PERFORMANCE COMPARISON OF (2TX1R) AND (2TX2R) MIMO CDMA SYSTEM USING SPACE TIME BLOCK CODE (STBC)

Ms Neha Sharma[1], Sachin Chawla[2] , Taruna Sikha[3]

[1-2]M.Tech Scholar, [3]Assistant Professor, Department of Electronics & Communication Engineering, SPGOI Rohtak (India)

ABSTRACT

The demand for wireless communication systems with high data rates and high capacity has dramatically increased. CDMA (Code Division Multiple access) plays an important role in modern wireless communication systems. MIMO refers to links with multiple antennas at the transmitter and receiver side. For next generation cellular system CDMA & MIMO is very necessary technology and performance of depend upon the spreading strategy. We proposed MIMO-CDMA system with STBC (Space-Time Block Code) matrices for spreading and outcome permutation spreading method. Simulation results shows that gain improvement with STBC approach as compared to other existing techniques. MIMO is a technique to increase data rate significantly with multiple antennas at both the transmitter and receiver. MIMO takes the advantage of random fading and multipath delay spread. MIMO systems will need to function reliably in interference limited environment in order to be effective. CDMA systems are designed to operate in an interference free environment and for this reason it is used in modern cellular systems. The combination of MIMO and CDMA can further improve the system transmission rate over the traditional CDMA system. Multiuser MIMO CDMA systems are considered where each user has multiple transmit antennas, different transmit antennas of the same user use the same spreading code.

In this paper space time block coding with 2 transmit antenna and two receive antenna can be consider Using MATLAB as a simulation tool. A comparison statement is develop between 2x1 and 2x2 transmitter and receiver combination and obtain performance of the system with one, two, transmitting antenna over the rayleing channel.

Keywords: Discrete Cosine Transform, Fast Fourier Transform, JPEG

I. INTRODUCTION

Wireless communication is the transfer of information over a distance without the use of electrical conductors or "wires". We can optimize various types of mobile, fixed and two-way radios, cellular system and wireless system which demand the wireless communication services grown tremendously. For the next generation system like 3rd generation network has been much slower than already existing system and our goal to introduce much higher network against exiting network. Researchers are already investigating 4th generation systems and this system will transmit at much higher rates than the actual 2G systems, and even 3G systems, in an ever crowded frequency spectrum. Signals in wireless communication environments are impaired by fading and multipath delay spread and due to fading the overall performance of the system become degrade. Hence, several

avenues are available to mitigate these impairments and fulfill the increasing demands. The demand for wireless communication systems with high data rates and high capacity has dramatically increased. CDMA (Code Division Multiple access) plays an important role in modern wireless communication systems. MIMO refers to links with multiple antennas at the transmitter and receiver side. In CDMA systems, the narrowband message signal is multiplied by a very large bandwidth signal is a Spread sequence as space time block code Space–time block coding is a technique used in wireless communications to transmit multiple copies of a data stream across a number of antennas and to exploit the various received versions of the data to improve the reliability of data-transfer. In this work MIMO-CDMA(with two transmitter and two receiver) system is designed with STBC (Space-Time Block Code) matrices for spreading [2]. The proposed technique outperforms the design permutation spreading method and also the conventional method. Simulation results shows that gain improvement with STBC approach as compared to other existing techniques. This work deals with orthogonal space-time block coding schemes and a realistic channel model was used. In MIMO-CDMA to improve the bit error rate performance parity bit selected spreading sequences are introduced initially [2], in this linear block coding technique is used. In that Parity bits are used to select the spreading sequence from a set of orthogonal spreading sequences. Information can be added with spreading code and at receiver, the spreading code help out to determine the filter output and Message bits are recover from the specific match filter. Error in specific information can be correct by assuming that parity bits are correct. In this paper, Spreading permutations scheme is introduce to improve the BER performance for MIMO CDMA System. As earlier techniques, this technique improves the BER but additional complexity introduces [3]. Recently, there are a large number of researches for multiple inputs multiple outputs (MIMO) in CDMA transmission.

II. STBC AND EXPERIMENT STEP

MIMO systems can be defined as arbitrary wireless communication system, consider a link in which the transmitting ends as well as the receiving end is equipped with multiple antenna elements as shown in Figure 1. The idea behind MIMO is that the signals on the transmit (TX) antennas at one end and the receive (RX) antennas at the other end are “combined” in such a way that the quality (bit-error rate or BER) or the data rate (bits/sec) of the communication for each MIMO user will be improved. Such an advantage can be used to increase both the network’s quality of service and the operator’s revenues significantly [4][5][6][7].

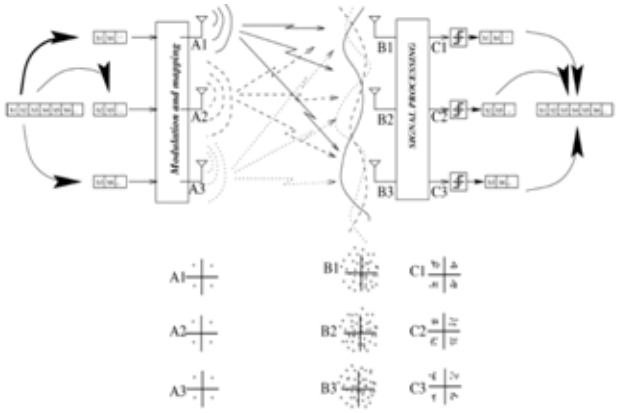


Figure 1: Multiple Input Multiple Output system.

Core idea in MIMO [1] systems are space–time signal processing in which time (the natural dimension of digital communication data) is complemented with the spatial dimension inherent in the use of multiple spatially distributed antennas. As such MIMO systems can be viewed as an extension of the so-called smart antennas, a popular technology using antenna arrays for improving wireless transmission dating back several decades. It is important to note that each antenna element on a MIMO system operates on the same frequency and therefore does not require extra bandwidth. Also, for fair comparison, the total power through all antenna elements is less than or equal to that of a single antenna system. i.e.,

$$\sum_{k=1}^{N} p_k < p$$

Where N is the total number of antenna elements, pk is the power allocated through the kth antenna element, and P is the power if the system had a single antenna element. Effectively, the equation ensures that a MIMO system consumes no extra power due to its multiple antenna elements [5][6][8][11]. At the transmitter side, a block of two symbols is taken from the source data and sent to the modulator. After that, Alamouti space-time encoder takes the two modulated symbols, in this case called s1 and s2 creates encoding matrix S where the symbols s1 and s2 are mapped to two transmit antennas in two transmit time slots.

The encoding matrix is given by:

$$S = \begin{bmatrix} s1 & s2 \\ -s_{12}^{*} & s_1^{*} \end{bmatrix}$$

The fading coefficients denoted by h1(t) and h2(t) are assumed constant across the two consecutive symbol transmission periods and they can be defined as:

$$h1(t) = h1(t+T) = h1 = |h1|e^{j\theta 1}$$
$$h2(t) = h2(t+T) = h2 = |h2|e^{j\theta 2}$$

The receiver receives r1 and r2 denoting the two received signals over the two consecutive symbol periods for time t and t+T. The received signals can be expressed by:

$$\begin{bmatrix} r_1 \\ r_2 \end{bmatrix} = \begin{bmatrix} s_1 & s_2 \\ -s_2^{*} & s_1^{*} \end{bmatrix} \begin{bmatrix} h_1 \\ h_2 \end{bmatrix} + \begin{bmatrix} n_1 \\ n_2 \end{bmatrix} = \begin{bmatrix} h_1 s_1 + h_2 s_2 + n_1 \\ -h_1 s_2^{*} + h_2 s_1^{*} + n_2 \end{bmatrix}$$

The maximum likelihood (ML) decoder chooses a pair of signals (s1, s2) from the signal constellation to minimize the distance metric over all possible values of s1 and s2.

$$d^2(r_1, h_1\hat{s}_1+h_2\hat{s}_2) + d^2(r_2, -h_1\hat{s}_2^{*} + h_2\hat{s}_1^{*})$$
$$= |r_1-h_1\hat{s}_1-h_2\hat{s}_2|^2 + |r_2+h_1\hat{s}_2^{*}-h_2\hat{s}_1^{*}|^2$$

For phase-shift keying (PSK) signals, the decision rule can be expressed by:

$$d^2(\hat{s}_1, s_i) \le d^2(\hat{s}_1, s_k) \vdash i \ne k$$
$$d^2(\hat{s}_2, s_i) \le d^2(s2, s_k) \vdash i \ne k$$

$$\begin{bmatrix} \tilde{s}_1 \\ \tilde{s}_2 \end{bmatrix} = \begin{bmatrix} h_1^{*} & h_2 \\ h_2^{*} & -h_1 \end{bmatrix} \begin{bmatrix} r_1 \\ r_2^{*} \end{bmatrix} = \begin{bmatrix} h_1^{*} r_1 + h_2 r_2^{*} \\ h_2^{*} r_1 - h_1 r_2^{*} \end{bmatrix}$$

The combiner shown in Figure 2 builds the following two combined signals that are sent to the maximum likelihood detector.

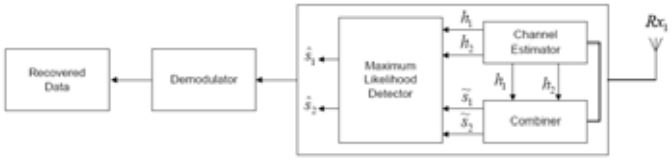


Figure 2: Alamouti space-time decoder

The principle of space time block coding with 2 transmit antenna and one receive antenna with STBC. With two receive antenna's the system can be modeled as shown in the figure below

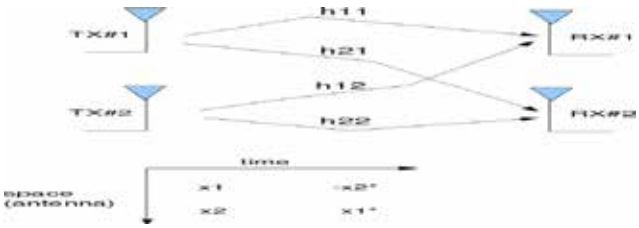


Figure: 3 Transmit 2 Receive with STBC

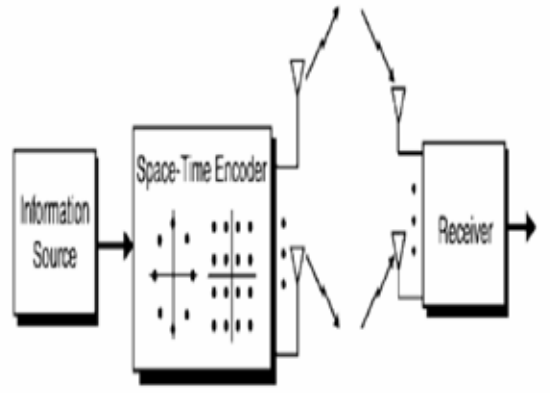


Figure 4: Overall Block diagram

In conventional MIMO-CDMA, each user use a different spreading code for each transmitting antenna. In conventional MIMO-CDMA system the spreading waveforms are fixed.

Wmi =Cmi (t-nT) ---------- (1)

Where Wmi is the spreading waveform for ith data stream of user m and Cmi is the orthogonal spreading sequence. Each antenna uses one spreading waveform, for Nt =4 antennas system 4 spreading waveforms are required per user. At the receiver side, the received data is given bank of matched filters. Orthogonal space-time block codes (O-STBC) achieve high transmit diversity and have a low complexity decoding algorithm at the receiver using any number of transmit and receive antennas [10][11].

III. MIMO-CDMA DESIGN

The receiver performs a time correlation operation to detect only the specific desired codeword. All other code words appear as noise due to decorrelation [12]. For detection of the message signal, the receiver needs to know the codeword used by the transmitter. Each user operates independently with no knowledge of the other users. CDMA is achieved by modulating the data signal by Space Time Block Code [13].

Fig4:-Block Diagram for Transmission

Figure 5:-Block Diagram for Reception

Improving the capacity of code-division-multiple access (CDMA) systems through advanced signal processing has been an area of intensive research for many years, with limited success. Multiantenna technologies called multiple-input multiple outputs (MIMO) are an obvious candidate to increase, particularly, downlink capacity. Nearly all research on MIMO–CDMA, however, has focused on increasing the throughput achieved per user, rather than increasing the number of supportable users, which is still the most important design goal in QoS-constrained voice systems[16]. The objective is to evaluate the MIMO OFDM performance and to reach its optimal data transmission. This was accomplished by selecting an OFDM standard and evaluating its performance under several user-channel profiles[17][21][22].

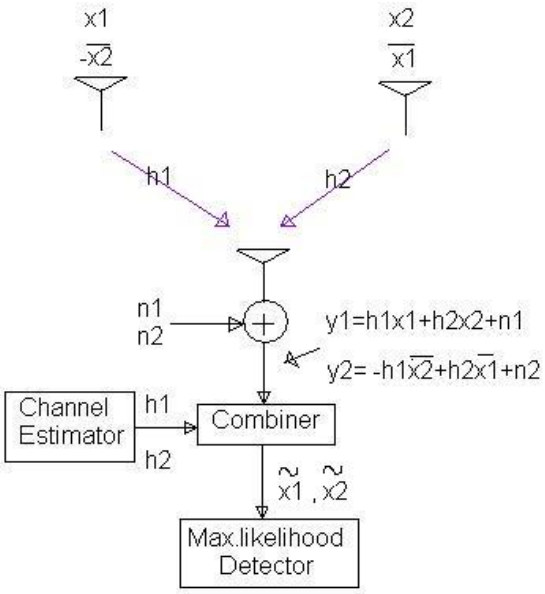


Figure 6: MIMO STBC STBC 2TX1R

In this case study we can consider two scenarios to perform the performance the comparison in 2Tx1R and 2Tx2R transmitter –receiver combination and goal of the research to introduce MIMO Technology in CDMA using state space block coding. A novel transmission scheme is developed to effectively combine permutation

spreading technique with MIMO-OFDM to obtain improved bit error rate performance in the presence of frequency selective fading channels with low system complexity [18]. Unlike conventional MIMO-OFDMA, where users are separated in different frequency bands (sub channels), and each user is coded separately using STBC or SFBC, the proposed new scheme enables multi access by joint code design across multiple antennas, subcarriers, and users. Such system will benefit from the combined space and frequency domain freedom as well as multiuser diversity [19]. Hence, better spectrum efficiency is achieved while improving bit error rate performance with respect to signal-to-interference ratio.

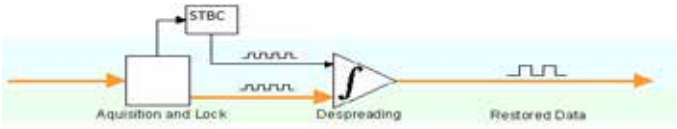


Fig5: space-time decoder/Encoder

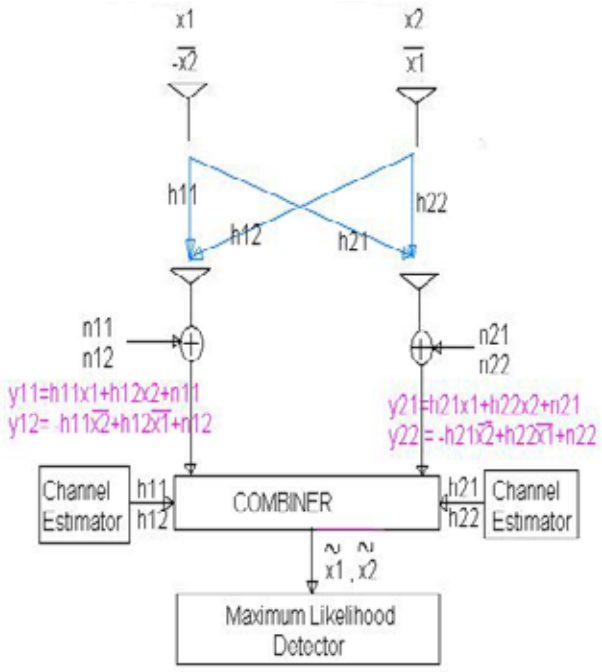


Figure 7 MIMO STBC 2Tx2R

Frequency selectivity challenge due to the large bandwidth in the next generation wireless communications is a major problem; as a result subcarriers in OFDM may experience high frequency dependent attenuations on transmission over such frequency selective fading channels. In a non-line-of sight multipath transmission environment, the symbols carried by the subcarriers are consequently erased by the channel attenuations and cannot be accurately recovered at the receiver, which results a poor system performance. It thus becomes fundamental to exploit the spatial diversity made possible by MIMO system especially when the channel and array structures are such that the transfer functions between different transmit and receive antenna pairs are sufficiently uncorrelated. ST coded MIMO-OFDM cannot neither achieve multipath diversity nor high rate, on the other hand, SF-coded MIMO- OFDM is considered the best candidate for future wireless communication. By mapping the symbols on other sub-channels, it can exploit the multipath diversity. However, the system complexity is a major obstacle and the decoding complexity problem has to be tackled. In addition to that, most of the existing ST/SF codes are designed for single user systems only, for multiple access channels (MAC), the

single-user ST/SF codes are always applied to each user independently, which results a reduced transmission rate.

This technique was originally proposed for CDMA in and recently adapted for MIMO-CDMA in the presence of frequency selective fading channel. A novel approach is developed here to effectively combine and permutation block spreading techniques with MIMO-OFDM to obtain improved bit error performance in the existence of frequency selective fading channel and greatly lower system complexity. In MIMO-OFDMA, users are separated in different frequency bands (sub-channels), and each user is coded separately using STBC or SFBC, leading to data rate reduction for each user when the number of users is increasing. The proposed new scheme enables multi access through the use of orthogonal spreading codes, where multiple data symbols share common subcarriers while their signals remain separable at the receiver. With suitable selections of spreading codes, the frequency diversity created by multipath propagation in the communications channel is exploited to improve the bit error rate (BER) over standard OFDM. Based on the matched filters decision, the transmitted data is estimated. Space–time block coding is a technique used to improve the performance of a wireless transmission system, where the receiver is provided with multiple signals carrying the same information. The concept behind space-time block coding is to transmit multiple copies of the same data through multiple antennas in order to improve the reliability of the data-transfer through the noisy channel. This is shown in

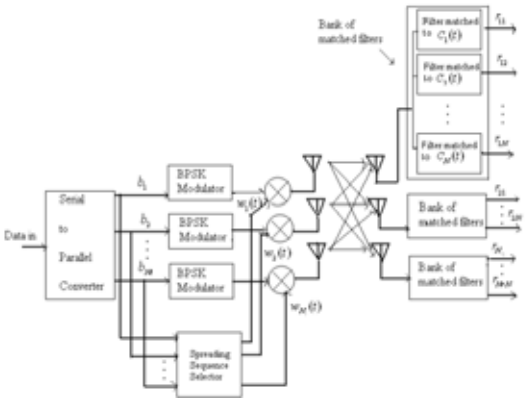


Figure 8: Overall Block diagram for MIMO-CDMA with STBC

The Matlab performs the following operation

1. Generate random binary sequence of +1′s and -1′s.
2. Group them into pair of two symbols
3. Code it as per the Space Time code, multiply the symbols with the channel and then add white Gaussian noise.
4. Equalize the received symbols
5. Perform hard decision decoding and count the bit errors

Repeat for multiple values of Eb/No and plot the simulation and theoretical results.

IV. MODEL FOR SIMULATION AND SCENARIO

An antenna is a device used for transmitting and/or receiving electromagnetic waves which are operated in radio frequencies (RF), a range of 10 kHz to 300 GHz. The size and shape of antennas are determined from the frequency of the signal they are designed to receive. An antenna must be tuned to the same frequency band that

the radio system to which it is connected operates in, otherwise reception and/or transmission will fail. Therefore, antennas couple electromagnetic energy from the space to other mediums. In the recent years, due to the wireless cellular evolution many antenna technologies were proposed which provide more quality, capacity, and coverage. These types of antenna systems are the sectorized antenna systems, diversity antenna systems and many others. However, antennas are operated in a noisy environment where many hostile effects should surpassed or minimize in order the communication.

Multipath interference is a phenomenon where two or more waves are transmitted at the same time from a base station and travel through different paths towards the receiving end whereas, before the reception they interfere with each other causing a phase shift

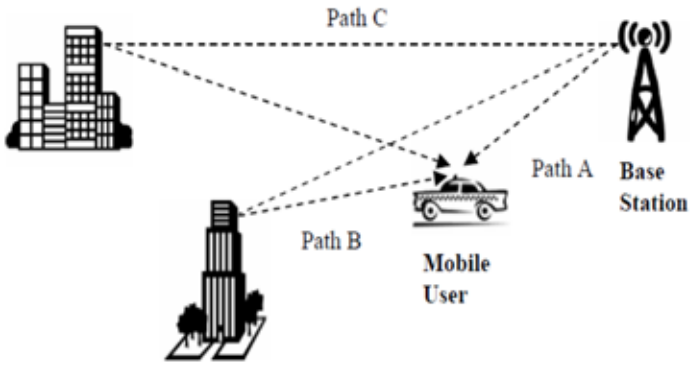


Figure 9: Fading Model

Wireless communication industry has recently turned to a strategy called Multiple- Input Multiple-Output (MIMO). MIMO is the single most important wireless technology as of today. MIMO is a technology evolution where both ends of the wireless link are equipped with antenna array this can improve the quality (bit-error rate) and the data rate (bits per sec). Therefore, a superior quality of service (QoS) can be achieved, which revenues the wireless provider. Many space-time block codes for different number of transmit/receive antennas have been developed in order to achieve maximum diversity. MIMO takes advantage of multipath interference effect to increase the user and data capacity; it converts it into a positive feature by using the multiple transmitters and/or receivers to increase throughput and reliability. Usually, multiplexing would cause interference, but MIMO uses the additional pathways to transmit more information and then combines the signal at the receiving end; thus provides robustness against multipath fading. MIMO systems can be designed with the receiver knowing the channel state coherent case) or not (not-coherent case).

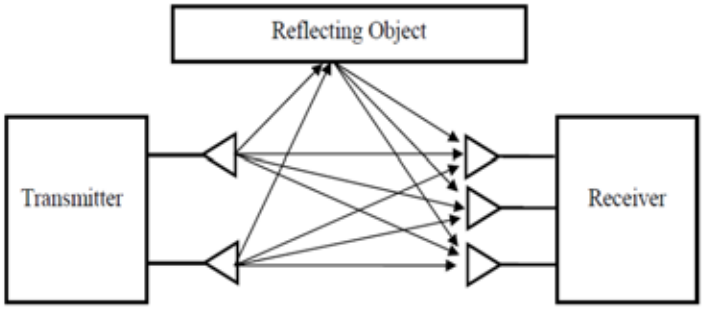


Fig9: Multipath Fading Tansmission And Reception

An efficient way to improve data rate and transmission reliability over wireless links is through the use of MIMO systems each pair of transmit-receive antennas has a single scalar channel coefficient**.** In this paper, our main focus to calculate the performance of the system for (2:2) transmitter- receiver and (4:4) transmitter-receiver scenario. Performance comparison shows complexity of the system and BER of the system.

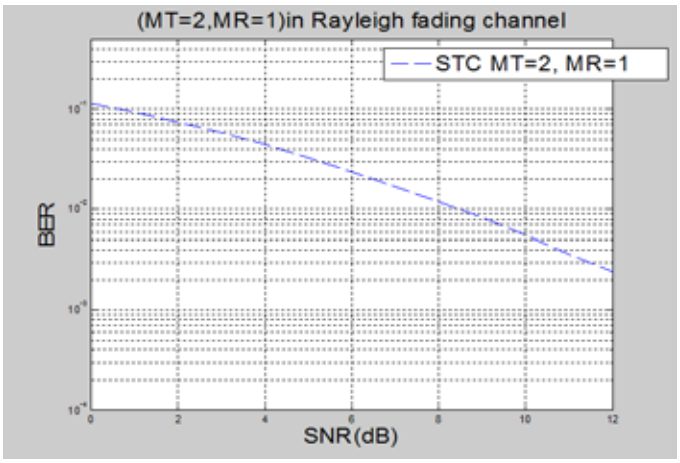


Figure 10: BER vs SNR at MT=2 and MR=1

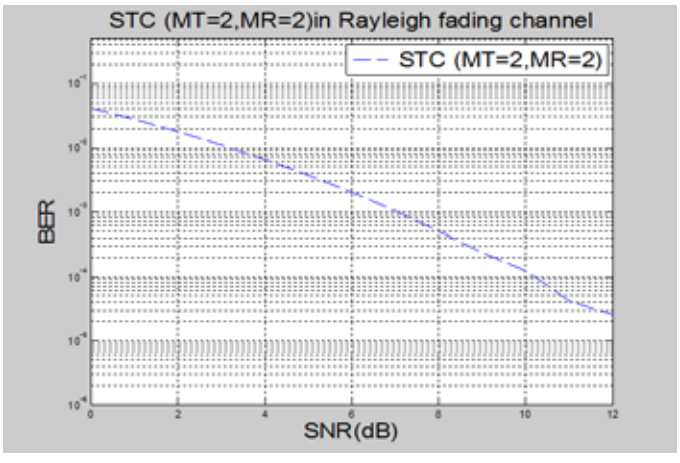


Figure 11: BER vs SNR at MT=2 and MR=2

V. RESULT AND FUTURE SCOPE

We can observe that better results are produced by the system which uses more number of receiver antennas. This is due to the fact that as the number of receiver antennas increases, the diversity of the system will increase.

