HIGH PERFORMANCE COMPUTING AND VIRTUAL NETWORKING IN THE AREA OF BIOMETRICS

Jadala Vijaya, Chandra, Roop Singh Thakur, Mahesh Kumar Thota
Asst Profs., Deptt. of Computer Science and Engineering, Warangal Institute of Technology and Science, Oorugonda (V), Atmakur (M), Warangal, A.P., India.

ABSTRACT

Virtual networking is an important step in the evolution of data networks. The key idea of network virtualization is to build a diversified Internet to support a variety of network services and architectures through a shared substrate. Pattern Recognition is the process of establishing a close match between some new stimulus and previously stored stimulus patterns. This Paper describes the necessity of biometric systems for Network Data and Information Security, Role of virtual LAN's in supporting the error free security system. An Attempt is made to use the finger print of an individual for accessing the secured network. On an experimental basis, a biometric attendance system of staff and students of college is done to test and validate the working of the designed algorithm using Cellular Neural Network. Designing of algorithm using Cellular Neural Network to carry out the front end software, Backend software to implement in the Virtual network and implemented on digital Signal Processor (DSP). Ideal finger implemented on Digital Signal Processor (DSP). Ideal finger print data was considered for analysis without any error.

KEYWORDS: *Biometric, Cellular Neural Network, Digital Signal Processor, Virtual LAN.*

I. INTRODUCTION

Human finger prints are unique to each person and can be regarded as a sort of signature, certifying the person's identity. Because no two finger-prints are exactly alive, the process of identifying a fingerprint involves comparing the ridges and impressions on one fingerprint to those another. This first involves capturing the likeness of the fingerprint, either through use of a fingerprint scanner (Biometric Reader) which takes the digital picture of a live fingerprint. A virtual LAN is used to connect different Biometric Readers and the Server.

A Practical approach is taken to connect Biometric Reader and Server for the Students and Staff Attendance, The matching of fingerprints is accomplished by using Neural Networks(NN), Cellular Neural Networks(CNN) and the NN and CNN paradigms use repetitive multiplication and Addition (MAC), the Digital Signal Processor Architecture Super Harvard Architecture(SHARK) is ideal for MAC operations.

A High Performance Computing HN36 Biometric machine is taken and It is connected to the Virtual Local Area Network of Internet Protocol Address as Server, we taken Microsoft SQL Server to activate the biometric at the Back End Access to the reports from one computer to another computer in the network that increases performance, security, and the resources required Biometric Devices, Captures the Finger Print and Image will be processed using Cellular Neural Network and Pattern Matching Algorithm with the help of Hash Functions. The analysis of fingerprints for matching purposes generally requires the comparison of several features of the print pattern. In this network, here set of finger prints are captured as training data set in the files. Once the finger print is captured it automatically monitors the files. Where the training data set is stored. These stored files are having large bulk of training data sets. So we are using pattern matching. The pixel value equivalent of the finger prints and these files are stored. Pattern matching is carried out to find out the convergence of the fingerprint.

II. BIOMETRIC READER

A Biometric Reader HN36 is taken which is portable and having high capacity of 3000 data storage capacity and 80000 transaction storage capacity, This finger print reader can interact with external devices and this readers have all the necessary communication standards which includes RS232, RSS485, TCP/IP and USB.

Further, A real time clock and a graphical LCD of 128/64 assist this Reader to perform more efficiently. It works best in an operating temperature range of 0 to 45 degrees and can withstand humidity levels from 20% to 80%, it equipped with a rechargeable battery which provides un interrupted power back up of about 2 hours, Their high matching speed ensures that they can match 1000 fingerprints in less than 2 seconds which effectively means that they have an identification time of less than 1 second. It is a Standalone connecter but at this practical approach we connected it to the Virtual Local Area Network which is connected with 12 Biometric Readers to the Server. It supports both the finger prints and password for the attendance, it having high speed scratch proof sensor 500 DPI (Digital Processing Image)

A sensor is a device that measures or detects a real-world condition, such as motion, heat or light and converts the condition into an analog or digital representation.

