International Journal of Emerging Engineering Research and Technology
Volume 3, Issue 2, February 2015, PP 7-11
ISSN 2349-4395 (Print) & ISSN 2349-4409 (Online)

Implementation of Internet of Things for Home Automation

Mamata Khatu, Neethu Kaimal, Pratik Jadhav, Syedali Adnan Rizvi

Department of Computer Engineering SKN-Sinhgad Institute of Technology and Science, Lonavala, Maharashtra, India

ABSTRACT

Internet of Things (IoT) is a concept that envisions all objects around us as part of internet. IoT coverage is very wide and includes variety of objects like smart phones, tablets, digital cameras and sensors. Once all these devices are connected to each other, they enable more and more smart processes and services that support our basic needs, environment and health. Such enormous number of devices connected to internet provides many kinds of services. They also produce huge amount of data and information. Cloud computing is one such model for on-demand access to a shared pool of configurable resources (computer, networks, servers, storage, applications, services, and software) that can be provisioned as infrastructures ,software and applications.

Cloud based platforms help to connect to the things around us so that we can access anything at any time and any place in a user friendly manner using customized portals and in built applications. Hence, cloud acts as a front end to access IoT. Applications that interact with devices like sensors have special requirements of massive storage to store big data, huge computation power to enable the real time processing of the data, information and high speed network to stream audio or video. Here we have describe how Internet of Things and Cloud computing can work together can address the Big Data problems. We have also illustrated about Sensing as a service on cloud using few applications like Augmented Reality, Agriculture, Environment monitoring,etc. Finally, we propose a prototype model for providing sensing as a service on cloud.

Keywords: Internet of Things, Wireless sensor Network, Home Automation, ZigBee; Energy Management; Secured hash function.

INTRODUCTION

In this paper, with a vision to achieving maximized automation we have reported an effective implementation for Internet of Things used for monitoring regular domestic conditions by means of low cost ubiquitous sensing system. It would effectively create a relay of machines that provide stimulus to each other and require the minimum human intervention. The description about the integrated network architecture and the interconnecting mechanisms for reliable measurement of parameters by smart sensors and transmission of data via internet is being presented.

The longitudinal learning system will be able to provide self-control mechanism for better operations of the devices during monitoring. The framework of the monitoring system is based on combination of pervasive distributed sensing units, information system for data aggregation, reasoning. The reliability of sensing information transmission through the proposed integrated network architecture is roughly 97%. The prototype will be tested to generate real-time graphical information.

IoT coverage is very wide and includes variety of objects like smart phones, tablets, digital cameras and sensors. Once all these devices are connected to each other, they enable more and more smart processes and services that support our basic needs, economies, environment, health etc. Such enormous number of devices connected to internet provides many kinds of services and produce huge amount of data and information.