Higher diversity will give better performance. So while designing the STBC for a particular application, it is needed to select the number of antennas at both ends of the communication link, the modulation and the rate of transmission. By using the proper STBC technology, it is possible to improve the data rate and range of the wireless communication systems

Finally as a future expansion of this paper, it is possible to introduce different modulation schemes to increase the data rates. Also we can increase the number of antennas at both transmitter and receiver without introducing any interference in between the antennas.

ACKNOWLEDGMENT

This research was supported by the SPGOI Rohtak under their strategic award program. I am thankful to Ms. Taruna Sikka for their support and proper giddiness.

REFERENCES

[1] Daniel W. Bliss, Keith W. Forsythe, and Amanda M. C “MIMO Wireless Communication “, Lincoln Laboratory Journal , Vol.15, No.1, 2005.

[2] Vahid Tarokh, Nambi Seshadri, and A. R. Calderbank (March 1998). "Space–time codes for high data rate wireless communication: Performance analysis and code construction". *IEEE Transactions on Information Theory* **44** (2) 744–765.

[3] Digital Communication: Third Edition, by John R. Barry, Edward A. Lee, David G. Messerschmitt

[4] V.V.S.N Bharat Kumar, Tripty Singh ,Mithun R ”BER and LLR Analysis with MC-CDMA using BPSK/QAM Techniques for Wireless Communication” ISSN (Online): 2347 - 2812, Volume-2, Issue -3, 2014

[5] P. Sreesudha, M. Vijaya Lakshmi “Ber enhancement of mimo-cdma based on Space-time block codes” Computer Science & Information Technology (CS & IT) David Bracewell, et al. (Eds): AIAA 2011,CS & IT 03, pp. 21–26 , 2011. © CS & IT-CSCP 2011

[6] R. C. de Lamare †and R. Sampaio-Neto “Blind Adaptive MIMO Receivers for CDMA Systems with Space-Time Block-Codes and Low-Cost Algorithms” arXiv.org > cs > arXiv:1410.5510v1

[7] Gourav Rajak, Rajesh Nema ,“Analysis of space-time block Coded system for wireless Communication”, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering Vol. 2, Issue 7, July 2013

[8] Nordin Bin Ramli, Tetsuki Taniguchi, and Yoshio Karasawa, “Subband adaptive array for Mimo-cdma space-time block coded system”

[9] Prabagarane Nagaradjane, Arvind Sai Sarathi Vasan, **“**Adaptive Co-Channel Interference Suppression Technique for Multi-User MIMO MC DS/CDMA Systems, Int. J. Communications, Network and System Sciences, 2009, 2, 822-826

[10] K.Sureshkumar, R.Rajalakshmi, A.Vetrikanimozhi” , Channel Estimation for MIMO MC-CDMA Systems”, International Journal of Distributed and Parallel Systems (IJDPS) Vol.2, No.6, November 2011

[11] Bramha Swaroop Tripathi, Monika Kapoor , "Review on ds ss-cdma transmitter and receiver for ad hoc network using vhdl implementation", International Journal of Advances in Engineering & Technology, Jan. 2013

[12] M. Abu Faisal, Mohima Hossain and Shaikh Enayet Ullah", Performance Evaluation of a Multi Antenna MC-CDMA System on Color Image Transmission under Implementation of Various Signal Detection Techniques

[13] http://en.wikipedia.org/wiki/History_of_mobile_phones

[14] Bijan Golkar, Florence Danilo-Lemoine, "Space-time coding and spatial multiplexing in mimo Multicarrier cdma" The 18th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC'07)

[15] M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[16] L. Hanzo, T. H. Liew, and B. L. Yeap, Turbo Coding, Turbo Equalization and Space-Time Coding for Transmission over Fading channels. John Wiley & Sons, 2002.

[17] G. H. Golub and C. F. V. Loan, Matrix computations. Baltimore & London: Johns Hopkins Univ. Press, 1996.

[18] X. Zhang and B. Ottersten, "Performance analysis of V-BLAST structure with channel estimation errors," 4th IEEEWorkshop on Signal Processing Advances in Wireless Commun. SPAWC 2003, pp. 487–491, June 2003

[19] Matthias stege and Fettweis G, "Multistratum-permutation codes for Multiple input multiple outputcommunication",

[20] IEEE Communication Letters, Vol. 21, June 2003, Page No. 774-782.

[21] Amours C.D, and Chouinard J, "Parity bit selected and permutation spreading for MIMO-CDMA systems, in Proc. IEEE Vehicular Technology, Apr 2007, Page No. 1475-1479.

[22] Adel Omar D, and Amours C.D, "Spreading strategies for MIMO-CDMA in presence of channel

[23] estimation errors and spatial correlation", Vehicular Technology Conference, Nov 2009, Page No. 1-5

[24] Nordin Bin Ramli, Tetsuki Taniguchi and Yoshio Karasawa," Sub band Adaptive Array for MIMO STBC CDMA System", IEICE Trans. Fundamentals, Vol. E90–A, Oct. 2007, Page No. 2309-2317.

[25] Min Shi, Amours C.D, "Design of Spreading Permutations for MIMO-CDMA based on Space-TimeBlock Codes", IEEE Communication Letters, Vol. 14, Jan 2010, Page No. 36-38.

[26] V. Tarokh, H. Jafarkhani, and A. R. Calderbank, "Space-time block codes from orthogonal designs,"IEEE Trans. Inf. Theory, vol. 45, pp. 1456- 1467, July 1999

Ms Anjali Sheoran is presently pursuing M. Tech. final year in Electronics & Communication Engineering Department (from SPGOI Rohtak, India.

Mr. Sachin Chawla is presently pursuing M. Tech. final year in Electronics & Communication Engineering Department (from SPGOI Rohtak, India

Mr. Ajay Khokhar is working as an Assistant Professor in Electronics & Communication Engineering Department (from SPGOI Rohtak, India).

360 DEGREE APPRAISAL SYSTEM AND ITS SUITABILITY FOR INDIAN PRIVATE SECTOR BANKS- AN EMPIRICAL STUDY

Dr.K.Vivekanandan[1], Dr.N.Mohan[2]

[1]Professor and Director, [2]Professor and Head of the Department,
Gnanamani Institute of Management Studies, Namakkal (India)

ABSTRACT

PAS (Performance Appraisal System) is a very predominant component of overall HRD system in any organization. Whether it is manufacturing sector or services sector, periodic appraisal of employees is a very important HR developmental tool towards focusing career development of an organization. A large number of organizations have been using 360 degree feedback in India as leadership development intervention. The concept of performance appraisal is still emerging and finding space in both academic and practitioner spheres. This paper focuses on appraisal in Indian private banking sector. Banking sector, a live catalyst for business sector as it contributes to economic development of a nation. PAS is being used to evaluate whether employees at various levels of perform their assigned jobs as per the expectations of their supervisors & set standards. PAS in Private sector banks has been in vogue over past many decades and periodic changes are getting introduced in this system. This paper brings out features of 360 degree Appraisal and its suitability & relevance for Private Sector Banks in our country.

Keywords: Banking sector, Performance Appraisal, PAS, 360 degree appraisal, , PMS.

I. INTRODUCTION

Performance appraisal system (PAS) is an important Human Resource Development (HRD) mechanism designed and utilized for the all round development and growth of employees as well as organizations.

Organizations use a variety of methods for evaluating employee performance. There are so many types of performance management methods, understanding how each of them works will help to determine the best one to use within your organization. Each type has benefits and drawbacks. Performance appraisal systems solve the review process problem—normally a formidable and complicated task—by making it both efficient and effective for managers and employees. HR often gets bogged down with the process, and managers are often untrained in delivering effective reviews that actually reflected in workforce performance and
help to grow the business.

But there's a much bigger business impact to be had from an online performance appraisal system than simply time saving method. The centralisation will lead to thrive the managers effectively and caus. The managers can more easily communicate business strategy and create measurable goals for their employees that will support overall company objectives. This, in turn, gives management the tools to measure individual performance throughout the organization and identify top performers for further development and establish a pay-for-performance compensation plan.

II. 360 DEGREE FEEDBACK

The use of a 360 degree feedback appraisal system is ideal to may prove the businesses that value the input of employees concerning the effectiveness of supervisors and managers. This type of performance appraisal method solicits input from employees of all ranks who interact with the employee being evaluated. Everyone from executive leaders to frontline workers receive anonymous and carefully considered feedback from co-workers. Using a 360 degree feedback method requires training on how to evaluate others. Individuals who do not have the experience of composing appraisal statements may need additional training pertaining to evaluating the quality of work rather than the employee's personality or popularity. Nevertheless, this is a very effective way to get a good reading on your management talent by obtaining commentary from the people who frequently interact with managers.

Many managers aspire that PAS occupy more time in their productive hours without adequate rewards; quit in few organizations are in search of perfect performance appraisal system for their organizations to promote and inculcate a performance culture among the employees. In the present research, efforts will be made to diagnose the factors involved for discontent among the employees at different levels about the operations of PAS and to know the remedy for the same. The present piece of research is also an attempt to identity the relevancy of 360 degree appraisal at organizational levels to make the appraisals more acceptable, more effective, more workable and more palatable.

2.1 Research Objective

The research Objective is to understand the relevance of 360 degree performance appraisal system particularly in context of Indian private Banking sectors only in urban area and to present the study findings based on individual perception of working bankers about their preference towards introducing 360 degree performance appraisal system within private sector banks.

2.2Literature Review

(Spriegel and Mumma, 2006 Rudrabsavaraj 2007; Levinson 2010)

Performances appraisal system provides information to management about and employee’s performance which can be used for succession plan by identifying the people with potentialities. It helps the management to take administrative decisions such as, pay increase, promotion, placement, transfer and lie off to help supervisors to know their subordinates and give an opportunity to the subordinates to know where they are in front of supervisors and stand with the boss

(Thathachary 2000, Latham & Wexley 2001 and Rao 2002)

Research has also indicated that quite often appraisal system practices are ill designed in most organizations this is mainly due to the fact that existing system is not effective. The reason was being the objective of this system does not need out nor made known to the employees. Many managers view that PAS occupy too much of their productive time without adequate rewards, quite a few organizations are in search of perfect performance appraisal system for their organizations to promote and inculcate a performance culture among the employees

(Rai and Singh, 2012)

360-degree feedback has been linked to several positive outcomes like improved performance, better interpersonal communication, smoother work relationships, etc

Himanshu Rai and Manjari Singh (2012)

In a recent study of the mediating effects of *360 Degree feedback* Himanshu Rai and Manjari Singh (2012) empirically examined the mediating effects in the relationship between 360-degree feedback and employee performance with a sample of executives (N=198) working in four organizations in Western India. The results showed that interpersonal communication and quality of working life (QWL) had a complete mediating effect. Leader member exchange quality and perceived organizational support were found to have a partial but significant mediating effect.

2.3 Results from Empirical study

During 2013-2014, a perceptional study was carried out among 100 senior private bankers randomly from different private sector Indian banks. The questionnaire was got responded during informal interactions in some training programs at training colleges of different banks.

2.4 Would you prefer 360 Degree Appraisal?

Response	**Percentage**
Yes	74 respondents
No	26 respondents
No comments	Nil

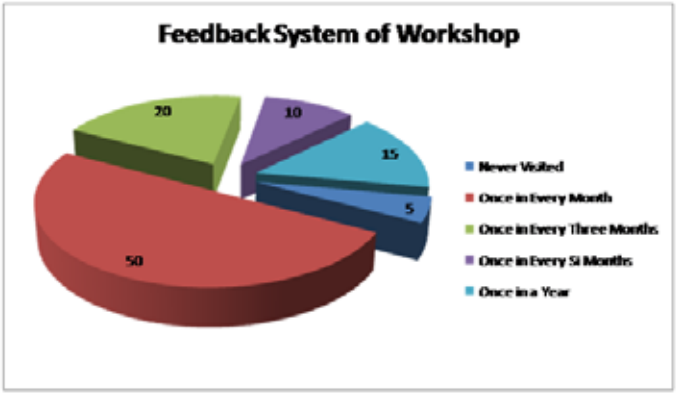
III. IMPACT AT INDIVIDUAL LEVEL

3.1To what extent individuals think “the leadership development” has been achieved through 360-degree feedback

The collected data interprets and outcomes as furnished below. Around 40 respondents felt that 360 Degree Feedback had fully achieved its aim of “leadership development”. 20 respondents felt that 75% of leadership development was achieved through 360 Degree Feedback system. 14 respondents felt that leadership development was achieved to an extent of 50% through 360 Degree Feedback system. 16 respondents felt that leadership development was achieved to a limited extent i.e. less than 50% out of only 5 individual felt that leadership development was achieved to an extent of 25% through 360 Degree Feedback system and the 5 felt that no development was achieved

3.2How often have you visited your 360 degree feedback data after the feedback system of workshop?

Review of 360 Degree Performance appraisal system	**No of respondents**
Never visited	5
Once in every month	50
Once in every three months	20
Once in every six months	10
Once in a year	15
Total	100



The above table shows that the no. of visitors over a period of tie to private banks. While analysing the data it has been noticed considerable visitors in percentage every month is high when compared with never visited customers.

3.3Top three changes that you have observed in yourself after the 360-degree feedback analysis (v1, v2 & v3).

The common areas where participants observed a change after 360 degree feedback are

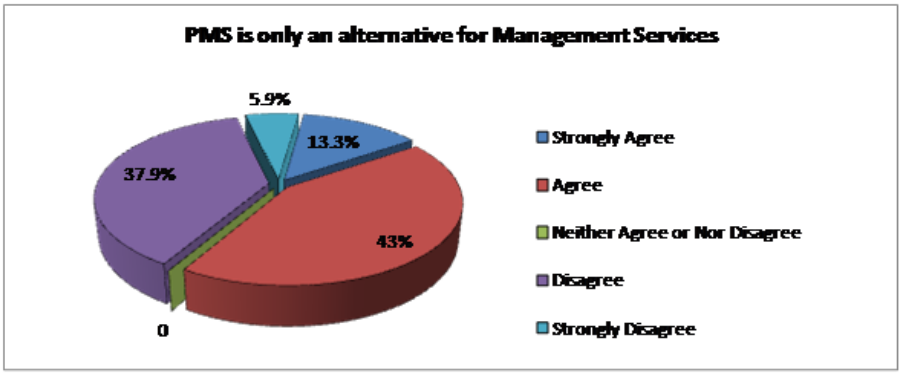
a little more interactive, is how to control my anger in difficult situation, recognizing and acknowledging other's contribution, articulate the vision/culture of department with colleagues, avoid sarcasm , become a better listener and less reactive among bank employees.

IV.ATTITUDE TOWARDS ORGANIZATIONAL SUCCESS

Perception towards Components of Organizational Success

Component	Strongly Agree	Agree	Neither Agree or nor Disagree	Dis Agree	Strongly Disagree	Mean and SD	Percentage Mean
1. PMS is only an alternative for Management Success. (V1)	30 (5.9%)	194 (37.9%)	O	220 (43.0%)	68 (13.3%)	2.63± 0.78	65.92
2. PMS is better than traditional performance appraisal system (V2)	16 (3.1%)	70 (13.7%)	0	230 (44.9%)	196 (38.3%)	3.18± 0.78	79.59
3. It helps in reducing strain, de-motivation and Conflicts. (V3)	30 (5.9%)	158 (30.9%)	0	224 (43.8%)	100 (19.5%)	2.76± 0.82	69.24

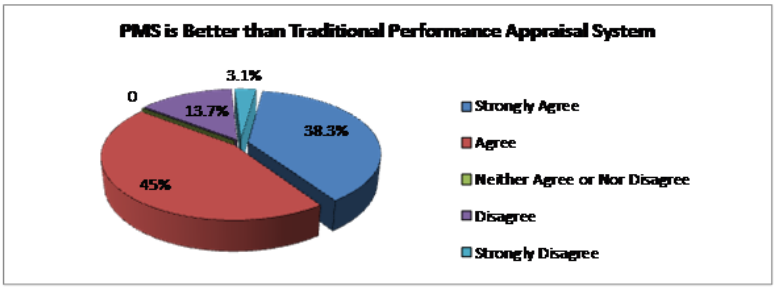
4.1 Performance Management System (PMS) is only an alternative for management success (V1)



As per the above table, we have chosen 512 respondents for our study. Only Five Point LIKERT Scale is used to collect data and interpreted for three variables such as PMS is only an alternative for management success (V1), PMS is better than traditional performance appraisal system (V2) and PMS helps in reducing strain, de-motivation and conflicts (V3).

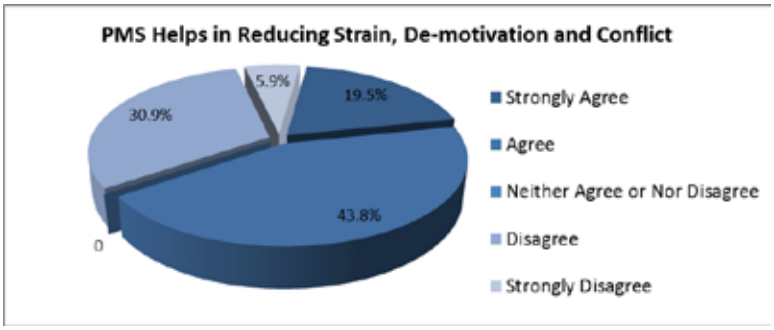
From the studies 5.9%of the respondents strongly agree, 37.9% of them agree, 43.0% respondents disagree, and 13.3% of them strongly disagree. The percentage mean 65.92 (Mean and SD (V1) 2.63±0.78) shows that PMS is only an alternative for management success as it falls in the category of **51%** to **75%.**

4.2 PMS Is Better Than Traditional Performance Appraisal System (V2)



The researcher has identified that 3.1% of the respondents strongly agree, 13.7% of them agree, 44.9% of them disagree, 38.3% of them strongly disagree that PMS is better than traditional performance appraisal system with Mean and SD (V2) 3.18±0.78. The percentage Mean 79.59 shows that PMS is better than traditional appraisal system as it falls in the category of **76%** to **100%.**

4.3 It Helps In Reducing Strain, De-Motivation and Conflict (V3)



Based on research studies 5.9% of the respondents strongly agree, 30.9% of them agree, 43.8% of them disagree, 19.5% of them strongly disagree that PMS helps in reducing strain, de-motivation and conflicts

among employees with Mean and SD (V3) 2.76±0.82 percentage Mean 69.24, this shows that PMS helps in reducing strain, de-motivation and conflicts among employees as 69.24% falls in the category of **51%** to **75%.**

V. CONCLUSION

The main finding of this research supports that the view of Performance Appraisal System (PAS) should be HRD oriented. Besides being a base for making administrative and developmental decisions, performance appraisal can be useful instrument for a) building a good relationship with employees, b) planning employee performance, c) discovering employee potential and improving organizational effectiveness. Organizations are increasingly implementing the self-appraisal and 360 degree appraisal instead of traditional top-down appraisal in hopes of improving satisfaction towards Performance appraisal (PA) practices. This study suggests that 360 degree appraisal system including multiple appraisal and developmental value based appraisal system can overcome the threat of personal bias. While no major attempt has so far been made to experiment and introduce 360 degree appraisal for officials in private sector banks. From this study it appears that a reasonable majority of bankers are really interested in using a 360 degree appraisal system and they felt a high relevancy of introducing the system in private sector banks in India. Moreover we may eradicate the empirical study on performance appraisal, most of the officials and top management cadre employee deal with their subordinates in biased manner. Hence this method of PAS motivates all levels of employees in the bank sector to improve their service levels in a better manner.

"FOR EVERY FAILURE THIS TIME, THERE WILL BE BETTER CHANCE NEXT TIME".

REFERENCES

[1] Rao, T. V. and Chawla, Nandini 360 Degree feedback and Assessment and Development Centres New Delhi: Excel Publications, 2005

[2] Landy F.J., & Farr, J.L. (1983), "The measurement of work performance: Methods, theory and Applications", New York: Academic Press.

[3] Roberts, Garry, E., (1995), "Performance appraisals in Fortune 1300", in Fimburn, Charles et al. (ed.) Strategic Human Resource Management, New York, Wiley

[4] Monappa, A., (1974), "Performance Appraisal", Case Material, Indian Institute of Management, Ahmedabad, IOB: 135

[5] Spiegel W.R. and Mumma E.W. (1998), "Merit Rating of Supervisors and Executives, Panel Study No. 14". Bureau of Business Research, University of Texas

[6] Mathis, Robert L., and John H. Jackson. *Human Resource Management*. 13th ed. Mason, OH: Thomson/South-Western, 2011.

[7] Dessler, Gary. *Human Resource Management*. 12th ed. Boston: Prentice Hall, 2011

[8] Mathis, Robert L., and John H. Jackson. *Human Resource Management*. 13th ed. Mason, OH: Thomson/South-Western, 2011.

[9] Noe, Raymond A., John R. Hollenbeck, Barry Gerhart, and Patrick M. Wright. *Human Resource Management: Gaining a Competitive Advantage*. 7th ed. Madison, WI: McGraw-Hill Irwin, 2010.

[10] Adler, N.J. (1991). *International dimensions of organizational behaviour*. Boston: PWS-Kent Publishing Company.

[11] Aron, A., & Aron, E.N. (1999). *Statistics for psychology*. (2nd ed.). New Jersey: Prentice-Hall International, Inc.

[12] Hartmann, L.C. (1998). The impact of trends in labour-force participation in Australia. In M. Patrickson & L. Hartmann (Eds.), *Managing an ageing workforce* (3-25). Warriewood, Australia: Woodslane Pty Limited.

[13] Adams, J.S. (1965). Inequity in social exchange. In L. Berkowitz (Ed.), *Advances in experimental social psychology* (Vol. 2, 267-299). New York: Academic Press.

[14]Forteza, J.A., & Prieto, J.M. (1994). Aging and work behaviour. In H.C. Triandis, D. Dunnette, & L.M. Hough (Eds.), *Handbook of industrial and organizational psychology*. (2nd ed., Vol. 4, 447-483). Palo Alto, CA: Consulting Psychologists Press.

[15] Hewstone, M., & Brown, R. (Eds.). (1986). *Contact and conflict in intergroup encounters.* Oxford: Basil Blackwell Ltd.

[16] Dow, Warren. "Consultants: the Rodney Dangerfield's of the Nonprofit World." (2000)

BIOGRAPHICAL NOTES

Bard Kuvaas (2006), "Performance appraisal satisfaction and employee outcomes", International Journal of Human Resource Management, Vol. 17 No. 3 Journal Papers

Bedford:cranfield university,Centre for Business Performance (2006), "Literature Review on Performance Measurement and Management", Agency, Improvement and Development Agency: 39.

M Singh, N Vohra Multi-faceted feedback for organisational heads for self and organisational International Journal of Training and Development, 2005.

PERFORMANCE COMPARISON BETWEEN OFDMA AND SC-FDMA USING RAYLEING FADING CHANNEL

[1] Monika Sehrawat, [2] Ritika Singh, [3] Priyanka Sharma

[1,2] M.Tech Scholar, [3] Assistant Professor,

Department of Electronics & Communication Engineering, SPGOI *Rohtak (India)*

ABSTRACT

To meet the increasing demands on the mobile radio systems and data traffic, a successor of UMTS, which runs on an evolution of the existing infrastructure used by over 80 percent of mobile subscribers globally, has been worked on by 3GPP, called Long Term Evolution (LTE). This will permit more powerful and better spectral efficiency of the transmission. The major parts of LTE are Single Carrier Frequency Division Multiple Access (SC-FDMA) & Orthogonal Division Multiple Access (OFDMA). OFDMA is used as multiple access method and it's providing immunity of multi-path and frequency selective fading. SC-FDMA is introduced recently and it became handy candidate for uplink multiple access scheme in LTE system.

