

Est'd. 1964

Celebrating



& beyond

BHARATI VIDYAPEETH



# *BHARATI VIDYAPEETH'S*

## *Technical Magazine*

*2015-2016*



**COMPILATION OF BEST RESEARCH PAPERS**

# Table Of Content

<b>Sr No.</b>	<b>Title of Research Paper</b>
<b>1</b>	<b>Application of Fontus for Supplying Water in Areas facing Water Shortage</b> Aaquib Bhathiwala
<b>2</b>	<b>Application of Internet of Things in Artificial Heart Pacemakers and its Impact on Security</b> Aman Kulkarni, Prof. Suhasini Vijaykumar
<b>3</b>	<b>Survey of data mining tools and techniques for Customer Relationship Management(CRM).</b> Jyoti Kharade,Rohit Yadav
<b>4</b>	<b>Security Issues and its Solution in Cloud Computing</b> Rahul Yadav, Uttara Athawale
<b>5</b>	<b>Enhancing the Application of Visible Light Communication in organization using Li Fi</b> Varsha Bhosale, Prof. Suhasini Vijaykumar

---

# Application of Fontus for Supplying Water in Areas facing Water Shortage

Aaquib Bhathiwala

*Bharati Vidyapeeth's Institute of Management and Information Technology, Navi Mumbai*

---

**Abstract**—This research looks at the working of the Fontus which is an auto self-filling water bottle which converts the moisture into clean drinking water using a condenser just like the natural water cycle. This mechanism can be implemented in rural area facing water shortage regularly by implanting windmills which will be used to absorb the air moisture connected with a condenser that will convert the air moisture into water. The water can be used for various purposes like farming, drinking, and various daily household activities. Finally, this report consists of all the pros and cons as well as the aspects which will make this application more effective and efficient.

**Index Terms**—Air, condensation, EoleWater Wind turbines, EWA, Fontus, Fontus Airo, Fontus Ryde, hydrophobic surface, purification, Solar panels, Spider's Web, WarkaWater towers.

---

## I. INTRODUCTION

The main problem is in the drought areas where the water shortage exists out of which many such areas are still facing this problem due to either climatic conditions or due to the altitude where these area are situated, or may be due to the improper civic amenities supplying them unclean water. Harvesting water from the air moisture is a method that has been practiced since many centuries. The Earth's atmosphere contains almost around 12,800km<sup>3</sup> of mostly unexploited fresh water. The Fontus project was an attempt to discover these resources. It was invented in order to bring an alternative way of collecting safe drinking water to drought regions and areas facing unclean water supply. Fontus was used along with the easiest and cheapest means of transportations such as bikes and bicycles, especially in the developing countries. It resulted in a clever way of acquiring fresh water in the regions of the world where groundwater is scarce but air humidity is high. There have been many projects undertaken to resolve this problem and many scientists are in this process too since then. The Fontus operation is very much effective in the monetary terms as it would be a one-time investment by the government of that country for the regions facing water shortage problems also a cheap alternative to harvest water from air moisture. The concept behind Fontus is to ease the mountaineers and bikers for a long run or travel by being water handy every one hour generated automatically by the bike attachment device or also by a handy device named AIRO which uses a small portable solar panel that can be attached with an USB port to the bottle head ported with a condenser when the traveler or mountaineer is halting somewhere for some time. Further we will see the working of the Fontus in detail along with the proposed application of harvesting water from air on large scale using windmills. The Pros and Cons of the harvesting water from air and also the proposed application will be explained. Using the methodology of The Fontus we will try to apply it into a new alternative for the same which will help in the production of clean water from air on a large scale in drought and unclean water supply areas. The rest of the paper is structured as follows, Methodology and working of the Fontus, Results and Findings of the proposed application and lastly Conclusion. I wish you the best of success.

### A. Literature Survey

In the year 2010, Chinese scientists have discovered the secret behind a spider's web using an electron microscope. The architecture of a spider's web is interestingly effective in catching dew drops. Using the secret behind these minute architectures many scientists have come up with similar

inventions to catch dew drops.



*Fig. 1. Spider's Web Secret*

PhysOrg states that The secret lies in the silk structure of their web which are tail-shaped protein fibres which change their shape in response to the water. Once these structure are in contact of humidity, the tiny portions of the thread crumple up into knots. These knots have nano-fibres which provide a rough knob like textures. The joints between these knots collect small droplets condensed by air which slides down to the knots making the joints free to collect more droplets. The reason behind which spider makes these minute web structures is that the spider does not have to leave its web in search of water. The researchers are coming up by mimicking these structure to collect fog and water condensed from air. Lei Jiang, a lead researcher at Chinese Academy of Sciences in Beijing created an artificial spider web structure in order to improve the directional water collection capability.

In the year 2012, Arturo Vittori from an Italian design firm named Architecture and Vision in Ethiopia created towers which were used to collect dew, these towers were hand- woven made from bamboo stalks as their exterior structure and consisting of a plastic mesh textile on their interior sides which helped in collecting condensation from air which is funneled down into a small reservoir kind of structure at the base.



*Fig. 2. WarkaWater Tower Structure*



*Fig. 3. Interior Plastic Mesh*



*Fig. 4. WarkaWater Tower Prototype*

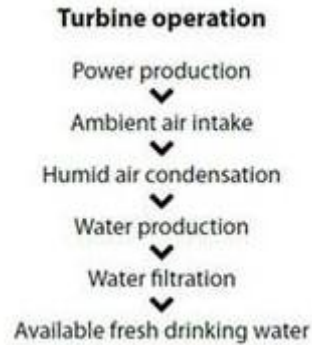
These towers were about 30 feet tall and weighed around 88 pounds and each tower could be built in about a week with a team of 3 to 4 villagers. These towers were also called as WarkaWater Towers. The advantage of these WarkaWater Towers was that it can collect up to 100 litres of water in a day but it would be favorable only in areas where air moisture is high. This led to its failure in the areas where the air moisture is not so good. Moreover the water collected by these towers was not filtered and may be contaminated by pollution present in the air.

An Israeli company EWA which stands for Extraction of Water from Air states that they have developed a clean source of collecting drinking water from thin air even in desert areas with a small amount of energy in the whole process. Their process included a unique water absorption technology which employs a solid desiccant which helps in trapping the water along with a special energy saving condenser that states the reusability of about 85 percent of the input energy in the whole process. Etan Bar, a former researcher at Ben Gurion University in the year 2014 by a research of over 9 years evolved with three main steps to this process. Firstly, the absorption of water from the humidity of air. Secondly, the removal of water from the silica based gel granules which hold the water after absorption. And lastly, condensation. Still purity of water wasn't achieved which led to additional amount of resources required for the water purification.

The next was a technology by Eole Water based on wind turbine which used a power of about 30kW electricity to harvest water from the humid air present in the deserts of Abu Dhabi in October 2012. Air is taken from the nose of the wind turbine where the vents are present to absorb the air which is then heated using a generator to produce steam which then goes through a cooling compressor which helps in creating moisture which is condensed and collected in storage tanks. These wind turbines are capable of producing about 500 to 800 litres of clean water but the disadvantage of this prototype was that it required wind speed of about min 15 miles per hour or more plus it required electrical power for the whole process and installation of electric power in the heart of desert is a tough task.



*Fig. 5. EoleWater Wind Turbines*



*Fig. 6. EoleWater Process*

Kristof Retezar from University of Applied Arts Vienna, Austria came up with a new portable invention to collect water from air moisture and condense it into a small bottle of about a litre. This was named after an ancient Roman religion God of wells and springs, Fontus. Fontus device consists of a series of hydrophobic surfaces which turns the vapour into water droplets. Fontus device was launched in two various designs, Fontus Ryde and Fontus Airo. Fontus Ryde was designed for long bicycle rides whereas Fontus Airo was designed for



*Fig. 7. Fontus Ryde*



*Fig. 8. Fontus Airo*

camping in forests, hiking in mountains and survival trips in deserts. Fontus was shortlisted for a Dyson Award. The advantage of this device was that it was portable. Also it was powered by a solar panel battery fitted with a filter attached which kept the dust and bugs away from the water produced inside the bottle. This device can produce about half a litre of water in about 50 to 60mins.

## II. METHODOLOGY

The previous researches in regards with harvesting of water from the humidity of air are somewhere lacking of efficient methodology. If two or more previous researches are combined with

their methodologies, it will be proven to be a successful one. As researched by Kristof Retezar both models of Fontus are potentially capable enough to be applied on a larger scale which will help the water scarce areas in providing them with clean water for daily purposes. Being it a drought region or a desert area air in the atmosphere contains enough amount of moisture which can be condensed to produce water from it. As explained, [1] biologically inspired engineering is proven to be a very ecofriendly method for acquiring natural process of any molecules present around us in the earth's environment. Ancient ways of harvesting water from rain led to the evolution of biologically inspired engineering processes.

Joseph [2] states researchers are still trying to enhance these Energy Harvesting methods in order to reduce the cost of energy harvesting projects as well as to enhance their functionality and working. Energy harvesting from natural sources viz. moisture, humidity, rain water, electricity generation from dam water, etc are the basic known projects which are famous nowadays, Researches are still on for these kinds of energy harvesting projects so as to utilize the nature's potential energy in order to make it useful to human beings.

K-C Park [3] stated in his findings that even though the earth has 1,386,000,000 cubic kilometers (km<sup>3</sup>) of water available in the form of oceans, seas, ice-caps, rivers, lakes, atmospheric water, groundwater and even the water present in the plants and trees out of which 10,633,450 km<sup>3</sup> of fresh water is present, around 99 percent of the total fresh water amount is groundwater which is not accessible to humans.

Water Sources	Amount of water (cubic kilometers)
Oceans, Ice caps, Seas, Rivers, Lakes, Groundwater	1,386,000,000 km <sup>3</sup>
Groundwater	10,633,450 km <sup>3</sup>
Fresh Water	93,113 km <sup>3</sup>

Fig. 9. Water Resources on Earth

Igor [4] surveyed and found that about 93,113 km<sup>3</sup> of water is the fresh water available in all the lakes and rivers which are considered as surface water resources which can satisfy most people and life needs for water consumption.

Wind Turbine prototypes used in the deserts of Abu Dhabi in order to condense the water from the humidity of desert air proved to be an effective way to harvest water from air. But due to its disadvantage of the power consumption of about 30kW of energy required to start the harvesting process of capturing the air moisture led to its failure. Many Areas on earth are still without electricity and deep provinces on earth such as poor villages or forests and landscapes where electricity power cannot reach will not be able to utilize the effective water produced by these wind turbines. So, in order to make use of such prototypes and benefit most of the human population on earth who are facing water shortage or scarcity due to their climatic conditions or the areas facing drought is to collaborate the working plan with Kristof Retezar's invention of Fontus.

The Fontus working is based somewhat similar to the wind turbine prototype but in an enhanced way in order to be efficient and more effective. The Fontus Ryde gear is a portable device which can be attached to a bicycle whose moving momentum will absorb the moisture from the air. When the bicycle is in the motion the humid air enters through the front side filter facing towards the front tyre of the bike which is captured using a wind stopper mesh created by plastic hole structures. The filter at the front side prevents dust materials to enter the device. The captured wind then goes through a series of condensing surface which is connected to the peltier element attached just below it which has two sides. The hot side is towards the hot wind inlet and the cold side is towards the series of

condensing surface. The hot side of peltier element is attached to a volt amplifier via pair of copper wire with a switched storage battery used to generate power and cool the cold side peltier element which will help



*Fig. 10. Fontus Ryde Working*

in condensation of the air. At the of the series of condensation surface is a small pipe which carries the condensed water towards the bottle container attached using a bolt and bottle holder where the bottle can be twisted and held firm to collect the water through the whole process. The condensed water is again filtered using a small filter before it is collected in the bottle container.

