ISSN Application No. 21725

Global Journal of Computer and Digital Techniques

Volume No. 12

Issue No. 2

May - August 2024

ENRICHED PUBLICATIONS PVT.LTD

JE - 18,Gupta Colony, Khirki Extn,
Malviya Nagar, New Delhi - 110017.
E- Mail: info@enrichedpublication.com
Phone :- +91-8877340707

Global Journal of Computer and Digital Techniques

Aims and Scope

Global Journal of Computer and Digital Techniques publishes technical papers describing recent research and development work in all aspects of digital system-on-chip design and test of electronic and embedded systems, including the development of design automation tools (methodologies, algorithms and architectures). Papers based on the problems associated with the scaling down of CMOS technology are particularly welcome. It is aimed at researchers, engineers and educators in the fields of computer and digital systems design and test.

Global Journal of Computer and Digital Techniques

Global Journal of Computer and Digital Techniques

(Volume No. 12, Issue No. 2, May - August 2024)

Contents

Cross Sensor Multibiometric Authentication System

Dhara Heble[1], Rupali Nikhare[2]
[1]Student, Information Technology, Master of Engineering, Pillai College of Engineering, New Panvel, India
[2] Asst. Professor, Computer Engineering, Pillai College of Engineering, New Panvel, India

ABSTRACT

Precise identification of claimed identity is very important to the operation of our increasingly electronically interconnected information society. As a rapidly evolving technology Biometrics has been widely used in forensics, such as identifying criminals and prison security, and has the good potential to be adopted in a very broad range of civilian applications. The proposed system is trained using neural network (NN) algorithm and support vector machine (SVM) to achieve sensor adaptability. The result of training gives the adaptive parameters which will be stored into database. These stored adaptive parameters will be used at the time of matching for verification. The output of the system will be whether to accept the claimed identity or to reject

Keywords: Iris; Fingerprint; Multimodal; Machine Learning; Cross Sensor

I. INTRODUCTION

Single biometric systems have limitations like uniqueness, high spoofing rate, high error rate, non-universality and noise, and have increased the necessity of the more strong and powerful authentication system. So, using multiple biometrics is recommended. Due to increasing popularity of biometrics authentication, new sensors are being developed for acquiring input from persons, so it is beneficial if sensors are interoperable. Instead of using pure image processing, if we apply some machine learning techniques to select the learning adaption parameters will reduce the complexity and duration to complete the recognition process.

The iris is a protected but an externally visible organ whose epigenetic patterns are stable throught the life. These characteristics make iris very attractive for use as a biometric for identifying individuals. The human iris is rich in features which can be used to distinguish between two eyes. These features and patterns can be used to Measure their spatial relationships to each other provides other quantifiable parameters useful to the identification process.

Fingerprint identification is one of the well-known biometrics, because of their uniqueness and consistency over time. Fingerprints have been used for identifying people for over a century. Due to advancements in computing capabilities these days identification using fingerprints becoming automated. A fingerprint is a unique pattern of ridges and valleys on the finger surface of an individual. A ridge is a single curved segment, and a valley is the area between two neighbouring ridges. The local ridge discontinuities are known as minutiae points.

1.1 LITERATURE SURVEY

The paper[1] presents iris and fingerprint fusion system. Iris and fingerprint images are preprocessed to extract the ROIs (Regions of Interest). Then normalized data is given to the Gabor filters. The database contains five iris images and five fingerprint images of each person. The matching score is calculated through the Euclidean Distance calculation.

In paper[2], for fingerprint minutiae based matching, for face the eigenface approach is used.

Anatomical variations found amongst different people and the differences in their learned speaking habits manifest themselves as differences in the acoustic properties of the speech signal. Decision level fusion is used in this system.

Mohamad Abdolahi, Majid Mohamadi& Mehdi Jafari[3], presented a novel fusion strategy for personal identification using fingerprint and iris at the decision level fusion scheme. Hamming distance and fuzzy logic are used for decision.