In our paper, we analyzed the performance of SCFDMA and OFDMA for BPSK Modulation scheme on the basis of BER by simulating the model of SCFDMA & OFDMA in MATLAB. We used Additive White Gaussian Noise (AWGN) channel and introduced frequency flat fading in the channel by using Rayleigh fading model to evaluate the performance in presence of noise and fading.

Though the total channel is a frequency selective channel, the channel experienced by each subcarrier in an OFDM system is a flat fading channel with each subcarrier experiencing independent Rayleigh fading.

Keywords: LTE, 3GPP, SCFDMA, OFDMA, AWGN

I. INTRODUCTION

Designing an efficient wireless communication system is always a challenge. With increase in demand for high data rate this task has become even more challenging. To achieve this challenging goal next generation system came in to existence. Recent standard introduced by 3GPP group which promises high-speed data, multimedia unicast and multimedia broadcast services for next generation cellular concept. Single Carrier Frequency Division Multiple Access (SC- FDMA) & Orthogonal Division Multiple Access (OFDMA) are the major parts of the Long Term Evolution (LTE). OFDMA is used in the LTE downlink as a multiple access method as it provides good bandwidth efficiency, immunity to multi-path and frequency selective fading, and less complex equalization at the receiver[1].

OFDMA is a multiple access technique which uses Orthogonal Frequency Division multiplexing (OFDM) for each user. In this technique each user is allotted separate channel and available frequency band of that channel is divided into number of orthogonal frequency subcarriers. The high speed serial data from each user is first converted into low speed parallel bit streams with increased symbol duration then it is modulated on each

subcarrier using conventional modulation schemes. OFDMA allows achieving high data rate for each user. With little modification to air interface it can be deployed across different frequency bands. OFDMA reduce the effect of multipath fading because data from each user is modulated over several orthogonal frequencies rather than a fixed frequency for entire connection period. In addition, the OFDMA is bandwidth efficient as orthogonal frequency carriers with small spacing is used. All these advantage make it to be used in the downlink transmission of LTE[2][3]. OFDM is referred as multicarrier modulation. It uses multiple RF carrier signals at different frequencies which send some of the bits on each of the assigned channels. This seems to be similar to FDM but in the case of OFDM, total subcarriers are divided into sub channels and these sub channels are mapped to one single data/traffic source[4].

SC-FDMA is a multiple access method. Its structure is same as OFDMA with an addition of Fast Fourier Transform (FFT) block. The parallel data streams are first passed through FFT block then are modulated on subcarriers because of this the SC-FDMA is also called DFT-Precoded OFDM. The main difference between OFDMA and SC-FDMA is, in OFDMA, each data symbol is carried on a separate subcarrier while, in SC-FDMA, multiple subcarriers carry each data symbol due to mapping of the symbols' frequency domain samples to subcarriers. As SC-FDMA is derived from OFDMA it has same basic advantages as OFDMA but the spreading of each data symbol over multiple subcarriers gives it the profound advantage of lower PAPR value as compare to that of OFDMA. Hence PAPR is a useful parameter for uplink it is used in uplink transmission [4][5].

SC-FDMA one extra module DFT is added before IFFT module in the transmitter chain and IDFT is added in the receiver chain. This converts OFDM chain into SC-FDMA chain. Without this two modules the chain is referred as OFDM transmit and receive chain. SC-FDMA system usually will have low PAPR (Peak to Average Power Ratio) compare to OFDM system. SC-FDMA system is less sensitive to frequency offset compare to OFDM system.

Our objective of this work is to analyze the performance system by considering two multiple access techniques (SC-FDMA and OFDMA) with adaptive modulation techniques BPSK. We have considered BER parameters to evaluate the performance of LTE. We have considered these parameters because they are vital in communication systems and we have achieved our results by simulating the OFDMA and SC-FDMA models in MATLAB [5][6].

II. EXPERIMENTAL APPROACH

In OFDMA transmitter, the high speed serial data from each user is first converted in to low speed parallel data streams. This increases the symbol duration which reduce the Intersymbol Interference (ISI) at the receiver. Then the parallel data streams are passed through modulator, where adaptive modulation schemes BPSK, is applied. This modulated data streams are then mapped to orthogonal subcarriers by dividing the available spectrum into number of orthogonal frequency subcarriers. This makes the time domain data stream from user a frequency domain data stream or signal as at different frequency different low speed data stream will be present. The IFFT stage converts these complex data streams into time domain and generates OFDM symbols. A guard band or cyclic prefix (CP) is inserted between OFDMA symbols in order to cancel the ISI at the receiver. The CP is inserted by taking some part from end of the OFDM symbol and putting it at the start of the symbol as shown in figure 2.1. The duration of these CP should be greater than the channel impulse response or delay

spread. After appending CP the data streams are converted to a serial data stream to be transmitted in the channel[8][9].

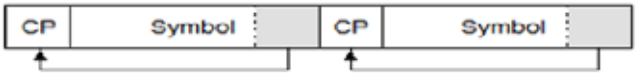


Figure 1: Inserting Cyclic prefix (CP)

At the receiver, the inverse processes of the transmitter occur. The serial data is converted to parallel data streams, CP is removed from each symbol and FFT stage converts the OFDM symbols in to frequency domain followed by subcarrier de-mapping and demodulation. Finally parallel data streams are converted to high speed serial data stream shows the block diagram of the model we used to simulate OFDMA system[10]. We wrote a MATLAB program to simulate the model shown in Figure 2.

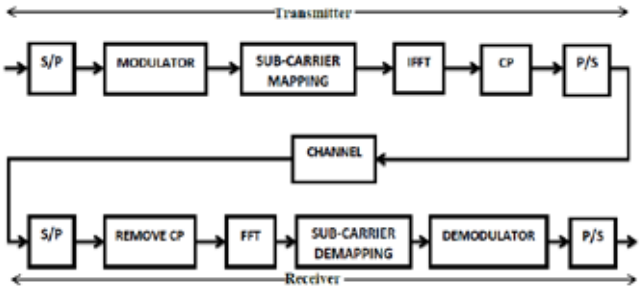


Figure 2: Block diagram of the OFDMA system mode

In SC-FDMA transmitter, after modulating parallel low speed data streams, the transmitter groups the modulated symbols into a block of *N* symbols. An *N*-point FFT block transforms these symbols in time domain into frequency domain. The frequency domain samples are then mapped to a subset of *M* subcarriers where *M* is typically greater than *N*. Similar to OFDMA, an IFFT block is used to generate the time-domain samples of these subcarriers, which is followed by appending cyclic prefix and parallel to serial conversion.

At the receiver just the opposite processes take place. Serial to parallel conversion, removing CP, taking FFT to convert to frequency domain, sub-carrier demapping followed by IFFT and demodulation[11].

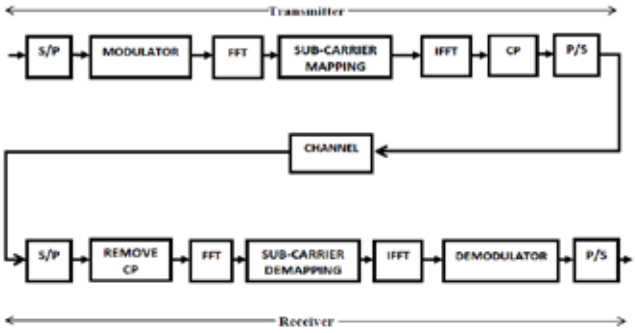


Figure 3: Block diagram of the SC-FDMA system model

Figure 3 shows the block diagram of the model we used to simulate SC-FDMA system. The model is same as that of OFDMA except an FFT block is inserted before sub-carrier mapping at the transmitter while an IFFT block is placed after sub-carrier demapping at the receiver. The steps for creating the program to simulate the model are same as that of OFDMA except we took FFT before sub-carrier mapping and IFFT after sub-carrier demapping.

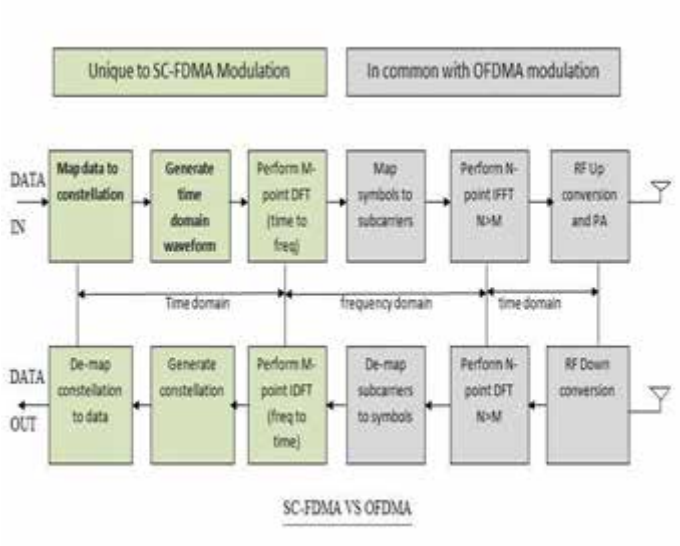


Figure 4: Comparison between SC-FDMA and OFDMA

The block diagram of SC-FDMA and OFDMA system in Figure 4 mentions modules unique to the SC-FDMA and in common with OFDMA system. As mentioned DFT before IFFT of OFDMA and IDFT after DFT of OFDMA system makes it SC-FDMA. The main contribution of this work is the analysis of the performance, in terms of BER and spectral efficiency, of a SC-FDMA system over fading channels. We paid special attention to the Rayleigh fading channel, which can be seen as a particular case of Nakagami-μ fading channel [12][13]. The obtained results were first validated through simulations and, then, compared to those obtained with OFDMA. These comparisons allow us to determine the difference in performance between both technologies. Other contributions made during the development of this work are listed next [15] .

III. DESIGN & PARAMETERS

OFDM also has many advantages compare to SC-FDMA. Frequency selective fading will be able to affect few of the sub channels/subcarriers and not entire band. OFDM overcomes effect of ISI occurring mostly in multipath channel environment. OFDM is used to achieve high data rate over single carrier system. Due to multiple carriers OFDM leads to high PAPR (Peak to Average Power Ratio) to overcome PAPR scrambler (randomizer) is used in OFDM based systems which spread the energy across wide bandwidth. There are various techniques to reduce the PAPR the same is explained in PAPR article. OFDMA transmits 4 qpsk symbols in parallel, one data symbol per subcarrier. SC-FDMA transmits qpsk symbols in the series but at 4 times the rate compare to OFDMA. Here qpsk symbol occupy much wider bandwidth about M x 15KHz where M is no. subcarriers

The BER is ratio of number of error bits and total number of bits transmitted. It is given by the following formulae.

BER = Number of Error Bits / Total Number of Transmitted Bits

To plot BER performance first we simulated the developed model, calculated BER for different Signal to Noise Ratio (SNR) values using the above formulae and then we plotted these values against corresponding SNR values[4][5][9][16].

The relation between **symbol energy** and the **bit energy** Eb/No and Es/No in OFDM is as follows

$$\frac{E_s}{N_0} = \frac{E_b}{N0}\left(\frac{nDSC}{nFFT}\right)\left(\frac{Td}{Td+Tcp}\right).$$

Expressing in decibels,

$$\frac{E_s}{N_0}dB = \frac{E_b}{N0}dB + 10log_{10}\left(\frac{nDSC}{nFFT}\right) + 10log_{10}\left(\frac{Td}{Td+Tcp}\right)$$

PARAMETERS	ASSUMPTION
Number of Sub-carriers	64
CP Length	7
Range of SNR in dB	0 to 35
Modulation	BPSK,
Data Block Size	16
Channel	AWGN Channel
System Bandwidth	5 MHz
FFT and IFFT size	64
Fading	Rayleigh (frequency flat) fading

It is imperative that OFDMA is multi-carrier system with one data symbol carried over by one subcarrier; while SC-FDMA is a single carrier system where in each qpsk symbol is carried by one much wider bandwidth subcarrier. Refer difference between SC vs OFDM page to understand concepts of Single Carrier (SC) vs OFDM. Though symbol length remains same in both OFDMA and SC-FDMA which is about 66.7µS; SC-FDMA symbol contains more than one sub-symbol which represents qpsk data symbols. Parallel multiple data symbol transmission will lead to higher PAPR (Peak to Average Power Ratio) in the OFDMA system. In SC-FDMA, PAPR is same as that of original qpsk data symbols as M qpsk data symbols are transmitted in series at M time's rate compare to OFDMA[17].

SC-FDMA is widely used in LTE subscriber terminals in the transmit path and its variant OFDMA is used in the eNodeB downlink (or receive path of LTE subscribers). While OFDM is used in many broadband technologies such as wimax-16d/16e, WLAN-11a/11n/11ac

IV. DISCUSSION AND RESULT

Following are the steps or algorithm we followed while writing the program to simulate the model.

1. First we generated binary stream of data.
2. We converted this stream of data in to number of parallel streams of data.
3. We modulated these streams of data using different modulation schemes.(we used BPSK)
4. Then these modulated streams of data are mapped to different sub-carriers.
5. Then we took the IFFT of these mapped streams of data
6. CP was appended by taking some portion from end of each symbol and adding it at the beginning of the symbol.
7. Then the resultant parallel streams were converted to long serial data stream.

8. Then we created an AWGN channel by using a built in function in MATLAB in which the noise level is described by SNR per sample, which is one input parameter to the function.
9. We passed serial data stream through this channel (function).
10. For Rayleigh fading channel simulation we introduced fading using a built in function in MATLAB for Rayleigh frequency flat fading.
11. Corrupted data from channel were then converted to parallel data streams.
12. From each symbol CP were removed.
13. Then FFT of the streams were taken.
14. Data streams were de-mapped from the subcarriers.
15. Demodulations of data streams were done.
16. Finally parallel data streams were converted to serial data stream.

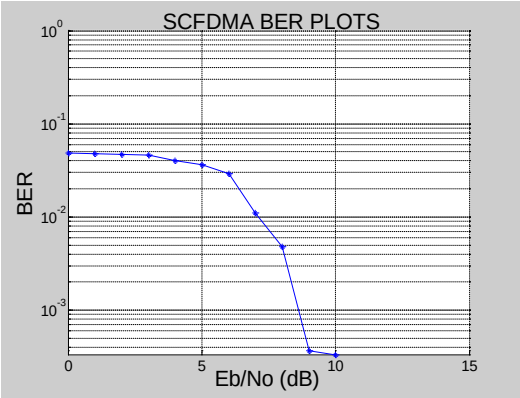


Fig 5: BER for SCFDMA

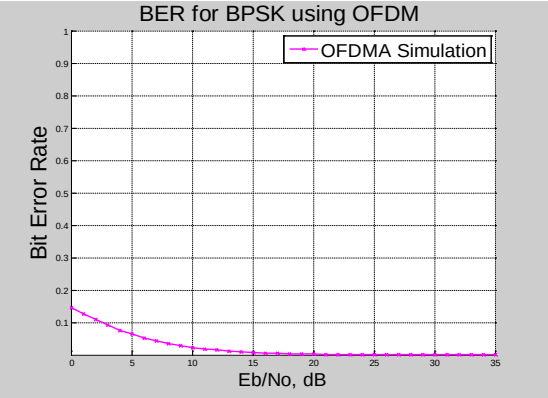


Fig 6: Vs BER for OFDMA

V. CONCLUSION & FUTURE WORK

BER is the key parameter for indicating the system performance of any data link. In our paper we analyzed that for different values of SNR, the BER increases for high order modulation in both the multiple access techniques (OFDMA and SC-FDMA) used in next generation system and hence it is easily affected by the noise. BER Performance of SC-FDMA and OFDMA are very similar but a part of them SCFDMA have good performance as compare to the OFDMA

For future prospect we can add more modulation scheme and also calculate more parameter such as Peak to Average Power Ratio**,** congestion and many more**.**

VI. ACKNOWLEDGMENT

This research was supported by the SPGOI Rohtak under their strategic award program. I am thankful to Priyanka Sharma for their support and proper giddiness

REFERENCES

[1] H. Holma and A. Toskala, “LTE for UMTS: OFDMA and SC-FDMA based radio access”, John Wiley & Sons Inc, 2009.

[2] Digital Communication: Third Edition, by John R. Barry, Edward A. Lee, David G. Messerschmitt

[3] S. Sesia, I. Toufik, and M. Baker, "LTE, the UMTS long term evolution: from theory to practice", John Wiley and Sons, 2009.

[4] Hyung G. Myung, Junsung Lim, and David J. Goodman, "SCFDMA for uplink wireless transmission", Polytechnic University

[5] S. Haykin, "Communication system", John Wiley & Sons, New Jersey, 2001.

[6] PJ.G Proakis and M. Salehi, "Digital Communications", Mc Graw Hill International, 5th edition.

[7] Ian Poole, "Cellular Communication Explained", Elsevier

[8] T.S. Rappaport, "Wireless Communication", Pearson, Second edition

[9] H.Taub, D.L. Schilling and G. Saha, "Principles of Communication Systems", Mc Graw Hill, 3rd edition.

[10] http://en.wikipedia.org/wiki/History_of_mobile_phones

[11] Alka Kalra, Rajesh Khanna ,"BER Performance comparison of SCFDMA & OFDMA in Multipath Channels", Thapar University.

[12] M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[13] Satish Singh, Rakesh Ranjan Pani," Software implementation of OFDM scheme for mobile radio channel", NIT Rourkela. G. H. Golub and C. F. V. Loan, Matrix computations. Baltimore & London: Johns Hopkins Univ. Press, 1996.

[14] X. Zhang and B. Ottersten, "Performance analysis of V-BLAST structure with channel estimation errors," 4th IEEEWorkshop on Signal Processing Advances in Wireless Commun. SPAWC 2003, pp. 487–491, June 2003

[15] Matthias stege and Fettweis G, "Multistratum-permutation codes for Multiple input multiple outputcommunication",

[16] IEEE Communication Letters, Vol. 21, June 2003, Page No. 774-782.

[17] estimation errors and spatial correlation", Vehicular Technology Conference, Nov 2009, Page No. 1-5.

Ms. Monika Sehrawat is presently pursuing M. Tech. final year in Electronics & Communication Engineering Department (from SPGOI Rohtak, India.

Ms. Ritika Singh is presently pursuing M. Tech. final year in Electronics & Communication Engineering Department (from SPGOI Rohtak, India.

Mr. Priyanka Sharma is working as a Assistant Professor in Electronics & Communication Engineering Department (from SPGOI Rohtak, India).

GREEN BUILDINGS-THE ENVIRONMENT SAVIOUR

Juhi Gupta[1], Anu Shrivatava[2]

[1,2]*Department of Electronics and Communication, SRM University, (India)*

ABSTRACT

Green buildings is the practice of creating structures and using processes that are environmentally responsible and resource efficient throughout a building's life-cycle from siting to design, construction, operation, maintenance, renovation and deconstruction. For certification of Green building LEED (Leadership in Energy and Environmental Design) is established.

It is assumed that the Green Buildings can be utilise for residential, office, school or industrial purpose. The construction of building should be done in such a way that they don't harm the environment as well as human beings. The design parameters not only reduce energy, water, and material resource but also it improves the indoor environmental quality, including reducing indoor pollution, improving thermal comfort, and improving lighting and acoustic environments that affect occupant health and productivity.

Green building is a possibility to create harmless, energy efficient and environmentally friendly buildings. Conventional building consumes too much natural sources, like energy, water, woods etc. while green building uses renewable resources as sunlight, plants, rainwater. The green building have more advantage over conventional building in the field such as Cost, Higher Property Value ,Energy efficiency , Water efficiency ,Material efficiency ,Maintenance.etcGreen Building are the steps towards the healthy and green future.

Keywords: Construction, Eco Friendly, Energy, Environmental Design And Green Building

I. INTRODUCTION

The term "green" refers to environmentally friendly practices from building design to the landscaping choices. It also encompasses energy use, water use, and storm water and wastewater reuse. The terms "green" and "green building" apply not just to products, but to construction strategies, building design and orientation, landscaping, building operations, maintenance, and more. The less impact a building has on human health and the environment,

The more green it is. A green building may cost more up front but, in the long run, will save money through lower operating costs over the life of the building. The green building approach applies a project lifecycle cost analysis to determining the appropriate up-front expenditure. This analytical method calculates costs over the useful life of the asset. A green building is not an assemblage of "environmental" components or a piecemeal modification of an already-designed, standard building. True green building takes a holistic approach to programming, planning, designing, and construction (or renovating) buildings and sites. It involves connecting often-interlinked issues such as site and climate, building orientation and form, lighting and thermal comfort, materials, etc., and optimizing all these aspects in concert.

II. METHODOLOGY INDULGE IN MAKING GREEN BUILDING

The methodology indulge in the making of green building is as follows:

2.1. Setting Green Goals and Objective

In the making of green building first steps is the establishment of firm environmental goals for the project. During this session, it is important to set specific measurable goals for things like energy efficiency, water conservation, on-site treatment of rain water and storm water, material and resource management, construction waste management, and to assign responsibility for meeting these goals to specific members of the design team. If the building is to be built in accordance with the United States Green Building Council (USGBC) Leadership in Energy and Environmental Design (LEED) green building rating system, it will be helpful to review the requirements of LEED as part of the green project goal setting session, begin targeting which elements of LEED are going to be pursued, and establish firm criteria for meeting those goals.

2.2. Building a Green Team

Hiring a design team with prior green design experience is highly desirable, but not essential provided that the design team is augmented with architects or engineering consultants who do have experience in green building and site design principles and technologies. The collective knowledge, experience, and dedication of the design team will determine the overall success of the green project. Once the goal setting process has been completed it may become obvious that meeting certain goals may require expertise that lies outside the current design team. Specialized consultants may need to be engaged for specific elements of the design and construction process or to oversee all elements of the green design program. These specialists will be able to bring new ideas and solutions to the table for consideration and should be included in the project as early as possible.

2.3. Integrated Design Process

Building a green building is not just a matter of assembling a collection of the latest green technologies or materials. Rather, it is a process in which every element of the design is first optimized and then the impact and interrelationship of various different elements and systems within the building and site are re-evaluated, integrated, and optimized as part of a whole building solution. For example, interrelationships between the building site, site features, the path of the sun, and the location and orientation of the building and elements such as windows and external shading devices have a significant impact on the quality and effectiveness of natural daylighting. These elements also affect direct solar loads and overall energy performance for the life of the building. Without considering these issues early in the design process, the design is not fully optimized and the result is likely to be a very inefficient building. This same emphasis on integrated and optimized design is inherent in nearly every aspect of the building from site planning and use of on-site storm water management strategies to envelope design and detailing and provisions for natural ventilation of the building.

III.THE DESIGN AND BUILDING SPECIFICATION FOR GREEN BUILDINGS

Green buildings are structures that are built in an environmentally responsible manner by maximizing use of materials, minimizing use of resources and ensuring the health and well-being of occupants and the surrounding built environment both today and for generations to come.

With respect to the LEED guidelines there are seven topics that should be addressed in the designing and building of new environmentally friendly buildings.

3.1 Sustainable Sites

Sites should be selected by determining which site would pose the least environmental threat if construction were to take place. Sites should be closer to urban development where supporting infrastructure is available. There should be use of landscape design to preserve and restore the region's natural habitat and heritage while emphasizing the use of indigenous, hardy, drought resistant trees, shrubs, plants and turf. Make best use of existing mass transit systems and make buildings and sites pedestrian and bike friendly, including provisions for safe storage of bicycles. There should be development of programs and incentives that promote car-pooling including preferred parking for commuters who carpool. Optimize the use of on-site storm water treatment and ground water recharge. There should be minimization in the boundaries of the construction area, avoid needless compaction of existing topsoil, and provide effective sedimentation and silt control during all phases of site development and construction

3.2 Water Efficiency

The main goal is to increase water efficiency use within the building, thereby reducing the amount of water needed for operations. Some methods which can be designed in a building include water efficient landscaping to reduce irrigation requirements and the use of innovative wastewater management technologies. The design and location of buildings and site improvements should be done in order to optimize use of low-impact storm water technologies such as bio-retention, rain gardens, open grassy swales etc. Establishment of a water budget for the building and implement a design that minimizes the use of potable water by using low-flow plumbing fixtures and toilets and waterless urinals.

