International Conference on Emerging Trends in Technology, Science and Upcoming Research in Computer Science
DAVIM, Faridabad, 25th April, 2015 ISBN: 978-81-931039-3-7

THE YARD SIDE APPROACH FOR A SMART HARBOUR

Jarina Raihan A[1], Mrs MeenakshiVidya P[2]

[1]PG Scholar, ECE, [2]Asst. Prof SL Grade, Easwari Engineering College Ramapuram, Anna University, Chennai, (India)

ABSTRACT

There are many maritime container terminals found all around the world. The performance and the efficiency of such container terminals depends on how well the containers are handled by the quay cranes, yard cranes and the yard trucks which are employed inside the harbours. There are two common approaches for dealing with the harbours, one is the quay side approach and the other one is the yard side approach. This paper deals with the yard side approach which involves yard cranes optimization, RF ID process and the ship balancing.

Keywords: Smart Harbour, Yard Side Approach, Container Terminal, Logistics, Yard Allocation Algorithm

I. INTRODUCTION

In a container terminal there are three most important things which are found. Those are: quay cranes QC (which is used to unload the containers from the ship),yard cranes YC (which is used to unload the container from the truck into the storage yard) , yard trucks YT (which are used to take the containers from quay side to the storage yard).[3]

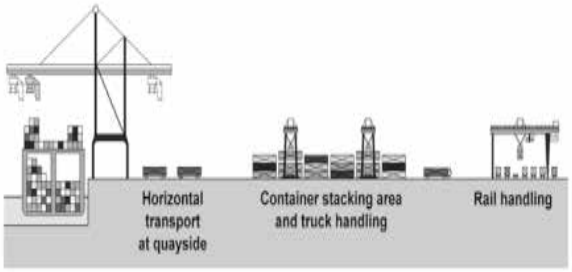


Fig 1:Container Terminal Operation

Fig 1 shows the exact operations at the container terminal. The sea side is called the quay side and the storage side is called the yard side. As soon as the ship arrives it is the duty of the quay cranes to serve the ships and unload the containers within the specified time. There are few cranes which are present inside the ships for emergency operations. The derick cranes are those which are fixed and are used to carry heavy containers[7]. These cranes can move a very small distance so as to cover the entire ship. Few cranes are movable and are used when needed.

Once the containers are unloaded then it is the duty of the yard trucks to serve the cranes immediately. The trucks are allocated based on the weight of the containers. The containers are measured in terms of TEU (twenty foot equivalent units) so depending on this the trucks are allocated manually to serve the cranes[6]. Once the

containers are loaded into the trucks the plan will be given to the drivers which tells them as which yard to go and store the containers.

The truck will move to the needed yard as per the plan and the yard crane will be present to unload the containers from the truck to the yard. The containers will be stacked one above the other. So by this way the containers are unloaded from the ship and are loaded into the yard side. The vice versa operation will take place loading the shipalso.

II.YARD SIDE APPROACH: YARD CRANE OPTIMIZATION

The yard serves as a buffer for loading, unloading and transhipping containers.The yard is separated into blocks. The position of the containerinside a block is identified by bay, row and tier [4]. In order to optimize the yard cranes the:

1. policies are followed for groups of containers at block and bay level:
   - To make a balanced workload among blocks
   - To reduce the total distance covered to move containers from quay to yard.

2.Re-marshalling of containers are made according tothe ship loading plan,to:
   - Speed-up loading operations and the unloading operation.

3. Yard cranes deployment involves allocation of cranes among blocks, routing andscheduling of operations,to:
   - Minimize the time taken to complete a job.

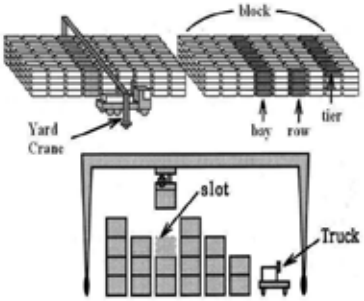


Fig 2: Yard Crane Operation

The yard shown in the fig 2 is usually the bottleneck of the terminal.Traffic, congestion and capacity issues originate from here. Main issue: the “schedule” of the outgoing flow is unknown to the terminal.The two types of the yard management terminals are

1. Import/export terminals: yard management is strictly connectedto gate operations (trucks and trains).
2. Transhipment terminals: yard management is strictlyconnected to mother vessels and feeders.

III. RFID

RFID stands for radio frequency identification here the RFID is used as a card for the truck drivers to know the yard position as well as the availability [5].There are three types of RFID tags one is the Passive tag that uses the reader field as a source of energy for the chip and for Communication from and to the reader. The power which is available from the reader field, reduces very rapidly with distance and is also controlled by strict regulations. This results in a restriction in the communication distance of 4-5 m when the UHF frequency band is used which is of the range 860 MHz – 930 MHz. Semi-Passivetags which are also called as the battery assisted backscatter tags have built in batteries. This implies that they do not require energy from the reader field

to power the chip. This is an advantage, because this allows them to function with lower signal power levels, which results in a greater distances of up to 100 m. Active tags are battery-powered devices that have an active transmitter. Unlike passive tags, active tags generate RF energy and apply it to the antenna. The coverage distance is more, but it is much costlier compared to the other two.

Fig 3: Flow of the RFID Process

The flow of the RF ID process is shown in the fig 3. The container terminals will have many lanes through which the yard trucks enter inside the terminal. Here in this method by using the RF IDs which are provided to the truck drivers the task becomes easier. The exporters who take away the containers from the yard are provided with extra facility of booking the slot or the lane they are in need of so that they can take that particular lane n carry away the containers with ease. Once the trucks arrive near the gate the validation of the tags are made then depending on the information in the tag the drivers are directed to the needed yards.

IV. VESSEL BALANCING

In any maritime container terminal the most important issue is balancing the ship or the vessel. Balancing the ship means that when the containers are being unloaded form the ship care should be taken in order to remove the containers in an orderly manner so that the ship does not sink or get imbalanced. So, to maintain this balanced, the hatch plan must be made and it has to be given to the crane operator so that he is aware of the weights of the containers and thus he removes the containers in the mentioned manner thus reducing the loss caused by imbalance of the ship.

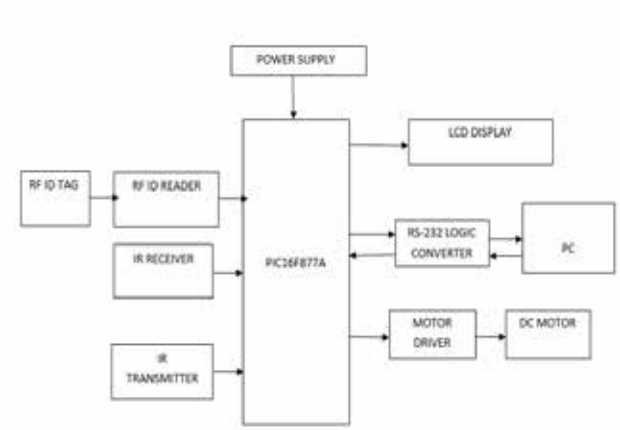


Fig 4: Block Diagram of the System

V. BLOCK DIAGRAM OF THE PROPOSED SYSTEM EMBEDDED CONTROLLER

Fig 4 shows the block diagram of the system which depicts the yard side approach. The embedded controller is preferred because of its software and industrial advantages in power electronics like built in ADC, DAC, ROM, RAM, USART. This leads to lesser space occupation by the circuit and also the speed of embedded controllers are more compared to other processors. The embedded controller which is chosen here is PIC16F877A due to its

various features. Peripheral Interface Controller (PIC) is enhanced version of microcontrollers. It has a high-performance RISC (Reduced Instruction Set Controller) CPU. Only 35 single word instructions are present. All are single cycle instructions except for program branches which are two cycle. It has 4K x 14 words of Program Memory (EPROM), 256 x 8 bytes of Data Memory (RAM), Interrupt capability (up to 14 internal/external interrupt sources), eight level deep hardware stack,12-bit multi-channel ADC,Universal Synchronous Asynchronous (USART) Receiver and USART Transmitter.

5.1 DC Motor

A DC motor relies on the fact that like poles repel and unlike poles attract each other. It has a coil of wire through which the current runs and that generates an electromagnetic field which is aligned with the centre of the coil. A simple DC motor typically has a set of magnets in the stator and an armature with a series of two or more windings of wire wrapped in insulated stack slots around iron pole pieces with the ends of the wires terminating on a commutator. The total amount of current sent to the coil, the size of the coil and the wrapped material dictate the strength of the electromagnetic field. By turning on and off coils in sequence a rotating magnetic field can be created. To create a force on the armature which causes the motor to rotate,the rotating magnetic fields interact with the magnetic fields of the magnets (permanent or electromagnets). At high power levels, DC motors are always cooled using air that is forced inside.

5.2 Infrared Transmitter and Receiver

IR Transmitter has a simple and clear infrared LED on it. The Infrared LED which is present operates at around 940nm and work well for generic IR systems including remote control and touch-less object sensing. IR receiver has an IR detector mounted on it.IR detector has little microchips with a photocell each. They are almost always used for remote control detection.

5.3 LCD

A liquid-crystal display (LCD) is a flat panel display that uses the light modulating properties of liquid crystals. The crystals which are used here do not emit light directly. LCDs are available to display images as in a general-purpose computer display or fixed images which can be displayed or hidden. The arbitrary images are made up of a large number of small pixel this concept is used. Here the LCD is used to display the information about the yard as well as the quay cranes.

VI.RESULTS AND DISCUSSION

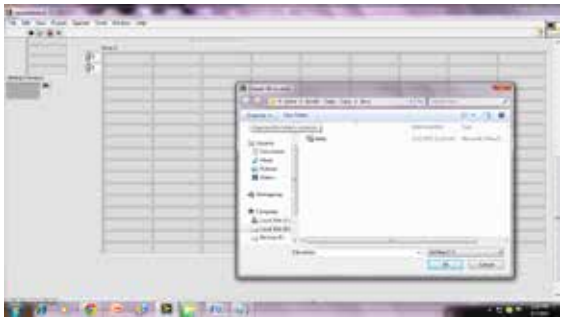


Fig 5: Indicates how the Selection of the Database is Made

There may be many ships which arrive at the particular harbour at a time so now in order to choose which ship is arriving and to schedule accordingly this selection of the database is done which is shown in fig 5.

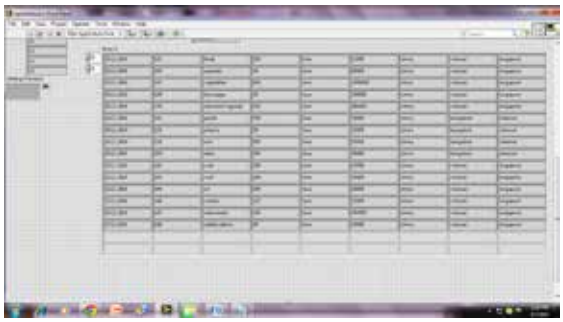


Fig 6: Shows how the Containers are Allotted Based on the Insertion Sort

Here, one the selection of the database is made then the insertion sorting algorithm which is used sorts the containers accordingly and helps in reducing the time taken for dumping materials at the yard.

Fig 7: The Smart Harbour Demo Kit

Fig 8: Performance Chart

The Entire Performance of This Smart Harbour is Tested Using the kit shown in the fig 7 which proves to be efficient if implemented in real time scenarios. The performance analysis shown in the fig 8 is made between the real time and the simulation pattern and thus the result concluded was the smart harbour provides efficient results compared to the present existing harbours.

VII.CONCLUSION AND FUTURE WORK

The yard side approach dealt in this paper seems to be an efficient one compared to the traditional approach. The methods proposed in this paper has reduced the congestion and miscommunication caused in and around the harbours. The extension of this can be any new innovations that can further reduce the issues. This paper can also be extended considering an integrated approach of both the quay and the yard side approaches.

REFERENCES

[1]. Pasquale Legato, Lina Mary Mazza, Roberto Trunfio," Simulation based optimization for the quay crane scheduling problem",2008,Proceedings of the 2008 Winter Simulation Conference, PP. 2717-2715

[2]. Chun Yew Cheong, Muhammed SalahuddinHabibullah, "Multi-objective optimization of large scale berth allocation and quay crane assignment problems"2010,PP. 669-676.

[3]. CAO Jinxin, SHI Qixim,"Integrated and yard truck schedule problem in container terminals"2010.

[4]. Dandhan Wang, Qian Wang, "A two stage composite heuristic for dual cycling quay crane scheduling problem" 2011,PP. 1902-1907.

[5]. Vu DucNguyen,Kap Hwan Kim,"Heuristics algorithm for constructing transporter pools in container terminals", 2013 ieee transactions on intelligent transportation systems, vol. 14, no. 2, june 2013 pp. 517-526

[6]. PhatcharaSriphrabu, KanchanaSethanan, and BancharArnonkijpanich,I.J."ASolution of the Container Stacking Problem by Genetic Algorithm". Intelligent Systems and Applications, 2010, 2, 41-47Published Online December 2010 in MECS (http://www.mecs-press.org/) Copyright © 2010 MECS I.J. Intelligent Systems and Applications, 2010, 2, 41-47

[7]. Meng Yu College of Logistics Engineering, Wuhan University of Technology, Wuhan,"Multi-agent-based Fuzzy Dispatching for Trucks at Container Terminal" P.R. China ymmona@126.com Yanwei Zhang College of Logistics Engineering, Wuhan University of Technology.

AN IMPROVED SECURITY MECHANISM FOR WIRELESS SENSOR NETWORKS

Lokana S[1], Lokashree S[2], Dr.M.V.Sathyanarayana[3]

[12]pg Scholar, Rajeev Institute of Technology, Hassan, Karnataka, (India)
[3]director(Training&Placement), Dept Of Ece, Rajeev Institute of Technology, Hassan, Karnataka, (India)

ABSTRACT

Secure data transmission is very important in wireless sensor networks.Clustering is one of the most effective way to increase the system performance of WSN. Wireless communication is one of the most important communication methods in our day to day life due to providing its devices with portability and rapid hardware cost reduction. A secure data transmission for cluster based WSNs are called SET-IBS and SET-IBOOS.In this paper the feasibility of the SET-IBS and SET-IBOOS protocols with respect to security analysis against major attacks is proposed.ECC algorithm is used for Encryption and Decryption. The calculations and simulations are also provided to illustrate the efficiency of the algorithm proposed.

Keywords: Clustering, Wireless Sensor Network, SET- IBS, SET-IBOOS.

I. INTRODUCTION

The wireless sensor network is comprised of small size, low power, and light weight, affordable wireless nodes called sensor nodes that are utilized in physical or environmental condition. The individual nodes have the capacity to sense their environments, which process the information data locally, and send the data to one or more collection points in a WSN. The sensor nodes will have the ability to communicate either among each other or directly with a base station. These types of nodes are heavily utilized in an agreed geographical area to self-organize into ad-hoc wireless networks to assemble and collect data. The ad hoc nature of sensor networks constitutes remarkable challenges with their reliability, efficiency and security. Hence, advanced security measures are required to address these unique sensor networks security challenges.The cost of data transmission is costlier than that of processing the data.

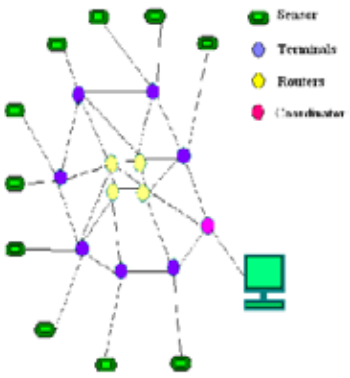


Fig: WSN Architecture

Efficient and reliable data transmission is one of the foremost issues for WSNs. Data in wireless sensor network are bound either downstream to nodes from a sink node or upstream to a sink node from nodes. Wireless sensor network are a kind of application specific network. Cluster Network consists of large number of Sensor Nodes that are grouped into different clusters. Each Cluster in network is comprised of a single Cluster Head (CH) sensor node that will be elected independently and cluster member nodes or leaf (non CH) joins the cluster that depends upon the receiving signal strength. Here, Cluster Head (CH) will get sensed data from the leaf (non CH) and combines the sensed data and then transfers it to the base station.

II. RELATED WORK

Wireless sensor networks (WSNs) have recently attracted much interest in the research community due their wide range of applications. Due to distributed nature of these networks and their deployment in remote areas, these networks are vulnerable to numerous security threats that can adversely affect their proper functioning. Hence; this problem is more crucial if the network is utilized for some mission-critical applications such as in a military. Accidental node failure is also very likely for deployment in real-life scenarios. Due to constraints in resources in the sensor nodes, older security mechanisms with a huge overhead in communication and computation are infeasible in sensor network. Therefore, Security in WSN is a highly challenging task [2].

A wireless sensor network (WSN) which is comprised of a large number of small sized sensors can be an efficient tool for assembling data in various kinds of environments. The data gathered by each and every sensor is relayed to the base station that forwards the data to end users. Clustering approach is introduced in WSNs since it has proved effectiveness to provide better data aggregation and also scalability for large sensor networks. Clustering approach conserves limited energy resources of the sensors [3].

Networking hundreds of inexpensive micro sensor nodes will allow users to effectively monitor remote environment by combining the data from the individual sensor nodes. Low-energy adaptive clustering hierarchy (LEACH) is an architecture for the micro-sensor networks which combines the ideas of media access and energy-preserving cluster-based routing together with the application-specific data aggregation to achieve excellent performance in terms of system latency, lifetime, and also application-perceived quality. LEACH includes a unique distributed cluster formation methodology that enables the self-organization of massive number of nodes as well as algorithms for adapting clusters and rotating cluster head positions to evenly share the energy load among all the nodes, and techniques to enable distributed signal processing to save communication resources [4].

WSNs are a class of ad hoc networks. They will find an increasing deployment in coming years, since they enable trustworthy monitoring as well as analysis of untested and unfamiliar environments. Advancements in technology have made it possible to have tiny, low powered sensor devices equipped with programmable computing, wireless communication capability, and multiple parameter sensing [5].

III. CLUSTER NETWORK ARCHITECTURE

Cluster wireless sensor networks have the following features:

· It includes two kinds of nodes:

Sensor nodes: These will have a limited energy and can sense their own residual energy.

Base Station (BS): These will not have any energy restriction.

· Sensor nodes will sense the environment at a fixed rate and they always have information to send to the BS.

- Cluster head CH will perform data aggregation and Base Station will receive the compressed data.
- All sensor nodes will use direct transmission or multi-hop transmission to communicate with the BS.
- The lifespan of sensor network is the total amount of time previous to the first sensor node runs out of power.

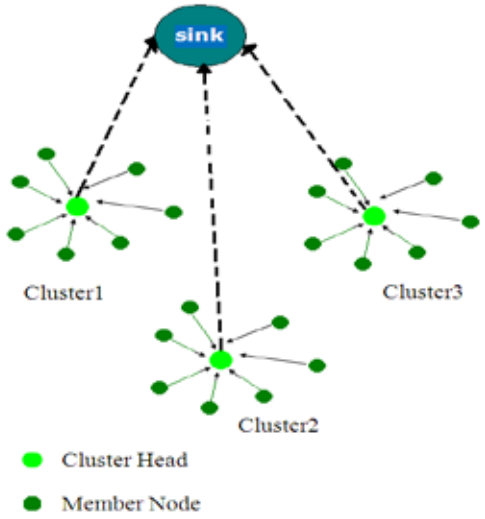


Fig: Cluster Network Architecture

IV. SECURITY IN WSNS

The security in wireless sensor networks includes:

Availability: The node must be able to utilize the resources and the network must be available for the flow of data.

Integrity: Assurance that the information is reliable and accurate.

Confidentiality: The set of rules limiting access to the information. The messages communicated from a sensor network must be confidential i.e. messages must be protected from attacker.

Authentication: Whether the messages are transferred from the node, it claims to be.

The major security attacks:

1. *Message deception*: The attacker modifies the message contents which violates integrity of the message.
2. *Traffic Analysis*: There is a high probability that the attacker analyze the communication patterns even if the message is encrypted.
3. *Selective forwarding*: The adversary may drop or delay the data flow.
4. *Sinkhole attacks*: The attacker attracts the traffic to a compromised node.
5. *Wormholes*: The attacker who is closer to the base station can completely disrupt the traffic by tunneling messages over a low latency link.
6: *False node*: The attacker adds a fake node to inject malicious data.
7. *Malfunctioning node*: The malfunctioning node generates inaccurate data which harms integrity of the sensor network especially if the node is cluster head.
8. *Passive information* Gathering: If the information from sensor networks are not encrypted, then the adversary can easily collect the information.

V. IBS AND IBOOS FOR CWSNS

Secure and efficient data transmission is exclusively significant and is demanded in many practical WSNs.Hence Secure and Efficient data Transmission (SET) protocols, called SET-IBS and SET-IBOOS are introduced, by using the Identity-Based digital Signature (IBS) scheme and the Identity-Based Online/Offline digital Signature (IBOOS) scheme. It is introduced in order to reduce the computation and storage costs to authenticate the encrypted sensed data, by employing digital signatures to message packets, which are systematic in communication and applying the key management for security and reliability. In both the protocols, pairing parameters are distributed and loaded before in all sensor nodes by the BS initially, that swamps the key escrow problem in ID-based crypto-systems.

