SURVEY ON DIGITAL WATERMARKING TECHNIQUES

Rutuja Sonar[1], Shivaputra S. Panchal[2]

[1]MTech Student, [2]Assistant Professor, Dept. of Computer Science and Engg,
Dr.P.G.Halakatti Engineering College, Vijayapur

ABSTRACT

A digital watermark is a kind of marker concealed embedded in a noise tolerant signal such as audio or image data. It is typically used to identify ownership of the copyright of such signal. "Watermarking" is the process of hiding digital information in a carrier signal. Embedding a digital data with information which cannot be removed easily is called digital watermarking. Digital watermarks may be used to verify the authenticity or integrity of the digital data or to show the identity of its owners. This paper provides a comprehensive survey on various digital watermarking techniques such as robust, fragile and semi fragile watermarking techniques.

I. INTRODUCTION

Growth of computer and network technology has led to tremendous opportunities for creation and distribution of digital media content. And the digital data is easy to be edited and illegal duplication, and thus the technology to resolve such issues is in demand. The Digital watermarking technique makes use of a data hiding scheme to insert some information in the image.Digital watermarking is a technique which embeds additional information called digital signature or watermark into the digital content in order to secure it. A watermark is a hidden signal added to images that can be detected or extracted later to make some affirmation about the host image. The major point of digital watermarking is to find the balance among the aspects such as robustness to various attacks, security and invisibility. The invisibleness of watermarking technique is based on the intensity of embedding watermark. Better invisibleness is achieved for less intensity watermark. So we must select the optimum intensity to embed watermark. In general there is a little tradeoff between the embedding strength (the watermark robustness) and quality (the watermark invisibility). Increased robustness requires a stronger embedding, which in turn increases the visual degradation of the images.

II. CLASSIFICATION

The digital image watermarking scheme can be divided into two categories. They are visible digital image watermarking and invisible image watermarking techniques. In visible watermarking, the information is visible in the picture or video. Typically, the information is text or a logo which identifies the owner of the original document.

In invisible watermarking, information is added as digital data to audio, picture or video, but it cannot be perceived as such. Further, the invisible watermarks are categorized into watermarking techniques as robust, fragile and semi-fragile.

- **Robust** - Generally, a robust mark is generally used for copyright protection and ownership identification because they are designed to withstand nearly all attacks such as lossy compression, filtering operations and

geometric distortions. These algorithms ensure that the image processing operations do not erase the embedded watermark signal.

- **Fragile**– In fragile techniques, even one bit change in image is not allowable. They are mainly applied to content authentication and integrity attestation, because they are sensitive to almost all modifications.
- **Semi-fragile**– Semi-fragile methods are robust to incidental modifications such as JPEG compression, but fragile to other modifications such as high impact additive noises. That is, some incidental image manipulations have to be considered allowable during the process of media transmission and storage, while other malicious modifications (e.g. alteration of content) from attackers should be rejected.

III. WATERMARKING TECHNIQUES

The various watermarking techniques are:

3.1 Spatial Domain Techniques

Spatial domain watermarking slightly modifies the pixels of one or two randomly selected subsets of an image. Modifications might include flipping the low-order bit of each pixel. Various spatial domain techniques are as follows:-

- Least Significant Bit Coding (LSB)
- Predictive Coding Schemes
- Correlation-Based Techniques

3.2 Frequency Domain Techniques

In Frequency domain the secret data are hidden in thelower or middle frequency portions of the protected image,because the higher frequency portion is more likely to be suppressed by compression. Various frequency domain techniques are as follows:-

- Discrete cosine transform (DCT) based technique
- Discrete Fourier Transformation (DFT) based technique
- Discrete wavelet transform (DWT) based technique

3.3 Wavelet Transform based Watermarking

The wavelet transform based watermarking technique divides the image into four sidebands – a low resolution approximation of the tile component and the component's horizontal, vertical and diagonal frequency characteristics.

3.4 Block-Wise Technique

One of the first fragile block-wise watermarking schemes with tamper localization was proposed by Wong. In this scheme, an image is divided into non-overlapping blocks and watermarking is performed for each block independently. The seven most significant bits (MSBs) of all pixels in a block are hashed using a secure key-dependent hash. The hash is then XORed with a chosen binary logoand inserted into the LSBs of the same block. The verification process starts in the reverse order by calculating the key-dependent hash of the seven MSBs in each block and XOR operation is performed with the LSBs.The tampered blocks can be found by comparing the output with the used logo.

3.5 Literature Survey on Temper Detection in Digital Watermarking

In this paper [1], three public image watermarking techniques are proposed. The first one, called Single Watermark Embedding (SWE), uses the concept of Visual Cryptography (VC) to embed a watermark into a digital image. The second one, called Multiple Watermarks Embedding (MWE) extends SWE to embed multiple watermarks simultaneously in the same host image. Finally, Iterative Watermark Embedding (IWE) embeds the same binary watermark iteratively in different positions of the host image, to improve the robustness.

In this [2] Progressive image transmission (PIT) provides multiple image resolutions that favors a time-critical or a low-band channel environment. Author proposes, a PIT based watermarking for multi-resolution image authentication. The image content with progressive characteristic is taken as the authentication code. The authentication code is then embedded according to multi-resolution image encoding.

In this [3] author proposes a technique which embeds information into a carrier image with virtually imperceptible modification of the image. The present paper found a novel fact that by inserting the watermark using Least Significant Bit (LSB), the grey value of the image pixel either remains same or increases or decreases to one.

In this [4], author present three counterfeiting attacks on the block-wise dependent fragile watermarking schemes. We consider vulnerabilities such as the exploitation of a weak correlation among block-wise dependent watermarks to modify valid watermarked images, where they could still be verified as authentic.

In this [5], author propose a novel multipurpose watermarkingscheme, in which robust and fragile watermarks are simultaneously embedded, for copyright protection and content authentication. By quantizing a host image's wavelet coefficients as masking threshold units (MTUs), two complementary watermarks are embedded using cocktail watermarking and they can be blindly extracted without access to the host image.

In this [6], Watermarking techniques which are fragile to intentional modifications while robust to incidental or unintentional manipulations are referred to as Semi-fragile. This paper proposes a semi-fragile watermarking technique which embeds watermark signal into the host image in order to authenticate it.

This [7], paper presents a novel invisible robust watermarking scheme for embedding and extractinga digital watermark in an image. The novelty lies in determining a perceptually important sub-image in the host image. Invisible insertion of the watermark is performed in the most significantregion of the host image such that tampering of that portion with an intention to remove ordestroy will degrade the esthetic quality and value of the image.

In this [8] paper, author propose an efficient image tamper detection method using block-wise technique which is able to detect the tamper locations. In the proposed method, a digital signature is generated from the hash code of the blocks of the final level where the watermark is inserted and the blocks of the upper level where those blocks are included in the image division process and this signature is used as the watermark, which is randomly inserted into selected image blocks. The proposed method was confirmed to be able to detect the tampered parts of the image without testing the entire block of the watermarked image. The image block-wise watermarking method was proposed by using digital signature. The tampered blocks could be detected faster by testing the hash code of the upper level first without testing all inserted blocks with watermarks inserted.

IV. APPLICATIONS

Digital watermarking can be used for the following purposes:

- **Copyright Protection:**This is by far the most prominent application of watermarks. With tons of images beingexchanged over insecure networks every day, copyright protection becomes a very important issue. Watermarking an image will prevent redistribution of copyrighted images.
- **Authentication:**Sometimes the ownership of the contents has to be verified. This can be done by embedding a watermark and providing the owner with a private key which gives him an access to the message. ID cards, ATM cards, credit cards are all examples of documents which require authentication.
- **Broadcast Monitoring:** As the name suggests broadcast monitoring is used to verify the programs broadcasted on TV or radio.
- **Content Labeling:** Watermarks can be used to give more information about the cover object. This process is named as content labeling.
- **Tamper Detection:** Fragile watermarks can be used todetect tampering in an image. If the fragile watermark isdegraded in any way then we can say that the image ordocument in question has been tampered.
- **Digital Fingerprinting:** This is a process used to detectthe owner of the content. Every fingerprint will beunique to the owner.
- **Content protection:** In this process the content stampedwith a visible watermark that is very difficult to removeso that it can be publicly and freely distributed.

V. CONCLUSION

This paper provides a comprehensive survey on various digital watermarking techniques, their requirements and applications. The use of different type of watermark is application dependent. Digital watermarking research hasgenerally focused upon two classes of watermarks, fragile and robust. Robust watermarks are designed to be detected even after attempts are made to remove them. Fragile watermarks are used for authentication purposes and are capable of detecting even minute changes of the watermarked content. But neither type of watermark is ideal when considering "information preserving" transformations (such as compression) which preserve the meaning or expression of the content and "information altering" transformations (such as feature replacement) which change the expression of the content. And it provides the temper detection of digital watermarking image using bloc-wise technique.

REFERENCES

[1] B. Surekha and D. N. Swamy, “A Spatial Domain Public Image Watermarking”, International Journal of Security and its Applications, vol. 5, no. 1, (2011), pp. 1-12.

[2] P. Tsai, Y.-C.Hu, H.-L.Yeh and W.-K. Shih, “Watermarking for Multi-Resolution Image Authentication”, International Journal of Security and its Applications, vol. 6, no. 2, (2012), pp. 161-166.

[3] G.RoslineNesaKumari,B.VijayaKumar, L.Sumalatha, and DrV.V.Krishna, “Secure and Robust Digital Watermarking on Grey Level Images”, International Journal of Advanced Science and TechnologyVol. 11, October, 2009

[4] M. Holliman and N. Memon, "Counterfeiting Attacks on Oblivious Block-Wise Independent Invisible Watermarking Schemes", IEEE Transaction on Image Processing, vol. 9, no. 3, (2000), pp. 432-441.

[5] Chun-Shien Lu and Hong-Yuan Mark Liao, "Multipurpose Watermarking for Image Authentication and Protection", IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 10, NO. 10, OCTOBER 2001, pp. 1579-1592

[6] Dr.M.Mohamed and SathikS.S.Sujatha, "Authentication of Digital Images by using a semi-Fragile Watermarking Technique", Volume 2, Issue 11, November 2012 ISSN: 2277 128X, pp. 39-44

[7] Saraju P. Mohanty and Bharat K. Bhargava, "Invisible Watermarking Based on Creation and Robust Insertion-Extraction of Image Adaptive Watermarks", ACM Journal Name, Vol. V, No. N, February 2008, Pages 1–24.

[8] Chan-Il Woo and Seung-Dae Lee, "Digital Watermarking for Image Tamper Detection using Block-Wise Technique", International Journal of Smart Home Vol.7, No.5 (2013), pp.115-124 ISSN: 1975-4094 IJSH.

 ISBN: 978-81-931039-3-7

SURVEY ON AMES: ADAPTIVE MOBILE VIDEO STREAMING AND EFFICIENT SOCIAL VIDEO SHARING IN THE CLOUDS

Laxmi Sharma[1], Laxmi Shabadi[2]

[1]M.tech(Student), [2]Assistant Professor, Department of CSE,

BLDEA's Dr.P.G.Halakatti College of Engineering & Technology, Vijayapur, (India)

ABSTRACT

The media data has grown over years in all streams of technology. Video and imagesplays a vital role in communication around the globe. The usage of mobile device along with media has boomed year age of technology. The usage of traditional networking and service providers lacks to provide the quality centred and reliable service to the mobile users concerning with the media data. The vital problems that leads to the poor services from the service providers would be low bandwidth which affects the efficient transfer of video to the user, the disruption of video streaming also occurs due to the low bandwidth. The buffer time of the video over mobile devices which moves from place to place affects the smooth streaming and also sharing of video from one user to another user over social media. Our survey shows the functioning of various methods and architecture which used cloud to provide effective solution for providing better service to the users. AMES is cloud architecture built specially to provide video service to the user. The study has came up with a optimal solution, proposing with video cloud, which collects the video from video service providers and providing the reliable service to the user.

I. INTRODUCTION

The era of cloud computing reigns with advancements in technology, the technology provides various services to the human's need and also it urges the more necessity for the emerging technology. Cloud computing provides a platform for other advanced technologies like bigdata, mobile computing to inculcate its service and provide the QoS to the customers. The cloud has grown to a vast extend over the period of years. All the services that are provided to thecustomer are done using could as their backbone, it give vast amount of resources and infrastructure to consumer who acts as vendors to small scale business and cloud could provide services to fully fledged organization with less cost.Organizing the service and extending the service depending upon the growing needs of the customer cloud be achieved by cloud service and infrastructure[1,5]. The major issue is the resources, while any service needs to be extended, there sources with the service vendor plays a vital role. Investing huge sum of dollars on hardware is just one part of extension, maintaining the hardware along the services provided would carry tons of dollars. Where cloud provides space for extending the services as a service provider and also it can provide infrastructure service to small scaleservice vendors. The era of hardwarelimitation has vanished, new age has begun the hardware limitation are not considered but the situation turns out that, ifthe hardware resources are not utilized effectively, maintain the resourcesbecomes very serious problem. The data thatis being used

among the computing world has faced drastic change. These data occupies large amount of data, needvery heavy processing powers. All the needed resources such as storage space and processing power are provided by the cloud and can be extended depending upon the service. The problem doesn't rise until these data are transferred on the internet. The data created on the host, should be sent to the cloud for storage, the problem of data transfer with these high ended multimedia data starts. in this paper we are in particularly going to focus on the videos , video – data.

The processing and transferring of video to the service provider and between hosts became an issue. As the usage of video data over the years have increased, the management of resources supporting the video data service has tobe monitored and extended for providing reliable service. The trend in the technology changes as per the needs of the users. Users are comfortable with the mobile and portable devices than stationary hosts[6][9][10].The problem with providing service to the mobile device, user is unavailability to service reaching the user in constant range. Since the location of the user changes every second of the time, the bandwidth of their network also changes constantly due to various reason and main reason would be change in location. Providing quality oriented service to the mobile users are far difficult than to wired users. The mobile devices which works under mobile network follows and entirely different path in providing service to its users. The mobile devices plays most important roles in the upcoming technologies around the computer science and technology. Any methodology or technology that has been developed are enhanced for mobile technology, the mobile devices provides various comfortably to the user in providing service. the devices itself are handy to be used. the user does not need to be stationed in one place or has to be waiting in place to get the service. The cloud computing technology supports its entire service for mobile devices. As the type of data changes from text to multimedia data such as video, the devices are also changes from laptop to smart phones[2].

II. ADAPTIVE AND EFFICIENT VIDEO STREAMING AND SHARING IN CLOUD

The figure 1 shows the architecture of the adaptive and efficient way of enhancing the video streaming and sharing of video to the mobile users. The architecture was constructed based on the video service provided in cloud called as AMES. The architecture contains

A. Video service provider (VSP) : the originated place of actual video data. It used the traditional video service provider. VSP can handle multiple request at the same time, while coming to the QoS with the mobile users , the VSP does not provide service up to the mark.

B. Video cloud (VC): the cloud step up has been established with many components working together , virtually to get the original video data from the VSP and provide the reliable service to the mobile user and it also provides availability of video and makes the sharing of those videos among the users much easier.

C. Video base (VB): Video base consists of the video data that are provided as the service to the mobile users in cloud.

D. Temp video base(TVB): it contains the most recently accessed video data and it also contains most frequently accessed video data.

E. Vagent: it is an agent created for every mobile user who requests for the video service to the video cloud.

F. Mobile users: the users who are mobile and providing the availability of the service to their location is difficult.

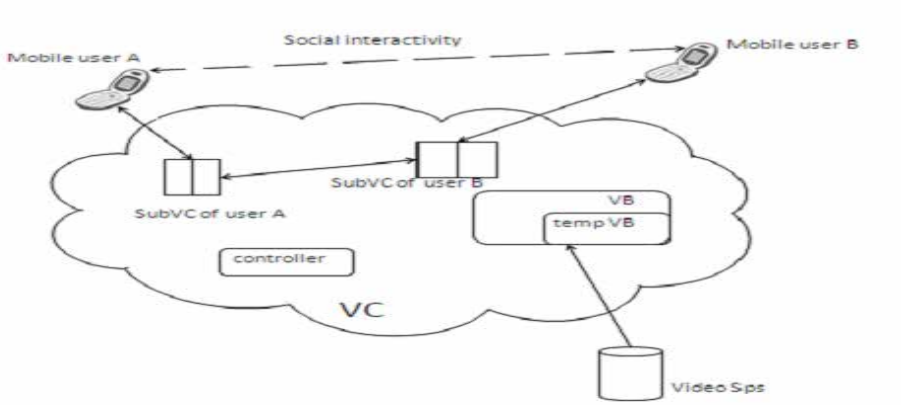


Figure1. VC architecture

The video cloud provides services under two main methodologies adaptive mobile video streaming and efficient mobile video sharing. The video streaming and video sharing plays the vital role in providing the reliable service to the customers. The rate in which frames of the videos are streams determines the quality and availability of the video service. Video data are most commonly shared among the users in the network. Mobile users are most commonly found to use social networking sites more offently[6,7]. The mobile device and mobile computing provides them space to be connected on the social network. Multimedia data such as images and videos are shared among the friend and users of the social media. The request of the video and sharing of video are two main action requested from customer. Video cloud provides platform to provides these two service in better way.The video service provider (VSP) contains the raw video data , the videos available in VSP can be used to service the customer's request. But VSP does not have sufficient resource to provide QoS and better video sharing among mobile devices and users. The Video cloud (VC) contain video base (VB) which collect the requested videos from the VSP and keeps the copy of the video , so as the request for the videos can be services. The Temporary video base (TempVB) stores the link of the videos that are accessed more recently and frequently, the links provides faster access to the videos on the VB. The controller plays the important role of managing the working and coordination of all the components on the video cloud and mobile users[2,7,10]. For every mobile user who comes for the service in cloud, one agent is created Vagent. This video agent is responsible for processing the user's request and delivery the servers' response to the user. The requested videos link will be saved in vagent for retransmission and for services if the same videos are requested again by the client. The Vagent can communicate among themselves for providing adaptive streaming of services. The video source or link available to one Vagent can be accessed and used by another Vagent. The mobile user can also communicate among themselves. The social interaction are carried out, the sharing of videos are also tracked and carried out through the Vagent of each user. Hence tracking of the video source availability and provides video to the requested user becomes easier. The video sharing in social media becomes efficient for video streaming.

2.1 Scalable video coding

SVC is an extension to the H.264/AVC standard. It is classified as a layered video codec which can encode a video stream in several types and numbers of enhancement layers on top of the H.264/AVC-compatible base layer. These enhancement layers can be added or removed from the bit stream during streaming without re-encoding of the media. The transmission rate of scalable video streams in the

mobile network can be controlled by using TCP- friendly rate control. The streams are encoded using the Scalable Video Coding (SVC) extension of the H.264/AVC standard. Adding or removing the layers is decided based on the TFRC during varying channel conditions of the mobile network SVC provides a high quality multimedia communication services inheterogeneous network environment, especially when the client processing power, system resources, and network state unknown.

2.2 TFRC

The bit rate of the stream can be dynamically adapted to the changing channelconditions which greatly improves all performance indicators such as interruption time, loss rate, delay and buffer requirements. This also implies that more users could be admitted to the cell and it would still be able to guarantee certain service qualities. This is especially true in loaded situation where there are not enough radio resources to combat bad reception quality in order to maintain guaranteed throughput to some users. However, since the TFRC was not designed for a mobile environment, we expect that it can be further optimized.

2.3 H.264/SVC

In the scalable video coding extension of the H.264/AVC standard, an exhaustive search technique is used to select the best coding mode for each macro block. This technique achieves the highest possible coding efficiency, but it demands a higher video encoding computational complexity which constrains its use in many practical applications. This proposes combined fast sub-pixel motion estimation and a fast mode decision algorithm for inter-frame coding for temporal, spatial, and coarse grain signal-to-noise ratio scalability. The correlation is used between the macroblock and its enclosed partitions at different layers. It has been observed that there is a highcorrelation between the MB and its enclosed partitions when estimating the motion at different resolutions. Therefore a two step fast sub-pixel motion estimation scheme based on this observation has been developed.

III. PERFORMANCE ANALYSIS

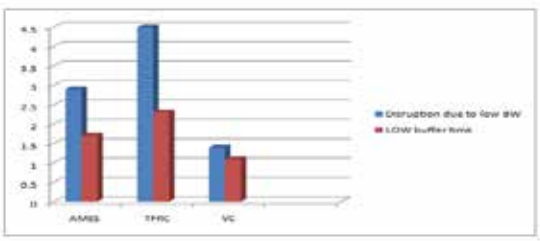


Figure 2. Comparison of Performance

The performance of video cloud is better than the previously used techniques. Weconsider the comparison of AMES Cloud and TFRC to our proposed method Video Cloud. The working of the AMES and VC are more equal and most of the extra loaded components which are found in AMES are reduced[5]. Vagents carry out most of the pre-processing of the video streaming sharing in media. Vagents alsoprefetch the requested video by the user from TempVB or VB for providing better services. TRFC does not provide any dedicated method to improved the service to the user, it tells how the transfer medium could be monitored and bandwidth level could be negotiated so as the data transfer can be achieved very

efficiently[3][13] . The over comparison of the services provided based on bandwidth and buffer time is considered. Figure 2 show the graph of VC provides better result than AMES . the disruption due to low and varying bandwidth , the buffer time at the client side usually takes long time due to delay in perfecting of video from service provider, VC provides Vagent to minimize it comparatively.