3.3 Energy and Atmosphere

Energy systems should be properly installed and calibrated to perform to their intended efficiency levels. Various methods for on-site renewable energy production can reduce the overall footprint of the building and other means of using green power. The Optimization of building orientation, massing, shape, design, and interior colors and finishes should be done in order to maximize the use of controlled natural day lighting which significantly reduces artificial lighting energy. Window frames, sashes and curtain wall systems should also be designed for optimum energy performance including the use of multiple thermal breaks to help reduce energy use. Use state-of-the art, high efficiency, heating, ventilation and air conditioning (HVAC) and plumbing equipment, chillers, boilers, and water heaters, etc. Use variable speed drives on fan and pump motors. Use heat recovery ventilators and geothermal heat pump technology for up to 40% energy savings. The consideration for on-site small-scale wind, solar, and/or fuel cell based energy generation and co-generation should be done and

purchasing of environmentally preferable "green" power from certified renewable and sustainable sources should be preferred.

3.4 Indoor Environmental Quality

To enhance the well-being of occupants, design should use low emitting materials in construction including sealants, adhesives, paints, coatings, flooring, wood and agrifibre. Ventilation systems that promote outdoor air ventilation are preferable. Buildings should be designed to maximize the use of natural light for all occupants. Maximum usage of the natural daylighting should be done. Optimize solar orientation and design the building to maximize penetration of natural daylight into interior spaces. Try to provide a smoke free building. Assure that air from smoking areas does not get distributed to other areas of the building does not re-enter the building through doors or vestibules, operable windows, or building fresh air intakes. Prevent contamination of the building during construction and take steps to minimize the creation and spreading of construction dust and dirt. Protect construction materials from the elements so that they do not become damp, moldy or mildewed. Use biodegradable and environmentally friendly cleaning agents that do not release VOCs or other harmful agents and residue.

3.5 .Materials and Resources

There should be minimum use of non-renewable construction materials and other resources such as energy and water through efficient engineering, design, planning and construction and effective recycling of construction debris. Maximize the use of recycled content materials, modern resource efficient engineered materials, and resource efficient composite type structural systems wherever possible. Maximize the use of re-usable, renewable, sustainably managed, bio-based materials. Optimize the use of engineered materials which make use of proven engineering principles such as engineered Trusses, composite materials and structural systems (concrete/steel, other…), structural insulated panels (stress skin panels), insulated concrete forms, and frost protected shallow foundations. Identify ways to use high-recycled content materials in the building structure and finishes. Consider everything from blended concrete using fly ash, slag, recycled concrete aggregate, or other admixtures to recycled content materials such as structural steel, ceiling and floor tiles, carpeting, carpet padding, sheathing, and gypsum wallboard. Identify ways to reduce the amount of materials used and reduce the amount of waste generated through the implementation of a construction waste reduction plan. Explore the use of bio-based materials and finishes such as various types of agriboard (sheathing and or insulation board made from agricultural waste and by products, including straw, wheat, barley, soy, sunflower shells, peanut shells, and other materials). The use lumber and wood products from certified forests where the forest is managed and lumber is harvested using sustainable practices. Use resource which are efficient engineered wood products in lieu of full dimension lumber which comes from older growth forests.

3.6 Innovation in Design

Design decisions should be made early in the process as good design can greatly reduce the energy consumption of a building; for example, the orientation and location of a building can compromise shading and ventilation decisions.

For innovative design a Low Carbon Design Taskforce should be created and that this taskforce could develop a blueprint that focuses on four levels in design:

• Site selection – transport and integration with other services;
• Orientation – to maximize daylight, shade, and ventilation naturally;
• Thermal issues – shape, density, materials and systems for winter heating and summer cooling
• Use of renewable forms of energy.

3.7 Regional priority

Designs should be maximized to take into account regional priorities. In colder climates buildings could be designed to maximize heating efficiency; in hotter climates, cooling and water usage would gain more importance in the design process.

IV. LEED- SETTING STANDARD FOR GREEN BUILDING

The Green Buildings can be rated for their environmentally sustainable construction. One such rating system is the LEED (Leadership in Energy and Environmental Design). This building rating system was developed by the U.S. Green Building Council (GBC) and was created to:

• Define “green building” by establishing a common standard of measurement;
• Promote integrated, whole-building design practices
• Recognize environmental leadership in the building industry
• Stimulate green competition;
• Raise consumer awareness of green building benefits
• Transform the standard building market to a green building market.

GBC members, representing every sector of the building industry, developed and continue to refine LEED. The LEED® green building certification programme is a voluntary, consensus-based national rating system for buildings designed, constructed and operated for improved environmental and human health performance. LEED addresses all building types and emphasizes state-of-the-art strategies in six major areas:

1. Sustainable sites
2. Water
3. Energy and atmosphere
4. Materials and resources
5. Indoor environmental quality
6. Innovation and design process

The LEED certifies Green Buildings in the three categories Silver, Gold and Platinum.

Some Excellent Example of Green Building based on LEED certification are:

1.Vattenfall HAUS is located in the City Nord, north of the Stadtpark in the city of Hamburg. The City Nord as well as VattenfallHaus are distinctive gemstones within the architectural landscape of the city. the VattenfallHaus boasts numerous innovative technological and energetic features such as the dual-use of cooling

water for ventilation/cooling, the reverse flow heat exchange for the heating system, the use of drainage water for sanitary installations and a highly modern Building automation system (BAS).

Besides getting the LEED certification level Platinum, which was quite a challenge for a building designed and built in 1969, the value of applying LEED to this project was the development of energy efficiency measures and capital improvement.

2. Pathways School Gurgaon is the first school serving all grades K-12 in the world to achieve LEED-EB Platinum certification from USGBC. Among all educational facilities worldwide who have achieved this top distinction, which includes only one high school and a small number of university projects, Pathways is the highest rated.

3. Suzlon Energy Limited pledged to create the greenest office in India. The building is three levels high and is sited on 10.5 acres. It achieved LEED for New Construction Platinum certification from the India Green Building Council, as well as Five-Star GRIHA (Green Rating for Integrated Habitat Assessment) certification. 5% (154 kilowatts) of its annual energy is generated on-site through conventional and building-integrated photovoltaic panels (20%) and wind turbines (80%). All balance energy required for the campus is generated through Suzlon's off-site wind turbines, making One Earth technically a zero energy project.

4. Itc Maurya Hotel in New Delhi, built in 1977, is also Platinum certified under LEED .In India there are total 489 certified green building projects.

V. ADVANTAGES OF GREEN BUILDING OVER CONVENTIONAL BUILDING

The green buildings are the high-performance building and they have advantage over similar conventional buildings are:

(A) It reduces energy, water, and material resource use.

(B) It improves indoor environmental quality, including reducing indoor pollution, improving thermal comfort, and improving lighting and acoustic environments that affect occupant health and productivity.

(C) It reduces negative impacts on the environment throughout the life-cycle of the building, including air and water pollution and waste generation.

(D) It increases the use of environmentally preferable products, including bio based, recycled content, and nontoxic products with lower life-cycle impacts.

(E) It increases reuse and recycling opportunities.

(F) It integrates systems in the building.

(G) It reduces the environmental and energy impacts of transportation through building location and site design that support a full range of transportation choices for users of the building.

VI. CONCLUSION

Green Building is a revolutionary step towards energy efficiency programme. For existing buildings as well as new construction, various methods can be adopted to save energy. In India some world class Green Buildings have constructed in past few years, but still the concept of green buildings for general masses is in infancy stage. Present work is an attempt in the direction to make people, communities and general public aware about the advantages of green buildings for sustainable environmental development and management .It is a step towards safeguard of nature and it will pave a way towards healthy and green future.

VII. ACKNOWLEGEMENT

We would like to take this opportunity to express our profound gratitude and deep regard to our teachers for their exemplary guidance, valuable feedback and constant encouragement throughout the duration of the project. Their valuable suggestion were of immense help throughout making of research paper. We would also like to give our sincere gratitude to all the friends, colleagues and family member without their support this research paper would be incomplete.

REFERENCES

[1] U.S. Environmental Protection Agency. (October 28, 2009). Green Building Basic Information. Retrieved December 10, 2009,

[2] Pushkar, S., Becker, R., & Katz, A.(2005). A methodology for design of environmentally optimal buildings by variable grouping. Building and Environment.

[3] Kats, Greg, Leon Alevantis, Adam Berman, Evan Mills, Jeff Perlman. The Cost and Financial Benefits of Green Buildings, November 3rd, 2008 [4]. Lee YS, Guerin DA, Indoor environmental quality differences between office types in LEED-certified buildings in the US, Building and Environment (2009),

[5] Schaefer, Valentin and Sulek, Marty. Green Links: Connecting Ecosystem Fragments in the City. New Westminster, B.C.: Douglas College, Institute of Urban Ecology, c1997. Biodiv QH106.2 .B7 S32 1997.

[6] Abair, Jesse W. "Green buildings: what it means to be 'green' and the evolution of green building laws.(Recent Developments in Land Use, Planning and Zoning)." The Urban Lawyer 40.3 (Summer 2008): 623(10). General OneFile. Gale. Goochland High School. 9 Oct. 2008

[7] ASHRAE Greenguide: The Design, Construction and Operation of Sustainable Buildings. 2nd ed. Atlanta: American Society of Heating, Refrigerating and Air-Conditioning Engineers, 2006.

[8] Attmann, Osman. Green Architecture: Advanced Technologies and Materials. New York: McGraw-Hill, 2010.

[9] Glavinich, Thomas E. Contractor's Guide to Green Building Construction. Hoboken: Wiley, 2008

[10] Beattie, P. and David M. 2008. "Green Roofs and Sedums Shine as Buffers for Stormwater Runoff and Acid Rain" Progress, Volume 19, Arlington, VA: Water Environment Research Foundation.

[11] Wendt, A. 2008. "Bringing Nature Indoors: The Myths and Realities of Plants in Buildings" Enviornmental Building News (October 1).

[12] Reder, Linda. Guide to Green Building Rating Systems: Understanding LEED, Green Globes, Energy Star, the National Green Building Standard, and More. Hoboken: Wiley, 2010

[13] Nunan, Jon. The Complete Guide to Alternative Home Building Materials & Methods: Including Sod, Compressed Earth, Plaster, Straw, Beer Cans, Bottles, Cordwood, and Many Other Low Cost Materials. Ocala, FL: Atlantic Publ. Group, 2010.

[14] Chiras, Daniel D. The New Ecological Home : The Complete Guide to Green Building Options. Chelsea Green Guides for Homeowners. White River Junction, Vt.: Chelsea Green Pub. Co., 2004.

[15] Ehrlich, Chuck. Intelligent Building Dictionary Terminology for Smart, Integrated, Green Building Design, Construction, and Management. San Francisco: Hands-on-Guide, 2007

BIG DATA ANALYTICS – AN OVERVIEW OF RESEARCH OPPORTUNITIES AND CHALLENGES

Aftab Yaseen[1] , P. M. Khan[2]

[1]*Assistant Professor, Department of CSE, Integral University Lucknow, (India)*

[2]*Director, Computer Centre, Aligarh Muslim University Aligarh, (India)*

ABSTRACT

For quite some time, processing capabilities and architectural constraints of conventional database technologies continued to be a limiting factor, in making it a viable option to handle Big Data in real sense. With recent advancements of technology and increasing ability to process large volumes of data, there is an ever growing interest of industry and researchers to explore the hidden treasures of Big Data. While a few companies like Google and Facebook are forerunners in Big Data research and development projects, but the potential application domains are virtually countless - like healthcare, banking, finance, biotechnology, life sciences, engineering & technology etc. While the data types and structures are diverse in Big Data, but application of Big Data Analytics has potential to reveal patterns and clues that can help organizations and businesses to address underlying causes of problems and take informed decisions in real-time that can be strategic for businesses. This paper is the result of a study undertaken to provide an overview of Big Data, technology options, research issues & challenges ahead in this field.

Keywords: Big Data, Big Data Analytics, Hadoop, Map Reduce

I. INTRODUCTION

The term Big Data refers to the massive collections of datasets which cannot be processed or analyzed with the help of conventional data management tools. The volume of big data is growing exponentially every year due to the generation of large amount of data by the IT companies, social networking sites, industrial and health care systems. The nature of big data can be characterized by its volume, velocity and variety. The limitation of existing storage and processing architectures differentiate the volume of data to be considered as big data. The most immediate challenge to the conventional processing architectures is the volume of big data. This volume questions about the scalability of existing storage, and the processing of data in distributed manner. The velocity of big data refers to the increasing rate of generation of data.

The variety is the diversity in different forms of the source data including text, images, audio, video and sensor data generated by modern IT, industrial and other systems. Integrating such type of diverse data for processing is a challenge for companies. There are two processing options available to deal with these massive volumes of data. The first one is the data warehousing approach which involves the predetermined schemas, best suited for datasets which are evolving with a lower velocity. The Apache Hadoop-based solution is the other approach as it can process the data irrespective of the structure of the data. In the following sections we discuss the big data analytics techniques including the Hadoop MapReduce and the underlying challenges in implementing them. We will also discuss the various approaches for classification of big data.

II. BIG DATA ANALYTICS

Big data analytics provides deep insights hidden by big data that go beyond the processing capability of existing systems. In the past decades, the data was mostly used to only record and report business activities and scientific events. In future data will be used also to gain new insights, to influence business decisions and to speed up scientific innovations. There are several steps involved in big data analytics like data preprocessing which include data cleaning, integration, transformation and reduction etc. and data visualization for decision making.

The latest technologies such as cloud computing, parallel processing and distributed processing frameworks has enabled the big data analytics as an emerging field of research. For distributed and large scale computations like in cloud computing environment Hadoop MapReduce programming model is widely used. The key challenge in big data analytics is to provide the right platforms and tools to make reasoning of big data easy and simple.

III. APACHE HADOOP-BASED SOLUTIONS

The Apache Hadoop is an open source framework that allows for the distributed processing of large data sets across clusters of computers using simple programming models. This framework is so designed that it can be scaled from a single server to thousands of machines. All these machines offer local computation and storage. Without depending on the hardware for delivering high-availability, the library is designed in such a manner that it detects and handles failures at the application layer resulting in a high availability of services on top of a cluster of computers, each of which may be prone to failures [1]. The projects surrounding Apache Hadoop consists of following modules:

- **Hadoop Common:** The common utilities that support the other Hadoop modules. It has utilities and scripts for starting Hadoop components and interfaces to access the file system supported by Hadoop [2].
- **Hadoop Distributed File System (HDFS):** The Hadoop Distributed File System (HDFS) is a highly fault tolerant distributed file system designed to provide high throughput access to application data [3].
- **Hadoop YARN:** A framework for job scheduling and cluster resource management. YARN is the prerequisite for Enterprise Hadoop, providing resource management and a central platform to deliver consistent operations, security, and data governance tools across Hadoop clusters [4].
- **Hadoop MapReduce:** A YARN-based distributed programming model for parallel processing of large data sets. Users specify a map function that processes a key/value pair to generate a set of intermediate key/value pairs, and a reduce function that merges all intermediate values associated with the same intermediate key [5].

Other Hadoop related projects at Apache are summarized in **Table I:**

Table I: Hadoop related projects at Apache [1]

Ambari™	A web-based tool for provisioning, managing, and monitoring Apache Hadoop clusters.
Avro™	A data serialization system.
Cassandra™	A scalable multi-master database with no single points of failure.
Chukwa™	A data collection system for managing large distributed systems.
HBase™	A scalable, distributed database that supports structured data storage for large tables.

Hive™	A data warehouse infrastructure that provides data summarization and ad hoc querying.
Mahout™	A Scalable machine learning and data mining library.
Pig™	A high-level data-flow language and execution framework for parallel computation.
Spark™	A fast and general compute engine for Hadoop data.
Tez™	A generalized data-flow programming framework, built on Hadoop YARN.
ZooKeeper™	A high-performance coordination service for distributed applications.

IV. HADOOP MAPREDUCE PROGRAMMING MODEL

The Hadoop MapReduce provides a programming model for large scale data processing and an execution environment for MapReduce jobs. A MapReduce job is executed in two phases: the Map phase and the Reduce phase. The input data to these two phases are in the form of a key/value pairs. In the Map phase, data is read from a distributed file system. This data is then partitioned among a set of computing nodes in the cluster and send to the nodes as a set of key/value pairs. After processing these partitioned data independently an intermediate result is produced by the map task as key/value pairs. These intermediate results are stored on the local disk of the node running the Map task. After completing the Map tasks, the Reduce phase begins whose task is to aggregate the intermediate data with the same key. The advantage of MapReduce programming model is that it does the computations to where the data is located which results in decreasing the transmission of data and hence improving efficiency. This model is well suited for parallel processing of large scale data in which the data analysis tasks can be accomplished by independent Map and Reduce tasks. Google has used the MapReduce programming model successfully for many different purposes. The reason behind this is that this model is easy to use, even for programmers without experience with parallel and distributed systems, since it hides the details of parallelization, fault-tolerance, locality optimization, and load balancing. There is another reason of using this model is that a large variety of problems can be easily modeled into MapReduce programming model.

V. RESEARCH OPPORTUNITIES AND CHALLENGES

The sources of Big Data can be finance and business where huge amount of stock exchange, banking, and online shopping data flows via Internet every day and are then confined and stored for knowledge discovery in inventory analysis, customer and market behavior. The field of life sciences is another major producer of large and massive datasets including genome sequencing, clinical data and patient data. These data are analyzed and used to advance breakthroughs in medical sciences & research. Astronomy, oceanography, and engineering are the other areas of research where Big Data is of essential importance [6]. In the area of drug discovery large volume of structured and unstructured biomedical data stemming from a wide range of experiments and surveys collected by hospitals, laboratories, pharmaceutical companies or even social media. The challenge is to develop such algorithms to discover the hidden patterns in such data for predictions that may be used to determine possible drug structures with different desirable properties. In this field big data analytics may contribute to better drug efficacy and safety for pharmaceutical companies and regulators [7]. There is a number of emerging research areas relating to the use of Big Data Analytics for evidence based medicine (EBM). El-Gayar, Timsina [8] presented a study that provides a research agenda for health informatics researchers and data scientists to

address issues of reducing the cost and improving the cost of healthcare by broadening the practice of evidence based medicine through the applications of business intelligence big data analytics [8]. Cardenas et al. [9] highlighted the challenges related to the security issue in big data. These challenges are privacy, data provenance problem and human computer interaction. The privacy depends largely on the technological constraints on the ability to extract, analyze, and correlate potentially sensitive datasets. With the advancement in big data analytics different tools were developed to extract and correlate this data, and hence making the privacy violations easier. For data provenance related issues the authenticity and integrity of data used in such tools should be reconsidered in order to produce accurate results. Some machine learning and statistical techniques can be used to identify the maliciously inserted data and to deal with it. The use of human computer interaction or visual analytics helps in analyzing the query results. Although human-computer interaction in big data has received less attention but it is one of the primary tools of big data analytics, because its purpose is to provide information in a most effective manner [9]. Big data analytics use data mining algorithms which are computationally intensive and require efficient high performance processors for producing results in a given time frame. For computational and data storage requirement in big data analytics, cloud computing infrastructures can serve as an effective platform. Advanced data mining techniques and associated tools for knowledge discovery can help in extracting information from massive and complex datasets. Hence big data analytics and knowledge discovery techniques with scalable computing systems can be combined to give useful results in timely manner. The challenging areas in which the cloud based data analytics can be used are the development of scalable higher-level models and tools. Interoperability of data and tools is another major issue in large scale applications [10].

VI. CONCLUSION

It is evident from this study that Big Data Analytics approaches are increasingly being used to obtain valuable information from big data. Organizations are trying to develop multiple analytic platforms that can synthesize traditional structured data with semi-structured and unstructured sources of information. This paper focused on the thrust areas of research in the field of big data analytics. Based on the study of various research papers and articles on big data analytics, it is found that a lot of research is needed to develop tools for big data analytics that can help organizations. Findings from this study have also confirmed that discovery of hidden patterns in data, privacy and security issues of organizations and development of a cost effective system are major challenges in the field of big data analytics. Scalability and efficiency are other issues identified with cloud based systems. Volumes of research possibilities in these areas needs to be explored further, and will continue to attract attention of researchers and practitioners, globally.

REFERENCES

[1]. http://hadoop.apache.org/, Retrieved 2015.

[2]. A. Bagha,V. Madisetti, *cloud computing: a hands-on approach* (University Press India Private Limited, 2014).

[3]. http://hadoop.apache.org/docs/r1.2.1/hdfs_design.html, Retrieved 2015.

[4]. http://hortonworks.com/hadoop/yarn/, Retrieved 2015.

[5]. J. Dean, S. Ghemawat, MapReduce: Simplified Data Processing on Large Clusters, In Proc. of the 6th Symposium on Operating Systems Design and Implementation, San Francisco CA, Dec. 2004, 137-149.

[6]. H. Gali, M. Henk, The Evolution of Big Data as a Research and Scientific Topic, Research Trends Special Issue on Big Data, Elsevier 30 Sep 2012, 03-06.

[7]. Chan, K.C.C., Big data analytics for drug discovery, IEEE International Conference on Bioinformatics and Biomedicine, 18-21 Dec. 2013.

[8]. El-Gayar O., Timsina P., Opportunities for Business Intelligence and Big Data Analytics In Evidence Based Medicine, 47th Hawaii International Conference on System Science, 6-9 Jan. 2014, 749-757.

[9]. Cardenas, A.A. ; Manadhata, P.K. ; Rajan, S.P., Big Data Analytics for Security, Security & Privacy, IEEE, Vol. 11,Issue 6, Nov-Dec. 2013, 74-76.

[10]. Talia D., Clouds for Scalable Big Data Analytics, Computer, IEEE, Vol. 46, Issue 5, May 2013, 98-101.

DEVELOPMENT OF STEEL FIBRE REINFORCED GEOPOLYMER CONCRETE.

G.Ramkumar[1], S.Sundarkumar[2], A.Sivakumar[3]

[1]Student, [3]Program chair, School of mechanical and building science, VIT university, (India)

[2]Advanced materials lab,CSIR-SERC, (India)

ABSTRACT

Efforts will be earnestly in progress all over the world todevelopconstruction materials, which make least utility of quick decreasing common assets and help to decrease greenhouse gas emanationsGeopolymers are indicating extraordinary potential and a few scientists have basically analyzed the different perspectives of their feasibility as binder framework. Geopolymer concretes (GPCs) are new class of building materials that have risen as an elective to Ordinary Portland cement concrete (OPCC) and have the potential to change the building development industry. Significant research has been done on improvement of Geopolymer concretes (GPCs), which include ambient temperature curing and use of stainless steel fibre and mild steel fibre. In this paper an attempt is made to study steel fibrereinforcedgeopolymerconcrete.Three GPC mixes of fly ash(50%) and GGBS(50%) in the binder stage were considered.with control GPC mix , GPC mix with added stainless steel fibre and mild steel fibres. The studies showed that the load carrying capacity of most of the GPC mix was in most cases more than that of the conventional OPCC mix.The deflections at diverse stages including service load and peak load stage were higher for GPC beams.

Keywords: Geopolymer, Steel Fibre, Flyash , GGBS, Load Deflection

I.INTRODUCTION

Davidovits proposed geopolymer cement and cement industry applies this innovation as an option for binder in portland concrete. The Carbondioxide emanation in the climate is around 80% to the air which is created by cement and aggregate industries. Geopolymerisation is a methodology in which the source material (rich in silicon and aluminum) responds with high alkaline solution for produce binding material. Investigation of common asset , utilization of high energy and outflow of green house gasses are connected with generation of ordinaryportland cement. GGBS, Flyash can be in part substituted for OPC. GPC's commitment to ecoefficiency of the worldwide economy is noteworthy. Alkaline cements acquired through alkaline initiation and geopolymerisation methodology and result of distinctive industries can be substituted for OPC. ALkali activator is utilized to initiate a reaction or arrangement of reaction with alkali cements which delivers alkali activated slag cement. The different natural advantages of alkali activated concrete is as per the following , industry by-product use , utilization of low energy and low discharge of green house gas. Since 1940's the standards of alkali activation of slag is known. Since 1960's these binders is connected in development industry in Ukraine. Mortars and cement has been alkali activated in colombia for research purpose including GGBS as just binder. Magnificent mechanical and strength properties have been attained to. The drawbacks distinguished is found to endure drying shrinkage. Slag microstructure, fineness, alkaliactivator, nature,concentration and

curing condition will impact drying shrinkage in concrete. The shrinkage control of brittle matrices and mechanical performance have been enhanced just through the expansion of fibres. The fracture toughness gave by fiber bridging over on main crack plane before crack extension increments. The bridging action is controlled by debonding , sliding and pulling out of fibres. The bridging action of fiber controls the opening and development of cracks toward the start of macrocracking. The demand of energy for the crack to propogate is expanded. In low volumetric fiberportion , the straight elastic behaviour of matrix couldn't have the capacity to influence altogether. At the point when the durability , strength and toughness of material is increased , the post cracking behaviour can be changed. This paper reports the impact of incorporation of steel fiber on flexural properties of alkali actuated concrete at early age of time of curing. This paper concentrate on perspective to identify their execution and potential application as building material. Particularly in those system reinforced with fibres that oblige enhanced crack behaviour and stability.