Fig 2.1 HN-36 Biometric Machine

Fig2.2 Fingerprint

III. VIRTUAL LOCAL AREA NETWORK

The actual or physical LAN may be considered as a group or combination of computers connected by some network device such as hub or switch. It forms a single broadcast domain, that is, if a machine wants to broadcast a message then the message is received by all other machines in the LAN. Now-a-days

LAN can be configured logically with the help of networking device software. With this, k number of machines physically connected to a switch may be grouped into ‘n’ number of logical LANs. This is known as Virtual Local Area Network (VLAN).

As the Strength of students and staff is more in the college and the requirement of the Biometric Readers will be increase year by year, and the computer systems which are in the college will be increased by year by year going for virtual LAN is much better than the LAN. Sometimes it is required to reflect the organizational structure of a college rather than its physical layout, Physical LAN reflects only the physical layout of a college, rather than its logical layout. VLAN only can do this Job. VLAN reduces the migration cost of moving a station from one LAN to another, In a Physical LAN if a station is to move from one place or another keeping it in the same previous LAN, then the System Administrator has to physically reconfigure the wiring of the switch but this is done very easily in VLAN. The network Administrator will have to configure the switch with software without any physical labour. VLAN gives the facility of creating virtual workgroup without affecting the physical layout of the LAN. The members of a workgroup can exchange there views very easily as VLAN creates logical workgroup, broad caste in a group means distribution of message with in a single logical LAN rather than physical LAN. So VLAN provides n number of logical broadcast domain this provides security to the system.

3.1 Basic VLAN Architecture VLAN can be implemented in VLAN cable switch, no other special device is required at all. The switch contains built in software which the network administrator has to configure to form the VLAN. He has to form the workgroups give membership to them monitor them, if required reconfigure them.

3.2 Membership Different characteristics of Network are used for Including a station in a VLAN.

3.2.1 Port Number Port Number of the switch may be used as a membership parameter for example stations attached to port number **1,4,5,8 and 10** are in VLAN 1 stations attached to port number **2, 3,9,16** are in VLAN 2 and so on.., here VLAN 1 Station is of the Clients (Computers) and VLAN 2 Station is of the DSP(Biometric Readers).

3.2.2 MAC ADDRESS: 48 bit MAC address may also be used as a Membership parameter for example stations with MAC Address **AC23-E234 : BC10** And **FEA1 : CC43 : 100 C** may be included in VLAN1 and so on.

3.2.3 IP ADDRESS: 32-bit IP Address may also be used for Configuring VLAN for Example stations with IP Address **192.168.1.10** and **192.168.1.14** may be included in VLAN 1, Stations with IP Address **192.168.1.100** and **192.168.1.12** may be included in VLAN2.

