IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 5, May 2017

Review on Neural Based Expert System for Home Automation

Gunjan[1], Saurabh Charaya[2]

Dept of Computer Science and Engineering, Om Institute of Technology & Management, Hisar, India[1,2]

Abstract: Cloud services are offering the flexible and scalable services. But there is always issue of security. When data is transferred from centrally located server storage to different cloud the compromise of person and private data would increase. There is always risk to the confidentiality and availability of data prior to selecting a cloud vender or choosing own cloud and cloud service migration. In order to program & control flow of information in Internet of Things, a predicted architectural direction is required. It is being called BPM. Everywhere that is a blending of traditional process management and special capabilities to automate control of large numbers of coordinated devices.

Keywords: IOT, Integration, Home automation, Machine to Machine.

I. INTRODUCTION

Cloud may be network or internet and it is something that is available at remote place. It provides services over network that are public and private. They are used in wide area network, local area network or virtual private network. Several application like email and web based conferencing executes on cloud.

Platform independency is offered by cloud computing because there is no need to install software on personal computer. So we can say that our business applications are mobile and collaborative due to cloud computing.

Cloud Server model

Type of access to cloud has been defined by Deployment model. There are four types of accessibility in cloud that are public access, private access, Hybrid access and Community access.

Public Cloud

Access to general public is allowed by public cloud. Due to openness public cloud is less secure

Private Cloud

Due to its private nature private cloud is considered more safe and secure.

Community Cloud

Accessibility to a particular group is allowed by community cloud.

Home automation

Home automation is residential extension of building automation & involves control & automation of lighting, heating (such as smart thermostats), ventilation, air conditioning (HVAC), & security, as well as home appliances such as washer/dryers, ovens or refrigerators/freezers that use WiFi for remote monitoring. Modern systems generally consist of switches & sensors connected to a central hub sometimes called a gateway from which system is controlled within a user interface that is interacted either within a wall-mounted terminal, mobile phone software, tablet computer or a web interface, often but not always internet cloud services. While there are much competing vendors, there are very few world-wide accepted industry standards & smart home space is heavily fragmented.

II. LITERATURE REVIEW

John A. Stankovic, Life Fellow, IEEE wrote research on Research Directions for Internet of Things Several technical communities are pursuing researches that donate to Internet of Things. As sensing & actuation control has become ever sophisticated, there is important overlap in such communities, sometimes from slightly many perspectives. Cooperation among communities has been encouraged.

Jayavardhana Gubbi,Rajkumar Buyya. Slaven Marusic, Marimuthu Palaniswami Internet of Things: A Vision, Architectural Elements, & Future Directions[6]

Sensing enabled by Wireless Sensor Network technologies cuts across several areas of modern day living. Proliferation of these devices in a communicating actuating network creates Internet of Things, wherein, sensors & actuators blend seamlessly with environment around us, & information is shared across platforms in order to develop a common operating picture.

In 2014 Abhay Kumar & Neha Tiwari published a research titled Energy Efficient Smart Home Automation System told about energy required by home instruments & air-con systems ,develops homes one among foremost important

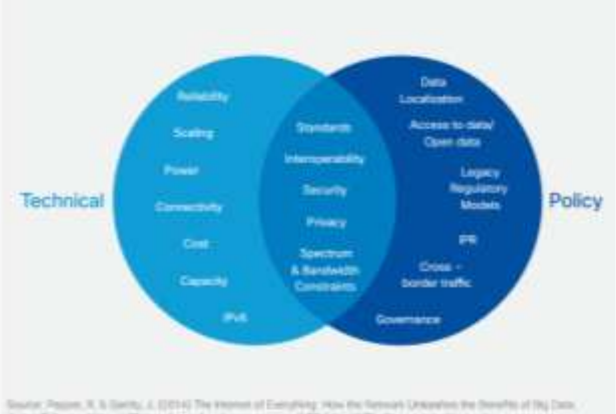
DOI10.17148/IJARCCE.2017.6521

areas for impact of energy consumption on natural surroundings. Objective for planning of such system is to reduce energy wastage with efficiency controlling devices operation modes.
Authors Juan Felipe Corso Arias in 2014 published their research paper heading “Wireless Sensor System According to Concept of IOT -Internet of Things
In this research they focus on design of a wireless communication system. They keep responding to sensor concept that has been applied to industrial process. Here temperature variables used. Sensors have been connected to internet in order to be monitored remotely. Sensor data gets downloaded from cloud with graphical programming in order to control. It communicates system with programmable logic controller. Monitoring process was done with a SCADA system & modeling of communication system was done using formalism of Petri nets, as a system that responds in terms of several events.