Megan Treacy [8] explained how Marc Parent, the founder of EOLE Water invented the 30-kW wind turbine which comprises and powers the entire system. The vents at the nose cone of the wind turbine are the entry point for the air which is then heated by a generator to produce steam. This steam is then cooled by a cooling compressor which helps in creating moisture which is then condensed and collected in the tanks attached to the wind turbines. The water collected in the steel storage tanks is then sent for purification. The problem with this technique of harvesting water from air is that the air is not filtered when it is taken inside the system through the vents. Polluted air may be taken inside along with dust particles which may be harmful. The cost of purification of water also remains intact as the collected water is not pure and purification needs to be done before it is supplied to humans. The concept of EOLE water can be utilized with the Fontus Airo and Ryde technology in order to produce pure water by the whole process and avoiding purification costs later.



*Fig. 11. Fontus Airo Working Step-1*

The Fontus Airo comprises of a steady device which is powered by a small silicon solar panel which is wrapped around the Airo device.



*Fig. 12. Fontus Airo Working Step-2*



*Fig. 13. Fontus Airo Working Step-3*

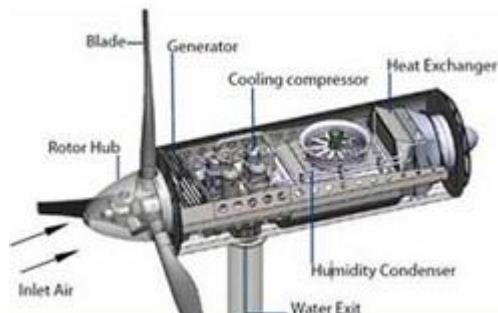


*Fig. 14. Fontus Airo Working Step-4*

When camping or resting for some time the device head of Airo consists of a wind turbine like structure which has small vents for the inlet of air. The air entering the vents is through a small filter at the top to prevent dust particles to enter the device. This turbine like structure is powered by the solar panel attached. The air entered is as it is hot due to the heat generated by the solar panel. This air is then cooled with a coolant in order to condense the air moisture and convert it into safe drinking water. The amount of water produced in that bottle is about a litre.

To produce about a litre of water through this device takes about just an hour. When implemented on a large scale along with the concept of EOLE Water it can produce about 500 to 600 litres of safe and clean drinking water a day. The EOLE Wind turbines can be powered using

Solar panels in order to save electricity and also the cost of transporting heavy generators in remote areas in order to provide these turbines the required amount of power. Also A filter can be implanted at the opening of vents from where the air enters the tower system for the condensation process. The towers being a large unit will produce more amount of water which will help the humans to consume for their needs. The internal working of the EOLE wind turbine can be seen in the figure below.



*Fig. 15. EOLE Wind Turbine Working*

The wind turbine can be powered using solar panels which will help reduce the usage of other non-renewable sources of energy such as electricity also will help the cost of installation of such prototypes.

### III. RESULTS AND FINDINGS

Following are some of the results and findings :

- Total Power generated by the wind turbine is about
- 15kW (kilo-Watts) which is enough to power the cooling compressor
- The solar panel will help to power the heat exchanger in order to carry out the condensation process
- Solar panel will help in generating more power which can be stored in the generator which can be used to provide electricity to the remote areas or villages
- Energy generated by the solar panel can also be implemented to regulate the speed of the rotor hub which in turn will help the rotor blades to rotate and absorb the air even when wind speed is slow

### IV. CONCLUSION

The implementation of these EOLE wind turbines along with the Fontus working will help improve the production of water in more quantity which will be approximately around 2,19,000 litres per year with a single EOLE wind turbine which will also be in pure form. Along with which more energy can be generated using solar panels which can be used for providing electricity in the remote areas by lighting up street lights during night time and also in small homes in those villages. The amount of energy produced by the combination of the EOLE wind turbines along with Solar panels will be approximately 140-300 kWh per year which will be enough to light up 1500 homes.

### REFERENCES

- [1] Harvard John A., Paulson School of Engineering and Applied Sciences (SEAS) and the Wyss Institute for Biologically Inspired Engineering at Harvard University.
- [2] Joseph A. D., *Works in Progress-Energy Harvesting Projects*, IEEE Per- vasive Computing, January-March 2005, pp.69-71.
- [3] K-C. Park et al, *Nature*, 2016, DOI: 10.1038/nature16956.
- [4] Igor Shiklomanov's chapter, *World Fresh Water Resources*, in Peter H. Gleick (editor), 1993, *Water in Crisis: A Guide to the Worlds Fresh Water Resources*, Oxford University Press, New York.
- [5] Kansal A. and Srivastava M. B., *Distributed Energy Harvesting for Energy Neutral Sensor Networks*, IEEE,

Pervasive Computing, v.4, January- March 2005.

- [6] Kansal A. and Srivastava M. B., *An Environmental Energy harvesting framework for Sensor Networks*, IEEE, Proceedings of International Symposium on Low Power Electronics and Design (ISLPED '03). ACM Press, 2003, pp.481-486.
- [7] Kansal A. and Srivastava M. B., *Performance Aware Tasking for Environmentally Powered Sensor Networks*, IEEE, Proceedings on the Measurement and Modeling of Computer Systems in Joint International Conference, ACM Press, 2004, pp.223-234
- [8] Megan Treacy, *Wind Technology*, 2012, DOI: 1204/wind12042012.

---

# Application of Internet of Things in Artificial Heart Pacemakers and its Impact on Security

Aman Kulkarni<sup>1</sup>, Prof. Suhasini Vijaykumar<sup>2</sup>

<sup>1,2</sup>*Bharati Vidyapeeth's Institute of Management and Information Technology,  
Navi Mumbai, India*

---

**Abstract**—This research looks at the putting into use of Internet of Things (IoT) in the working of implantable healthcare devices like artificial heart pacemaker. IoT is the network of physical objects - devices, vehicles, buildings and other items which are embedded with electronics, software, sensors, and network connectivity, which enables these objects to collect and exchange data. This technology can be used to enable healthcare providers to embed life-saving devices and treat patients remotely which can be hugely useful in conditions where direct treatment is very hard or sometimes not possible. This paper also covers the different arguments for and against the use of IoT and the security aspects that can be put into use to make the application more secure and strong and healthy.

**Index Terms**—Arrhythmia, Defibrillator, Healthcare, Internet of Things, Pacemaker, Security

---

## I. INTRODUCTION

In earlier days, medicine and surgery were the only two ways for treatment of Arrhythmia. Although medicines were the usual to-go option, in critical conditions, surgery was the only option one could go with. Since the inception of implantable devices such as pacemakers and defibrillators, there has been a tremendous growth and enhancement into making these devices more sophisticated and more powerful. Furthermore, in the past few years, the market for IoT devices has expanded many folds, opening up a whole new world of possibilities for healthcare and medical applications. Advancements in sensors, battery, and wireless networking have allowed devices like pacemakers to be connected to the Internet.

Such progress in implantable devices was nearly unimaginable. Remotely controlling ones heartbeats was something that was considered absurd or simply crazy. The transition from surgery to pacemakers to remote controlled pacemakers has certainly raised many eyebrows. The advantages of such modern technology are many, but there are various things that one has to take into consideration before making use of these devices as one may simply tap the network and send a signal that may cause your heart to beat fast or slow according to his/her disposal or simply could kill the user. This may result into a massive murder scenario if not kept under scrutiny. So, security is one of the major aspects in this application.

Rest of the paper is structured as follows, literature survey consisting of the details about IoT, Radio Frequency Identifier (RFID), and pacemakers, implementation and working of IoT in pacemakers, Results and Findings of the proposed application and lastly Conclusion.

### A. Literature Survey

IoT is a system of connected calculating devices, mechanical and digital machines, objects, animals or people that are given unique identifiers and the ability to move data over a network without needing human-to-human or human-to-computer interaction [1]. A thing, in the Internet of Things, can be a person with a heart monitor implant, a car that has built-in sensors to alert the driver when tire pressure is low, or any other natural or man-made object that can be assigned an IP address and gave/given with the ability to move (from one place to another) data over a network. IoT has

changed and gotten better from the coming together of wireless technologies, micro electromechanical systems (MEMS), micro services and the Internet. The coming together has helped tear down the silo walls between operational technology (OT) and information technology (IT), allowing without rules, schedules, etc. machine-created data to be carefully studied for understandings of deep things that will drive improvements.

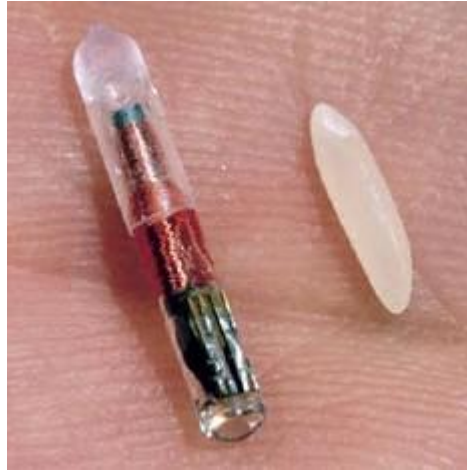
Although the idea wasn't named until 1999, the IoT has been in development for at least 20 years. The first Internet gadget, was a Coke machine placed at Carnegie Melon University in the early 1980s. The programmers connected to the machine over the Internet to check whether there is a chilled bottle of coke available or not.

A thing, in the big picture of the IoT, is a thing/business or physical object that has a unique identifier, an embedded system and the ability to move from one place to another data over a network [2]. A unique identifier (UID) is a number-based or containing letters and numbers string that is related to a single thing/business within a given system. UIDs make it possible to address that thing/business, so that it can be accessed and interacted with. Common example of unique identifier used on a thing in IoT is the RFID.

RFID (Radio Frequency Identification) devices are wireless microchips used for tagging objects for automated identification. RFID can identify objects wirelessly without line-of-sight. RFID systems consist of a reading device called a reader, and one or more tags. The reader is a powerful device with big/enough memory and math-based/computer-based useful things/valuable supplies. Truly smart objects will be embedded with both an RFID tag and a reader to measure data. The sensor may record ups and downs in the surrounding temperature, changes in amount, or other types of information.



*Fig. 1: RFID Tags*



*Fig. 2: An Implantable RFID*

The problems of authentication and privacy are fundamental to RFID security. RFID is poised to become one of the sensory organs of our computing networks. The integrity of the data collected by RFID systems and appropriate curbs on the technology's X-ray power are essential. RFID is a technology with great promise, but it invites numerous security and privacy issues. Deployed naively, embedding of RFID tags in consumer items or in implants can present a serious danger to privacy and security of consumers and enterprises in the future.

A pacemaker is a small device that's placed in the chest or abdomen to help control different from what's usually expected heart rhythms. This device uses electrical pulses to cause the heart to beat at a commonly and regular rate [3]. Pacemakers are used to treat abnormal heartbeats. Abnormal heartbeats are problems with the rate or rhythm of the heartbeat. During an abnormal heartbeat, the heart can beat too fast, too slow, or with an irregular rhythm. During an abnormal heartbeat, the heart may not be able to pump enough blood to the body. This can cause signs of sickness such as tiredness, shortness of breath, or fainting. Extreme abnormal heartbeats can damage the body's (heart, lungs, liver, etc.) And may even cause loss of awareness or death. A pacemaker can relieve some heartbeat-related signs of sickness, such as tiredness and fainting. A pacemaker also can help a person who has different from what's usually expected heart rhythms resume a more active way of living.