IV. CONCLUSION

Multimedia data has occupied vast empire in the growing technology of computing. The latest technology in handled devices also increases rapidly day by day. The entire computing and social media are made compactable in the arm of a man using mobile devices. The usage such devices also increased the change in usage of data format from textual to multimedia data main video and images and audios. The video place more important in convey most of the information in its content. The usage of such video has increased varying over the years.The mobile users requests the video service which could a video file, it could be video call. The service isbeen provided by the traditional service providers who has the video servicing resource. But when number request and amount of data increases the service providers way of processing the request does not provide optimal service to the user. Other than mentioned problem, there are various other issues such as disruption due to low bandwidth and unknown buffer time. The serviceprovider cant handles external issues as mention to provide quality oriented service and availability of resource to the customer. The cloud environment default provides adaptable and optimal infrastructure to any cloud user. The video serviceprovider is added as one of the resource in video cloud. The cloud base and Vagents plays vital role in keep track of videos and updating the link so as to provide undisrupted service to the customer. It also provides better video sharing in social media, where the transmissions of videos are highly carried out.

REFERENCE

[1] XiaofeiWang,MinChen,TedTaeyoungKwon,Laurence.Yang, Victor C.M.Leung , ―AMES –cloud: A framework of adaptive mobile video streaming and efficient social video sharing in the clouds,‖ IEEE transaction on multimedia,Vol 15, no.4, June 13.

[2] V.Sarangan,J. C. Chen,Comparative study of protocols for dynamic servicenegotiation in the next-generation Internet,‖ IEEE Commun. Mag., vol. 44, no. 3, pp. 151–159, Mar. 2006.

[3] I. F.Akyildiz, J. Xie, S. Mohanty, A survey on mobility management in next generation all-IP based wireless systems,‖ IEEE Wireless Commun., vol. 11, no. 4, pp. 16–28, Aug. 2004.

[4] N. Banerjee, W. Wu, S. Das, S. Dawkins, J. Pathak, ―Mobility support in wireless Internet,‖ IEEE Wireless Commun., vol. 10, no. 5, pp. 54–61, Oct. 2003.

[5] R. Ramjee, K. Varadhan, L. Salgarelli, S. R. Thuel, S. Y.Wand, T.L. Porta, ―Hawaii: A domain-based approach for supporting mobility in wide-area wireless networks,‖ IEEE/ACM Trans. Netw., vol. 10, no.3, pp. 396–410, Jun. 2002.

[6] M. Liu, Z. Li, X. Guo, E. Dutkiewicz, ―Performance analysis and optimization of handoff algorithms in heterogeneous wireless networks,‖ IEEE Trans. Mobile Comput., vol. 7, no. 7, pp. 846–857,july. 2008.

[7] R. Stewart , ―Stream control transmission protocol,‖ in RFC 2960,Oct. 2000.

[8] S. Fu, M. Atiquzzaman, ―SCTP: State of the art in research, products, and technical challenges,‖ IEEE Commun. Mag., vol. 42, no. 4, pp. 64–76, Apr. 2004.

[9] L. M. F. Yu, V. C. M. Leung, ―A new method to support UMTS/ WLAN vertical handover using SCTP,‖ IEEE Wireless Commun., vol. 11, no. 4, pp. 44–51, Aug. 2004.

[10] R. Fracchia, C. Casetti, C. Chiasserini, and M. Meo, WiSE: Best-path selection in wireless multihoming environments,‖ IEEE Trans. Mobile Comput., vol. 6, no. 10, pp. 1130–1141, Oct. 2007.

[11] M. Jain, C. Dovrolis, End-to-end available bandwidth: Measurement methodology, dynamics, and relation with TCP throughput,‖ IEEE/ACM Trans. Netw., vol. 11, no. 4, pp. 537–549,Aug. 2003.

[12] A. Abdelal, T. Saadawi, M. Lee, LS-SCTP: A bandwidth aggregation technique for stream control transmission protocol,‖ Comput.Commun., vol. 27, no. 10, pp. 1012–1024, Jun. 2004.

[13] L. Magalhaes, R. Kravets, MMTPMultimedia multiplexing transport protocol,‖ in Proc. 1st ACMWorkshop Data Communicationsin Latin America and the Caribbean, Apr. 2001.

[14] Xiaofei Wang,AMES-Cloud: A Framework of Adaptive Mobile Video Streaming and EfficientSocial Video Sharing in the Clouds.,ieee transactions on cloud computing vol:15 no:4 year 2013.

POWER QUALITY DYNAMICS – A REVIEW

Chamandeep Kaur

Assistant Professor, Department of Electrical Engineering Bhutta Group of Institutions, (India)

ABSTRACT

A power quality in electrical networks is one of today's most concerned areas of electrical power system. The power quality has serious economic implications for consumers, utilities and electrical equipment manufactures. Modernization and automation of industry involves increasing use of computers, microprocessors and power electronic systems such as adjustable speed drives. Integration of nonconventional generation technologies such as fuel cells, wind turbines and photo-voltaic with utility grids often requires power electronic interfaces. The power electronic systems also contribute to power quality problems(generating harmonics).Under the deregulated environment, in which electric utilities are expected to complete with each other, the customer satisfaction becomes very important. The impact of power quality problems is increasingly felt by customers- industrial, commercial and even residential.

Keywords: PQ, HC

I. INTRODUCTION

The PQ issue is defined as "any occurrence manifested in voltage, current, or frequency deviations that results in failure, damage, upset, or disoperation of end-use equipment.A simpler word power quality is a set of electrical boundaries that allow a piece of equipment to function in its intended manner without significant loss of performance or life expectancy. This definition embraces two things that we demand from an electrical device which are performance and life expectancy.

II. PROBLEMS ASSOCIATED WITH POWER QUALITY

2.1 Momentary Phenomena

2.1.1Transients

Transients are power quality disturbances that involve destructive high magnitudes of current and voltage or even both. It may reach thousands of volts and amps even in low voltage systems. However, such phenomena only exist in a very short duration from less than 50 nanoseconds to as long as 50 milliseconds. This is the shortest among PQ problems, hence, its name. Transients usually include abnormal frequencies, which could reach to as high as 5 MHz.

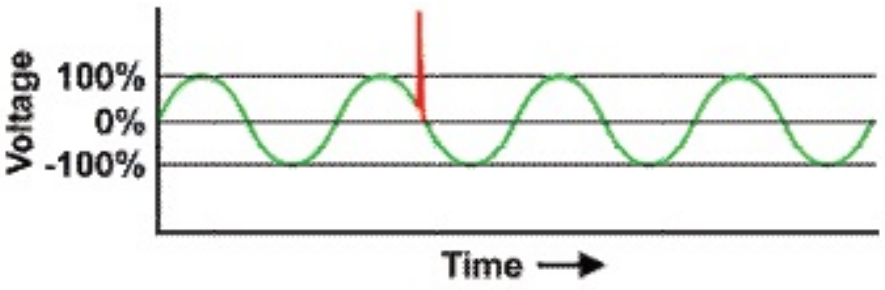


Figure - 1: Transients

2.1.2 Long Duration Voltage Variations

These are defined as the rms variations in the supply voltage at fundamental frequency for periods exceeding one minute. These variations are classified as-:

- Ø Over voltages
- Ø Under voltages
- Ø Sustained interruption

2.1.3 Short Duration Voltage Variation

The short duration voltage variation are generally caused by fault conditions like single line to ground or double line to ground and starting of large loads such as induction motor. The voltage variations can be temporary voltage dips i.e. sag or temporary voltage rise i.e. swell or absolute loss of voltage which is known as interruptions.

These are classified as:-

- Ø Sag
- Ø Swell
- Ø Interruptions

2.1.3.1 Sag

The American "sag" and the British "dip" are both names for a decrease in voltage to between 10% and 90% of nominal voltage for one half cycle to one minute .Sags account for the vast majority of power problems experienced by end users. They can be generated both internally and externally from an end users facility. Sags coming from the utility have a variety of causes including lightning, animal and human activity and abnormal utility equipment operation.

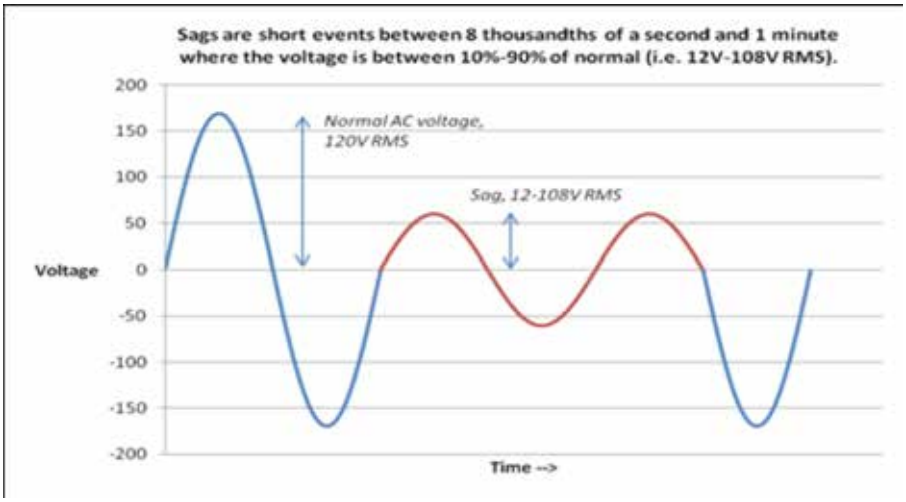


Figure-2: Sags are Short Events Between 8 Thousandths of a Second and 1 Minute Where The Voltage is Between 10%-90% of Normal

2.1.3.2 Swell

A swell is the opposite of a sag an increase in voltage above 110% of nominal for one half cycle to one minute. Although swells occur infrequently when compared to sags, they can cause equipment malfunction and premature wear. Swells can be caused by shutting off loads or switching capacitor banks on.

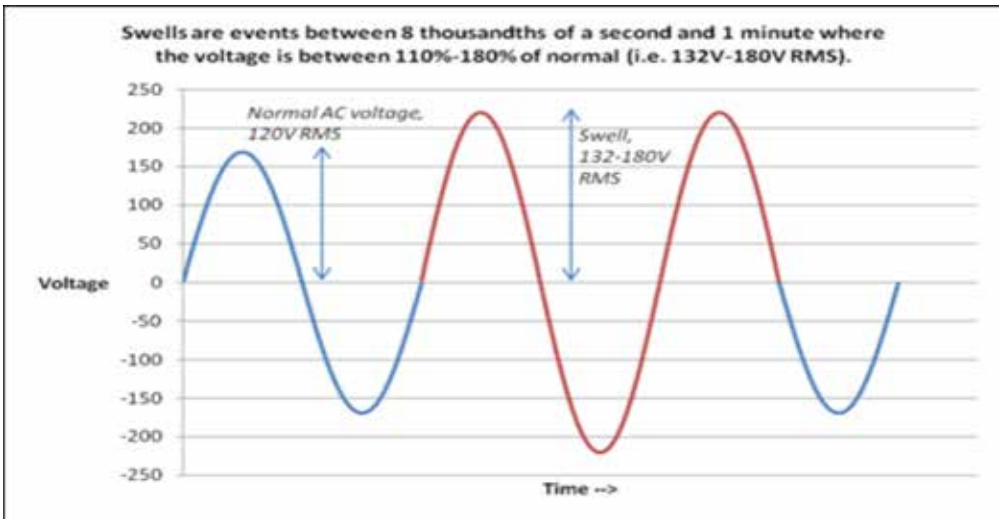


Figure 3:Swells are Event Between 8th Thousandth of a Second and 1 Minute Where The Voltage is Between 110%-180% of Normal

2.1.3.3 Interruptions

When the voltage drops below 10% of its nominal value it is called an interruption or a blackout. Interruptions have three classifications:-

Momentary (lasting 30 cycles to 3 seconds)

Temporary (lasting 3 seconds to 1 minute)

Sustained (lasting more than one minute)

Although interruptions are the most severe form of power problem, they are also the least likely to occur. Voltage sags are often mistaken for an interruption because equipment shuts down or lightening goes off since the voltage dropped below the point that these devices can operate. Where sags and under voltage typically represent more than 92% of power problem events, interruptions represent less than 4% of such problems.

2.2 STEADY STATE PHENOMENA

2.2.1 Waveform Distortion

This is defined as a steady state deviation from an ideal sine wave of power frequency There are five types of waveform distortion:-

- Ø DC offset
- Ø Harmonics
- Ø Notching
- Ø Noise

2.2.2 Voltage Unbalance

2.2.3 Voltage Fluctuations and Flicker

2.2.4 Power Frequency Variations

III. INVESTIGATION ON POWER QUALITY PROBLEMS

Now-a-days, the customers have become more aware of the 'quality of service' of the electricity. The network operator is obliged to deliver a voltage at the customer's terminal that should remain within certain limits as specified in the national grid code or the standard. It is generally noticed that the electricity as it is produced in a conventional power plant by the utility is generally of high quality. But when it reaches the customer's terminal,

it might be distorted due to the disturbances in the transmission and distribution networks or for other reasons. Moreover, the electrical equipment's have become more complex in terms of their functionalities and the way they interact with other equipment's present in the network. Therefore, it is becoming an increasing problem for the utility to maintain good voltage quality because of the interactions of the customer's loads with the network

'Quality of service' defines the as a combination of the supply reliability, the power quality and the commercial relationship between the utility and the customer. Power quality is often considered as a combination of voltage and current quality. It is generally noticed that the network operator is responsible for voltage quality (VQ) at the point of connection (POC) while the current quality (CQ) at the POC is largely influenced by the customer's loads. These two characteristics VQ and CQ influence each other by mutual interaction that might cause distortion in the power supply at the POC.

PQ disturbances can be classified into two categories:

1) 'Continuous' or 'variation type' and

2) 'Discrete' or 'event type'.

Continuous type disturbances are present in every cycle and typically include voltage variations, unbalance, flicker and harmonics. The discrete type disturbances appear asisolated and independent events and mainly include voltage sags (sags), swells and oscillatory or impulsive transients.

IV. POWER QUALITY COMPLAINTS

Typical PQ complaints arise from the customer side when the functioning of the customer's sensitive devices (for example computers, data processing equipments, variable speed drives, electronic ballasts) is affected leading to data loss, corruption or damage of data, physical damage of sensitive devices, flickering of computer screens, or complete loss of the power supply. From various national and local surveys in the India and other countries like USA, it was found that about 70% of PQ disturbances at the POC are caused by the customers themselves or their neighbours due to the operation of the devices at their premises while the other 30% of PQ problems are originated from the network side because of natural events or other reasons. These results concluded that voltage sags (dips) andswells, transient over-voltages (due to capacitor switching), harmonics and grounding related problems are presented in Fig. 4

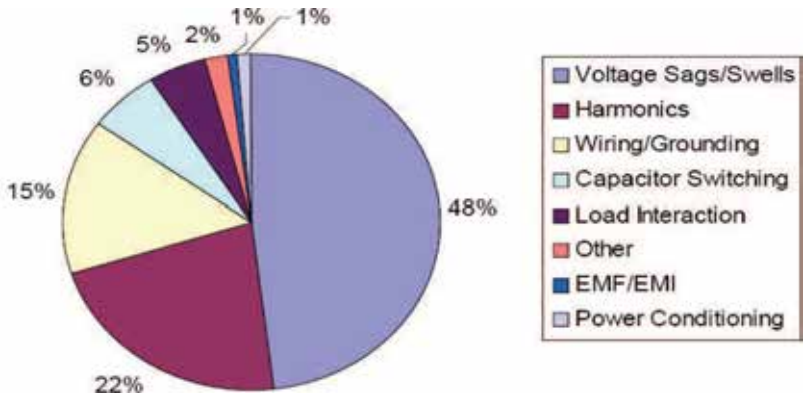


Figure: 4 PQ Problems Experienced by the Customers

V. POSSIBLE CAUSES OF POWER QUALITY PROBLEMS

The frequency of PQ disturbances and their associated problems depend on many factors such as: the type of customer and the equipment under use, the topology and length of the electric lines supplying the customers and

the geographical area. The number and severity of PQ problems varies with climate conditions, operating practicesand the behaviours of the load.

Various circumstances that causePQ problems are as follows:

- Natural phenomena that leads to system disturbances. It can be due to the weather (e.g. storm, lightning etc.) and animal activity.
- Normal utility operations that include capacitor and load switching which cause transients in the power system operation.
- Neighbouring customers who are connected to the same or adjacent feeder of the network might cause PQ problems due to the operation of large or periodic high demand loads.
- The operation of customer's sensitive loads which have nonlinear behaviour and produce current harmonics in their operations. The current harmonics in combination with the network impedances produce distortions

VI. EFFECTS OF POOR POWER QUALITY

The effect of poor PQ on the electrical equipment varies from component to component. Each type of sensitive electronic equipment differs in the amount and intensities of electrical stress that it can tolerate before failing. The critical factors that determine the tolerances of the equipment are as follows:

- the nature, magnitude and duration of the PQ event
- the frequency of the event
- the sensitivity of the component to the event
- the location of the equipment within the customer's installations
- the age of the component

VII. TECHNICAL IMPACTS OF POOR POWER QUALITY

Two distinct methods of measuring the economic impact of poor PQ have been identified.

- The first method is the direct method which is an analytical approach to consider the probabilities and impacts of the events. This method leads to a precise answer about the cost of a PQ event but it is often difficult to obtain correct input values.
- The second method is an indirect method which considers historical data for analysis and the customer's willingness to pay in solving PQ problem.

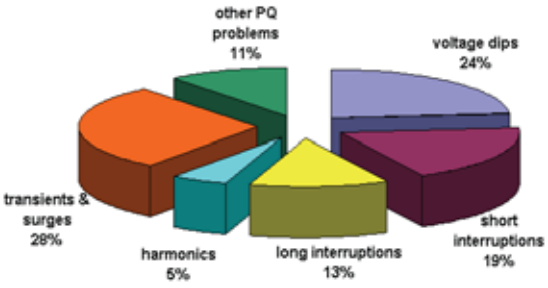


Fig. 5: Percentage Share of PQ and Interruption Costs

The survey was done over two years period among 62companies from different industries and service sectors. It was found that 90% of the totalfinancial losses are accounted to the industries. Fig. 5 shows the percentage shares of totalfinancial losses on various PQ aspects. It shows that 56% of total financial loss is a result of

voltage dips and interruptions, while 28% of the costsare due to transients and surges. Other financial losses (16%) are because of harmonics,flicker, earthing and EMC related problems.

VIII. ECONOMIC IMPACT OF POWER QUALITY

The cost related to a PQ disturbance can be divided in

i) Direct costs: the cost that can be directly attributed to the disturbance. Include the damage and the equipment, loss of production, loss of raw material, restart cost etc.

ii) Indirect costs: These costs are very hard to evaluate. Investments to prevent PQ problemsmay be considered an indirect cost.

iii) Non material inconvenience: some inconvenience due to power disturbance cannot beexpressed in money, such as not listening to the radio or not watching TV. The only way toaccount is to establish an amount of money that the consumer is willing to pay to avoid thisinconvenience.

IX. METHODS FOR POWER QUALITY PROBLEMS CORRECTION

Correction methods include the following:

- Proper designing of the Load equipment.
- Application of passive, active and hybrid harmonic filters.
- Proper designing of the power supply system
- Application of voltage compensators.
- Use of uninterruptible power supplies (UPSs)
- Reliability on standby power

X. CONCLUSION

- Power quality maintenance is an important aspect in the economic operation of the system
- Various PQ problems may lead to another undesirable problems

REFERENCES

[1]. Third EditionBhim Singh, Kamal Al-Haddad, Senior Member, IEEE, and Ambrish Chandra, Member, IEEE(1999) “A Review of Active Filters for Power Quality Improvement “IEEE Transactions Industrial Electronics , VOL. 46, NO. 5, OCTOBER 1999.

[2]. Adil M. Al, -Zamil, Member, IEEE, and David A. Torrey, Member, IEEE(2001), “A Passive Series, Active Shunt Filter for High Power Applications”, Transactions of Power Electronics, Vol. 16 NO. 1, 2001.

[3]. C. NaliniKiran, SubhransuSekhar Dash, S.PremaLatha (2011)“A Few Aspects of Power Quality Improvement Using Shunt Active Power Filter” International Journal of Scientific & Engineering Research Volume 2, Issue 5, May-2011 .

[4]. Jinn-Chang , Hurng-Liahng , Kuen-Der , Hsin-Hsing Hsiao (2012), “Three-phase four- wire hybrid power filter using a smaller power converter” Electric Power Systems Research 87 (2012)

[5]. Mark F,Roger C.[2012] “Electrical Power System Quality” Tata McGraw-Hill

 ISBN: 978-81-931039-3-7

CRITERIA OF ARTIFICIAL NEURAL NETWORK IN RECONITION OF PATTERN AND IMAGE AND ITS INFORMATION PROCESSING METHODOLOGY

Khagesh Kumar Dewangan[1], Naresh Kumar Dewangan[2], Purushottam Patel[3]

[1,2,]Student Bachelor of Engg. [3] Faculties Bachelor of Engg. (Computer Science Engg.)
Kirodimal Institute of Technology Raigarh (C.G.) (India)

ABSTRACT

An Artificial Neural Network (ANN) is a biological implementation of neuron. Neurons are information processing unit that is inspired by the way biological nervous systems, such as the brain, process information. The key element of this paradigm is the novel structure of the information processing system. In last few years neural network (NN) technique has been applied to a variety of real word problem. For example speech generation and recognition, vision and robotics, hand written character recognition, medical diagnostic and game playing. This paper is describes techniques of Artificial Neural Network (ANN) in pattern recognition and image recognition and also gives a methodology about information of Artificial Neural Network (ANN).