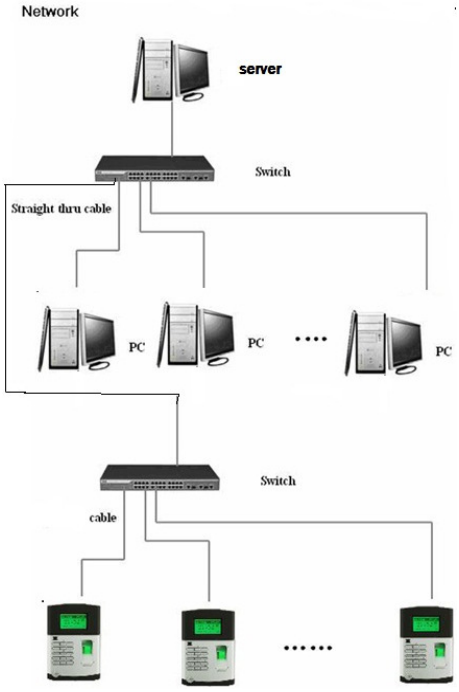

Fig 3.1 Virtual Local Area Network

IV. SOFTWARE FOR BIOMETRIC READER

Time Tracking Software is a category of computer software that allows its users to record time spent on tasks. It is accounting software used to maintain timesheets. Fingerprint biometric time attendance system and a perfect add-on to current human resource management helping to automate data collection and process timesheets. The Software helps to prepare attendance reports faster for organizations of any size, Improve overall workforce punctuality. Queue up faster with one touch login. By using this system the students and staff of the college can give the attendance 99.9% accurately, No password to remember, no cards to hold, no buddy-punching, just by using users own finger. By using this method we found the management of human resource is improved, and it gives a full overview of workforce time attendance in seconds. This software can generate the reports according to the user's requirements and the reports can also export to MS-Excel.

V. MICROSOFT SQL SERVER

Microsoft SQL Server is used to activate the biometric at the Back End Access to the reports from one computer to another computer in the network. It is used to Secure information so nobody can manipulate the data except

Appropriate person that is System Administrator and user can export data at LAN or Virtual LAN or can create custom reports or applications (like a web report). In all these scenarios, the best way to perform the installation is in two separate machines: One holding the database (Server), and the other one holding the Punch Clock (Client).

VI. BLOCK DIAGRAM OF A BIOMETRIC SYSTEM

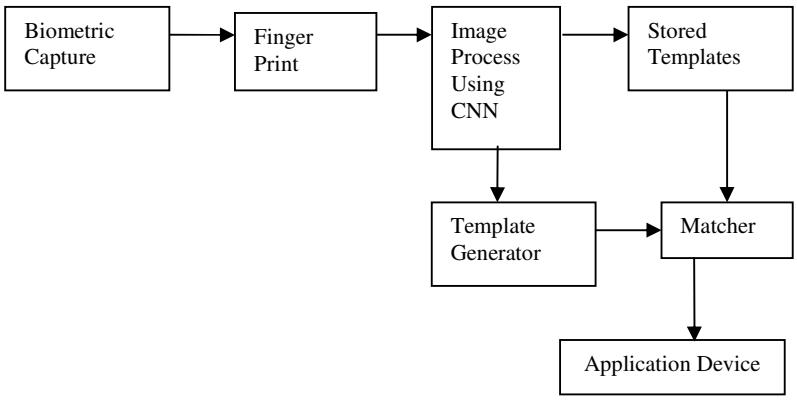

Fig 6.1 Block Diagram of a Biometric System

Biometric Devices, Captures the Finger Print and Image will be processed using Cellular Neural Network, the above block diagram shows the extraction and identification process and it checks the present template matches with the stored template or not.

VII. CONCEPT OF FINGERPRINT SDK

A fingerprint SDK is a software toolkit that allows the integration of biometric fingerprint recognition into various applications. Typically a Windows-based SDK will utilize either a DLL or ActiveX (COM) control to interface with the integrated application. By referencing these DLL or COM objects, developers are able to utilize the fingerprint functionality from within a desired application.

VIII. ALGORITHM APPROACH

8.1. Methodology

Cellular Neural Network (CNN) is a Data to Information processing paradigm which is inspired by the way of human brain system. Here in our mathematical models for CNN are in differential equations form as a data for information processing has variables which can be represented in differential equation form and this n^{th} order differential equations, which makes processing the proposal MAC method Ideal.

8.1.1. Algorithm A standard CNN differential equation is shown in a equation 1, which is a simplify and standard differential equations

$$x_{ij} = -x_{ij} + \sum_{k=-r}^{r} \sum_{l=-r}^{r} a_{kl}\, y_{i+k,\,j+l} + \sum_{k=-r}^{r} \sum_{l=-r}^{r} b_{kl} u_{i+k\,,\,j+l} + z$$

Where

X_{ij} is the first derivative of $X_{ij,}$ a and b are the elements of the space invariant template matrices. Solving the standard differential equations, x= (h : w)

Where x = x(t)

$X(0) = x_0$

This can be solved by Standard Numerical Integration Methods. The simplest one is the forward Eulu Formula, which calculates the value of x (t + Δt) from x(t) ,Δt be the time step.