5.1 The Proposed Set-Ibs Protocol

In SET-IBS scheme the time is split into consecutive time intervals. Time stamps are denoted by Ti for leaf-to-CH communication and Tt for BS-to-node communication. User's public key is denoted by IDp under an IBS scheme. The respective private pairing parameters are preloaded in the sensor nodes during the protocol initialization. If a sensor node wishes to authenticate itself to other node, it need not obtain its private key at the starting of a new round. During node revocation, the BS broadcasts the compromised node IDs to all sensor nodes; each node then stores the revoked IDs within the current round. An additively homomorphic encryption scheme is adopted to encrypt the plaintext of sensed data; where in a specific operation is performed on the plaintext which is equivalent to the operation performed on the ciphertext. This method allows effective aggregation of encrypted data at the CHs and the BS and hence guarantees data confidentiality. In the protocol initialization, the base station performs the following operations of key predistribution to all the sensor nodes:

Setup phase:

Step1: Bs=>GS :< IDbs, Ti, nonce>

Step2: CHa=>GS :< IDa, Ti, adv, Za, Ca>

Step3: Lb à CHa:< IDa, IDb, Ti, join, Zb, Cb>

Step4: CHa=>GS :< Ida, Ti, sched (.., IDb/tb...), Za, Ca>

Steady-state phase:

Step5: Lb à CHb:< Ida, IDb, tb, Cb, Zb, Cb>

Step6: CHa à Bs:< IDbs, Ida, Ti, F, Za, Ca>

Description:

Step1: The BS broadcasts its information to all the nodes.

Step2: The elected CHs broadcast their information.

Step3: A leaf node joins the cluster of a CH a.

Step4: A CH a broadcasts the scheduled message to its members.

Step5: A leaf node b transmits the sensed data to its CH a.

Step6: A CH a transmits the aggregated data to the BS [6].

5.2 The Proposed Set-Iboos Archıtecture

In order to lower the computation and storage costs of signature signing process in the IBS scheme, SET-IBS is improved by the introduction of IBOOS for security in SET-IBOOS. The protocol is initialized in the similar manner as that of SET-IBS; the operations are as follows:

Setup phase:

Step1: Bs=>GS :< IDbs, Ti, nonce>

Step2: CHa=>GS :< IDa, Ti, adv, Ra, Za, Xa>

Step3: Lb à CHa :< IDa, IDb, Ti, join, Rb, Zb, Xb>

Step4: CHa=>GS :< Ida, Ti, alloc (.., IDb/tb ...), Ra, Za, Xa>

Steady-state phase:

Step5: Lb à CHb :< Ida, IDb, tb, Cb, Rb, Zb, Xb>

Step6: CHa à Bs :< IDbs, Ida, Ti, F, Ra, Za, Xa>

Description:

Step1: The BS broadcasts its information to all the nodes.

Step2: The elected CHs broadcast their information.

Step3: A leaf node joins the cluster of a CH a.

Step4: A CH a broadcasts the allocation message.

Step5: A leaf node b transmits the sensed data to its CH a.

Step6: A CH a transmits the aggregated data to the BS.

Notations:

=>, à : Broadcast and unicast transmission.

Lb, Cha, GS :leaf node, Cluster Head, Set of sensor nodes.

Ti, tb : Time stamps denoting time slot for transmission in set up and steady phases.

Ida, IDbs : The IDs of sensor node a and the BS.

Cb, Fa : The encrypted sensed data of node b and the aggregated data of CH a.

adv,join,alloc, sched :Message string types which denote the advertisement join_request,allocation messages and schedule messages.

<Za,Ca> :The ID based digital signature concatenated with data from node a.

<Za,Xa> :The online signature of node a concatenated with Data [6].

5.3 Enhancement Algorıthm

ECC algorithm is used. Elliptic curve cryptography (ECC) is an approach to the public-key cryptography which is based on the algebraic structure of elliptic curves over finite fields. One of the major benefits in comparison with non-ECC cryptography is that the same level of security is provided by keys of smaller size. Elliptic curves are applicable for encryption, digital signatures, pseudo-random generators and other tasks. They also are useful in integer factorization algorithms that have applications in cryptography.

Encryption

```
Random      r = new Random ();
            BigIntegerP =BigInteger.probablePrime(3, r);
           Big Integer Q = BigInteger.probablePrime(3, r);
          Big Integer N =P.multiply (Q);
           Random rand3 = new Random ();
           Int kval= N.intValue ();
```

```
Int kres=rand3.nextInt (kval-1);
BigInteger k=BigInteger.valueOf (kres);
BigInteger b1=k.multiply (P);
BigInteger M=new BigInteger(msg.getBytes ());
BigInteger b2=M.add (b1);
Encmsg=b1+","+b2;
```

Decryption

```
String spt[]=encrypted_data.split(",");
BigInteger b1=new BigInteger (spt[0]);
BigInteger b2=new BigInteger (spt[1]);
BigInteger m=b2.subtract (b1);
Stringfiledata=NewString (m. toByteArray ());
    return filedata;
```

VI. RESULTS

In this paper, we first reviewed data transmission issues and the security issues in CWSNs.We then presented two secure and efficient data transmission protocols for CWSNs, SET-IBS, and SET-IBOOS. We also provided feasibility of the proposed SET-IBS and SET-IBOOS with respect to the security requirements and analysis against routing attacks. SET-IBS and SETIBOOS are efficient in communication and applying the IDbased cryptosystem, which achieves security requirements in CWSNs. Lastly, we implemented ECC algorithm which is highly secure and it makes the hacking task complicated. With respect to both computation and communication costs, SET-IBOOS has less security overhead and is preferred for secure data transmission in CWSNs.An example snapshot is shown below.

Plain text for before applying ECC algorithm:

Cipher text after applying the ECC algorithm

REFERENCES

[1] T. Hara, V.I. Zadorozhny, and E. Buchmann, Wireless Sensor Network Technologies for the Information Explosion Era, Studies in Computational Intelligence, vol. 278. Springer-Verlag, 2010.

[2] Y. Wang, G. Attebury, and B. Ramamurthy, "A Survey of Security Issues in Wireless Sensor Networks," IEEE Comm. Surveys &. Tutorials, vol. 8, no. 2, pp. 2-23, Second Quarter 2006.

[3] A.A. Abbasi and M. Younis, "A Survey on Clustering Algorithms for Wireless Sensor Networks," Computer Comm., vol. 30, nos. 14/ 15, pp. 2826-2841, 2007.

[4] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Microsensor Networks," IEEE Trans. Wireless Comm., vol. 1, no. 4, pp. 660- 670, Oct. 2002.

[5] A. Manjeshwar, Q.-A. Zeng, and D.P. Agrawal, "An Analytical Model for Information Retrieval in Wireless Sensor Networks Using Enhanced APTEEN Protocol," IEEE Trans. Parallel & Distributed Systems, vol. 13, no. 12, pp. 1290 1302, Dec. 2002.

[6] Huang Lu, Jie Li and Mohsen Guizani,"Secure and Efficient Data transmission for Cluster Based Wireless Sensor Networks", IEEE Trans. Parallel & Distributed Systems, vol. 25, no. 3, March.2014.

 ISBN: 978-81-931039-3-7

AN EFFICIENT MECHANISM TO PROTECT CLOUD FROM INTERNET ATTACKS

Lokashree S [1], Lokana S [2], Dr.M V Sathyanarayana [3]

[1] PG Student, [2] PG Student, Computer Science & Engineering,
Rajeev Institute of Technology, Hassan, Karnataka, (India)
[3]Technical Director, Rajeev Institute of Technology, Hassan, Karnataka, (India)

ABSTRACT

Due to rising threat of internet attacks, especially distributed denial-of-service (DDoS), traceback problem has become very relevant to internet security these days. The web services can get vulnerable to denial of services (DoS) or xml denial of services (xdos) attack which hamper web services by crashing the service provider and its services. In order to rescue from such attacks, there are some techniques that are being introduced such as traceback architecture, framework, grid, authentication and the validation. Simple Object Access Protocol (SOAP) allows the communications interaction between different web services. The messages of SOAP are constructed using either Hyper Text Transport Protocol (HTTP) and/or Extensible Mark-up Language (XML). In a way to find the real source of Internet attacks, we must be capable of discovering the origin of IP packets without having to rely on the source IP address field. This capability is known as IP trace back. To address the problem of kinds of internet attacks against cloud web services discussed above there is a need to differentiate the legitimate and illegitimate messages. This work has been used to not only trace DDoS attacking packets but it also enhances filtering attacking traffic. This holds a wide array of applications for other security systems. We have taken three types of filters namely MATCH, MARK, MAKE OVER and DUMP[13]. Then we use ECC algorithm to protect the genuine/legitimate data. The ECC algorithm will compress the original file, encrypts the plaintext data into cipher text and then hides the message being exposed to the attacker.

Keywords: Traceback, SOAP, Ddos Attack, Filters, ECC Algorithm.

I. INTRODUCTION

Cloud computing involves deploying groups of remote servers and software networks that allows centralized data storage and online access to computer services or resources. In a Cloud computing environment, resources are pooled to provide infrastructure, platform and software as services to many possible users by sharing the available resources. In this model customers sign in into the cloud to access IT resources that are priced and provided on-demand. Due to the rising threat of internet attacks, especially distributed denial-of-service (DDoS) attack, Traceback problem has become very relevant to internet security. Since the DDoS attackers spoof the source address, tracing them is very difficult. DDoS attack actually hamper web services by crashing the service provider and its services. The proposed approach is very simple to implement, scalable enough and helps rescue from DDoS attacks more effectively since these attacks can only be detected and cannot be prevented. This approach uses ECC(Elliptical Curve Cryptography)algorithm to compress/encrypt/hide the original data being exposed to the attacker.

1.1 Attributes of Cloud

Some of the essential attributes of the cloud model are security, reliability, availability, scalability, QoS, on-demand self service, broadband network access, resource pooling and rapid elasticity. The cloud can be characterized as private, public, community or uses. In public cloud computing model, services such as applications and storage, are available for general use over the Internet. Services of public cloud may be offered on a pay-per-usage mode or other purchasing models. IBM's Blue Cloud is an example of a public cloud. Private cloud is a virtualized data center that operates within a particular firewall. These types of cloud are highly virtualized, joined together by mass quantities of IT infrastructure into resource pools, and privately owned and managed. A hybrid cloud is a mixture of public and private clouds. Community cloud is an infrastructure shared by several organizations which supports a specific community. The cloud delivers its services in the form of software, platform and infrastructure. Costly applications like ERP, CRM will be offloaded onto the cloud by provider. They run at providers cost. Platform includes the languages, libraries etc. and the database, operating system, network bandwidth comes under infrastructure.

1.2 Security Concerns

Trustworthiness is one of the key concerns of the cloud service provider. Organizations are carefully deceiving both their sensitive and insensitive data to cloud to fetch required services. Cloud works on pay per use basis. Suppose a DoS attacker intentionally sends numerous requests to cloud then the owner of that particular cloud will have to process more requests at a time. Meanwhile, if other genuine users sends request to the server on cloud, their service will be denied since the server will be busy serving the DoS attacker. The other worst case is DDoS attack, where the attacker compromises some more hosts to send the flood request.

1.3 Denial-of-Service Attack/ Distributed Denial-of-Service Attack

A **denial-of-service attack** (**DoS attack**) or **distributed denial-of-service attack** (**DDoS attack**) is an attempt to make a machine or network resource unavailable to its intended users. A DoS attack generally consists of efforts to temporarily or indefinitely interrupt or suspend services of a host connected to the internet. This attack hamper web services by crashing the service provider and its services. DoS attacks are illustrated in figure 1.3(a).

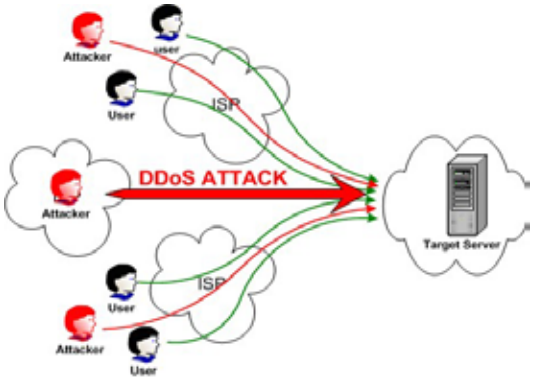


Fig1.3(a): DDoS Attack

1.3.1 Modes of Attack

In a denial-of-service attack, the attacker makes an explicit attempt to prevent legitimate users of a service from using that service. Two common forms of DoS attacks are: 1. those that crash services and, 2. those that flood services.

II. RELATED WORK

In a Cloud computing environment, cloud servers that provide requested cloud services, may sometime crash after they receive huge amount of request [16]. This situation is called Denial Of service attack. Cloud Computing is one of today's most exciting technologies due to its ability to reduce costs associated with computing while increasing flexibility and scalability for computer processes. Cloud Computing is changing the IT delivery model to provide on-demand self-service access to a shared pool of computing resources (physical and virtual) via broad network access to offer reduced costs, capacity utilization, higher efficiencies and mobility. Recently Distributed Denial of Service (DDoS) attacks on clouds has become one of the serious threats to this buzzing technology. Distributed Denial of Service (DDoS) attacks continue to plague the Internet. Distributed Denial-of-Service (DDoS) attacks are a significant problem because they are very hard to detect, there is no comprehensive solution and it can shut an organization off from the Internet. The primary goal of an attack is to deny the victim's access to a particular resource. In this paper, we want to review the current DoS and DDoS detection and defence mechanism.

The main problem faced in a cloud environment is the Distributed denial of service (DDoS) [17]. During such a DDoS attack all consumers will get affected at the same time and will not be able to access the resources on the cloud. All client users send their request in the form of XML messages and they generally make use of the HTTP protocol. So the threat coming from distributed REST attacks are more and easy to implement by the attacker, but such attacks are generally difficult to detect and resolve by the administrator. So to resolve these attacks we introduce a specific approach to providing security based on various filters. We make use of five different filters which are used to detect and resolve XML and HTTP DDoS attack. This allows the security expert to detect the attack before it occurs and block or remove the suspicious client.

Pushback is a mechanism for defending against distributed denial-of-service (DDoS) attacks [18]. DDoS attacks are treated as a congestion-control problem, but because most such congestion is caused by malicious hosts not obeying traditional end-to-end congestion control, the problem must be handled by the routers. Functionality is added to each router to detect and preferentially drop packets that probably belong to an attack.

Upstream routers are also notified to drop such packets (hence the term Pushback) in order that the router's resources be used to route legitimate traffic. In this paper we present an architecture for Pushback, its implementation under FreeBSD, and suggestions for how such a system can be implemented in core routers.

Cloud Computing is an emerging area nowadays. Researchers are working on all aspects of cloud viz [19]. cloud network architecture, scheduling policies, virtualization, hypervisor performance scalability, I/O efficiency, data integrity and data confidentiality of data intensive applications. The dynamic nature of cloud presents researchers new area of research that is cloud forensics. Cloud Forensics is the branch of forensics for applying computer science knowledge to prove digital artifacts. The DDOS is the widely used attack in cloud environment. To do the forensics of DDOS if it is identified a possible detection and prevention mechanisms would aid in cloud forensics solutions and evidence collection and segregation. This paper presents different types of DDOS attack at the different layers of OSI model with increasing complexity in performing attack and focuses more on prevention and detection of DDOS at different layer of OSI and effect of DDOS in cloud computing.

The theoretical background of our proposed work is taken from reference [13]. We are giving security to the confidential data by using ECC algorithm. This algorithm inhibits stronger encryption, efficient performance, high scalbility and future of crypto tech.

III. PROPOSED WORK

Flaws either in users' implementation of a network or in the standard specification of protocols has resulted in gaps that allow various kinds of network attack to be launched. Of the kinds of network attacks, denial-of-service flood attacks have caused the most severe impact. Cloud computing suffers from major security threat problem by HTTP and XML Denial of Service (DoS) attacks. The combination of HTTP and XML messages that are intentionally sent to flood and destroy the communication channel of the cloud service provider is called as HX-DoS attack. To address this issue, there is a need to differentiate the genuine or legitimate message and illegitimate message.

HX-DoS attack involves an attacker who compromises a client having an account to access the cloud service provider server. Therefore, the attacker gets direct connection through the system. Then the attacker will install HX-DoS attack program at the user end and initiates it. The XDoS attack can take place in few ways: First, a network can be flooded with XML messages (instead of packets), in order to prevent legitimate users to network communication. Next, if the attacker floods the web server with XML requests, it will affect the availability of these web services. Finally, attackers manipulate the message content, so that the result web server gets crash. In order to differentiate them, the first method adopts Intrusion Detection System (IDS) by usinga decision tree classification system called as MATCH filter. MATCH filter is located one hop away from host. The rule set of MATCH filter has been built up over time to identify the known HDoS and X-DoS messages. The well known HX-DoS attack is XML injection or XML Payload Overload, MATCH filter is trained and tested to identify these known attacks. After thedetection of HX-DoS message, MATCH filter drops the packet which matches the rule set. The packets are subjected to marking after they are examined by the MATCH filter. The ECC algorithm is used to convert the plaintext data into corresponding cipher text so that the attacker cannot view the original data being transmitted. The ECC algorithm will compress the file, encrypts it and hides the message from DDoS attacker.

IV. DESIGN CONSIDERATIONS

Consider two legitimate users and an attacker. User sends data through three filters namely, MATCH filter, MARK filter and MAKE OVER and DUMP filter to the server.

The message will be identified and if it is from an attacker then that message will be dropped before it reaches the server.

Modulo packet marking consists of two routers:

1. Edge router
2. Core router

On the victim side, by the time the victim starts collecting marked packets, all routers in the network will already have invoked the packet marking procedure. In extension, the victim does not have any knowledge about the real network or the attack graph. But the victim only knows the marking probability that the routers use.

It is appareled with the ability to mark packets as in the original Probabilistic Packet Marking(PPM) algorithm where each router shares the same marking probability. In specific, a router can either be a transit router or a leaf router. A transit router is a router that forwards traffic from upstream routers to its downstream routers or to the victim, whereas a leaf router is a router whose upstream router is connected to client computers and not to routers and forwards the clients' traffic to its downstream routers or to the victim. Assuredly, the clients are mixed with genuine as well as malicious parties. Likewise, every router will be having only one outgoing route toward the victim named "outgoing route toward the victim" and this can be further justified by the fact that modern routing algorithms favor the construction of routing trees.The plaintext data inside the packet will be converted into cipher text data using ECC algorithm so that when an attacker tries to get the data, he will be unable to read the original plain text data. The most essential features of an ECC are as follows: stronger encryption, efficient performance, high scalbility and future of crypto tech.

1.Stronger encryption:

- shorter key than RSA.
- 256-bit ECC = 3072-bit RSA.
- 10 times harder to crack than RSA 2048.
- meets NIST standards.

2.Efficient Performance:

- efficiency increases with higher server loads.
- utilizes less server CPU.
- ideal for mobile devices.

3. High Scalability:

- large SSL deployment without additional hardware.
- securing the enterprise: uses fewer resources, lower costs.

4. Future of crypto tech:

- viable for many years.
- built for internet of Things.
- supports billions of new devices coming online.
- Ideal for open networks.
- truly "future proof" trust infrastructure in place.

4.1 Goals

The denial-of-service (DDoS) attacks are addressed, where they try to suspend services of a host connected to the internet. The major goal of this project is to filter the genuine message from the message and pass that genuine message to the server, so that only genuine user can get resources of Cloud server. And the ECC algorithm is used so that the raw data is encrypted and is converted to cipher text so as to make it difficult the attacker to identify the message. Figure 4.1(a) demonstrates ECC.

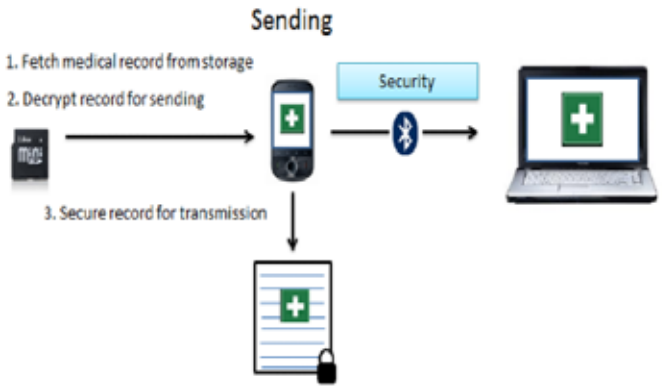


Fig4.1(1): Elliptical Curve Cryptography

4.2 Modules

In a DDoS attack, an attacker compromises a client who has an account to access the cloud service provider server. By this way they get a direct connection through the system. The attacker then installs the DoS attack program at the user end and initiates it. To differentiate them, the first method adopts Intrusion Detection System (IDS) by using a decision tree classification system called as MATCH. MATCH filter is located one hop away from host. MATCH's rule set has been built up over time to identify the known DDoS messages. With the help of known DDoS attacks like XML injection or XML Payload Overload, MATCH filter is able to be trained and tested to identify these known attributes. Upon detection of DDoS message, MATCH filter drops the packet which matches the rule set. After MATCH examines all the packets, they are subjected to marking.

Next marking scheme is the Mark algorithm. As the packets travel via network, they are marked with router information using modulo technique. Upon trace-back request, reverse modulo is used to make over the path traversed by the packets. The marking is done on both edge and core routers. When an edge router decides to mark an incoming packet, it fetches the code to be marked that corresponds to physical address of the host from the lookup table and encodes it into the packet. The edge router requires one bit for indicating whether the packet is marked or not and few bits for marking code and it maintains a lookup table called MAC to ID table, which has physical address of the hosts attached to the network and equivalent numeric code for each of the physical addresses.

The core router marks the packet only if that packet has been already marked by the edge router. Else, it would simply forward the packets. Core router maintains a table called MAC to Interface which contains the physical addresses of all of its hardware input interfaces and link numbers assigned to each of these interfaces.

When a router decides to mark, it consults the table to find the link number assigned to the inbound interface. The core router uses the modulo technique for marking is calculated as in Equation 1,

New marking information= current marking information × number of interfaces on the router + the link number (1)

Make over and Dump filter, which is built from the IDP and its location is one hop back from the victim. Specifically, the host follows the same path (shortest path) across the routers for sending the packet to its destination. Make Over and Dump component maintains the information about each host and its equivalent packet marking value. If the marking value matches the stored value, it forwards the packet to respective host. During the time of the attack, when host spoofs the IP address of another host, the packet marking value differs

from the value stored in the Make Over and Dump filter. This happens because: For marking, MATCH filter uses MAC address instead of the IP address. Therefore, the packets are dumped at the victim side and Make Over and Dump requests for the trace-back.