II.LITERATURE REVIEW

Susan.A.Bernal.et.al (June 2013) focuses on gel nanostructure in alkali-activated binders based on slag and flyash and effects of accelerated carbonation. Binders formed through alkali-activation of slags and fly ashes, including ‘fly ash geopolymers’, provide appealing properties as binders for low-emissions concrete production. However, the changes in pH and pore solution chemistry induced during accelerated carbonation testing provide unrealistically low predictions of in-service carbonation resistance. The aluminosilicate gel remaining in alkali-activated slag system after accelerated carbonation is highly polymerised, consistent with a decalcification mechanism an, while fly ash-based binders mainly carbonate through precipitation of alkali salts (bicarbonates at elevated CO2 concentrations, or carbonates under natural exposure) from the pore solution, with little change in the binder gel identifiable by nuclear magnetic resonance spectroscopy. In activated fly ash/slag blends, two distinct gels (C–A–S–H and N–A–S–H) are formed; under accelerated carbonation, the N–A–S–H gel behaves comparably to fly ash-based systems, while the C–A–S–H gel is decalcified similarly to alkali-activated slag. This provides new scope for durability optimisation, and for developing appropriate testing methodologies.

Sanjay Kumar etal (September 2009) studied the use of GGBFS in altering the behaviour of flyash. The effect of varying amount (5% -50%) of GGBFS on the reaction kinetics has been studied using isothermal conduction calorimetry. It has been observed that at 27ºC the reaction is dominated by GGBFS but at 60ºC the reaction is due to combined interaction of flyash and GGBFS. The characteristics of reaction product of geopolymerisation are determined by X-ray analysis and SEM analysis. A-S-H and Ca-S-H are the main reaction products formed and its co-existence shows the interaction of flyash and GGBFS on geoploymerisation. From this study it was also concluded that geopolymerisation is along process of dissolution, precipitation, restructing, and polycondensation. Dissolution and precipitation occurs at early stages and polycondensation occurs at higher temperatures. At 27ºC, typical dissolution and precipitation of C-S-H takes place due to alkali activation of GGBFS. The increase in compressive strength due to the addition of slag may be due to the presence of A-S-H and Ca-S-H gel phases and compactness of microstructure.

C.K.Yipetal(October 2004) discussesthe coexistence of geopolymeric gel and calcium silicate hydrate the early stage of alkaline activation.Scanning electron microscopy was used to study the effects of the addition of ground granulated blast furnace slag (GGBFS) on the microstructure and mechanical properties of metakaolin(MK) based geopolymers. It was found that it is possible to have geopolymeric gel and calcium

silicate hydrate (CSH) gel forming simultaneously within a single binder. The coexistence of these two phases is dependent on the alkalinity of the alkali activator and the MK/GGBFS mass ratio. It has been found that the formation of CSH gel together with the geopolymeric gel occurs only in a system at low alkalinity. In the presence of high concentrations of NaOH (N7.5 M), the geopolymeric gel is the predominant phase formed with small calcium precipitates scattered within the binder. The coexistence of the two phases is not observed unless a substantial amount of a reactive calcium source is present initially. It is thought that voids and pores within the geopolymeric binder become filled with the CSH gel. This helps to bridge the gaps between the different hydrated phases and unreacted particles; thereby resulting in the observed increase in mechanical strength for these binders.

P. De Silva. et.al (January 2007) discusses the early stage reaction kinetics of Metakaoline/sodium hydroxide/sodium silicate geopolymer system. The early strength development characteristics and associated mineral and micro structural phase development of mixtures containing varying ratios of SiO_2/Al_2O_3 cured at 40°C for 72 hours is studied. It has been observed that setting time is being controlled by the amount of alumina content. Setting time can be increased by increasing the amount of SiO_2/Al_2O_3 ratio in the initial mixture. The ratio of SiO_2/Al_2O_3 is found to be responsible for increase in strength at later stages. An increase in alumina content leads to reduction of strength accompanied by microstructures with increased amounts of Na-Al-Si containing massive grains. In general, inorganic geopolymer can be synthesized by alkali activation of SiO_2 and Al_2O_3. It was concluded from the studies that amount of available Si has dominant effect in controlling setting time. It was also shown that increasing the molar ratios up to 3.4-3.8 is highly responsible for strength development. The properties of geopolymer can be significantly altered by minor changes in Al and Si concentrations.

SravantiPuligillaetal (October 2012) discusses the microstructural development and hardening rate of flyash slag geopolymers. In this work , the activator solution used is the combination of potassium silicate and potassium hydroxide. Microstructural development was investigated using ultrasonic wave reflection (UWR), proctor penetration method, semi-adiabatic calorimetry and SEM imaging with EDS. Both UWR and Proctor penetration methods capture changes in hardening rate due to changes in the reaction mechanism. It was observed from the experiments that an increase in addition of slag increased the rate of hardening. It was also observed that calcium dissolving from the slagis important for both early and late age properties. Slow reaction rate and low strength development has been confirmed when flyash with low calcium content is activated with low concentration alkali and curved without any heat treatment.

Tiang Sing Ng etal (June 2013) studied the shear strength characteristics of fibre reinforced geopolymer concrete beams. Shear tests were conducted on five sets of 120mm × 250mm beams spanning 2250mm. The beams does not contain any stirrups. Instead the beam is reinforced by hooked and straight steel fibre of various dosages which vary between 0% - 1.5%. The results showed that the shear strength asa well as the crack behaviour improved on addition of fibres. Also, 100mm×100mm×500mm beams and 100mm×200mm cylinder were cast to determine the mechanical properties. The results of the test were compared with the fib Model Code 2010 alternative model for shear strength of steel-fibre reinforced concrete in combination with the variable engagement model for the determination of the tensile strength of steel-fibre-reinforced concrete. It was concluded from the studies that the beams without FRP, arching action is important in determining the failure load and failure mode. Ultimate strength and cracking load increased with increase in fibre volume

III. EXPERIMENTAL INVESTIGATION

3.1. Materials used

The GPC was acquired by blending distinctive mixes of Ground Granulated blast Furnace Slag (GGBS), Fly Ash (FA), fine aggregates, coarse aggregates and Alkaline activator solution(AAS). FA fitting in with grade 1 of IS 3812 and GGBS from Andhra cements, Vishakhapatnam conforming to IS 12089 were utilized. Stream sand available in Chennai was utilized as fine totals. They were tested according to IS 2386. In this investigation, generally accessible blue granite crushed stone aggregates of maximum size 12mm and down was utilized and characterization tests were done according to IS 2386.The properties of the materials utilized are indicated as a part of Tables 1. potable water was utilized for the GPC and distilledwater was utilized for the RGPCs.The alkaline activator solution (AAS) used in GPC mixes was a combination of sodium silicate solution (SiO2/Na2O=2.2), sodium hydroxide pellets and distilled water. The part of AAS is to break down Si and Al present in the reactive portion of source materials, for example, FA furthermore GGBS and give a high alkaline liquid medium for condensation polymerization reaction. The sodium hydroxide was taken as form of flakes of 3mm in size. The sodium hydroxide (NaOH) arrangement with obliged concentration was arranged by dissolving the processed measure of sodium hydroxide flakes in distilled water. The NaOH solution and sodium silicate solution were prepared independently and mixed at the time of casting. Since lot of heat is created when sodium hydroxide chips respond with water, the sodium hydroxide arrangement was prepared a day prior to casting. It ought to be noted here that it is crucial to attain to the desired level of workability of the GPC concrete. Notwithstanding, overabundance water can bring about development of pore system, which could be the source of low quality and low toughness.Experimental work is designed to study the effect of steel fibres on mechanical and elastic properties on geopolymer concrete. The materials used for making fly ash geopolymer concrete composite specimens are low-calcium fly ash, course and fine aggregates, steel fibres, alkaline solution, and water.

3.1.1 Fly Ash

Fly ash is the residue from the combustion of pulverized coal collected by mechanical or electrostatic separators from the flue gases of thermal power plants. The spherical shape of particle improves the flow ability and reduces the water demand. In this experimental work, the fly ash used is obtained from the silos of Ennore Thermal Power Station, Chennai, India, which is of low calcium, Class F. Low calcium fly ash makes substantial contributions to the workability, chemical resistance, and reduction in thermal cracking. Table 1 shows the chemical composition.

Table 1 : Chemical Composition of Fly Ash

Compound	SiO_2	Al_2O_3	Fe_2O_3	CaO	MgO	Na_2O	K_2O	TiO_2	Mn_2O_3	SO_3	P_2O_5
Fly Ash	49.45	29.61	10.72	3.47	1.3	0.31	0.54	1.76	0.17	0.27	0.53

3.1.2 Ground Granulated Blast Furnace Slag

GGBS is a by product from Iron smelting Industry, Chennai. Table 2 describes the composition of GGBS.

Table 2 : Chemical Composition of GGBS

Compound	SiO_2	Al_2O_3	Fe_2O_3	CaO	MgO	Na_2O	K_2O	TiO_2	Mn_2O_3	SO_3
GGBS	33.45	13.46	0.31	41.7	5.99	0.16	0.29	0.84	0.40	2.74

3.1.3 Sodium Hydroxide (NaOH)

The most common alkaline activator used in geopolymerisation is a combination of sodium hydroxide (NaOH) or potassium hydroxide (KOH) and sodium silicate or potassium silicate. The type and concentration of alkali solution affect the dissolution of fly ash. Leaching of Al^{3+} and Si^{4+} ions are generally high with sodium hydroxide solution compared to potassium hydroxide solution. Alkali concentration is a significant factor for controlling the leaching of alumina and silica from fly ash particles, geopolymerization process and mechanical properties of hardened geopolymer. Duchesneetal confirmed that in presence of NaOH in the alkaline activating solution, the reaction takes place more rapidly and the gel is less smooth.

3.1.4 Sodium Silicate Solution (Na_2SiO_3)

Sodium silicate is the common name for a compound sodium metasilicate, Na_2SiO_3, also known as water glass or liquid glass. It is available in both aqueous solution and solid form and is used in cements, passive fire protection, refractories, textile and lumber processing, and automobiles. Sodium carbonate and silicon dioxide react in molten state to form sodium silicate as well as carbon dioxide.

3.1.5 Alkaline Solution

Sodium hydroxide (NaOH) in the form of flakes and sodium silicate are used as alkaline activators to give a good binding solution for the geopolymeric mix.The alkaline liquid used in geopolymerisation is a combination of sodium hydroxide (NaOH) and sodium silicate as activators. Sodium silicate solution was purchased from a local supplier in bulk. The sodium hydroxide in flakes or pellets was purchased from a local supplier in bulk.

- Alkaline liquid is prepared by mixing sodium silicate solution and sodium hydroxide solution with proper proportion.
- Sodium-based solutions were selected because they were cheaper than potassium based solutions.
- The sodium hydroxide solids were a commercial grade in pellets form (3 mm).

3.1.6 Aggregates

Locally available river sand sieved through 4.75mm is used as fine aggregates and crushed stones of nominal size 10mm coarse aggregates is used.

3.1.7 Steel Fibres

Use of crimped steel fibres of aspect ratio (a/d) 60 is used.For the geopolymer mix we have used crimped stainless steel fibres and crimpes mild steel fibres. The use of fibres in concrete has the property to resisitance against cracking and crack propogation. The fibre composite pronounced post cracking ductility which is unheard of in ordinary concrete. The transformation from a brittle to a ductile type of material would increase substantially the energy absorption characteristics of the fibre composite and its ability to withstand repeatedly applied shock or impact loading. These fibres are short, discrete lengths having an aspect ratio in the range of 20-100, with any cross section that are sufficiently small to be randomly dispersed in an unhardened concrete mixture using usual mixing procedures.

3.2 Mix Proportion of GeopolymerMix

Fly ash, GGBS, coarse and fine aggregate and steel fibres are mixed thoroughly in a dry state and then alkaline solution is added to make the mix wet until it gains homogeneous state. Mix proportion and quantity of fibre content in each mix is explained below in table 3.

Table 3 :Geopolymer Mix Proportion

Mix	Fly Ash (kg)	GGBS (kg)	C.A. (kg)	F.A. (kg)	SH (kg)	SS (kg)	CSS (kg)	CMS (kg)	Water (kg)
CM	25.85	25.85	141.35	80.553	3	6	--------	--------	22.2
GP-1	25.85	25.85	141.35	80.553	3	6	7.471	--------	22.2
GP-2	25.85	25.85	141.35	80.553	3	6	--------	7.471	22.2

Table 4 : Mix Details

MATERIALS	**MIX 1**
MOLARITY (NaOH)	3.5M
$NaoH/Na_2SiO_3$ (Kg/m3)	1:2
FLY ASH (Kg/m3)	203.5
GGBS (Kg/m3)	203.5
Sodium hydroxide (Kg/m3)	23.62
Sodium silicate(Kg/m3)	47.24
Water (Kg/m3)	174.8
F.A (Kg/m3)	634.2
C.A (Kg/m3)	1112.9
DENSITY (Kg/m3)	2600

3.3 Collection of By Products

The materials used for the study like fly ash (Thermal power plant, Ennore); GGBS (Iron smelting industries, Chennai) ; fibres and alkaline solution (Local suppliers, Chennai).

3.4 Preparation of Geopolymer

3.5M molarity geopolymer are produced with alkali activator ratios of 1:2 and mixes for GP concrete with the following combinations are given :

- (Fly ash – 50%) + (GGBS -50 %) – Control mix
- (50 % Fly ash + 50 % GGBS) + (0.75% Crimped stainless steel fibres)
- (50% Fly ash + 50 % GGBS) + (0.75% Crimped mild steel fibres)

The mass of NaOHflates was taken depending on the concentration of the solution expressed in terms of molar, M. To get desired alkaline solution the sodium hydroxide solution which is prepared one day before is mixed with sodium silicate at the time geopolymer concrete preparation

IV.TEST SPECIMENS AND TESTING

4.1 Preparation of Specimens

Before casting, the inward walls of moulds were covered with greasing up oil to avoid adhesion with the solidifying concrete. GPC were mixed in a tilting drum mixer machine of 350kg limit for around 5-8 minutes. The concrete was put in the shape in three layers of equivalent thickness and every layer was vibrated until the concrete was completely compacted. Three no's of 100mm cubes were casted to focus the 28 day compressive strength.specimens were demoulded after 24 hrs.The split tension test were conducted on cylinder specimen after 28 days. The flexure test conducted on beam specimens showed higher results because of the addition of steel fibres and the high bondage strength. Table 4 briefly explains the test analysis values.

V. TEST RESULTS AND DISCUSSIONS:

Table 5 : Test Results on Compressive Strength.

Mix	Compressive Strength, MPa			SplitTensile Strength, MPa (28 days)	Flexure Strength Test, MPa (28 days)
	3rd day	7th day	28th day		
GPCM	21.21	32.37	44.16	3.372	6.61
GPCS	34.61	37.21	52.164	5.317	8.14
GPCMS	32.15	38.313	53.13	5.91	8.19

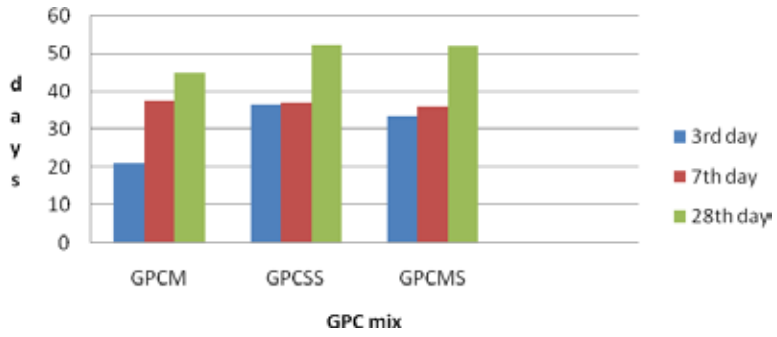


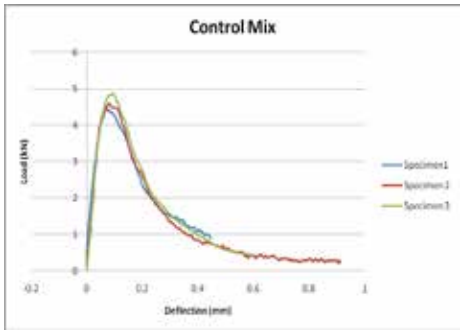
Chart 1 : Plot Between Geopolymer Mixes And Duration (Days).

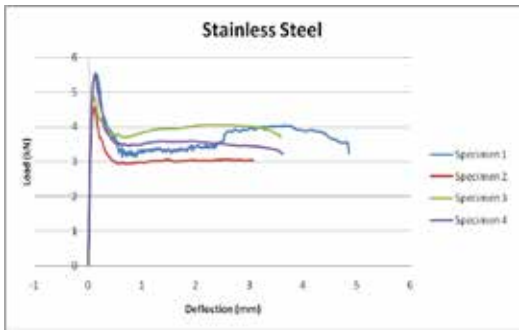
5.1 Load-Deflection Behavior

As the load was applied on the notched beam specimen (100*100*500mm) slowly no cracks were formed until the peak load was attained. A crack started to propogate at the end of the notched part faster in the ligament when the load reached its peak value. Failure started to propogate by opening a single crack in the geopolymer

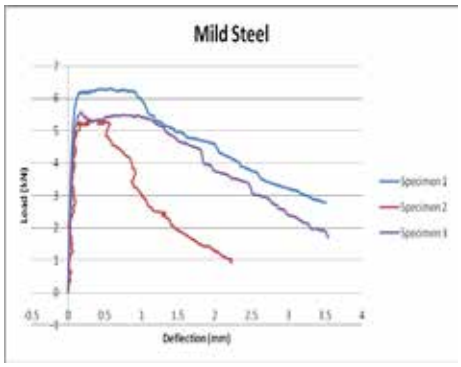
concrete specimens. The typical load–deflection diagrams of GPC concrete specimens are given. It is seen from these figures that the peak load of geopolymer concrete specimen was higher similar to its compressive strength.

Figure 1: Load deflection curves for each batch





a)Load Deflection Curve For Control Mix **b) Load Deflection Curve For Steel Fibres Mix**



c) Load Deflection Curve for Steel Fibres Mix

5.2 Curing of Geopolymer Concrete

The Geopolymer samples were cured under ambient temperature. Water curing is not required. Geopolymer concrete attains its full strength only after 28 days.

VI. RESULTS AND DISCUSSIONS

Table demonstrates the compressive strength developed by different mixes at 3, 7 and 28 days of age. It might be seen that the mixes accomplished the normal level of 28 day strength. In spite of the fact that all in all it is required for geopolymer concrete to achieve strength at a speedier rate, in the present mixes. Consequently it can be normal there would be some unreacted flyash in the mix which could credit to further strength pick up with age. However the present goal was to attain to a workable mix with strength of around 30 MPa at 28 days with no extraordinary curing necessities, since the vast majority of the concrete utilized as a part of India are in this evaluation and are insitu made. Alkali activated slag based geopolymer concrete with ambient air curing with a compressive strength at 28 days in abundance of 30 MPa was attained to for all the mixes. From the perception all the mixes has sufficient retention period and it can be embraced for making of GGBS based geopolymer concrete. The most essential parameter of workability and slump maintenance for sufficient time was attained to in this mixes.

VII. CONCLUSION

Based on the experimental work the following conclusions are drawn

- There is no need of exposing geopolymer concrete to higher temperature to achieve most extreme strength
- With the addition of steel fibres in GPC diminished the workability of concrete mix.
- The necessity of water substance is reduced because of the addition of alkaline solution which helps in increasing the compressive strength of concrete.
- The compressive strength is increased by 2.25% (appx) when steel fibres are utilized .
- GPC mix with added steel fibres are approximately 20% more than GPC control mix in compression behaviour.
- GPC mix with added stainless steel fibres is 57% more than control mix and GPC mix with added mild steel fibres is 75% more than control mix in split tensile strength behaviour.
- 82.3% of compressive strength was attained by control mix in only 7days and 70-73% of compressive strength was accomplished in just 7 days .
- Flexural strength of GPC with added fibres is approximately 24% more than control mix.
- The addition of fibres diminishes the crack propogation in concrete and can achieve higher peak value.

REFERENCES

[1] J. Davidovits, Chemistry of geopolymeric systems, in: Terminology, Geopolymer'99 Second International Conference, Saint-Quentin, France, 1999, pp. 9–39.

[2] H. Xu, J.S.J. van Deventer, The geopolymerization of alumino-silicateminerals, Int. J. Miner. Process. 59 (2000) 247–266.

[3] J.C. Swanepoel, C.A. Strydom, Utilization of fly ash in a geopolymericmaterial, Appl. Geochem. 17 (2002) 1143–1148.

[4] J.G.S. van Jaarsveld, J.S.J. van Deventer, G.C. Lukey, The effect of compositionand temperature on the properties of the fly ash- and kaolinite-basedgeopolymers, Chem. Eng. J. 89 (2002) 63–73.

[5] V.F.F. Barbosa, K.J.D. MacKenzie, Thermal behaviour of inorganicgeopolymers and composites derived from sodium polysialate, Mater. Res.Bull. 38 (2003) 319–331.

[6] Hardjito D, Wallah SE, Sumajouw DMJ, Rangan BV. On the development of flyash-based geopolymer concrete. ACI Mater J 2004;101(6):467–72.

[7] Lloyd N, Rangan BV. Geopolymer concrete; sustainable cementlessconcrete.In: Proceedings of the 10th ACI international conference on recent advances inconcrete technology and sustainability issues, Seville, ACI SP-261-03; 2009. p.33–54.

[8] Lloyd N, Rangan BV. Geopolymer concrete with fly ash. In: Secondinternational conference on sustainable construction materials andtechnologies; 2010.

[9] Rangan BV. Mix design and production of fly ash based geopolymerconcrete.IndianConcr J 2008;82(5):7–15.

SECURITY OF SENSITIVE DATA IN XML OR FILE SYSTEM USING ENCODING THROUGH URL

[1] Kajal Shukla, [2] S. K. Singh

[1] M. Tech. Student, [2] Professor VIET, Dadri G. B. Nagar UP (India)

ABSTRACT

Database services have the web applications which are interactive targeted by an SQL Injection. User gives some data as a input and at last that coded input data is being used as to form SQL statement at runtime in these applications. A person who is a n attacker can be able to input a malicious or harmful query segment when user inputs any SQL statement during SQL Injection attacks, that is the result which could be used in many more different database request. Sensitive/Confidential information can be added or modified by an attacker to form attacks of SQL Injection. SQL Injection vulnerability could be used by an attacker as an IP scanner rudimentary. There are several paper published in literature having discussed that how to secure sensitive data in xml or file system , by checking SQL dynamic query commands.SQL Injection attacks However, for secure stored procedures in the database higher level layer / application layer a very less attention is given, which surely can be too suffered from attacks of SQL Injection .

Keywords*: *SQL query, SQL server, SQL Injection.

I. INTRODUCTION

One of the most demanding and challenging causes which can make impacts on the business and industry level in a Structured Query Language is that it can explore all of the sensitive information which is stored in our database, including most highly important information such as credit card details, usernames, addresses, passwords, names, phone, email id etc. To inject a Structured Query Language is the liability that when attacker gets the ability with SQL queries which can be passes to a database. The query which is passed through an attacker in to the database, an attacker can allows the query to database which is supporting element with database and our operating system. SQL Query which is able to accept the inputs from the attacker sides can harms our real web application. Attacker always try to insert harmful SQL query commands into a database so as on execution the query they can destroy or alter the database i.e. this technique is called code injection technique. So this attacker is also called attack vector for websites and this kind of attacker is used by any kind of SQL database.

According the study last year, Security Company **"**Imperva**"** find that the most web application attacks is done 4 times per month and other side retailers company is attacked by 2 times per month. That is not a good practice on the behalf of security.

II.TYPES OF SQL INJECTION

- Redirection and reshaping of a query
- Based on Error message
- Blind injection

2.1 Blind SQL Injection

- Formation of queries that results in Boolean values, and interprets output of HTML Pages is provided by Blind SQL injection technique IN database.
- Final result of SQL injection gives significant data theft and/or attacks in data modification.
- Essentially Blind attack playing 20 questions with the web server.

2.2 Focus on Blind SQL Injection

- This type of SQL Injection is as common as any other type of injection.
- An incorrect or wrong sense of security on the host is provided by the Blind holes.
- Requires a larger of time investment to properly execute manual penetration against.