2. ARCHITECTURE OF CROSS SENSOR MULTIBIOMETRIC AUTHENTICATION SYSTEM

The basic idea of this approach is to provide sensor adaptability and to provide high security using multi biometric concept i.e. Iris and Fingerprint.

Here, we focus on the sensor adaptability as it is not necessary that the sensor used at the time of enrolment is still being used by the system.

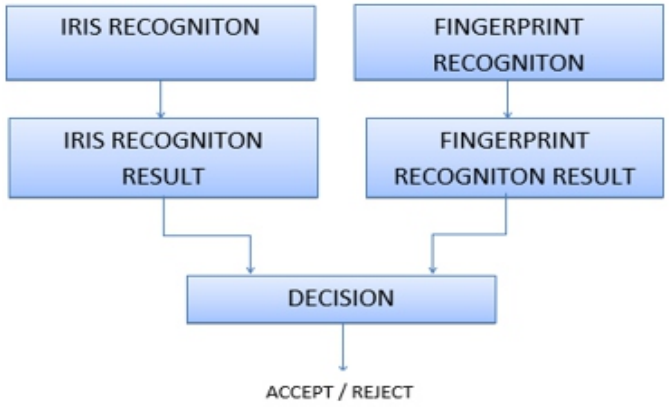


Figure 1. High Level Diagram of Proposed Approach

The System mainly contains 3 modules: Iris Recognition, Fingerprint Recognition and Decision Module

2.1. IRIS RECOGNITION

Iris Recognition module is responsible for the enrolment of users' iris, learning and sensor adaption and verification process of the user iris.