$x(t + \Delta t) = x(t) + \Delta t x(t) = x(t) + \Delta t h(x(t):(w))$

This equation used for calculating the time of CNN dynamics range. So we are finding the group of finger print by using Eulurs Formula of above equation. Every time step is calculated to find the pattern of finger print.

Fig 8.1 Finger Print

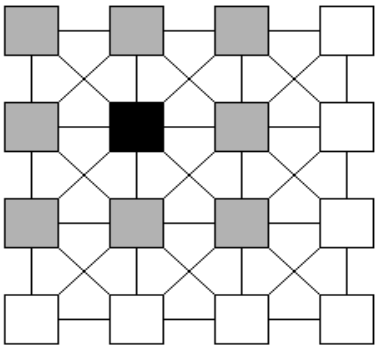

Fig 8.2 Cellular Neural Networks

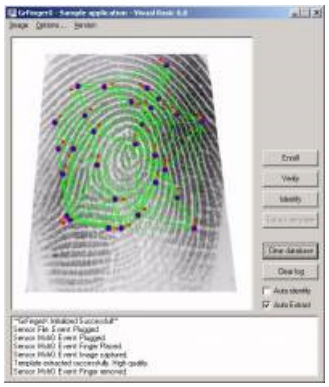

Fig 8.3 Finger Print in Time Track Software

In this figure we have used two dimensionally fully connected CNN with competitive learning method for training. In competitive learning we have used both feed-forward neural network and feedback neural network. so that once finger print is going to find in training dataset.

It will take some synaptic weights which were given in training data set and match with old weights which were given by user new weights. This weights and inputs are calculated in MAC form(matrices multiplication and addition).so that this were calculated by pixels form such as address bus and data bus and it will act as row and column. It is associated by the form of cell of pixels C(6,8),C(4,9) so on. These are the sample training data sets. Every cell is interconnected between cellular neural networks and their neighbor cells are also connected. Actually it is necessary to capture the cells of the training data sets, so if it is required the cell is connected to each other on demanded process. Because if all cells are connected then there is a problem of CNN dynamics range. Then there is only one winner neuron. In the above figure consider an MXN cells arranged in M rows and N columns. We denote the cell on the ith and the jth column as C(i,j),as in figure. Generic processors use von Neumann architecture, where in the data bus and address bus are multiplexed. This hampers the

processing speed for repetitive processes like the one represented in equation 1. However, this type of architecture gives the advantage of storing the program and data on the same memory. But these types of processors fail for MAC type of processing. DSPs are implemented using SHARK where in the data bus and address bus are separate and the stored program and stored data are separate but interlinked. This type of architecture is highly advanced as the prior architecture lacked the facility of interlinking of stored program and stored data on different memory hence making processing relatively slow, when compared to SHARK architecture , but fast when compared to von Neumann architecture as it had different buses for address bus and data bus. Hence SHARK architecture is ideal for repetitive tasks like MAC. The DSP used here for processing i.e.., computing the distances or weights after repetitive feed forward training is of fixed point origin, the software developed for DSP was written in high level language and later converted to assembly level language and finally to machine level language.