Address for correspondence

khatumamata24@gmail.com

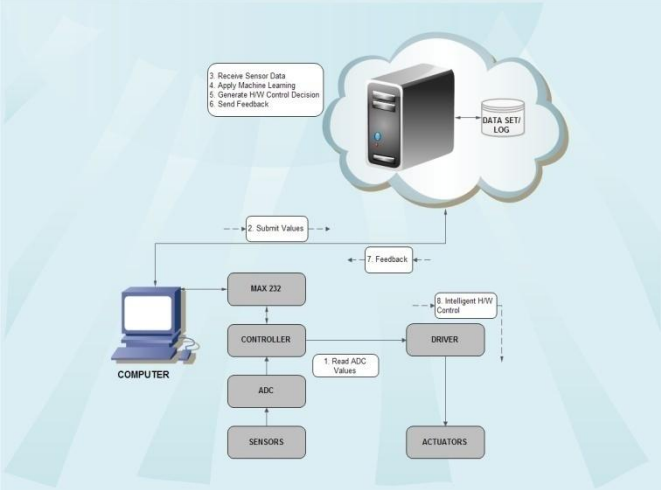

Fig1. *Detailed Architecture*

PROBLEM STATEMENT

Internet of Things (IoT) is a concept that visualizes all objects around us as part of internet. Internet of things coverage is very wide and includes variety of objects like smart phones, digital cameras, sensors, etc. Once all these devices are connected to each other, they enable more and more smart processes and services that support our basic needs, economies, environment, health etc. Such large number of devices connected to internet provides many kinds of services and produce huge amount of data and information. Cloud computing is a one such model for on-demand access to a shared pool of configurable resources (compute, networks, servers, storage applications, services, software etc.) that can be easily provisioned as Infrastructure, software and applications (SaaS). Cloud based platforms help to connect to the things around us so that we can access anything at any time and any place in a user friendly manner using customized portals and in built applications (SaaS). Hence, cloud acts as a front end to access IoT. Applications that interact with devices like sensors have special requirements of huge storage to store big data, huge computation power to enable the real time processing of the data i.e information, and high speed network to stream audio or video. In this paper, we describe how IoT and Cloud computing can work together to provide automation of domestic things so as to reduce human intervention and save time and energy.

LITERATURE REVIEWS

The Internet of Things (IoT) is the interconnection of uniquely identifiable embedded computing devices within the existing Internet framework.Typically, IoT is expected to offer advanced connectivity of devices and systems, and services that goes beyond M2M i.e. machine-to-machine communications and covers a variety of protocols, various domains, and applications. The interconnection of all these embedded devices which also includes smart objects, is expected to lead in automation in nearly all fields enabling advanced applications like a Smart Grid. According to Gartner, there will be nearly 26 billion devices on the Internet of Things by 2020. ABI Research has estimated that more than 30 billion devices will be wirelessly connected to the Internet of Things by 2020.According to the recent survey and study done by Pew Research Internet Project, a huge majority of the technology experts and engaged Internet users who responded 83 percent agreed with the conception that the Internet of Things, embedded, wearable computing will have widespread and beneficial effects by 2025.It is clear that the IoT will consist of a very large number of devices being connected to the Internet.

The Internet of Things (loT) refers to uniquely recognizable objects and their virtual representations in an Internet-like structure. Internet of Things refer to day-to-day objects, that are understandable, distinguishable, locatable, addressable, and or controllable via the Internet using either RFID, wireless LAN, wide-area network, or other means. These objects include not only the day to day usable electronic devices or the products of higher technological development such as vehicles and equipment, but also include various things like food, clothing, shelter; materials, their parts, and sub-assemblies; commodities and luxury items; boundaries, landmarks, and monuments; and all the miscellany of commerce and culture. Ubiquitous computing refers to a new genre of computing in which the computer completely permeates the life of the user. Internet of Things (IoT) will comprise

of billions of devices that can sense, communicate, calculate and potentially actuate. Data streams coming from these devices will challenge the traditional approaches to data management and contribute to the emerging paradigm of Big Data. IoT has burst onto the stage, interconnecting everyday objects over the Internet, which acts as everlasting sources of information. The occurrence has required a combination of three developments.

ALGORITHMS USED

A. Secured Hashing Algorithm(Sha1)

In cryptography, SHA-1 is a cryptographic hash function designed by the National Security Agency and published by the NIST as a U.S. Federal data Processing Standard. SHA stands for "secure hash algorithm". The three SHA algorithms are designed differently and are well-known as SHA0, SHA1, and SHA2. SHA-1 is very similar to SHA-0, but corrects the flaw in the original SHA hash specification that led to significant weaknesses. The SHA-0 algorithm was not implemented by many applications. On the other hand SHA-2 significantly differs from the SHA-1. SHA-1 is the very often used of the existing SHA hash functions, and is working in several widely-used security applications and protocols. SHA-1 produces a 160-bit message digest based on principles similar to those used by Ronald L. Rivest of MIT in the design of the MD4 and MD5 message digest algorithms, but has a more conventional design. The original description of the algorithm was published in 1993 as the Secure Hash Standard, FIPS PUB 180, by US government standards agency NIST (National Institute of Standards and Technology). This version is now often stated as SHA-0 hash function. It was withdrawn by NSA shortly after publication and was superseded by the reviewed version, published in 1995 in FIPS PUB 180-1 and commonly referred to as SHA-1. SHA-1 differs from SHA-0 only by a bitwise rotation in the message schedule of its compression function; this was done, according to NSA, to correct an error in the original algorithm which reduced its cryptographic security. However, NSA did not provide any further explanation or identify the error that was corrected. Weaknesses have consequently been reported in both SHA and SHA-1. SHA-1 appears to provide greater resistance to attacks, supporting the NSA's assertion that the change increased the security.