III.PROBLEM FORMULATION

Despite all exciting possibilities brought about by I.o.T. & Big Data, significant challenges persist. Same infrastructure that enables people to create, store & share information might also jeopardize their privacy & security. These same techniques could be used for large-scale & targeted surveillance. Abuse of these techniques could turn ‘Information Society’ into ‘Surveillance Society’, as identity management systems improve without parallel emphasis on anonymity & ownership of personal data.

Society’s most advanced systems & infrastructures are now so complex that some of them are becoming hard to manage effectively. Where they are designed wisely & used effectively, policy & regulatory frameworks could help development of IoT. However, outdated or poorly designed frameworks could prove hindrance & obstacle to further growth of IoT. While many parts of daily life become more connected, some remain woefully under connected. Conversely, other elements of individual’s daily life might be overwhelmed as explosion of new devices would require new infrastructure & technologies.
Technological & human capabilities are often insufficient in developing countries. Financial support might be lacking. There are often not enough technically literate people with IT skills in local areas who are capable of implementing use of sensors or other devices into their daily lives.



Source: Pepper, R. & Garrity, J. (2014) The Internet of Everything: How the Network Unleashes the Benefits of Big Data. Global IT Report 2014, WEF. http://www3.weforum.org/docs/GITR/2014/GITR_Chapter1.2_2014.pdf

Figure 4.2 summarizes some of emerging challenges in relation to I.o.T. & data.

Reliability would be concern with regard to durability of devices to withstand external conditions. Sensors, too, need to be calibrated to ensure proper measurements. In terms of scalability, way in which resources are scaled to match growth in I.o.T. might matter. Data centers, for example, are constantly being redesigned in terms of electrical power, cooling resources, & space design to advance current capabilities. However, connectivity requirements of billions, as opposed to millions, of connected objects impose very different demands on data centers. As I.o.T. scales up & expands from billions into tens of billions of connected devices, IP networks have to be able to manage huge scale of device connectivity.

Power requirements vary greatly, with higher bandwidth devices requiring much more power. Connectivity challenges were discussed earlier, & include limited data network coverage. According to Laura Hosman of Inveneo, top five hardware challenges in application of ICTs in development are: electricity/ power/energy; cost; environment; connectivity; & maintenance & support. 1 costs associated with sensors, connectivity modules & connectivity service could still prove prohibitive for many interventions (such as for individual small shareholding farmers). Organizations

DOI10.17148/IJARCCE.2017.6521

are starting to explore shared models of sensor module ownership such as community ownership, or ‘sensors as service’. Inadequate human capacity might prove major issue in some locations. Small-scale organizations might not be trained properly to use technology. There might also be underlying issues that inhibit training. For instance, if 80% of target population would be illiterate, would be SMS text really best form of communication? There might also be inadequate no. of trained people or technicians to respond, once system signals problem. If it would be difficult to fix manual pumps on-the-ground, it might be difficult to find resources to fix more complicated, seemingly.
Five key I.o.T.issue areas are examined to explore some of most pressing challenges & questions related to technology. These include security; privacy; interoperability & standards; legal, regulatory, & rights; & emerging economies & development.

• Security:
While security considerations are not new in context of information technology, attributes of many I.o.T. implementations present new & unique security challenges. Addressing these challenges & ensuring security in I.o.T. products & services must be fundamental priority. Users need to trust that I.o.T. devices & related data services are secure from vulnerabilities, especially as that technology become more pervasive & integrated into our daily lives. Poorly secured I.o.T. devices & services could serve as potential entry points for cyber attack & expose user data to theft by leaving data streams inadequately protected. Interconnected nature of I.o.T. devices means that every poorly secured device that would be connected online potentially affects security & resilience of Internet globally. That challenge would be amplified by other considerations such as mass-scale deployment of homogenous I.o.T. devices, ability of some devices to automatically connect to other devices, & likelihood of fielding these devices in unsecure environments. As matter of principle, developers & users of I.o.T. devices & systems have collective obligation to ensure they do not expose users & Internet itself to potential harm. Accordingly, collaborative approach to security would be needed to develop effective & appropriate solutions to I.o.T.security challenges that are well suited to scale & complexity of issues.