The ECC algorithm takes place in following steps [14]:

Step1: Select any master file from embed message.

Step2: Select a random picture from the local drive.

Step3: After master file has been selected, select output file to embed message.

Step4: If the file should be compressed, then click on check box compress.

Step5: If the message should be encrypted, then Click on checkbox encrypt message.

Step6: If the message should be hidden, then type message in message box and click on go button, then dialog will be appear with operation is successful or not.

Step7: Close embedding message window by clicking on close button.

Step8: To retrieving encrypted, hidden, compressed message click on retrieve message button and select the output file.

Step9: click on go button and enter the encrypted password for retrieving message.

ElGamal Elliptic curve encryption algorithm is as follows:

Input: Parameters field of elliptic curve (p,E,P,n), public key Q, plain text m.

Output: Ciphertext(C1,C2).

Begin

1. Represent the message m as a point M in E (Fp)
2. Select k ∈ R^[1,n 1].
3. Compute C1 = kP
4. Compute C2 = M+kQ.
5. Return (C1,C2)

End.

ElGamal Elliptic curve decryption algorithm is as follows:

Input: Parameters field of elliptic curve (p, E, P, n), private key D,cipher text (C1,C2).

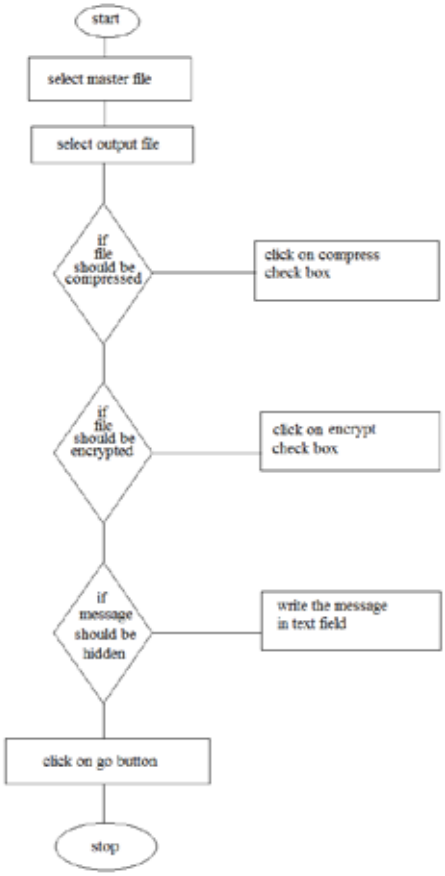
Output: Plain text m.

Begin

1. Compute M = C2 – dC1, and m from M.
2. Return (m).

End.

4.3 Flowchart



Flow Chart

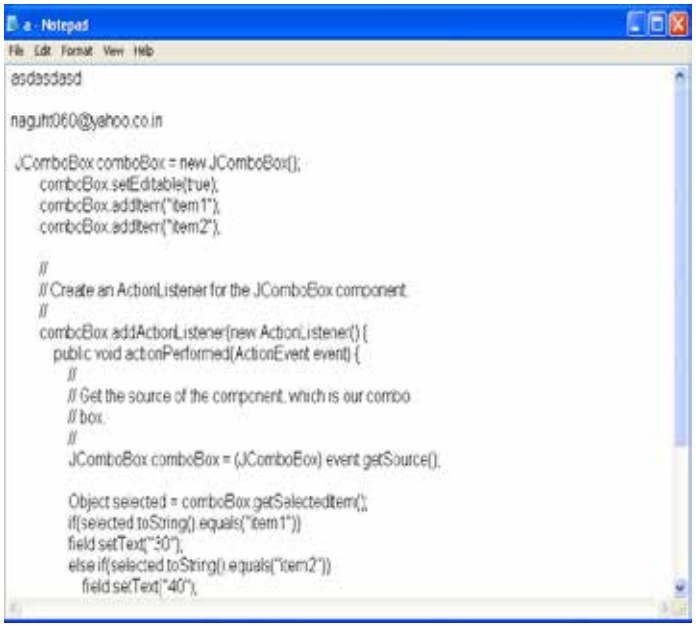
V. CONCLUSION

HTTP or XML-Based DoS attacks are one of the most serious threats to cloud computing. Detection of these attacks can be effectively done by using marking approach based on packets on the attacker side and the detected packets are filtered by dropping the marked packets on the victim side. Therefore, the packet marking overhead and the false positive rate of DoS attacks are effectively reduced. DDoS attack detection scenario is improved by replacing the Cloud Protector with Make Over and Dump on the victim side and the introduction of MATCH filter and MARK filter at the source side. By this, enhancement of the reduction of the false positive rate is done and increase in the detection and filtering of DDoS attacks is possible. By the use of ECC algorithm, the victim can never be able to access the original text. The future work can be extended by integrating the proposed system with the source end defensive systems to detect on MAC spoofing[13].

VI. SNAPSHOTS

The snapshots of the output after we apply ECC algorithm to our plaintext is as shown below:

Plain text for before applying ECC algorithm



Cipher text after applying the ECC algorithm

REFERENCES

[1] A.Belenky and N.Ansari (2003), 'Tracing Multiple Attackers with Deterministic Packet Marking (DPM)', Proceedings of IEEE Pacific Rim conference on communications, computers and signal processing, Vol. 1, pp. 49–52.

[2] A.Chonka W. Zhou and Y.Xiang (2008a), 'Protecting Web Services with Service Oriented Traceback Architecture', Proceedings of the IEEE eighth international conference on computer and information technology, pp. 706-711.

[3] A.Chonka, W.Zhou and Y.Xiang (2008b), 'Protecting Web Services from DDoS Attacks by SOTA', Proceedings of the IEEE fifth interna-tional conference on information technology and applications, pp. 1-6.

[4] A.Chonka, W.Zhou, J.Singh and Y.Xiang (2008c), 'Detecting and Tracing DDoS Attacks by Intelligent Decision Prototype', Proceedings of the IEEE International Conference on Pervasive Computing and Communications, pp. 578-583.

[5] A.Chonka, W.Zhou and Y.Xiang (2009a), 'Defending Grid Web services from X-DoS Attacks by SOTA', Proceedings of the third IEEE international workshop on web and pervasive security (WPS 2009), pp. 1-6.

[6] A.Chonka, W.Zhou and J.Singh (2009b), 'Chaos Theory Based Detec-tion against Network Mimicking DDoS Attacks', Journals of IEEE Communications Letters, Vol. 13, No. 9, pp. 717-719.

[7] A.Chonka, Y.Xiang, W.Zhou and A.Bonti (2011), 'Cloud Security Defence to Protect Cloud Computing against HTTP-DoS and XML-DoS attacks', Jour-nal of Network and Computer Applications, Vol. 34, No. 4, pp. 1097-1107.

[8] D.Dean (2002), 'An algebraic Approach to IP traceback', Journal ACM Transactions on Information and System Security', Vol. 5, No. 2, pp.119-137.

[9] S.Savage, D.Wetherall, A.Karlin and T.Anderson (2000), 'Practical Network Support for IP traceback', Proceedings of the conference on Applications, Technologies, Architectures, and Protocols for Com-puter Communication, pp. 295-306.

[10] H.Shabeeb, N.Jeyanthi and S.N.Iyengar (2012), 'A Study on Security Threats in Clouds', Journal of Cloud Computing and Services Sci-ence, Vol. 1, No. 3, pp. 84-88.

[11] X.Xiang, W.Zhou and M.Guo (2009), 'Flexible Deterministic Packet Marking: an IP Traceback System to Find The Real Source of At-tacks', Journal of IEEE Transactions on Parallel and Distributed Sys-tems, Vol. 20, No. 4, pp. 567-580.

[12] K.H.Choi and H.K.Dai (2004), 'A Marking Scheme using Huffman Codes for IP Traceback', Proceeding of 7th International Symposium on Parallel Architectures, Algorithms and Networks (SPAN'04).

[13] E.Anitha and Dr.S.Malliga (2014), 'A Packet Marking Approach To Protect Cloud Environment Against DDoS' Computer Science and Engineering Department, Kongu Engineering College Perundurai, India mallisenthil@kongu.ac.in .

[14] Randhir Kumar, Akash Anil (2011), 'Implementation of Elliptical Curve Cryptography' IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 4, No 2, July 2011 ISSN (Online): 1694-0814.

[15] K.Santhi, (2013), 'A Defense Mechanism to Protect Cloud Computing Against Distributed Denail of Service Attacks, volume 2, Issue 5, May 2013.

[16] Nisha H. bhandari (2013), 'Survey on DDoS Attacks and its Detection & Defence Approaches' IJISME.

[17] R. Vivek, R. Vignesh & V. Hema (2013), 'An Innovative Approach to Provide Security in Cloud by Prevention of XML and HTTP DDoS Attacks' ISSN(PRINT : 2320-8945, volume-1,Issue-1,2013.

[18] John Ioannidis, Steven M. Bellovin (2010) 'Implementing Pushback: Router-Based Defense Against DDoS Attacks' .

[19] J.J. Shah, Dr. L.G. Malik (2013), 'Impact of DDOS Attacks on Cloud Environment', Communication Technology, vol 2, Issue 7, July-2013.

 ISBN: 978-81-931039-3-7

RESONANCE CHARACTERISTICS OF MICROSTRIP ANTENNA AS A FUNCTION OF SUBSTRATE THICKNESS

RitikaTandon[1], Alpana Singh[2], Saurabh Khanna[3]

[1,2]M.Tech Scholar, Subharti University Meerut, U.P. (India)

[3]Assistant Professor, EN Department NIT, Meerut, U.P. (India)

ABSTRACT

A set of measurements of annular ring slot antennas on substrates of varying thickness is presented. The most important factors in design of microstrip circuit and antenna are choice of the best substrate thickness and the dielectric constant to have low losses. In this case an attempt has been made by selecting various dielectric thicknesses to study return loss. For this, an annular ring slot microstrip antenna (ARSMSA) is designed at 3.0 GHz and simulated on different substrate thicknesses ranging from 0.5mm to 3.0 mm using Zeland IE3D software. The variation in return loss is found from -5.869dB to -42.16.

Keywords: Microstrip Annular Ring Slot Antenna (ARSMSA), Return Loss, VSWR, Dielectric Thickness

I. INTRODUCTION

Recent interest has developed in radiator etched on electrically thick substrates as these antennas are used for high frequency applications. However, microstrip antennas inherently have narrow bandwidth. In many cases, their increased impedance bandwidth is also paid for poorer radiation characteristics. Recent interest in millimeter wave systems and monolithic fabrication, however, has created a need for substrates that are electrically thicker, and/or have high permittivity. Increased bandwidth is another reason for interest in electrically thicker substrates. Anomalous results have been previously observed for printed antennas on such substrates. Many of the theoretical models, which worked well for thin, low dielectric constant substrates, fail to give good results for thicker or higher permittivity substrates.

In order to determine the range of validity of these models, and to provide a database of measured data for the testing of improved models, this paper describes the results of a comprehensive set of measurements of annular ring slot microstrip antennas. Ten individual antennas were designed and simulated with different substrate thickness viz.(0.2mm, 0.5mm, 0.75mm, 1.25mm, 1.75mm, 2.0mm, 2.5mm, 2.75mm and 3.0mm).The dielectric constant is assumed constant as 4.2 and fed with a coaxial probe. The measured resonant frequencies are reported for each case. The simulated results are then compared with the antennas on different thickness of substrates.

II. ANTENNA GEOMETRY AND DESIGN

The geometry of the proposed antenna is shown in Fig.1.The ground plane lies at the bottom side of the antenna with a very compact size of 21.75mm × 31mm × (0.5 to 3.0) mm. The radiation elements of the proposed antenna consist of an annular ring slot, operating approximately at 2.9 GHz (however a slight variation is also noticed in table 1 which is negligible for wideband operations).m. The operating frequency is taken as 3 GHz. The other parameters are calculated using [7] and found as: W=31mm, h= (0.5 to 3.0) mm (assumed), ε_{eff}=4.63, L_{eff}=23.2mm, ΔL=0.72mm and L=21.75mm at ε_r=4.2. For a rectangular microstrip antenna the resonant frequency is given as:

$$f_r = \frac{c}{2(L+\Delta L)\sqrt{e_r}}$$

Where length extension (ΔL):

$$\Delta L = 0.412h\frac{(e_{eff}+0.3)\left(\frac{W}{h}+0.264\right)}{(e_{eff}-0.258)\left(\frac{W}{h}+0.8\right)}$$

Optimum value of W:

$$W=\frac{l_o}{2}\left(\frac{(e_r+1)}{2}\right)^{-1/2} \text{ and } \frac{\Delta f_r}{f_r}=\frac{\sqrt{e_r}-\sqrt{e_{e0}}}{\sqrt{e_o}}\text{; also } \sqrt{e_e}=\sqrt{e_{eo}}+\Delta\sqrt{e_e}$$

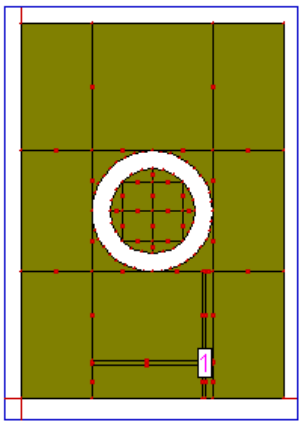


Fig.1: annular ring slot antenna with W=31mm, h= (0.5 to 3.0)mm (assumed), ε_{eff}=4.63, L_{eff}=23.2mm, ΔL=0.72mm and L=21.75mm at ε_r=4.2. fed by coaxial probe at (15.15mm, 2.975mm)

III. MEASUREMENTS AND RESULTS

Microstrip antenna of annular ring slot shape is designed at 3.0 GHz. various substrates thickness has been used to simulate the antenna. The ARSMSA is fed by a coaxial probe at (15.15mm, 2.975mm). The antennas were tested for VSWR and return loss using Zeland IE3D software. A careful simulation study of resonant frequency, bandwidth and return loss of the antenna was undertaken and the results of return loss are presented. . The radiation elements of the proposed antenna consist of an annular ring slot, operating approximately at 2.9 GHz (however a slight variation is also noticed in table 1.

 ISBN: 978-81-931039-3-7

The results obtained are given in table 2**.** It can be observed that, variation in return loss is found from -5.869dB to -42.16 dB obtained for various substrates thickness.

Table I

Return Loss for Different Dielectric Thickness and Resonance Frequency

Return Loss(dB)→ Frequency (MHz)↓	**Thickness of Dielectric Substrate (mm)**									
	0.2	**0.5**	**0.75**	**1**	**1.25**	**1.75**	**2**	**2.5**	**2.75**	**3**
2.874	-1.331	-4.535	-2.263	-2.287	-2.697	-4.578	-6.12	-11.48	-17.1	-27.63
2.879	-1.686	-6.325	-2.728	-2.652	-3.072	-5.149	-6.878	-13.09	-20.33	**-30.49**
2.889	-2.995	-16.05	-4.283	-3.757	-4.156	-6.748	-9.012	-18.31	**-42.16**	-20.31
2.896	-4.432	**-19.8**	-5.964	-4.817	-5.141	-8.151	-10.91	-25.01	-25.02	-16.72
2.897	-4.697	-17.19	-6.301	-5.016	-5.322	-8.404	-11.26	-26.72	-23.74	-16.28
2.905	-6.446	-8.187	-9.83	-6.917	-6.981	-10.7	-14.52	**-29.89**	-17.68	-13.61
2.912	**-5.869**	-4.776	-16.16	-9.894	-9.413	-14.03	-19.62	-19.53	-14.27	-11.67
2.913	-5.701	-4.57	**-16.8**	-10.24	-9.689	-14.41	-20.22	-19	-14.02	-11.52
2.92	-3.933	-3.069	-15.19	-14.52	-13.07	-18.86	**-24.26**	-15.05	-11.95	-10.18
2.927	-2.515	-2.115	-9.302	**-16.68**	-17.46	**-20.66**	-18.49	-12.24	-10.23	-8.999
2.93	-2.198	-1.901	-8.068	-15.32	**-17.87**	-19.24	-16.8	-11.54	-9.775	-8.672

Table II

Return Loss (Maximum Value) for Different Dielectric

Dielectric thickness	**Maximum dB value**
0.2	**-5.869**
0.5	**-19.8**
0.75	**-16.8**
1	**-16.68**
1.25	**-17.87**
1.75	**-20.66**
2	**-24.26**
2.5	**-29.89**
2.75	**-42.16**
3	**-30.49**

The **plots** of return loss for different dielectric thickness are given from figure 2 to figure 11. However, other parameters such as VSWR, radiation resistance and smith chart are not included this time.

 ISBN: 978-81-931039-3-7

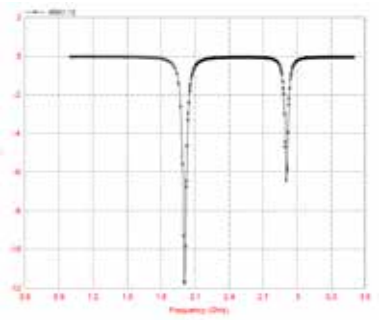


Fig.2: Return Loss (Substrate Thickness 0.2mm)

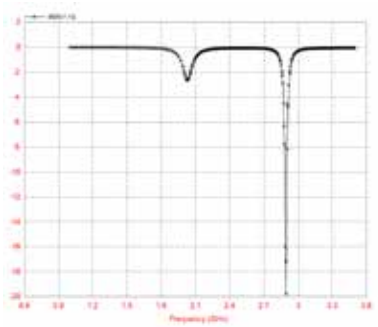


Fig.3: Return Loss (Substrate Thickness 0.5mm)

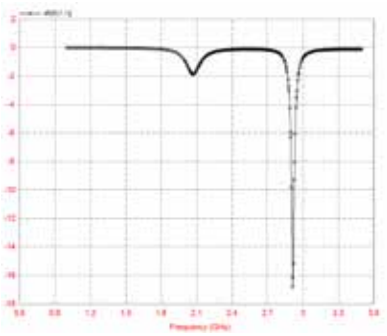


Fig.4: Return Loss (Substrate Thickness 0.75mm)

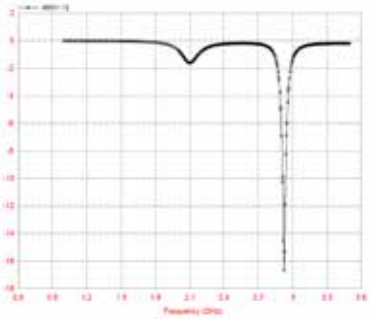


Fig 5: Return Loss (Substrate Thickness 1.0mm)

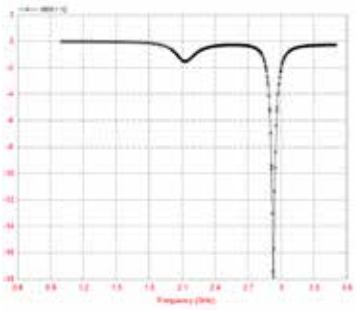


Fig.6: Return Loss (Substrate Thickness 1.25mm)

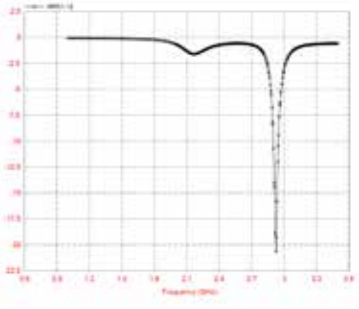


Fig.7: Return Loss (Substrate Thickness 1.75mm)

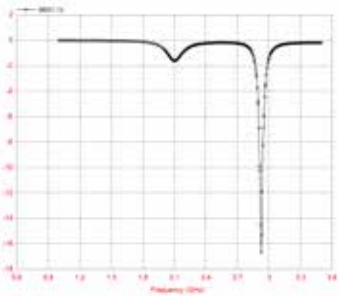


Fig 8: Return Loss (Substrate Thickness 2.0mm)

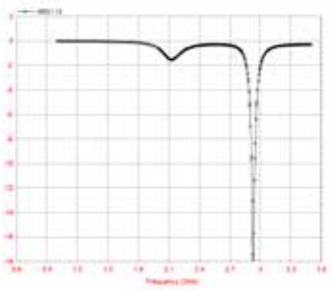


Fig.9: Return Loss (Substrate Thickness 2.5mm)

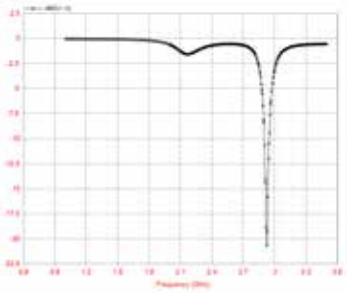


Fig.10: Return Loss (Substrate Thickness 2.75mm)

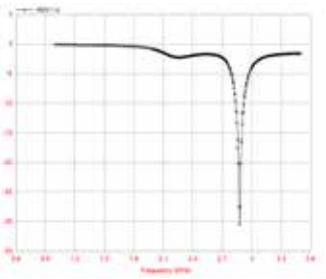


Fig 11: Return Loss (Substrate Thickness 3.0mm)

IV. CONCLUSION

This paper has presented a set of measurements of annular ring slot antennas on substrates of different thickness and fixed permittivity equal to 4.2.Therefore for the design of a radiator se1ection of suitable substrate thickness is very essential. The results shown in figure 12 are very useful f o r selection of suitable substrates for specific annular ring slot antenna applications. For the annular ring slot microstrip antenna (ARSMSA) designed at 3.0 GHz and simulated on different substrate thicknesses ranging from 0.5mm to 3.0 mm using Zeland IE3D software, the variation in return loss is found from -5.869dB to -42.16. A slight variation in resonance frequency is also noticed which can be neglected for wideband application.

