RESEARCH ARTICLE OPEN ACCESS

A Strategic Review on Internet of Things (IOT)

Bijoy Tapan Mohan Nayak, U Abinash Patro,
Gandhi Institute of Excellent Technocrats, Bhubaneswar, India
Vijayanjali Institute of Technology, Balasore, Odisha, India

ABSTRACT
Internet, a revolutionary invention, is always transforming intosome new kind of hardware and software making it unavoidablefor anyone. The form of communication that we see now is eitherhuman-human or human-device, but the Internet of Things (IoT)promises a great future for the internet where the type of commu-nicationismachine-machine(M2M).Thispaperaimstoprovidea comprehensive overview of the IoT scenario and reviews its en-abling technologies and the sensor networks. Also, it describes asix-layered architecture of IoT and points out the related key chal-lenges.
Keywords: InternetofThings,RFID,WSN,IOTarchitecture,IoTVision,IoTapplications,IoTsecurity.

I. INTRODUCTION

With the continuous advancements in technology a potential in-novation,IoTiscomingdowntheroadwhichisburgeoning asan ubiquitous global computing network where everyone and ev-erything will be connected to the Internet [1]. IoT is continuallyevolving and is a hot research topic where opportunities are infi-nite.Imaginationsareboundlesswhichhaveputitonthe vergeof reshaping the current form of internet into a modified and inte-grated version. The number of devices availing internet services isincreasing every day and having all of them connected by wire orwirelesswillputapowerfulsourceofinformationatou rfingertips.Theconceptofenablinginteractionbetwee nintelligentmachinesisa cutting-edge technology but the technologies composing the IoTare not something new for us [2]. IoT, as you can guess by its name,istheapproachofconvergingdataobtainedfromd ifferentkindsofthingstoanyvirtualplatformonexisting Internetinfrastructure[3].

The concept of IoT dates back to 1982 when a modified coke ma-chine was connected to the Internet which was able to report thedrinks contained and that whether the drinks were cold [4].

Later,in1991,acontemporaryvisionofIoTintheformo fubiquitous

computing was first given by Mark Weiser [5]. However in 1999,Bill Joy gave a clue about Device to Device communication in histaxonomyofinternet[6].Intheverysameyear,Kevin Ashtonpro-posed the term ”Internet of Things” to describe a system of inter-connecteddevices[7].

The basic idea of IoT is to allow autonomous exchange of usefulinformation between invisibly embedded different uniquely iden-tifiable real world devices around us, fueled by the leading tech-nologieslikeRadio-FrequencyIDentification(RFID)andWirelessSensor Networks (WSNs) [2] which are sensed by the sensor de-vices and further processed for decision making, on the basis ofwhichanautomatedactionisperformed[1].

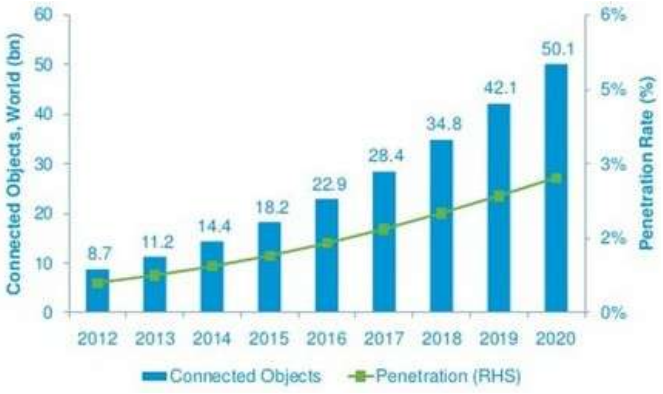

Fig. 1.Expected penetration of connected objects by the year 2020, ac-cordingtoCisco

Thepaperisorganizedasfollows.Section2analyzesthevisionofthe IoT. Section 3 describes the generic architecture of the IoT. Sec-tion 4 discusses the technologies that IoT is composed of. Section5 forecaststhefutureapplications.Section6discusses theprivacyand security challenges posed by IoT and finally Section 7 con-cludesthepaper.

VISION

In 2005, ITU reported about a ubiquitous networking era in whichall the networks are interconnected and everything from tires toattireswillbeapartofthishugenetwork[8].Imagineyourselfdo-ing an internet search for your watch you lost somewhere in yourhouse. So this is the main vision of IoT, an environment wherethings are able to talk and their data can be processed to performdesired tasks through machine learning [9]. A practical implemen-tation of IoT is demonstrated by a soon-to-be released Twine, acompactandlow-powerhardwareworkingtogetherwithreal-timeweb software to make this vision a reality [10]. However differentpeople and organizations have their own different visions for theIoT[11].