IoT Security Questions
A no. of questions has been raised regarding security challenges posed by Internet of Things devices. Many of these questions existed prior to growth of IoT, but they increase in importance due to scale of deployment of I.o.T. devices. Some prominent questions include:

a) Good Design Practices.
What are sets of best practices for engineers & developers to use to design I.o.T. devices to make them more secure? How do lessons learned from Internet of Things security problems get captured & conveyed to development communities to improve future generations of devices? What training & educational resources are available to teach engineers & developers more secure I.o.T. design?

b) Cost vs. Security Trade-Offs.
How do stakeholders make informed cost-benefit analysis decisions with respect to Internet of Things devices? How do we accurately quantify & assess security risks? What would motivate device designers & manufacturers to accept additional product design cost to make devices more secure, and, in particular, to take responsibility for impact of any negative externalities resulting from their security decisions? How would incompatibilities between functionality & usability be reconciled with security? How do we ensure I.o.T. security solutions support opportunities for I.o.T. innovation, social & economic growth?

c) Standards & Metrics.
What would be role of technical & operational standards for development & deployment of secure, well-behaving I.o.T. devices? How do we effectively identify & measure characteristics of I.o.T. device security? How do we measure effectiveness of Internet of Things security initiatives & countermeasures? How do we ensure security best practices are implemented?

d) Data Confidentiality, Authentication & Access Control.
What would be optimal role of data encryption with respect to I.o.T. devices? would be use of strong encryption, authentication & access control technologies in I.o.T .devices adequate solution to prevent eavesdropping & hijacking attacks of data streams these devices produce? Which encryption & authentication technologies could be adapted for Internet of Things, & how could they be implemented within I.o.T. device’s constraints on cost, size, & processing speed? What are foreseeable management issues that must be addressed as result of IoT-scale cryptography? Are concerns about managing crypto-key lifecycle & expected period during which any given algorithm would be expected to remain secure being addressed? Are end-to-end processes adequately secure & simple enough for typical consumers to use?

DOI10.17148/IJARCCE.2017.6521

e) Field-Upgradeability.
With extended service life expected for many I.o.T. devices, should devices be designed for maintainability & upgradeability in field to adapt to evolving security threats? New software & parameter settings could be installed in fielded I.o.T. device by centralized security management system if each device had integrated device management agent. But management systems add cost & complexity; could other approaches to upgrading device software be more compatible with widespread use of I.o.T. devices? Are there any classes of I.o.T. devices that are low-risk & therefore don't warrant these kinds of features? In general, are user interfaces I.o.T. devices expose (usually intentionally minimal) being properly scrutinized with consideration for device management (by anyone, including user)?

f) Shared Responsibility.
How could shared responsibility & collaboration for I.o.T. security be encouraged across stakeholders?

g) Regulation.
Should device manufacturers be penalized for selling software or hardware with known or unknown security flaws? How might product liability & consumer protection laws be adapted or extended to cover any negative externalities related to Internet of Things & would that operate in cross-border environment? Would it be possible for regulation to keep pace & be effective in light of evolving I.o.T. technology & evolving security threats? How should regulation be balanced against needs of permission-less innovation, Internet freedom, & freedom of expression?

h) Device Obsolescence.
What would be right approach to take with obsolete I.o.T. devices as Internet evolves & security threats change? Should I.o.T. devices be required to have built-in end-of-life expiration feature that disables them? Such requirement could force older, non-interoperable devices out of service & replace them with more secure & interoperable devices in future. Certainly, that would be very challenging in open marketplace. What are implications of automatic decommissioning I.o.T. devices?

IV. DISTRIBUTED IOT BASED HOME AUTOMATION SYSTEM

Distributed IOT Based home automation system, consists of server, hardware interface modules used. Server controls hardware one interface module, & could be easily configured to handle more hardware interface module. Hardware interface module in turn controls its alarms and actuators. Server is a normal PC, within built in Wi-Fi card, acts as web server. System could be accessed from web browser of any local PC in same LAN using server IP, or remotely from any PC or mobile handheld device connected to internet within appropriate web browser supports asp.net technology through server real IP. Wi-Fi technology is selected to be network infrastructure that connects server and hardware interface modules. Wi-Fi is chosen to improve system security by using secure Wi-Fi connection, & to increase system mobility & scalability.
Though user intends to add latest hardware interface modules out of coverage of central access point, repeaters or managed wireless LAN would perfectly solve that type of problem. Main functions of server are to manage, control, & monitor distrusted system components that enables hardware interface modules to execute their assigned tasks through actuators, & to report server within triggered events from sensors.