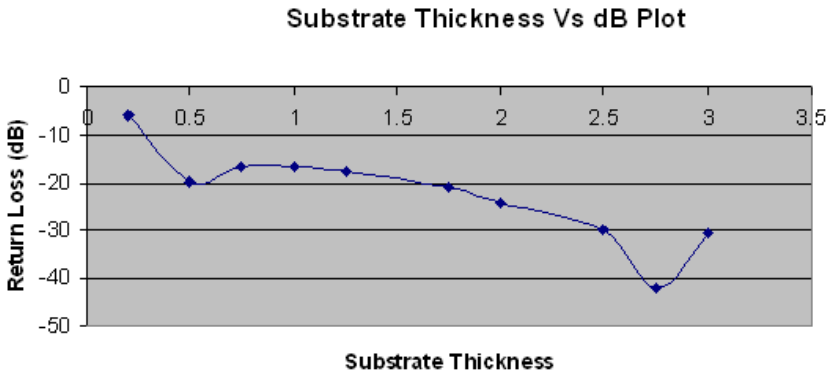


Fig 12. Return Loss vs Substrate Thickness Curve

REFERENCES

[1]. Bahl I J & B Bhartia,"Microstrip Antennas", Arctech House. pp. 1-65.

[2]. D M Pozar & S M Voda, " A Rigorous Analysis of Microstripline fed patch antenna" IEEE Trans. on A & P, Vol. No.6, 1982.

[3]. M Kara, "Effective p e r m i t t i - v i t y of rectangular microstri p antenna elements w i t h various thickness of substrates", Microwave 8 Optical Technology, Vol. 10, Issue 4, Nov. 1995.

[4]. Daniel H. Schaubert,David M. PozarAndrew Adrian" 1989Effect of Microstrip Antenna Substrate Thickness and Permittivity: Comparison of Theories with experiment" IEEE transactions on antennas and propagation, vol. 31, No. 6.

[5]. J. Bahl and P. Bhartia, "Design of microstrip antennas covered with a dielectric layer," IEEE Trans. Antennas Propagat., vol. AP-30, pp. 314-318, Mar.1982.

[6]. C. A. Balanis, Antenna Theory Analysis and Design. 3rd ed., Hoboken, New Jersey: Wiley, 2005.chapter 14.

[7]. K. Chang, Microwave Ring Circuits and Antennas, John Wiley & Sons., 1996, pp. 125-189

[8]. Dau-Chyrh Chang , Ji-Chyun Liu , Bing-Hao Zeng , Ching-Yang Wu , Chin-Yen Liu "Compact Double-ring Slot Antenna with Ring-fed for Multiband Applications" International Symposium on Antennas and Propagation— ISAP 2006 pp-1-5.

ANALYSIS OF ANNULAR RING SLOT MICROSTRIP ANTENNA FOR MULTIBAND OPERATION

Alpana Singh[1], RitikaTandon[2], Saurabh Khanna[3]

[1,2]*M.Tech Scholar, Subharti University, Meerut, U.P. (India)*

[3]*Assistant Professor, EN Department NIT, Meerut, U.P. (India)*

ABSTRACT

This paper presents a compact interconnected double ring slot [1] antenna operating at 1.151 GHz and 2.766 GHz. The radiating elements of the proposed antenna are composed of a interconnected Double ring slot. The antenna size is very compact (48.51mm ×62.02mm × 1.6mm), and can be integrated easily with other RF front-end circuits. It is demonstrated that the proposed antenna is a dual band antenna with satisfactory radiation characteristics. The simulations are carried out using Zeland IE3D software

Keywords: Double Ring Slot Antenna (ARSMSA), Return Loss, VSWR, Dual Band

I. INTRODUCTION

Recent interest has developed in radiator etched on electrically thick substrates as these antennas are used for high frequency applications. However, microstrip antennas inherently have narrow bandwidth. In many cases, their increased impedance bandwidth is also paid for poorer radiation characteristics. Recent interest in millimeter wave systems and monolithic fabrication, however, has created a need for substrates that are electrically thicker, and/or have high permittivity. Ring slot antennas have been of great interest to many researches and engineers and many related studies have been reported in the open literature. Many characteristics of the ring-slot antenna have been demonstrated [2, 3, and 4]; however, little information on the effects of a finite ground plane on the impedance and radiation characteristics of the ring-slot antennas is presented.

In order to determine the range of validity of these models, and to provide a database of measured data for the testing of improved models, this paper describes the results of a comprehensive set of measurements of interconnected double ring slot microstrip antennas.

II. ANNULAR-SLOT ANTENNA CONFIGURATIONS AND OPERATIONS

For the proposed annular-slot antenna, the first mode is mainly determined by the circumference of the inner and outer slot-rings (in case of multiple slots), and the second mode is mainly determined by the outer circumference. The annular-slot widths and the microstrip feed line parameters also have a significant effect on performance. An approximation is given by [5]:

$$\lambda_{gs}=2\pi R \quad (1)$$

where R is the radius of annular-slot, λ_{gs} is slot guided wavelength where:

$$\lambda_{gs}= \lambda_o\{1.045 - 0.365\ln\varepsilon_r + \frac{6.3(W/h)\, e_r^{0.945}}{(238.64+100W/h)} - [0.148 - \frac{8.81(e_r+0.95)}{100e_r}]\ln(h/\lambda_o)\} \quad (2)$$

he slot antenna is tightly coupled to the coaxial probe and hence, the feed line parameters are key factors. To achieve different dual band characteristics, it is necessary to tune and optimize the slot widths (for multiple rings).

For a single ring, when the mean circumference of the ring is equal to an integral multiple of the guided wavelength, the resonance is established and expressed as [6]:

$$l=2\pi R = n\lambda_{gs}, \text{ for } n= 1, 2, 3 .... \quad (3)$$

zWhere l is the mean circumference of the ring, λ_{gs} is the guided wavelength. The guided wavelength is related to the effective dielectric constant as:

$$\lambda_{gs}=\frac{l_o}{\sqrt{e_{eff}}}; \quad (4)$$

Where λ_o is the wavelength in free space, ε_{eff} is the effective dielectric constant. Thus, the resonant frequencies can be represented as:

$$f_n=\frac{nc_o}{l\sqrt{e_{eff}}}, \quad (5)$$

for mode n=1, 2, 3 …where c is the speed of light. Equation 1 is applicable for multiple slot ring structure. This equation holds good for the analysis of slot ring (multiple ring) for multiband operation.

III. ANTENNA GEOMETRY AND DESIGN

The geometry of the proposed antenna is shown in Fig.1.The ground plane lies at the bottom side of the antenna with a compact size of 48.51mm × 62.02mm × 1.6mm.The radiation elements of the proposed antenna consist of interconnected double ring slot, operating approximately at operating at 1.151 GHz and 2.766 GHz). The design frequency is taken as 1.5 GHz. The antenna is proposed to design on a glass epoxy material with dielectric constant 4.2 and the thickness equal to 1.6mm. Fig. 1 is the exact figure as designed in Zeland IE3D The other parameters are calculated using [7] and found as: W=62.02mm, h= 1.6mm (assumed), ε_{eff}=3.998, L_{eff}=50.01mm, ΔL=0.75mm and L=48.51mm for ε_r=4.2. For a rectangular microstrip antenna the resonant frequency is given as[8]:

$$f_r=\frac{c}{2(L+\Delta L)\sqrt{e_r}} \quad (6)$$

Where length extension (ΔL):

$$\Delta L = 0.412h\frac{(e_{eff}+0.3)\left(\frac{W}{h}+0.264\right)}{(e_{eff}-0.258)\left(\frac{W}{h}+0.8\right)} \quad (7)$$

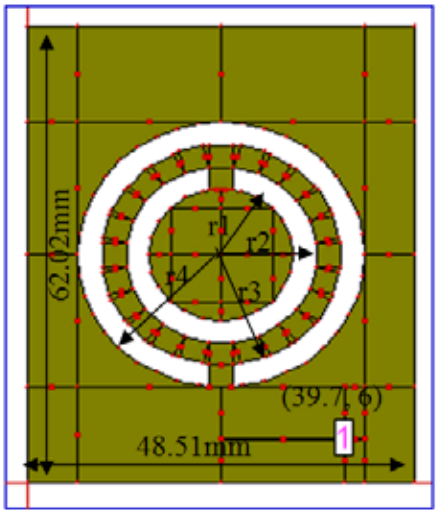


Fig.1: annular ring slot antenna W=62.02mm, h=1.6mm(assumed), ε_{eff}=3.998, L_{eff}=50.01mm, ΔL=0.75mm and L=48.51mm for ε_r=4.2.r1=18mm, r2=15mm, r3=12mm, r4=9mm

IV. SIMULATION AND RESULTS

The simulated return-loss (RL) and VSWR curve for the interconnected double ring slot antenna are shown in Fig. 2 and fig. 3. The substrate with dielectric constant ε_r = 4.2 and thickness h = 1.6 mm is used. A 50Ω coaxial probe is directly feeds at point (39.7, 6). Figure 2 shows the simulated return loss of the proposed slot antenna. The simulated result shows that the resonant frequency located at 1.151 and 2.766 with satisfactory radiation characteristics covering some UWB spectrum.

The antennas were simulated for VSWR and return loss using Zeland IE3D software. A careful simulation study of resonant frequency, bandwidth and return loss of the antenna was undertaken and the results of return loss are presented. The radiation elements of the proposed antenna consist of an interconnected double ring slot, operating at dual frequency.

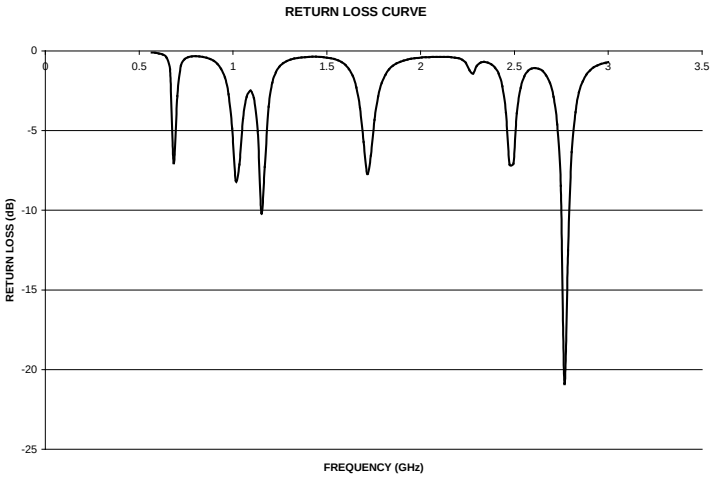


Fig.2: Return Loss Curve for Proposed Antenna

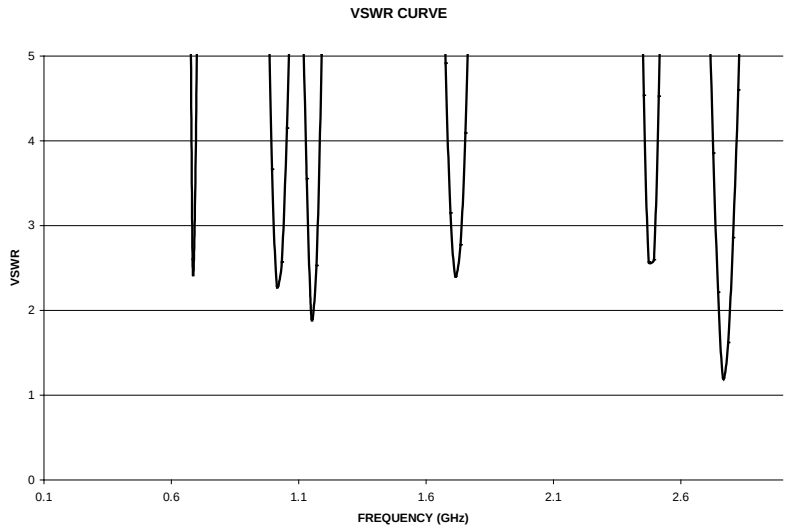


Fig.3: VSWR Curve for Proposed Antenna

Fig. 3 and fig.4 represents VSWR and smith chart respectively. The values of VSWR are taken below 5 only.

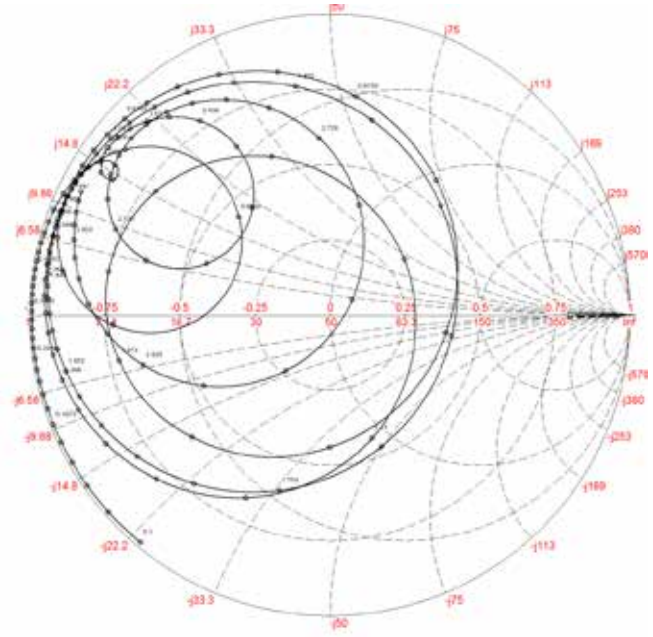


Fig.4: VSWR Curve for Proposed Antenna

V. CONCLUSION

The interconnected double ring slot microstrip antenna has been designed and analyzed in this paper. The structure is smaller in size and easy to fabricate. Its operations cover the applications around center frequencies 1.151 GHz and 2.766 GHz) with satisfactory radiation characteristics for return loss less than -10dB. Simulation results agree with the verified frequency responses and radiation characteristics. In applications, it can be applied to the UWB bands and others applications lying in ultra wide band.

REFERENCES

[1]. X.L.Bao, M.J. Ammann," Microstrip-fed dual-frequency annular-slot antenna loaded by split-ring-slot" IET Microw. Antennas Propag., 2009, Vol. 3, Iss. 5, pp. 757–764

[2]. Hooman Tehrani and Kai Chang, "Multifrequency Operation of Microstrip-fed Slot-Ring Antennas on Thin Low-Dielectric Permittivity Substrates", IEEE Trans., Sept. 2002, AP-50, pp. 1299-1308.

[3]. Jin-Sen Chen, "Dual-frequency annular-ring slot antennas fed by CPW feed and microstrip line feed",IEEE Tran., 2005, AP-53, pp. 569 – 573.

[4]. Row, J.-S., Sim, C.Y.D. and Lin, K.-W., "Broadband printed ring-slot array with circular polarization", Electronics Letters, 2005, Vol. 41, Issue 3, pp.110 – 112.

[5]. J.R. James, P.S.Hall,"Handbook of Microstrip Antennas," IEE Electromagnetic Series 28, pp.611-620.

[6]. Dau-Chyrh Chang , Ji-Chyun Liu , Bing-Hao Zeng , Ching-Yang Wu , Chin-Yen Liu "Compact Double-ring Slot Antenna with Ring-fed for Multiband Applications" International Symposium on Antennas and Propagation— ISAP 2006 pp-1-5

[7]. C. A. Balanis, Antenna Theory Analysis and Design. 3rd ed., Hoboken, New Jersey: Wiley, 2005.chapter 14.

[8]. Bahl I J & B Bhartia,"Microstrip Antennas", Arctech House. pp. 1-65.

 ISBN: 978-81-931039-3-7

DECENTRALIZED ACCESS CONTROL WITH ANONYMOUS AUTHENTICATION OF DATA USING MULTI-CLOUD STORAGE

[1]S. Thirumurugan, [2]S. Vignesh

[1,2] Department of Computer Science and Engineering,

Christ College of Engineering and Technology, Puducherry, (India)

ABSTRACT

A new decentralized access management theme for secure knowledge storage in clouds that support anonymous authentication. During this theme, the cloud verifies the believability of the user while not knowing the user's identity before storing knowledge and additionally has value-added the feature of access management during which solely valid users area unit ready to rewrite the hold on data. The theme prevents reply attack and supports creation, modification, and reading the information hold on within the cloud user and additionally has the address user revocation. Moreover, our authentication and access management theme is decentralized and sturdy, in contrast to alternative access management schemes designed for Multi-Cloud Storage. The communication, computation, and storage overheads area unit resembling centralized approaches. If the user doesn't have credentials to urge the key and incorrectly coming into key to access the file implies that persona non grata identification activates the system to transfer a pretend file to the persona non grata and inform to the administrator of the system {and the|and therefore the|and additionally the} user who created that file is try and access and also hide the attribute and access policy of a user.

Keyword: Trespasser Identification, Attribute Based Encryption, Attribute Based Signature, ID-DPDP Protocol

I. INTRODUCTION

Cloud Computing refers to manipulating, configuring and accessing the applications on-line. It offers on-line information storage, infrastructure and application by putting in a bit of computer code on our native laptop and this can be however the cloud computing overcomes platform dependency problems. Hence, the Cloud Computing makes the business application mobile and cooperative like Google Apps, Microsoft on-line and infrastructures like Amazon's EC2, Eucalyptus, Nimbus, and platforms to assist developers write applications like Amazon's S3, Windows Azure. A lot of the information hold on in clouds is extremely sensitive those square measure medical records and social networks.

Security and privacy square measure the important problems in cloud computing. The user ought to evidence itself before initiating any tasks. User privacy is additionally needed in order that the cloud or the opposite users don't recognize the identity of the user. The cloud will hold the user in command of the information it outsources and therefore the services it provides. The validity of the user World Health Organization stores the information is additionally verified.

Cloud computing has received plenty of recognition within the previous couple of years and market observers believe it to be the longer term, however not if security issues persist. For folks that aren't accustomed to cloud computing, it's the apply that involves usage of network servers that square measure remotely settled. Users will access the remote servers via the web to manage, store and method relevant information, instead of on the non-public pc of an area server. Several businesses square measure victimization cloud computing that typically seems to be cheaper, quicker and simple to take care of. Now, not solely businesses however regular web users also are victimization cloud computing services like Google Docs, Drop box and additional to access their files whenever and where they require.

Cloud computing has accelerated with the wide use of the web services similarly as development of mobile devices like good phones and tablets. Many of us carry their transportable devices once not on their table and simply access their documents, media and photos on cloud storage via the web. With the event in technology market, consultants also are disturbed regarding the magnified security wants for cloud computing. While there area unit advantages, there area unit privacy and security issues too. Security problems, the necessity to segregate information once handling suppliers that serve multiple customers, potential secondary uses of the data—these area unit areas that organizations ought to detain mind once considering a cloud supplier and once negotiating contracts or reviewing terms of service with a cloud supplier. on condition that the organization transferring this info to the supplier is ultimately in control of its protection, it has to make sure that the private info is suitable handled.

Clouds will offer many varieties of services like applications, infrastructures, and platforms to assist developers write applications uses a rhombohedral key approach and doesn't support authentication further. Provides privacy protective echt access management. However, the authors take a centralized approach wherever one key distribution centre (KDC) distributes secret keys and attributes to all or any users. sadly, one KDC isn't solely one purpose of failure however tough to take care of thanks to the big range of users that area unit supported in an exceedingly cloud atmosphere. We, therefore, emphasize that clouds ought to take a localised approach whereas distributing secret keys and attributes to users. it's conjointly quite natural for clouds to possess several KDCs in several locations within the world.

A single KDC is employed however tough to take care of thanks to the big range of users that area unit supported in an exceedingly cloud atmosphere. rhombohedral key approaches offer key to user. Authentication isn't needed.In cloud computing, remote knowledge integrity checking is a very important security downside. The clients' large knowledge is outside His management. The malicious cloud server might corrupt the clients' knowledge so as to realize additional advantages. Several researchers projected the corresponding system model and security model. In 2007, demonstrable knowledge possession (PDP) paradigm was projected by Ateniese et al. within the PDP model; the voucher will check remote knowledge integrity with a high chance. Supported the RSA, they designed 2 incontrovertibly secure PDP schemes. After that, Ateniese et al. projected dynamic PDP model and concrete theme though it doesn't support insert operation. so as to support the insert operation, in 2009,Erway et al.

Presented the primary proof of retrievability (POR) theme with demonstrable security. In POR, the voucher will check the remote knowledge integrity and retrieve the remote knowledge at any time. The state of the art will be found. On some cases, the shopper might delegate the remote knowledge integrity checking task to the third party. It ends up in the third party auditing in cloud computing. One amongst advantages of cloud storage is to change universal knowledge access with freelance geographical locations. This means that the tip devices are

also mobile and restricted in computation and storage. Economical integrity checking protocols area unit additional appropriate for cloud shoppers equipped with mobile finish devices.

II. MATHEMATICAL BACKGROUND

2.1 System Intialization

Select a primary letter of the alphabet, and teams *G1* and *G2*, that square measure of order letter of the alphabet. We have a tendency to outline the mapping *ˆe:G1 ×G1 → G2.* Let *g1, g2* be generators of *G1* and *hj* be generators of *G2*, for *j ∈ [tmax]*, for capricious *tmax.* Let *H* be a hash perform. Let *A0 = hao0,* wherever *a0 ∈Z∗q* is chosen indiscriminately. *(TSig,TVer)* mean *TSig* is that the personal key with that a message is signed and television er is that the public key used for verification. the key key for the trustee is *TSK = (a0, TSig)* and public secret's *TPK = (G1, G2, H, g1, A0, h0, h1, . . . , htmax, g2, TVer).*

2.2 User Audition

Added users square measure able to choose here. The Search Results panel helps you to find users in your organization's user directory and add them to the list of users for the sort you've elite. To seek out and add user names to a job is to enter a reputation within the Search text box, and so click Search. Contribute shows the nearest matches it finds within the Search Results list. Choose the name of the user you wish to feature to the role, and click on increase move that user to the list of Users to feature. The roles square measure characteristic the attribute to be used here. The attributes square measure typically able to establish the access policy of the files and contents of it.