Fig.1

2.3 Concepts of SQL Injection Attacks

- SQL injection attack is a process to find the query which is entered through the user for execution the command.
- SQL attackers create crafted manually input data so that SQL interpreter has to accept the query and give the permission to execute the commands and give his desired results.
- SQL Injection attack breaks the security of the database layer. When attacker breaks flaws through the SQL injection then attackers can drop, modify, create, and alter our sensitive database.

III. SECURITY IN SQL INJECTIONS

Web vulnerabilities minimum 20% of all that is being related to SQL Injection, called as the one of the most widespread type of catalog application security and as well as the subsequent most common software susceptibility which have the find and prevent capability .SQL Injection always must be on high priority for web developer and also for security basis. Generally a SQL Injection assault diminishes any web network application software which has not provided a proper validation or we can say coded by a user given input data. In the last phase that crafted input data is being used as an element of query over again whichever back-end database. Acquire an example, what time we generate any form it always asks for the ID that is called as identity. After that URL:"http://www.anywebsite.com/id/id.asp?id=anymanualdata" is created.

An invader, using the SQL Injection may perhaps go through any data or "1=1". At the particular time if the application software of the web network is not specified proper validation or incorrectly encoded the user given data that is directly send in the direction of database, and as well as input with the vulnerable query will reach there in reply that will depict every single one ids in the database ever since the condition is "1=1" is for all time true. The example given is an indispensable example however it illustrates the consequence of sanitizing client input data prior to using it in a SQL database query or SQL commands.

IV. LITERATURE REVIEW

Our web applications allow the visitors to enter or submit or retrieve database using any web browser through the internet. These kinds of data have to centralize therefore they be capable of storing data which is needed for websites. If any Suppliers, Employees, a host of stakeholders, customers etc. want to achieve specific content from database side then he can receive it

.Company statistics, User Details, financial, economical and payment information etc are stored in our database which is access through custom web applications. Our Database and Web applications allow us to run the production business frequently.

The Process which attempt to get ahead of commands or statements of SQL intended for implementation through the database over the web network application is called hacking technique in SQL Injection. If their attempts are right then our database allows hackers to view their desire information from the database and he can hampers our database, and be able to do the whole lot which he wants.

For example Like feedback forms , Shopping carts , Search pages , product and support request forms, figure current websites , provide businesses and login pages etc pages are very necessary to commune with customers for keep our customer in touch. These kinds of pages of websites are very to use customer. These types are pages are suspicious for SQL hackers and foremost they attempts to try on these pages .We cannot hide this category of pages on website. If we do it then our client cannot be handling with us. So hacking the website is becoming very easy task for Hackers.

For Simple Example

To access the catalog database , normal user would input their username and password to come into their profile and access his personal details and change the contents which is allow by the administrative section i.e. authenticate user

are allowed to access our database. In other sides, our web network application which controls the authentication page will foremost communicate with our database through the specific planned commands as a result they be able to filter that he is authenticate user or not. In the case of valid user, database allows to access the contents.

In other sides, In case of SQL Injection, Specifically craft SQL commands with the intent of passing the login form difficulty is inputted by the hacker. In case of SQL Injection vulnerabilities, Hackers are eligible to converse with our database directly. Script languages which are Dynamic like JSP, PHP, and ASP.NET, CGI etc are the target technologies by the hacker. For publicity, our website wishes to be communal public so our safety mechanism will agree to to be communal public with our application (generally at beyond port 80/443).

SELECT count (*)

FROM person_list_table

WHERE

username=**'FIELD_USERNAME'** AND password=**'FIELD_PASSWORD"**

This SQL command is given instruction to the catalog database to compare User Id and secret code (password) filled by the current user to the combination that it has already stored in its database. Each and every web network application is hardly coded with specified SQL query so as to it will implement when executing functions and communicating with the database. If any data input of web network application is not accurately encoded, a hacker possibly will introduce extra vulnerable SQL queries which enlarge the area of SQL commands.

An attacker will therefore have a plain channel of communiqué to the web application database irrespective of the entire intrusion uncovering systems vulnerability and network based security equipments installed on the database layer.

V. SQL INJECTION IMPACT

When a hacker feels that a organism is ready to SQL Injection attacks, he is now able to insert SQL Commands to the n/w database an input from field. This is similarly like as to say attacker comes to make changes in our catalog and allow him to do insert or delete like DROP in to database. Execution of illogical SQL queries on the susceptible structure may be done by an attacker. This may break the reliability of your secure information. It depends on the back-end database, SQL injection vulnerabilities can be lead to varying levels of data/system access to the attacker. Manipulate in any existing queries, to UNION that is used to select related information from two tables use sub-selects arbitrary data, or append additional queries.

Some of the SQL Servers like Microsoft SQL Server contains stored and extended procedures for database server functions. In certain cases, it can be possible to read in or write out in files, and can execute shell commands on the underlying operating system. Data is being stolen through the various attacks at all the time. Hackers rarely get caught which are more expert.

Any attacker that can obtain access, it could spell disaster. A SQL injection attacks involves the modification of SQL statements that are used in a web application through the use of attacker-input data. Unfortunately the harm of SQL Injection is only found when the theft is discovered. Improper validation and improper construction and incorrect input of SQL statements in web applications can lead them theft to SQL injection attacks. Thus SQL

injection is a potentially destructive and prevalent attack that the Open Web Application Security Project (OWASP) listed it as the number one threat to web applications.

VI. PROPOSED SOLUTION

SQL injection can helps to retrieve sensitive information like password or credit card details, to prevent SQL injection developer should has to take some measure steps like use session in place of query string to transfer value from one page to another. Store sensitive information like password or credit card to XML or file system which is not easily accessible. If using Query

String is necessary try using URL Encoding technique. Now a day's some DBMS like MS SQL server supports Regular expression validation which protect data insertion like " ' ". All DBMS doesn't support ""handle it is very Necessary replace it with some other character.

Blindfolded SQL Injection techniques

(a) Boolean queries and WAIT FOR DELAY are used by Blind folded injection technique.

(b) By using commands such as BETWEEN, LIKE, IS NULL Comparison in queries is done.

IDS signature evasive SQL Injection techniques

(a) By using CONVERT & CAST commands by masking the attack payload.

(b) By using Null bytes to break the signature patterns.

(c) By using HEX encoding mixtures.

(d) By using SQL CHAR ( ) to convert ASCII values as numbers.

Example, when the attacker decided to go with a attack using: 1 = 1, at that time when it is entered as input box. The server recognizes 1 = 1 as a true statement and -- symbol is used for comment, everything after that is ignored making it possible to the attacker to access to the database. Through this SQL injection example page you can see precisely how this attack works on:

Welcome to SQL Injection Application

Logged in as: or '1=1--'AND Password='

Other sample pages:

BadProductList- Product List that is vulnerable to SQL Injection.

BetterProductList- Product List that is still vulnerable but that uses a lower privilege account to minimize damage.

EncryptCnxString- Utility for encrypting any string: use it to encrypt cnxWindBest connection string in web config.

AddSecureUser- Add new users to Secure User table: Password will be hashed use it with BestLoginaspx.

PRODUCT LIST:

Product **Filter: 'UPDATE** Products SET Unit Price=0.0

Product Id	**Product Name**	**Quantity Per Unit**	**Unit Price**
1.	pen	10 boxes*20 bags	0.0000
2.	Alcohol	24-12 oz bottles	19.0000
3.	paper	36 boxes	21.3500
4.	Aniseed Syrup	12-550 ml bottle	0.0111
5.	Seasoning	48-6 oz jars	22.0000
6.	Jelly	12-8 oz jars	25.0000
7.	Uncle Bob's Organic Pears	12-1 ib pkgs.	30.0000
8	Cranberry Sauce	12-12 oz jars	40.0000
9.	Jam	18-500 g pkgs.	97.0000
10.	Pickle	12-200 ml jars	31.0000

WHERE Product=Set Filter

Fig.2

OUR ALGORITHM STEPS OF URL ENCODING ARE

string strCnx = ConfigurationSettings.AppSettings["cnxNWindBad"]; SqlConnection cnx = new SqlConnection(strCnx); cnx.Open();

string strQry = "SELECT Count(*) FROM Users WHERE UserName='" +

```
txtUser.Text + "' AND Password='" + txtPassword.Text + "'";
int intRecs;
SqlCommand cmd = new SqlCommand(strQry, cnx); cmd.CommandType= CommandType.Text;
intRecs = (int) cmd.ExecuteScalar(); if (intRecs>0)
{
FormsAuthentication.RedirectFromLoginPage(txtUser.T ext, false);
}
else
{
lblMsg.Text = "Login attempt failed.";
}
cnx.Close();
//Prevention string strCnx =
ConfigurationSettings.AppSettings["cnxNWindBetter"]; using(SqlConnection cnx = new SqlConnection(strCnx))
{
cnx.Open(); SqlCommand cmd = new
SqlCommand("procVerifyUser", cnx); cmd.CommandType= CommandType.StoredProcedure; SqlParameter prm
= new SqlParameter("@username",SqlDbType.VarChar,50); prm.Direction=ParameterDirection.Input;
prm.Value = txtUser.Text; cmd.Parameters.Add(prm); prm = new
SqlParameter("@password",SqlDbType.VarChar,50);
prm.Direction=ParameterDirection.Input; prm.Value = txtPassword.Text; cmd.Parameters.Add(prm);
string strAccessLevel = (string) cmd.ExecuteScalar(); if (strAccessLevel.Length>0)
{
FormsAuthentication.RedirectFromLoginPage(txtUser.T ext, false);
}
else
{
lblMsg.Text = "Login attempt failed.";
}
}
```

VII. CONCLUSION

SQL attackers create crafted input data so that SQL interpreter has to accept the query and give the permission to execute the commands and give his desired results. SQL Injection attack breaks the security in the database layer and can alter, steal or destroy our database through using web application.

REFERENCES

(1) Ke Wei, M. Muthuprasanna, Suraj Kothari , Dept. of Electrical and Computer Engineering , Iowa State University Ames, IA – 50011 ,Email: {weike,muthu,kothari}@iastate.edu

(2) Cerrudo. Manipulating Microsoft sql server using sql injection.

(3) http://www.appsecinc.com/presentations/Mani pulating SQL Server Using SQL Injection.pdf, White Paper.

(4) William G.J. Halfond, Jeremy Viegas, and Alessandro Orso College of Computing Georgia Institute of Technology {whalfond|jeremyv|orso}@cc.gatech.edu

(5) Z. Su and G. Wassermann. The Essence of Command Injection Attacks in Web Applications. In The 33rd Annual Symposium on Principles of Programming Languages (POPL 2006), Jan. 2006.

(6) F. Valeur, D. Mutz, and G. Vigna. A Learning-Based Approach to the Detection of SQL Attacks. In Proceedings of the Conference on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA), Vienna, Austria, July 2005.

(7) T. M. D. Network. Request.servervariables collection. Technical report, Microsoft Corporation, 2005. http://msdn.microsoft.com/library/default. asp?url=/library/en-us/iissdk/html/9768ecfe-8280-4407-b9c0-844f75508752.asp.

(8) José Fonseca CISUC - Polithecnic Institute of Guarda, Marco Vieira, Henrique Madeira DEI/CISUC - University of Coimbra. Testing and comparing web vulnerability scanning tools for SQL injection and XSS attacks. Retrieved July 10, 2007, from http://ieeexplore.ieee.org

(9) Yuji Kosuga, Kenji Kono, Miyuki Hanaoka Department of Information and Computer Science Keio University. Sania: Syntactic and Semantic Analysis for Automated Testing against SQL Injection. Retrieved November 12, 2007, from IEEE Computer Society. http://ieeexplore.ieee.org

(10) Benjamin Livshits and U´ lfar Erlingsson. Microsoft Research. Using Web Application Construction Frameworks to Protect Against Code Injection Attacks. Retrieved June 14, 2007, from http://ieeexplore.ieee.org

ANALYSIS OF SHA-1 IMPLEMENTATION USING BASELINE ARCHITECTURE AND MULTI-INPUT ADDING

Deepika Sharma

Student, Department of Electronics and Communication Engineering,
School of Engineering and Technology, Poornima University, Jaipur (India)

ABSTRACT

Due to the rapid developments in the wireless communications area and personal communications systems, providing information security has become a more and more important subject. This security concept becomes a more complicated subject when next-generation system requirements and real-time computation speed are considered. In order to solve these security problems, lots of research and development activities are carried out and cryptography has been a very important part of any communication system in the recent years.The hardware is described in VHDL and verified on Xilinx FPGAs. The advantages and open issues of implementing hash functions using a processor structure are also discussed. This constitutes the physical design. Being an elaborate and costly process, a physical design may call for an intermediate functional verification through the FPGA route. The circuit realized through the FPGA is tested as a prototype. It provides another opportunity for testing the design closer to the final circuit.

Keywords: Cryptography, Hash functions

I. INTRODUCTION

Cryptography is the branch of computer science that deals with security. It supports operations such as encryption and decryption. The cryptography is implemented in the form of hash functions, symmetric key algorithms, and public key algorithms. The symmetric and public key algorithms are used for encryption and decryption while hash functions are one way functions as they don't allow the retrieval of processed data. As MD5 and SHA are the two mostly used algorithms in the industry, this paper focuses on secure hash algorithm. Hash algorithms, also commonly called as message digest algorithms, are algorithms generating a unique fixed-length bit vector for an arbitrary-length message *M*. The bit vector is called the hash of the message and it is here denoted as *H*. The hash can be considered as a fingerprint of the message.

The hash function *H* must have the following properties:

- *One-way property*: for any given value *h*, it is computationally infeasible to find *x* such that $H(x) = h$.
- *Weak collision resistance*: for any given message *x*, it is computationally infeasible to find $y \neq x$ with $H(y) = H(x)$.
- *Strong collision resistance*: it is computationally infeasible to find any pair (x, y), such that $H(x) = H(y)$.

II. SHA-1 ALGORITHM

Secure Hash Algorithm (SHA) is described in the National Institute of Standards and Technology's (NIST) Federal Information Processing Standard (FIPS) 180-2: Secure Hash Standard (SHS) [3]. SHS describes the following algorithms: SHA-1 (SHA-160), SHA-256, SHA-385 and SHA-512, where the number is the length of the hash *H* in bits. In this report, only SHA-1 (SHA-160) is considered. SHA-1 is widely used in various public-key cryptographic algorithms, e.g. in Digital Signature Algorithm (DSA) [6]. SHA-1 calculates a 160-bit *H* for a *b*-bit *M*. The algorithm consists of the following steps:

1. *Appending Padding Bits:* - The *b*-bit *M* is padded in the following manner: a single 1-bit is added into the end of *M*, after which 0-bits are added until the length of the message is congruent to 448, modulo 512.
2. *Appending Length:* - A 64-bit representation of *b* is appended to the result of the above step. Thus, the resulted message is a multiple of 512 bits.
3. . *Buffer Initialization:* - Let H0, H1, H2, H3 and H4 be 32-bit hash value registers. These registers are used in the derivation of a 160-bit hash H. At the beginning, they are initialized as follows:

H0 = x″67452301″
H1 = x″e f cdab89″
H2 = x″98badc f e″
H3 = x″10325476″
H4 = x″c3d2e1 f 0″

1. *Hash Calculation:* SHA1 may be used to hash a message, M, having a length of *l* bits, where $0 \leq l \leq 264$. The algorithm uses:

- A message schedule of 80x32-bit words. The words of the message schedule are labeled W0, W1.
- Five working variables of 32-bits each. The working variables are labeled as: A, B, C, D and E.
- A hash value of five 32-bit words. The words of the hash value are labeled as: H0(i), H1(i), H2(i), H3(i), H4(i) which will hold the initial hash value H(0), replaced by each intermediate hash value (after each message block is processed) H(i) where i denotes the number of 512 bit block being processed in the message M, and ending with the final hash value, H(N) where N is the number of the last 512 bit block in the message M.
- A single temporary word, T. Previously defined constants which are labeled Kt, where t is the round number.

The calculation is carried out as follows:

The message schedule is prepared, i.e. the message word that is going to be used in that round is prepared. This computation is done as described in the following formula:

$Wt = Mti \; 0 \leq t \leq 15$

$Wt = ROTL(Wt\text{-}3 \oplus Wt\text{-}8 \oplus Wt\text{-}14 \oplus Wt\text{-}16) \; 16 \leq t \leq 79$

In the above formula Mit denotes the tth 32-bit message word of the ith 512-bit message block in the message M. The 5 working variables A, B, C, D and E that are going to be used in the computation are prepared as follows:

A = H0 (i–1) B = H1 (i–1)

C = H2 (i–1) D = H3 (i–1) E = H4 (i–1)

After these initializations, the final values of the working variables for that round are calculated as described below:

$T = S^5(A)+f(t;B,C,D) + E + Wt + Kt$

$E = D$

$D = C$

$C = S^{30}(B)$

$B = A$

$A = T$

Finally, when all 80 steps have have been processed, the following operations are performed:

$H0 \leftarrow H0+A$

$H1 \leftarrow H1+B$

$H2 \leftarrow H2+C$

$H3 \leftarrow H3+D$

$H4 \leftarrow H4+E$

4. *Output:* - When all *Mj* have been processed with the above algorithm, the 160-bit hash *H* of *M* is available in *H*0, *H*1, *H*2, *H*3 and *H*4.

III. VERILOG IMPLEMENTATION

In this study the aim is to implement the designed hash function core on Verilog. The whole package and separate modules were synthesized and analyzed using Xilinx ISE 12.1 tool.

- The Verilog implementation was divided into five modules: *Initial module:* - It collects the serial input bits and sends 512 bit blocks to the next module.
- *Round module:* - It performs the hashing calculations and operations on the input message block and previous hash output to generate a new hash value.
- *Last Block module:* - At the end of the message bit stream the final message block of 512 bits has to be prepared by adding 64 bits of message length at the end of 448 bits of input message block, padded accordingly to suffice the word size requirement. This final message block does this function of preparing the last message block.
- *Final module:* - This module computes the hash value by adding the previous hash value to the new hash value achieved from the Round module. Then it sends the 160 bit hash value, bit by bit (serially).

Top module: - This module is the control unit for controlling the functioning of the rest of the modules and to ensure that the SHA1 algorithm flow is followed and maintained

IV. METHODOLOGIES/SOLUTION APPROACHES

[Aianhua He, et-al, 2009] has proposed the FPGA based and performance analysis of a compatible SHA series design. The novelty of the design is that it can provide all of the SHA functions: SHA-1, SHA-256, and SHA-512 with limited trade- off. Block RAM, the base element of FPGA, is used to diminish the logic block consumption, while the scalable Wt generator and the arithmetic logic reuse decrease the proneness of the extra resource consumption. The Mixed-SHA is able to achieve 442Mbps. Two other assumptions, SHA_1_256,

SHA_1_512, are made to discuss the bottleneck of the design, and providing two other optional compatible designs, at the same time, to face different requirements of the application. The throughput then raise to 1.2Gbps

With using about 1100 Slices, less than 1% of the total resources in xc5vlx220. In all, by comparing with the performance of the design that quote from other authors, the Mixed-SHA implementation has a comparable performance, and better compatibility than other design [2].

[Brian Baldwin, et-al, 2010] has presented a methodology for fair and accurate comparisons of the SHA-3 hash functions. Author implemented and tested as many designs as was necessary to obtain full coverage of all of the hash variants as required by NIST. Author developed a hardware wrapper to allow inclusion of padding and interfacing, to obtain the full timing and area analysis, and for completeness compared the area and speed of the hash designs both internal and external of this wrapper. Finally author presented throughput results for both long and short hash messages inclusive of this wrapper [3].

[Bernhard Jungk, et-al, 2011] has focused on area-efficient FPGA implementations of the SHA-3 finalists. The performance of Gristle is considered the best alongside Keycap in terms of the throughput-area ratio; BLAKE follows closely, while Skein and JH trail behind. If the focus lays on pure area consumption, the situation reverses and it is much easier to implement a really small JH or BLAKE design.Keccak, Gristle and Skein are much bigger. There is still room for improvements of almost all implementations. For example, the area of Keycap could probably is further reduced by making a design which usesonly4slices in parallel and JH could be much faster, if more parallelism is used [5].

[C.P Arsenal, et-al, 2007] has discussed different design architectures of Blake-256 implemented on FPGA. Design uses large hardware resources gives maximum throughput i.e. 8G design requires only 14 clock cycles for Hash value calculation resulted throughput of 2.6 Gbps. 1G design gives most efficient results in terms of number of slices utilized. The optimized delay path is utilized in 4G design with respect to Virtex 5 architecture. That's gives maximum TPA of 2.1. Appropriate selection of number of slice LUTs and Slice registers and their placement according to the Virtex 5 Device Architecture Resources gives the optimized results. The selection of architecture is dependent upon type of application either high speed requirements or low area constraints, suitable optimization could be performed in a particular domain to achieve best design results [4].

[Fatma Kahri, et-al, 2013] has presented an architecture and efficient hardware implementation of SHA -256. Author reported the implementation results of SHA-256 and new hash function on Xilinx Virtex 2, Virtex 5, Virtex 6 and Virtex 7 FPGAs. The performance of the implementation in terms of area, throughput, frequency and efficiency and compared the standard with the newest hash function [9].

V. STRENGTHS AND LIMITATIONS

- MD5 and SHA-1 both have very fast bitwise operators that make up the function , so they can be computed very, very quickly on a modern processor.
- Hash functions are the most important cryptographic algorithms and used in several fields of communication integrity and signature authentication.
- It is used in Digital signature algorithms and Throughput improvement.

- Rather than storing a user's password, a system will typically store the hash of the password instead. When a user enters their password, the hash is then computed and compared with the stored hash. If the hash matches, due to the collision resistance property of hashing algorithms, it implies that the passwords match.
- The sender can hash a file before sending to the recipient. The recipient will then hash the file received and check the hashes match. This can also be used for the storage of files, to ensure files have not been corrupted or modified.

VI. IMPLEMENTATION RESULTS

As shown in Table 1 the proposed SHA-1 implementation reduces the area by 24.5% and increases the speed by 13.6%.Meanwhile my implementation with the same clock speed reduces the area by 39.7% which meant significant decrease in area.

Table 1 Implementation Results

	Frequency(MHz)	Area
Proposed	714	6067.8
	625	5469.5
[3]	625	9064.5

VII. CONCLUSION

It is stated that SHA-1 can be efficiently implemented on FPGAs with minimal logic resources. In this study hash functions SHA1 is implemented in a processor structure using the same hardware blocks. These hash functions are examined in detail and a new instruction set is proposed. Hash processor is fully designed and captured using VERILOG HDL in Xilinx ISE software environment. The design is also implemented on Xilinx FPGA and implementation results are given. The designed hash function core has serial interface that makes communication with the external units such as a personal computer possible.

VIII. ACKNOWLEGDEMENT

I would like to express my deep gratitude and thanks to **Prof. Mahesh Bundele (Coordinator, Research), Poornima University** for giving me an opportunity to work under his guidance for review of research papers and his consistent motivation & direction in this regard. I would also express my sincere thanks to **Mr. Dipesh Patidar (Asst.Professor, ECE), PIET** for their guidance and support.