Keywords: Pattern Recognition, Image Recognition, Artificial Neural Network (ANN)

I. INTRODUCTION

Pattern recognition is the study of how machines can observe the environment, learn to distinguish patterns of interest from their background, and make sound and reasonable decisions about the categories of the patterns. In spite of almost 50 years of research, design of a general purpose machine pattern recognizer remains an elusive goal. The best pattern recognizers in most instances are humans, yet we do not understand how humans recognize patterns. [1] The main characteristics of neural networks are that they have the ability to learn complex nonlinear input-output relationships, use sequential training procedures, and adapt themselves to the data. The most commonly used family of neural networks for pattern classification tasks [2] is the feed-forward network, which includes multilayer perceptron and Radial-Basis Function (RBF) networks. Artificial neural networks (ANNs) provide a new suite of nonlinear algorithms for feature extraction (using hidden layers) and classification (e.g., multilayer perceptrons). In addition, existing feature extraction and classification algorithms can also be mapped on neural network architectures for efficient (hardware) implementation. Image pre-processing is the technique of enhancing data images prior to computational processing. Preprocessing is the first phase of document analysis. The purpose of preprocessing is to improve the quality of the image being processed. It makes the subsequent phases of image processing like recognition of characters easier. Image preprocessing methods use the considerable redundancy in images. This paper also shows that how the use of artificial neural network simplifies development of a character recognition application, while achieving highest quality of recognition and good performance one of the most classical applications of the Artificial Neural Network is the Character Recognition System. [4]

II. PATTERN RECOGNITION

The recognition problem here is being posed as a classification or categorization task, where the classes are either defined by the system designer (in supervised classification) or are learned based on the similarity of patterns (in unsupervised classification).These applications include data mining (identifying a "pattern", e.g., correlation, or an outlier in millions of multidimensional patterns), document classification (efficiently searching text documents), financial forecasting, organization and retrieval of multimedia databases, and biometrics. The most commonly used family of neural networks for pattern classification tasks [2] is the feed-forward network, which includes multilayer perceptron and Radial-Basis Function (RBF) networks. Another popular network is the Self-Organizing Map (SOM), or Kohonen-Network [3], which is mainly used for data clustering and feature mapping. The learning process involves updating network architecture and connection weights so that a network can efficiently perform a specific classification/clustering task. The increasing popularity of neural network models to solve pattern recognition problems has been primarily due to their seemingly low dependence on domain-specific knowledge and due to the availability of efficient learning algorithms for practitioners to use. Interactive Voice Response (IVR) with pattern recognition based on Neural Networks was proposed by Syed Ayaz Ali Shah, Azzam ul Asar and S.F. Shaukat [5] for the first time in 2009. In this case, after entering the correct password the user is asked to input his voice sample which is used to verify his identity. The addition of voice pattern recognition in the authentication process can potentially further enhance the security level. The developed system is fully compliant with landline phone system. The results are promising based on false accept and false reject criteria offering quick response time. It can potentially play an effective role in the existing authentication techniques used for identity verification to access secured services through telephone or similar media. Over here speaker specific features are extracted using Mel Frequency Cepstral Coefficient (MFCC) while Multi Layer Perceptron (MLP) is used for feature matching. Our model is based on 8 kHz, 8 bit format using Pulse Code Modulation (PCM). At highest level, all speaker recognition systems contain two modules: Feature Extraction and Feature Matching. Similarly they operate in two modes: Training and Recognition/Testing modes. Both training and recognition modes include Feature Extraction and Feature Matching. In training mode speaker models are created for database. In this mode, useful features from speech signal are extracted and model is trained. The objective of the model is generalization of the speaker's voice beyond the training material so that any unknown speech signal can be classified as intended speaker or imposter. Inrecognition mode, system makes decision about the unknown speaker's identity claim. In this mode features are extracted from the speech signal of the unknown speaker using the same technique as in the training mode. Finally decision is made based on the similarity score. For speaker verification, the decision is either accepted or rejected for the identity claim. Two types of errors occur in speaker verification system- False Reject (FR) and False Accept (FA). When a true speaker is rejected by the speaker recognition system, it is called FR. Similarly FA occurs when imposter is recognized as a true speaker. Neural networks learn complex mappings between inputs and outputs and are particularly useful when the underlying statistics of the considered tasks are not well understood. Neural Networks being relatively new approach is investigated in this proposed solution. In this technique, a feed forward back propagation network is used for classification of speakers. The network is trained with the training sets extracted from the input speech by using MFCC technique of feature extraction. The model developed is a text-independent speaker verification system which can identify only a specific speaker based on his voice and rejects the claim of any other speaker.[5] Multilayer Perceptron (MLP) having four layers comprising of one input layer, two hidden layers and one output layer has been used. The

input layer has nineteen (19) neurons (as there are nineteen feature vectors from MFCC processor) and uses linear transfer function. The output layer has one neuron (as binary decision is to be made) and uses linear transfer function. It is trained using back propagation algorithm. The network is trained by using a built in train function .This function trains the network on training data (Supervised Learning). A three-layer feed forward neural network is typically composed of one input layer, one output layer and one hidden layers. In the input layer, each neuron corresponds to a feature; while in the output layer, each neuron corresponds to a predefined pattern. The best situation is that once a certain sample is input into the network, the output will be a vector with all elements as zero only except the one corresponding to the pattern that the sample belongs to.

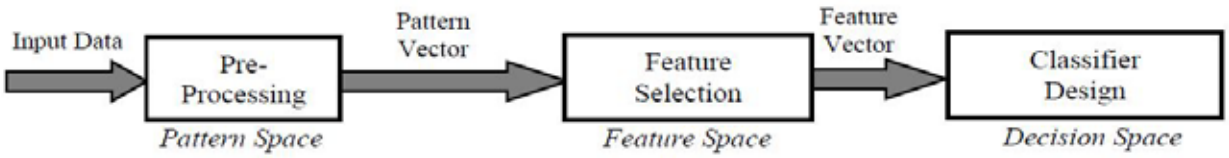


Fig 1:- Block Diagram of Pattern Recognition System

III. IMAGE RECOGNITION

This section will explain the proposed algorithm, i.e. what are different steps involve achieving in Image Preprocessing on Character Recognition Using Neural Network. In first step optical scanners are used, which generally consist of a transport mechanism plus a sensing device that converts light intensity into gray levels, through the scanning process a digital image of the original document is captured.

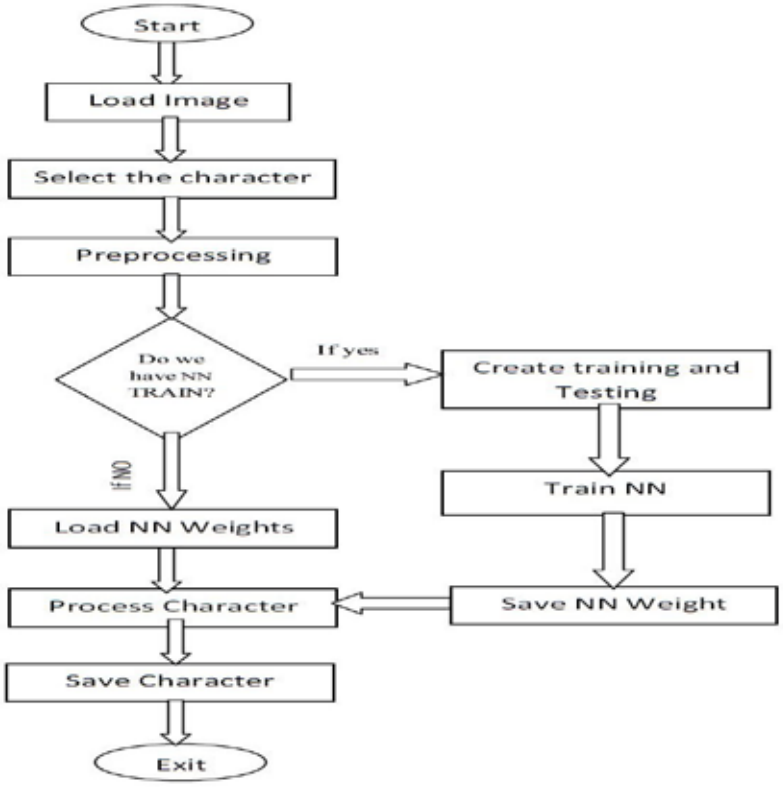


Fig 2:- Image Recognition Flowchart

The image resulting from the scanning process may contain a certain amount of noise due to defected medium or by others. In the second step describe implementation of preprocessing technique by loading the image. The

algorithm requires three major steps that define the system working theory and reason to behind their implementation.1) Image preprocessing 2) Neural network recognition 3) Back propagation Algorithm.[6]

3.1 Necr – Neural-Based Emotional Content Retrieval System

As we have mentioned above, the research investigates the feasibility of use of visual features for the retrieval of emotional content of images and tests feasibility of training ANN to accomplish classification task. To achieve this goal, a prototype system has been designed and implemented. In below system in order to test an influence of the visual feature descriptors on an ability to recognize the emotional content of images and to find similar images, we have considered three various groups of emotion classification:

• positive-negative with neutral option,

• groups of adjectives:

– warm, cold, neutral,

– dynamic, static, neutral,

– heavy, light, neutral,

– artificial, natural; to distinguish between photos and hand-made pictures,

• 5 basic emotions (happiness, sadness, anger, disgust and fear).[7]

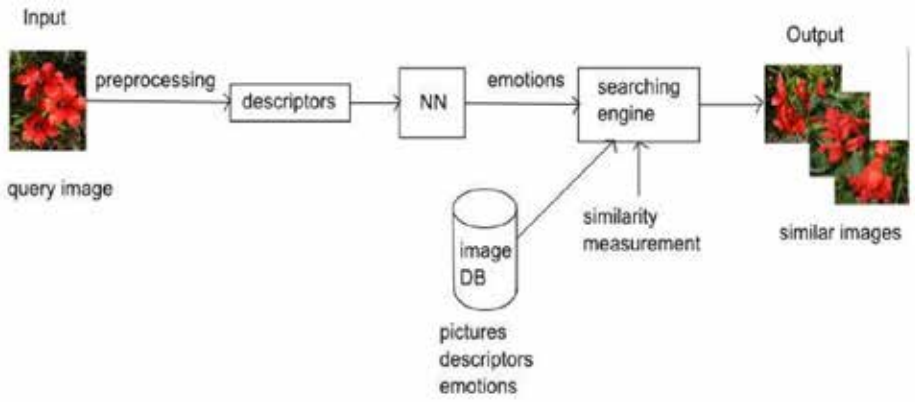


Fig 3:- Nuclear Based Emotional Contain Retrieval System

3.2 Back Propagation Algorithm in a Real Plane

Back propagation algorithm has been used extensively in neuron models. This algorithm is a development from the simple Delta rule in which extra hidden layers (layers additional to the input and output layers, not connected externally) are added. The network topology is constrained to be feed forward or loop-free - generally connections are allowed from the input layer to the first hidden layer; from the first hidden layer to the second and from the last hidden layer to the output layer. In a typical back propagation network, the hidden layer learns to recode (or to provide a representation for) the inputs. More than one hidden layer can be used. The architecture is more powerful than single-layer networks: it can be shown that any mapping can be learned, given two hidden layers (of units). The units are a little more complex than those in the original perceptron. Their input/ output graph is shown above. As a function:

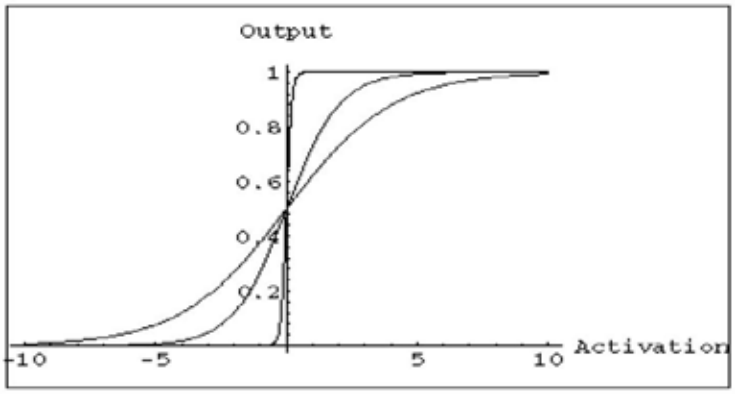


Fig 4:- Input/ Output Graph of a Back-Propagation Unit

$$Y=1 / (1 + e^{(-k.(\sum w \text{ in } * \text{ in}))})$$

The graph shows the output for *k=0.5, 1, and 10,* as the activation varies from -10 to 10.[8]

3.3 Methodology

The images were gathered to first train the neural network. Some of the images on which we trained our NN have been displayed above. Each image was read as a 2D array of pixel intensities for ORL database. Now the images read were converted to grayscale if they were in RGB format. Then masking was performed on the images. The grayscale images were masked off using a mast, an elliptical mask. This helped in extracting the oval face of a person and also removing the unnecessary background images.

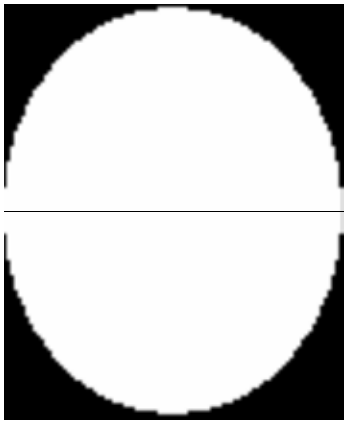


Fig 5:- Mask Used to Extract the Face

All these masked images were of resolution 92*112 so we resize them to 30*30 using the bilinear interpolation method with no filter. The resized images were then used to calculate the complex eigenvalues of the respective images. Thus the image of size 30*30 gives an array of eigenvalues of size 30. These 30 complex values are used as inputs to the complex Back propagation algorithm. The network uses complex weights and has 30 complex inputs and one output (complex). Then the network was trained for a given complex value for a given person.

3.4 Face Recognition System Using Image Processing and Neural Networks

Face recognition has become a very active area of research in recent years mainly due to increasing security demands and its potential commercial and law enforcement applications. with emphasis on such applications as human-computer interaction (HCI), biometric analysis, content-based coding of images and videos, and surveillance[9].

In their survey, they describe a preprocessing step that attempts to identify pixels associated with skin independently of facerelated features. This approach represents a dramatic reduction in computational requirements over previous methods.

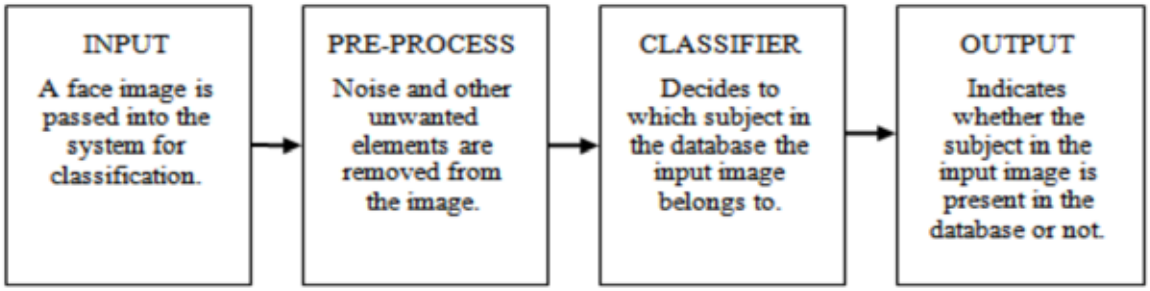


Fig 6:- Generic Representation of a Face Recognition System

The recognition stage typically uses an intensity (grayscale) representation of the image compressed by the 2D-DCT for further processing [9]. This grayscale version contains intensity values for skin pixels.

IV. INFORMATION PROCESSING METHODOLOGY IN AAN

The study of the human brain is thousands of years old. With the advent of modern electronics, it was only natural to try to harness this thinking process. The first step toward artificial neural networks came in 1943 when Warren McCulloch, a neurophysiologist, and a young mathematician, Walter Pitts, wrote a paper on how neurons might work. They modeled a simple neural network with electrical circuits. Neural networks, with their remarkable ability to derive meaning from complicated or imprecise data, can be used to extract patterns and detect trends that are too complex to be noticed by either humans or other computer techniques. A trained neural network can be thought of as an "expert" in the category of information it has been given to analyse. Other advantages include:

1. Adaptive learning: An ability to learn how to do tasks based on the data given for training or initial experience.
2. Self-Organisation: An ANN can create its own organisation or representation of the information it receives during learning time.
3. Real Time Operation: ANN computations may be carried out in parallel, and special hardware devices are being designed and manufactured which take advantage of this capability.
4. Fault Tolerance via Redundant Information Coding: Partial destruction of a network leads to the corresponding degradation of performance. However, some network capabilities may be retained even with major network damage. [10]

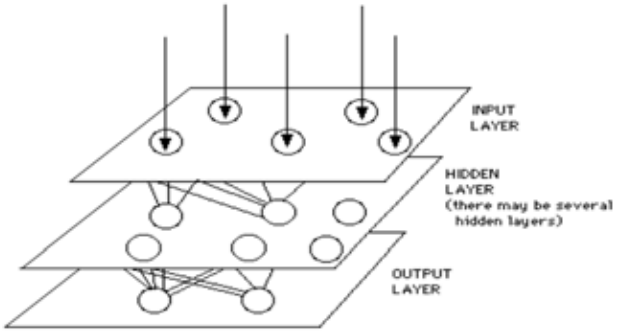


Fig 7:- A Simple Neural Network Diagram

Artificial neural networks have a similar structure or topology as shown in Figure1. In that structure some of the neurons interface to the real world to receive its inputs. Other neurons provide the real world with the network's outputs. This output might be the particular character that the network thinks that it has scanned or the particular image it thinks is being viewed. All the rest of the neurons are hidden from view.

Another type of connection is feedback. This is where the output of one layer routes back to a previous layer. An example of this is shown in Figure 8.

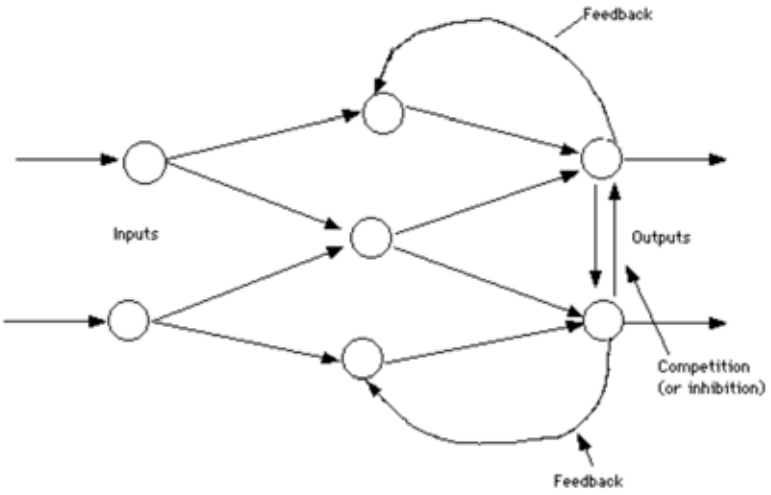


Fig 8:- Simple Network with Feedback and Competition.

4.1Biological Model of Neural Network

The brain and nervous system are enormously complex. The brain itself is composed of billions of nerve cells. The orchestration of all of these cells to allow people to sing, dance, write, talk, and think. Neuroscientist [11] calls the brain the *great integrator*. The brain does a wonderful job of pulling information together. The brain integrates all functions of the world including sounds, sights, touch, taste, genes and environment. Neurons are the nerve cells that actually handle the information processing function. The human brain contains about 100 billion neurons. The

average neuron is as complex as a small computer and has as many as 10,000 physical connections with other cells.

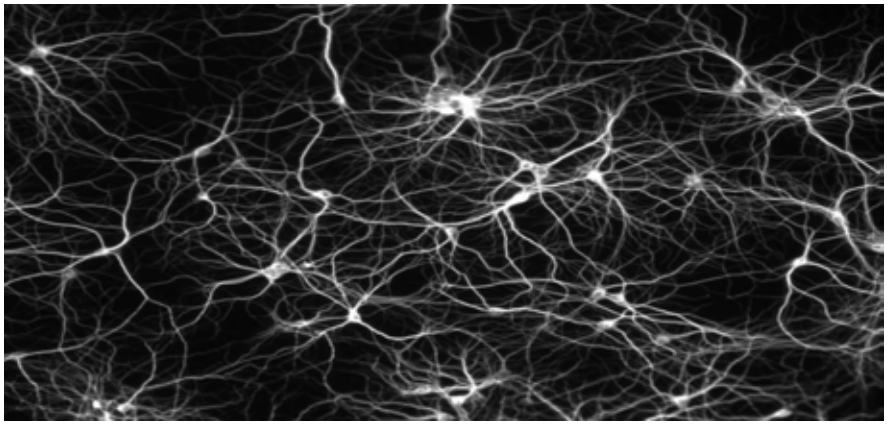


Fig 9:- Neural Network in Human Body

A neuron is a special biological cell that process information from one neuron to another neuron with the help of some electrical and chemical change. It is composed of a cell body or soma and two types of out reaching tree

like branches: the axon and the dendrites. The cell body has a nucleus that contains information about hereditary traits and plasma that holds the molecular equipments or producing material needed by the neurons *[12]*. The whole process of receiving and sending signals is done in particular manner like a neuron receives signals from other neuron through dendrites. The Neuron send signals at spikes of electrical activity through a long thin stand known as an axon and an axon splits this signals through synapse and send it to the other neurons *[13]*.