2.3 Files Access

Attribute based mostly File Access has been wide deployed during this systems in recent years. The event of knowledge and communication technologies, square measure teams and departments square measure raising that needs dynamic user-role and permission-role assignments. In these situations it's impracticable, if not possible, for few security officers to handle the assignment for varied applications. During this project, we have a tendency to project this approach for redistributed systems.

2.5 Attribute Verification

Attribute Verification one in every of variety of Identity knowledge. Login to a Managed System typically comprises a User ID and word. Identification might also use a PKI certificate, and Authentication could use Tokens or biometry or a collection of private queries that the user should answer. Here I hooked up the method of attribute based mostly access role for every file having the safety lock to access it. The attributes square measure collected from the user's profile that got login currently. The attributes lock system and also the set of attributes grant access square measure already designed by the creator of the file.

2.5 2 Layer Approach

A 2 layer approach is mostly used once one party desires to reveal the contents of messages sent to a different one and encrypted with a key the receiver. This approach is developed because the cipher text is remodeled to the Encoded kind at the primary layer of encoding. Then the encoded text are encrypting with the generated key mistreatment MD5 algorithmic program. This generates a replacement key that may use to decode the message. If we have a tendency to send a message that was encrypted beneath a key, the proxy can alter the message,

permitting decipherment it then decrypting it. This methodology permits for variety of applications law-enforcement observance, and content distribution. Since the goal of the many re-encryption schemes is to avoid revealing either of the keys or the underlying plaintext to the proxy, this methodology isn't ideal.

2.6 Trespasser Identification

The system can work for the users United Nations agency square measure have the login credentials and also the attributes to access the cipher text knowledge contents and by the approach of Secret keys. The key keys square measure exploring from KDC. If the user doesn't have credentials to urge the key and incorrectly coming into key to access the file means trespasser identification activates the system to transfer a faux file to the trespasser and inform to the administrator of the system and also the user United Nations agency created that file is try and access.

2.7 Multiple Kdc Setup

A typical operation with a KDC involves asking from a user to use some service. The KDC can use crypto logical techniques to demonstrate requesting users as themselves. It will conjointly check whether or not a private user has the correct to access the service requested. If the echt user meets all prescribed conditions, the KDC will issue a price ticket allowing access. KDCs operate with MD5 algorithmic program and Attribute based mostly encoding key on this.

The KDC produces a price ticket supported a server key. The user receives the price ticket and submits it to the acceptable server. The server will verify the submitted price ticket and grant access to the user submitting it. Security systems mistreatments KDCs embody practicality between 2 totally different agents. The only KDC will build bother whereas we have a tendency to accessing with most variety of users. In this we separate the KDC to 2 gateways. One work for little size files contents key and security handling another one is for to assist the utmost file sized contents key.

2.8 Multi-Cloud Storage (Id-Dpdp Protocol)

Private verification, delegated verification and public verification: Our projected ID-DPDP protocol satisfies the non-public verification and public verification. Within the verification procedure, the information within the table Tcl and R ar indispensable. Thus, it will solely be verified by the consumer UN agency has Tcl and R i.e., it's the property of personal verification. On some cases, the consumer has no ability to see its remote knowledge integrity, as an example, he takes half within the battle within the war. Thus, it'll delegate the third party to perform the ID-DPDP protocol. The third party is also the third auditor or the proxy or different entities. The consumer can send Tcl and R to the recipient. The recipient will perform the ID-DPDP protocol. Thus, it's the property of delegated verification. On the opposite hand, if the consumer makes Tcl and R public, each entity will perform the ID-DPDP protocol by himself. Thus, it's conjointly the property of public verification.

III. PROPOSED DECENTRALIZED ACCESS CONTROL WITH ANONYMOUS AUTHENTICATION OF DATA STORED IN CLOUDS

Proposed a decentralised approach, their technique doesn’t manifest users, World Health Organization need to stay anonymous whereas accessing the cloud. In AN earlier work, Ruj et al. planned a distributed access management mechanism in clouds. However, the theme gives user authentication. Alternative the opposite} disadvantage was that a user will produce and store a file and other users will solely browse the file. Write

access wasn't permissible to users apart from the creator. Within the preliminary version of this paper, we have a tendency to extend our previous work with value-added options that permits to manifest the validity of the message while not revealing the identity of the user World Health Organization has keep info within the cloud. During this version we have a tendency to conjointly address user revocation. We have a tendency to use attribute primarily based signature theme to realize legitimacy and privacy.

Advantages extend our previous work with value-added options that permits to manifest the validity of the message while not revealing the identity of the user World Health Organization has keep info within the cloud. Users attributes area unit hide and conjointly hide access policy from unauthorized user.

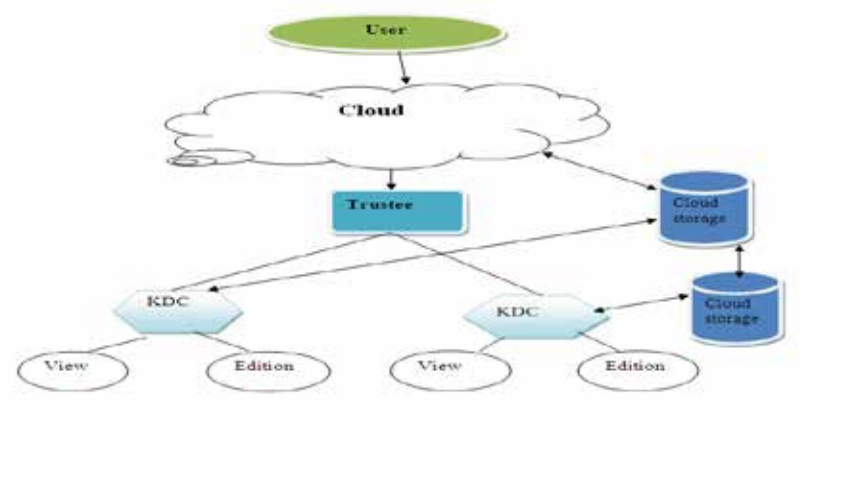


Fig 1: Cloud Storage/Retrieve Process

3.1 Knowledge Storage In Clouds

A user Uu 1st registers itself with one or a lot of trustees. For simplicity we have a tendency to assume there's one trustee. The trustee provides it a token $\gamma = (u; Kbase; K0; \rho)$, wherever ρ is that the signature on u ‖Kbase signed with the trustees personal key T Sig (by (6)).The KDCs area unit given keys PK[i]; SK[i] for encryption/decryption and ASK[i]; APK[i] for signing/verifying. The user on presenting this token obtains attributes and secret keys from one or a lot of KDCs. A key for associate degree attribute x happiness to KDC Ai is calculated as $Kx = K1/(a+bx)$ base , wherever (a; b) € ASK[i]. The user additionally receives secret keys skx,u for encrypting messages. The user then creates associate degree access policy X that could be monotone mathematician operate. The message is then encrypted underneath the access policy as

C = ABE.Encrypt(MSG, X) 1

The user additionally constructs a claim policy Y to change the cloud to demonstrate the user. The creator doesn't send the message seasoning as is, however uses the time stamp ┬ and creates H(C)‖┬. this is often done to forestall replay attacks. If the time stamp isn't sent, then the user will write previous stale message back to the cloud with a legitimate signature, even once its claim policy and attributes are revoked. the initial work by Maji et al. [24] suffers from replay attacks. In their theme, a author will send its message and proper signature even once it now not has access rights. In our theme a author whose rights are revoked cannot produce a replacement signature with new time stamp and, thus, cannot write back stale info. It then signs the message and calculates the message signature as

σ = ABS.Sign(Public key of trustee, Public key of KDCs, token, key, message, access claim) 2

The following info is then sent within the cloud c = (C,┬,σ, Y)

The cloud on receiving the knowledge verifies the access claim victimization the formula ABS.verify**.** The creator checks the worth of V = ABS.Verify(TPK,σ,c,Y)**.** If **V = 0,** then authentication has unsuccessful and also the message is discarded. Else, the message (C,┬) is keep within the cloud.

3.2 Reading from the Cloud

When a user requests knowledge from the cloud, the cloud sends the ciphertext C victimization SSH protocol. Decoding return victimization formula ABE. Decrypt(C,) and also the message seasoning

3.3 Writing to the Cloud

To write to associate degree already existing file, the user should send its message with the claim policy as done throughout file creation. The cloud verifies the claim policy, and provided that the user is authentic, is allowed to write down on the file.

3.4 User Revocation

We have simply mentioned the way to forestall replay attacks. we are going to currently discuss the way to handle user revocation. It ought to be ensured that users should not have the power to access knowledge, even though they possess matching set of attributes. For this reason, the house owners ought to amendment the keep knowledge and send updated info to alternative users. The set of attributes Iu possessed by the revoked user Uu is noted and every one users amendment their keep knowledge that have attributes i € Iu. In [13], revocation concerned ever-changing the general public and secret keys of the smallest set of attributes that area unit needed to decode the information. we have a tendency to don't contemplate this approach as a result of here totally different knowledge area unit encrypted by a similar set of attributes, thus such a smallest set of attributes is totally different for various users. Therefore, this doesn't apply to our model. Once the attributes Iu area unit known, all knowledge that possess the attributes area unit collected. for every such knowledge record, the subsequent steps area unit then carried out:

1. A replacement worth of s, s^{new} € ZZq is chosen.
2. The primary entry of vector v_{new} is modified to new s^{new}.
3. $\lambda x = Rxv_{new}$ is calculated, for every row x akin to leaf attributes in Iu.
4. C1,x is recalculated for x.
5. New worth of C1,x is firmly transmitted to the cloud.
6. New C0 = Me (g,g)s^{new} is calculated and keep within the cloud.
7. New worth of C1,x isn't keep with the information, however is transmitted to users, WHO would like to decode the information. We note here that the new worth of C1,x isn't keep within the cloud however transmitted to the non-revoked users WHO have attribute akin to x. This prevents a revoked user to decode the new worth of C0 and obtain back the message.

3.5 ID-DPDP Protocol

3.5.1 Additive Pairings

Let G1 and G2 be 2 cyclic increasing teams with identical prime order letter of the alphabet. Let e : G1 × G1 → G2 be a additive map [25] that satisfies the subsequent properties:

1) Bilinearity: ∀g1, g2, g3 ∈ G1 and a, b ∈ Z_q,

e(g1, g2g3) = e(g2g3, g1) = e(g2, g1)e(g3, g1)

$e(g1^a, g2^b) = e(g1, g2)^{ab}$

2) Non-degeneracy: ∃g4, g5 ∈ G1 such e(g4, g5) ≠1G2 .

3) Computability: ∀g6, g7 ∈ G1, there's AN economical formula to calculate e(g6, g7).

Such a additive map e is created by the changed Weil [23] or John Orley Allen Tate pairings on elliptic curves. Our IDDPDP theme depends on the hardness of CDH (Computational Diffie-Hellman) downside and also the easiness of DDH (Decisional Diffie-Hellman) downside. they're outlined below.

Definition five (CDH downside on G1): Let g be the generator of G1. Given g, ga, gb ∈ G1 for indiscriminately chosen a, b ∈ Zq, calculate g^{ab}∈ G1.

Definition half-dozen (DDH downside on G1): Let g be the generator of G1. Given (g, g^a, g^b, ˆg) ∈ G4 one for indiscriminately chosen a, b ∈ Z∗q , decide whether or not g^{ab} ?= ˆg.

In the paper, the chosen cluster G1 satisfies that CDH downside is troublesome however DDH downside is simple. The DDH downside is solved by creating use of the additive pairings. Thus, (G1, G2) are outlined as GDH (Gap Diffie-Hellman) teams.

3.5.2 The Concrete ID-DPDP Protocol

This protocol includes four procedures: Setup, Extract, TagGen, and Proof. Its design is pictured in Figure a pair of. The figure is represented as follows:

1. within the section Extract, PKG creates the personal key for the shopper.

2. The shopper creates the block-tag combine and uploads it to combiner. The combiner distributes the block-tag pairs to the various cloud servers in keeping with the storage information.

3. The booster sends the challenge to combiner and also the combiner distributes the challenge question to the corresponding cloud servers in keeping with the storage information.

4. The cloud servers respond the challenge and also the combiner aggregates these responses from the cloud servers. The combiner sends the aggregative response to the booster. Finally, the booster checks whether or not the aggregative response is valid.

The concrete ID-DPDP construction primarily comes from the signature, obvious knowledge possession and distributed computing. The signature relates the client's identity together with his personal key. Distributed computing is employed to store the client's knowledge on multi-cloud servers. At identical time, distributed computing is additionally wont to mix the multi-cloud servers' responses to reply the verifier's challenge. supported the obvious knowledge possession protocol, the ID-DPDP protocol is made by creating use of the signature and distributed computing. while not loss of generality, let the quantity of keep blocks be n. for various block Fi, the corresponding tuple (N_i,CS_{li} , i) is additionally completely different. F_i denotes the i-th block. Denote metal because the name of F_i. F_i is keep in CS_{li} wherever l_i is that the index of the corresponding atomic number 55. (N_i,CS_{li} , i) are wont to generate the tag for the block F_i. The algorithm is represented intimately below.

IV. CONCLUSION

A decentralized access control technique with anonymous authentication, which provides user revocation and prevents replay attacks. The cloud does not know the identity of the user who stores information, but only verifies the user's credentials. Key distribution is done in a decentralized way. Here using two Key approach attribute based encryption and attribute based signature. Attribute based encryption used CP-ABE (Cipher text –

policy attribute based Encryption algorithm) and Attribute based Signature used the MD5. One limitation is that the cloud knows the access policy for each record stored in the cloud. In future, we would like to hide the attributes and access policy of a user. Creating a virtual environment for identify the hacker and compromise him/her (Intrusion detection). Create two Gateway table to access the key information one for large file content another one for small file contents. The future enhancement of this system is using more providers for maintaining large number of data and large number user in cloud and it also acts a best organizer.

REFERENCES

[1] Wang, H.;School of Information Engineering, Dalian Ocean University, Dalian, China "Identity-Based Distributed Provable Data Possession in Multi-Cloud Storage", Mar -2014.pp 328 – 340

[2] S. Ruj, Member, IEEE, M. Stojmenovic, Member, IEEE, and A. Nayak, Senior Member, IEEE"Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds",Feb-2014,pp.384-394

[3] S. Ruj, M. Stojmenovic, and A. Nayak, “Privacy Preserving Access Control with Authentication for Securing Data in Clouds,” Proc. IEEE/ACM Int’l Symp. Cluster, Cloud and Grid Computing, pp. 556-563, 2012.

[4] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, “Toward Secure and Dependable Storage Services in Cloud Computing,” IEEE Trans. Services Computing, vol. 5, no. 2, pp. 220-232, Apr.- June 2012.

[4] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, “Fuzzy Keyword Search Over Encrypted Data in Cloud Computing,” Proc. IEEE INFOCOM, pp. 441-445, 2010.

[5] S. Kamara and K. Lauter, “Cryptographic Cloud Storage,” Proc. 14th Int’l Conf. Financial Cryptography and Data Security, pp. 136- 149, 2010.

[6] H. Li, Y. Dai, L. Tian, and H. Yang, “Identity-Based Authentication for Cloud Computing,” Proc. First Int’l Conf. Cloud Computing (CloudCom), pp. 157-166, 2009.

 ISBN: 978-81-931039-3-7

DESIGN AND MODELING OF GAAS/ INGAP/ INGAAS/ GE III –V TRIPLE-JUNCTION SOLAR CELL

Santosh Kumar Ray[1], Rahul Kumar[2], Tapas Chakrabarti[3]

[1] M.Tech (VLSI) Student, [2] B.Tech Student, [3] Asst. Professor,

Department of Electronics and Communication Engineering, Heritage Institute of Technology, Kolkata, West Bengal,(India)

ABSTRACT

The solar cell efficiency is the most important parameter, in the research area of solar cell. The researchers concentrate their work in multidimensional for better efficiency, better performance. In this work, the Tandem solar cell is considered with III-V compound materials, to improve the efficiency of Tandem solar cell. One Triple-Junction Tandem solar cell with III-V compound material, made of GaAs/InGaP/InGaAs/Ge has been modeled and simulated in Virtual Fabrication Lab of Silvaco TCAD (ATLAS). The newly modeled TJ tandem solar cell made of GaAs/InGaP/InGaAs/Ge gives promising results and has achieved the conversion efficiency of 32.848% and the Fill Factor (FF) of this solar cell is 89.71% under the AM1.5 illumination (1000 suns).

Keywords: Tandem Solar Cell, TCAD, Efficiency (H), Absorption Coefficient(A), Band-Gap Energy(E_g)

I. INTRODUCTION

The proposed triple junction tandem solar cell is made of III-V compound optical semiconductor materials. This type of devices has very high potential of converting solar irradiation to electrical energy. Now a day, solar cells are very useful in every area like solar-powered building to solar power satellite and vehicles [1]. Solar cell is necessary to use for saving the natural sources of energies like coal, petroleum etc. as because the fossil fuels are prime source of conventional energy production. The burning of fossil fuel discharges huge amount of green house gases and carbon dioxide. When photon of appropriate energy strikes this combination of materials an electron by acquiring energy from photon moves from one layer to another and consequently generates electricity. Modern technologies are using this phenomenon for production of solar cells but less efficiency and high cost are major setback for them.

The solar cells receive photons in the form of solar irradiation and convert the light energy in to electrical energy. Depending upon the absorption of light the efficiency will vary. The absorption of photon depends on the band gap suitable of wave length of light. As the solar irradiation is consists of different wave length of radiation, and apart from the visible spectrum, the ultra violet and infrared wave are also there. The visual spectrum of light also consists of different wave length of light. Keeping in mind of different wave length, the different layer of tandem solar cells are developed which can arrest more spectrums and ultimately increases the efficiency of the cell.

In this work, a Triple junction (TJ) tandem solar cell is designed using of III –V compound material [2] GaAs/InGaP/InGaAs/Ge using Silvaco ATLAS. The software ATLAS tool is a virtual fabrication and

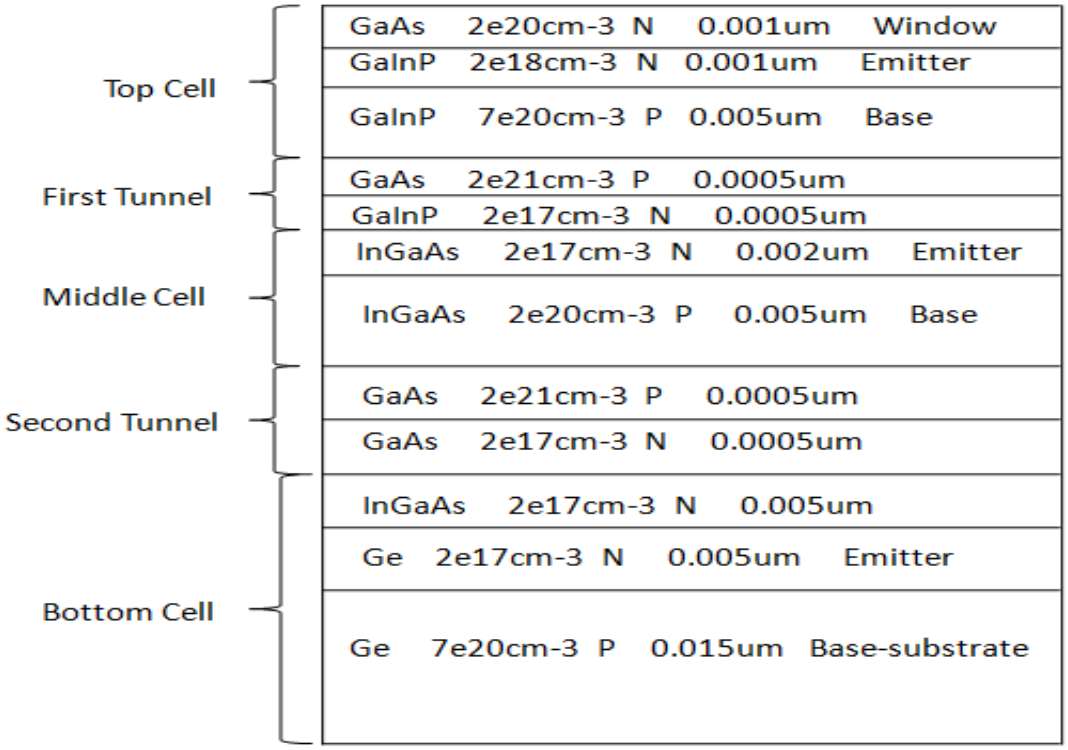
simulation tool, which are considered the different mathematical models and solved them and gives the simulated structural design and the I-V curve of output result. The materials are chosen on the basis of their band gap. The mobility and concentration of doping are the other parameters which causes the output current. After these entire process cell factors are calculated from general equations. The efficiency of the proposed TJ solar cell is 32.848 % presence of AM1.5 illumination (1000 suns) [2].

II. DEVICE STRUCRURE AND MODELS OF TJ CELL

Structure of Triple Junction tandem solar cell designed on the basis of materials' band gap. Schematic diagram of TJ solar cell structure shown below in figure1 and also net doping profile is given in figure 3.

2.1 Cell Simulation

Three individual cells shown in figure-1 that is top cell, middle cell and bottom cell. Top cell made by three layers the first layer is n-type GaAs (0.001 um), second layer is n-type GaInP (0.001 um), and the third layer is made by p-type GaInP (0.005 um). Top cell materials have largest band gap. The middle cell materials have a lower band gap than top cell. It made by two layers of GaAs. InGaAs (0.002 um) and another p-type InGaAs (0.005 um) are used. The bottom cell has least band gap compare of top cell and middle cell. The bottom cell made by three layers. The first layer is n-type acceptors InGaAs (0.005 um), second layer may by n-type Ge (0.005 um) and the third layer is p-type Ge (0.015 um).