IX. ANALYSIS AND USABILITY

The analysis of fingerprints for matching purposes generally requires the comparison of several features of the print pattern. These include patterns, which are aggregate characteristics of ridges, and minutia points, which are unique features found within the patterns. It is also necessary to know the structure and properties of human skin in order to successfully employ some of the imaging technologies.
In figure 9.1 we show the biometric finger print implemented in capturing the finger of human being. A set of finger prints are captured, which are given access
The fingerprint is composed of various “ridges” and “valleys” which form the basis for the loops, arches, and swirls that one can easily see on his/her fingertip. The ridges and valleys contain different kinds of breaks and discontinuities. These are called “minutiae”, and it is from these “minutiae” that the unique features are located and determined. There are two types of “minutiae”:

- Ridge endings (the location where the ridge actually ends)
- Bifurcations (the location where a single ridge becomes two ridges)

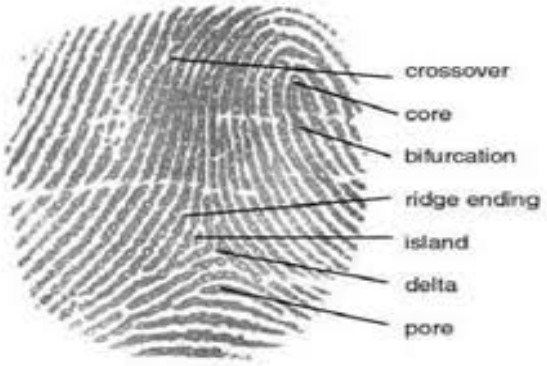

Fig : 9.1 Basic patterns of fingerprint

Template Creation Based upon the unique features found in the “minutiae”. The location, position, as well as the type and quality of the “minutiae” are factors taken into consideration in the template creation stage. Each type of fingerprint recognition technology has its own set of algorithms for template creation and matching.

Template Matching The system will either attempt to verify or identify a individual, by comparing the enrolled template against the verification template.

Biometrics growth and advantages The biometrics is experiencing fast development across the world because

1. Evolutions and rapid expansion of Information technology and web which claims for secure access control and secure data transfer.
2. Terrorism has put a lot of threat to Governments, which has raised the demand for accurate identification of individuals.

The three basic patterns of fingerprint ridges are the arch, loop, and whorl. An arch is a pattern where the ridges enter from one side of the finger, rise in the center forming an arc, and then exit the other side of the finger. The loop is a pattern where the ridges enter from one side of a finger, form a curve, and tend to exit from the same side they enter. In the whorl pattern, ridges form circularly around a central point on the finger. Scientists have found that family members often share the same general fingerprint patterns, leading to the belief that these patterns are inherited.

Table :1 Figure print data by Class

period	Finger Print Type		
	Arch	Loop	Whorl
1	6	9	8
2	6	7	6
3	5	6	7
4	10	5	10
5	9	6	7

X. COMPUTATIONAL BASIS

In this network, here set of finger prints are captured as training data set in the files. Once the finger print is captured it automatically monitors the files. Where the training data set is stored.

These stored files are having large bulk of training data sets. So we are using pattern matching. The pixel value equivalent of the finger prints and these files are stored. Pattern matching is carried out to find out the convergence of the fingerprint. Maximum convergence will occur for a non pattern matching algorithm. During pattern matching after training of CNN, changes in the trained CNN.Pixel value equivalent of the pattern when compared yield minor changes in the actual value which is trained in CNN. Higher number of learning epochs in training process also leads to redundancy in trained CNN. Comparison of pixel data, which is repetitive in nature, can increase the speed of processing as MAC(matrices of multiplication and addition) architecture specializes in increasing the speed of identical data types. Pixel values, if exceeding a certain limit, can be averaged using pixel averaging technique to remove the redundancy in values. The repetition of pixel values calculation is absolute as it decreases the speed of recognition. Hence, pixel averaging technique processing is improved in terms of speed of convergence and improvement in processing ability. Equivalent pixel values are stored and processed with freedom of analysis for testing after the training process is complete, inherent noise addition is possible during storage and retrieval of data. To overcome this problem, reduction algorithms can be used. However, in this work, data without any noise (i.e.. ideal data) is considered for evaluation of results. Trials can be carried out for noise inclusion by changing the pixel values in the stored file. These will, however, be unpredictable noise inclusion and cannot be incorporated to any actual noise. Actual noise data can be a cut in the thumb, peeling of skin etc…, of the authentic user. In pattern matching the trained data is stored in form of patterns. So in this paper we propose “finger printing” to preprocess the input string. So we are taking three basic patterns of finger print ridges are the archs, loops, and whorl. Suppose we are trying to find a pattern string ‘p’ in a long document D. hash the pattern ‘p’ into say a 16bit value. Now run through the file, hashing each set of |p| consecutive characters into a 16bit value. If we ever get a match for a pattern, we can check to see if it corresponds an actual pattern match (in the case we want to double check and not report any false matches!) otherwise we can just move on. We can use more than 16-bits, too; we would like to use enough bits so, that we will obtain few false matches.this scheme is efficient as long as hashing is efficient. Of course hashing can be very expensive operation, so in order for this approach to work, we need to be able to hash quickly on average. In fact, a simple hashing technique allows us to do so in constant time for operation! The easiest way to picture the process is to think of the file as a sequence of digits, and the pattern as a number. Then we move a pointer in the file one character at a time, seeing if the next |P| digits give us a number equal to the