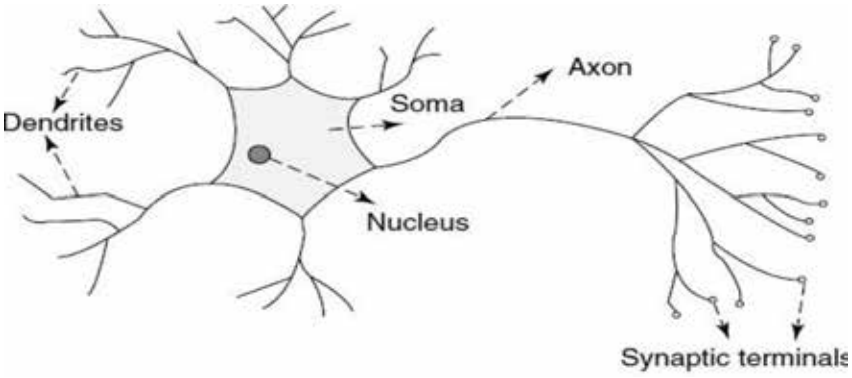


Fig 10:- Biological Model of Neuron.

V. CONCLUSION

The computing world has a lot to gain or benefits from neural networks approaches. Their ability to learn by example makes them very flexible and powerful. An approach has been made to increase the accuracy of recognition of handwritten scanned character. The neural networks can be used for image preprocessing pretty well with many advantages over normal image preprocessing methods. At last in this paper biological model of neuron is gives working principle of ANN (Artificial Neural Network).

VI. ACKNOWLEDGMENT

We would like to thank all the persons involved in paper directly or indirectly. This is a fruitful way of work and hereby all the authors are equally responsible for the paper. We express our gratitude towards various authors of different study materials from which references has been taken.

REFRENCES

[1] P.E. Ross, “Flash of Genius”, Forbes, pp. 98-104, Nov, 1998.

[2] A.K. Jain, J. Mao, and K.M. Mohiuddin, “Artificial Neural Networks: A Tutorial”, Computer, pp. 31-44, Mar, 1996.

[3] T.Kohonen, “Self-Organizing Maps”, Springer Series in Information Sciences, Berlin, vol.30,1995.

[4] NOHAJ, Miroslav, and Rudolf JAKŠA. "Image preprocessing for optical character recognition using neural networks." Prediction of multidimensional economic data in Civilization computer game.... 30 Dávid Chochol, Ing. Rudolf Jakša, PhD. Construction of self learning system able to recognize visual information..... 44 Jozef ˇCorba, prof. Ing. Peter Sincák, CSc. Multiagent Adaptive Fuzzy Control of LEGO Robots..... 64.

[5] Syed Ayaz Ali Shah, Azzam ul Asar and S.F. Shaukat, “Neural Network Solution for Secure Interactive Voice Response”, World Applied Sciences Journal 6 (9), 1264-1269, 2009.

[6] Hong, Weibin, Wei Chen, and Rui Zhang. "The Application of Neural Network in the Technology of Image Processing." Proceedings of the International MultiConference of Engineers and Computer Scientists. Vol. 1. 2009.

[7] Y. Kim, Y. Shin, Y. Kim, E. Kim, and H. Shin, “Ebir: Emotion-based image retrieval,” in Digest of Technical Papers International Conference on Consumer Electronics, 2009, pp. 1–2.

[8] Lipmann R. P., “An introduction to computing with neural nets”, IEEE Acoustic, Speech and Signal Processing Magzine, pp. 4-22, April 1987.

[9] A. Abdallah, M. Abou El-Nasr, and A. Lynn Abbott, “A New Face Detection Technique using 2D DCT Self Organizing Feature Map” in Proc. of World Academy of Science, Engineering and Technology, Vol. 21, May 2007, pp. 15-19.

[10] Bradshaw, J.A., Carden, K.J., Riordan, D., 1991. Ecological ―Applications using a Novel Expert System Shell‖. Comp. Appl. Biosci. 7, 79–83.

[11] John W. Santrock, University of Texas, Dallas, 2005, Psychology, 7th Edition, ISBN: 0072937769 Published by McGraw-Hill, Chapter 3, Biological foundations of behaviors, pp 76-115.

[12] Anil K Jain, Jianchang Mao and K.M Mohiuddin, “Artificial Neural Networks: A Tutorial”, Michigan State University, 1996.

[13] Christos Stergiou and Dimitrios Siganos, “Neural Networks”. [8] Limitations and Disadvantages of Neural Network from website http://www.ncbi.nlm.nih.gov/pubmed/8892489

 ISBN: 978-81-931039-3-7

A REVIEW DIFFERENT APPROACH FOR ANAPHORA RESOLUTION

Md.Safdar[1], Dr. Md.Jawed Ikbal Khan[2], Pervez Hussain[3]

[1]*Research Scholar, Inst. of Information Sciences & IT M. U. Bodh-Gaya, Gaya, Bihar, (India)*

[2]*Assistant Professor, Mirza Ghalib College, Gaya, Bihar, (India)*

[3]*Faculty, Management Department, IGNOU, New Delhi, (India)*

ABSTRACT

A huge numbers of feature words appear as noun phrases in review sentences are referenced by anaphoric pronouns present in the review document. Anaphora resolution is a rich source of natural language processing (NLP) task that contains of determining which mentions in a discourse refer to the same entity or event. These are consists of noun phrases (NP), named entities (NEs), embedded nouns, and pronouns. It challenges to decide noun phrase coreference, anaphora and their associating relations. It has implemented some of the state-of-the-art approaches in the area of machine learning approaches to anaphora resolution, particularly the position and the joint anaphor identification with the antecedent selection. This is a survey for anaphora resolution using different approaches and their good selection of feature for noun phrases.

Keywords: Anaphora Resolution, Approached For Anaphora Resolution

I. INTRODUCTION

Currently a day available large datasets from merchandise web sites, they consist of a numerical or text file and they can be structured, semi-structured or non-structured. It has been used methods and techniques to apply extract useful information from these data sets. The various different information retrieve techniques and tools have been proposed according to different data types. Sentiment analysis is, also known as opinion mining, is to identify and extract subjective information in the review document, which can be *positive, neutral, or negative* [1,2]. Using appropriate mechanisms and techniques, this vast amount of data can be processed into information to support operational, managerial, and strategic decision making. A sentiment analysis have classified into two task– identifying whether the text is subjective or objective, and detecting whether the subjective text is positive or negative. Anaphora resolution is the difficulty of finding the reference of a noun phrase. This noun phrase can be a fully specified NP (definite or indefinite), a pronoun, a demonstrative or a reflexive. Typically this problem can be divided into two parts –

a) Finding the co-reference of a full NP.
b) Finding the reference of a pronoun or reflexive.

In above sentence (a), are commonly denoted to as co-reference resolution and sentence (b), are commonly denoted to as anaphora resolution. NLP provide presenters with a range of ways to refer to entities. Two referring expressions that are used to refer to the same real-world entity are said to corefer. Reference to an entity that has been previously introduced into the discourse is called anaphora. Anaphor is the referring expression and the entity to which it refers is its antecedent. An anaphora and all its antecedents form a

coreference sequence called coreferential chain. The term anaphora denotes the act of referring, whereas the word that actually does the referring is sometimes called an anaphor (or cataphor). The term anaphora is used into two important tasks i.e. *Anaphora* and *Cataphora*. Firstly, an anaphora it denotes the act of referring a noun phrases. Which is given expression denotes to another related entity, anaphora is existent. Secondly, Cataphora, which act of referring pointing to the right. A cataphor when it points to its right toward its postcedent. Both effects together are called *endophora*.

a) It does take pictures in low light as it uses the flash.

b) It's small and compact enough to fit in your pocket to take with you anywhere you go.

In above sentences has been saw review documents in digital camera, large numbers of feature words explicitly present as noun phrases review sentences are referenced by anaphoric pronouns present in next sentences of a review document. For example, anaphora words '*It*' in sentence basically referring to the product feature *pictures* of the sentence another sentence is reference *small* and *compact*.

II. FEATURE SELECTION

The feature selection for anaphora resolution consists of 12 features;

- There were 5 features which indicated the type of noun phrase- definite NP, demonstrative, pronouns, or proper names.
- They had a distance feature, which captured the distance between an anaphoric NP and its coreferrent.
- Number agreement
- Gender Agreement
- Semantic class agreement which included basic and limited semantic classes such as male, female, person, organization, location, date, time, money,etc.
- Features for identification of Proper names such as alias feature, proper-name feature, etc.
- Appositive Feature

III REVIEW LITRETURE

In paper [3], authors presented the machine learning approach to resolve the pronominal anaphora resolution for opinion mining. They have used 16 feature attributes divided into three categories: 1. *Anaphoric Pronoun*, 2. *Antecedent Candidate*, 3. *Relation Feature*.

In anaphoric features are:

F1 - dec_ana	: Declension case of anaphora.
F2 – sf_ana	: Syntactic function of anaphora.
F3 – phrase_ana	: Whether the anaphor has the phrase tag or not.
F4 – num_ana	: Number of anaphor.

In antecedent candidate are:

F5 - word	: Word of antecedent
F6 - lemma	: Lemma of antecedent
F7 – cat_np	: Syntactic category of NP
F8 – dec_np	: Declension case of NP
F9 – num_np	: Number of NP

F10 – Degree : Degree of the NP that contains a comparative

F11 – np : Whether the noun phrase is a simple NP or a com posed NP.

F12 – sf_np : Syntactic function of NP.

F13 – enti_np : Type of entity.

In relation Feature is:

F14 _ dist : the distance between the anaphor or noun phrase.

F15 _ same_sent : if the anaphor are present in same sentences.

F16 _ same_num : whether is singular and plural number?

They used a corpus of 50,000 words containing 249 pronominal anaphora's for experimental purpose, which is quite small. For implementation [4] toolkit is used, and various machine learning techniques such as SVM, Multi layer Perceptron, Naïve Bayes, k–NN (k = 1), Random Forest (RF), NB-Tree and Voting Feature Interval are used with 10 fold cross validation. Experimental result shows that highest precision i.e. 0.803 is observed using SVM, whereas, highest recall and f-measure values i.e. 0.702, and 0.683 is obtained using RF.

In [5], authors proposed machine learning technique**,** opinion can be classified into two categories: the document classification approach and the information extraction approach. In the document classification approach orientation such as positive or negative entity. And information extraction approach, the task of extracting the elements which constitute opinions. In [3] Turney, P. D. (2002, July) Opinion extractions are triplet form i.e. Subject, Aspect, Evaluation.

- *Subject:* Subject is a specific entity of the given class. Such as product name, service name, person name, organization name.
- *Aspect*: Aspect has been used to physical parts, (engine and tire, interior) attributes (size, colour, design and performance) and related object (manufacture and dealer).
- *Evaluation*: It has been used evaluation on the subject. Such as good, high, excellent, poor. They used automobile domain with 4,442 sentences for experimental purpose. They contain 2,191 evaluations with explicit aspect and 420 evaluations without an explicit aspect. The proposed models achieve result nearly 0.8 precision and 0.7 recalls.

In noted [6], authors presented weakness in the area of anaphora resolution and proposed workbench Mitkov, R. (2000) [7]. It has been used pre-processing tool. Experiment is generated by running an XML parser, this list consists of a record containing:

- *A word form*
- *The lemma of word or of the head of the noun phrase.*
- *The starting position in the text.*
- *The ending position in the text.*
- *The part of speech*
- *The grammatical function*
- *The index of the sentences that contains the referent*
- *The index of the verb whose argument this referent is.*

An author has been proposed three approaches: Kennedy and Bogurev [8, 9] the extraction of pronoun resolution they are mainly reflexive and possessives. CogNiac [10] author stated that resolve only those anaphora satisfying very high confidence rules and ambiguous antecedents are left unresolved in order to obtain

high precision. Author reported that the performance of CogNiac remain good during extraction of opinion targets referenced by personal pronouns. However, the algorithm does not yield high precision when resolving impersonal and demonstrative pronouns Mitkov's approach [7] is a best technique for anaphora resolution extraction of texts which has been applied indicators for antecedent. Which boosting indicator assigns a positive score to a NP, reflective a positive like hood that it is the antecedent of the current pronoun? Other hand negative score to a NP, reflective a lack of confidence that it is the antecedent of the current pronoun. Using score is calculated based on these indicators and their referent with the highest aggregate value is selected as antecedent. Author has been used experiment on corpus contains 28,272 words with 19,305 noun phrases and 422 pronouns out of which 362 are anaphoric found in the texts review was 56.9% for Mitkov's method, 49.72% for CogNiac and rest 61.6% for Kennedy and Boguraev's method. In [10], authors presented a machine learning approach for resolving other-anaphora. Feature set (F1) are proposed to compare string in review sentences and extract syntactic feature. These feature extractions using WordNet Fellbaum, C. [13] and Name Entity (NE) Recognition algorithm. They proposed Weka ML library [14]. The training data was generated procedure produced a set of 3,084 antecedent-anaphor pairs, of which 500 data were used positive instances and rest negative training instances are paired of anaphors, used with 10 fold cross validation.

Following 9 features are used:

- *NP_FORM*: Surface form (for all NPs), such as definite, indefinite, demonstrative, pronoun etc.
- *RESTR_SUBSTR*: does lemmatized antecedent string contain lemmatized anaphor string, yes or no.
- *GRAM_FUNCTION*: Grammatical role (for all NPs), subject, object, unknown.
- *SYN_PAR*: Anaphor antecedent with respect to grammatical function, yes, no.
- *SDIST*: Distance between anaphor and antecedent.1, 2,3,4,5…
- *SEMCLASS*: Semantic class (for all NPs), person, organization, location, date, money, number, things, abstract, unknown.
- *SEMCLASS_AGR*: Anaphor antecedent agreement with respect to semantic class, yes or no.
- *GENDER_AGR*: Anaphor antecedent agreement with respect to gender. Same, compatible, incompatible, unknown.
- *RELATION*: Type of relation between anaphor and antecedent. Same predicate, compatible, incompatible, unknown.

Using Naïve Bayes classifier, authors have compared their result with baseline. The extracted values for precision, recall and F-score was observed as 51.7, 40.6 and 45.5 respectively for the F1 features. Whereas, in case of baseline all the three values remain same as 27.8.

IV. APPROACHES FOR ANAPHORA RESOLUTION

NLP tools like part of speech taggers and development of machine learning. These approaches are divided into four categories; *Rule based approaches, Corpus Based Approaches, Knowledge-Poor Approaches, and Discourse Based Approaches;*

4.1. Kennedy and Boguraev

The extraction of pronoun resolution they are mainly personal pronoun, reflexive and possessives. This anaphora resolution based on *Lappin and Less* approach [9] without using deep employing syntactic parsing.

The general idea of the method is to construct coreference equivalence that have an associated value based on set of ten factors [8].It is expected for this method to perform better then Baldwin's and Mitkov's approach since it achieve more syntactic information for determining disjoint reference.

4.2. Baldwin's CogNIAC

It is knowledge-poor approaches to anaphora resolution that is based on a set of rules which are applied over the pronoun. The set of rules are according to their importance and relevance to anaphora resolution. That resolve only those anaphora satisfying very high confidence rules and ambiguous antecedents are left unresolved in order to obtain high precision. The performance of CogNIAC remains good during extraction of opinion targets referenced by personal pronouns. However, the algorithm does not yield high precision when resolving impersonal and demonstrative pronoun [10].

4.3. Mitkov's Approach

A best technique for anaphora resolution extraction of texts which has been applied indicators for antecedent [7]. Which boosting indicator assigns a positive score to a NP, reflective a positive like hood that it is the antecedent of the current pronoun? Other hand negative score to a NP, reflective a lack of confidence that it is the antecedent of the current pronoun. Using score is calculated based on these indicators and their referent with the highest aggregate value is selected as antecedent. In below table.1 summary for different methods for pronoun anaphora resolution.

Methods	Algorithm's	Author's
Rules Based Approaches	Tree search algorithm	Hobb, 1978
	Shallow processing approach	Carter, 1987
	Multistrategy approach	Carbonell and Brown,1988
	Syntax based approach	Lappin and Leass, 1994
	Combination of linguistic and statistical methods	Mitkov, 1996
Corpus Based Approaches	MUC-5 system.	McCarthy and Lehnert, 1995
		Soon Ng and Lim, 2001
	Knowledge based feature	Ng and Cardie 2002
Knowledge Poor Approaches		Kennedy and Boguraev, 1996
	Robust knowledge poor approach	Mitkov, 1996-1998
	CogNIAC	Baldwin, 1997
	ROSANA	Stuckardt, 2001
Discourse Based Approaches	Centering theory	Grosz et al, 1995
		Kameyama, 1986
	BFP algorithm	Brennan et al, 1987
	S-List algorithm	Strube, 1998
	LRC algorithm	Tetreault, 2001

Table.1.Summary for Anaphora Resolution Approaches and Algorithms

V. ISSUES AND CHALLENGES

NLP in general is very difficult but after working hard on anaphora resolution we have learned that it is *particularly* difficult. We shall briefly outline several issues for anaphora resolution;

- ü It is determine to pleonastic 'it'.
- ü The pre-processing is a chain reaction: usually inaccurate POS tagging affects NP extraction which in turns affects parsing which in turns deteriorates anaphora resolution.
- ü The resolution of bridging (indirect) anaphora requires semantic or world-knowledge. The lexical or domain resources available are still insufficient.
- ü Centering and other discourse theories often rely on anaphora resolution; anaphora resolution relies on them as well.
- ü The action-noun anaphora, the verb-phrase antecedent counterpart of the regular noun-phrase.
- ü Use adjective phrases, subjects of "have" verbs and possibly other structures to obtain further attribute information

VI. EVALUATION

Precision and recall are two commonly used measures for calculating the value of results. Precision can be seen as a measure of accuracy, while recall is a measure of completeness. The sum of true positives and false positives, which are pairs incorrectly labeled as coreferent and the sum of true positives and false negatives, which are pairs which were not labeled as coreferent but should have been.

Regularly, precision and recall scores are combined into a single measure, the F-measure, which is the calculating precision and recall.

	Correct Classification	
Obtain Classification	True Positive (TP)	False Positive (FP)
	False Negative (FN)	True Negative (TN)

Fig.1. Matrix Classification of A Noun Phrase Pair and The Desired Correct Classification

These three parameters are used to calculate the value of *precision*, *recall*, and *f-score* using equations 4.1, 4.2 and 4.3, respectively.

$$precision = \frac{TP}{TP + FP} \quad (4.1)$$

$$recall = \frac{TP}{TP + FN} \quad (4.2)$$

$$F\text{ - }score = \frac{2 * precision * recall}{precision + recall} \quad (4.3)$$

VII. CONCLUSION AND FUTURE WORK

The anaphora resolution is mainly used for machine learning and rule based approach. Whereas large anaphora resolution systems did not follow a common evaluation approach, creating it challenging to difference

presentation in absolute, measurable terms, newer machine learning techniques have together the anaphora resolution problem along with the superior noun phrases co-reference problem. In our future work we have to find anaphora resolution with coreference using different machine learning techniques or classifier using Support Vector Machine (SVM), Multi-layer Perceptron (MLP), Naïve Bayes (NB), k–NN (k = 1), Random Forest (RF) and Voting Feature Interval (VFI).

REFERENCES

[1] Safdar, M., & Khan, M. J. I. Opinion Mining for Customer Feedback: A Survey, International Journal of Scientific and Engineering Studies, ISSN 2349-8869

[2] Safdar. M., Khan, M. J. I., & Daiyan. M., Mining Explicit Features for Opinion Mining of Customer Reviews**,** International Journal of Emerging Technology and Advanced Engineering (IJETAE), An ISO 9001:2008

[3] Arregi, O., Ceberio, K., de Illarraza, A. D., Goenaga, I., Sierra, B., & Zelaia, A. (2010). Determination of Features for a Machine Learning Approach to Pronominal Anaphora Resolution in Basque. Procesamiento del language natural, 45, 291-294.

[4] Written, I. H., & Frank, E. (2005). Data Mining: Practical machine learning tools and techniques. Morgan Kaufmann.

[5] Turney, P. D. (2002, July). Thumbs up or thumbs down?: semantic orientation applied to unsupervised classification of reviews. In Proceedings of the 40th annual meeting on association for computational linguistics (pp. 417-424). Association for Computational Linguistics.