An article published in Network World revealed IoT strategies oftop IT vendors, they carried out some interviews from the key ITvendors. As of HP's vision, they see a world where people are always connected to their content. Cisco believes in the industrialautomationandconvergenceofoperationaltechnology.Intelisfo-cusedonempoweringbillionsofexistingdeviceswithintelligence.Microsoft does not consider IoT as any futuristic technology; theybelieve that it already exists in today's powerful devices and thatthedevicesjustneedtobeconnectedforalargeamountofinforma-tion which could be helpful. While, IBM has a vision of a SmarterPlanetbyremotelycontrollingthedevicesviasecuredservers[12].

Despite of having different visions, they all agree about a networkof interconnected devices therefore more developments within thecoming decades are expected to be seen including that of a newconvergedinformationsociety[13].

ARCHITECTURE

Morethan25Billionthingsareexpectedtobeconnectedby2020 [14]whichisahugenumbersotheexistingarchitectureofInternetwith TCP/IP protocols, adopted in 1980 [15], cannot handle a net-workasbigasIoTwhichcausedaneedforanewopenarchitecturethat could address various security and Quality of Service (QoS)issues as well as it could support the existing network applicationsusingopenprotocols[16].Withoutaproperprivacyassurance,IoTis not likely to be adopted by many [17]. Therefore protection ofdataandprivacyofusersarekeychallengesforIoT[18].

ForfurtherdevelopmentofIoT,anumberofmulti-layeredsecurityarchitectures are proposed. [19] described a three key level architectureofIoTwhile[20]describedafourkeylevelarchitecture.

[21] proposed a five layered architecture using the best features ofthe architectures of Internet and Telecommunication managementnetworks based on TCP/IP and TMN models respectively. Similarlyasix-layeredarchitecturewasalsoproposedbasedonthenetwork hierarchical structure [22]. So generally it's divided into sixlayersasshownintheFig.2.

ThesixlayersofIoTaredescribedbelow:

1.1 CodingLayer

CodinglayeristhefoundationofIoTwhichprovidesidentificationto the objects of interest. In this layer, each object is assigned auniqueIDwhichmakesiteasytodiscerntheobjects[22].

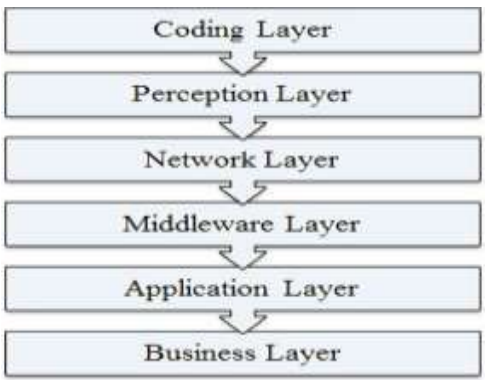

Fig.2.Six-LayeredArchitectureofIoT

1.2 PerceptionLayer

This is the device layer of IoT which gives a physical meaning toeachobject.Itconsistsofdatasensorsindifferentform slikeRFIDtags, IR sensors or other sensor networks [23] which could sensethe temperature, humidity, speed and location etc of the objects.This layer gathers the useful information of the objects from thesensor devices linked with them and converts the information intodigital signals which is then passed onto the Network Layer forfurtheraction.

1.3 NetworkLayer

The purpose of this layer is receive the useful information in theformofdigitalsignalsfromthePerceptionLayerand transmititttotheprocessingsystemsintheMiddlewareL ayerthroughthetrans-missionmediumslikeWiFi,Bluetooth,WiMaX,Zigbe e,GSM,3GetcwithprotocolslikeIPv4,IPv6,MQTT,D DSetc[24].

1.4 MiddlwareLayer

This layer processes the information received from the sensor de-vices[2].ItincludesthetechnologieslikeCloudcomput ing,Ubiq-uitous computing which ensures a direct access to the database tostore all the necessary information in it. Using some Intelligent Pro-cessing Equipment, the information is processed and a fully auto-mated action is taken based on the processed results of the infor-mation.

1.5 ApplicationLayer

ThislayerrealizestheapplicationsofIoTforal lkindsofindustry,basedontheprocesseddata.Because applicationspromotethede-velopmentofIoTsothislayerisveryhelpfulinthelarges calede-velopmentofIoTnetwork[21].TheIoTrelatedapplicat ionscouldbesmarthomes,smarttransportation,smartp lanetetc.