number corresponding to the pattern. Each time we read a character in the file, the number we are looking at changes is a natural way; the left most digit 'a' is removed and the new right most bit 'b' is inserted. Hence ,we update an old number 'N' and obtain a new number N□ by computing

$$N□ = 10.(N – 10^{|P|-1}.a)+b$$

When dealing with a string, we will be reading characters (bytes) instead of numbers. Also, we will not want to keep the whole pattern as a number. If the pattern is large then the corresponding number may be too large to do effective comparison. Instead, we hash all the numbers down into say 16 bits, by reducing they modulo some appropriate time p. We then do all the mathematics (multiplication, addition) |P|

$$N□= [10.(N – 10^{|P|-1}.a)+b] \bmod P$$

All operations mod P can be made quite efficient, so, each new hash value takes only constant time to compute! The idea is that the hash of the pattern creates an almost unique identifier of the pattern-like a finger print. If we ever find two fingers prints that match, we have a good reason to expect that they must come in the same pattern. Ofcourse, unlike real finger prints, hashing based finger prints do not actually uniquely identify a pattern, we will need to check for false matches, but since false matches should be rare, the algorithm is very efficient.

A natural approach is to choose the prime p randomly. This way, nobody can set up a bad pattern and document in advance, since they are not sure what prime we will choose.

P=17935

P=251

P mod p =114

6386179357342…….

63861 mod p = 107

38617 mod p = 214

86179 mod p = 86

61793 mod p = 47

17935 mod p = 114

79357 mod p = 41

93573 mod p = 201

35734 mod p = 92

57342 mod p = 114

This pattern P is a five digit number. Note successive calculations take constant time:

38617|P|=(63861 mod p) - (60000 mod p)).10+7 mod p. also note that a false matches are possible (but unlikely): 57432=17935 mod p.

Let us make this a bit more rigorous Π(x) represents the number of primes that are less than or equal to x. it will be helpful to use the following fact.

Fact: $\frac{x}{\ln x} \le \prod(x) \le 1.26\frac{x}{\ln x}$

Consider any point in the algorithm, where the pattern and document do not match. if our pattern has length |P|, then at that point we are comparing two numbers that are each less than 10^|P|.what is the probability that a random prime divides this difference? That is, what is the probability that for random prime we choose, the two numbers corresponding to the pattern and the current |P| digits in the document are equal modulo P.

First note that there are at most ---------- distinct primes that divide the differences, since the difference is at most 10^|P|(in absolute value),an each distant prime divisor is at least 2.hence,if we choose our prime randomly from all primes upto Z. the probability we have a false match approach is at most

$$\frac{\log_2 10^{|p|}}{\prod(Z)}$$

Now, the probability that we have a false match anywhere is at most |D| times the probability that we have a false match in any single location, by the union bound. Hence the probability that we have a false match anywhere is at most

$$\frac{|D|\log_2 10^{|p|}}{\prod(Z)}$$

XI. EXPERIMENTAL RESULTS AND ANALYSIS

Regardless of dip water of wet finger, and dry finger, and dip mud, and oil, and dust, dirty finger are can validation by, can adaptation any bad of natural environment and weather. In the Experiment we got 97.9 % success rate.