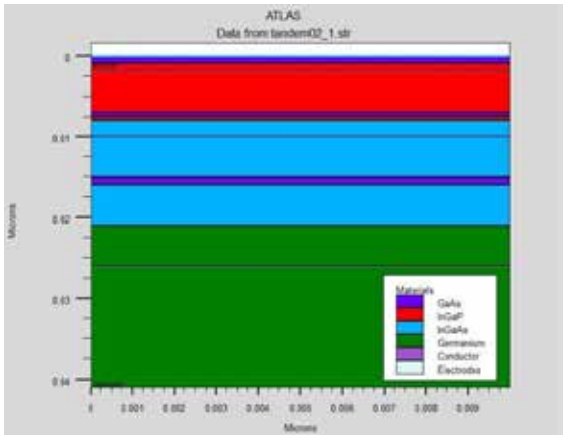


Figure-2. Schematic Diagram of Triple Junction Solar Cell

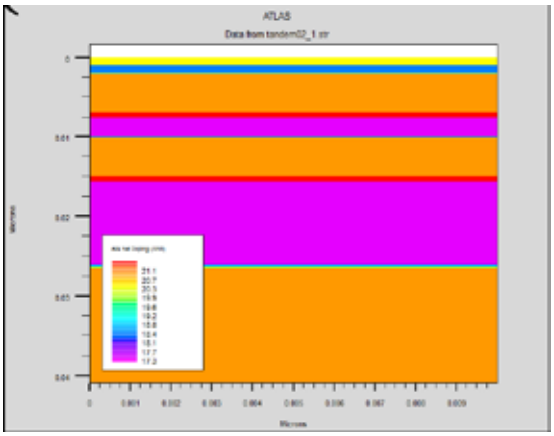


Figure-3. Net Doping Profile of Triple Junction Solar Cell

2.2 Tunnel Junction Simulation

Tunnel junction is a very important layer, essential in vertical stacking of more than one cell, in order to construct a multi-junction configuration. It should be optically transparent and connect the component cells in the multijunction structure with the minimum of electrical resistance [3]. Dissimilar layers regions of Triple Junction solar cell reducing the current flow for this cause using tunnel junction because tunnel junction reduce this type of factors from the junction. In this Triple junction solar cell have two tunnel junctions. First tunnel junction made of two layers one is p-type donors GaAs (0.0005 um) and other is n-type GaInP (0.0005 um) and Second tunnel made of two layers of GaAs of thickness of 0.0005um.

Simulation of this structure is done through ATLAS (SILVACO). ATLAS virtually generates a photocurrent in the device which is generated by a beam of user defined wavelength. We have used wavelength of 300nm for this study. ATLAS then mathematically solves the structure to get the cathode current using different user defined mathematical models. In this study, we have used the models namely, SRH, CONMOB, OPTR, AUGER, BGN [3].

2.3 Srh Recombination

It specifies Shockley Red Hall recombination using fixed lifetimes.

$$R_{SRH} = \frac{Pn - nie\text{^}2}{TAUPo[P + nie\ \exp\left(\frac{ETRAP}{kTL}\right)] + TAUNo[P + nie\ \exp\left(\frac{-ETRAP}{kTL}\right)]}$$

where, ETRAP is the difference between trap energy and intrinsic Fermi level, TL: is the lattice temperature in Kelvin, TAUN0 and TAUP0 are electron and hole lifetimes, p and n are hole and electron densities and nie is intrinsic carrier density[4].This model is activated by using the SRH parameter of the MODELS statement. The electron and hole lifetime parameters, TAUN0 and TAUP0, are user-definable in the MATERIAL statement.

2.4 Auger Recombination

Auger recombination technique, is given by the equation

$$U\text{auger} = \Gamma n\ (\text{np} - ni\text{^}2) + \Gamma p\ (\ \text{p} - ni\text{^}2\ )$$

here again, n and p are hole and electron densities and ni is the intrinsic carrier density [5].

2.5 Optical Recombination (Optr)

The optical recombination model which can be stated as

$$R\text{auger}=\text{AUGN (pn^2 - } nnie\text{^2) + AUGP (}np\text{^2 } - nie\text{^2)}$$

Where, p, n, nie are as described earlier. AUGN and AUGP are user definable whose default values are 8.3e-32 cm6/s and 1.8e-31 cm6/s respectively. Here, neither Klaassens temperature dependent model nor the narrow bandgap model is incorporated, as the BGN model is used [6].

2.6 Band Gap Narrowing (BGN)

Specifies band gap narrowing models which is expressed as an analytical model relating to variation in bandgap to doping concentration given by

$$\Delta E_g = BGN.N\{ln\frac{N}{BGN.N} + \left[\left(ln\frac{N}{BGN.N}\right)^2 + BGN.C\right]^{\frac{1}{2}}\}$$

We can specify BGN.E, BGN.N, BGN.C parameters according to Klaassens model. The default values for BGN.E, BGN.N, and BGN.C are 9.0e-3 V, 1.3e7 cm-3 and 0.5 respectively. Variation of bandgap models are not introduced here as our material band-gap is not variable [7].

2.7 Concentration Dependent Mobility (Conmob)

Specifies that a concentration dependent mobility model be used for silicon and gallium arsenide. This model is a doping versus mobility table valid for 300K only. This model is used to solve the top layer and substrate.

In addition to all these equations, Fermi level and models for fixed Fermi are solved for the final current calculation. The simulator solves basic Poisson equation and continuity equation for holes and electrons separately which fall under the drift diffusion model. All important generation and recombination mechanisms are taken into account. The spontaneous recombination and optical absorption can be calculated with quantum mechanics using Fermi's golden rule, which may be important for novel solar cells using quantum well and quantum dot materials. For optical simulation relating to electron and hole generation due to incident light, simulator takes into account Fresnel's reflection, refraction and transmission. The optical and electrical properties of the materials are taken from the sopra database [8].

III. RESULTS AND DISCUSSIONS

The triple junction solar cell shown in figure-2 all cell are modeling and simulate the program very well from that graph is plotted on the basis of Open-circuit voltage (V_{oc}), Short circuit current density (J_{sc}), Maximum power (P_m), maximum voltage (V_m) and the Current (I_m) using all these formulae calculated Fill Factor (FF) and Efficiency all these values shows in Table-1.On these basis plotted the graph of Cathode current vs. Anode voltage shows in figure-3

Table -1

Jsc	1.387e-10 Amp/m^2
Voc	1.20021 Volt
Pm	1.494e-10 Watt/m^2
Vm	1.1 Volt
Jmin	-7.212e-10 Amp/m^2
FF	89.71%
Eff	32.848%

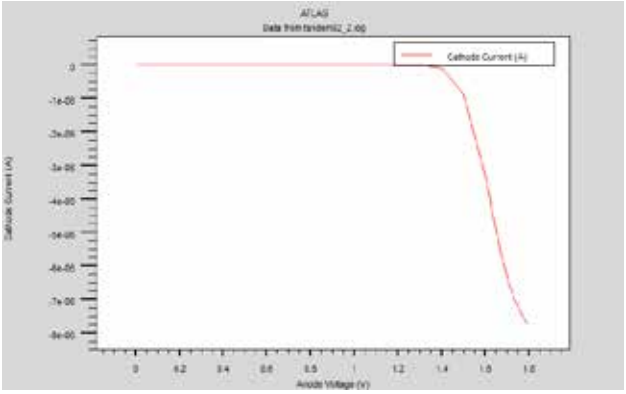


Figure-4. The graph of Cathode Current vs. Anode Voltage

IV. CONCLUSION

In this work we have designed and modeled triple junction solar cell with the III-V compound semiconductor material (**GaAs/InGaP/InGaAs/Ge**). This work has been done in Silvaco ATLAS. This Triple junction solar cell has achieved an efficiency of 32.84% and the fill factor of 89.71%. Short-circuit current (Isc) 0.01388mA and the open-circuit voltage (Voc) 1.20021v have been observed .This paper is completely done by computer aided design Silvaco ATLAS tools. More exploration is required in selecting of materials and the modeled solar cell is to be fabricated in physical lab and the efficiency of that physical lab should match with the simulated one as the virtual environment considered all the physical parameters, then only the validation of this cell will over.

REFERENCE

[1]. "Monolithic crystalline multijunction solar cell development and analysis at the US Air Force research laboratory" by C.S. Mayberry, K.C. Reinhardt and T.L. Kreifels, Renewable Energy 28 (2003) 1729–1740

[2]. "Silvaco ATLAS User's Manual ", 2010. http://www.silvaco.com

[3]. "A Simulation Study of Experimental GaInP/InGaAs/GeTriple-Junction Solar Cell" byVeljko Nikolić, Nebojša Janković, - Proceedings of Small Systems Simulation Symposim 2012, Niš, Serbia, 12th-14th February 2012

[4]. "Statistics of the Recombinations of Holes and Electrons" by W. Shockley and W. T. Read, JrPhys. Rev. 87, 835 – Published 1 September 1952© 1952 The American Physical Society.

[5]. http://www.nextnano.com/nextnano3/tutorial/1Dtutorial_AlGaInP_onGaAs.htm

[6]. "Carrier Generation and Recombination in P-N Junctions and P-N Junction Characteristics" by Chih-Tang Sah; Shockley Semiconductor Lab., Mountain View, Calif. Noyce, R.N.; Shockley, WProceedings of the IRE (Volume: 45, Issue: 9) Sept. 1957 IEEE Journals and Magazines

[7]. "Band-gap narrowing in novel III-V semiconductors" by S. C. Jain, J. M. McGregor and D. J. Roulston68, 3747 (1990) © 1990 American Institute of Physics

[8]. "Modelling of high efficiency AlGaInP based PIN Solar cells with comparative analysis" by Tapas Chakrabarti and Rudrarup Sengupta, Published December 17-19, 2014, ICAMET 2014

CATEGORIZING THE RISK LEVEL OF AUTISTIC CHILDREN USING DATA MINING TECHNIQUES

Mohana E[1], Poonkuzhali.S[2]

[1]PG Scholar, [2]Professor, Department of Information Technology

Rajalakshmi Engineering College, chennai (India)

ABSTRACT

Autism spectrum disorders (ASD) are enclosure of several complex neurodevelopmental disorders characterized by impairments in communication skills and social skills with repetitive behaviors. It is widely recognized for many decades, yet there are no definitive or universally accepted diagnostic criteria. Studies indicate early intervention services, for young children with ASD significantly improve the children's prognosis and should begin as early as 18 months of age. The Modified Checklist for Autism in toddlers, better known as the M-CHAT, is a free screening tool that can be administered to children between 16 and 30 months-of-age. Hence by using the M-CHAT, this paper focuses on finding the best classifier with reduced features for predicting the risk level of autism. The four feature selection algorithms such as Fisher filtering, ReliefF, Runs filtering and Stepdisc are used to filter relevant feature from the dataset, and then several classification algorithms are applied on this reduced features. Finally performance evaluation is done on all the classifier results.

Keywords: Accuracy, Autism Spectrum Disorder, Classification, M-CHAT Screening Tool, Feature Selection

I. INTRODUCTION

Autism is a neurodevelopmental disorder. The autistic children are characterized by lack of social interaction, communication and behavior. ASD is a spectrum disorder as its impact on every child varies. ASDs affect one out of every 68 children in the U.S. They occur more often among boys than girls. The causes of autism has different source. It cannot be confined to a particular factor. For example it may be due to medical reason or genetically induced. It has a unique feature and severity in each child. It varies from level to level. The children with autism are attached to things; possess repetitive behavior like arranging things in a row. Even though they lack these factors, some children master in a particular area. The children may seem to appear normally, but still they might have some risk level of autism which is very difficult to predict at the early stage of autism. M-CHAT is the Modified Checklist for Autism in Toddlers. It is a screening tool for diagnosing autism in age between 16 to 30 months. In case of timely diagnosis of autism, the early intervention program can be started. Data mining is the process of analyzing through large amounts of data for useful information. It uses artificial intelligence techniques, neural networks, and advanced statistical tools (such as cluster analysis) to reveal trends, patterns, and relationships, which might otherwise have remained undetected. It is the step of the knowledge discovery in databases (KDD) process concerned with the algorithmic means by which patterns or structures are enumerated from the data. Predicting the outcome of a disease is one of the most interesting and challenging tasks where to develop data mining applications. The use of computers with automated tools, large volumes of medical data are being collected and made available to the medical research groups. As a result data

mining techniques has become a popular research tool for medical researchers to identify and exploit patterns and relationships among large number of variables, and made them able to predict the outcome of a disease using the historical datasets [13].Feature selection algorithm used to find the subset of input variables by eliminating the features with less or no predicting information. It significantly improves the accuracy of the future classifier models formed by different classification algorithms.

And then several classification algorithms such as BVM, C4.5, C-RT, CS-MC4, CS-CRT, C-SVC, CVM, ID3, K-NN, Rnd Tree etc., is applied on the reduced datasets produced by feature selection algorithms. Finally performance evaluation is done to find a best classifier. So that with minimum attributes toddler children's autism level can be found.

II. RELATED WORK

JyotiSoni et.al [1] compared predictive data miningtechniques such as Decision tree, Naïve Bayes, K-NN, and classification based on clustering for analyzing the heart disease dataset. The classified data is evaluated using 10 fold cross validation and the results are compared. Decision Tree outperforms and sometime Bayesian classification is having similar accuracy as of decision tree but other predictivemethods like KNN, Neural Networks, Classification based on clustering are not performing well. The second conclusion is that the accuracy of the Decision Tree and Bayesian Classification further improves after applying genetic algorithm to reduce the actual data size to get the optimal subset of attribute sufficient for heart disease prediction.

Carloz Ordonez et al., [4] applied association rule mining on heart disease data. Search constraints and test data validation reduces the number of association rules with high predictive accuracy.In the survey of [5] the author proposed the minimal subset of attributes for predicting heart disease. In future this work can be expanded and enhanced for the automation of heart disease prediction. Real data should be collected from health care organizations and agencies are taken to compare the optimum accuracy with all data mining technique.

G. Parthiban et al., [6] applied Naïve Bayes classification through WEKA ("Waikato Environment for Knowledge Analysis") tool to diagnose heart disease of diabetic patient. 10 folds cross validation is used to avoid any bias in the process and improve efficiency of the process.AbdelghaniBellaachi et al., [7] analysed breast cancer data with three data mining techniques such as Naïve Bayes, Back-Propagated Neural Network and C4.5. In that, C4.5 produces more accuracy of about 86.7%.

GeethaRamani et al., [8], applied feature relevance algorithm and then different classification algorithm on the selected features. Error rate and accuracy of the different classification tool is calculated using Tanagra. In that, Rnd tree produced 100% accuracy.

S. Poonkuzhali et al., [10], taken TP53 germline database for classification. First feature construction done by converting all input to disc to cont function. Then different filtering algorithm is applied to reduce the number of features. Different classification algorithm produced on the reduced dataset. Finally performance evaluation is done. Rnd tree produces 100% accuracy using ReliefF filtering.

Christina Schweikert et al., [14], applied Combinatorial Fusion Analysis(CFA) and Association Rule Mining(ARM) to autism, lead, and mercury data. CFA revealed that autism prevalence has strong correlation with rank combination of mercury and lead than individual. ARM discovered a trend where increase in mercury strongly related to increase in autism prevalence.

Gondy Leroy et al.,[15], autism children are videotaped before, during and after therapy applied to them. Four conditions are taken to monitor child’s inappropriate and appropriate behaviour like when alone, accompanied

with parent, stranger and therapist. Decision tree and rule mining algorithm are applied on the above noted data to find out their level of behaviour.

M.S. Mythili et al., [16], taken autism children's learning skills dataset and the decision tree classifier (J48), Normalized PolyKernel based classifier (SVM) were enforced in weka tool. Visual image of decision trees are formed and accuracy of both the algorithms are calculated. In that SVM having high accuracy(95%) , correctly classified the dataset.

M.S. Mythili et al., [17], analysed the dataset of autism containing three attributes such as language, social and behaviour. Values of these attributes are represented with three discrete values like mild, moderate and heavy and the level of autism is detected from these attributes. Neural Network, Support Vector Machine and Fuzzy logic algorithms are used to produce classification model.

III. ARCHITECTURAL DESIGN

The architectural design of the proposed system is given in Fig 1 and each block is explained in the following sections.

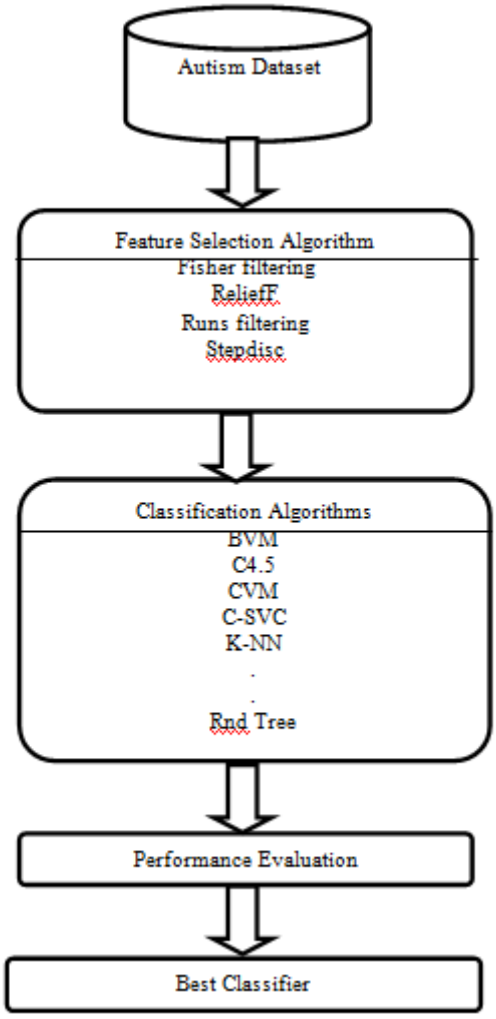


Fig. 1 Artichitecture Design of the Proposed System

3.1Autism Dataset

The Autism Dataset is formed with M-CHAT-R tool (Modified Checklist for Autism in Toddlers Revised tool) which is valid only for children in the age of 16 to 30 months. This tool contains 20 Yes/No questions, and

produce risk number of the child as output. The autism dataset contains 20input attributes which represent yes/no answers for 20 questions in a tool, one class attributewhich denotes the corresponding risk value which range from 0 to 20 and 438 instances. The description of the attributes of this autism dataset is given in Table I.

Table. I Attribute of Autism Dataset

Attribute No.	Attribute Description (Questions)
1	If you point at something across the room, does your child look at it?
2	Have you ever wondered if your child might be deaf?
3	Does your child play pretend or make-believe?
4	Does your child like climbing on things
5	Does your child make unusual finger movements near his or her eyes?
6	Does your child point with one finger to ask for something or to get help?
7	Does your child point with one finger to show you something interesting?
8	Is your child interested in other children?
9	Does your child show you things by bringing them to you or holding them up for you to see – not to get help, but just to share?
10	Does your child respond when you call his or her name?
11	When you smile at your child, does he or she smile back at you?
12	Does your child get upset by everyday noises?
13	Does your child walk?
14	Does your child look you in the eye when you are talking to him or her, playing with him or her, or dressing him or her?
15	Does your child try to copy what you do?
16	If you turn your head to look at something, does your child look around to see what you are looking at?
17	Does your child try to get you to watch him or her?
18	Does your child understand when you tell him or her to do something?
19	If something new happens, does your child look at your face to see how you feel about it?
20	Does your child like movement activities?
21	Risk level of child

3.2 Feature Selection Algorithm

The autism dataset contains 21 attributes of which 20 input attributes are discrete and the target attribute risk is continous attribute (0-20) . In order to apply filtering algorithm, target attribute has to be transformed into discrete attribute.Then the filtering algorithms such as Fisher Filtering, ReliefF, Runs Filtering and Stepwise Discriminant Analysis are applied to the feature constructed dataset and the results are given in Table II.

Table. II Feature Selection

S.No	Feature selection algorithm	No. of attributes Before Filtering	No. of attributes After Filtering	Attribute No. After Filtering
1	Fisher Filtering	20	20	All attributes
2	ReliefF	20	9	17,16,18,10,15,9,8, 14,11
3	Runs Filtering	20	13	3,5,7,9,11,12,14,15,16, 17,18,19,20
4	Stepdisc	20	20	All attributes

3.3 Classification Algorithm

Classification algorithms such as BVM, C4.5, C-RT, CS-CRT, CS-MC4, C-SVC, CVM, ID3, K-NN, Linear Discriminant Analysis, Multilayer perceptron, Naïve bayes continuous, Multinomial Logistic Regression, PLS-DA, PLS-LDA and Rnd Tree are applied to each of the above filtering algorithms and the results are given in Table III.

IV. EXPERIMENTAL RESULTS AND PERFORMANCE EVALUATION

Different classification algorithms are compared in terms of error rate, accuracy, recall and precision. Each are discussed below.