1.6 BusinessLayer

This layer manages the applications and services of IoT and is re-sponsible for all the research related to IoT. It generates differentbusinessmodelsforeffectivebusinessstrategi es[1].

II. TECHNOLOGIES

The development of a ubiquitous computing system where digi-tal objects can be uniquely identified and can be able to think andinteract with other objects to collect data on the basis of which au-tomated actions are taken, requires the need for a combination ofnew and effective technologies which is only possible through anintegrationofdifferenttechnologieswhichcanmake theobjectstobeidentifiedandcommunicatewitheacho ther[25].Inthissectionwediscusstherelevanttechnolo giesthatcanhelpinthelarge-scaledevelopmentofIoT.

1.7 RadioFrequencyIDentification(RFID)

RFID is the key technology for making the objects uniquely iden-tifiable. Its reduced size and cost makes it integrable into any ob-ject[19].Itisatransceivermicrochipsimilartoanadhesi vestickerwhich could be both active and passive, depending on the type ofapplication[26].Activetagshaveabatteryattachedto themdueto which they are always active and therefore continuously emitthedatasignalswhilePassivetagsjustgetactivated whentheyaretriggered. Active tags are more costly than the Passive tags howeverthey have a wide range of useful applications [2]. RFID system iscomposed of readers and associated RFID tags which emit the iden-tification, location or any other specifics about the object, on get-tingtriggeredbythegenerationofanyappropriatesigna l[27].Theemitted object related data signals are transmitted to the Readersusing radio frequencies which are then passed onto the processorstoanalyzethedata.

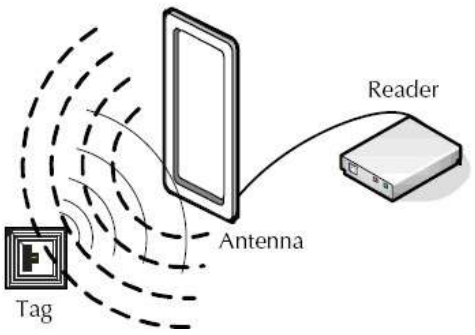

Fig.3.RFIDScenario

Depending on the type of application, RFID frequencies are dividedintofourdifferentfrequenciesranges[28],whicharegivenbelow:

(1) Lowfrequency(135KHzorless)
(2) HighFrequency(13.56MHz)
(3) Ultra-HighFrequency(862MHz928MHz)
(4) MicrowaveFrequency(2.4G,5.80)

BarCodeisalsoanidentificationtechnology whichhasalmostthesame function as an RFID but RFID is more effective than a BarCode due to a number of its benefits. RFID being a radio technology doesn't require the reader to be physically in its vision whileBar Code is an optical technology which cannot work unless itsreader is placed in front of it. Moreover, an RFID can work as anactuator to trigger different events and it has even modification abilitieswhichBarcodesclearlydon'thave.

1.8 WirelessSensorNetwork(WSN)

WSNisabi-directionalwirelesslyconnectednetworkofsensorsina multi-hop fashion, built from several nodes scattered in a sensorfieldeachconnectedtooneorseveralsensorswhichcancollecttheobject specific data such as temperature, humidity, speed etc andthen pass on to the processing equipment [26]. The sensing nodescommunicate in multi-hop Each sensor is a transceiver having anantenna, a micro-controller and an interfacing circuit for the sensorsas a communication, actuation and sensing unit respectively alongwith a source of power which could be both battery or any energyharvestingtechnology[29]However[2]haspro posedanadditionalunit for saving the data, named as Memory Unit which could alsobe a part of the sensing node. A typical sensing node is shown inthefigurebelow:

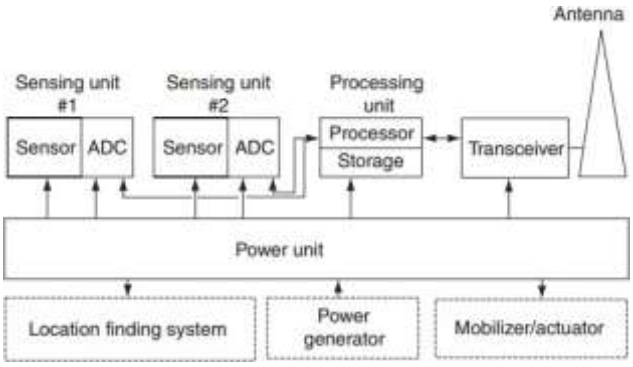

Fig.4.Atypicalsensingnode

WirelessSensorsNetworktechnologyandRFIDtechnologywhencombined together opens up possibilities for even more smart de-vices, for which a number of solutions have been proposed [26]. AnexamplesolutionisprovidedbytheIntelResearchLabsintheformof Wireless Identification Sensing Platform (WISP) [30]. WISP is apassivewirelesssensornetworkwithbuilt-inlight,temperatureandmany other sensors [31]. Both WSN and RFID Sensor Networkshave their own advantages but RFID Sensor Networks have a lowrangeandtheircommunicationisAsymmetricwhileWSNshavea comparatively longer range and their communication is Peer-to-Peer.MoreovermostoftheWSNsarebasedontheIEEE 802.15.4standard[26],whichspecifiesthePhysicalandMAClayerofLow-RateWirelessPersonalAreaNetworks(LR-WPANs)[32].

ThetechnologiesthatenablestheintegrationofWSNwiththeIOTare a hot research topic, many solutions have been proposed for thatincluding that of a 6LOWPAN standard [33], that allows IPv6 packetstobetransmittedthroughthenetworksthatarecomputationallyrestricted.Alsothere'sROLLroutingstandardforend-to-endrout-ingsolutions[34].

1.9 CloudComputing

Withmillionsofdevicesexpectedtocomeby2020[14],thecloudseems to be the only technology that can analyze and store all thedataeffectively.Itisanintelligentcomputingtechnologyinwhichnumber of servers are converged on one cloud platform to allowsharingofresourcesbetweeneachotherwhichcanbeaccessedat any time and any place [35]. Cloud computing is the most importantpartofIoT,whichnotonlyconvergestheservers butalsoprocesseson an increased processing power and analyzes the useful infor-mation obtained from the sensors and even provide good storagecapacity[36].Butthisisjustabeginningofunleashingthetruepo-tential of this technology. Cloud computing interfaced with smartobjects using potentially millions of sensors can be of

enormousbenefitsandcanhelpIoTforaverylargescale developmentsore-searches are being carried out since IoT will be totally dependentontheCloudComputing.

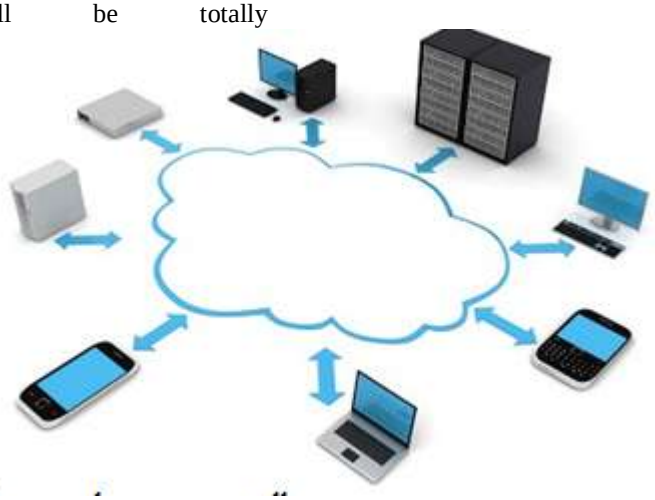

Fig.5.AtypicalCloudComputingScenario

1.10 NetworkingTechnologies

These technologies have an important role in the success of IoTsince they are responsible for the connection between the objects,soweneedafastandaneffectivenetworktohandlealargenumberofpotentialdevices.Forwide-rangetransmissionnetworkwecom-monly use 3G, 4G etc. but As we know, mobile traffic is so muchpredictablesinceitonlyhastoperformtheusualtaskslikemakingacall,sendingatextmessageetc.soaswestepintothismodderneraof ubiquitous computing, it will not be predictable anymore whichcallsforaneedofasuper-fast,super-efficientfifthgenerationwire-lesssystemwhichcouldofferalotmorebandwidth[37]. Similarlyforashort-rangecommunicationnetworkweusetechnologieslike Bluetooth,WiFietc.

1.11 NanoTechnologies

This technology realizes smaller and improved version of the thingsthat are interconnected. It can decrease the consumption of a sys-tem by enabling the development of devices in nano meters scalewhich can be used as a sensor and an actuator just like a normaldevice.SuchananodeviceismadefromnanocomponentsandtheresultingnetworkdefinesanewnetworkingparadigmwhichisInternetofNano-Things[38].