- Increase the speed a slow heart rhythm.
- Help inhibit the speed of an abnormal or fast heart rhythm.
- Ensure that the ventricles are contracting normally if the atria are quivering instead of beating with a normal rhythm.
- Coordination of the electrical signaling between the chambers and ventricles of the heart.
- Pacemakers that do this are called Cardiac Resynchronization Therapy (CRT) devices. CRT devices are used to treat heart failure.
- Prevent dangerous arrhythmias caused by a disorder called long QT syndrome.
- Pacemakers also can monitor and record your heart's electrical activity and heart rhythm. More advanced pace- makers can adjust your heart rate according to various aspects like breathing rate, changes in your activity etc.

Pacemakers can be temporary or permanent. Temporary pacemakers are used to treat short-term heart problems, such as a slow heartbeat that's caused by a heart attack, heart surgery, or an overdose of medicine. Temporary pacemakers also are used during emergencies. They might be used until

your doctor can implant a permanent pacemaker or until a temporary condition goes away. If you have a temporary pacemaker, you'll stay in a hospital as long as the device is in place. Permanent pacemakers are used to control long-term heart rhythm problems. This article mainly discusses permanent pacemakers, unless stated otherwise. Doctors also treat abnormal heartbeats with another device called an implantable cardioverter defibrillator (ICD). An ICD is just like a pacemaker. However, besides using low-energy electrical pulses, an ICD also can use high-energy pulses to treat death causing abnormal heartbeats.

A pacemaker is usually inserted into the patient through a simple invasive surgery using either local or a general anesthetic [6]. In most cases the pacemaker is inserted in the left shoulder area where a cut is made below the collar bone creating a small pocket where the pacemaker is actually placed inside the patient's body. The lead(s) are inserted into the heart through a large vein using a fluoroscope to watch for changes, unusual things, etc. the progress of inserting the leads. The lead placed in Right Ventricle would be positioned away from the tip of the right Ventricle and up on the interventricular bridge, below the outflow area, to prevent worsening of the strength of the heart. The actual surgery may take about an hour.

Following surgery, the patient should exercise reasonable

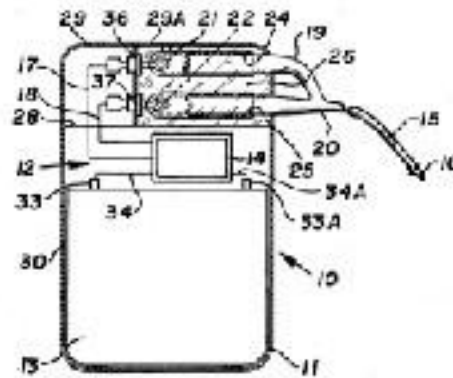


Fig. 3: Worlds first Lithium Iodide cell powered pacemaker. Cardiac Pacemakers Inc. 1972 [4]

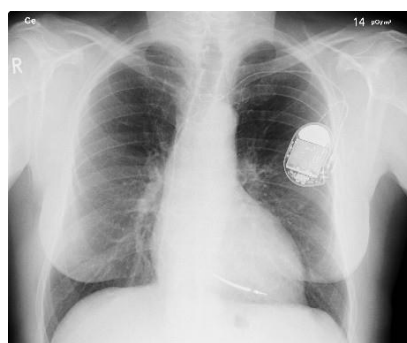


Fig. 4: X-ray image of installed pacemaker showing wire routing

Care about the wound as it heals. There is a follow-up session during which the pacemaker is checked using a "programmer" that can communicate with the device and allows a health care professional to figure out the worth, amount, or quality of the system's wholeness or completeness and figure out the settings such as pacing voltage output. The patient should have the strength of his or her heart carefully studied often with echocardiography, every 1 or 2 years, to make sure the

that placement of the right ventricular lead has not led to weakening of the left ventricle. Since a pacemaker uses a groups of tests, the device itself will need replacement as the batteries lose power. Device replacement is usually a simpler procedure than the original insertion as it does not in a common and regular way require leads to be inserted. The typical replacement demands a surgery in which a cut is made to remove the existing device, the leads are removed from the existing device, the leads are attached to the new device, and the new device is inserted into the patient's body replacing the previous device.

## II. IMPLEMENTATION

As stated earlier, a pacemaker is a device that is implanted near the heart and its nodes attached near the right atrium and ventricle to send small electrical impulses the heart to maintain its pace. Other devices like ICD (Implantable Cardioverter Defibrillator) have additional components like a monitor and powerful nodes implanted to monitor the heart beats and defibrillate respectively.

Application of IoT with the help of RFIDs, extends the BAN (Body Area Network) to the Internet making its application both useful and prone to attacks. The usual pacemaker or ICD is connected to an external programmer which is a device to monitor and/or send impulses to the device and also change the internal settings of the device. Now, these settings and programs can be accessed through the Internet. But as these can't be accessed by any random Jack on the Internet and only those who have proper authentication and authorization like the patients cardiologist or the patient himself. Furthermore, it must be made sure that the communication between the programmer device and the pacemaker is also secure either by encryption or any other mechanism that ensures data confidentiality to make sure that the signals that are sent between both the devices are secure and not eavesdropped or tampered.

### *B. Security Aspects*

In the year 2008, researchers at the University of Massachusetts released a paper demonstrating how an ICD can be compromised from a short range using a software radio.[5] They considered three classes of attackers/adversaries. Although these classes are defined considering the programmer device and ICD/pacemaker are in close vicinity and not connected to the internet, these classes can still be considered as the attack conditions still remain the same.

- 1) An attacker with an external programmer device: an external device commercially produced and marketed for use with pacemakers/ICDs. This is considered as an attack because there are no mechanisms to ensure that programmer devices can be operated only by authorized personnel.
- 2) A passive eavesdropper who eavesdrops on the signals that are transmitted between the pacemakers/ICDs and the programmer devices: This attacker can record RF messages output by ICDs and programmer devices. This adversary might any standard mechanism that is used to eavesdrop or tap into the network. This hampers the data confidentiality.
- 3) An active attacker that extends the passive attacker and tries generating arbitrary signals, send in traffic or modify actual signals, not conforming to the expected input. This impacts the integrity of data transferred and moreover it may directly kill the patient.

The following are the various active attacks that can be implemented on a pacemaker/ICD that is connected to the internet:

<b>Types of attacks</b>	<b>Description</b>
Replay Attack	An attacker captures a legitimate message that was sent correctly and after certain amount of time, resends the same message again and again so as to increase the traffic in the network which may result in denial of service.
Triggering pacemaker/ICD identification	The programmer device triggers a 1.5 second auto-identification trace message which is responded by the pacemakers own identification message. So the attacker may spoof the former's trace message to get the details about the pacemaker. Just knowing that the patient has an implanted device that is connected to the Internet is by itself a dangerous thing.
Disclosing patient data	Just like in previous case, the attacker may get the ID of the pacemaker and on that information, he may trace the information about the patient.
Disclosing cardiac data	Replaying certain messages that gives the attacker the information about the current cardiac condition of the patient
Setting the clock of pacemaker	The pacemaker is set to act differently at different times of the day for example: the pacemaker may be targeting a higher average heart rate during the day time and a lower average at the night time, So if the attacker changes the time, the pacemaker may work abruptly which may lead to sleeplessness or may even prove fatal.
Changing therapies	Therapies are ICDs responses to cardiac events. The programmer device can be set to enable and personalize therapies for an individual patients medical needs. So the attacker can manipulate into the settings of such therapies to change the behavior of the ICD during any such cardiac event.
Denial of service	The attacker might ensure that the pacemaker/ ICD remains in a state of inactive while it is constantly interacting with the programmer device, so during such condition if the patient really needs a pulse to set his heart rate back to normalcy, the pacemaker will fail to do so as it is busy responding to the messages of the attacker.
Other attack vectors	There may be other attack vectors against pacemakers and ICDs like insecure software updates, buffer overflow vulnerabilities.

- Turning dumb machines smart, and making them re- motely controllable or attaching them to the Internet makes them vulnerable to cyber-criminals in a way they never were before.

#### **IV. CONCLUSION**

The high-tech pacemakers which are connected to the Inter- net using IoT made today have a ton of benefits, especially for patients who require constant checks and intensive control of their health. These machines have connections that allow them to exchange information with the hospital staff and doctors, as well as the machine's vendor. Although the pacemakers are not always active, these connections are used to configure and set the parameters of the devices, to remotely monitor its activity, and to transmit the data to its carrier. But there is a downside to it, such devices can be hacked. It was rumored that a renowned hacker named Barnaby Jack developed a software to hack pacemakers, making it possible to kill anyone wearing one no matter the distance. Sadly, he died shortly before he could prove it at the Black Hat conference in Las Vegas [8]. If there is a possible

way to control the pacemaker through an Internet connection, regardless of distance, there is still no published research that confirms or disproves it.

## V. FINDINGS

The following are some of the findings that were discovered:

- With great advancements in the IoT in healthcare, there is an even greater advancements in hacking mechanisms and methods that are used in breaking such systems.
- With that said, the companies that are making such technologies that help connect implantable devices to the Internet are also making sure that their stack is robust and impenetrable. Also, they ensure that their code is bug-free and not revealed to anyone except those who are working on it.
- Furthermore, the whole application of IoT in pacemakers and defibrillators needs still more advancements so as to make it lesser prone to the aforementioned attacks.
- With the increase in practical attacks demonstrated against pacemakers and other medical devices, has prompted the US government to recommend FDA to consider this threat considerably. The FDA has issued an exhaustive list of the security do's and don'ts. [7]

## REFERENCES

- [1] Internet of Things Global Standards Initiative <http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx>
- [2] Thing in IoT <http://internetofthingsagenda.techtarget.com/definition/thing-in-the-Internet-of-Things>
- [3] What is pacemaker? <http://www.nhlbi.nih.gov/health/healthtopics/topics/pace>
- [4] US 3822707
- [5] Daniel Halperin [University of Washington]  
[http://scholarworks.umass.edu/cgi/viewcontent.cgi?article=1067&context=cs\\_faculty\\_pubs](http://scholarworks.umass.edu/cgi/viewcontent.cgi?article=1067&context=cs_faculty_pubs)
- [6] de Oliveira JC, Martinelli M, Nishioka SA, Varejo T, Uipe D, Pedrosa AA, Costa R, D'Avila A, Danik SB (2009). "Efficiency of antibiotic prophylaxis prior to the implantation of pacemakers and cardioverter-defibrillators: Results of a large, prospective, randomized, double-blinded, placebo controlled trial". *Circ Arrhythmia Electrophysiol* <http://circep.ahajournals.org/content/2/1/29>
- [7] FDA Should Expand Its Consideration of Information Security for Certain Types of Devices <http://www.gao.gov/assets/650/647767.pdf>
- [8] Barnaby Jack, Hacker of ATMs and Pacemakers, Died from an overdose <http://motherboard.vice.com/blog/barnaby-jack-hacker-autopsy>

# Survey of Data Mining Tools and Techniques for Customer Relationship Management (CRM)

Rohit Yadav<sup>1</sup>, Dr. Jyoti Kharade<sup>2</sup>

<sup>1</sup>PG Student, <sup>2</sup>Assistant Professor, BVIMIT, Navi Mumbai

**Abstract**— The domain of Customer Relationship Management (CRM) has been gaining significance in various business management processes. CRM includes all the series of action that an organization uses to create and establish good relationships with the customers. Deploying technologies and tools of data mining in CRM can introduce a new area where companies can obtain competitive advantage. Using CRM, a company can make its process to launch better services at a minimized price. By the use of data mining tools & techniques, companies can obtain invisible data of customers from relatively huge databases. Hence, corporations can determine the worth of customers and estimate their future actions and needs. Data mining tools can provide solutions to business problems which were complex to trail down before. So, it is feasible to improve CRM effectiveness and have productive and quick answers to customer needs, by combining CRM and data mining techniques. In this study I explore some major concepts of CRM and data mining. Also I present an idea to employ data mining techniques in CRM. This analysis shows by that applying data mining tools & techniques in CRM that could improve CRM's effectiveness and give us a better forecasting ability to companies and industries to obtain a financial advantage.