[6] Kobayashi, N., Inui, K., & Matsumoto, Y. (2007, June). Extracting Aspect-Evaluation and Aspect-Of Relations in Opinion Mining. In EMNLP-CoNLL (pp. 1065-1074).

[7] Barbu, C., & Mitkov, R. (2001, July). Evaluation tool for rule-based anaphora resolution methods. In Proceedings of the 39th Annual Meeting on Association for Computational Linguistics (pp. 34-41). Association for Computational Linguistics.

[8] Mitkov, R. (2000). Towards More Comprehensive Evaluation in Anaphora Resolution. In LREC.

[9] Kennedy, C., & Boguraev, B. (1996, August). Anaphora for everyone: pronominal anaphora resolution without a parser. In Proceedings of the 16th conference on Computational linguistics-Volume 1 (pp. 113-118). Association for Computational Linguistics.

[10] Lappin, S., & Leass, H. J. (1994). An algorithm for pronominal anaphora resolution. Computational linguistics, 20(4), 535-561.

[11] Baldwin, Breck. "CogNIAC: high precision coreference with limited knowledge and linguistic resources." Proceedings of a Workshop on Operational Factors in Practical, Robust Anaphora Resolution for Unrestricted Texts. Association for Computational Linguistics, 1997.

[12] Mitkov, R. (1998, August). Robust pronoun resolution with limited knowledge. In Proceedings of the 36th Annual Meeting of the Association for Computational Linguistics and 17th International Conference on Computational Linguistics-Volume 2 (pp. 869-875). Association for Computational Linguistics.

[13] Fellbaum, C. (1998). WordNet. Blackwell Publishing Ltd.

[14] http://www.cs.waikato.ac.nz/~ml/weka/.

 ISBN: 978-81-931039-3-7

EFFECT OF SIZE ON DEBYE TEMPERATURE OF AU AND CU NANOMATERIALS

Madan Singh[1], Hlabana K.C[2], Krishna Chandra[3], Mahipal Singh[4]

[1,2]*Department of Physics and Electronics, National University of Lesotho, P.O. Roma, Lesotho (India)*

[3,4] *R.H. Govt. Post Graduate College, Kashipur, Udham Singh Nagar Uttarakhand, (India)*

ABSTRACT

By studying the surface effect, the Debye temperature of nano solids (nano particles, nano wires, nano films) has been predicted based on surface dependent cohesive energy. Nano size material shows many motivating properties that cannot be seen from their bulk equivalent. The cause for the size dependent properties of the nano materials is observed as the presence of the large fraction of the surface atoms. Because, free surface atoms experience a different environment than do atoms in the bulk of the materials. As a consequence, the energy associated with these atoms is different from that of atoms in the bulk. In this paper, on exposing the surface effect, the Debye temperature of the Au and Cu nano materials of nano sphere, nano wire and nano film has been studied based on particle size dependent cohesive energy. It is observed that Debye temperature decreases with the decrease in grain size. Furthermore, the Debye temperature increases for nano wire and nano film as compared with the spherical form of same size

Keywords: Nano Materials, Debye Temperature, Cohesive Energy

I. INTRODUCTION

When the particle size of materials transforms the nanometre scale, the electronic, magnetic, biomedical and thermodynamic properties vary noticeably as compared with its bulk counterparts [1, 2]. The important characteristics of the nano materials are its size effects. It is recognized that the size dependence of thermal stability in nano materials is increasingly becoming one of the major concerns in upcoming technologies [3]. Numerous experimental and theoretical efforts have been implemented to investigate the size-dependent cohesive energy of nano materials [4]. Size dependence of cohesive energy of W was carried out by Kim *et al.* [5]. Cohesive energy of Ag and Co nano particles is studied by Hou *et al.* [6] using computer simulations. Gold and silver at the nano scale have demonstrated many intriguing chemical and physical properties that their bulk counterparts do not have. The size dependent elastic modulus of Cu and Au thin film studied by Liang *et al.* [7] and suggested that the elastic modulus of metallic free thin films increases as the thickness of the film increases. Size dependent melting behavior of Zn nano wire using X ray diffraction and transmission electron microscopy studied by Wang *et al.* [8]. The size dependence melting temperature of Au nano material has been studied and it is shown that the melting temperature decreases as the size decreases [9]. Nano materials are inspiring since they reveal strong size and shape effect which cannot be defended by the traditional theories. Extensive theoretical and vibration of atoms.

In the present work, we report a theoretical model for studying the grain size dependent Debye temperature of Au and experimental investigations have been executed by the researchers in reviewing the special properties of nano materials [7-9] and motivating results have been obtained.

Counting these properties of nano materials, the Debye temperature of nano materials has received great attention, because it is a central physical quantity to characterize many material properties, such as phase transitions and thermal Cunano solids in different shapes such as nano particles, nano wires, and nano films with free surface. The study based on surface effect at decreased grain size, licences interpolation and extrapolation to the region for which adequate experimental data are not available. The model predictions agree well with the available experimental data.

1.2 Theoretical Formulation

The entire cohesive energy of the nano materials is due to the involvement of the surface atoms as well as the interior atoms may be listed as [10]

$$E_{total} = E_0(n - N) + \frac{1}{2}E_0 N \qquad (1)$$

Where n is the total number of atoms of nanosolids and the number of its surface atoms is N .Consequently, $(n - N)$ is the total number of interiors atoms of the nanomaterials. E_0 is the cohesive energy of the bulk materials per atom. Eq. (1) may be inscribedequally

$$E_p = E_b(1 - \frac{N}{2n}),$$

Where E_p is the cohesive energy per mole of the nanomaterials, which is given by AE_{total} / n , here, A is the Avogadro constant. E_b is defined as the cohesive energy per mole of the corresponding bulk materials which is given by $E_b = AE_0$ .The relation between the melting point of nanomaterials and bulk are reported by Qi [10] as: $T_p = T_b\left(1 - \frac{N}{2n}\right)$ (2)

One may get the connection between the melting point and the Debye temperature from the Lindemann'sproportional. According to this, a crystal will melt when the root mean square displacement of an atom exceeds a certain fraction of the interatomic distance in the crystal [11]. Connecting the specific heat theory with the Lindemann's melting formula; the characteristic temperature square is proportional to the melting point of the crystal. So, the Debye temperature for the bulk material is inscribed as [12]

$$q_{Db}^{\ 2} \mu \left(\frac{T_b}{MV^{2/3}}\right), \qquad (3)$$

Evenly for nanomaterial

$$q_{Dp}^{\ 2} \mu \left(\frac{T_p}{MV^{2/3}}\right), \qquad (4)$$

Where, M is the molecular mass.

Equations (3) and (4) give the following relation, we acquire

$$\left(\frac{q_{Dp}^2}{q_{Db}^2}\right) = \frac{T_p}{T_b} \qquad (5)$$

Consequently, from Eq. (2) and (5) we obtain

$$\left(\frac{q_{Dp}}{q_{Db}}\right) = \left(1 - \frac{N}{2n}\right)^{1/2} \qquad (6),$$

The technique to find $N/2n$ for different shape of nanomaterials has been debated by Qi [10]. The value of $\frac{N}{n}$ is $\frac{4d}{D}, \frac{8d}{3l}$ and $\frac{4d}{3h}$ for spherical nanosolids, nanowires and nanofilms respectively [10]. Where, d is the diameter of atom and D is the diameter of the spherical nanosolids. Here, l is the diameter of nanowire and h is the height of the nanofilm.

Table1. Input parameters used in present work [13, 14, 15]

Nanomaterials	Debye Temperature($q_{Db}(K)$	Atomic Size d(nm)
Au	165	0.2884
Cu		0.256

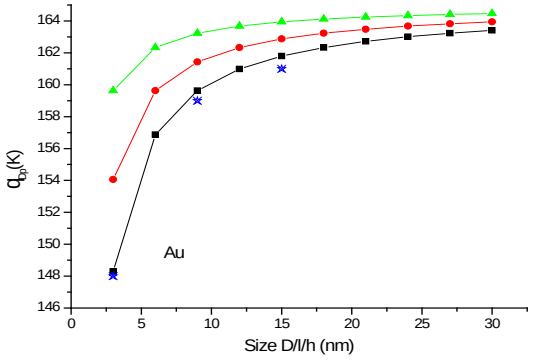


Fig. 1. Size dependence Debye temperature q_{Dp} of Au (nanosphere, nanowire and nanofilm) calculated from Eq. (6). The lines with Symbols square, circle and triangle are for nanosphere, nanowire and nanofilm respectively. Experimental values for nanosphere are shown by stars [16].

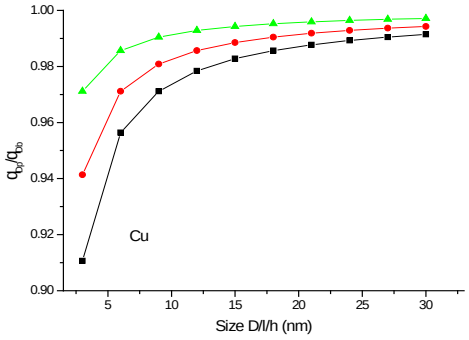


Fig. 2. Size dependence q_{Dp}/q_{Db} of Cu (nanosphere, nanowire and nanofilm) calculated from Eq. (6). The lines with Symbols square, circle and triangle are for nanosphere, nanowire and nanofilm respectively

II. RESULTS AND DISCUSSION

It is shown by Eq. (6) that the Debye temperature is the function of particle size and the shape of the nanomaterials. So, we can discuss the Debye temperature variation with the size of the particles and shapes of the materials. The variation tendency of the relative Debye temperature with respect to particle size and shape of nanomaterials calculated by Eq. (6) is shown in Fig. 1 and 2. Input parameters in our calculation are recorded in Table 1[13-15]. The variation of Debye temperature with particle size and shape of Au nanomaterial calculated from Eq. (6) is shown in Fig. 2 along with the available experimental values for Au nanosphere [16], which support well to our calculated results. This added the validity of the modelused. For the comparison purpose we have plotted the nanosphere, nanowire and nanofilm on the same Fig 1. It is observed that the effect of size decrease as we go from spherical to nanowire to nanofilm. The size and shape dependent Debye temperature of Cu nanomaterial computed using Eq. (6) is shown in fig 2. As exposed in figure, the Debye temperature goes down with the decrease of the particle size. For the sake of comparison, we plotted nanosphere, nanowire and nanofilm materials on the same graph. It is shown that on decreasing the particle size Debye temperature decreases more in spherical nanosolid in comparison to nanowire and nanofilmFor Cu nanomaterial, experimental values are not available. The main reason for the size dependent Debye temperature of nanomaterials is observed as the presence of the large fraction of surface atoms. When size decreases the surface to volume ratio increases, which increases the surface energy. Therefore, the value of $N/2n$ increases. Since the values of $N/2n$ are $\frac{2d}{D}, \frac{4d}{3l}$ and $\frac{2d}{3h}$. On decreasing D, l, h the factor $N/2n$ increases, accordingly the Debye temperature decreases and its effect is more on nanosphere and decreases from nanowire to nanofilm. These results may be of great attention of researches engaged in the experimentalreports.

III. CONCLUSION

We have examined a simple theoretical method to study the size dependence Debye temperature of nanomaterials in different shapes like nanosphere, nanowire and nanofilm. It is shown that the calculated results of Debye temperature of Au and Cu nanomaterials are consistent with the existing experimental results. Moreover, it is also realized that the particle shape effect the Debye temperature of the nanomaterials. The effect on Debye temperature becomes more with the reducing of particle size. Due to the simple process and the applicability of the model, theory may be extended to range of nanomaterials.

REFERENCES

[1] R Lamber, S Wetjen, I Jaeger,Size dependence of the lattice parameter of small palladium particles, Phys Rev B, 1995, 51,10968.
[2] H. Gleiter, Nanostructured materials: Basic concepts and microstructure, Acta Materialia, 2000, 48 1–29.
[3] T. Chookajorn, H.A. Murdoch, C.A. Schuh, Science 2012, 337, 951–954.
[4] S F Xiao, W Y Hu, J Y Yang, J Phys Chem B, 2005, 109, 20339.
[5] H K Kim, S H Hu, J W Park, J W Jeong, G H Lee, Chem, Phys Let, 354, 2002, 165-172.
[6] M Hou, M E Azzaoui, H Pattyn H, J Verheyden, G Koops, G Zhang, Phys Rev B, 2000, 62, 5117
[7] L H Liang, J C Li, Q Jiang, Solid state Communi, 2002, 121, 453.
[8] X W Wang, G T Fei, K Zheng, Z Jin, L D Zhang, Applied Phys Lett, 2006, 88, 173114.

[9] M Cottie, The weired world of nanoscale, University of Technology, Sydney, P O Box 123, Broadway NSW, Australia, 2007.

[10] W.H.Qi, Size effect on melting temperature of nanosolids Physical B, 2005, 368, 46.

[11] F.A. Lindemann, the Calculation of Molecular Vibration Frequencies, Phys. Z, 1910, 11, 609.

[12] J.G. Das, History of the search for continuous melting, Rev. Mod. Phys., 1999, 71, 1737.

[13] H.W. King, R.W.Cahn (Ed.), Physical Metallurgy, North Holland, Amsterdam, 1970.

[14] G. Kastle, H. G. Boyen, A. Shroder, A. Plettl, P. Ziemann, Phys. Rev. B, 2004, 70, 165414.

[15] HLiang, MUpmanyu, H Huana, Phys Rev B, 2005, 71, 241401.

[16] A. Balerna, S. Mobilio,Dynamic properties and Debye temperatures of bulk Au and Au clusters studied using extended x-ray-absorption fine-structure spectroscopy, Phys. Rev. B Condens. Matter, 1986, 34, 2293.

 ISBN: 978-81-931039-3-7

AN ANDROID APPLICATION FOR EMERGENCY SERVICES

Rishi Nandedkar[1], Shubhum Farkase[2], Anurag Mishra[3], Piyush Gajbe[4]

[1,2,3,4] *Department of Computer Technology,*

Rajiv Gandhi College of Engineering and Research, Nagpur (India)

ABSTRACT

In an era where calamities whether they are natural or man-made can stuck any time of a year, efficient disaster management is the need of the hour. The disaster management is a very crucial phrase after a calamity has stuck. One of the immediate challenges after a disaster is to rescue as many human lives as possible. To this an efficient way to call for help should be developed which responds immediately to any kind of calamity ranging from road, rail accidents, and mudslides to earthquakes, floods or an air crash. This application is specifically developed to cater to such needs. This paper provides an in-depth analysis of the application.

I. INTRODUCTION

According to United Nations University for Environment and Human Security (UNU-EHS), India ranks 100th out of a total of 172 countries in the world with a disaster risk of 7.17 %. In India, 138,258 people died of road accidents in India in 2012. This number is alarming. Also many 143,039 deaths occurred because of natural calamities. Due to climate change this calamities are rising every year causing more number of deaths. Various counter measure techniques are undertaken such as Humanitarian aid, Emergency population warning, Emergency Alert System, Evacuations, Emergency management, Crisis management, Disaster risk reduction. This application is focused on Emergency Alert System which will help people to flee or protect themselves from the incoming disaster.

II. RELATED WORK

The first Emergency Alert System was developed by U.S.A. which was used to publish information about tornadoes and flash floods. The system was used in many situations where human help could not reach, and it alerted the people to take safety measures for the disaster. This system was constantly upgraded over the years and was recently used in New York City to inform people about incoming Hurricane Sandy.

2.1 Proposed Work

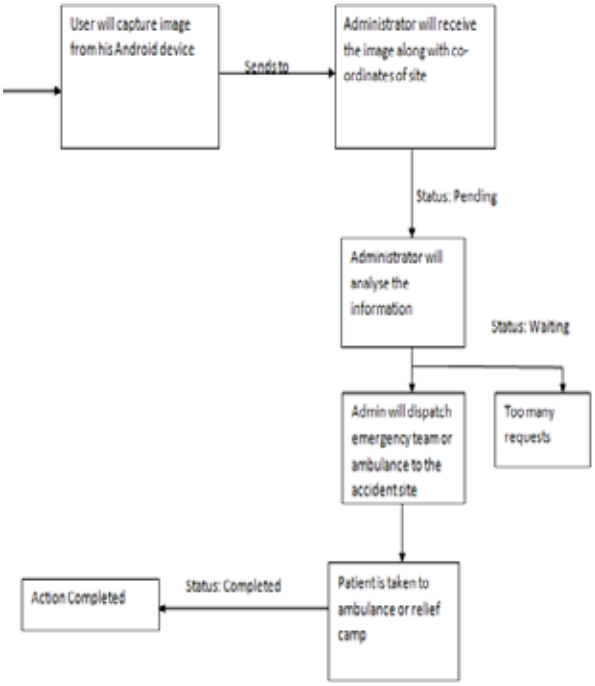
When the app is opened on the Smartphone of the user, it checks if the data connection and the GPS system is turned on or not. If it is not, it prompts the user to do so, since both these services are essential to the functioning of the application Once the GPS and the data connection has been enabled, the user can start using the app.

1. The user can click a picture to be sent along with his report. To do so, the user has to click on the “Take photo” button, after which the camera will start, enabling the user to click a photograph of something he feels would be helpful in the report.
2. The user can also submit some comment along with his report. The comment should be ideally short and should clearly state the nature of the problem. The comment is optional.

3. The GPS activity keeps running in the background, trying to get the location coordinates of the phone. Whenever the location coordinates are set, a toast is displayed saying so. If for some reason, the location coordinates aren't set by the time the user chooses to submit his report, the app prompts him to enter his address manually.

4. After all this, the user clicks on the submit button to send all the data back to the web server, where a PHP file catches it and inserts it into a database table.

2.2 Proposed Architecture



2.2 Implementation

This project consists of two modules:

1. The server side: It consists of a dummy server created on a certain website. An account on that website and created various fields such as latitude, longitude, image, id etc. The data received from the user gets stored in this table. The administrator computer receives this data and quickly responds to the request.

Fig 2.1 Database of Stored Information

2. The application side: The actual functioning application on an Android device is created using Software Development Kit. The application's background and user interface is created in this module.

III. RESULT

Fig 3.1: User interface of the application

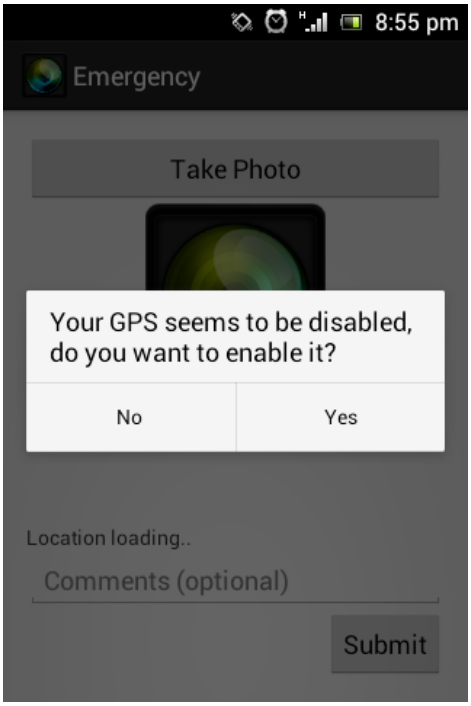


Fig 3.2: Application asking for location services

This is the application side as seen from any Android device

IV. CONCLUSION

In this paper, we have presented an Android Application which can be used in times of tragedy. We have showed that this application takes minimal time to provide speedy relief to accidents or disasters' victims.

V. FUTURE SCOPE

1. The application in future can also be run on Apple's iOS , Microsoft's Windows and Symbian Operating System.
2. This application can be upgraded to handle more requests and serve more people.

REFERENCES

1. www.wikipedia.com

2. www.worlddisastersreport.com

3. Status Solutions' SARA Awareness Model

 ISBN: 978-81-931039-3-7

SURVEY PAPER ON ENHANCED ADAPTIVE ACKNOWLEDGMENT (EAACK) FOR MANETS

Shrilata Savakar[1], Prof. Anand Hiremath[2]

[1,2] *Department of Computer Science,*

BLDEA's Dr. P. G. Halakatti Engineering Institute and Technology Vijayapura,(India)

ABSTRACT

A mobile ad hoc network (MANET) is a continuously self-administering, less-infrastructure network of mobile devices connected without wires. Each device in a MANET is free to move independently in more directions, and it can change its links to other devices frequently. The general challenge in building a MANET is equipping each device to continuously maintain the information required to its route traffic. Every node works as both a transmitter and a receiver. They may contain one or multiple and different transceivers between nodes. This results in a highly – dynamic, autonomous topology .on individual layer like Application Layer , Transport Layer(Session hijacking, Flooding) attacks on MANETs challenge the mobile infrastructure in which nodes can join and leave easily with dynamics requests without a static path of routing this makes mantes vulnerable to a malicious attackers. we need to develop efficient intrusion-detection mechanisms to protect MANET from attacks. To overcome attacks on Mantes we have to provide more security by expanding MANETS into industrial applications based on improved technology and reduced hardware cost. Here we developed a new intrusion-detection system named Enhanced Adaptive Acknowledgment (EAACK) specially designed for MANETs has been developed. EAACK demonstrates higher malicious-behavior detection rates in certain circumstances while does not greatly affect the network performances.