1.12 Micro-Electro-Mechanical Systems (MEMS)Technologies

MEMS are a combination of electric and mechanical componentsworkingtogethertoprovideseveralapplicationsincludingsensingand actuating which are already being commercially used in manyfieldintheformoftransducersandaccelerometer setc.MEMScombined with Nano technologies are a cost-effective solution forimprovising the communication system of IoT and other advan-tages like size reduction of sensors and actuators, integrated ubiq-uitouscomputingdevicesandhigherrangeoffrequenciesetc[39].

1.13 OpticalTechnologies

RapiddevelopmentsinthefieldofOpticaltechnologiesintheformof technologies like Li-Fi and Cisco's BiDi optical technologycould be a major breakthrough in the development of IoT. Li-Fi,anepoch-makingVisibleLightCommunication(VLC)technology,willprovideagreatconnectivityonahigherbandwidthfortheob-jects interconnected on the concept of IoT. Similarly Bi-Directional(BiDi) technology gives a 40G ethernet for a big data from multi-fariousdevicesofIoT[40].

III. APPLICATIONS

Most of the daily life applications that we normally see are al-ready smart but they are unable to communicate with each otherand enabling them to communicate with each other and share use-ful information with each other will create a wide range of inno-vative applications [41]. These emerging applications with someautonomouscapabilitieswouldcertainlyimprovethequalityofourlives. A few of such applications are already in the market [26], let'staketheexampleoftheGoogleCarwhichisaninitiativetoprovideaself-drivingcarexperiencewithreal-timetraffic,roadconditions,weather and other information exchanges [42], all due to the con-ceptofIoT.Thereareanumberofpossiblefutureapplicationsthatcan be of great advantage. In this section,

we present few of theseapplications.

5.0.1 SmartTrafficSystem.Trafficisanimportantp artofasoci-ety therefore all the related problems must be properly addressed.There is a need for a system that can improve the traffic situationbased on the traffic information obtained from objects using IoTtechnologies [43]. For such an intelligent traffic monitoring sys-tem, realization of a proper system for automatic identification ofvehicles and other traffic factors is very important for which weneed IoT technologies instead of using common image processingmethods[44].Theintelligenttrafficmonitorin gsystemwillprovidea good transportation experience by easing the congestion. It willprovide features like theft-detection, reporting of traffic accidents,lessenvironmentalpollution.Theroadsofthi ssmartcitywillgivediversions with climatic changes or unexpected traffic jams due towhich driving and walking routes will be optimized [1]. The traf-fic lighting system will be weather adaptive to save energy. Avail-ability of parking spaces throughout the city will be accessible byeveryone.

5.0.2 SmartEnvironment.Predictionofnaturaldis asterssuchasflood,fire,earthquakesetcwillbepossible duetoinnovativetech-nologies of IoT. There will be a proper monitoring of air pollutionintheenvironment.

5.0.3 SmartHome.IoTwillalsoprovideDIYsoluti onsforHome Automation with which we will be able to remotely con-trol our appliances as per our needs. Proper monitoring of utilitymeters, energy and water supply will help saving resources anddetecting unexpected overloading, water leaks etc. There will beproperencroachmentdetectionsystemwhichwillpr eventburglar-ies. Gardening sensors will be able to measure the light, humidity,temperature, moisture and other gardening vitals, as well as it willwatertheplantsaccordingtotheirneeds.

5.0.4 Smart Hospitals.Hospitals will be equipped with smartflexiblewearableembeddedwithRFIDtagswhic hwillbegiventothe patients on arrivals, through which not just doctors but nurseswillalsobeabletomonitorheartrate,bloodpress ure,temperatureand other conditions of patients inside or outside the premises ofhospital[45].Therearemanymedicalemergenciessu chascardiacarrest but ambulances take some time to reach patient, Drone Am-bulances are already in the market which can fly to the scene withtheemergencykitsoduetopropermonitoring,doct orswillbeableto track the patients and can send in the drone to provide quickmedicalcareuntiltheambulancearrive.

5.0.5 Smart Agriculture.It will monitor Soil nutrition, Light,Humidity etc and improve the green housing experience by au-tomatic adjustment of temperature to maximize the production.Accurate watering and fertilization will help improving the waterqualityandsavingthefertilizersrespectively[46] .

5.0.6 Smart Retailing and Supply-chain Management.IoT withRFID provides many advantages to retailers. With RFID equippedproducts, a retailer can easily track the stocks and detect shoplift-ing.Itcankeepatrackofalltheitemsinastoreandtopreve ntthemfromgoingout-of-stock,itplacesanorderautomatically.Moreoverthe retailer can even generate the sales chart and graphs for effec-tivestrategies.