**Keywords**— Data Mining, Data Mining Tools, Customer Retention, Customer Relationship Management (CRM), CRM Applications.

## I. INTRODUCTION

The concept of mass production and enhanced marketing strategies first created during the [1] Industrial Revolution are being superseded by new beliefs in which customer relationships is of greatest significance.

### A. CRM

Customer satisfaction ensures competitive advantage and good earnings for businesses in the long run. Customer bases created over a span of time has been of great aid in expanding the extend of a business's product or service. However, the current rise in the operating costs of businesses is compelling companies to evolve their loyalty programs among its present customers while trying to lure new ones. CRM can be defined as the process of forecasting customer behavior and selecting actions to affect their behavior for the benefit of the company. [2]

The goal of CRM applications is to attract, retain and manage an organization's beneficial customers.

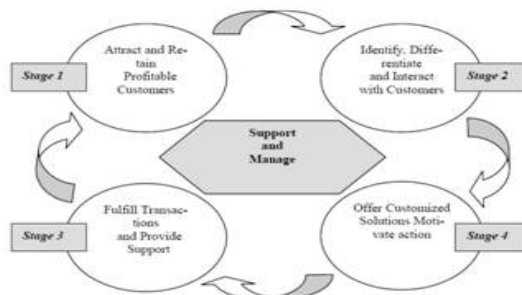


Fig No.1: Process model For CRM [11]

### B. Data Mining

Data mining has been gaining huge focus in the information industry in recent years. Due to the ease of use of huge amounts of information and the fast approaching need for converting such data into useful knowledge and information. The data and knowledge gathered can be used for various applications varying from customer retention, market analysis and fraud detection etc.

Data mining is the process of extracting adequate information from large quantities of data. DM is the technique of finding new interesting patterns and relationships concealed in huge amounts of data. Holshemier and Siebes (1994).

## International Journal for Research in Applied Science & Engineering Technology (IJRASET)

### C. Applications of Data Mining Tool in CRM

Some of the data mining applications are given below [10]

- 1) *Customer Retention*: Its program begins with modelling those customers to find out discrete segments in their bases by means of supplementary variables exceeding conventional analysis.  
*Warranties*: Makers can predict the customer profile who can submit warranty claims.
- 2) *Manufacturing*: Manufacturers have begun to customize their products for customers enabling them to anticipate which features can be included to meet customer demands.
- 3) *Frequent flier incentives*: Airlines identify customers who can be given benefits to fly more.
- 4) *Telecommunication*: By distinguishing customer segments having similar patterns, companies. Can develop attractive pricing and feature promotions.
- 5) *Sales and Customer Services*: When data is collected properly and supplied to frontline service professionals, customer service is considerably improved. If customer data is available on time, software can be used to automatically endorse their products and also help in resolving decision for stock.
- 6) *Database marketing*: Many retailers create customer profiles with some definite behaviour, like those who people who purchase designer labels clothing. This data can be used to target cost effective promotions.
- 7) *Fraud Detection*: Industries are aware that fraud detection is very important. There is a huge concern of dishonest employees and retailers continue to look for ways to minimize the number of dishonest cashiers. Many supermarkets have began using digitized CCTV's, together with Point of sale data mining to allow loss prevention managers to expose cashier stealing.
- 8) *Risk Management*: Data mining allows banks to find and reduce risks by helping them recognize what their customers intends to do. Supermarkets can focus on customers who are more likely to buy a certain product.
- 9) *Marketing*: Marketing depends greatly on correct information for executing retention programs, loyalty cards, targeted promotions, etc. By having the entire profile of the customer, promotions can be focused and targeted thereby dramatically increasing response rates and reduce campaign cost.

### D. Data Mining Techniques for CRM

Data mining techniques involves discovery and learning. These techniques are helpful to achieve the objective of CRM by obtaining or observing hidden customer attributes and behaviours from big databases. Following are the some mining techniques [6]:

- 1) *Association Rule Learning*: It is a popular method for uncovering interesting relationship between items that exist with each other in a given record. This rules was established to find regularities between products in high quantities of transaction data recorded via point-of-sale (POS) systems. This type of data can be used for decision making regarding marketing activities like promotional pricing, Market basket analysis.
- 2) *Classification & Prediction*: Prediction and classification are two types of data analysis techniques that are used to extract important data classes and to forecast future trends. Classification focuses to plot a data item into one of numerous predefined certain classes (Mitra et al., 2002, Berson et al., 1999; Chen et al., 2003; Ahmed, 2004). Example, a classification model can be able to identify loan applicants in low, medium, or high credit risks categories [3]. Prediction aims at building a model to predict future customer behaviours through record patterns. Data classification techniques include decision tree classifier, Bayesian classifier, rule-based classifiers, and support vector machines. Prediction technique includes linear regression, non-linear regression.
- 3) *Clustering*: Clustering enables to map data by similar type of records that are grouped together. Usually, clustering is performed to give the end user a high-level view of what is happening in the database. Clustering gives a birds-eye view of the business.
- 4) *Regression Analysis*: Regression analysis helps us to give a real-value prediction variable and analysing how the value of one dependent variable varies when one of their independent variables is altered, while the other independent variables remain same. Ex. Curve fitting, including forecasting.
- 5) *Visualization*: Visualization refers to the arrangement of data so that users can view complex patterns. (Shaw, 2001).

It is used together with other mining models to provide a clear understanding of the uncovered patterns or relationships. (Turban et al., 2010).

According to Friedman (2008) the main aim of data visualization is to convey information effectively and clearly through graphical means. Ex. mind maps.

## International Journal for Research in Applied Science & Engineering Technology (IJRASET)

6) *Sequence discovery*: Sequence discovery helps in finding patterns where one event leads to another event. It helps in predicting future trends thereby helping the organization.

Customer's lifetime is to understand customer's behaviour and include the following four basic steps[12]:

- a) *Prospects*: people who are not customers yet but are in the market as a target customer.
- b) *Responders*: people who display an interest towards a product .
- c) *Active Customers*: prospects who are using the product or service currently.
- d) *Former Customers*: they may be unacceptable customers who did not make bill payment or who sustained outrageous costs.

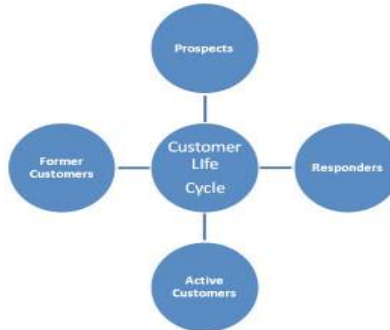


Fig. No. 2 : Customer life cycle[12]

### E. CRM Dimensions

According to [4] and [5], CRM is made up of four dimensions:

- 1) *Customer Identification*: This phase involves closing on the people who are likely to be a customer or profitable to the company through analysis of customers' underlying characteristics. Identification includes target customer segmentation and customer analysis.
- 2) *Customer Attraction*: After customer identification, the organization concentrates all the energy and resources to attract the profitable customer through direct marketing.
- 3) *Customer Retention*: The best way to retain customers and restoring them is by increasing their satisfaction. It is the core of CRM. It includes complaints management and loyalty programs.
- 4) *Customer Development*: It aims to increase customer transaction size with the company. Its elements include market basket analysis and customer lifetime value analysis. The customer lifetime value is the total earnings expected to be achieved from the customer during his link with the organization .Market basket analysis increases customer transactions by revealing orders in the customers' purchase behavior.

## II. INTEGRATION OF CRM AND DATA MINING TECHNIQUES

Each CRM dimension can be categorized further into various levels. Customer identification consist of customer analysis and customer segmentation; Customer Attraction focuses only on one task that is direct marketing. Customer Retention is split into many levels: Loyalty programs, 1:1 marketing and Complaints Management. Customer development consists of customer lifetime value, up/cross selling and market basket analysis. The function of CRM dimensions can be accomplished using more than one technique; although some techniques perform better than others. Table shows the techniques that are superior for each task. The table has been extracted from several previous researches such as: [4], [5], [6] and [7].

## International Journal for Research in Applied Science & Engineering Technology (IJRASET)

S. No.	CRM	CRM Dimensions	Data Mining Techniques
1.	Customer Identification	Target Customer Analysis	Classification Clustering Visualization
		Customer Segmentation	Classification Clustering Regression
2.	Customer Attraction	Direct Marketing	Classification Clustering Regression
3.	Customer Retention	Loyalty Programs	Classification Clustering Regression Sequence Discovery
		1:1 Marketing	Classification Clustering Association
		Complaints Management	Clustering Sequence Discovery
4.	Customer Development	Customer Life Time Value	Classification Clustering Forecasting Regression
		Up/cross Selling	Sequence Discovery Association
		Market Basket Analysis	Sequence Discovery Association

Table No.1: CRM with Dimensions and DM techniques

### III. SELECTION OF DATA MINING TOOLS FOR CRM

There are many data mining tools available in the market. Nisbet (2004) pointed out that there are no best tool as each tool has its strengths and weaknesses; each tool may be the best for particular needs in particular companies. Yet the most persistent data mining tools used for the CRM are SAS, SPSS, ORACLE and Insightful miner (2007). They give various features to its user that helps companies to achieve financial gain. These tools can be categorized in following categories[6].

a) application specific tools; b) general purpose tools ; c) integrated OLAP/ DM tools .

The general purpose tools have a sizable amount of the market and are not specific to the application. Examples include SAS Enterprise Miner, Unica Pattern Recognition Workbench , XLMiner, IBM Intelligent Miner, IBM SPSS Modeler, Oracle Darwin, Ghost Miner, CART & MARS, SGI Mineset, Angoss Knowledge Seeker, Rapid Miner, Weka etc.

Integrated OLAP/DM tools has an actual and convincing need for business and has a single multi-utility tool helping in decision making that gives management reporting, online analytical processing and data mining capacity . Examples in this group include: Cognos Scenario, Business Objects etc.

The application-specific tools are swiftly attaining speed. It provides many business solutions. Some tools of this group are: KD1 which emphasizes on retail, ESTARD Data Miner which emphasizes on insurance industry, Unica Detect, Unica Leaders, Unica Predictive Insight emphasizes on fraud detection etc.

Some limitations of applying Data mining tools in CRM are given below[8]:

- A. *Data Privacy*: It can generate results which will violate customer privacy. This causes problems for firms dealing with the data mining tools.
- B. *Legal Issues*: Many countries do not allow data to be combined from different sources and use it for various purposes from those for which they have been collected.
- C. *Challenge of obtaining data for extensive interpretation*: Gathering of data is still a problem in many industries. Some methods are unwanted and expensive to use.
- D. *Better utilization of outcome*: How to utilize the output in performing various task is critical and it involves huge effort.
- E. *Cost of Tools*: The complexity of the tools elevates its price. Greater the attributes in the tool, more costly the tool becomes

## International Journal for Research in Applied Science & Engineering Technology (IJRASET)

F. The table shown below gives brief features of some of the Data mining tools for effective CRM along with the help of [8] and [9].