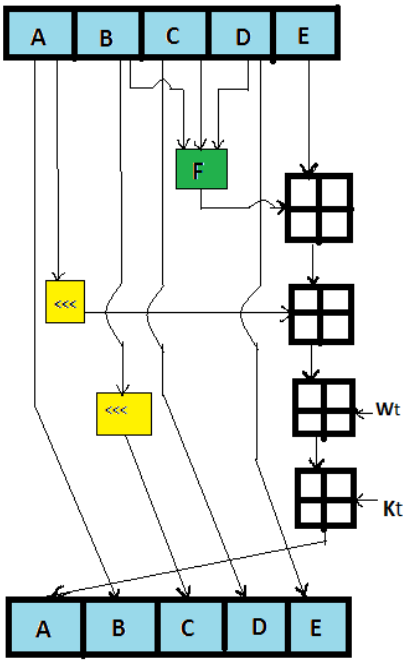

Fig5. *SHA1 Flow*

To maintain data integrity we create digital signature of particular data. Digital signature is used uniquely identify the data. When the data is reformed, SHA1 is used.

B. Naïve Bayes Algorithm

A **naive Bayes classifier** is a simple probabilistic classifier based on applying Bayes' theorem with strong (naive) independence assumptions. A more descriptive term for the underlying probability model would be "independent feature model". In simple terms, a naive Bayes classifier assumes that the presence (or absence) of a particular feature of a class isunrelated to the presence (or absence) of

any other feature, given the class variable. For example, a fruit may be considered to be an apple if it is red, round, and about 4" in diameter. Even if these features depend on each other or upon the existence of the other features, a naive Bayes classifier considers all of these properties to independently contribute to the probability that this fruit is an apple. Depending on the precise nature of the probability model, naive Bayes classifiers can be trained very efficiently in a supervised learning setting. In many practical applications, parameter estimation for naive Bayes models uses the method of maximum likelihood; in other words, one can work with the naive Bayes model without believing in Bayesian probability or using any Bayesian methods.

THE NAIVE BAYES PROBABILISTIC MODEL

Abstractly, the probability model for a classifier is

A conditional model

$$\boldsymbol{p(C|F1, \ldots\ldots, Fn)}$$

over a dependent class variable C with a small number of outcomes or classes, conditional on several feature variables $\boldsymbol{F1}$ through $\boldsymbol{Fn}$. The problem is that if the number of features is large or when a feature can take on a large number of values, then basing such a model on probability tables is infeasible. We therefore reformulate the model to make it more tractable.

Using Bayes' theorem, we write

$$\boldsymbol{P(C|F1, \ldots\ldots, Fn) = \frac{p(C)p(C|F1, \ldots\ldots, Fn|C)}{P(F1, \ldots\ldots, Fn)}}$$

In plain English the above equation can be written as

$$\textbf{posterior} = \frac{\textbf{prior} * \textbf{likelihood}}{\boldsymbol{evidence}}$$

The Bayes Naive classifier selects the most likely classification Vnb given the attribute values a1, a2, ….., an.