IV. SECURITY AND PRIVACY CHALLENGES

IoTmakeseverythingandpersonlocatablean daddressablewhichwill make our lives much easier than before; however without alackofconfidenceaboutthesecurityandprivacyofthe user'sdata,it'smoreunlikelytobeadoptedbymany[47] .Soforitsubiquitousadoption, IoT must have a strong security infrastructure. Some ofthepossibleIoTrelatedissuesareasfollowed:

1.14 UnauthorizedAccesstoRFID

Anunauthorizedaccesstotagsthatcontainsth eidentificationdatais a major issue of IoT which can expose any kind of confidentialinformationabouttheusersoitneedstobea ddressed.Notjustthetagcanbereadbyamiscreantreade rbutitcanevenbemodifiedorpossiblybedamaged.Inth iscontext,[47]summarizedsomeofthereallifethreatso fRFIDwhichincludesRFIDVirus,SideChannelAttac kwithacell-phoneandSpeedPassHack.

1.15 Sensor-NodesSecurityBreach

WSNs are vulnerable to several types of attacks because sensornodesarethepartofabi-directionalsensornetworkasdiscussedinSection 4.2, which means other than the transmission of data, ac-quisitionofdataisalsopossible.[48]describedsomeoft hepossi-ble attacks that includes Jamming, tampering, Sybil, Flooding andsomeotherkindsofattacks,whicharesummarizeda sfollowed:

(1) Jamming obstructs the entire network by interfering with thefrequenciesofsensornodes.

(2) Tamperingistheformofattackinwhichtheno dedatacanbe extracted or altered by the attacker to make a controllablenode.

(3) Sybil attack claims multiple pseudonymous identities for

anodewhichgivesitabiginfluence.

(4) Flooding is a kind of a DOS attack caused by a large amountoftrafficthatresultsinmemoryexhaustion.

1.16 CloudComputingAbuse

Cloud Computing is a big network of converged servers whichallow sharing of resources between each other. These shared re-sources can face a lot of security threats like Man-in-the-middleattack (MITM), Phishing etc. Steps must be taken to ensure thecomplete security of the clouding platform [49]. Cloud SecurityAlliance (CSA) proposed some possible threats among which feware Malicious Insider, Data Loss, Accounts Hijacking and Mon-strous use of Shared Computers etc [50] which are summarized asfollowed:

(1) MaliciousInsiderisathreatthatsomeonefrom theinsidewhohaveanaccesstotheuser'sdatacouldbein volvedindatama-nipulating.

(2) Data Loss is a threat in which any miscreant user who has anunauthorized access to the network can modify or delete theexistingdata.

(3) Man-in-the-middle (MITM) is a kind of Account Hijackingthreat in which the attacker can alter or intercept messages inthecommunicationbetweentwoparties.

(4) Cloud computing could be used in a monstrous ways because iftheattackergetstouploadanymalicioussoftwareinth eserver
e.g. using a zombie-army (botnet), it could get the attacker acontrolofmanyotherconnecteddevices.

V. CONCLUSION

With the incessant burgeoning of the emerging IoT technologies,the concept of Internet of Things will soon be inexorably develop-ing on a very large scale. This emerging paradigm of networkingwill influence every part of our lives ranging from the automatedhouses to smart health and environment monitoring by embeddingintelligence into the objects around us. In this paper we discussedthe vision of IoT and presented a well-defined architecture for itsdeployment. Then we highlighted various enabling technologiesandfewoftherelatedsecuritythreats.And finallywediscusseda number of applications resulting from the IoT that are expectedtofacilitateusinourdailylives.Researches arealreadybeingcar-ried out for its wide range adoption, however without addressingthe challenges in its development and providing confidentiality oftheprivacyandsecuritytotheuser,it'shighlyunlikely forittobe an omni-present technology. The deployment of IoT requiresstrenuouseffortstotackleandpresentsolutions foritssecurityandprivacythreats.

REFERENCES

[1] Rafiullah Khan, SarmadUllah Khan, RifaqatZaheer andShahidKhan,"FutureInternet:TheInternet ofThingsArchi-tecture, Possible Applications and Key Challenges," in Pro-ceedingsofFrontiersofInformationTechnolog y(FIT),2012,pp.257-260

[2] GuichengShen and Bingwu Liu, "The visions, technologies,applicationsandsecurityissuesof InternetofThings,"inE-BusinessandE-Government(ICEE),2011,pp.1-4

[3] Ling-yuanZeng,"ASecurityFrameworkforInternet ofThings Based on 4G Communication," in Computer ScienceandNetworkTechnology(ICCSNT),2 012,pp.1715-1718

[4] "The "Only" Coke Machine on the Internet," Carnegie MellonUniversity,SchoolofComputerScience .