4.1. Error rate

Error rate of a classifier was defined as the percentage of the dataset incorrectly classified by the method. It is theprobability of misclassification of a classifier. Error rate of different classifier before filtering and after filtering is represented in table III.

$$\textit{Error rate} = \frac{\textit{No.of incorrectly classified samples}}{\textit{Total no of Sample in the class}}$$

Table. III Error Rate of Different Classifiers

Classification Algorithm	Error Rate Before Filtering	Error rate after filtering	
		ReliefF	Runs Filtering
BVM	**0.0160**	**0.1073**	**0.0479**
C4.5	**0.0160**	**0.1187**	**0.0685**
C-RT	0.1073	0.1370	0.1187
CS-CRT	0.1073	0.1370	0.1187
CS-MC4	0.1073	0.1256	0.0868
C-SVC	**0.0183**	**0.1096**	**0.0502**
CVM	**0.0114**	**0.1073**	**0.0479**
ID3	0.2237	0.2237	0.2237
K-NN	**0.0731**	**0.1370**	**0.0685**
LDA	**0.0388**	**0.1142**	**0.0639**
MP	0.0548	0.1096	0.0548

MLR	**0.9795**	**0.1164**	**0.0479**
NBC	0.0457	0.1256	0.0982
PLS-DA	0.0662	0.1233	0.1119
PLS-LDA	0.0502	0.1233	0.0776
Rnd- tree	**0.0639**	**0.1073**	**0.0502**

4.2 Accuracy

Accuracy of a classifier was defined as the percentage of the dataset correctly classified by the method. The accuracy of all the classifiers used for classifying this autism dataset are represented in Table IV.

$$Accuracy = \frac{No\ of\ correctly\ Classified\ Samples}{Total\ no\ of\ Sample\ in\ the\ class}$$

Table. IV Accuracy of Classifiers

Classification Algorithm	Accuracy(%)
BVM	**95.2**
C4.5	93.2
C-SVC	94.97
CVM	**95.2**
K-NN	93.2
LDA	93.6
Rnd Tree	94.97
MLR	**95.2**

4.3 Recall

Recall of the classifier was defined as the percentage of errors correctly predicted out of all the errors that actually occurred. The recall of the best classifiers for three levels of autism is represented in Table V and graphically represented in fig. 2.

$$Recall = \frac{True\ Positive}{True\ positive + False\ Negative}$$

4.4 Precision

Precision of the classifier was defined as the percentage of the actual errors among all the encounters that were classified as errors. Precision of BVM, CVM and MLR classifiers for three levels of autism is represented in Table V.

$$Precision = \frac{True\ Positive}{True\ positive + False\ Positive}$$

The terms positive and negative refer to the classifier's prediction, and the terms true and false refer to classifier's expectation.

Table. V Precision and Recall of Classifiers

Classification algorithm	Class	Precision	Recall
BVM	Low	0.5714	0.0769
	Medium	0.9812	0.0457
	High	0.9388	0.0515
CVM	Low	0.5714	0.0769
	Medium	0.9812	0.0457
	High	0.9388	0.0515
MLR	Low	0.5714	0.0769
	Medium	0.9781	0.0429
	High	0.9490	0.0606

Recall for three classifiers BVM, CVM and MLR having high accuracy (95.21%) is represented in fig. 2.

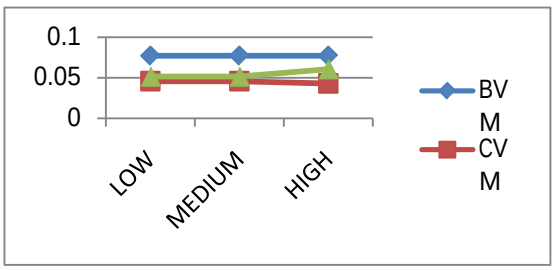


Fig.2 Recall of BVM,CVM and MLR Classifiers

V. CONCLUSION

In this paper, autism affected children of age 16-30 months dataset is taken. The dataset is pre-processed and taken for feature selection. Feature Selection Algorithm such as Fisher Filtering, ReliefF, Runs Filtering and Stepdisc is applied. In that Fisher Filtering and Stepdisc does not filter any features. So Runs filtering and ReliefF is chosen. Then different classification algorithm is applied on the subset produced by both feature selection algorithm. Finally, performance evaluation is done on the results such as error rate, recall and accuracy. This paper helps in finding the best classifier for autism dataset through feature relevance analysis and classification algorithm. Among different classification algorithm applied , algorithms such as BVM, CVM AND MLR produced high accuracy of 95.21% using Runs Filtering and it also accurately classified the test dataset.

VI. ACKNOWLEDGEMENT

This research work is the part of the funded project titled Interactive Teaching Aid for Autistic Children (ITAAC),D.O. No.: SEED/TIDE/034/2013 under TIDE programme of SEED division from Department of Science & Technology, Ministry of Science and Technology, New Delhi.

REFERENCES

[1]. Han, J., Kamber, M.: "Data Mining Concepts and Techniques", Morgan Kaufmann Publishers, 2006.

[2] "Data mining: Introductory and Advanced Topics" Margaret H. Dunham

[3]. JyotiSoni, Ujma Ansari, Dipesh Sharma, SunitaSoni "Predictive Data Mining for Medical Diagnosis: An Overview of Heart Disease Prediction" IJCSE Vol. 3 No. 6 June 2011.

[4]. Carloz Ordonez, "Association Rule Discovery with Train and Test approach for heart disease prediction", IEEE Transactions on Information Technology in Biomedicine, Volume 10, No. 2, April 2006.pp 334-343.

[5] M. ANBARASI, E. ANUPRIYA, N.CH.S.N.IYENGAR, "Enhanced Prediction of Heart Disease with Feature Subset Selection using Genetic Algorithm", International Journal of Engineering Science and Technology Vol. 2(10), 2010, 5370- 5376.

[6] G. Parthiban, A. Rajesh, S.K.Srivatsa "Diagnosis of Heart Disease for Diabetic Patients using Naive Bayes Method" .

[7] BellaachiaAbdelghani and ErhanGuven, "Predicting Breast Cancer Survivability using Data Mining Techniques,"Ninth Workshop on Mining Scientific and Engineering Datasets in conjunction with the Sixth SIAM International Conference on Data Mining," 2006.

[8] R. GeethaRamani, G. Sivagami, Parkinson Disease Classification using Data Mining Algorithms, International Journal of Computer Applications (0975 – 8887) Volume 32– No.9, October 2011.

[9]ShomonaGracia Jacob, R.GeethaRamani, Discovery of Knowledge Patterns in Clinical Data through Data Mining Algorithms: Multiclass Categorization of Breast Tissue Data, International Journal of Computer Applications (0975 – 8887) Volume 32– No.7, October 2011.

[10] S. Poonkuzhali, R. GeethaRamani, R. Kishore Kumar,Efficient Classifier for TP53 Mutants using Feature Relevance Analysis, in International Multiconference of Engineers and computer scienctists, Vol 1, 2012.

[11] Tanagra-Data Mining tutorials http://data-mining- tutorials.blogspot.com

[12] Arun K Pujari, Data Mining Techniques, University Press 2001

[13] ShwetaKharya, "International Journal of Computer Science, Engineering and Information Technology (IJCSEIT)", Vol.2, No.2, April 2012.

[14] Christina Schweikert, Yanjun Li, David Dayya, David Yens, Martin Torrents, D. Frank Hsu," Analysis of Autism Prevalence and Neurotoxins Using Combinatorial Fusion and Association Rule Mining", in Ninth IEEE International Conference on Bioinformatics and Bioengineering, 2009.

[15] Gondy Leroy, Annika Irmscher, Marjorie H. Charlop-Christy,"Data Mining Techniques to Study Therapy Success with Autistic Children".

[16] M.S. Mythili, A.R.MohamedShanavas," A Novel Approach to Predict the Learning Skills of Autistic Children using SVM and Decision Tree", in (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (6) , 2014.

[17] M.S.Mythili, A. R. Mohamed Shanavas," A Study on Autism Spectrum Disorders using Classification Techniques", in International Journal of Soft Computing and Engineering (IJSCE) ISSN:2231-2307,Volume-4Issue-5,November2014.

 ISBN: 978-81-931039-3-7

ELECTRONIC HUMAN RESOURCE MANAGEMENT: AN OVERVIEW

Shoeb Ahmad

Associate Professor, Dept. of MIS, College of Business Administration,
University of Ha'il, Saudi Arabia

ABSTRACT

Electronic HRM is the new technological tool which is gaining widespread importance within business organizations around the world. It proves to be beneficial for business in many aspects among which, the major ones are to make organizations go paperless, be more proficient and competent, and become more adaptable to the contemporary needs. Internet technology, especially the World Wide Web, in the last two decades has helped transform many HR processes and practices such as, recruitment, selection, performance management, compensation and many more in a positive way. In facilitating these HR services, e-HR plays a significant role at all levels - basic, intermediate and top . The paper- highlights the importance of e-HRM in business organizations. It also provides with a brief overview the aims and scope of e-HRM in these organizations .The paper finally concludes with some basic suggestions.

Keywords: ***E-HRM, HR Process, Human Resources, Internet, Organizations***

I. INTRODUCTION

Computerized technology (Digital, ICT, IT, Automation and many more) along with other technological advances has reshaped the world perhaps positively in a significant way. Everything including our way of thinking, living, communicating and working has changed drastically. On a major landscape, our culture, economies, demographics and even society has been affected by these technological changes.

Modern scientific inventions and fast changing technologies have changed the face of the universe. Distances between the countries have been reduced and a new era of co-operation and international business has dawned. No nation now can live in isolation unmindful of the state of affairs in other countries of the world. Changing business scenario has cast its spell on all aspects of life and industrial relations have to be judged in the new perspectives. Human resources have to be utilized and nourished in an entirely new grammar of administration and technology. These technological paradigm shifts in business has brought about a colossal change in delivering HR functions, organizational environment, managerial initiatives and employee management in the form of what we call the term, 'e-HRM'.

Today e- HRM has become a tool that facilitates fast, accurate and paperless dispensation of various HRM processes namely: Payroll; Time & Attendance; Benefits Administration; HR Management Information System; Recruiting; Training; Employee Self-Service and many more. Further it empowers both the management and the employee within organization, as they can access the typical HR functions through intranet or other communication networks related to computer technology ."The empowerment of managers and employees to perform certain chosen HR functions relieves the HR department of these tasks, allowing HR staff to focus less

on the operational and more on the strategic elements of HR, and allowing organizations to lower HR department staffing levels as the administrative burden is lightened"[1] .

II. OBJECTIVE OF THE STUDY

The paper aims to:

- present a brief overview on the different aspects of e-HRM in a simplified manner that may help the reader to gain a basic understanding of the topic and,
- add to the extant literature related to the area of e-HRM research and development.

III. LITERATURE REVIEW

We all know that human resource is all about managing people, the most vital of all the resources in an organization. It is the total skill, knowledge, talent, creative ability and aptitude of people in a workplace along with the approaches, beliefs, values and aptitude of the individuals in an organization. This definition of human resource is quite wide spread but in the present scenario this definition needs a revision because now internet technology has been associated profoundly with HRM. The term e-HRM came into existence in early 1990s at the time when e-commerce was spreading its wings within the business arena. Complementing the trend was recent technological developments, which realized the concept of paperless office and business at finger touch .In fact e-HRM has transformed the traditional business into a more realistic, informative and interactive business.

Researchers in the area of e-HRM became active somewhat late and, to an extent, have not yet reached their desired aim to catch up with practice. Hence, we can say that research on e-HRM is still in its nascent stage with researchers still looking out for relevant and adequate theory with empirical evidences that can fully comprehend the concept of e-HRM.

We define the term e-HRM as implementation of HRM practices in organizations together with use of internet or web based technology .Similarly the term e-HR is used to describe technology's role in enabling the transformation of HR activity. It describes the impact of internet on how HR management is practiced or raises HR issues prompted by employees' use on the internet in an organization. E-HRM can be used for transactional activities (i.e. those that involve day-to-day transactions and record keeping); traditional HRM activities such as recruitment, selection, training, compensation and performance management; and transformational activities that add value to the organization [2].It is the (planning, implementation and) application of information technology for both networking and supporting at least two individual or collective actors in their shared performing of HR activities[3].

Electronic Human Resource Management System (e-HRM System) is a web-based solution that takes advantage of the latest web application technology to deliver an online real-time human resource management solution [4]. Previous literature suggests that e-HRM can augment the effectiveness of HR activities, improve, HR service delivery and transform the role of the HR function into one that is more strategic [5].e-HRM is the complete integration of all HR systems and processes based on common HR data and information and on interdependent tools and processes, properly developed e-HRM could provide the data gathering tools, analysis capabilities and decision support resources for HR professionals to hire, pay, promote, terminate ,assign, develop, appraise and reward employee[6].

IV. E-HRM IMPLICATIONS

Computer technology has streamlined our way of living, working, communicating and even the way of conducting business .The emergence of Information technology in business world has significantly changed the way how HR departments handle their record keeping and information sharing process.

Today, more HR functions are becoming available electronically or done over the internet. Everyday organizational tasks such as approving pay rises, sorting out training and checking holiday entitlements, which were earlier performed by skilled professionals are now being handled by the computers. Moreover, in addition to performing the traditional tasks of accounting and pay roll calculations, computers are now being engaged to maintain easily accessible employee data that are valuable for job placement and labor utilization, to track and report affirmative action activity, employee training, compensation management etc.

A large number of HR managers are now using internet to recruit personnel, conduct research using electronic data bases, send e-mails and also engage in valuable networking and discussions on line. Adoption of e-HR seeks to minimize or eliminate intervention from HR staff, change the way many HR managers operate and allows managers and employees to perform HR tasks directly with the self service tools. E-HRM improves the strategic orientation of HRM, helps in Cost reduction/efficiency gains, improve the Client service and facilitating management and employee [7].

The main objective of e-HRM is to facilitate the monitoring of human resources demand and supply imbalances within an organization. This system eventually automates employees' related information and leads to faster response to employees' related services and HR related decisions. E-HRM also offers the potential to improve efficiency and cost effectiveness within the HR department, and allow HR to become a strategic partner. Above all, it provides data security and personal privacy to the users which are the most in demand concept in today's world. e-HRM provides an opportunity to improve HR services within both employees and management perspective as well as facilitates efficiency and cost effectiveness within HR department.

V. TYPES OF E-HRM

e-HRM is a fully integrated, organization-wide electronic network of HRM related data, information, services, databases, tools, applications, and transactions that are generally accessible at any time by the employees, managers, and HRM professionals [8]. Wright and Dyer [9] specify three areas of HRM where organizations can choose to 'offer' HR services face-to-face or through an electronic means: transactional HRM, traditional HRM, and transformational HRM. Lepak and Snell [10] also made a distinction regarding e-HRM, namely, operational HRM, relational HRM and transformational HRM.

5.1 Operational E-HRM

Operational E-HRM is deals with the basic administrative activities of the HR department such as payroll, Personnel data management, departmental record maintenance besides others. According to Snell et al. [11], about 75-75 percent of the workload is related to this type of activities.

5.2 Relational E-HRM

Relational e-HRM, emphasizes upon HR activities that support a mutual relationshipbetween HR department and other departments both inside or outside the organization. The major activities concerned with this type of e-HRM are e-recruitment, e- learning, E-performance management and so on. Strohmeier [12], considers relational e-HRM as a means of interaction and networking among different players associated with an organization. About 15-30 percent of HR workload is related to this type of activities [13].

5.3 Transformational E-HRM

Transformational e-HRM is the most complex type concerned with the strategic activities of HRM, such organizational change processes, strategic re-orientation, strategic competence management, and strategic knowledge management. "Finally, in terms of transformational HRM, it is possible to create a change-ready workforce through an integrated set of web-based tools that enables the workforce to develop in line with the company's strategic choices or to have paper-based materials[14].

It totally depends upon an organization to practice E-HRM policies from any number of these three types to achieve their HR goals.

VI. FUTURE DIRECTIONS FOR SOME E-HRM FUNCTIONS

An increase in quality and pace of HR tasks is achieved due to e-HR. The traditional administrative processes were quite slow and inefficient, but now with the help of e-HR not only manpower saving is attained but, processing time can also be reduced drastically. E-HR also reduces the workload of HR department as the employee could log in online anywhere and anytime without being in the office and without the leave card. The important Hrm functions that has benefited due to e-HR are discussed below.

6.1 Recruitment and Selection

E-recruiting is the hottest area of all HR field and includes posting of open positions on the worldwide web home page and various other career services. In the HR arena websites such as Career Mosaic, Higher Ed., Monster, Naukri.com offer employer profiles, job openings career information and human resource forums. With e-recruitment the company gets an additional possibility besides the normal application by paper to recruit people over the web in an online-application process. With appliance of ICT in recruitment process, organizations can post their job vacancies online, can attract the best from the world wide talent pool investing less time, effort and ,cost.

e-HR performs multiple functions which are similar to the functions of resource management. Functions such as matching CVs to person's specifications for short listing purposes and linking with internet recruiting processes are performed by e-HR. Procedures like letter writing, acknowledgements, invitations to interview, offers and rejections, management reports, analysis of response by media and monitoring recruitment costs, and evaluating applicants, employees and analyzing and designing jobs become systematized and convenient and helps in selecting, placing, promoting, terminating and transferring employees.

6.2 Payroll and Performance Appraisal

E-HR technology is used for forecasting future payroll costs on the basis of assumptions about members, promotions and pay levels and administering pay reviews, producing review forms, analyzing proposals against the budgets and calculating the cost of performance related pay awards in accordance with different assumptions

about amounts and the distribution of awards within a budget. The technology can also be used for generating forms, analyzing and reporting on the results of performance reviews showing the distribution of people with different degrees of performance at different levels, highlighting individuals with particular skills or special characteristics, writing role definitions, and generating employees opinion surveys online.

6.3 Training and Development

In the sphere of training and development, e-HR technology can be utilized for training and developing employees, storing e-learning modules on the database which enables trainers to select an appropriate module or mix of modules to meet a specified learning need, analyzing the training recommendations contained in performance review reports to identify collective and individual training needs, and informing employees about the arrangements for courses.

As organizations become more e-HR savvy, they are beginning to see the benefits almost immediately because, with modern technology every document, transaction, records have become paperless and hence there is no need to maintain a heavy stack of written records. It is advisable to collect data and information available through the *e-HR* process that can be later communicated across all organizations. These include employer facilities such as learning opportunities and flexible benefits. It can provide links that enable managers and other employees to interface directly with *HR* applications and make changes or enquiries.

VI. LIMITATIONS

Although E-HRM majorly contributes positively to the organizations, it is not free from flaws and limitations. e-HRM is accompanied by its own negative consequences, that can be best described as computerized or digitalized scrap or junk. The primary function of e-HRM is to collect and store online data, but associated with this came complexities and delays, which are the key elements to reduce for which E-HRM was incorporated and introduced in modern organizations.

Establishment of e-HRM can prove to be quite costly in terms of both investment and human resource requirements as it needs induction of sophisticated technology and highly skilled personnel who are adept in handling these technologies. Further, the users do not get exactly the reports which they want as computers cannot substitute human being. At best they can aid human effort. There is lack of face to face communication between the employee and the employer which may have an adverse effect on the assessment of the employees by the employer and vice-versa. Our proposition to these negative aspects of e-HRM is that the solution should not be looked for, in innovating new technologies, instead should be looked within the innovative thinking about core HR practices and systems. HR practitioners should concentrate on incorporating innovative HR functions rather follow a traditional path in their service delivery system.

The automation of various tasks results in the staff reducing strategy of an organization which may further lead to the de-motivation of the employees as they will always be under the pressure of great threat of using their jobs. The traditional social task of HR department may be affected badly since their tasks were confined to small localized area which has now been converted into a global expansion with the implementation of e-HR. To capitalize on these e-developments, the HR function needs to embrace changing technology and provide both transactional and transformational services. In facilitating these HR services, e-HR can be analyzed at all levels - basic, intermediate and top.

A basic-level e-HR might incorporate the internet provision of all live information. This can be on training courses, vacancies, employees' benefits entitlement and the staff handbook. Further, the online availability of HR policies and procedures such as discipline, grievance and health and safety can also find their way. Interactive facilities such as changes in employees details, management reporting and requests for basic information on staff turnover or pay rates are next to be incorporated.

VIII. CONCLUSIONS AND SUGGESTIONS

Currently e-HRM has become an inseparable part of the functioning of almost all the business niches of different levels irrespective of size and capacity. It has established a positive connection between different organizational initiatives at departmental levels and provide precise and opportune personnel information on-line without any time limitations.

E-HRM is a way of applying HR strategies, policies, and practices within organizations with a deliberate and intended for assistance of a complete web-technology-based network. Nevertheless, each technology has its own inherent risk associated with its implementation- that of huge financial investment, reduction of human involvement and materialistic approach, e-HRM is no exception. Introduction of new technologies and the management approaches have added to the challenges facing human resource managers. To meet these challenges of the future, 21st century corporations must adapt itself to management related via web.

Though, e-HRM is a novel and hot topic for research, it lacks the impetus or the driving force that can inspire academicians and experts in the field to explore its potential to its full extent. In other words, the academic community can apply new thinking to suggest alternative ways to do HRM. Combining technology, theory and empirical research with innovative exploration and science, the field of HRM can let go of its past and move into a new realm (Welbourne,2010)

REFERENCES

[1] IT Knowledge Portal, Human Resource Management , http://www.itinfo.am/eng/human-resource-management/

[2] Thite M. and Kavanagh M. (2009). Evolution of human resource management and human resource information systems: the role of information technology. In:M. Kavanagh and M. Thite, Human Resource Information Systems: Basics, Applications and Future Directions. Thousand Oaks: Sage.

[3] Strohmeier, S. ,Research in e-HRM: Review and implications. Human Resource Management Review,17 ,2007, 19-37.

[4] Gowan, M., eHRM:An internet guide for human resource management(New Jersey: Prentice Hall,2001).

[5] Ruël, H., Bondarouk T., and Looise J. "E-HRM: innovation or irritation. An explorative empirical study in five large companies on web-based HRM", Management Revue 15(3), 2004, 364–381.

[6] Shamina,H.,e-HRM-a contemporary issue of human resources management, 2011,Articlebase http://www.articlesbase.com

[7] Ruël, H., Bondarouk T., and Looise J. "E-HRM: innovation or irritation. An explorative empirical study in five large companies on web-based HRM", Management Revue 15(3), 2004, 364–381.

[8] Hussain, Z, Wallace, J. & Cornelius, N.,The use and impact of human resource information systems on human resource management professionals, Information and Management, 44, 2007, 74-89.

[9] Wright, P. M. & Dyer,L., People in the E-Business: New challenges, new solutions (CAHRS Working Paper #00-11,2000), Ithaca, NY: Cornell University.