S. No.	Tools	Application Area	Data mining Functions	Techniques
1.	<b>Kxen</b>	Embedded in an application	Association rules, clustering, classification, prediction	Decision trees, K-means, Binary classification and regression (linear), rule induction
2.	<b>SPSS Clementine</b>	To support customer behavior modeling	Association rules, classification, clustering, factory analysis, forecasting, prediction, sequence discovery	Apriori, BIRCH, CARMA, Decision trees(C5.0),K-means clustering, neural network, regression (linear, logistic) rule induction(C5.0)
3.	<b>Insightful Miner</b>	Support strategic marketing operations	Association rules, clustering, classification, prediction, sequential patterns, time series	Decision trees(modified CART), K-means, neural networks ( back propagation), regression (linear)
4.	<b>XL-Miner</b>	In Financial operation based on spreadsheets	Association rules, classification, clustering, prediction, time series	Discriminant Analysis Logistic Regression with best subset selection Classification Trees Naive Bayes Classifier Neural Networks k-Nearest Neighbors
5.	<b>SAS Enterprise Miner</b>	Dm tools, Embedded in an application, to support management rules reporting	Association rules, classification, clustering, prediction, time series	Decision trees,K nearest neighbors, regression(linear, logistic), memory-based reasoning, neural networks
6.	<b>Statistica Data Miner</b>	DM tools, in the Databases, Support of direct mail operations.	Variable Filtering, Association Rules, Interactive Drill-Down Explorer, Cluster Analysis, General Classification	Regression, K- nearest neighbors technique, general neural n/w explorer, general classifier.
7.	<b>Weka</b>	Tools for educational purposes and research	data pre-processing, classification, regression, clustering, association rules, and visualization	Decision trees, K-means, Regression, K- nearest neighbors technique, Classification Trees Naive Bayes Classifier Neural Networks k-Nearest Neighbors
8.	<b>Rapid Miner</b>	Tools for research, education, training, rapid prototyping	Association Rules and Clustering	Decision Trees, Bayesian Learner, Rule Learner, Logistics Learner

Table No. 2: Data mining Tools survey.

### IV. CASE STUDY ON LEADING TECHNOLOGY ORGANIZATION ORACLE

Oracle's Data mining model shows that Oracle has Oracle Advanced Analytics that suggests following Data Mining functions for Oracle database as a DBMS Package for CRM.

Choosing a suitable algorithm to use for a specific task can be a challenge. Expert analysts sometimes use one algorithm to deduce the most fruitful inputs then apply a different algorithm to predict a particular outcome based on that information. The Table below depicts which data mining functions are used in different application along with their methods.

Data Mining Functions	Applications For CRM	Methods
Classification	Classification of customers	Neural Networks
	Rules/Transparency	Decision Trees
Forecast	Retaining customers	Decision Tree
Estimation	Reviewing websites	Cluster Analysis
Clustering	Spot irregularity	Nearest Neighbors
	Product Grouping	Hierarchical k-Means
Deducing relations among variables	Data survey in Marketing	Conclusion of Law Genetic
	Predict Stock market trends	Algorithm
Regression	Wide/ Narrow Data/ Text	Support Vector Machines
Association	Next best offer/Market Basket analysis	Apriori

Table No. 3 : DM techniques applications for CRM

## International Journal for Research in Applied Science & Engineering Technology (IJRASET)

According to the research of Seyyed Pishvayi, utilization of Data mining for CRM in various domains is shown below with sales/marketing having the highest usage of data mining applications followed by customer retention, buyer behavior, cost utilization and Quality control also detection of fraud.

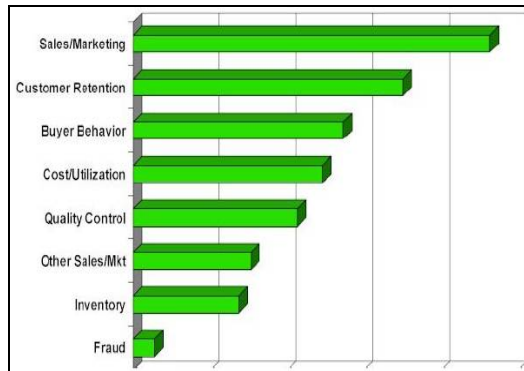


Fig. No. 3 : Usefulness of data mining with CRM for companies

### A. Choosing an Algorithm by Task for CRM

A study of Data Mining Algorithms used by Microsoft SQL Server Data mining in CRM:

The algorithms provided in Microsoft SQL Server Data Mining are the well-researched and most popular methods of deriving patterns from data. To help in selecting an algorithm for work in a certain task, the table below suggests the types of tasks for which each algorithm is conventionally used.

Applications	Algorithms
<b>Forecasting distinct characteristics</b> 1. Spot the customers in a potential buyers list as good or poor prospects. 2. Calculate the probability that a server will fail within the next 6 months. 3. Categorize patient outcomes and explore related factors.	Microsoft Decision Trees Algorithm Microsoft Naive Bayes Algorithm Microsoft Clustering Algorithm Microsoft Neural Network Algorithm
<b>Forecasting steady characteristics</b> 1. Forecast next year's sales. 2. Predict site visitors given past historical and seasonal trends. 3. Generate a risk score given demographics.	Microsoft Decision Trees Algorithm Microsoft Time Series Algorithm Microsoft Linear Regression Algorithm
<b>Predicting a series</b> 1. Perform series of click analysis of a company's Web site. 2. Analyze the factors leading to server failure. 3. Capture and analyze sequences of activities during outpatient visits, to formulate best practices around common activities.	Microsoft Sequence Clustering Algorithm
<b>Identifying set of common items</b> 1. Use market basket analysis to determine product placement. 2. Suggest additional products to a customer for purchase. 3. Analyze survey data from visitors to an event, to find which activities or booths were correlated, to plan future activities.	Microsoft Association Algorithm Microsoft Decision Trees Algorithm
<b>Identifying set of similar items</b> 1. Create risk profiles of patients based on characteristics such as demographics and behaviors. 2. Analyze users by browsing and buying patterns. 3. Identify servers that have similar usage characteristics.	Microsoft Clustering Algorithm Microsoft Sequence Clustering Algorithm

Table No. 4: Microsoft data mining Algorithms

## International Journal for Research in Applied Science & Engineering Technology (IJRASET)

### V. CONCLUSION

Data mining is of great significance as it helps in detecting credit card fraud, anticipating the interests of Web users, forecasting customer purchase behaviour, direct marketing etc. It helps companies in answering business problems by detecting patterns, correlations and associations which are hidden in the records stored in data bases. In choosing the right tool and technique, the company should deeply examine the tradeoffs between various tools. The more efficiently information is used about the customers to meet their demands, the more success an organization achieves. Through this paper we notice that there are various techniques and data mining tools in the market for CRM, but the right tools for the firms depend upon the procedure used in the firm and the objectives that the company needs to attain through the execution of the tools. Logically choosing the techniques and their right execution can prove advantageous for the organization and they would be capable to provide the right product to right group of customers through better offers which would steer them towards better customer relationship management. Hence Data Mining tools can help CRM with better interpretation of customer links and boost customer satisfaction and sharp gains for the firm.

### REFERENCES

- [1] Rado Kotorov, "Customer relationship management: strategic lessons and future directions", BPMJ9, 5 pp 566-571
- [2] R.K. Mittal, Rajeev Kumra - E-CRM In Indian Banks- An Overview, Delhi Business Review.
- [3] Berson, A., Smith, S., and Thearling, K. (1999). Building Data Mining Applications for CRM. McGraw-Hill, New York.
- [4] E.W.T. Ngai, Li Xiu, D.C.K. Chau, "Application of Data mining technique in customer relationship management: AI literature review and classification", Expert Systems with Applications, Vol.36, 2009, pp. 2592-2602.
- [5] Adela Tudor , Adela Bara , Iuliana Botha, "Data Mining Algorithms and Techniques Research in CRM Systems," Recent Researches in computational Techniques non-linear Systems and Control, pp. 265-269, 2010.
- [6] M. R. Farooqi and K. Raza, "a Comprehensive study of CRM Through Data Mining Techniques," in Proceedings of the National Conference ; NCCIST-2011, New Delhi, 2011.
- [7] C. Rygielski, J.-C. Wang, and D. C. Yen, "Data Mining techniques for customer relationship management," Technology in Society, pp. 483-501, 2002.
- [8] Dr. Jayanthi Ranjan, Vishal Bhatnagar, " A Review of Data Mining Tools In Customer Relationship Management "
- [9] Raghda M. Nasr, Sahar Nagaty, Mohammed B. Senousy "Survey and Challenges of Mining Customer Data Sets to Enhance Customer Relationship Management" .
- [10] S. Janakiraman, K. Umamaheswari "A Survey on Data Mining Techniques for Customer Relationship Management".
- [11] Savitha S. Kadiyala, Alok Srivastava " Data Mining For Customer Relationship Management".
- [12] "Aditya Kumar Gupta & Chakit " customer behavior using data mining techniques: optimizing relationships with customer.

# Security Issues and its Solution in Cloud Computing

Rahul Yadav<sup>1</sup>, Uttara Athawale<sup>2</sup>

<sup>1</sup>PG Student, <sup>2</sup>Assistant Professor, BVIMIT, Navi Mumbai

**Abstract**— Cloud computing is a rapidly increasing technology which includes splitting of computer resources. Cloud computing removes the necessity of having an entire infrastructure of hardware and software to meet user's needs and applications. The user gains access to software stored in the cloud network from a remote place by connecting to the cloud using the Internet. Despite having advantages which include multi-tenancy, resource pooling, storage capacity its various security faults including loss of sensitive data, data leakage and few others. As the technology of the cloud computing is increasing rapidly and implemented in different areas, legal/contractual, security and privacy issues still create significant challenges. Security is a major concern for corporate who have their businesses in cloud and sense a need for security. This paper identifies major challenges and highlights the techniques that are used to provide protection and privacy to reduce security risks and protect resources of various enterprises.

**Keywords**— Cloud computing, cloud infrastructure, security challenges, security solutions, Cloud data.

## I. INTRODUCTION

Cloud computing is a technology which allows convenient, easy and on-demand access to a shared pool of resources (eg. networks, servers, data storage, software, and services) that can be provided and delivered with minimal management or interaction with service provider. The major cloud providers include Amazon, Google, and Microsoft Azure. Some examples of applications which use Cloud Computing are Dropbox, Google Docs, Google Calendar, and Gmail etc. Cloud Computing utilizes large group of servers with specific connections to servers that provide distributed processing of data with other servers.

Cloud Computing works on distributed architecture that resources of centralized server on scalable platform so as to provide on demand computing services. The plan is to shift from desktop computing to a service-oriented platform via virtual server at data centers. Generally, cloud offers three types of services i.e. Platform-as-a-Service, Software-as-a-Service and Infrastructure-as-a-Service. The reasons for organizations to migrate to cloud computing include paying for the resources on consumption basis, make use of increasing computing power to execute millions of instructions per second, minimize the usage cost of computing resources and provide quality of service [1].The user does not require any knowledge to manage the infrastructure of clouds; it provides only abstraction. Cloud computing is seen as a business necessity, as it provides infrastructure without managing it.

Cloud computing is a technology that increases the capacity dynamically without requiring investing in infrastructure, training people, or buying new software. But as more and more data is being stored in the cloud, security concerns of the cloud environment begin to grow.