V. CONCLUSION

In order to program & control flow of information in Internet of Things, a predicted architectural direction is necessary. It is being called BPM. Everywhere that is a blending of traditional process management & special capabilities to automate control of large numbers of coordinated devices. In Internet of Things, significance of an event will not essentially base on a deterministic approach but would in its place to be based on framework of event itself: this is also being a semantic web. Consequently, this will not necessarily require common standards that will not be able to prefer every context or use: some actors' services, components, avatars accordingly be self-referenced & if ever needed, adaptive to active common standards. Some researchers give that sensor networks are most essential compo nent of Internet of Things.

REFERENCES

1. M1 Security & Automation Controls. http://www.elkproducts.com/m1 controls.html.
2. Apple app store. http://www.apple.com/osx/apps/app-store.html.
3. Control4 Home Automation and Control. http://www.control4.com.
4. http://www.phonearena.com/news/Androids-Google-Playbeats- App-Store-with-over-1-million-apps-now-o_ciallylargestid45680.
5. Jayavar dhana Gubbi,Rajkumar Buyya. Slaven Marusic, Marimuthu Palaniswami Internet of Things: A Vision, Architectural Elements, and Future Directions

6. Jayavardhana Gubbi,Rajkumar Buyya. Slaven Marusic, Marimuthu Palaniswami Internet of Things: A Vision, Architectural Elements, & Future Directions
7. 7. T.Abdelzaher, S.Prabh, & R.Kiran, On Real-Time Capacity Limits of ad hoc Wireless Sensor Networks, RTSS, December 2004.
8. 8.Y. Aguiar, M.Vieira, E. Galy, J.Mercantini, & C. Santoni, Refining a User Behavior Model based on Observation of Emotional States. COGNITIVE , 2011.
9. 9.V. Bradshaw. The Building Environment: Active & Passive Control Systems. John Wiley & Sons, Inc., River Street, NJ, USA, 2006.
10. 10.B. Brumitt, B. Meyers, J. Krumm, A. Kern, & S. A. Shafer. Easyliving: Technologies for Intelligent Environments. HUC, 2000.
11. 11.G. Burnham, J. Seo G. Bekey, A. Identification of Human Driver Models in Car Following. IEEE Transactions on Automatic Control 19, 6, 1974, pp. 911–915.
12. 12.J. Deng, R. Han, & S. Mishra, Secure Code Distribution in Dynamically Programmable Wireless Sensor Networks, Proc. of ACM/IEEE IPSN, 2006. pp. 292-300.
13. 13.R. Dickerson, E. Gorlin, & J. Stankovic, Empath: a Continuous Remote Emotional Health Monitoring System for Depressive Illness. Wireless Health , 2011.
14. 14. M. Huang, J. Li, X. Song, & H. Guo, Modeling Impulsive Injections of Insulin: Towards Artificial Pancreas. SIAM Journal of Applied Mathematics 72, 5, 2012, pp. 1524–1548.
15. 15.M. Kay, E. Choe, J. Shepherd, B. Greenstein, N. Watson, S. Consolvo, & J. Kientz, Lullaby: a Capture and Access System for Understanding the Sleep Environment. UbiComp, 2012.
16. 16. A Liu, & D. Salvucci, Modeling & Prediction of Human Driver Behavior, Intl. Conference on HCI , 2001.
17. 17. J. Lu, T. Sookoor, V. Srinivasan, G. Gao, B. Holben J. Stankovic, E. Field, & K. Whitehouse, The Smart Thermostat: Using Occupancy Sensors to Save Energy in Homes, ACM SenSys, 2010.
18. 18. M. Maroti, B. Kusy, G. Simon, & A. Ledeczi, The Flooding Time Synchronization Protocol, ACM SenSys, November 2004.
19. 19. S. Mohammed, P. Fraisse, D. Guiraud, P. Poignet, & H. Makssoud, Towards a Co-contraction Muscle Control strategy for Paraplegics. CDC-ECC, 2005.
20. S.Munir, J.Stankovic, C. Liang, & S. Lin, New Cyber Physical System Challenges for Human-in-the-Loop Control, 8th International Workshop on Feedback Computing, June 2013.

DOI10.17148/IJARCCE.2017.6521