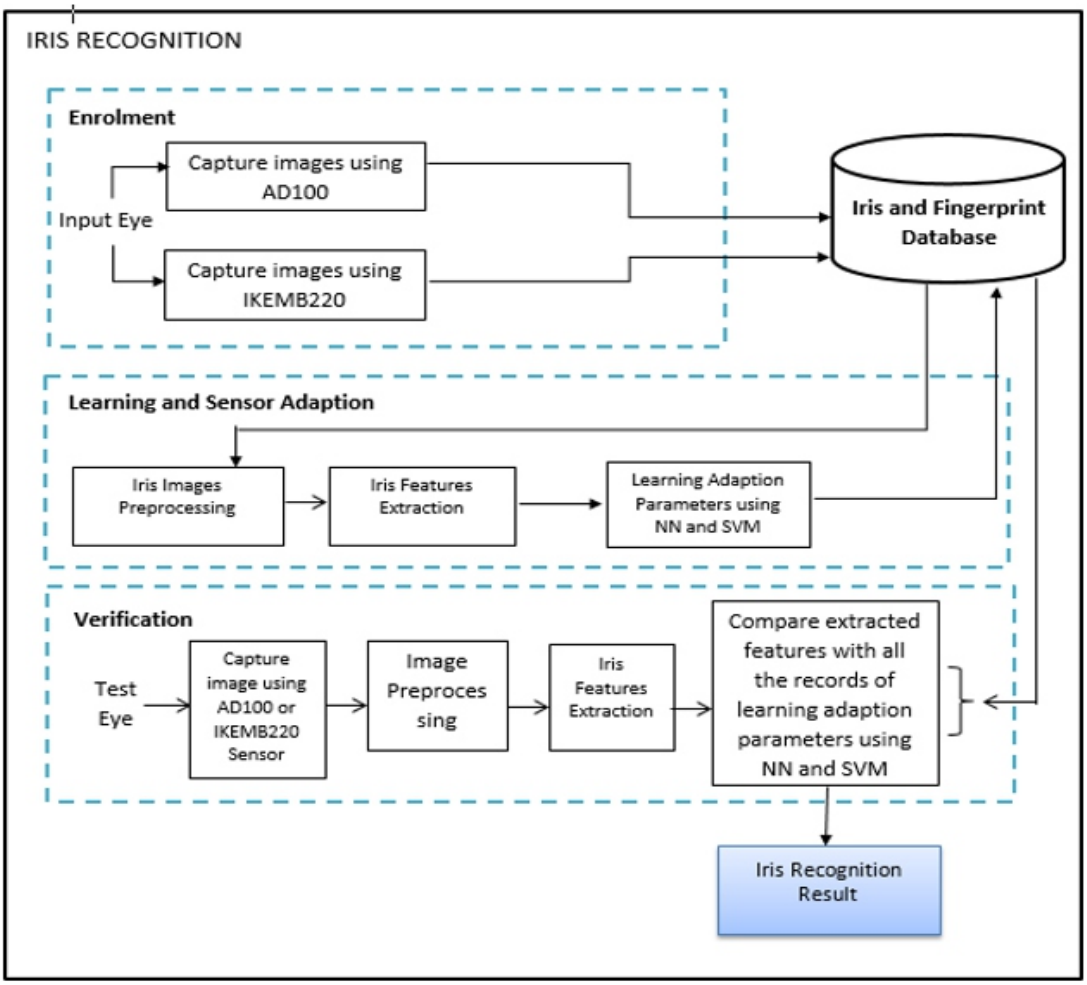


Figure 2. Iris RecognitionModule

2.2 . FINGERPRINT RECOGNITION

Fingerprint Recognition module is responsible for the enrolment of the users' fingerprint, learning and sensor adaption and verification process of the user fingerprint.