### A. Cloud Computing Service Model

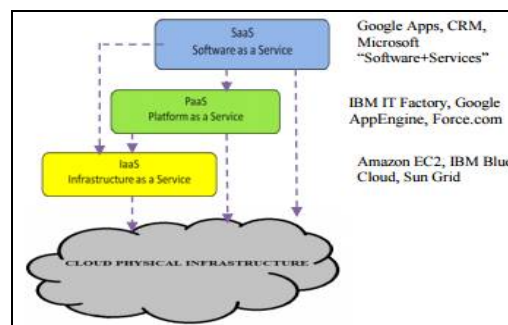


Fig. No. 1 Cloud service model

1) *Infrastructure-as-a-Service (IaaS)*: Services include computation resources, data storage and network as an internet services.

## International Journal for Research in Applied Science & Engineering Technology (IJRASET)

This model is based on the virtualization technology. ex. Amazon EC2.

- 2) *Platform-as-a-service (PaaS)*: Services include platforms, tools and other business services that allow customers to create and deploy their own applications, without installing any of these platforms by hosting on top of the cloud infrastructures .ex. Google Apps Engine and Microsoft Windows Azure.
- 3) *Software-as-a-service (SaaS)*: Services include applications hosted on the cloud infrastructure such as services based on internet for users, applications. ex. Salesforce CRM.

### II. NEED FOR SECURITY IN CLOUD COMPUTING

Security is the most important issue in cloud computing. According to the IDC's on the cloud services, security is the most important issue under cloud computing [4][5].

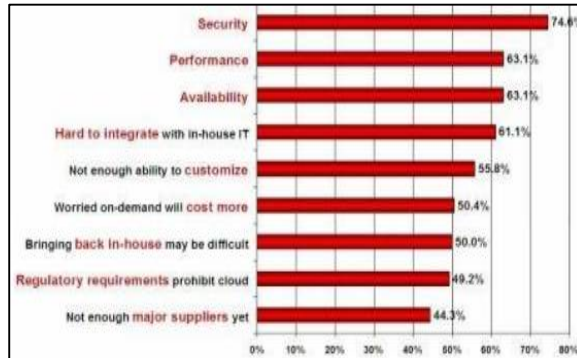


Fig. No. 2 Major issues in cloud computing

Cloud Computing security is a major problem to be addressed nowadays. If security mechanisms are not implemented for data operations and management then data is at risk [6]. Since cloud computing provides services to a group of users to access the stored information, there is a possibility of having data at risk. Strong security plan must implemented by identifying security issues and solutions to handle them.

Many businesses using cloud may not have the basic assets particularly from a security perspective. If there is a security breach occurs in cloud where data is stored, it would result in even more problems and damage. In the recent era, many companies are using cloud to store data about their organization, business and their customers. As a result, information classification becomes more vital. For ensuring data security, techniques such as encryption, logging, must be implemented. The challenge of preventing and detecting advanced threats and intruders must be solved. Not only security but also data privacy challenges exist in industries and corporate having data on cloud. With the increasing use of cloud in business, many organizations are dealing with privacy issues. In a survey, 47% of those who currently use a cloud computing service reported they have encountered a data security issue or lapse with the cloud service their company. India had the highest rate of incident (67%), followed by Brazil (55%) [7].

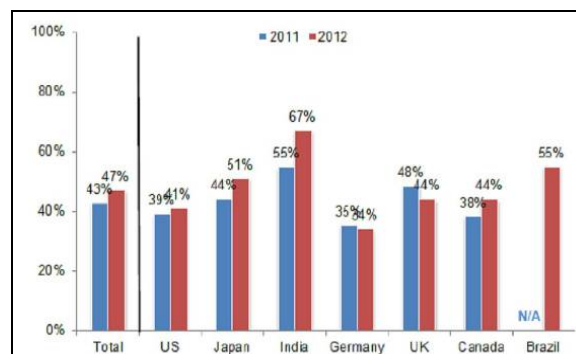


Fig. No. 3 Cloud security issues in various countries

### III. SECURITY ISSUES AND CHALLENGES

The security issues in cloud computing infrastructure can be divided into network levels.

## International Journal for Research in Applied Science & Engineering Technology (IJRASET)

*Network level:* The issues that can be divided under network level include network protocols and network security, like distributed nodes, distributed data.

*Authentication level:* The issues that can be divided under user authentication level deals with encryption and decryption techniques, authentication methods like administrative rights, authentication of applications, and logging.

*Data level:* The issues that can be divided under data level deals with data integrity and privacy such as data protection.

*Generic types:* The issues that can be divided under general level are traditional security tools, and use different technologies.

### A. Network security Challenges

- 1) *SQL injections:* Hackers inject a malicious code in order to gain unauthorized access to databases to manipulate the contents, retrieve confidential data or even take control of the web server.
- 2) *Cross-site scripting:* Hackers inject malicious scripts, such as JavaScript, VBScript and ActiveX into a web page to execute the scripts on victim's web browser. The attack could be used for illegal activities to access the victim's information.
- 3) *Man in the Middle attacks:* In this attack, an entity tries to intrude in an ongoing conversation between a cloud server and a client to insert false information and to access information about important data being transferred between them.
- 4) *Sniffer Attacks:* These types of attacks are created by applications which can collect packets passing through a network and if the data is sent in these packets, it can be read if they are not encrypted. Packet sniffing is listening to the network for packets which are important.
- 5) *Denial of service attacks (DoS):* This attack is to make sure that targets computer resources become unavailable. The attacker aims to floods the victim with a large number of packets in a short duration of time to consume the whole bandwidth and resources of the target computer.

### B. Data Security Challenges

- 1) *Data Integrity:* Sensitive data stored in cloud computing environment emerges as a major issue with regard to security in a cloud based system. Since anyone can access data from the cloud as the data may be public, private or sensitive. So concurrently, many cloud computing users and providers access and modify data. Thus there is a need of some mechanism to ensure data integrity in cloud computing.
- 2) *Data Loss and Leakage:* Data loss is a common problem in cloud computing. Data can be lost or damaged due to miss happening, natural disaster, and fire and there will be a loss of information. Data is always in danger of being lost or stolen by unauthorized access. Due to above situation, data may be inaccessible to users.
- 3) *Data Confidentiality:* Confidentiality means that only the authorized and intended users are given permission to access the data. Cloud Computing system offers applications and infrastructures which operate on public networks. Therefore, maintaining confidential data of user's secret in the cloud is a necessity.
- 4) *Losing control over data:* Exporting data means losing significant control over data. Large organization don't want to run a software delivered in the cloud that risk their data through interaction with some other software [8][9].
- 5) *Multi-tenancy:* One the main features of cloud computing is multi-tenancy. Since multi-tenancy allows storing data by multiple users on cloud servers, there is a possibility of intrusion by attacker. By injecting a client code data can be intruded.
- 6) *Privacy Issues:* The cloud service provider must take measures to ensure that customer information is isolated from other customer and user. As the servers are external, the cloud provider should identify who is maintaining and accessing the data and the server so as to protect the user information.

### C. Cloud Security Challenges

- 1) *Abuse of Cloud Computing Resources:* A simple example of this is the use of malicious application to spread spam and malware. Intruders can access a public cloud and find a way to upload malware to computers in cloud and use the ability of the cloud environment to attack other systems.
- 2) *Insecure Application Programming Interface:* An API is used as an interface to interact with cloud services. They must have extremely secure authorization, access control, encryption and logging mechanism especially when third parties use them.
- 3) *Malicious Insiders:* The malicious insider is an important threat as many providers still don't disclose how they recruit people, how they grant them access to sensitive data or how they control them. Transparency is vital to create a secure cloud, along with compliance reporting and breach notification.

## International Journal for Research in Applied Science & Engineering Technology (IJRASET)

- 4) *Authentication Process*: Authentication is a critical function for every organization as data should not be accessible to unauthorized user. It ensures that only privileged user gets access to data and no intruder gets into cloud. Authorization describes which user has which privileges and what a user is allowed to do. It is the next step after authentication. Authentication can be determined based on user identity and/or by user role.
- 5) *Access Control*: Data stored on the cloud server can be accessed by people who are not privileged users such as employees of cloud service provider's company and there is no control over those people. If access control policy is not implemented properly, user's data will not remain secure.
- 6) *Security related to Third-Party*: A Trusted Third Party is an organization which allows secure interactions between two parties. The Third Party evaluates all critical communications between the parties. There is a need of transparency and control when a third party holds critical business data.
- 7) *Logging*: If logging is not present it is very difficult to identify if someone has breached the cloud or altering of data maliciously has occurred which needs to be reverted. In the absence of logging, internal users can do unauthorized data manipulations without getting noticed.
- 8) *Virtual Machine Security*: It brings new options for attackers because of the added layer. Security of Virtual machine becomes as important as physical machine security, and any vulnerability in one machine may affect the other. Virtual machine is vulnerable to all types of attacks for normal infrastructures.

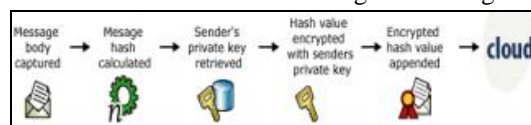
### IV. SOLUTIONS TO SECURITY CHALLENGES

#### A. Solution to Network Security

- 1) *SQL injection attacks*: Filtering techniques are used to sanitize the user data and check these attacks. SQL Injection attacks are prevented by using proxy based architecture which automatically extracts and detects users' inputs for suspected SQL control sequences has been proposed [20]. It is necessary to remove stored procedures that are not usually used. Also, allocate least possible privileges to users who have access to the database.
- 2) *Cross Site Scripting attacks*: Techniques like Web Application Vulnerability Detection, Content Based Data Leakage Prevention and Active Content Filtering, technique, technique are used to prevent this attacks [16]. These mechanisms use various methods to detect security flaws and fix them. An approach to minimize the dependency on web browsers is by spotting unchecked content over the network has been proposed in [17].
- 3) *Man in the Middle attacks*: It involves evaluating software as a service security [18]. Proper implementation of SSL configuration and data exchange tests between authorized parties can be useful to reduce the threat of this attack. Various tools implement strong encryption mechanism like: Dsniff, Ettercap, Wsniff and Airjack etc. have been developed to provide safeguard against them.
- 4) *Sniffer Attacks*: A sniffing detection mechanism using RTT (round trip time) and ARP (address resolution protocol) can be used to detect sniffing in a cloud running on a network [19]. If a hacker gets control over the hypervisor, he can manipulate the data passing through the hypervisor [20]. Stronger authentication and isolation between virtual machines can provide protection against such attacks.
- 5) *Denial of Service Attacks*: Intrusion Detection System is the most accepted technique to detect and take corrective actions to prevent it [21]. Behavior checking detects the attacks by identifying unusual behavior. Route based packet filtering and Secure Overlay Services are used to prevent this attack. Using strong firewall can also prevent this attack.

#### B. Solutions to Data Security

- 1) *Data Integrity Solution*: To solve this issue concept of public key cryptography using Digital Signature is used. A hash value is calculated and encrypted using senders private key and appended to the message and stored in cloud. When attacker changes data, the hash calculated by cloud by will not match hash of new message and changes are not accepted.



- 2) *Data Loss Solution*: Cloud Service provider needs to ensure that all sensitive enterprise data is regularly backed up to allow quick recovery in case of disasters. Also use of strong encryption mechanism to protect backup data is advised to prevent

## International Journal for Research in Applied Science & Engineering Technology (IJRASET)

leakage of information.