REFERENCES

[1] Dai Zibin; Zhou Ning, "FPGA implementation of SHA-1 algorithm," ASIC, 2003. Proceedings. 5th International Conference on, vol.2, no., pp.1321, 1324 Vol.2, 21-24 Oct. 2000

[2] Docherty, J.; Koelmans, A., "A flexible hardware implementation of SHA-1 and SHA-2 Hash Functions," Circuits and Systems (ISCAS), 2011 IEEE International Symposium on, vol., no., pp.1932, 1935, 15-18 May 2011

[3] Eiroa, S.; Baturone, I., "Hardware authentication based on PUFs and SHA-3 2nd round candidates," Microelectronics (ICM), 2010 International Conference on, vol., no., pp.319, 322, 19-22 Dec. 2010

[4] El-Hadedy, M.; Gligoroski, D.; Knapskog, S.J., "Low Area Implementation of the Hash Function "Blue Midnight Wish 256" for FPGA Platforms," Intelligent Networking and Collaborative Systems, 2009. INCOS '09. International Conference on, vol., no., pp.100, 104, 4-6 Nov. 2009

[5] Eun-Gu Jung; Daewan Han; Jeong-Gun Lee, "Low area and high speed SHA-1 implementation," SoC Design Conference (ISOCC), 2011 International , vol., no., pp.365,367, 17-18 Nov. 2011

[6] Guoping Wang, "An Efficient Implementation of SHA-1 Hash Function," Electro/information Technology, 2006 IEEE International Conference on , vol., no., pp.575,579, 7-10 May 2006

[7] Iumoka, A.A., "Efficient prediction of hash function in VLSI using neural networks," Electrical Performance of Electronic Packaging, 2000, IEEE Conference on. , vol. no., pp.87, 90, March 2000

[8] Junmou Zhang; Friedman, E.G., "Power Estimation for Cycle-Accurate Functional Descriptions of Hardware," Circuits and Systems, 2004. ISCAS '04. Proceedings of the 2004 International Symposium on, vol.2, no., pp.II, 529-32 Vol.2, 23-26 May 2004

[9] Kayu, R.; Maheshwari, V.; A.K., "ASIC-hardware-focused comparison for hash functions MD5, RIPEMD-160, and SHS,"Computing Communication and Networking Technologies (ICCCNT), 2010 International Conference on, vol., no., pp.1,6, 29-31 July 2010

[10] Kitsos, P.; Sklavos, N.; Koufopavlou, O., "An efficient implementation of the digital signature algorithm," Electronics, Circuits and Systems, 2002. 9th International Conference on, vol.3, no., pp.1151, 1154 vol.3, 2002

[11] Khalil-Hani, M.; Nambiar, V.P.; Marsono, M.N., "Hardware Acceleration of OpenSSL Cryptographic Functions for High-Performance Internet Security," Intelligent Systems, Modelling and Simulation (ISMS), 2010 International Conference on, vol., no., pp.374, 379, 27-29 Jan. 2011

[12] K.K. Murthy, N.S.; Rao, N.B., "An efficient power estimation model for high speed VLSI," Advances in Computing, Communications and Informatics (ICACCI), 2013 International Conference on, vol., no., pp.1358, 1362, 22-25 Aug. 2013

[13] K.M. Banerjee, and Amit Mehrotra, "A Novel Power Estimation Method for On-chip VLSI Distributed RLCG Global Interconnects Using Model Order Reduction Technique," IEEE Transactions On Computer-Aided Design of Integrated Circuits And Systems, Vol. 21, No. 8, August 2013

[14] Lao, R.; Maheshwari, V.; Agarwal, V.; Choudhary, A.; Singh, A.; Mai, A.K.; Bhattacharjee, A.K., "Accurate estimation of delay for step input," Computer and Communication Technology (ICCCT), 2010 International Conference on , vol., no., pp.673,677, 17-19 Sept. 2010

[15] L. V.; Mondal, S.; Maqbool, M.; Mal; Bhattacharjee, A.K., "A Novel Power Estimation Method for On-chip VLSI," Advances in Computer Engineering (ACE), 2010 International Conference on, vol., no., pp.105, 109, 20-21 June 2010

[16] Lin Zhou; Wenbao Han, "A Brief Implementation Analysis of SHA-1 on FPGAs, GPUs and Cell Processors," Engineering Computation, 2009. ICEC '09. International Conference on , vol., no., pp.101,104, 2-3 May 2009

[17] Li Hong-Qiang; Miao Chang-yun, "Hardware Implementation of Hash Function SHA-512," Innovative Computing, Information and Control, 2006. ICICIC '06. First International Conference on, vol.2, no., pp.38, 42, Aug. 30 2006-Sept. 1 2006

[18] Michail, H.; Goutis, C., "Holistic methodology for designing ultra high-speed SHA-1 hashing cryptographic module in hardware," Electron Devices and Solid-State Circuits, 2008. EDSSC 2008. IEEE International Conference on, vol., no., pp.1, 4, 8-10 Dec. 2008

[19] Michail, H.E.; Kakarountas, A.P.; Milidonis, A.; Goutis, C.E., "Efficient implementation of the keyed-hash message authentication code (HMAC) using the SHA-1 hash function," Electronics, Circuits and Systems, 2004. ICECS 2004. Proceedings of the 2004 11th IEEE International Conference on, vol., no., pp.567, 570, 13-15 Dec. 2004

[20] Michail, Harris; Kakarountas, A.P.; Koufopavlou, O.; Goutis, C.E., "A low-power and high-throughput implementation of the SHA-1 hash functions," Circuits and Systems, 2005. ISCAS 2005. IEEE International Symposium on, vol., no., pp.4086, 4089 Vol. 4, 23-26 May 2005

[21] M. L. L. X. Wang, H. Yu, "Finding collisions in the full SHA-1," in Advances in Cryptology, Proceedings Crypto'05, IEEE Transactions on, pp. 17-36, May 2005

[22] N. Ahmad and A. S. Das, "Analysis and detection of errors in implementation of SHA-512 Algorithms on FPGAs," Computer Journal, vol. 50, pp. 728-738, May 2007

[23] N. Ferguson, B. Schneier, and T. Kohno, "Cryptography engineering: design principles and practical application", IEEE Transactions on, vol., no., pp.673, 677, 17-19 Sept. 2004

[24] N.K. Satoh and T. Inoue, "ASIC-hardware-focused comparison for hash functions MD5, RIPEMD-160, and SHS," in International Conference on Information Technology: Coding and Computing, ITCC, 2005, pp. 532-537 May 2004

[25] N. I. o. S. a. Technology, "Announcing the Standard for Secure Hash Standard," 50th Midwest Symposium on, vol., no., pp.21, 24, 5-8 Aug. 2007

[26] P. K. Yuen, Practical cryptology and web security. Harlow: Addison-Wesley, IEEE Transactions on, vol., no., pp.673, 677, 17-19 March 2005

[27] P. Chang, Y. Chu, and C. Jen, "Low-cost subsystem power estimation", IEEE Trans. Circuits Syst. II, vol. 47, pp. 137–145, Feb. 2007

[28] R. Puri and C.T. Chuang, "SO1 Digital Circuits: Design Issues," Thirteenth International Conference on VLSI Design, pp. 474-479, 2008

[29] Roy M. Pelella, "Hysteresis in Floating- Body PD/SOI CMOS Circuits," International Symposium on VLSI Technology Systems and Applications, pp. 278-281, March 2008

[30] Putri Ratna, A.A.; Dewi Purnamasari, P.; Shaugi, A.; Salman, M., "Analysis and comparison of MD5 and SHA-1 algorithm implementation in Simple-O authentication based security system," QiR (Quality in Research), 2012

[31] S. Steinke, M. Knauer, L. Wehmeyer, and P. Marwedel,"An Accurate and Fine Grain Instruction- Level Energy Model Supporting Software Optimizations," in Proc. Int. Wkshp Power & Timing Modeling, Optimization & Simulation (PATMOS), March 2008

[32] Sinha and A. P. Chandrakasan, "Joule Track - A Web Based Tool for Software Energy Profiling," in Proc. Design Automation Conf., pp. 220–225, April 2009

[33] S. B. Kamble and K. Ghose, "Analytical Models for Energy Dissipation in Low Power Caches," in Proc. Int. Symp. Low Power Electronics & Design, pp. 143–148, March 2009

[34] Selimis, G.; Sklavos, N.; Koufopavlou, O., "VLSI implementation of the keyed-hash message authentication code for the wireless application protocol," Electronics, Circuits and Systems, 2003. ICECS 2003. Proceedings of the 2003 10th IEEE International Conference on, vol.1, no., pp.24, 27 Vol.1, 14-17 Dec. 2003

[35] Sklavos, N.; Dimitroulakos, G.; Koufopavlou, O., "An ultra high speed architecture for VLSI implementation of hash functions," Electronics, Circuits and Systems, 2003. ICECS 2003. Proceedings of the 2003 10th IEEE International Conference on, vol.3, no., pp.990,993 Vol.3, 14-17 Dec. 2003

[36] Tang Qiong; Ye Jianwu, "Implementation and Optimization of the High Performance SHA-1 Model Based on FPGA," Computer Science & Service System (CSSS), 2012 International Conference on, vol., no., pp.687, 690, 11-13 Aug. 2012

[37] Thang Qiong; Ye Jianwu, "Implementation and Optimization of the High Performance SHA-2Model Based on FPGA," Computer Science & Service System (CSSS), 2012 International Conference on, vol., no., pp.687, 690, 11-13 Aug. 2011

[38] Thamrin, N.M.; Ahmad, I.; Khalil Hani, M., "A secure field programmable gate array based System-on-Chip for Telemedicine application," Information Society (i-Society), 2011 International Conference on, vol., no., pp.105, 109, 27-29 June 2011

[39] Yu Ming-yan; Zhou Tong; Wang Jin-xiang; Ye Yi-zheng, "An efficient ASIC implementation of SHA-1 engine for TPM," Circuits and Systems, 2004. Proceedings. The 2004 IEEE Asia-Pacific Conference on, vol.2, no., pp.873, 876, 6-9 Dec. 2004

[40] Zhou Hua; Liu Qiao, "Hardware design for SHA-1 based on FPGA," Electronics, Communications and Control (ICECC), 2011 International Conference on, vol., no., pp.2076, 2078, 9-11 Sept. 2011

ATTRIBUTE-BASED SECURE DATA RETRIEVAL SCHEME USING CP-ABE

M.Baby[1], T.Brindha[2], A.Dhivya[3], B.Gnanamozhi[4]

[1,2,3,4] *Information Technology, Panimalar Engineering College, (India)*

ABSTRACT

Mobile nodes in military environments such as a battlefield or a hostile region suffer from intermittent network connections and frequent partitions. Disruption-tolerant network (DTN) technologies are best solutions that allow wireless devices carried by soldiers to communicate and access the confidential information or command reliably by exploiting external nodes. Cipher text-policy attribute-based encryption (CP-ABE) is a cryptographic solution to the access control issues. The problem of applying CP-ABE in decentralized DTNs generates several security and privacy issues with attribute updation, key escrow problem, and attribute coordination issued from different key authorities. We propose a attribute based secure data retrieval scheme for decentralized DTNs where multiple key authorities manage their attributes separately. In this paper,we are proposing CP-ABE using MD5 algorithm and two channels are required for secure data retrieval. We demonstrate how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption-tolerant military network.

I. INTRODUCTION

In several military networks,wire-less devices gets disconnected due to jamming, environmental factors, and changes in position, mainly when they operate in remote environments. Disruption-tolerant network (DTN) technologies are best solutions that allow nodes to communicate with each other in extreme networking environments. When there is no end-to-end connection, the messages from the source node may need to wait in the intermediate nodes for a substantial amount of time until the connection would be eventually established.

Roy and Chuah introduced storage nodes in DTNs where data is stored or replicated such that only authorized mobile nodes can access the necessary information quickly and efficiently. In many scenarios, it is desirable to provide differentiated access services such that data access policies are defined over user attributes.The key authorities will manage these data access policies. For instance, in a Disruption-tolerant military network, a sender may store confidential information at a intermediate node, which must be accessed by "Battalion 1" who are participating in "Region 2." In this case, it is a reasonable assumption that multiple key authorities are likely to manage their own dynamic attributes for soldiers in their deployed regions or echelons, which could be frequently changed. We refer DTN architecture where multiple authorities issue and manage their own attribute keys independently as a decentralized DTN.

The concept of attribute-based encryption (ABE) is a promising approach that fulfills the requirements for secure data retrieval. ABE enables an access control over encrypted data using access policies and ascribed

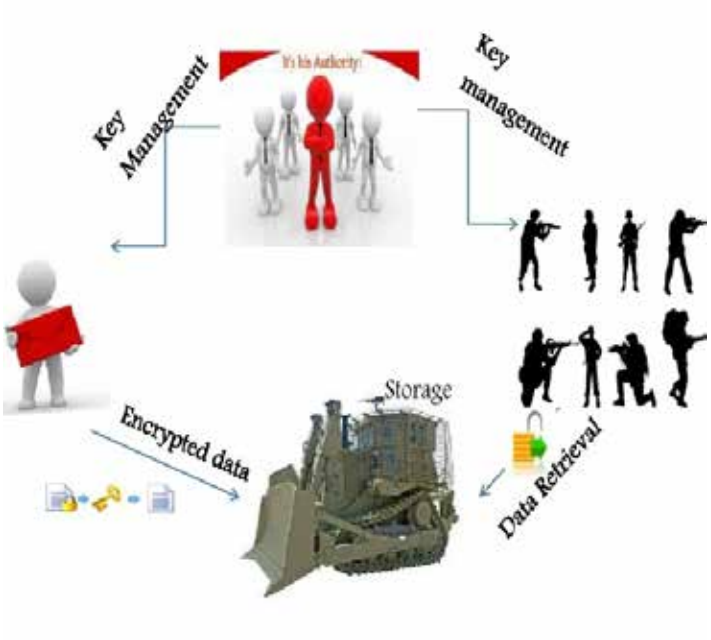
attributes among private keys and cipher texts. Especially, cipher text-policy ABE (CP-ABE) provides a scalable way of encrypting data such that the encryptor defines the attribute set that the decryptor needs to possess in order to de-crypt the cipher text . Thus, different users are allowed to decrypt different pieces of data per the security policy.

However, the problem of applying the ABE to DTNs introduces several security and privacy issues. Since users may change their associated attributes at some point (for ex-ample, mobility), or some private keys might be compromised, key revocation (or update) for each attribute is necessary in order to make systems secure. However, this issue is more challenging, mainly in ABE, since each attribute is conceivably shared by multiple users (we refer to such a collection of users as an attributes). This shows that attribute revocation or any single user in an attribute group would affect the other users in the group. For instance, if a member joins or leaves an attribute group, the corresponding attribute key should be changed and redistributed to all the other members in the same group for backward or forward secrecy. It may cause problem during rekeying procedure, or degrade the security due to the windows of vulnerability if the previous attribute key is not updated immediately.

Another challenge is the key escrow . In CP-ABE, the key authority provides private keys by applying the authority's master secret keys to members' associated set of at-tributes. Thus, the key authority can dechiper every cipher text to specific users by generating their attribute keys. If the key authority is compromised by hackers when deployed in the remote environments, this could be a main threat to the data confidentiality or privacy especially when the data is highly sensitive. The key escrow is an main problem in the multiple-authority systems as long as each key authority has the whole access to generate their own attribute keys with their own master secrets. Since the key generation mechanism based on the single master secret is the basic method for the asymmetric encryption systems such as the attribute-based or identity-based encryption rules, removal of key escrow in single or multiple-authority CP-ABE is a pivotal open problem.

The last issue is the coordination of attributes issued from different key authorities. When multiple key authorities manage and issue attributes keys to users with their own master secrets, which is very difficult to define fine-grained access policies over attributes issued from different key authorities. For instance,the attributes "role 1" and "region 1" are man-aged by the authority X, and "role 2" and "region 2" are man-aged by the authority Y.It is impossible to produce an access policy ("role 1" OR "role 2") AND ("region 1" or "region 2")) in the previous schemes because the OR logic between attributes issued from different authorities cannot be invented. Because, the fact that the different authorities generate their own attribute keys using their own independent and separate master secret keys. Hence, general access policies, such as " -out-of- " logic, cannot be expressed in the previous methods, which is a very practical and commonly required access policy logic.

II. NETWORK ARCHITECTURE



2.1 System Description and Assumptions

1)Key Authorities: Key authorities are key generation centers that generate public/secret parameters for CP-ABE. The key authorities contain a central authority and many local authorities. We take that there are secure and reliable communication channels between a central authority and every local authority during the initial key setup and generation phase. Each local authority maintains different attributes and provides associate attribute keys to members. They allow different access rights to each users based on the members' attributes. The key authorities are assumed to be honest. ie, they will execute the assigned tasks in the node, therefore they would learn information of encrypted contents as much as possible.

2)Storage node: Storage node is an entity that stores data from senders and provide access to members. It may be dynamic or static. Similar to the previous schemes, we also assume the storage node is honest-but-curious.

3)Sender: This is an entity who owns confidential messages or data (e.g., a commander) and wishes to store them into the external data storage node for ease of sharing or for reliable delivery to users in the extreme networking environments. A sender is responsible for defining (attribute- based) access policy and enforcing it on its own data by encrypting the data under the policy before storing it to the storage node.

4)User: This is a mobile node who wants to access the data stored at the storage node (e.g., a soldier). If a user possesses a set of attributes satisfying the access policy of the unreadable data explain by the commander, and is not revoked, then decrypt the ciphertext and obtain the data.

III. SYSTEM ANALYSIS

In this section, we describe the DTN architecture and define the security model

IV. EXISTING SYSTEM

In several military networks,wire-less devices gets disconnected due to jamming, environmental factors, and changes in position, mainly when they operate in remote environments. Disruption-tolerant network (DTN) technologies are best solutions that allow nodes to communicate with each other in extreme networking environments. When there is no end-to-end connection, the messages from the source node may need to wait in the intermediate nodes for a substantial amount of time until the connection would be eventually established.

Roy and Chuah introduced storage nodes in DTNs where data is stored or replicated such that only authorized mobile nodes can access the necessary information quickly and efficiently. In many scenarios, it is desirable to provide differentiated access services such that data access policies are defined over user attributes.The key authorities will manage these data access policies. For instance, in a Disruption-tolerant military network, a sender may store confidential information at a intermediate node, which must be accessed by "Battalion 1" who are participating in "Region 2." In this case, it is a reasonable assumption that multiple key authorities are likely to manage their own dynamic attributes for soldiers in their deployed regions or echelons, which could be frequently changed. We refer DTN architecture where multiple authorities issue and manage their own attribute keys independently as a decentralized DTN.

4.1 Disadvantages of Existing System

1. No Proper Encryption Schema is implemented.
2. security degradation.
3. Key escrow.

V. PROPOSED SYSTEM

The concept of attribute-based encryption (ABE) is a promising approach that fulfills the requirements for secure data retrieval. ABE enables an access control over encrypted data using access policies and ascribed attributes among private keys and cipher texts. Especially, cipher text-policy ABE (CP-ABE) provides a scalable way of encrypting data such that the encryptor defines the attribute set that the decryptor needs to possess in order to de-crypt the cipher text . Thus, different users are allowed to decrypt different pieces of data per the security policy.

However, the problem of applying the ABE to DTNs introduces several security and privacy issues. Since users may change their associated attributes at some point (for ex-ample, mobility), or some private keys might be compromised, key revocation (or update) for each attribute is necessary in order to make systems secure. However, this issue is more challenging, mainly in ABE, since each attribute is conceivably shared by multiple users (we refer to such a collection of users as an attributes). This shows that attribute revocation or any single user in an attribute group would affect the other users in the group. For instance, if a member joins or leaves an attribute group, the corresponding attribute key should be changed and redistributed to all the other members in the same group for backward or forward secrecy. It may cause problem during rekeying procedure, or degrade the security due to the windows of vulnerability if the previous attribute key is not updated immediately.

Another challenge is the key escrow . In CP-ABE, the key authority provides private keys by applying the authority's master secret keys to members' associated set of at-tributes. Thus, the key authority can dechiper every cipher text to specific users by generating their attribute keys. If the key authority is compromised by hackers when deployed in the remote environments, this could be a main threat to the data confidentiality or privacy especially when the data is highly sensitive. The key escrow is an main problem in the multiple-authority systems as long as each key authority has the whole access to generate their own attribute keys with their own master secrets. Since the key generation mechanism based on the single master secret is the basic method for the asymmetric encryption systems such as the attribute-based or identity-based encryption rules, removal of key escrow in single or multiple-authority CP-ABE is a pivotal open problem.

5.1 Authentication

This module helps to send the message safely from a commander to the soldier in the war field. They both should set a secret Key word for sending and receiving the message safely. Without that keyword the message cannot be read by the soldier.

5.2 Sending Message

When a commander is sending message to his soldier in war field he needs to set a secret key which is known to him and his soldier alone. So, when he sends a message to him the soldier should enter the secret key word and then only the message will be displayed.

5.3 Encryption

Encryption is a process of converting a message, called the Plaintext, into an unreadable message, called the Cipher text. This is usually accomplished using a secret Encryption Key and a cryptographic Cipher. It helps to avoid eaves dropping when the message is sent.

5.4 Receiver

When a soldier is receiving message from his commander in war field , he should enter the secret key and after decryption ,then the message will be displayed.

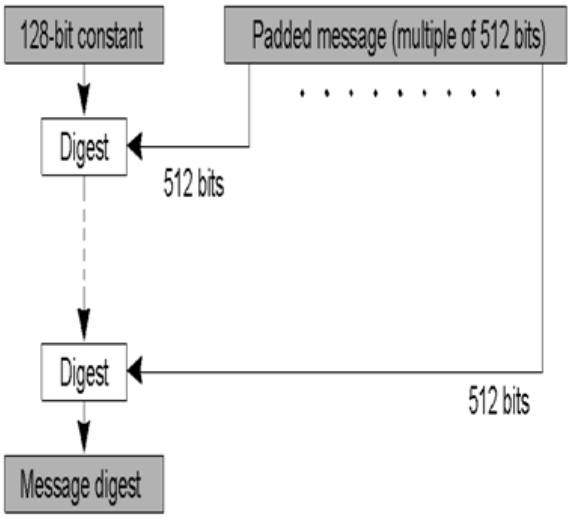
5.4.1 Advantages of Proposed System

1. Data Transmission without any interruption.
2. Secure transmission of data between nodes.

VI. METHODOLOGY

MD5 algorithm was introduced by Professor Ronald L. Rivest in 1991.MD5 algorithm takes as input a message of arbitrary length and produces as output a 128-bit "fingerprint" or "message digest" of the input …The MD5 algorithm is intended for digital signature applications, where a large file must be "compressed" in a secure manner before being encrypted with a private (secret) key under a public-key cryptosystem such as RSA."

6.1 MD5 Algorithm Structure



Step1 Append padding bits

The input message is "padded" so that its length (in bits) equals to 448 mod 512. Padding is performed, if the length of the message is already 448 mod 512. The input message is "padded" so that its length (in bits) equals to 448 mod 512. Padding is performed, if the length of the message is already 448 mod 512.

Padding is performed as follows: a single "1" bit is appended to the message, and then "0" bits are appended so that the length in bits of the padded message becomes congruent to 448 mod 512.The appending bits are atleast one bit and at most 512 bits

.Step2. Append length

A 64-bit representation of the message length is appended to the result of previous step. If the message length is greater than 2^64, only the low-order 64 bits will be used. The resulting message (after padding with bits and with b) has a length that is an exact multiple of 512 bits. The input message has length that is an exact multiple of 16 (32-bit) words.A 64-bit representation of the length of the message is appended to the result of previous step. If the message length is greater than 2^64, only the low-order 64 bits will be used.

The resulting message (after padding with bits and with b) has a length that is an exact multiple of 512 bits. The input message has the length that is an exact multiple of 16 (32-bit) words.

Step3. Initialize MD buffer

A four-word buffer (A, B, C, D) is used to compute the MD.A, B, C, D is a 32-bit register. These registers are used to the values in hexadecimal. The low-order bytes are arranged first.

word A: 01 23 45 67
word B: 89 ab cd ef
word C: fe dc ba 98
word D: 76 54 32 10

Step 4. Process message in 16-word blocks

Four functions will be defined such that each function takes an input of three 32-bit words and produces a 32-bit word output.

F (X, Y, Z) = XY or not (X) Z

G (X, Y, Z) = XZ or Y not (Z)

H (X, Y, Z) = X xor Y xor Z

I (X, Y, Z) = Y xor (X or not (Z))

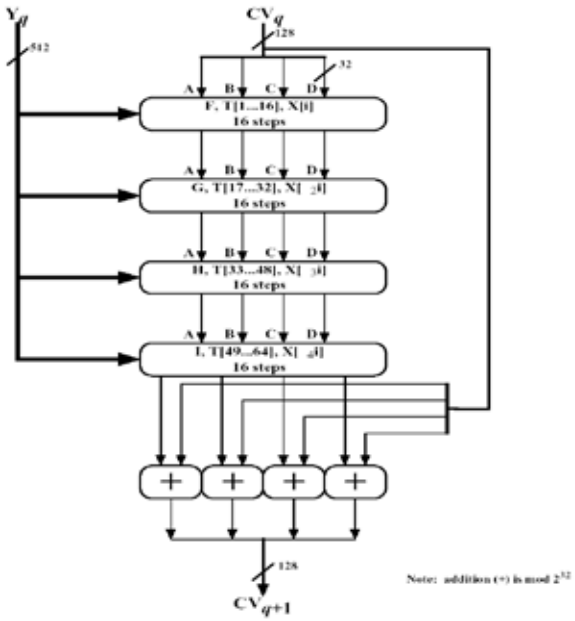


Figure 9.2 MD5 Processing of a Single 512-bit Block (MD5 Compression Function)

After processing of all 512 bit blocks, a 128 bit message digest is produced, which is a function of all the bits of your message.