Keywords: WATCHDOG, S-ACK, AACK, EAACK, MANET, IDS etc

I. INTRODUCTION

Over the past decade, there has been a growing interest in wireless networks, as the cost of mobile devices such as PDAs, laptops, cellular phones, etc have reduced drastically. The latest trend in wireless networks is towards pervasive and ubiquitous computing. Catering to both nomadic and fixed users, anytime and anywhere. Several standards for PDAs, laptops, cellular phones, etc have reduced drastically. The latest trend in wireless networks is towards pervasive and ubiquitous computing -catering to both nomadic and fixed users, anytime and anywhere. Several standards for wireless networks have emerged in order to address the needs of both industrial and individual users.One of the most prevalent forms of wireless networks in use today is the Wireless Local Area Network (WLAN). In such a network, a set of mobile nodes are connected to a fixed wired backbone. However, there is still a need for communication in several scenarios of deployment where it is not feasible to deploy fixed wireless access points due to physical constraints of the medium. Owing to the improved technology and reduced costs, wireless networks have gained much more preferences over wired networks in the past few decades.

By definition, Mobile Ad hoc Network (MANET) is a collection of mobile nodes equipped with both a wireless transmitter and a receiver that communicate with each other via bidirectional wireless links either directly or

indirectly. Industrial remote access and control via wireless networks are becoming more and more popular these days. One of the major advantages of wireless networks is its ability to allow data communication between different parties and still maintain their mobility. However, this communication is limited to the range of transmitters. This means that two nodes cannot communicate with each other when the distance between the two nodes is beyond the communication range of their own. MANET solves this problem by allowing intermediate parties to relay data transmissions. This is achieved by dividing MANET into two types of networks, namely, single-hop and multi hop. In a single-hop network, all nodes within the same radio range communicate directly with each other. On the other hand, in a multi hop network, nodes rely on other intermediate nodes to transmit if the destination node is out of their radio range. In contrary to the traditional wireless network, MANET has a decentralized network infrastructure. MANET does not require a fixed infrastructure; thus, all nodes are free to move randomly.

II. RELATED WORK

Since the nature of MANET node is distributed and requires cooperation to other nodes, Zhang,Lee, and Huang [[4], [5]] proposed "Intrusion detection (ID) and response system" should follow both the natures. In this proposed architecture model, each node is responsible for detecting signs of intrusion locally and independently, but neighboring nodes can collaboratively investigate in a broader range. Individual IDS agents are placed on each and every node. Each the IDS agent runs independently and monitors local activities (user and systems activities, and communication activities within the radio range). The agent detects intrusion from local traces and initiates response. If anomaly is detected in the local data, or if the evidence is inconclusive and a broader search is warranted, neighboring IDS agents will cooperatively participate in global intrusion detection actions. These individual IDS agents collectively form the IDS system to defend the wireless ad-hoc network.

2.1 Intrusion Detection System in Manets

Due to the limitations of most MANET routing protocols, nodes in MANETs assume that other nodes always cooperate with each other to relay data. This assumption leaves the attackers with the opportunities to achieve significant impact on the network with just one or two compromised nodes. To address this problem, Intrusion Detection System (IDS) should be added to enhance the security level of MANETs. If MANET can detect the attackers as soon as they enter the network, we will be able to completely eliminate the potential damages caused by compromised nodes at first time. IDSs usually act as the second layer in MANETs, and it is a great complement to existing proactive approaches and presented a very thorough survey on contemporary IDSs in MANETs. In this section, we mainly describe three existing approaches, namely, Watchdog, TWOACK and AACK.

2.2 Watchdog

Watchdog that aims to improve throughput of network with the presence of malicious nodes. In fact, the watchdog scheme is consisted of two parts, namely Watchdog and Pathrater. Watchdog serves as an intrusion detection system for MANETs. It is responsible for detecting malicious nodes misbehaviours in the network. Watchdog detects malicious misbehaviours by promiscuously listens to its next hop's transmission. If Watchdog node overhears that its next node fails to forward the packet within a certain period of time, it increases its failure counter. Whenever a node's failure counter exceeds a predefined threshold, the Watchdog node reports it

as misbehaving. In this case, the Pathrater cooperates with the routing protocols to avoid the reported nodes in future transmission. Many following researches and implementations have proved that the Watchdog scheme to be efficient. Furthermore, compared to some other schemes, Watchdog is capable of detecting malicious nodes rather than links. These advantages have made Watchdog scheme a popular choice in the field. Many MANET IDSs are either based on or developed as an improvement to the Watchdog scheme. Watchdog scheme fails to detect malicious misbehaviors with the presence of

- [illegible]
- [illegible]
- [illegible]
- [illegible]sbehavior report,
- [illegible]
- [illegible]

2.3 Twoack

TWOACK is neither an enhancement nor a Watchdog based scheme. Aiming to resolve the receiver collision and limited transmission power problems of Watchdog, TWOACK detects misbehaving links by acknowledging every data packets transmitted over each three consecutive nodes along the path from the source to the destination. Upon retrieval of a packet, each node along the route is required to send back an acknowledgement packet to the node that is two hops away from it down the route. TWOACK is required to work on routing protocols such as Dynamic Source Routing (DSR).The working process of TWOACK is demonstrated in Fig.1, node A first forwards packet 1 to node B, and then node B forwards Packet 1 to node C. When node C receives Packet 1, as it is two hops away from node A, node C is obliged to generate a TWOACK packet, which contains reverse route from node A to node C, and sends it back to node A. The retrieval of this TWOACK packet at node A indicates the transmission of Packet 1 from node A to node C is successful. Otherwise, if this TWOACK packet is not received in a predefined time period, both nodes B and C are reported malicious.

TWOACK scheme successfully solves the receiver collision and limited transmission power problems posed by Watchdog. However, the acknowledgement process required in every packet transmission process added a significant amount of unwanted network overhead. Due to the limited battery power nature of MANETs, Such redundant transmission process can easily degrade the life span of the entire network.

2.4 Aack

It is based on TWOACK Acknowledgement (AACK) similar to TWOACK,AACK is an acknowledgement based network layer scheme which can be considered as a combination of a scheme call ACK (identical toTWOACK) and an end-to-end acknowledgement scheme called ACK. Compared to TWOACK, AACK significantly reduced network overhead while still capable of maintaining or even surpassing the same network throughput. Source node S will switch to TACK scheme by sending out a TACK packet. The concept of adopting a hybrid scheme in AACK greatly reduces the network overhead, but both TWOACK and AACK still suffer from the problem that they fail to detect malicious nodes with the presence of false misbehaviour report and forged acknowledgement packets.

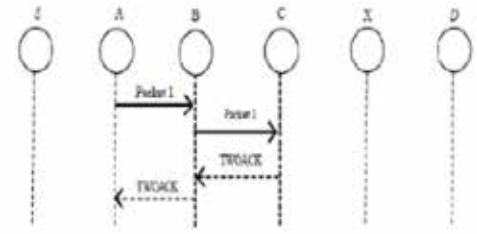


Figure 1: TWOACK

In fact, many of the existing IDSs in MANETs adopt acknowledgement based scheme, including TWOACK and AACK. The function of such detection schemes all largely depend on the acknowledgement packets. Hence, it is crucial to guarantee the acknowledgement packets are valid authentic.

III. EAACK

The proposed approach EAACK is designed to tackle three of the six weaknesses of Watchdog scheme, namely, false misbehaviour, limited transmission power, and receiver collision. As discussed in previous sections, TWOACK and AACK solve two of these three weaknesses, namely, receiver collision and limited transmission power. However, both of them are vulnerable to the false misbehaviour attack. In this research work, our goal is to propose new IDS specially designed for MANETs, which solves not only receiver collision and limited transmission power but also the false misbehavior problem. Furthermore, we extend our research to adopt a digital signature scheme during the packet transmission process. As in all acknowledgment-based IDSs, it is vital to ensure the integrity and authenticity of all acknowledgment packets.

3.1 Scheme Description

In this section, we describe our proposed Enhanced Adaptive Acknowledgement (EAACK) scheme in details. The approach described in this research paper is based on our previous work, where the backbone of EAACK was proposed and evaluated through implementation. In this work, we extend it with the introduction of digital signature to prevent the attacker from forging acknowledgement packets. EAACK is consisted of three major parts, namely: 1.Acknowledge (ACK),

2.Secure Acknowledge (S-ACK) And

3. Misbehaviour Report Authentication (MRA). In order to distinguish different packet types in different schemes, we included a two-bit packet header in EAACK. Flowchart in fig 3 describing EAACK scheme. Please note that in the proposed scheme, here assume that the link between each node in the network is bidirectional. Furthermore, for each communication process, both the source node and the destination node are not malicious. Unless specified, all acknowledgement packets described in this research are required to be digitally signed by its sender and verified by its receiver.

3.2 Aack

As discussed before, ACK is basically an end-to-end acknowledgement scheme. It acts as a part of the hybrid scheme in EAACK, aiming to reduce network overhead when no network misbehaviour is detected. In Fig.3, in ACK mode, node S first sends out an ACK data packet *ad*1 *P* t o the destination node D.

If all the intermediate nodes along the route between node S and node D are cooperative and node D Successfully receives *ad*1 *P*, node D is required to send back an ACK acknowledgement packet *ak*1 *P* along the

same route but in a reverse order. Within a predefined time period, if node S receives *ak*1 *P* , then the packet transmission from node S to node D is successful. Otherwise, node S will switch to S-ACK mode by sending out an S-ACK data packet to detect the misbehaving nodes in the route.

3.3 S-ACK

S-ACK scheme is an improved version of TWOACK scheme. The principle is to let each three consecutive nodes work in a group to detect misbehaving nodes. For each three consecutive nodes in the route, the third node is required to send an S-ACK acknowledgement packet to the first node. The intention of introducing S-ACK mode is to detect misbehaving nodes in the presence of receiver collision or limited transmission power. in S-ACK mode, the three consecutive nodes (i.e. F1, F2 and F3) work in a group to detect misbehaving nodes in the network.

Node F1 first sends out S-ACK data packet to node F2. Then node F2 forwards this packet to node F3. When node F3 receives, as it is the third node in this three-node group, node F3 is required to send back an S-ACK acknowledgement packet to node F2. Node F2 forwards back to node F1. If node F1 does not receive this acknowledgement packet within a predefined time period, both nodes F2 and F3 are reported as malicious. Moreover, a misbehaviour report will be generated by node F1 and sent to the source node S. 1 s adP1 s adP 1 s akP1 s akP. Nevertheless, unlike TWOACK scheme, where the source node immediately trusts the misbehaviour report, EAACK requires the source node to switch to MRA mode and confirm this misbehavior report. This is a vital step to detect false misbehavior report in our proposed scheme. Detect misbehaving nodes in the network.

Node F1 first sends out S-ACK data packet *s ad*1 *P* to no de F2. Then node F2 forwards this packet to node F3. When node F3 receives *s ad*1 *P* , as it is the third node in this three-node group, node F3 is required to send back an SACK acknowledgement packets *ak*1 *P* to node F2. Node F2 forwards *s ak*1 *P* back to node F1.

If node F1 does not receive this acknowledgement packet within predefined time period, both nodes F2 and F3 are reported as malicious. Moreover, a misbehaviour report will be generated by node F1 and sent to the source node S. Nevertheless, unlike TWOACK scheme, where the source node immediately trusts the misbehaviour report, EAACK requires the source node to switch to MRA mode and confirm this misbehaviour report. This is a vital step to detect false misbehaviour report in our proposed scheme.

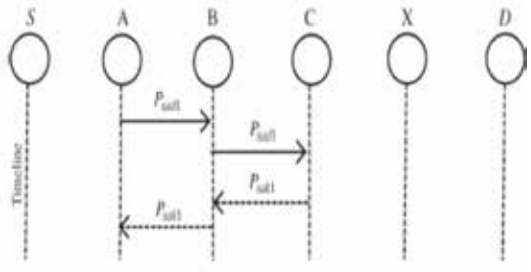


Figure 2: S-Ack Scheme Node C is Required to Send Back an Acknowledge Packet t o Node B

3.4 MRA

The Misbehavior Report Authentication (MRA) scheme is designed to resolve the weakness of Watchdog when it fails to detect misbehaving nodes with the presence of false misbehaviour report. False misbehaviour report can be generated by malicious attackers to falsely report that innocent nodes as malicious. This attack can be

lethal to the entire network when the attackers break down sufficient nodes and thus cause a network division. The core of MRA scheme is to authenticate whether the destination node has received the reported missing packet through a different route. To initiate MRA mode, the source node first searches its local knowledge base and seeks for alternative route to the destination node. If there is none other exists, the source node starts a DSR routing request to find another route. The path from the source to destination was vulnerable to spoofing attackers. There was no method proposed to detect the nodes attackers. Due to the nature of MANETs, it is common to find out multiple routes between two nodes.

By adopting an alternative route to the destination node, we circumvent the misbehaviour reporter node. When the destination node receives an MRA packet, it searches its local knowledge base and compare if the reported packet was received. If it is already received, then it is safe to conclude this is a false misbehaviour report and whoever generated this report is marked as malicious. Otherwise, the misbehaviour report is trusted and accepted.

Figure 3: System Flow of EAACK

3.5 Digital Signature

EAACK is an acknowledgement based IDS. All three parts of EAACK, namely: ACK SACK and MRA are acknowledgement based detection schemes. They all rely on acknowledgement packets to detect misbehaviours in the network. Thus, it is extremely important to ensure all acknowledgement packets in EAACK are authentic and untainted. Otherwise, if the attackers are smart enough to forge acknowledgement Packets, all of the three schemes will be vulnerable. With regarding to this urgent concern, we incorporated digital signature in our proposed scheme. In order to ensure the integrity of the IDS, EAACK requires all acknowledgement packets to be digitally signed before they are sent out, and verified until they are accepted.However, we fully understand the extra resources that are required with the introduction of digital signature in MANETs. To address this concern, we implemented both DSA and RSA digital signature scheme in our proposed approach. The goal is to find the most optimal solution for using digital signature in MANET.

IV. CONCLUTION AND FUTURE ENHANCEMENT

In this paper we have presented novel IDS for MANET's named as EAACK. This has top priority in network security issues. Because it was specially designed to prevent from attackers to initiating forged acknowledge

packets. We extend it by introducing digital signatures. Though it generates more ROs in some cases, as demonstrated in our experiment, it can vastly improve the network's PDR when the attackers are smart enough to forge acknowledgment packets compared it against other popular mechanisms in different scenarios through simulations. The results generated positive performances.

To increase the merits of our research work, we plan to investigate the following issues in our future research:

1) Possibilities of adopting hybrid cryptography techniques to further reduce the network overhead caused by digital signature;
2) Examine the possibilities of adopting a key exchange mechanism to eliminate the requirement of predistributed keys;
3) Testing the performance of EAACK in real network environment instead of software simulation.

REFERENCE

[1] E. M. Shakshuki , N. Kang and T. R. Sheltami "EAACK—A secure intrusion detection system for MANETs", IEEE Trans. Ind. Electron., vol. 60, no. 3, pp.1089 -1098 2013

[2] R. Akbani, T. Korkmaz, and G. V. S. Raju, "Mobile Ad hoc Network Security," in Lecture Notes in Electrical Engineering, vol. 127. New York: Springer-Verlag, 2012, pp. 659–666.

[3] R. H. Akbani, S. Patel, and D. C. Jinwala, "DoS attacks in mobile ad hoc networks: A survey," in Proc. 2nd Int. Meeting ACCT, Rohtak, Haryana, India, 2012, pp. 535–541.

[4] T. Anantvalee and J. Wu, "A Survey on Intrusion Detection in Mobile Ad Hoc Networks," in Wireless/Mobile Security. New York: Springer-Verlag, 2008.

[5] Y. Zhang, W. Lee, "Intrusion detection in wireless ad-hoc networks", The 6th Annual International Conference on Mobile Computing and Networking, pp. 275–283, 2000

[5]. Y. Zhang, W. Lee, and Y. Huang. "Intrusion Detection Techniques for Mobile Wireless Networks". Wireless Networks Journal (ACM WINET), 9(5): 545-556, 2003.

[6] V. C. Gungor and G. P. Hancke, "Industrial wireless sensor networks: Challenges, design principles, and technical approach," IEEE Trans. Ind.Electron., vol. 56, no. 10, pp. 4258–4265, Oct. 2009.

[7] Y. Hu, D. Johnson, and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," in Proc. 4th IEEEWorkshop Mobile Comput. Syst. Appl., 2002, pp. 3–13.

[8] Y. Hu, A. Perrig, and D. Johnson, "ARIADNE: A secure on-demand routing protocol for ad hoc networks," in Proc. 8th ACM Int. Conf. MobiCom, Atlanta, GA, 2002, pp. 12–23.

[9] G. Jayakumar and G. Gopinath, "Ad hoc mobile wireless networks routing protocol—A review," J. Comput. Sci., vol. 3, no. 8, pp. 574–582, 2007.

[10] D. Johnson and D. Maltz, "Dynamic Source Routing in ad hoc wireless networks," in Mobile Computing. Norwell, MA: Kluwer, 1996, ch. 5, pp. 153–181.

[11] N. Kang, E. Shakshuki, and T. Sheltami, "Detecting misbehaving nodes in MANETs," in Proc. 12th Int. Conf. iiWAS, Paris, France, Nov. 8–10, 2010, pp. 216–222.

[12] N. Kang, E. Shakshuki, and T. Sheltami, "Detecting forged acknowledgements in MANETs," in Proc. IEEE 25th Int. Conf. AINA, Biopolis Singapore, Mar. 22–25, 2011, pp. 488–494

.

 ISBN: 978-81-931039-3-7

DDoS ATTACKS & DEFENCE MECHANISMS AND ITS MITIGATION TECHNIQUES

Ritu Maheshwari Bansal[1], Deepika khurana[2], Ritika Bateja[3]

[1]Ph.D Scholar (Computer Science), Department of Computer Science,
Barkatullah University,Bhopal, Madhya Pradesh, (India)
[2,3]Assistant professor (CSE), Faculty of Engineering & Technology,
Manav Rachna International University, Faridabad, Haryana, (India)

ABSTRACT

DDoS attacks prevents legitimate users from using a victim computing system or network resource. Two main classes of DDoS attacks are: bandwidth depletion and resource depletion attacks. There are three essential components to DDoS countermeasures and based on which pro-active, post-active and location of defense based challenges have been found out. Several mitigation techniques have been analysed and discussed in this paper which can be taken as a base for further research work in the domain of mitigation of DDoS attacks at source, intermediate or at victim server side.

Keywords: ***DDoS, Defense Mechanism, Mitigation, Load Balancing, Filtering***

I. INTRODUCTION

A Denial of Service (DoS) attack is an attack that prevents legitimate users from using a victim computing system or network resource. A Distributed Denial of Service (DDoS) attack deploys many computers to launch attack to gain its purpose. It can be performed at network level, operating system level, application level and many more. In past, DDoS attack has been able to damage the companies like YAHOO, AMAZON, etc. in terms of services and finance. It is a large-scale, coordinated attack on the availability of services of a victim system or any network based resource that is launched indirectly by compromised hosts on the Internet.

In this attack, attacker fills the networks bandwidth with large amount of request packets that consumes the bandwidth and makes it difficult for the legitimate user to access the service. The attacker launch millions of machines for a DDoS attack, first scan millions of machines for vulnerable service and other weakness, then gain access and compromise these zombies or slave machines. These infected machines can recruit more zombies. When the assault starts, the real attacker hides the identity and sends orders to zombies to perform the attacks. The attackers are not going to thieve, modify or remove the information exchanged on networks, but they attempt to impair a network service, thus to block legitimate users from accessing the service. This attack is comprehensive and synchronized attack, initiated by a group of negotiated hosts upon a victim network resource. All operations like ecommerce, banking, trade, social activities and mail have now become easy on internet. To use the Internet for daily operations, increasing number of services are motivated. Internet security includes confidentiality, message integrity, non-repudiation, and authentication. Major issue is availability. DDoS attacks pose a big threat to availability of services on the Internet. Without being authenticated on the internet, any

packet can be sent to anyone. A packet that arrives to a provided service has to be processed by the receiver. Fake identity can be created by the attacker and malicious traffic can be sent.

In this paper, section II presents *Categorization of DDoS Attacks, its Architecture and Defense Mechanisms*, section III presents *DDoS Defense Mechanisms and Techniques*, section IV presents *Challenges in Defense Mechanisms* section V presents *DDoS Mitigation Techniques* and lastly, section VI presents *Conclusions*.

II. CATEGORIZATION OF DDOS ATTACKS

When a computer or a network is incapable of providing the desired services it means that Denial of Service attacks are occurred. In this, the services of the network are purposively blocked by the user. These DoS attacks doesn't cause any harm to the data but make the resources unavailable. [5]. Attack Pattern is a process to identify the view of attackers, that gives the information about the attack types, attack prerequisites, attack weaknesses, the knowledge so required to perform an attack and all the information related to the attack that had been taken place in the network [2].

Two main classes of DDoS attacks are: bandwidth depletion and resource depletion attacks [7]. A bandwidth depletion attack is created to flood the victim network with unwanted traffic that prevents legitimate traffic from reaching the victim system. It is an activity that aims to disable the services provided by the victim by sending unwanted traffic in large volume [11]. A resource depletion is an attack that is created to hold down the resources of a victim system. This attack targets a server or process at the victim making legitimate requests for service unavailable to the users [3]. There are two major impacts of bandwidth attacks i.e. consumption of the host's resources and consumption of the network bandwidth.