- 3) *Data confidentiality Solution:* This can be achieved through cryptographic techniques, where a client can check the integrity of his data by storing a hash in local memory and authenticates by calculating the hash of the received data and comparing it to the value stored locally. The cloud provider should identify and who is controlling and accessing the data the server so as to protect the user information.
- 4) *Losing control over data Solution:* Control over data is achieved by allowing access to data through authentication of the request using HMAC-SHA1 signature using the user's private key [10][11][12]. Also encrypt the data before storing it in cloud. Therefore, the customer has complete control over access to their data. [13].
- 5) *Multi tenancy Solution:* There is a need to store data independently from other customer's data. Problems with data multi tenancy can be detected using the tests such as SQL injection, data validation. To ensure that customers don't cross over each other's territory, monitoring and strong isolation is required. Another effective measure is to monitor environment for unauthorized activity, and promote strong access control and authentication and for administrative access.
- 6) *Data Privacy Solution:* Cloud services encrypt the user's data using a strong encryption technique like RSA. Data masking is another technique that is intended to hide all identifiable characteristics from data. This technique is aimed at reducing the risk of exposing sensitive information. This method is used to preserve the privacy of records and involves substitution of actual data values with keys to an external table that holds the actual data values.

### C. Solutions to Cloud Security

- 1) *Abuse and Use of Cloud Computing Solution:* It can be checked by implementing strict initial registration and validation processes. Another effective way is to enhance monitoring and coordination, and regular introspection of customer network traffic. Another useful step to take is to monitor public blacklists network blocks.
- 2) *Insecure Application Programming Interfaces Solution:* It can be checked by analyzing the security model of cloud provider interfaces. Another effective way is to ensure strong access controls and authentication are implemented with encrypted transmission and to understand the dependency chain associated with the API.
- 3) *Confronting Malicious Insiders Solution:* It can be checked by conducting a complete supplier assessment. Another effective way is to specify requirements as part of legal contracts, and transparency into overall information security and administrative policies. Implementing the access control matrix model reduces the access to the resources and function properly in their roles and responsibilities.
- 4) *Authentication Solution:* Authentication is achieved by various means, but all use a combination of authentication factors, something that an individual knows ex. a password, something they possess ex. a security token, or some quality that is intrinsic to them ex. a fingerprint. Stronger authentication requires two authentication factors such ex. a pin and a fingerprint. Another way to authenticate is by using Kerberos, using Key Distribution Centre and Public Key Infrastructure.
- 5) *Access control:* To apply access control, the cloud service provider must describe and ensure that only legitimate users can access the user or consumer's data. The different access controls are:
  - Discretionary Access Control (DAC) - In DAC, access control is decided by the owner of the object who decides who can access and what privileges they will have.
  - Role Based Access Control (RBAC) [14][15] - Access control is decided by the system. In RBAC access is assigned on the role of subject. A subject can use an object if their set of permissions allows it.
  - Mandatory Access Control (MAC)-Access control is decided by the system and is implemented by labels, which are allocated to subject and object. A subject's label defines its degree of trust, and an object's label defines the degree of trust which is required to access it. If a subject wants to gain access to an object, the subject must be at least as high as the object.
- 6) *Third Party Solution:* Some of the security requirements of third party are low and high level confidentiality and privacy, server and client authentication, separation of data, and certificate based authorization. A Trusted Third Party should be an impartial company delivering business confidence by providing technical security features to electronic transactions.
- 7) *Logging Solution:* All activities performed by users in cloud should be recorded by logging. These logs must be checked frequently to find any unauthorized activity performed by any user.
- 8) *Virtual machine Solution:* To effectively protect virtual machines, they should be isolated from other network and deep checking at the network level should be implemented to prevent them from internal and external attacks. Internal attacks can be restricted by applying by intrusion prevention systems and external attacks can be protected by implementing secure technologies like IPSec or SSL VPN.

# International Journal for Research in Applied Science & Engineering Technology (IJRASET)

## V. CONCLUSION

Cloud computing has gained a lot of interest worldwide because of its lower cost, reduced complexity for customers, and easier acquisition of services. With the benefits it also brings various security challenges. Many large financial company and businesses are still concerned about their data. In this paper, we identify the need for security in cloud computing. We also analyzed the security issues in clouds from three perspectives network security, data security and cloud security and discussed its solution. There is a necessity to make cloud more secure and robust to adapt to the requirements. Research is taking place in this area to find and standardize security in cloud environment. Cloud service providers should solve and implement these solutions on their cloud environment, to accomplish security and take advantage of cloud computing.

## REFERENCES

- [1] Harjit Singh Lamba and Gurdev Singh, "Cloud Computing-Future Framework for emangement of NGO's", IJoAT, ISSN 0976-4860, Vol 2, No 3
- [2] R. L Grossman, "The Case for Cloud Computing," IT Professional, vol. 11(2), pp. 23-27, 2009, ISSN: 1520-9202.
- [3] Rohit Bhadauria et. al. paper on "A Survey on Security Issues in Cloud Computing". hib, HP, India, July 2011.
- [4] Anthony T. Velte, Toby J. Velte and Robert Elsenpeter 2010. Cloud Computing- A Practical Approach. Publishing of Tata McGRAW Hil.
- [5] Nils Gruschka and Meiko Jensen, "Attack Surfaces: A Taxonomy for Attacks on Cloud Services". IEEE rd International Confrence on Cloud Computing,2010.
- [6] Shucheng Yu, Cong Wang, Kui Ren, and Wenjing Lou. Achieving secure, scalable and fine-grained data access control incloud computing, in: IN-FOCOM, 2010 Proceedings IEEE, 2010.p.1-9.
- [7] Char Sample, Senior Scientist, BBN Technologies, Diana Kelley, Partner, Security Curve, "Cloud computing security: Routing and DNS security threats
- [8] John Viega, McAfee, Cloud Computing and the Common Man," published on the IEEE Journal ON Cloud Computing Security, pp. 106-108, August 2009.
- [9] Marco Descher, Philip Masser, Thomas Feilhauer, A Min Tjoa, David Huemer, " Retaining Data Control to the Client Infrastructure Clouds", published on the IEEE, 2009 International Conference on Availability, Reliability and Security, pp. 9-15
- [10] Amazon White Paper, <http://aws.amazon.com/about-aws/whatsnew/2009/06/08/new-aws-security-center-and-securitywhitepaper/> , published June 2009.
- [11] Jinesh Varia, Amazon Web Services, "Building GrepTheWeb in the Cloud, Part 1: Cloud Architectures", Available: <http://developer.amazonwebservices.com/connect>, July 2008, pp. 1-7.
- [12] Jon Brodtkin, " Gartner: Seven Cloud-Computing Security Risks", Available: <http://www.infoworld.com>, published July 2008, pp. 1-3.
- [13] Amazon White Paper, "Introduction to Amazon Virtual Private Cloud", Available: <http://aws.amazon.com/about-aws/whatsnew/2009/08/26/introducing-amazon-virtual-private-cloud/> , published Aug 26, 2009, pp. 6-8.
- [14] L. Zhou, V. Varadharajan, and M. Hitchens.Enforcing role-based access control for secure data storage in the cloud.The computer Journal, 2011
- [15] American National Standard for Information Technology: Role -based access control. ANSI INCITS 359- 2004(2004)
- [16] Arshad, J. Townend, P. Jie Xu , "Quantification of Security for compute Intensive Workloads in Clouds", 15th International Conference on Parallel and Distributed Systems, School of Computation, pages 478-486, Dec. 2009, UK.
- [17] Jinpeng Wei, Xiaolan Zhang, Glenn Ammons, Vasanth Bala, Peng Ning. Managing security of virtual machine images in a cloud environment. CCSW '09: Proceedings of the 2009 ACM workshop on Cloud computing security pages 91-96. November 2009.
- [18] Miranda Mowbray, Siani Pearson. A Client-Based Privacy Manager for Cloud Computing. COMSWARE '09: Proceedings of the Fourth International ICST Conference on COMMunication System. June 2009
- [19] Flavio Lombardi, Roberto Di Pietro. Transparent Security for Cloud. SAC '10: Proceedings of the 2010 ACM Symposium on Applied Computing, pages 414-415. March 2010. International Journal of Application or Innovation in Engineering & Management (IJAIEM) Web Site: [www.ijaiem.org](http://www.ijaiem.org)
- [20] A. Liu, Y. Yuan, A Stavrou, "SQLProb: A Proxybased Architecture towards Preventing SQL Injection Attacks", SAC March 8-12, 2009
- [21] D. Gollmann, "Securing Web Applications", Information Security Technical Report, vol. 13, issue. 1, 2008

# Enhancing the Application of Visible Light Communication in Organization Using Li-Fi



## Computer Science

**KEYWORDS :** Light-Fidelity (Li-Fi), Light Emitting Diode (LED), Visible Light Communication (VLC), Organization devices, Speed.

<b>Varsha Bhosale</b>	Master of Computer Application, Bharati Vidyapeeths Institute of Management and Information Technology, Navi Mumbai
<b>Prof. Suhasini Vijaykumar</b>	Associate Professor, Master of Computer Application, Bharati Vidyapeeths Institute of Management and Information Technology, Navi Mumbai

**ABSTRACT** *Nowadays high bandwidth network (WAN, MAN, and internet, etc.) is a very important need of many people to get their task completed using wired or wireless network. As the number of internet access devices have been increased tremendously, a high speed network is on demand. Dr. Harald Haas has introduced a technique called Li-Fi technology- Light Fidelity, which will provide a high speed internet like never before. This paper gives a large view on the use of light for organizational benefits. Using copper wire for connecting devices for network access will be replaced by an LED light bulb that is used to fluctuate the light faster. Embracing Li-Fi in the organization will culminate to a secure and cheaper infrastructure with the help of light as a wireless data transmission medium.*

### 1. Introduction

This paper gives a comprehensive view on the use of light as a transmission medium for wireless communication. Nowadays Wi-Fi technology is rigorously used in organizations. Wi-Fi is based on radio frequencies for data transmission. But Wi-Fi is facing several challenges, namely capacity, availability, efficiency and security. The arrangement of Wi-Fi technology is costly with the implementing cost and maintenance cost. German Physicist Harald Haas introduced the term Li-Fi (Light-Fidelity). Li-Fi is based on VLC (Visible Light Communication) concept. A constant input power is given to LED (Light Emitting Diode) bulb and the produce output will also be constant. Faster the fluctuation in input power faster be the produced output power. Li-Fi is bidirectional technology.

Implementing Li-Fi in an organization will lead to access the high speed internet network for all the devices (example: Computer systems, router, employee’s mobile phone, etc.). Using LED bulbs for wireless data transmission will withdraw the harmful effect of radiation. Most importantly, as Li-Fi is visible light communication, the light signal will only reach till the nearest light source. This means it is highly secured [1].

### The rest of this paper is organized as follows:

Section2 covers possible applications. Section3 specifies the working of Li-Fi. Section4 illustrates the actual methodology used. Section5 illustrates the benefits of Li-Fi in the organization. Finally, Section6 ends with a conclusion.

### Literature Review

The Li-Fi system is the technology that transmits data through various intensities of light. On July 2011, Dr. Harald Haas demonstrated Light fidelity which is based on visible light communication. Li-Fi uses an LED light bulbs which are used currently in many organizations and homes. In this technique Li-Fi bulbs are outfitted with a chip that modulates the intensity of the light and then the signal is demodulated into electronic form for optical data transmission. The operational work of the LED is very simple. If the button of the LED light is on then it transmits a digital 1 and if the button of LED light is off then it transmits a digital 0. This operation occurs very quickly. Li-Fi provides a very high speed of internet access, up to 10 Gbps speed is tested. And its spectrum bandwidth is 10000 times greater than radio frequency. Li-Fi is very safe as it does not generate harmful radiation. It also provides mul-

tipale access at a time with the same high speed and data density [3].