The operations of the Functions F, G, H, I can be expressed as follows:

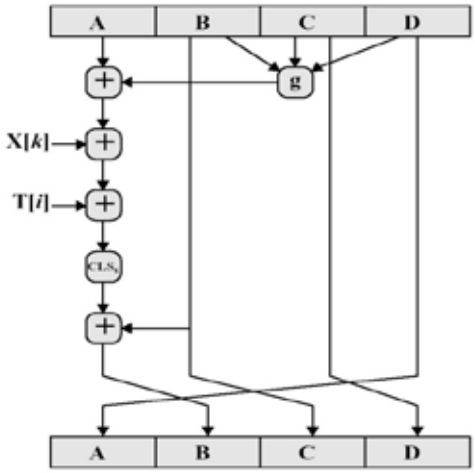


Figure 9.3 Elementary MD5 Operation (single step)

VII. CONCLUSION

DTN technologies are becoming successful solutions in military applications that allow wireless devices to communicate with each other and access the confidential information reliably by exploiting external storage nodes. CP-ABE is a scalable cryptographic solution to the access control and secure data retrieval issues. In this paper, we proposed an efficient and secure data retrieval method using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently. The inherent key escrow problem is resolved such that the confidentiality of the stored data is guaranteed even under the hostile environment where key authorities might be com-promised or not fully trusted. In addition, the fine-grained key revocation can be done for each attribute group. We demonstrate how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption-tolerant military network.

VIII. ACKNOWLEDGEMENT

First and foremost, we record our sincere thanks to Almighty GOD and our beloved parents who provided us this chance during our tenure in college. We are grateful to our college & **Dr. K. Mani, M.E, PhD**,our beloved principal. We are also thankful to **Mrs. M. Helda Mercy, M.E, PhD** Head of the Department of Information Technology for providing the necessary facilities during the execution of our project work. We also thank for her valuable suggestions, advice, guidance and constructive ideas in each and every step, which was indeed a great need towards the successful completion of the project.

This project would not have been a success without my Internal guide. So, I would extend my deep sense of gratitude to my Internal guide **Mrs. D. Karunkuzhali, Professor**, for the effort she took in guiding me in all the stages of completion of my project work.

REFERENCES

[1] J. Burgess, B. Gallagher, D. Jensen, and B. N. Levine, “Maxprop: Routing for vehicle-based disruption tolerant networks,” in Proc. IEEE INFOCOM, 2006, pp. 1–11.

[2] M. Chuah and P. Yang, “Node density-based adaptive routing scheme for disruption tolerant networks,” inProc. IEEE MILCOM, 2006, pp. 1–6.

[3] M.M.B.Tariq,M.Ammar,andE.Zequra,“Mesage ferry route de-sign for sparse ad hoc networks with mobile nodes,” inProc. ACM MobiHoc, 2006, pp. 37–48.

[4] S. Roy and M. Chuah, “Secure data retrieval based on ciphertext policy attribute-based encryption (CP-ABE) system for the DTNs,” Lehigh CSE Tech. Rep., 2009.

[5] M. Chuah and P. Yang, “Performance evaluation of content-based information retrieval schemes for DTNs,” inProc. IEEE MILCOM, 2007, pp. 1–7.

[6] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, “Plutus: Scalable securefile sharing on untrusted storage,” inProc. Conf. File Storage Technol., 2003, pp. 29–42.

[7] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, “Medi-ated ciphertext-policy attribute-based encryption and its application,” inProc. WISA, 2009, LNCS 5932, pp. 309–323.

[8] N. Chen, M. Gerla, D. Huang, and X. Hong, “Secure, selective group broadcast in vehicular networks using dynamic attribute based encryp-tion,” inProc. Ad Hoc Netw. Workshop, 2010, pp. 1–8.

[9] D.HuangandM.Verma,"ASPE:Attribute-based secure policy en-forcement in vehicular ad hoc networks,"Ad Hoc Netw., vol. 7, no. 8, pp. 1526–1535, 2009.

[10] A.Lewko and B.Waters, "Decentralizing attribute-based encryption," Cryptology ePrint Archive: Rep.2010/351, 2010.

[11] Sahai and B. Waters, "Fuzzy identity-based encryption," inProc. Eurocrypt, 2005, pp. 457–473.

[12] V.Goyal, O.Pandey, A.Sahai,and B. Waters, "Attribute-based en-cryption forfine-grained accesscontrol of encrypted data," inProc. ACM Conf. Comput. Commun. Security, 2006, pp. 89–98.

[13] J.Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," inProc. IEEE Symp. Security Privacy, 2007, pp. 321–334.

[14] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-based encryption with non-monotonic access structures," inProc. ACM Conf. Comput. Commun. Security, 2007, pp. 195–203.

[15] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," inProc. ASIACCS, 2010, pp. 261–270.

WI-MAX THROUGH ROF: A THEORETICAL STUDY AND SURVEY

Abhimanyu[1], Col. (Dr.) Suresh Kumar[2], Dr. Shelly Garg[3]

[1]*Research Scholar, UIET, MDU, Rohtak & Assistant Professor, Deptt. of ECE, JUS&T, Hisar (India)*

[2]*Assistant Professor, Deptt of ECE, UIET, MDU, Rohtak (India)*

[3]*Professor, IIET, Kinana, Jind. (India)*

ABSTRACT

Wireless technology has introduced high speed internet accessibility through wireless broadband. Radio over fiber; the integration of microwave and optical networks is the potential solution for reducing cost in terms of equipment, running finance and capacity enhancement in wireless communication systems. IEEE 802.16 Wi-MAX has emerged as a revolutionary wireless broadband access technique over past few years. This paper summarizes the advantages of incorporating RoF as a backhaul technology for providing Wi-MAX services. Various performance measures like data rate, attenuation, and dispersion errors have been studied and discussed in the paper for different types of fiber. Various features of Wi-MAX services offered by Bharat Sanchar Nigam Ltd. have also been summarized to develop better understanding and know practical implementation of the technique.

Key words: Radio over Fiber (ROF), Wi-MAX, Dispersion, Fiber Nonlinearities.

I. INTRODUCTION

As per the increasing demand for broadband services which leads to ever-growing data traffic volumes over these services. In addition to the high-speed, symmetric, and guaranteed bandwidth demands for future video services, the next-generation access networks are driving the needs for the convergence of wired and wireless services. RoF technology, the integration of microwave and optical networks as shown in figure 1, is an interesting and promising solution for increasing capacity and mobility as well as decreasing costs in the access network.

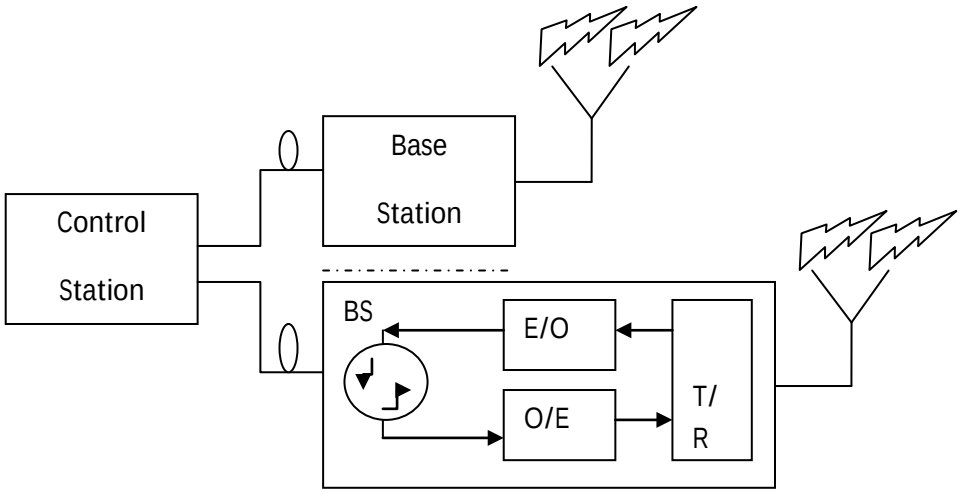


Figure1: General RoF System

The concept of RoF is to transport information over optical fiber by modulating the light with the radio signal. The modulation can be done directly with the radio signal or at an intermediate frequency. RoF technique has the potentiality to the backbone of the wireless access network. Such architecture can give several advantages, such as reduced complexity at the antenna site, radio carriers can be allocated dynamically to the different antenna sites , transparency and scalability [1]. To provide integrated broadband services, these systems will need to offer data transmission capacities well beyond the present-day standards of wireless systems. Wireless LAN offering up to 54 Mbps and operating at carrier frequencies around 2.4 and 5 GHz, and 3G mobile networks offering up to 2 Mbps and operating around 2 GHz, are some of today's main wireless standards. Optical wireless networking connectivity can typically be achieved using Radio Frequency (RF) or optical wireless approaches at the physical level. The RF spectrum is congested, and the provision of broadband services in new bands is increasingly more difficult. Optical wireless networking offers a vast unregulated bandwidth that can be exploited by mobile terminals within an indoor environment to set up high speed multimedia services. Optical signal transmission and detection offers immunity from fading and security at the physical level where the optical signal is typically contained within the indoor communication environment. The same communication equipment and wavelengths can be reused in other parts of a building, thus offering wavelength diversity [2].

II. ADVANTAGES

Due to availability of both wired and wireless facilities, RoF system offers following advantages:

(1) Low Attenuation Loss- Commercially available standard single mode fiber (SMFs) made from glass (silica) have attenuation losses below 0.2dB/km and 0.5dB/km

(2) Large Bandwidth- There are three main transmission windows, which offer low attenuation, namely the 850 nm, 1310 nm and 1550 nm wavelengths. For a standard SMF optical fiber, the combined bandwidth of the three windows is in the excess of 50 THz.

(3) Immunity to Radio Frequency Interference- This is so because signals are transmitted in the form of light through the fiber. Because of this immunity, fiber cables are preferred even for short connections at mm-waves.

(4) Reduced Power Consumption.

(5) Dynamic Resource Allocation- Since the switching, modulation, and other RF functions are performed at a centralized station, it is possible to allocate capacity dynamically.

(6) Millimeter Waves- Millimeter waves offer several benefits. Firstly, they provide high bandwidth due to the high frequency carriers. Secondly, due to high RF propagation losses in free space, the propagation distances of mm-waves are severely limited. This allows for well-defined small radio sizes (microcells and picocells), where considerable frequency reuse becomes possible so that services can be delivered simultaneously to a larger number of subscribers.

III. IEEE 802.16 WiMAX

Wi-MAX is one of the most widely used broadband technologies now a days in the world. WiMAX system

delivers broadband services in an economical way both to enterprise and residential customers. [3] WiMAX an alternative to wire technologies like DSL, T1/E1, cable modems is a wireless version based on Ethernet standards. More, WiMAX is an industry organization formed by leading equipment and component companies for compatibility and interoperability of wireless broadband access system confirms to IEEE 802.16. WiMAX operates similar to Wi-Fi but it provides greater distance coverage, high speed then Wi-Fi and can accommodate a large no of users. WiMAX can provide its services in an area difficult for wired connections to reach and also overcome the limitations the wired networks [4]. WiMAX formed in April 2001, operates in the frequency range of 10-66 GHz under IEEE 802.16 specifications, supports up to 40Mbps.

IV. FIBER NONLINEARITIES AND DISPERSION

Fiber Nonlinearities [5]: The optical nonlinearities considered are those that can give rise to gain or amplification, the conversion between wavelengths, the generation of new wavelengths or frequencies, the control of the temporal and spectral shape of pulses, and switching. They result from the interaction between several optical fields simultaneously present in the fiber and may also involve acoustic waves or molecular vibrations. Fiber nonlinearities can be distinguished in two different types

I) The nonlinearities that arise from scattering [Stimulated Brillouin Scattering (SBS) and Stimulated Raman Scattering (SRS).

II) The nonlinearities that arise from optically induced changes in the refractive index, and result either in phase modulation [Self-phase Modulation (SPM) and Cross phase Modulation (XPM)] or in the mixing of several waves and the generation of new frequencies [modulation instability (MI) and parametric processes, such as four wave mixing (FWM).

Kerr Effect: The refractive index n of many optical materials has a weak dependence on optical intensity.

$$n=n_0+n_2I$$

n_0= ordinary refractive index of the material

n_2=nonlinear index coefficient

So, this nonlinearity in the refractive index is known as Kerr nonlinearity. This nonlinearity produces a carrier induced phase modulation of the propagating signal, which is called Kerr effect.

Dispersion Effects [6]: Dispersion is a phenomenon of spreading of light pulse as it travels down the fiber. As a result of this Inter Symbol Interference (ISI) occurs, hence performance is adversely affected.

1) Intermodal Dispersion: It appears only in multimode fibers. It is a result of each mode having a different value of group velocity at a single frequency. This mechanism can be eliminated by single mode operation, but is important in multimode fibers.

2) Intramodal Dispersion: This effect takes place within a single mode. This spreading arises from the finite spectral emission width of an optical source.

(a) Material Dispersion: It arises due to the variations of the refractive index of the material as a function of wavelength[7]. Material dispersion is also referred as chromatic dispersion.

(b) Waveguide dispersion: It causes pulse spreading because only part of the optical power propagation along a fiber is confined to core. A fraction of the light power propagating in the cladding travels faster than the light

confined to the core since the index is lower in the cladding. Waveguide dispersion can be ignored in multimode fiber but its effect is significant in single mode fiber.

V. SURVEY:-WI-MAX THROUGH ROF

In India, WebSky created a joint venture with World-Wide Wireless India (WWWI) to design, build and run a network that could address 75m people. WebSky started providing the funding and constructed the system while WWWI contributed its licensed frequencies in 3.5GHz spectrum, which covered nine large cities, including Mumbai (Bombay), Delhi, Calcutta, Chennai (Madras), Bangalore and Hyderabad. The first build-out occured in the city of Ludhiana, in Punjab.

Also in India, telecom giant **Bharat Sanchar Nigam Limited (BSNL)** announced plans to roll out Wi-MAX services in 10 major cities, including Hyderabad, Pune, Ahemdabad and Bangalore in 2005. The installation and commissioning of Wi-MAX certified equipment of BSNL is currently available across many cities in India. On trial basis BSNL deployed Cambridge Broadband's Vectastar Equipment in Gurgoan near Delhi. Its consumer premises equipments (CPEs) are multi frequency and multi sector. Vectastar's technology product is used for both access and transmission with the network combining IP based access services with the backhaul of traffic from GSM, 3G, and Wi-MAX base stations.

French telecom major Alcatel joined hands in an agreement with the **Centre for Development of Telematics (CDoT)** to set up a global research and development centre in India for broadband wireless products. Alcatel believes that broadband wireless and particularly Wi-MAX is appropriate technology for India keeping in mind the requirements of the rural sector.

5.1 Types of Optical fiber Deployed

The International Telecommunication Union (ITU-T), which is a global standardization body for telecommunication systems and vendors, has standardized various fiber types. These include the Non dispersion-shifted fiber (G.652), dispersion-shifted fiber (G.653), 1550-nm loss-minimized fiber (G.654), and NZDSF (G.655).

1. Non dispersion-Shifted Fiber (ITU-T G.652)- The ITU-T G.652 fiber is also known as standard SMF and is the most commonly deployed fiber[8]. It has a zero-dispersion wavelength at 1310 nm and can also operate in the 1550-nm band, but it is not optimized for this region. The typical chromatic dispersion at 1550 nm is high at 17 ps/nm-km. Dispersion compensation must be employed for high-bit-rate applications. The attenuation parameter for G.652 fiber is typically 0.2 dB/km at 1550 nm, and the PMD parameter is less than 0.1 ps/ km.

2. Low Water Peak Nondispersion-Shifted Fiber (ITU-T G.652.C)-The legacy ITU-T G.652 standard SMFs are not optimized for WDM applications due to the high attenuation around the water peak region. ITU G.652.C-compliant fibers offer extremely low attenuation around the OH peaks. The G.652.C fiber is optimized for networks where transmission occurs across a broad range of wavelengths from 1285 nm to 1625 nm. Although G.652.C-compliant fibers offer excellent capabilities for shorter, unamplified metro and access

networks, they do not fully address the needs for 1550-nm transmission. The attenuation parameter for G.652 fiber is typically 0.2 dB/km at 1550 nm, and the PMD parameter is less than 0.1 ps/ km.

Based on optical power loss of fiber, spectrum ranges have been characterized for compatibility purposes with light sources, receivers, and optical components, including the fiber. Thus, the low-loss spectrum for single-mode fiber has been subdivided into smaller regions [9]. The S-band (short-wavelength or second window) is defined in the range 1280-1350 nm. The C-band (conventional or third window) is defined in the range 1528-1565 nm. This is also subdivided into the "blue band" (1528-1545 nm) and the "red band" (1545-1561 nm). The L-band (long-wavelength or fourth window) is defined in the range of 1561-1620 nm. The "new band" (or fifth window) is defined in the range of 1350-1450 nm. The S- and C-band ranges have found applications in WDM metropolitan networks. The C- and L-band ranges have found applications in ultra-high-speed (10-40 Gb/s) WDM networks [10]. The L-band takes advantage of the dispersion compensating fiber that effectively extends the C-band range to 1600 nm, thus doubling the number of wavelengths better suited to DWDM applications.

Sr. No.	Type	Wavelength Coverage	Dispersion	Application
1	6.652A	1310 nm , 1550 nm	0.5ps/km-nm	Supports 10Gbps upto 40 kms
2	6.652B	1310nm , 1550 nm, 1625 nm	0.2ps/km-nm	Supports 10Gbps upto 40 kms, attenuation is max at 1625 nm
3	6.652C	1310 nm , 1550 nm	0.5ps/km-nm	Similar to 6.652A, suitable for CWDM
4	6.652D	1310nm , 1550 nm, 1625 nm	0.2ps/km-nm	Similar to 6.652B, suitable for CWDM

ITU_T G.652 defines the different standards of single-mode optical fibre cable and its characteristics. This recommendation describes the geometrical and transmission attributes of single-mode optical fibre and cable with chromatic dispersion and cut-off wavelength that are not shifted from the 1310 nm wavelength region [11]. ITU_T G.653 describes the characteristics of a dispersion shifted single mode optical fibre cable. ITU_T G.654 describes the geometrical, mechanical and transmission attributes of a single mode optical fibre and cable which has the zero-dispersion wavelength around 1300 nm wavelength, and which is loss-minimized and cut-off wavelength shifted at around the 1550 nm wavelength region [12]. ITU_T G.655 describes the geometrical, mechanical, and transmission attributes of a single-mode optical fibre which has the absolute value of the chromatic dispersion coefficient greater than some non-zero value throughout the wavelength range from 1530 nm to 1565 nm [13]. This dispersion reduces the growth of non-linear effects which are particularly deleterious in dense wavelength division multiplexing systems. ITU-T G.656 describes the geometrical, mechanical, and transmission attributes of a single-mode optical fibre which has the positive value of the chromatic dispersion coefficient greater than some non zero value throughout the wavelength range of anticipated use 1460-1625 nm. This dispersion reduces the growth of non-linear effects which are particularly deleterious in dense wavelength division multiplexing systems. ITU_T G.657 to support this optimization by recommending strongly improved bending performance compared with the existing ITU-T G.652 single-mode fibre and cables. This is done by means of two categories of single-mode fibres, one of which, category A, is fully compliant with the ITU-T G.652 single mode fibres and can be deployed throughout the access network [14]. The other, category B, is not

necessarily compliant with recommendation ITU-T G.652 but is capable of low values of macro bending losses at very low bend radii and is intended for use inside buildings or near buildings. Attenuation Summary for various kinds of fibers-

Sr. No.	Fiber Type	Bending Radius	Attenuation
1	G 652	37.5 mm	0.5 dB
2	G 657 A1	15 mm	0.25 dB
3	G 657 A2	15 mm	0.03 dB
4	G 657 B2	15 mm	0.03 dB
5	G 657 B3	10 mm	0.03 dB

Wi-MAX service provided by BSNL offers following features and specifications-

Standard Range	50 kms
Shared data rate(Wi-MAX) (Wi-MAX release 2)	70 Mbps 365 Mbps for Mobile user, 1Gbps for fixed user
Peak downlink rate	365 Mbps
Peak Uplink rate	376 Mbps
Standard Cell coverage	8,000 square km
Frequency Band used (non line of sight) (Line of sight)	2 GHz to 11 GHz 10GHz to 66 GHz (both licensed and unlicensed)
Modulation formats	OFDM/OFDMA,QPSK, 16 QAM, Scalable OFDMA
Protocols followed	Logical Link Controller(standardized by IEEE 802.2) MAC (Media Access Control) layer that supports multiple physical layer
Peak Data Rate	75 Mbps(20 Mhz channel),18 Mbps(5 Mhz channel)
Standard antenna type	4*4 MIMO antenna
No of Sectors	3
Traffic engaged peak %	70 %

No. of T1 lines(1.544Mbps)	14
Average User Throughput	1-3 Mbps
Range Outdoor (Avg Cell)	2–10 kms
Channel BW	Scalable 1.5–20MHz
High end services offered	Real time multimedia and Voice over IP
Mobility Limit	Max of 60 km/h to maintain optimum throughput performance
Interference Source	2-3 GHz Band, only in non line of sight (Majorly Microwave Ovens)
Connectivity efficiency	Approx 60 business with T1-type connectivity and hundreds of homes with DSL-type connectivity

VI. APPLICATIONS

RoF is used in many areas such as following

(1) Cellular Networks
(2) Satellite Communications
(3) Video Distribution Systems
(4) Mobile Broadband Services
(5) Wireless LANs
(6) Vehicle Communication and Control

VII. CONCLUSION

In this paper we have discussed the role of RoF network as the backhaul concept for Wi-MAX service. The presented study helps to develop a better understanding of RoF technology. It is observed that BSNL make use of Non dispersion shifted fiber for transportation of radio signals. Though the losses occurring are very low as compared to dedicated wireless channel, yet performance can be improved by using dispersion compensated fiber. Quality of service will be enhanced once dispersion compensated fibers are installed for the purpose.

ACKNOWLEDGEMENT:- The data for the survey was collected from BSNL Advance level Telecom Training Centre(ALTTC),Ghaziabad.

REFERENCES

[1] Mohammad Shaifur Rahman, Jung Hyun Lee, "Radio over Fiber as a Cost Effective Technology for Transmission of WiMAX Signals", World Academy of Science, Engineering and Technology, pp 424-429, 2009.

[2] D. Opati, "Radio over Fiber Technology for Wireless Access" Ericsson Nikola Tesla, 2007.

[3] Riegel M, "Ethernet services over mobile Wimax" IEEE journals and magzines,Vol.46, 2008.

[4] M.Garcia Larrode and AMJ.Koonen, "Towards a reliable RoF infrastructure for broadband wireless access".IEEE proceedings symposium, 2006.

[5] Gerd Keiser,"Optical Fiber Communication", TMH Education pvt. ltd, 2011.

[6] G. P. Agrawal, "Fiber-Optic Communication Systems". New York: Wiley, 1997.

[7] Maria C.R. Medeiros, Manoj P. Thakur, Paula Laurêncio, and John E. Mitchell," Transmission limitations of wimax over fibre transmission employing optical up-conversion schemes" IEEE International conference, ICTON 2012

[8] Xiaoan HUANG, Ryuji KOHNO," 60-GHz ultra-wideband radio-over-fiber system employing SCM/WDM" IEEE International Conference on Ultra-Wideband (ICUWB),PP 85-90, 2013.

[9] Jhon James Granada Torres, Gloria Margarita Varón Durán , Neil Guerrero González ," Chromatic dispersion effects in a Radio over Fiber System with PSK modulation and coherent detection" " IEEE International conference, 2012.

[10] Natalia Arboleda-Alzate, Ferney Amaya-Fernández," Dispersion and nonlinear effects analysis for intensity and phase modulated optical signals" IEEE international conference 2013.

[11] S.Sugumarani, P.Arulmozhivarman," Effect of chromatic dispersion on four-wave mixing in WDM systems and its suppression" IEEE international conference 2013.

[12] Kohei Kimura, Satoshi Ebisawa and Joji Maeda," Evidence of modulation-dependent fading of signal amplitude due to fiber dispersion in Radio-over-Fiber transmission" IEEE international conference 2013.

[13] M. Droques, A. Kudlinski, G. Bouwmans, G. Martinelli, A. Mussot, A. Armaroli, F. Biancalana," Modulational instability phase-matched by higher-order dispersion terms in dispersion-oscillating optical fibers" IEEE international conference 2013.

[14] Ken-ichi Kitayama, Akihiro Maruta, Yuki Yoshida," Digital coherent technology for optical fiber and radio-over-fiber transmission systems" Journal of Lightwave Technology, PP 1-10, 2014.