECTS-IOT

[4] D. Chen, H. Zhao, "Data Security and Privacy Protection Issues inCloud Computing," International Conference on Computer Science andElectronics Engineering (ICCSEE), vol.1, pp.647-651, Mar. 2012

[5] A.D. Rubin, D. E. Geer, "A survey of Web security," Computer, vol.31,no.9, pp.34-41, Sept. 1998.

[6] CohesiveFT, "VPNCubed," http://www.cohesiveft.com/vpncubed/, 2008

[7] V. S. Iyengar, "Transforming data to satisfy privacy constraints," EighthACM SIGKDD international conference on Knowledge discovery anddata mining, pp.279-288, 2002

[8] J. Kim and W. Winkler, "Masking microdata files," Survey ResearchMethods ASA Proceedings, pp.114–119, 1995

[9] P. Samarati, L. Sweeney, "Protecting privacy when disclosinginformation: k-anonymity and its enforcement through generalizationand suppression.," Stanford Research Institute International, Mar. 1998

[10] L. Sweeney, "Datafly: A system for providing anonymity in medicaldata," 11th International Conference on Database Security, pp.356–381,1998

[11] P. Samarati, "Protecting respondents' identities in microdata release,"IEEE Transactions on Knowledge Engineering, vol.13, no.6, pp.1010–1027, Nov. 2001

[12] A. Hundepool, L. Willenborg, "μ- and τ- argus: Software for statisticaldisclosure control," 3rd Internation Seminar on StatisticalConfidentiality, 1996

[13] R.W. Baldwin, "Naming and Grouping Privileges to Simplify SecurityManagement in Large Databases," IEEE Symposium on ComputerSecurity and Privacy, 1990

[14] K.R. Poland, M.J. Nash, "Some Conundrums Concerning Separation ofDuty," IEEE Symposium on Computer Security and Privacy, 1990

[15] J. Joshi, et al., "Access Control Language for Multi-domainEnvironments," IEEE Internet Computing, vol.8, no.6, pp.40–50, 2004

[16] T. Yloenen, "SSH - Secure Login Connections over the Internet," 6thUSENIX UNIX Security Symposium, Jul. 1996