[5] M. Weiser, "The computer for the 21st century", Sci. Amer.,1991,pp.66-75

[6] JasonPontin,"BillJoy'sSixWebs,"MITTechn ologyReview,29September2005

[7] KevinAshton,"That'InternetofThings'Thing ",RFIDJour-nal,22June2009

[8] H.D. Ma, "Internet of things: Objectives and scientific chal-lenge," in Journal of Computer Science and Technology,2011,pp.919-924

[9] NichHeath,"WhattheInternetofThingsmeansf oryou".It can be accessed at:http://www.techrepublic.com/blog/europe an-technology/what-the-internet-of-things-means-for-you

[10] "Twine"bySupermechanical.Itcanbeaccessed at:http://supermechanical.com/twine

[11] De-Li Yang, Feng Liu and Yi-Duo Liang, "A Survey of the In-ternetofThings",inInternationalConferenceo nE-BusinessIntelligence(ICEBI),2010

[12] BobViolino,"TopITVendorsrevealtheirIOTst rategies".It can be accessed at:http://www.networkworld.com/article/260 4766/internet-of-things/top-it-vendors-reveal-their-iot-strategies.html

[13] HaraldSundmaeker, Patrick Guillemin, Peter Friess, SylvieWoelffl, "Vision and challenges for realising the Internet ofThings,"PublicationsOfficeoftheEuropean Union,2010

[14] Gartner,Inc.Itcanbeaccessedat:http://www.gartner.com/newsroom/id/2905717
[15] ”FromtheARPANETtotheInternet”byRonda Hauben-TCPDigest(UUCP).Retrieved2007-07-05Itcanbeaccessedat:http://www.columbia.edu/rh120/other/tcpdigestpaper.txtJian An, Xiao-Lin Gui, Xin He, ”Study on the ArchitectureandKeyTechnologiesforInternet ofThings,”inAdvancesinBiomedicalEngineering,Vol.11,IERI-2012,pp.329-335
[16] Lan Li, ”Study of Security Architecture in the Internet ofThings,” in Measurement, Information and Control (MIC),2012,Volume:1,pp.374-377
[17] ”TheInternetofThings,”ITUReport,Nov2005
[18] Wang Chen, ”AN IBE BASED SECURITY SCHEME OFINTERNET OF THINGS,” in Cloud Computing and IntelligentSystems(CCIS),2012,pp.1046,1049
[19] HuiSuo, Jiafu Wan, CaifengZou, Jianqi Liu, ”Security inthe Internet of Things: A Review,” in Computer Science andElectronicsEngineering(ICCSEE),2012,pp.648-651
[20] Miao Wu, Ting-lie Lu, Fei-Yang Ling, ling Sun, Hui-Ying Du,”Research on the architecture of Internet of things,” in Advanced Computer Theory and Engineering (ICACTE), 2010,pp.484-487
[21] XuCheng,MinghuiZhang,FuquanSun,”Architectureofin-ternet of things and its key technology integration based-onRFID,” in Fifth International Symposium on ComputationalIntelligenceandDesign,pp.294-297,2012
[22] DebasisBandyopadhyay, JaydipSen, ”Internet of Things - ApplicationsandChallengesinTechnologyand Standardization”inWirelessPersonalCommunications,Volume58,Issue1,pp.49-69
[23] YingZhang,”TechnologyFrameworkoftheInternetofTHings and Its Application,” in Electrical and Control Engineering(ICECE),2011,pp.4109-4112
[24] Benjamin Khoo, ”RFID as an Enabler of the Internet ofThings:IssuesofSecurityandPrivacy,”inInternetofThings(iThings/CPSCom),2011,pp.709-712
[25] L.Atzori,A.Iera,G.Morabito,”TheInternetofThings:Asur-vey,”inComputerNetworks-ScienceDirect
[26] H. Zhang, L. Zhu, ”Internet of Things: Key technology, ar-chitecture and challenging problems”, in Computer Scienceand Automation Engineering (CSAE), 2011, Volume: 4, pp.507-512
[27] L.G.Guo,Y.R.Huang,J.Cai,L.G.QU,”InvestigationofAr-chitecture, Key Technology and Application Strategy for theInternetofThings,”inCrossStraitQuad-RegionalRadioSci-enceandWirelessTechnologyConference(CSQRWC),2011,Volume:2,pp.1196-1199
[28] Sohraby,K.,Minoli,D.,Znati,T.”Wirelesssensornet-works: technology, protocols, and applications”, John WileyandSons,2007ISBN978-0-471-74300-2,pp.15-18
[29] ”WISP”byIntelLabs;Itcanbeaccessedat:http://wisp.wikispaces.com
[30] E. M. Tapia, S. S. Intille, and K. Larson, ”Portable wirelesssensorsforobjectusagesensingintheh ome:Challengesandpracticalities,” in Proceedings of the European Ambient IntelligenceConference.vol.LNCS4794BerlinHeidelberg:Springer-Verlag2007
[31] IEEE802.15WPANTaskGroup4.Itcanbeaccessedat:http://www.ieee802.org/15/pub/TG4.html
[32] G.Montenegro,N.Kushalnagar,J.Hui,D.Culler,”Transmis-sionofIPv6PacketsoverIEEE802.15.4Networks”
[33] R. Roman, C. ALcaraz, J.Lopez, N. Sklavos, ”Key Manage-ment Systems for Sensor Networks in the Context of the InternetofThings,”Computers&ElectricalEngineering,Volume:37,Issue:2,2011,pp.147-159
[34] B.B.P.Rao,P.Saluia,N.Sharma,A.Mittal,S.V. Sharma,”CloudcomputingforInternetofThings&sensingbasedap-plications,” in Sensing Technology (ICST), 2012 Sixth InternationalConference,IEEE
[35] X.Xiaohui, ”Study on Security Problems and Key TechnologiesofTheInternetofThings,”ComputationalandInformationSciences(ICCIS),2013,pp.407-410
[36] O.Vermesan, P.Friess, ”Internet of Things ? From ResearchandInnovationtoMarketDeployment,”RiverPublishers,pp.74-75
[37] I.AkyildizandJ.Jornet,”THEINTERNETOFNANO-THINGS,” IEEE Wireless Communications, Volume: 17 Issue:6,2010,pp.58-63
[38] V.M.Lubecke,Jung-ChihChiao,”MEMStechnologiesforenablinghighfrequencycommunicationscircuits,”inTelecommunications in Modern Satellite, Cable and BroadcastingServices,1999,Volume:2,pp.382-389