### General Working Principle

As shown in the Figure 1. The Light emitting diodes (LEDs) gets switched on and off faster since the operating speed of the LED is less than 1 ms. Data transmission is done using binary codes. When LED is switched on, it transmits binary ‘1’ and when it is off, it transmits binary ‘0’. A light sensitive device (photo detector) receives the signal and convert it back into the original data.

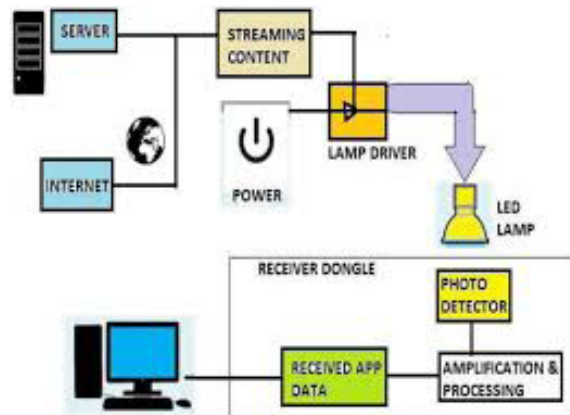


Fig 1. Li-Fi architecture [2]

Using rapid pulses of light to transmit information without using wire is called Visible Light Communication. Data which comes from the outer world (internet) or through LAN server is used to modulate the intensity of the LED light source. The photo detector picks up the signal and then converted into a data stream (original data) and sends to the client [2]-[5]-[6].

### 2. Application of Li-Fi

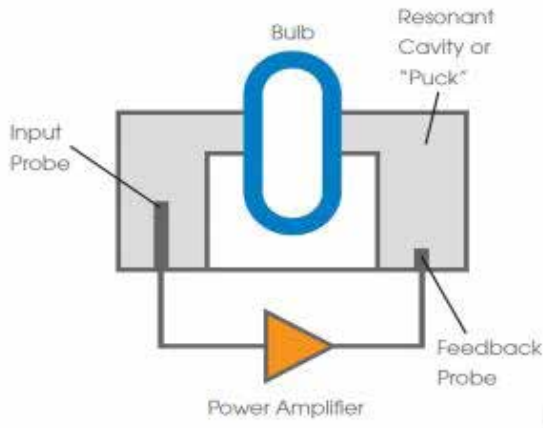
**a) Medical Application:** Use of Wi-Fi in hospitals is not allowed. Wi-Fi produces harmful radiations. It is unhealthy for the patient’s health. Li-Fi emits electromagnetic interference and it does not interfere with medical instruments available in the hospitals nor it interferes with MRI scanners [4].

**b) Internet in the Airways:** While traveling in the airways, passengers gets low speed internet access at very high cost. Wi-Fi, Bluetooth, infrared can not be used in airways be-

cause it may interfere with the navigation systems of the pilots. Use of Li-Fi in airways will provide high speed internet via LED light source which is available in the aircraft at low cost [6].

**c) Vehicle communication and Traffic management:** vehicle headlights and tail lights can be replaced with LED lights. Street lamps and traffic signal also can be replaced by LED lights. This will be used to communicate one vehicle to another. So that when any vehicle comes too close, LED lights can alert the drivers which will help to reduce the accident numbers and manage traffic as well [7].

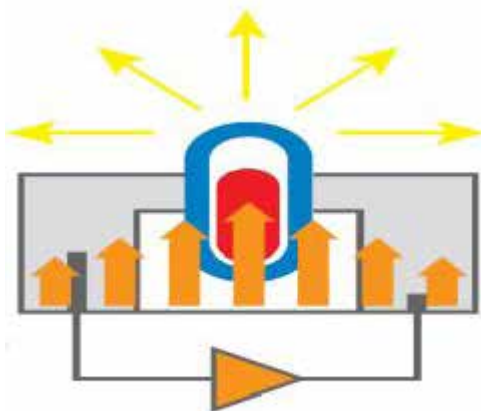
**3. How Li-Fi Works**



**Fig. 2. Assembled RF circuit [8]**

As shown in Fig.2, process of light generation in all Li-Fi systems can be understood in following steps:

1) First of all, RF circuit is formed by connecting the RF power source across cavity known as “puck”. When power source is connected to the RF driver then it generates electron flow assembly, which further leads to give high electric field.



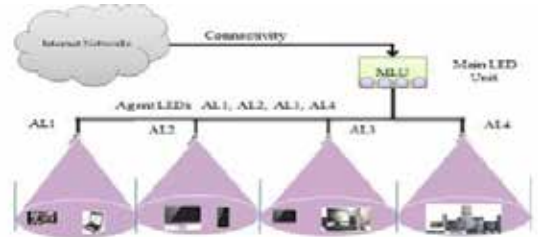
**Fig. 3. Emitting plasma column [8]**

2) This electric field ionizes the gases present inside the puck which in turn heats up and evaporates the metal-halide materials which form a bright plasma column within the bulb as illustrated in Fig.3

Process: The lamp driver i.e. power source is connected to LAN data. Accordingly, based on variation in the data, the source will generate digital signal and so as the corresponding intensity of light. In this way Li-Fi works [8].

**4. Methodology Used in Organization**

The LED bulb is fixed in the organization as per the requirement and structure of the organization. The employee can access the network from any location where the nearest light source is available.



**Fig. 4. The LED design for organization [10]**

The basic architecture of Li-Fi technology is based on Main LED Unit (MLU), Agent LED’s (AL) and Li-Fi cloud. The main line is connected to MLU and further it extends to smaller nodes, which are LED bulbs (example: AL1, AL2, AL3, etc.). The LED lamp is fixed to the walls and ceiling of the organization room. The position of the LED lamp is adjusted in such a way that it can cover the maximum area with high intensity of light [10]-[11]-[12]. Overall methodology will be illustrated in two parts. The first part covers the communication from the internet to the client, while the second part includes the client-internet communication.

**4.1 Internet-client communication:**

In recent years, the demand of IoT phenomena is increasing rapidly, but at the same time it also encounters with speed, security terms in large extent. Li-Fi has ability to overcome these aspects. For example, when any organization needs data from server with maximum speed and stringent security, it will employ following steps:

- i) First of all, information will be fetched from the internet. Further through ADSL router with dedicated IP address the information will pass on to LAN connectivity of the organization.
- ii) The flow of data coming from the LAN is fed to AL via MLU. According to the binary data, the chip inside the light unit will modulate the intensity of light.
- iii) The receiver section of client, i.e. photo detector will convert the light energy into electrical energy in analog form.
- iv) With the help of analog to digital converter (ADC), we can reconstruct the data sent by LAN.

**4.2 Client-Internet communication:**

Now the data traveling from the client end to the internet follows the steps shown below:

- i) Along with photo detector, client unit also possesses LED unit, which is activated when data coming from the client end. Where at this end the binary data coming will convert into the light energy.
- ii) The detector unit located on the floor of the organization will transform the light energy into electrical form, further via ADC the binary data will get fed to the ADSL router.
- iii) Finally via router the data are transferred to the internet [9].

### 5. Benefits of Li-Fi in organization

- 1) Multiple Access a fixed LED lights can allow different people to browse the internet and use the network at the same time.
- 2) Speed - Li-Fi has produced a speed of over 10 gbps. As Li-Fi gives a high bandwidth which 1000 times greater than the radio frequency. Thus speed can be achieved.

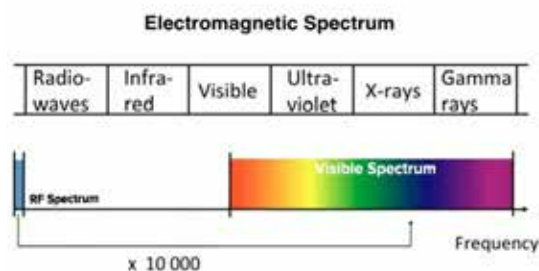


Fig. 4. The Light Spectrum [9]

3) **Instant start-time-** The LED bulb can be switched ON/OFF instantly.

4) **Energy Efficiency-** LED bulbs consume low electrical power. Usage of Li-Fi in the organization will save the electricity consumption as well as will give high brightness.

5) **Cost-** Deploying LED infrastructure of the organization, does not require huge investments.

6) **Security-** Light signal can not travel through the wall, and also it allows roaming access between lights.

7) **safety-** light emissions are not harmful to the human body.

### VI. CONCLUSION

Li-Fi is such technology, where the speed and security aspect makes it exceptional. Light is part of day to day life activities leads to easy access of the network. From the organization point of view, it is helpful in different aspects like easy availability of light source, safer, healthier, greener, etc. Henceforth Li-Fi plays an important role in providing massive speed with stringent security of information.

### ACKNOWLEDGMENT

This paper is completed under the guidance of Prof. Suhasini Vijaykumar, whose reminders and constant motivation encouraged me to meet the deadlines.

I would like to thank Mr. Pramod Dabhade (Manager HDFC Bank) to read my paper and advice throughout the paper.

I would also like to thank Mr. Prashant Kamble (Deputy Manager HDFC Bank) and Nilesh Shinde to share their knowledge and provide valuable suggestions.

### REFERENCES

- [1] Haas, H.; Yin, L.; Wang, Y.; Chen, C. "What is LiFi?", *Lightwave Technology*, Journal of, On page(s): 1533 - 1544 Volume: 34, Issue: 6, March 15, 2016
- [2] Vitthal S Saptasagare, Canara Engineering College, Mangalore, Karnataka, India. "Next of Wi-Fi an Future Technology in Wireless Networking Li-Fi Using Led Over Internet of Things". *International Journal of Emerging Research in Management and Technology*, March 2014. ISSN: 2278-9359

(Volume-3, Issue-3)

- [3] Fi Technology Transmission of data through light". Vol 5 (1),150-154, ISSN:2229-6093.
- [4] LIFI Technology A Visible Light Communication
- [5] LiFi Technology in Wireless Communication Revathi Ganesan
- [6] [www.slideshare.net/shivumanjesh/ss-47393388](http://www.slideshare.net/shivumanjesh/ss-47393388)
- [7] Novel Architecture for Future Li-Fi Wireless Technology
- [8] Durgesh Choudhary, Electrical and Electronics Engineering, O. P. Jindal Institute of Technology, Raigarh-496001,(CG) India, Next Generation Communication for LiFi Technology, *International Journal of Engineering Research and Technology (IJERT)*. Vol. 2 Issues 11, November - 2013 IJERT, ISSN: 2278-0181
- [9] Zimu Zhou, Zheng Yang, Chenshu Wu, Wei Sun, Yunhao Liu, CSE, Hong Kong Univ. of Sci. and Technol., Hong Kong, China, LiFi: Line-Of-Sight identification with WiFi, April 27 2014-May 2 2014, ISSN :0743-166X
- [10] Harald Haas, Erdal Panayirci, Tezcan Cogalan, Inst. for Digital Commun., Univ. of Edinburgh, Edinburgh, UK, "Power Control-Based Multi- User Li-Fi Using a Compound Eye Transmitter", 6-10 Dec. 2015
- [11] An IEEE Standard for Visible Light Communications [visiblelightcomm.com](http://visiblelightcomm.com), dated April 2011. Tsonev, D.; Sinanovic, S.; Haas, Harald (15 September 2013). "Complete Modeling of Nonlinear Distortion in OFDM-Based Optical Wireless Communication". *IEEE Journal of Light wave Technology* 31 (18): 30643076. doi:10.1109/JLT.2013.2278675
- [12] Jyoti Rani, Prerna Chauhan, Ritika Tripathi, Li-Fi (Light Fidelity)-The future technology In Wireless communication, *International Journal of Applied Engineering Research*, ISSN 0973-4562 Vol.7 No.11 (2012).