This results in:

$$\mathbf{V_{nb} = argmax_{\ vjE} V\ P_{(VJ)}\ YP_{(aijvj)}} \quad (1)$$

We generally estimate $\mathbf{P_{(aijvj)}}$ using m-estimates:

$$P_{(aijvj)} = n_c + m_p/n + m \quad (2)$$

Where:

n = the number of training examples for which $v = v_j$

n_c = number of examples for which $v = v_j$ and $a = a_i$

p = a priori estimate for $P_{(aijvj)}$

m = the equivalent sample size

PROPOSED SYSTEM

In our proposed system, we have portrayed a working model of the implementation of IOT in the household environment.

It encompasses the basic amenities present in a household and offers ways to manipulate the use without any human intervention; that being the basic concept of Internet of Things. A relay of such machines would effectively exhibit the potential and economy of the IoT implementation in the household.

A. Architecture

The process would initiate with the sensor registering an anomaly. The anomaly would be in the form of actuators which would set off the sensors. Then after the ADC, Controller would send the data to the cloud. The cloud would process the response and react according to the default algorithm of the said device. The Naïve Bayes Algorithm would be used in this process.

CONCLUSION AND FUTURE WORK

The Internet has changed drastically the way we live, moving interactions between people at a virtual level in several contexts spanning from the professional life to social relationships. The IoT has the potential to add a new dimension to this process by enabling communications with smart objects, thus leading to the vision of ''anytime, anywhere, any media, anything" communications.

To this purpose, we observe that the Internet of Things should be considered as part of the overall Internet of the future, which is likely to be vividly different from the Internet we use today.

FUTURE ENHANCEMENT

In the near future the Internet and wireless technologies will connect different sources of information such as sensors, mobile phones and cars in a tighter manner. The number of devices which connect to the Internet is – seemingly exponentially – increasing. These billions of components produce, consume and process information in different environments such as logistic applications, factories, airports and in the work and everyday lives of people. The society need new and scalable, compatible and secure solutions for both the management of the ever more broad, complexly-networked Internet of Things, and also for the support of various business models.

REFERENCES

[1]. *D. Giusto, A. Iera, G. Morabito, L. Atzori (Eds.), The Internet of Things, Springer, 2010. ISBN: 978-1-4419-1673-0.*

[2]. *National Intelligence Council, Disruptive Civil Technologies – Six Technologies with Potential Impacts on US Interests Out to 2025 –Conference Report CR 2008-07, April 2008, <http://www.dni.gov/nic/NIC_home.html>.L. Atzori et al. / Computer Networks 54 (2010) 2787–2805 2803*

[3]. *INFSO D.4 Networked Enterprise & RFID INFSO G.2 Micro &Nano systems, in: Co-operation with the Working Group RFID of the ETP EPOSS, Internet of Things in 2020, Roadmap for the Future, Version 1.1, 27 May 2008.*

[4]. *INTERNET Auto-Id Labs, <http://www.autoidlabs.org/>.*

[5]. *The EPCgobal Architecture Framework, EPCgobal Final Version 1.3, Approved 19th march 2009, <www.epcgloballinc.org>*

[6]. *K. Sakamura, Challenges in the age of ubiquitous computing: a case study of T-engine – an open development platform for embedded systems, in: Proceedings of ICSE'06, Shanghai, China, and May 2006.*

[7]. *M. Presser, A. Gluhak, and The Internet of Things: Connecting the Real World with the Digital World, EURESCOM mess@ge – The Magazine for Telecom Insiders, vol. 2, 2009, <http://www.eurescom.eu/message>.*

[8]. *M. Botterman, for the European Commission Information Society and Media Directorate General, Networked Enterprise & RFID Unit –D4, Internet of Things: An Early Reality of the Future Internet, Report of the Internet of Things Workshop, Prague, Czech Republic, May2009.*

[9]. *B. Sterling, Shaping Things – Media work Pamphlets, The MIT Press, 2005.*

[10]. *ITU Internet Reports, the Internet of Things, November 2005.*