[39] ”Cisco40GigabitModule”.Itcanbeaccessedat: http://www.cisco.com/c/en/us/products/interfaces-modules/40-gigabit-modules/index.html
[40] R. Abdmeziem, D.Tandjaoui, ”Internet of Things: Concept,Building blocks, Applications and Challenges, ComputersandSociety,CornellUniversity”
[41] ”Whatwe’redrivingat,”GoogleOfficialBlog.Itcanbeaccessedat:http://googleblog.blogspot.com/2010/10/what-were-driving-at.html
[42] Y.Cao,W.Li,J.Zhang,”Real-timetrafficinformationcollect-ing and monitoring system based on the internet of things,”inPervasiveComputingandApplications(ICPCA),20116thInternationalConference, pp.45-49
[43] L.Xiao,Z.Wang,”InternetofThings:ANewApplicationforIntelligentTrafficMonitoringSystem,”inJOURNALOFNETWORKS,2011
[44] P.Fuhrer,D.Guinard,”BuildingaSmartHospitalusingRFIDtechnologies,”
[45] F.TongKe, ”Smart Agriculture Based on Cloud ComputingandIoT,”inJournalofConvergence InformationTechnology(JCIT),Jan’13
[46] ”RFIDSecurityIssues-Generation2Security”.Itcanbeaccessedat:http://www.thingmagic.com/index.php/rfid-security-issues
[47] Y.Wang, G.Attebury And B.Ramamurthy, ”A Survey on Se-curityIssuesinWirelessSensorNetworks,”inIEEEcommu-nicationsSurveyandTutorials,2ndQuarter2006.
[48] M.Aamir,Prof.X.Hong,A.A.Wagan,M.Tahir, M.Asif,”Cloud Computing Security Challenges and their Compro-mised Attributes,” in International Journal of Scientific En-gineeringandTechnology,Volume3,Issue4,pp.395-399
[49] V. Ashktorab, S.R.Taghizadeh, ”Security Threats and Coun-termeasures in Cloud Computing,” in International Journal ofApplication or Innovation in Engineering and Management(IJAIEM),Volume1,Issue2,Oct’12.