III. DDOS DEFENCE MECHANISMS AND TECHNIQUES

There are three essential components to DDoS countermeasures [4]. There is the component for preventing the DDoS attack which includes preventing secondary victims and detecting and neutralizing handlers. There is the component for dealing with a DDoS attack while it is in progress, including detecting or preventing the attack, mitigating or stopping the attack, and deflecting the attack. Lastly, there is the post-attack component which involves network forensics. Based on the underlying strategies, we can categorize current DDoS detection and defense approaches into three categories: Proactive Mechanisms, Reactive Mechanisms and Post Attack Analysis [9].

3.1 Pro-Active or Preventive Defense Mechanisms

Instead of detecting the attacks by using attack pattern these mechanisms try to improve the reliability of the global Internet infrastructure by adding extra functionality to Internet components to prevent attacks and exploitation. Preventive mechanisms are the actions performed prior to an attack either to eliminate the possibility of being a target of attacks or to support the target to increase the effects of attacks sufficiently. Several preventive countermeasures are:

Planning a proper risk management strategy is a matter of preparing for attacks, determining what should be protected, how and at what cost. It is a plan of procedures that guides the responses to various attacks and the recovery of possible damages.

Load balancing refers to key services being distributed to multiple locations. Thus, if an attack is primarily engaged against a certain servers, the other servers may still be able to operate sufficiently. Acquiring

abundance of bandwidth is expensive. The aim is to acquire as much of bandwidth and other resources to retain operability even in case of a powerful attack.

Filtering of all unnecessary traffic is a method of defining the problem. Filtering of all unnecessary traffic is a precaution for protecting own hosts from being compromised.

3.2 Reactive Defense Mechanisms

These mechanisms deploy third-party Intrusion Detection Systems (IDS) to obtain attack information and take action based on this information. When IDS system detects the DDoS attack packets, filtering mechanism are then used to filter out the attack stream completely, even at the source network. If the IDS cannot detect the attack stream accurately, rate limiting is used. These mechanisms refer to the actions performed to mitigate the effects of one or more ongoing attacks and they consist of detection and response procedures.

Detection is the process of determining the target under attack, that must be detected first.

Response is the process of reaction after the detection procedure has verified that there is an ongoing attack. These methods include some form of traffic filtering. Most of the remaining responsive methods relate to tracing the approximate attack source, referred as IP-traceback.

3.3 Post-Attack Forensics or Post Active Methods

The aim is to either look for attack patterns that will be used by IDS or identify attackers using packet tracing. Packet tracing traces Internet traffic back to the true source. Post-active methods are the actions performed after an attack has occurred to mitigate the threat of DDoS. Post active methods are about tracing the attacker as well as analysing the vulnerabilities exploited by the attack and engaging into repairs. Tracing one or more attackers is a task that relies heavily on the information gathered during the attack.

The defense mechanisms, on the basis of location, can be categorized into three basic models: (1) the Victim Model (VM), a traditional defense model that identifies and filters attack traffic at a single location, the victim. (2) the Victim-Router Model (VRM), a cooperative model, that identifies and filters the attack traffic at multiple locations. The defense process is triggered by the signal from a victim and accomplished with the cooperation from participating routers. (3) the Router-Router Model (RRM) a distributed defense model that detects the attack traffic by sharing information among participating routers. Each model is classified according to the employment of the defense mechanism, and cooperation among the victim and router network components. [10]. The aim of DDoS defense is to filter attack traffic close to the attack sources so that both network and server resources will be saved.

IV. CHALLENGES IN DEFENCE MECHANISMS

4.1 Pro-Active Challenges

Proactive defense prevents the malicious packets from reaching the victim hence, they cannot impact the protected service [14]. Proactive solutions mitigate the DDoS attacks before they affect the performance of targets. The attacker can still spoof the addresses within the expected range. When the “attack army” consists of a large number of zombie machines, the attacker does not need to use IP spoofing, as each zombie machine can just flood a small volume of traffic with its own address. The aggregated malicious traffic is then, enough to overwhelm the victim network.

4.2 Post-Active Challenges

Once an attack is detected, the next response would be to block the attack traffic at its source. Unfortunately, there is no easy way to track IP traffic to its source. This is because of two aspects of IP protocol. The first is the ease with which IP source addresses can be forged. The second is the stateless nature of IP routing, where routers normally know only the next hop for forwarding a packet, rather than the complete end-to-end route taken by each packet [10].

4.3 Location of Defence based Challenges [22]

Source-initiated Challenge: Source sites are responsible for ensuring about attack-free outgoing packets. But, the viability of such approaches lies on cooperation among a majority of ingress network administrators Internet-wide.

Victim-initiated Challenge: The victim can initiate countermeasures to reduce incoming traffic. DDoS traffic is very low at sources which, is not easy to characterize attacks packets at the source [16]. Automation of real time response by generating alerts and collaborating with other defense nodes is difficult at the victim side.

4.4 Ddos Mitigation Techniques

Mitigation is the process to minimize the effect of an ongoing attack. The simplest method is to drop the packets belonging to the attacker [5]. But the problem lies in distinguishing between legitimate or illegitimate client.

Pushback [25] enables routers to congestion rate limit them by identifying high bandwidth aggregates. It requests its upstream neighbour's to help in rate limiting if the congested router cannot control the aggregate by itself. When attackers are not collocated on a path separate from the legitimate traffic, it inflicts collateral damage. It also cannot work in non-contiguous deployment and when core routers are not congested, it cannot detect attacks. Legitimate traffic can be protected by by pushing the defense frontier towards attack sources.

Selective pushback is an improved version of pushback [12]. By analyzing the traffic distribution change of all upstream routers at the target, it sends pushback messages to the routers closest to the attack sources It has two advantages. First, attack sources can be located more accurately by traffic distribution analysis as compared to volume-based approaches. Second, the pushback message can be sent to the routers closest to the attack sources directly, that can mitigate the attack damage more quickly than the original pushback scheme. But, accuracy of detection, and deployment across multiple ISP domains is an issue.

In [21] to decrease the impact of attack, designated controllers of multiple domains interact and traceback the attack path. The limitation under detecting and characterizing attack traffic is the use of third party detection. It is good to find ingress edges of attack, but attack signature should be as narrow as possible to lessen collateral damage. The communication between victim and controller and between agents and controllers should be possible in state of DDoS and should also be integral, authentic and confidential. But, single point failure due to DDoS attack at controller can damage the scene.

Filtering techniques are also used to stop the attack. If attack signatures are not accurate, adaptive rate limit would be better. To verify legitimate users and send their traffic on the overlay to secret servlets, SOS [13] uses access points (SOAPs) close to source that tunnel it to a distributed firewall protecting the victim. SOS offers good protection to the server but as it is routed on the overlay the traffic experiences a significant delay. SOS approach involves a authentication and overlay routing mechanisms and suffers from routing related drawbacks.

But, if attackers can gain massive attack power, all the SOAPs can be paralyzed, and the target's success will be disrupted.

Active Security System (ASSYST) [8] supports distributed response with nodes equivalent to classifiers being deployed only at edge networks and with non-contiguous deployment. COSSACK [6] that is deployed at source and victim networks, forms a multicast group of defense nodes and cooperate in filtering the attack. Both [1] and [20] that do not deploy their defense mechanisms cannot handle attacks from legacy networks. Parameter Based Defense [23] that rate limits an attack originated from one of its customer networks, constructs a multicast group at an ISP. It does not perform well in non-contiguous deployment and requires wide deployment. Yau et al. [15] propose a router throttle mechanism that is installed at the routers close to the victim. This defense system inflicts collateral damage to legitimate traffic by incorporating only core defense mechanisms and victim end. Some router based solutions with the aid of an overlay of routers traces and stops the attacks close to the source. Tracing inflicts collateral damage on legitimate users that share a network with an attacker which is done using signatures assigned to each source network.

DefCOM [24] can collaborate in DDoS detection and response through a dynamically-built overlay by providing added functionality to existing defenses. Three types of DefCOM functionalities are added to existing routers or defense nodes. A single physical node can host more functionality at a time. The functionalities are: (1) A classifier functionality that is capable of differentiating the legitimate traffic from the attack traffic is added to existing defenses. (2) A rate limiter functionality that runs a weighted fair share algorithm (WFSA) to prioritize traffic and forwards to the victim is deployed by routers. It rate limits this traffic to preserve victim's resources. (3) An alert generator functionality that can detect a DoS attack is added to defenses. An alert generator propagates the attack alert to other DefCOM nodes using the overlay. The alert contains the IP address of the attack's victim and specifies a desired rate limit. Extra infrastructure for overlay and cooperation at all points of the Internet are major issues. Collateral damage lies on accuracy of classifier.

Yau et al. [15] implemented router throttles to fight DDoS attacks against Internet servers. A proactive approach is followed. Routers along forwarding paths, regulate the contributing packet rates to more moderate levels before aggressive packets can converge to overwhelm a server. The mechanism to install a router throttle at an upstream router several hops away is for server. The throttle limits the rate at which packets destined for server will be forwarded through the router. Traffic exceeding the rate limit can either be rerouted to an alternate server or dropped. The throttle rate is reduced if the current throttle fails to bring down the load to below threshold. It is increased if the server load falls below a low-water mark.

ALPi, scheme with reduced implementation complexity and enhanced performance extends the packet scoring concept [17]. A leaky-bucket overflow control scheme facilitates high-speed implementation and simplifies the score computation. An attribute-value-variation scoring scheme increases the accuracy of detecting and differentiating attacks by analyzing the deviations of the current traffic attribute values.

DDoS attacks require new criteria to detect increasingly complex and deceptive assaults and hence mitigating the effects of the attack to ensure resource availability [18]. Normal Distribution is the process of finding the probability of failure, undesirable event in a large group of quantity. It is in practical, impossible to calculate and qualify all items in given specified time. Normal distribution is being used in various quantitative study to calculate large amount of such items.

In SIFF, aim is to protect privileged packets from unprivileged packet flooding, allowing packet receivers to terminate individual privileged flows selectively before arriving near the victim. For this, all network traffic is separated into privileged and unprivileged packets [19].

V. CONCLUSIONS

DDoS attacks have been categorized and it's proactive, reactive and post active defense mechanisms have been discussed. Challenging issues of these mechanisms and techniques have been found out. A number of mitigation techniques have been studied and analysed. These enable us to distinguish between legitimate and illegitimate traffic and accordingly either drop or detect the unwanted packets. This analysis work can be taken as a base for further research work in several DDoS mitigation techniques.

REFERENCES

[1] C. Papadopoulos, R. Lindell, J. Mehringer, A. Hussain, R. Govindan, "COSSACK: Coordinated Suppression of Simultaneous Attacks," IEEE Conference on DARPA Information Survivability, Information Sciences Institute, vol. 1, pp. 2-13, 22-24, April, 2003.

[2] A. Madhuri, A. Ramana Lakshmi, "Attack Patterns for Detecting and Preventing DDoS and Replay Attacks," International Journal of Engineering and Technology, vol. 2 (9), pp. 4850-4859, 2010.

[3] G. Zhang and M. Parashar, "Cooperative Defence against DDoS Attacks," Journal of Research and Practices in IT, vol. 38 (1), pp. 69-84, February 2006.

[4] R. Kumar, R. Karanam, R. Bobba, S. Raghunath, "DDoS Defense Mechanism," IEEE International Conference on Future Networks, VIT University, Vellore, India, pp. 254-257, 2009.

[5] D. Garg, "DDOS Mitigation Techniques-A Survey," International Conference on Advance Computing in Communication and Networks, pp. 1302-1309, 2011

[6] B.B. Gupta, R.C. Joshi, M. Mishra, "Distributed Denial of Service Prevention Techniques," IEEE International Journal of Computer and Electrical Engineering, vol. 2 (2), pp. 269-276, April, 2010.

[7] S. Liu, "Surviving Distributed Denial-of-Service Attacks," IEEE Journal on IT Professional, vol. 11 (5), pp. 51-53, 2009.

[8] R. K. Chang, "Defending against flooding-based DDoS attacks: A tutorial", IEEE Communications Magazine, vol. 40 (10), pp. 42-51, October 2002.

[9] L. Garber, "Denial-of-Service attack rip the Internet," IEEE Journal on Computer, vol. 33 (4), pp. 12-17, 2000.

[10] Tao Peng, "Defending Against Distributed Denial of Service Attacks," University of Melbourne, Doctorate Thesis, April 2004.

[11] J. Molsa, "Mitigating denial of service attacks: A tutorial," Journal on Computer Security, vol. 13, pp. 807-837, 2005.

[12] T. Peng, C. Leckie, K. Ramamohanarao, "Defending against distributed denial of service attack using selective pushback," 9th IEEE International Conference on Telecommunications, pp. 411-429, 2009.

[13] A.D. Keromytis, V. Misra, D. Rubenstein, "SOS: An Architecture For Mitigating DDoS Attacks," IEEE Journal on Selected Areas in Communication, Columbia University, New York, USA, vol. 22 (1), pp. 176-188, January, 2004.

[14] Z. Fu, "Multifaceted Defense against Distributed Denial of Service Attacks: Prevention, Detection, Mitigation," Chalmers University of technology, Sweden, Doctorate Thesis, 2012.

[15] D.K.Y. Yau, J.C.S. Lui, F. Liang, Y. Yam, "Defending against distributed denial of service attacks with Max-Min fair server-centric router throttles," 10th IEEE International Workshop on Quality of Service, Purdue University, USA, pp. 35-44, 2002.

[16] M. Sachdeva, G. Singh, K. Kumar, and K. Singh, "A comprehensive survey of distributed defense techniques against DDoS attacks," International Journal of Computer Science and Network Security, vol. 9 (12), pp. 7-15, December, 2009.

[17] P.E. Ayres, Huizhong Sun, H. Jonathan Chao, "ALPi: A DDoS Defense System for High-Speed Networks," IEEE Journal on Selected Areas in Communications, vol. 24 (10), pp. 1864-1876, October 2006.

[18] V. Shyamala Devi, Dr. R. Umarani, "Thwarting Distributed Denial of Service attacks using Normal Distribution and Weibull Theorem," International Journal of Engineering Research & Technology, vol. 1(6), pp. 1-12, August, 2012.

[19] A. Yaar, A. Perrig, D. Song, "SIFF: A stateless internet flow filter to mitigate DDoS flooding attacks," IEEE Symposium on Security and Privacy, Carneggie Melon University, Pittsburgh, USA, pp. 130-143, 9-12, May 2004.

[20] R. Canonico, D. Cotroneo, L. Peluso, S.P. Romano, G. Ventre, "Programming Routers to Improve Network Security," OPENSIG Workshop on Next Generation Network Programming, 2001.

[21] U.K. Tupakula, V. Varadharajan, "A controller agent model to counteract DoS attacks in multiple domains," 8th IFIP/IEEE International Symposium on Integrated Network Management, Macquarie University, Australia, pp.113-116, 24-28, March, 2003.

[22] Yoohwan Kim, Wing Cheong Lau, Mooi Choo Chuah, H. Jonathan Chao, "PacketScore: A Statistics-Based Packet Filtering Scheme against Distributed Denial-of-Service Attacks," IEEE Transaction on Dependable and Secure Computing, Nevada University, Los Vegas, vol. 3 (2), pp.141-155, April-June 2006.

[23] S. Chen, Q. Song, "Perimeter-Based Defense against High Bandwidth DDoS Attacks," Transactions on Parallel and Distributed Systems," IEEE Transaction on parallel and Distributed Systems, Florida University, USA, vol. 16 (6), pp. 526-537, June, 2005.

[24] G. Oikonomou, J. Mirkovic, P. Reiher, M. Robinson, "A Framework for a Collaborative DDoS Defense," 22nd IEEE Annual Conference on Computer Security Applications, delaware University, Newark, pp. 33-42, December, 2006.

[25] J. loannidis, S.M. Bellovin, "Implementing Pushback: Router-Based Defense against DDoS Attacks," 2002, [Online]. Available: https:// www.cs.columbia.edu /~smb / papers/ pushback-impl.pdf

 ISBN: 978-81-931039-3-7

A BUSINESS & ECONOMIC REVIEW OF E-COMMERCE IN INDIA

[1]Indrajit Ghosal, [2]Debansu Chatterjee,

[3]Purnima Bhavan, [4]Abhisek Banerjee

[1]Asst. Professor , Institute of Management Study (IMS), Kolkata (India)

[2]IMS Research Scholar, Faculty of EDI-Entrepreneurship Development Institute, Govt. of India (India)

[4]Faculty , Institute of Management Study, Kolkata (India)

ABSTRACT

Future of ecommerce is very innovative in India with even the stock exchanges coming online providing an online stock portfolio and status with a fifteen minute delay in prices. Now, country growing awareness among the business community in India about the opportunities offered by Ecommerce. The main factor of E-Commerce is adopting in India and the result of the study shows that the major problems facing Ecommerce in India. E-commerce stands for electronic commerce. E-commerce is improving standard among the business community in worlds, about the opportunities offered by E-commerce. And it's trading in goods and services through the electronic medium. There are the issues of security and citizen's income and therefore the implementation of sophisticated security measures could make a difference and change in Indian's mentality about E-Commerce. E-Commerce has unleashed yet another revolution, which is changing the way businesses buy and sell products and services. 200 primary data were collected for this research and proved that the economic growth of India on the field of e-commerce in the current scenario.

Keywords: E-Business, Electronic Card (Debit, Credit), E-Payment, E-Data Interchange, Electronic Funds, E-Services.

I. INTRODUCTION

E-business and Online shopping is a part of e-commerce where the customers or consumers buy goods / products / and other services directly from the merchants over the internet. Today E-commerce or E-business is a byword in Indian society and it has become an integral part of our daily life. There are websites providing any number of goods and services. Theoretically it is more convenient to buy products online due to its flexible nature, but in India the adoption rate of the technology is significantly different from other nations because of the country's unique social and economic characteristics. India has diverse culture and extreme disparities of income.

1.1 Internet in India

With the prove of statistics it is clear that forty-eight million users in India and the Internet community in India is the fifth largest in the world, although Internet users formed only about 4.3 percent of the country's population in 2005. Access is gradually expanding from the most heavily populated urban centers, currently 41 percent of users, to small cities and towns. The E-commerce Industry in India has come a long way since its

early days. The market has matured and new players have entered the market space. In the present dynamic scenario, e-commerce market in the B2C space is growing in demand as well as in the array of services. According to TOI article ("With 243 million," 2013), internet penetration in India may not have crossed 16% of the population, but that's enough to reach a number which is approximately 10 times the population of Australia. The report published by Internet and Mobile Association of India (IMAI) and Indian Market Research Bureau (IMRB) estimates 243 million internet users in the country by June 2014, overtaking the US as the world's second largest internet base after China. The following years that indicating to the internet market of india from the beginning stage…….

1986: ERNET project starts up; email exchange using UUCP protocol established between National Centre for Software Technology, Bombay, and IIT Bombay (Bombay was renamed Mumbai in 1995)

1987: Email exchange between ERNET institutions in metros; TCP over X.25 established between the ERNET gateway at NCST and internet via CWI in Amsterdam.1988: Leased lines used to connect ERNET partner institutions to ERNET gateway in Bombay.1989: LWBBS (Live Wire BBS) and BBS CiX launch online services; VSNL commissions a Gateway Packet Switching System (GPSS) running X.25 protocol; 1990: TCP/IP implemented for communication between ERNET centers connected by leased lines.1991: LWBBS turns into a paid subscription service and expands to other cities such as Ahmadabad, Madras (Chennai), Pune, Calcutta (Kolkata), Baroda, Vapi.

1992: Business India launches aXcess, a value-added service offering email as well as e-news, stock quotes.1997: Tamil newspaper *Dinamani* sets up website; Hotmail creator Sabeer Bhatia sells Hotmail to Microsoft for $400 million;

1998: Private ISPs allowed to set up internet infrastructure; LWBBS's Pune node, JabberWocky operated by WMI becomes the first ISP licensee;2000: Parliament passes Information Technology Act 2000; foreign portals like Yahoo and MSN set up Indian sites; Bazee.com launched based on the eBay model

2001: Subscription sites set up by thenewspapertoday.com and NaiDunia.com; Times of India group launches 8888 mobile service; India Today group launches 2424 mobile service; 2002: Malayalam Varikha.com, the website of weekly Malayalam magazine, launches paid site; NPTEL (National Programme on Technology Enhanced Learning) initiative launched;

2003: Air Deccan launches India's first online air ticketing site; 2004: DoT declares its Broadband Policy; BSNL introduces broadband; eBay buys Bazee.com; Monster.com buys Jobsahead.com; 2005: Social networking sites like Orkut make their presence felt; online registration of .IN domains begins; Indic language user interface appears on basic cell phones

2006: Facebook makes India debut; 2007: Major media websites switch to tab-based design; Arzoo.com re-launched as a travel portal by Sabeer Bhatia; Twitter makes its India debut; Google News launches Hindi service

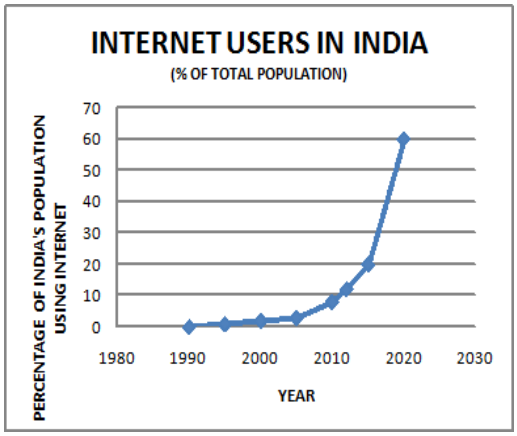
2008: India sets a world record by sending 10 satellites into orbit in a single launch; Apple iPhone debut in India; Internet Governance Forum (IGF) held in India; 2009: GoI puts forth the draft policy on Indian language IDNs.