XII. CONCLUSION

It can be concluded that convergence is faster and more accurate using the above technique. Fingerprint sensors are best for devices such as cell phones, USB flash drives, notebook computers and other applications where price, size, cost and low power are key requirements. Fingerprint biometric systems are also used for law enforcement, background searches to screen job applicants, healthcare and welfare. It is also the best method for the attendance systems in colleges, universities and schools. It is also used in Factories, Industries and Companies for the Employee attendance and for the Pay roll preparation based on the attendance. The software also used for the taxation and other deduction methods used in established employee payroll system. DSP used for implementing the CNN gives a higher degree of convergence. Increase in the number of iterations gives better convergence and accurate results in matching the biometric fingerprints. And this technique is entirely new and different from the conventional fingerprint technique.

REFERENCES

[1]. Kou-Yuan Huang and Yi-Hsian Chao (2004), "Seismic Pattern Recognition Using Neural Network and Time Automation", in Proceedings of IEEE Geo science and Remote Sensing Symposium. Vol. 5, September.
[2]. Object Recognition Using Cellular Neural Networks on Digital Signal Processors for Network Security, The ICFAI University Journal of Information Technology, vol. v, No 1. 2009.
[3].Simon Hay kin, "Neural Networks A Comprehensive Foundation" (2008), Pearson Education.
[4] IEEE 802.16 WG,"IEEE Standard for Local and Metropolitan Area Network Part 16: Air Interface for Fixed Broadband Wireless Access Systems" IEEE Std 802.16-2004 p.1 - p.857
[5] IEEE 802.16WG, "IEEE standard for local and metropolitan area networks part 16: Air interface for fixed and mobile broadband wireless access systems, Amendment 2," IEEE 802.16 Standard,
December 2005.
[6] Jianhua He, Kun Yang and Ken Guild"A Dynamic Bandwidth Reservation Scheme for Hybrid IEEE 802.16 Wireless Networks" ICC'08 p.2571-2575.
[7] Kamal Gakhar, Mounir Achir and Annie Gravey,"Dynamic resource reservation in IEEE 802.16 broadband wireless networks", IWQoS, 2006. P.140-148

Authors

Jadala Vijaya Chandra is a Post Graduate in Master of Computer Applications from Madurai Kamaraj University, Madurai, worked in Ethiopia and Qatar, visited Kenya, Dubai and Saudi Arabia, having Teaching Experience of 10 years and Interested areas are Networks and Data Security .Published a Research paper on "DATA SECURITY PRIVACY POLICIES AND PROCEDURES IN INTERNET USAGE" in the international at Omar el-mukhtar university albeida, Libya. Member of **IACSIT** and At present working as Asst Professors, Department of Computer Science and Engineering, Warangal Institute of Technology and Science, Oorugonda (V), Gudepadu X Roads, Atmakur (M), Warangal-506342.

Roop Singh Takur is a Post Graduate in Master of Technology from J.N.T University, in Computer Science and Engineering. having Teaching Experience of 02 years and at present Working as Asst Professors, Department of Computer Science and Engineering, Warangal Institute of Technology and Science, Oorugonda(V), Gudepadu X Roads, Atmakur(M), Warangal-506342.

Mahesh Kumar Thota is a Post Graduate in Master of Technology from J.N.T University, in Software Engineering. Having Teaching Experience of 02 Years and at present Working as Asst Professors, Department of Computer Science and Engineering, Warangal Institute of Technology and Science, Oorugonda (V), Gudepadu X Roads, Atmakur (M), Warangal-506342.