[10] Lepak, D.P. & Snell, S.A. , Virtual HR: strategic human resource management in the 21st century, Human Resource Management Review, 8(3), 2000, 215-234.

[11] Snell S. A., Stueber D., and Lepak D. P., "Virtual HR departments: Getting out of the middle", School of Industrial and Labor Relations, Center for Advanced Human Resource Studies (CAHRS Working Paper #01-08, 2001), Ithaca, NY: Cornell University.

[12] Strohmeier, S. ,Research in e-HRM: Review and implications. Human Resource Management Review,17 ,2007, 19-37.

[13] Snell S. A., Stueber D., and Lepak D. P., "Virtual HR departments: Getting out of the middle", School of Industrial and Labor Relations, Center for Advanced Human Resource Studies (CAHRS Working Paper #01-08, 2001), Ithaca, NY: Cornell University.

[14] Ruël, H., Bondarouk T., and Looise J. "E-HRM: innovation or irritation. An explorative empirical study in five large companies on web-based HRM", Management Revue 15(3), 2004, 364–381.

[15] Welbourne,T.M.,From e-HRM to Fast HRM Opportunities for Research and Practice Innovation, Academic Key Note. The Third Academic Workshop on electronic Human Resource Management (e-HRM), 20-21 May,2010, Saarland University, Germany . http://ceur-ws.org/Vol-570/570-complete.pdf

 ISBN: 978-81-931039-3-7

SYNTHESIS AND CHARACTERIZATION OF HIGH QUALITY LARGE AREA GRAPHENE OXIDE

Vinod Kumar

Lecturer, Janta Inter College Khera, Meerut, Uttar Pradesh (India) &
Department of Chemistry, Chaudhary Charan Singh University, Meerut, 200005,
Uttar Pradesh (India)

ABSTRACT

The increasing demand of graphene based materials with the improved properties, including electrical conductivity, thermal conductivity, and mechanical properties, are highly desirable for many disciplines. In this paper, we reports the synthesis of high quality large area graphene oxide (LGO) sheets by using modified Hummer's method. Lateral Size and morphology of LGO were characterized by scanning electron microscope and atomic force microscopy. Our LGO shows wide range of sheet size distribution range from ~ 1-50 μm with thickness of ~ 1 nm. UV-Visible, X-ray diffraction and Raman spectroscopy are further used to characterize the LGO sample. The chemical composition is confirmed by X-ray photoelectron spectroscopy. The overall results indicate that solution based method can be scalable and low cast route for high yield synthesis of high-quality large area graphene oxide.

Keywords: Large Area Graphene Oxide, Scanning electron microscopy, Raman Spectroscopy, X-ray Photoelectron Spectroscopy, X-ray diffraction

I. INTRODUCTION

Graphene is a single-atomic honeycomb arrangement of carbon atoms and plays a major role in the development of nanoscience and nanotechnology, owing to their unique excellent physical and chemical properties [1-3]. Graphene oxide (GO) consists of water-dispersible, soft carbon sheets that can be easily converted to a conductive form; this 2D material is continue to inspire many curiosity-driven discoveries and applications in a wide variety of fields including liquid-crystal display technology, materials science, and bioscience [1-6]. GO has been much attracted not only because of its promising precursor for production of graphene based materials but also due its excellent dispersion stability in water and organic solvents. Among several well-known synthesis methods, chemical exfoliation starting from the oxidation of graphite is an efficient process for large scale and low cast graphene oxide (GO) stable dispersion in water and organic solvents due to oxygen containing functional groups on their basal plane and edges [6-8]. GO dispersion can be reassembled as a free-standing thin film or paper like material, which can be tuned to conducting material by chemical reduction, thermal annealing or ultraviolet excitation and make it promising materials for many technological applications such as transparent conducting films, supercapcitors, electrode for Li-ion batteries, etc [9-11].

Many properties of GO based materials, including thermal conductivity, electrical conductivity, and mechanical properties are known to be critically dependent on the GO sheet size. Recently, a number of studies reported the effect of graphene flake size on the material performances. It has been reported that chemically exfoliated reduced large area graphene oxide thin film resulted in higher electrical conductivity due to lower inter-sheet contact resistance than small area GO sheets [12]. Chen et al also reported that large areas GO have stronger antimicrobial activity than smaller area GO sheets [13]. Lee et al. further reported that the catalytic activity of LGO was found to better than small area GO sheets [14]. In this paper, we report the synthesis of high quality large area graphene oxide by chemical exfoliation of graphite using modified Hummer's method. GO lateral dimension, structural and morphological properties were characterized by atomic force microscopy, scanning electron microscopy, XRD, XPS, and UV-Visible spectroscopy.

II. EXPERIMENTAL DETAILS

GO dispersion is prepared by the oxidative exfoliation of graphite powder (Sigma Aldrich, graphite flakes) using modified Hummer's method [6]. 1 g of graphite powder was oxygenated in 45 mL H_2SO_4, while stirring for 30 minutes, which was followed by slow addition of 3.5 g potassium permanganate under an ice bath. The mixture was then continuously stirred for 24 hour at 35 °C. After completion oxygenation, the excess amount of deionized water and 35 % H_2O_2 were added to the mixture. The obtained yellow mixture was thoroughly filter washed with 1 M HCl solution and deionized water and re-dispersed in 1 L of deionized water. The monolayer exfoliation was achieved by mild sonication. Subsequent purification was performed by dialysis membrane and centrifuged at 5000 rpm/3 times to remove the acidic or ionic impurities. In order to select the large area graphene oxide sheets, the GO dispersion was centrifuged at 1000 rpm. Upper part was carefully decanted and large area graphene oxide sheets from the bottom part of the centrifuge tube.

To characterize the GO sheet size and exfoliated monolayer thickness, extremely diluted GO dispersion was dried at SiO_2 substrate surface. Atomic force microscopy (SPA400) image was recorded in the non-tapping mode under an ambient condition. Lateral dimension of GO sheets was characterized by FE-SEM (Hitachi S-4800 SEM). The XRD patterns were recorded with a PANalytical X'Pert PRO diffractometer using a solid state detector with a monochromatized Cu k_α (λ_{Cu} = 1.54060A˚) radiation source at 45 kV. A Raman spectrum of GO powder was recorded using a Renishaw Raman microscope with Ar-ion laser excitation at 514 nm at 50 mW power. UV–vis absorption spectra were collected by using a Cecil model CE-7200 (Cecil Instrument, UK) spectrophotometer. XPS spectra was recorded with a Sigma Probe and monochromatic X-ray source (XPS, K-Alpha, Thermo Scientific) to analyze the elemental composition and the assignment of carbon peaks in freeze dried LGO sample.

III. RESULTS AND DISCUSSION

Fig. 1 shows the typical scanning electron microscopy (SEM) and atomic force microscopy (AFM) image of GO sheets as obtained by the modified chemical exfoliation of graphite flakes. Interestingly, the observed SEM image (Fig.1a) of the dried GO dispersion confirm that GO sheets have broad size distribution in their lateral size, typically ranging from 1 μm to 50 μm. However, the weight fraction of LGO is more due their large molecular weight. Figure 1b shows the AFM height profile with thickness of around 1 nm, confirming that

monolayer exfoliation of GO sheets were successfully prepared and no aggregation occurred during deposition on SiO2 substrate.

The UV–Visible absorption peak of GO dispersion is shown in Fig 2. The spectrum of graphene oxide has an absorption peak at 230 nm, which can be attributed to π - π* transition of aromatic C–C ring [15]. The UV-Visible spectrum was measured at different time interval and no intensity reduction was observed. This is confirming that our LGO dispersion is highly stable in water up to several months. The structure of the GO sheets was characterized using X-ray-diffraction (XRD) spectroscopy. Figure 3 shows the XRD patterns of both the graphite flakes and the LGO samples, indicating that the starting material represented a fully graphitic system with a sharp (002) peak at $2\theta = 26.7°$ corresponding to a *d*-spacing about 3.34 Å, while the as-prepared LGO had a distinct peak at $2\theta = 11.10°$, corresponding to a *d*-spacing of about 8.02 Å according to Bragg's law: $2d \sin\theta = n\lambda$, where *n* is an integer determined by the given order, and λ is the wavelength. This *d*-spacing value in LGO represents, approximately, a one-molecule-thick layer of water entrapped between the GO layers, presumably through a hydrogen bond. Some recent theoretical study also suggested that the water content controls the extent of these interlayer hydrogen-bond networks, thereby affecting the interlayer spacing [12]. The individual LGO sheets are connected *via* a non-uniform network of hydrogen bonds mediated by oxygenated functional groups and water molecules. This means that the interlayer spacing of GO sheets is proportional to the degree of oxidation.

Further characterizations are carried out by FTIR and Raman Spectra. Raman spectroscopy provides a non-destructive method for characterizing graphene. Fig. 4 shows the Raman spectra of the freeze dried LGO sample. The Raman spectrum of LGO displays two prominent peaks at 1355 and 1590 cm-1, which correspond to the well documented D and G bands, respectively. G-peak at 1590 cm-1is corresponds to the first order scattering of the E_{2g} mode. The D-peak at ~ 1350 cm-1 due to the scattering of A_{1g} mode and confirms the lattice distortions in the sample [12, 16]. In the present study, the I_D/I_G ratio is ~ 0.85, which are comparable to previous reported literatures. Further, we analyzed the chemical structure of LGO films through FTIR spectra as shown in Fig. 4b. It has been found that peak at 1741 cm^{-1}, attributes to the >C=O/COOH group, the peak at 1623 cm^{-1}, assigns to the contributions from the skeletal vibrations of the graphitic domains, the peaks at 1372 cm^{-1}, assign to C-OH stretching vibrations, and the peaks at 1058 cm^{-1} belongs to C-O alkoxy stretching vibrations [16]. The absorption peak at ~3300 cm^{-1} corresponds to the O-H stretching. The recorded FTIR spectrum is clearly shows oxygen containing functional groups in LGO sample.

In last, we employed the X-Ray photoelectron spectroscopy (XPS) to investigate the quality of LGO. The elemental compositions and surface chemistry of LGO powder is shown in Figure 5. High resolution C1s peaks, as shown in the Inset of Figure 5, was deconvoluted into to three peaks corresponding to the fallowing functional groups: ~284.4 eV (C=C/C-C), ~ 286.5 eV (C-O-C/C-OH) and ~ 288.3 eV (C=O/O-C=O). It was found that C/O atomic ratio, which is an important parameter to evaluate the degree of oxidation of GO sheets found to be 2.24, suggesting that the large area GO sheets contained efficient oxygenated functional groups on GO sheet surface [12].

IV. CONCLUSION

We have developed a modified chemical exfoliation method to produce large area GO sheets. The method produces a high yield, stable and well-oxidized hydrophilic graphene oxide. By using mild sonication and hand

shaking, GO sheets with a size up to ~ 50 um were obtained. Further, we found that the GO sheets were shown stable dispersion in water and good oxygen containing functional groups on their surface. AFM height profile shows the monolayer thickness of ~ 1 nm. Further, XRD and XPS results confirm the monolayer exfoliation of graphene oxide. These large area graphene oxide sheets is of significance in terms of the development of graphene based electronic devices with a large working area, such as field-effect transistors, biosensors, solar cells, transparent electrodes, and ultra low percolation threshold for composite applications.

V. ACKNOWLEDGMENTS

The author is thankful to CCS University and AIRF JNU for providing experimental facilities.

REFRENCES

[1] Z. Xu and C. Gao, Graphene chiral liquid crystals and macroscopic assembled fibres, Nature Communication, 2, 2011, 571-579.

[2] H.-P. Cong, X.-C. Ren, P. Wang and S.H. Yu, Wet-spinning assembly of continuous, neat, and macroscopic graphene fibers, Scientific Reports, 2, 2012, 613-618

[3] Y. Zhu , S. Murali , W. Cai , X. Li , J. W. Suk, J. R. Potts and R. S. Ruoff, Graphene and Graphene Oxide: Synthesis, Properties, and Applications, Advanced Materials, 22, 2010, 3906-3924.

[4] X. Du, I. Skachko, A. Barker and E. Andrei, Approaching ballistic transport in suspended graphene, Nature Nanotechnology, 3, 2008, 491-495.

[5] C. Lee, X. Wei, J. W. Kysar and J. Hone, Measurement of the Elastic Properties and Intrinsic Strength of Monolayer Graphene, Science , 321, 2008, 385-388.

[6] J. E. Kim, T. H. Han, S. H. Lee, J. Y. Kim, C. W. Ahn, J. M. Yun and S. O. Kim, Graphene Oxide Liquid Crystals, Angew. Chem. Int. Ed. 50, 2011, 3043-3047.

[7] P. Kumar, U. N. Maiti, K. E. Lee and S. O. Kim, Rheological properties of graphene oxide liquid crystal, Carbon, 80, 2014, 453-461.

[8] R. Jalili, S. H. Aboutalebi, D. Esrafilzadeh, K. Konstantinov, S. E. Moulton, J. M. Razal and G. G. Wallace, Organic Solvent-Based Graphene Oxide Liquid Crystals: A Facile Route toward the Next Generation of Self-Assembled Layer-by-Layer Multifunctional 3D Architectures, *ACS Nano*, 7, 2013, 3981–3990.

[9] J. Zhao, S. Pei, W. Ren, L. Gao, H.-M. Cheng, Efficient Preparation of Large-Area Graphene Oxide Sheets for Transparent Conductive Films, ACS Nano, 4, 2010, 5245-5252.

[10] U. N. Maiti , J. Lim , K. E. Lee, W. J. Lee and S. O. Kim, Three-Dimensional Shape Engineered, Interfacial Gelation of Reduced Graphene Oxide for High Rate, Large Capacity Supercapacitors , Advanced Materials, 26, 2014, 615–619.

[11] S. H. Ha, Y. S. Jeong and Y. J. Lee, Free Standing Reduced Graphene Oxide Film Cathodes for Lithium Ion Batteries, ACS Applied and Material Interfaces, 5, 2013, 12295-12303.

[12] X. Lin, X. Shen, Q. Zheng, N. Yousefi, L. Ye, Y.-W. Mai and J.-K. Kim, Fabrication of Highly-Aligned, Conductive, and Strong Graphene Papers Using Ultralarge Graphene Oxide Sheets, ACS Nano, 6, 2012,10708-10719.

[13]S. Liu, M. Hu, T. H. Zeng, R. Wu, R. Jiang, J. Wei, L. Wang, J. Kong and Y. Chen, Lateral Dimension-Dependent Antibacterial Activity of Graphene Oxide Sheets, Langmuir, 28, 2012, 12364−12372.

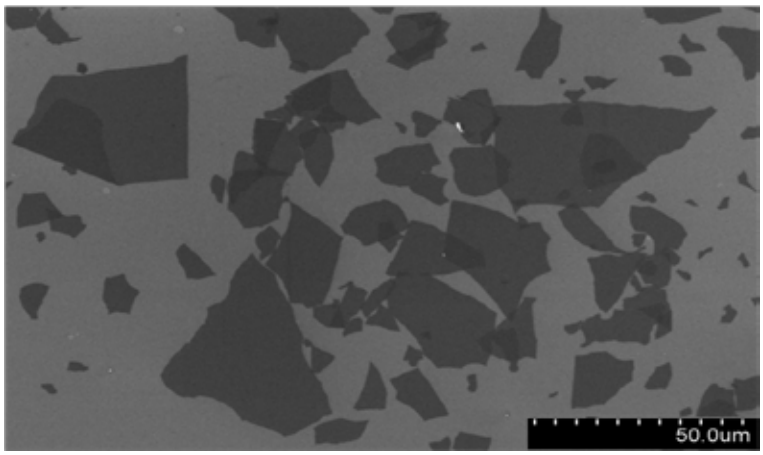
[14]K. E. Lee, J. E. Kim, U. N. Maiti, J. Lim, J. O. Hwang, J. Shim, J. J. Oh, T. Yun and S. O. Kim, ACS Nano, 8, 2014, 9073-9080.

[15]G. Eda, Y.-Y. Lin, C. Mattevi, H. Yamaguchi, H.-A. Chen, I. S. Chen, C.-W. Chen, M. Chhowalla, Blue photoluminescence from chemically derived graphene oxide, Advanced Materials, 22 2010, 505-509.

[16]M. A. Pimenta, G. Dresselhaus, M. S. Dresselhaus, L. G. Canc¸ado, A. Jorio, R. Saito, Studying disorder in graphite-based systems by Raman spectroscopy, Physical Chemistry Chemical Physics, 9, 2007, 1276-1291.

Figures

(a)



(b)

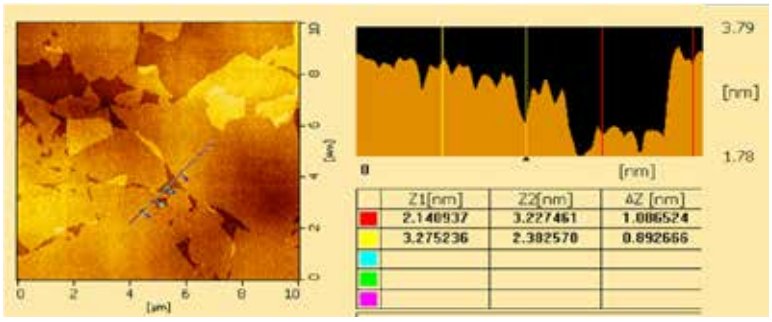


Fig. 1 SEM and AFM image of LGO with height profile with the thickness of ~ 1 nm.

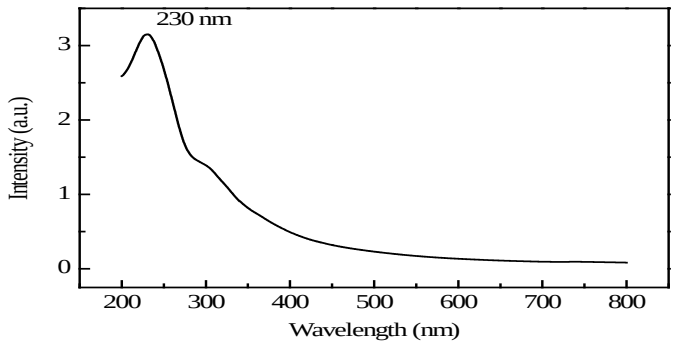


Fig 2. UV-Vis spectra of aqueous dispersion of LGO.

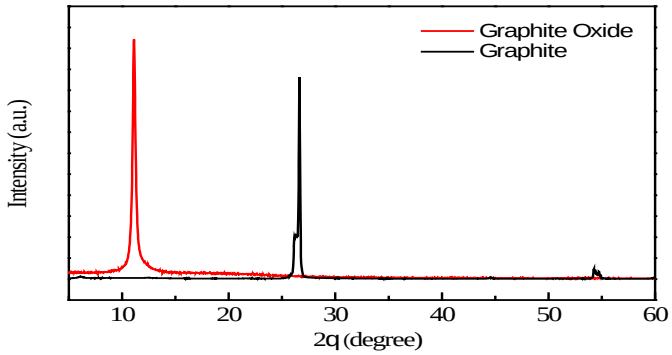


Fig. 3 XRD pattern of pristine graphite flakes and LGO samples.

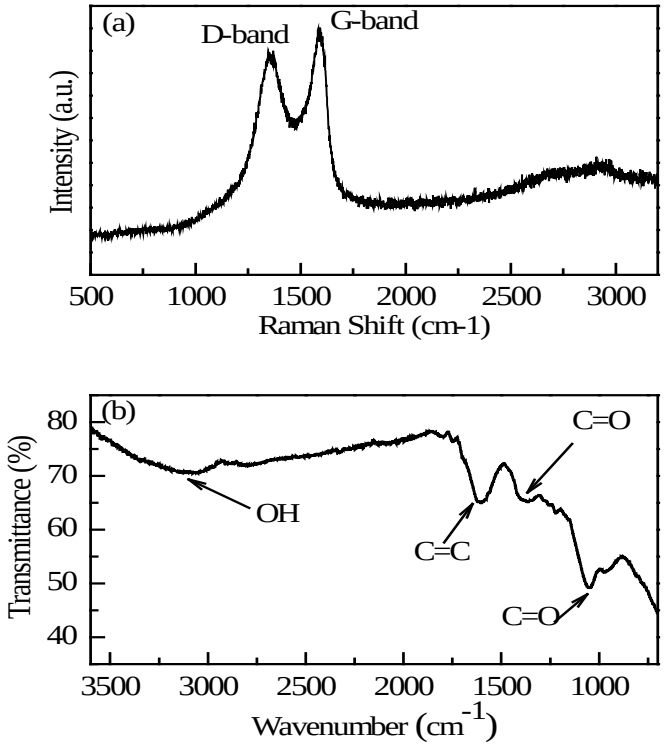


Fig. 4 (a) Raman spectra and (b) FTIR spectra of LGO

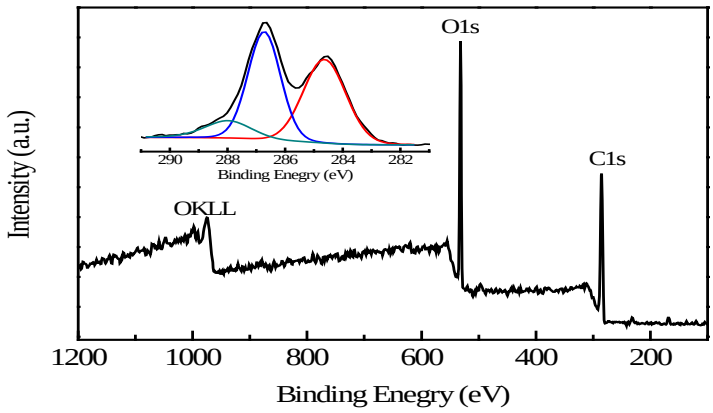


Fig. 5 General XPS spectra of GO. Inset shows the deconvolted C_{1s} spectra.