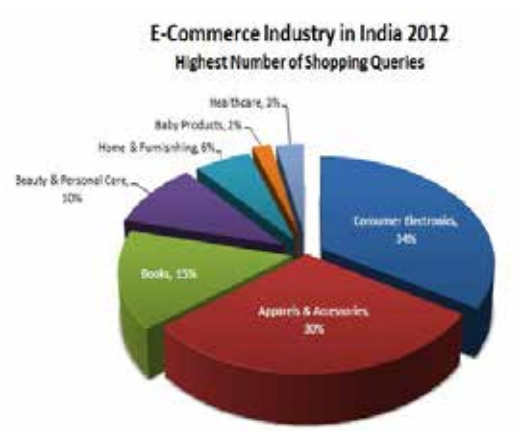
2010: 3G spectrum auctioned by telecom players 2011: Mobile number portability launched; ICANN approves 7 Indian language Internationalized Domain Names (IDNs) for India; iPad enters India market after its Dell and Samsung rivals; Pearson Group takes controlling stake in e-education startup Tutor Vista; Indian government

launches National Knowledge Network (NKN); The major drivers of internet penetration in India are mobile devices, with some of the cheapest and most basic hand-sets today offering access to the internet. India has 110 million mobile internet users of which 25 million are in rural India. The growth of internet penetration in rural India is driven largely by the mobile phone; 70% of rural India's active internet population accesses the web via mobile phones. This may have to do with the difficulty in accessing PCs.

Lastly am showing a graph which represents the using of internet users in the India from 1980-2030

The graph indicate the rate of internet users in India based on the population





1.2 E-Commerce in India

Over the last two decades, rising internet and mobile phone penetration has changed the way we communicate and do business. E-commerce is relatively a novel concept. It is, at present, heavily leaning on the internet and mobile phone revolution to fundamentally alter the way businesses reach their customers. While in countries such as the US and China, e-commerce has taken significant strides to achieve sales of over 150 billion USD in revenue, the industry in India is, still at its infancy. However over the past few years, the sector has grown by almost 35% CAGR from 3.8 billion USD in 2009 to an estimated 12.6 billion USD in 2013.Industry studies by IAMAI indicate that online travel dominates the e-commerce industry with an estimated 70% of the market share. However, e-retail in both its forms; online retail and market place, has become the fastest-growing segment, increasing its share from 10% in 2009 to an estimated 18% in 2013. Calculations based on industry benchmarks estimate that the number of parcel check-outs in e-commerce portals exceeded million in 2013. However, this share represents a miniscule proportion (less than 1%) of India's total retail market, but is poised for continued growth in the coming years. If this robust growth continues over the next few years, the size of the e-retail industry is poised to be 10 to 20 billion USD by 2017-2020. This growth is expected to be led by increased consumer-led purchases in durables and electronics, apparels and accessories, besides traditional products such as books and audio-visuals.

II. LITERATURE REVIEW

The different studies have highlighted the benefits that Internet shopping offers to consumers which include ability to shop round the clock at anywhere, to search and browse products, to compare prices, and to make flexible electronic payments (Hoffman et al., 1995; Alba et al., 1997; Peterson et al., 1997; Strauss and Frost, 1999; Shim et al., 2001).

Web design are typically not sufficiently academically inclined to formulate the relevant theories (Day, 1997). Elizabeth Goldsmith and Sue L.T. McGregor (2000) analyzed the impact of e-commerce on consumers, public policy, business and education. A discussion of public policy initiatives, research questions and ideas for future research are.

While previous research has examined Internet usage (Teo, Lim, & Lai, 1999),commercial websites (Gonzalez and Palacios, 2004), Mauricio S. Featherman, Joseph S. Valacich & John D. Wells (2006) examined whether consumer perceptions of artificiality increase perceptions of e-service risk.website design (Kim, Shaw, & Schneider, 2003), website effectiveness from the consumers' perspective (Bell & Tang, 1998)., pricing paid placements on search engine (Sen et al.2008), Search engine has become a necessity for people to surf the web [Hsien-Tsung Chang, 2011]. Khan and Mahapatra (2009) studied that the quality of internet banking (i-banking) services in India from customer's perspective. Malhotra and Singh (2007) carried out a research to find the I -banking adoption by the banks in India. Thus, it is high time that India should act fast and decisively in order to use the growing electronic trade to our advantage.

Lavie and Tractinsky (2004) have expressed the expressive aesthetics of web-sites that convey a sense of creativity and uniqueness. This type of aesthetics is likely to serve an important role when shopping for specialty goods. The expressive design is relevant to specialty goods because of their unique characteristics that emphasized the shopping experience. Bauer et al., (2006) have compared the services of online retail service vs. traditional retail services. They have identified that the online retail services are broken into two rather distinct phases: the client interaction phase taking place online and the fulfillment phase taking place offline. They also have suggested that web-site quality is a matter of delivering both hedonic and utilitarian elements.

India's e-commerce market was worth about $2.5 billion in 2009, it went up to $6.3 billion in 2011 and to $14 billion in 2012. About 75% of this is travel related (airline tickets, railway tickets, hotel bookings, online mobile recharge etc.). Online Retailing comprises about 12.5% ($300 Million as of 2009). India has close to 10 million online shoppers and is growing at an estimated 30% CAGR vis-à-vis a global growth rate of 8–10%. Electronics and Apparel are the biggest categories in terms of sales. (http://en.wikipedia.org/wiki/E-commerce_in_India) A recent statistical data has shown that Indians are purchasing all sorts of products through online shopping portals. In recent times even used computers are being purchased online. (Bhattacharjee Sarathi Partha,.et al., 2012;) investigates the relationship between globalization, ecommerce adoption or acceptance that lead to business performance and effectiveness.

The penetration of online shopping and money spent in India is much lesser when compared to USA and UK, but it is growing at a much faster rate than expected and with new entrants in larger number. Online shopping has truly revolutionized and influenced our society as a whole.

(Kumari Renu,.2013;) Use of technology has opened new doors and opportunities that enable for a more convenient lifestyle today. Variety of products, quicker services and reduced price are the three significant ways in which online shopping influenced people in India and world as a whole. However, this concept of online shopping led to the possibilities of fraud and privacy conflicts. Unfortunately, it has shown that it is possible for hackers to access personal information. Today with the latest features of technology, measures are being taken in order to stop hackers and criminals from accessing private databases. Through privacy and security policies, developers are doing their best to put an end to this unethical practice. That will pave the way for its success. (Patna, 2013)

III. NOW WHAT IS THE RELATIONSHIP BETWEEN FDI AND E-COMMERCE?

One group of e-commerce entrepreneurs argues that FDI would boost infrastructure development and manufacturing so there will be more efficient supply chain management and reduce costs while another group of e-commerce entrepreneurs argues that FDI in e-commerce sector may lead to multinationals availability of their cheaper products on the market may cause a negative impact on the Indian manufacturing sector generally on small and medium enterprises like small time businesses or kirana stores will be hurt by this, leading to large scale unemployment.

3.1 In India E-Commerce Accounts for Only a Small Fraction of India's Retail Industry Why?

Foreign money coming into e-commerce sector will certainly boost the capital intensive industry which has been struggling for raising funds for facilitate expansion and attain economies of scale. Actually for increasing e-commerce, the main requirements is the accessing of internet but current estimates are that only 15 percent of population. The 2nd issue is that population of our country is illiterate so visual or voice application will be developed to encourage them for utilizing the internet for E-commerce. The 3rd issue is of using vernacular language not English. Broadband connection in India should be encouraged.

Way of receiving FDI in Indian companies

An Indian company may receive FDI via two routes. These are:-

3.1.1 Automatic Route

FDI is allowed under the automatic route without the prior approval of government of reserve bank of India. For all activities/sectors included in FDI policy must be issued by government of India from time to time.

3.1.2 Government Route

FDI is allowed under this route requires prior approval of the government which are considered by the Foreign investment promotion board, Department of economic affairs and ministry of finance.

FDI of e-commerce in India.

FDI is totally banned in e-commerce before jury 2014. In august 2014 budget' time the commerce minister's statement comes at a time when Enforcement directorate is closely scanning the capital structures of various companies operating in the e-commerce scope.

Then it is found that many big e-commerce companies like Flipkart (retail) and many others violating the foreign exchange management act provisions ,The problem is in the thin line b/w operations of B2B (wholesale) company and a B2C (retail) company. So currently, India permits 100% FDI in B2B e-commerce activities but not in B2C companies. B2C companies have to adopt the marketplace model. Wherein they take order but which are filled by other domestic retailers. But problem arises when domestic B2C e-commerce Company operates through the marketplace model but uses their other FDI funded ventures in the B2B space for retail.

The companies which broke the rule that is using FDI in B2C they can be shakeout from the sector. Flipkart have to raise money to pay the penalties which will be three times the investment.

IV. OBJECTIVES OF THE STUDY

The e-Business market in India is in the introductory stage of its life cycle. There will be a huge growth in the market and seen that some risks are there to buying online. So this study is undertaken to investigate the present

market scenario from the customer point of view and find out the economic and business growth of online business in India .The major research objectives are as follows: -

1) To study the contribution of e-commerce industry towards the economic development in India.
2) To analyze changing paradigm of e-commerce in this current era.
3) To study e-commerce and its socio economic impact on entrepreneurship development in India.

V. E-COMMERCE: SOCIO-ECONOMIC DEVELOPMENT IN BTAD

Socio-economic condition in rural areas of BTAD is still in a very poor condition. As such socio-economic development in the rural areas is a crying need. In order to achieve its goal in the field
of business and employment generation a medium is required to reach to the teeming millions of rural people, and to act as an interface between the planners and the people. That medium can be provided by the Communication and Information Technology and Electronic commerce

VI. IMPACT OF E-COMMERCE ON ECONOMY [1]

Business and the economy are inextricably linked with the development and implementation of new technology (Tassabehji, 2003). Growth and development of any modern economy has been recognized by many economic theorists, such as Kondratieff, Schumpeter, Mensch and Porter, to be based on innovation of new technology. Porter (1990) emphasizes that the prosperity and competitive advantage of a nation is no longer as a result of a nation's natural resources and its labour force, but rather the ability of its industry to innovate and upgrade. This can be seen as a disruptive technology on a macro environmental level. And today, the impact of new technology on the economy of a nation is indisputable. Continuous growth of E-commerce is expected to have deep impact on structure and functioning of economies at various levels and overall impact on macro economy.
Socio-economic condition in rural areas of BTAD is still in a very poor condition. As such socio-economic development in the rural areas is a crying need. In order to achieve its goal in the field of business and employment generation a medium is required to reach to the teeming millions of rural people, and to act as an interface between the planners and the people. That medium can be provided by the Communication and Information Technology and Electronic commerce. Electronic commerce can play a big role in encouraging rural entrepreneurs of BTAD area and thereby promoting village (both Micro and Small–scale) industries.

6.1 E-Commerce in World Wide Web

E-commerce is one of the most important factors in the globalization business. Other factors comprise reduce in trade barriers, globalization of capital markets, the movement toward International Financial Reporting Standards (IFRS), and Internet financial reporting. Internet financial reporting has been predominantly helpful to e-commerce companies (Hunter and Smith 2008). IFRS is a global standard for accounting and financial reporting (Smith 2008). The annual growth rate of e-commerce globally has been predictable as high as 28 percent, while some individual countries have much higher growth rates. For example, in India, which has a younger than average market, the e-commerce growth rate has been projected as high as 51 percent.

VII. DATA ANALYSES METHODOLOGY

The data collected from the survey will be subjected to data cleaning in order to identify missing value, sample characteristics and meet the assumptions of normality. After this, the descriptive analysis will be used to summarize the respondents' demography. Factor analysis will also be employed in this regard to help in reducing the number of variables that do not measure the constructs in this study as perceived by the respondents. In this case, the component factor analysis with varimax rotation will therefore be conducted on all the variables to extract factors from the scales of each construct. The researchers will ensure that all items meet the acceptable limit level. Therefore, in this study, all items below 0.50 will not be retained and those having a loading factor limit of above 0.50 will all be retained. The validity of the instrument will be determined by content and construct validity. The construct validity will be determined through the factor analysis in which the Kaiser- Meyer (KMO) index of sampling adequacy and Bartlett's test of sphericity will equally be determined. All variables with KMO above .56 - .6 will be regarded as valid for this proposed study.

VIII. FACTOR ANALYSIS RESULTS

A total of 200 respondents were surveyed using the questionnaire. The raw data was analyzed through SPSS 17.0 (Green et al., 2000) and factor analysis in order to summarize the 20 variables (as each question in Part - 2 (Consumer opinion) of survey questionnaire represent one variable) into smaller sets. Then data was subjected to principal component analysis. Hence, these 20 variables were reduced to nine principal components through varimax rotation. Items with factor loadings of 0.50 or higher were clustered together to form separate constructs, as recommended by Hair et al. (2006). Here, the researcher had considered only those factors whose Eigen-values is more than one, as significant. Table 5 indicates that, in the present test the Kaiser-Meyer-Olkin (KMO) measure was 0.562 Bartlett's sphericity test also found highly significant; Chi-Square =1843.318, df = 351 with a significance of 0.000 it provide support for validity of the factor analysis of the data set and indicates that, factor analysis is appropriate.

Kmo and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.577
Bartlett's Test of Sphericity	Approx. Chi-Square	1268.892
	df	190
	Sig.	.000

Component Matrix(a)

	Component					
	1	2	3	4	5	6
BUSINESS	-.034	-.188	-.130	.513	-.495	.181
CONVIENI	-.119	.431	-.012	.562	.068	-.310
CROWD	.025	-.242	-.190	.680	-.294	.324
E_DATA	-.116	.575	-.177	.462	.232	-.092
ECO_DEV	.378	-.295	-.307	.262	.170	.479
E_PAYMNT	.120	.565	-.164	.260	.532	-.017
TIME	.693	-.161	-.301	-.089	.134	.135
LIFE_STL	.240	.669	-.138	-.076	.171	.188
B_ENV	.750	-.068	-.237	-.245	.029	.012
ECONOMY	.344	.606	-.073	-.212	-.119	.160
EBS_USE	.727	-.174	-.045	-.021	-.051	-.014
MODRNTY	.367	.562	.078	-.019	-.301	.185
CC_MUSE	.643	-.065	.208	.262	-.154	-.192
PRIVACY	.193	.505	.341	-.003	-.421	-.065
ORDER	.461	-.086	.491	.157	-.042	-.328
TECHNLGY	.002	.256	.680	-.032	-.215	.138
ISSUES	.306	-.287	.596	.140	.317	-.280
UNEMP	-.078	.012	.721	.016	.039	.418
E_BIZ_RQ	.193	-.245	.356	.318	.423	.055
CYBERLAW	-.150	.044	.400	-.048	.298	.626

Extraction Method: Principal Component Analysis.

a 6 components extracted.

In the Rotated Component Matrix table, each number represents the partial correlation coefficient between variable and rotated component. All the variables having factor loadings of greater than .50 for a given component define the component.

Factors like e payment, e-data, economy, technology unemployment solving issue are of more importance.

IX. CONCLUSION & SUGGESTION

The above factors represent different elements of e-commerce in India which form the above mentioned analysis. After a detailed discussion based on Factor Analysis with **KMO and Bartlett's Test** the following factors generally associated with e-commerce and economy in India, *viz.*

(i) E-business,

(ii) Economic ,

(iii) Business environment,

(iv) E-data interchange,

(v) Technology,

(vi) E-security.

The companies are looking forward to transact online and the existing companies already Providing e-business facilities have to focus on all the above factors. The most prominent and Vital characteristic for adoption of any new technology, is generating awareness among the Customers and educating them about that specific technology. Hence, if the consumers of India are not eagerly adopting Online Shopping, it may be because they are not aware about the most prominent and vital characteristic for adoption of any new technology is generating awareness among the customers and educating them about that specific technology. Hence, if the consumers of India are not adopting e-commerce, it may be because they are not aware about such a service being available and the added value that it offers. They should simplify the initial setup process and also provide troubleshooting.

Convenience & Trust is the second factor considered for this research study. In order to successfully implement the e-commerce, companies must ensure that the services are easy, simple, and rapid and of sufficiently high quality to give growth to the economy of the country so that the country's GDP rises in a sustainable manner and to ensure consumer satisfaction in order to maintain e-customers. A user friendly website with a good graphical user interface and easy to use navigation tools will certainly help in this regard.

Technology is the important factor of this study. Social network sites (like facebook, twitter) that is based on the different technology. Technology which helped to create and maintain the websites as well as make a web portal etc. The software like Php, .Net and JSP helped to maintain this. So basically technology helps to growth of economy from the different perspective in Indian current scenario. Our study is basically e-business oriented and all the social sites and online sites based on the different technologies and they can help to growth the economic position on the Indian market, because of many online shopper purchase the different product from the online sites and they are aware of the technology. Most of the people believe that online sites is best because of they are continuing offer more and more and they purchased the product from Merchander directly. Sites are like flipkart, Amazon, SnapDeal, e-bay, matra.com without that we can't purchase online product and it helps to economic growth of Indian market. So technology is very essential and without the technology we can't make the social sites as well as online sites.

Security and Risk is another important factor. The element of risk in this context would relate to the security of transacting for consumers and determine the acceptability rate of this alternative delivery channel in the long run. To control the risk factor marketers has to provide consumer reassurance and information. Improve application as well as online payment information security and privacy, train & advise e-customers for following secure online transaction practices and other risk related factors.

Develop easy & user friendly customer support applications for flexibility reasons.

The economy of the country rises from entrepreneurial developments but in this 21 century the main revolution happened in the field of technology so, entrepreneurs came in to being so the e business played the very essential role in the countries development.

According to our point of view the e business sector is one of the major important parts of the current system. Digital marketing is another area will develop to increase of Indian market economic scenario.

REFERENCES

[1] Elizabeth Gold smith and Sue L.T .McGregor (2000); E-commerce: consumer protection issues and implications for research and education;

[2] Venkatesh, V. and Morris, M. G., "Why Don't Men Ever Stop To Ask for Directions? Gender,Social Influence, and Their Role in Technology Acceptance and Usage Behavior," MIS Quarterly Vol. 24, No. 1: 115-139, 2000.

[3] Wang, F. and Head, M. (2002): "E-tailing: An analysis of web impacts on the retail market", Journal of Business Strategies, vol 19, no 1, ABI/INFORM Global, p. 73

[4] M. S.Khan and S. S.Mahapatra, "Service quality evaluation in internet banking: an empirical study in India", Int. J. Indian Culture and Business Management, vol. 2, no. 1,(2009),pp. 30-46.

[5] P.Malhotra and B. Singh, "Determinants of internet banking adoption by banks in India", Internet Research, vol. 17,no.3,(2007),pp. 323-339.

[6] H.-T.Chang and S.Wu,"A Switching Proxy for Web Search Engines. Advanced in Information Sciences and service Sciences", Advanced Institute of Convergence Information Technology,vol. 3, no. 5,(2011),pp. 52.

[7] R.Sen, S.Bandyopadhyay, J. D. Hess and J. Jaisingh,"Pricing paid placements on search engine", Journal of Electronic Commerce Research, vol. 9, no. 1,(2008),pp. 33-50.

[8] Xin Luo, Han Li, Jie Zhang, J.P. Shim, "Examining multi-dimensional trust and multi-faceted risk in initial acceptance of emerging technologies: An empirical study of mobile banking services," Decision Support Systems, vol. 49, no. 2, pp. 222-234, 2010.

[9] Zhang Lingying, Tan Wojie, Xu Yingcong, Tan Genlue, Dimensions of Consumers' Perceived Risk and Their Influences on Online Consumers' Purchasing Behavior. CISME Vol. 2, Iss. 7,2012, PP.8-14, www.jcisme.org ? C 2011-2012, World Academic Publishing.

[10] Jun, G., & Jaafar, N. I. (2011). A Study on Consumers' attitude towards Online Shopping in China. International Journal of Business and Social Science, 2(22), 122-132.

[11] A.Kulkarni Product Manager:http://yourstory.in/ 2013/01/indian-e-commerce-what-does-the-future-look-like/.

[12] Kumari Renu,. (2013) September. Problem and Prospects of E-commerce in Retailing. IJRESS (ISSN 2249-7382), Volume 3, Issue 9. Retrieved from http://www.euroasiapub.org/IJRESS/Sep2013/4.pdf

[13] Patna, H. C. (2013). Is online shopping booming in india? - an empirical study. Retrieved fromhttp://www.mbaskool.com/business-articles/marketing/7695-is-online-shopping-booming-in-india-an-empirical-study.html

[14] http://articles.timesofindia.indiatimes.com/2013-11-14/internet/44073307_1_internet-and-mobile-association- internet-penetration-rural-india