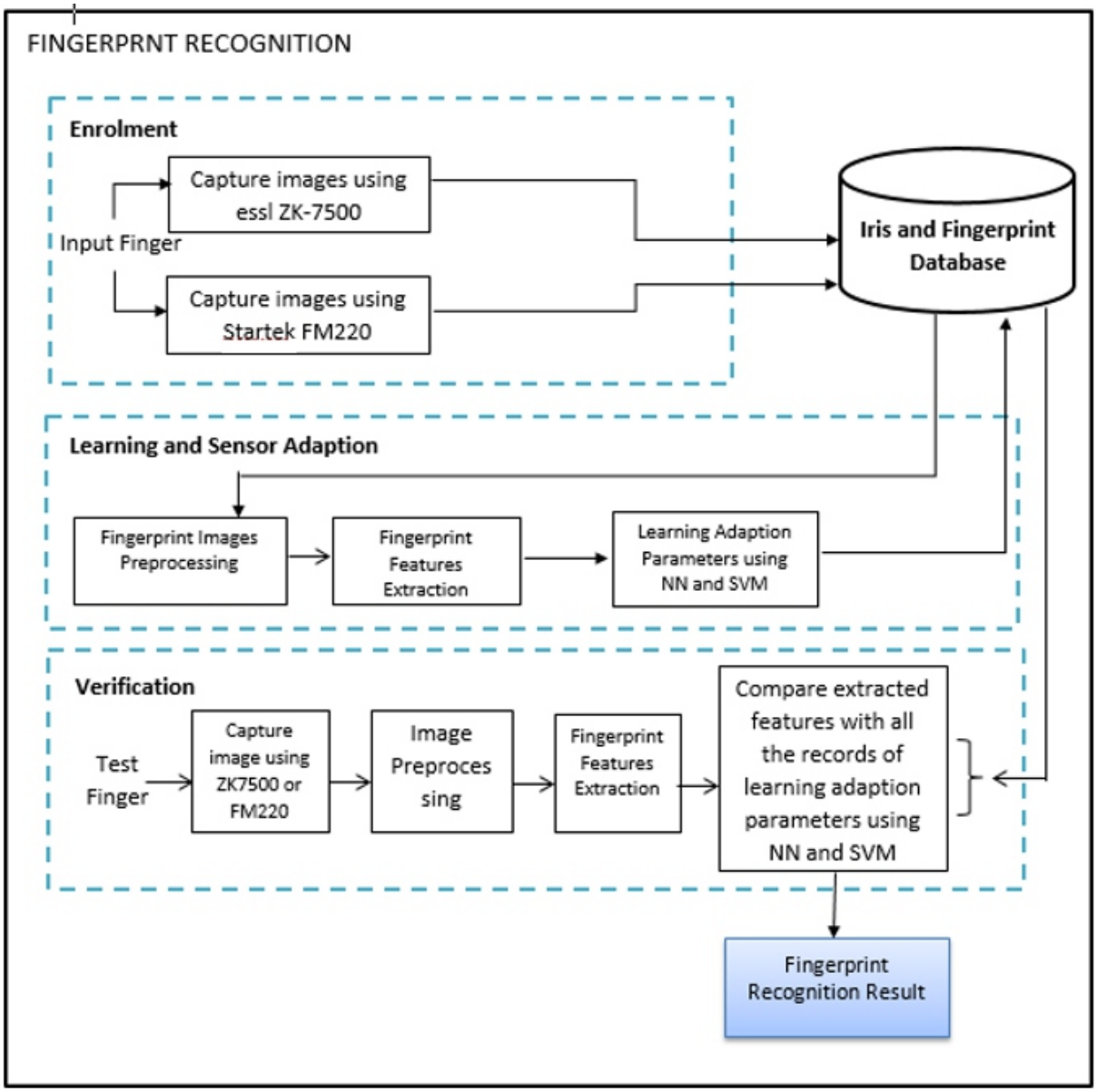


FIGURE 3. FINGERPRINT RECOGNITION MODULE

2.3 DECISION

Using the results of Fingerprint module and Iris module, decision about accepting or rejecting identity claimed is taken.

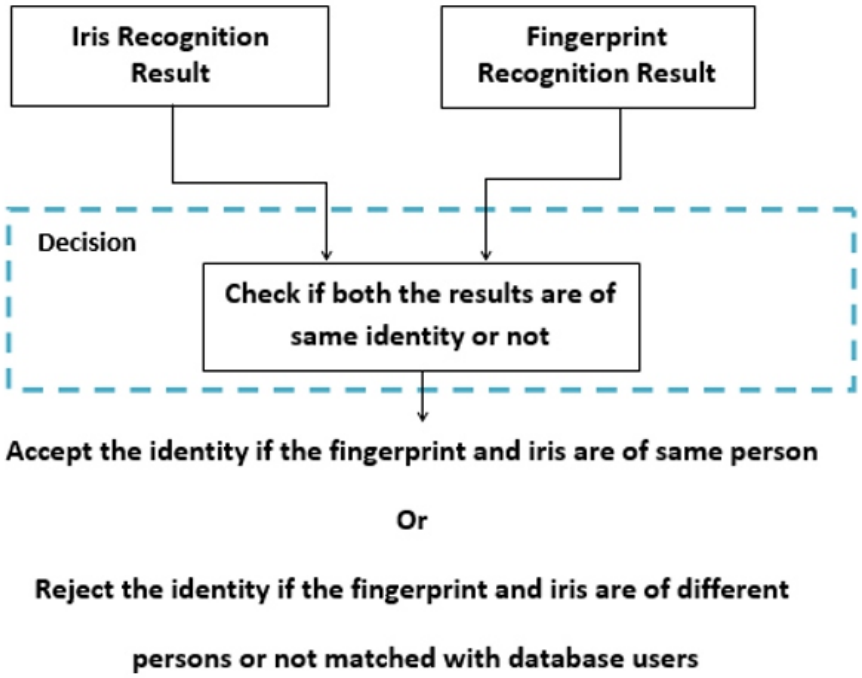


FIGURE 4. DECISION MODULE

2.3 ALGORITHM

Input: Iris and Fingerprint images captured with respective sensors

Output: Accept/Reject the Identity Claim

Enrolment

1. Capture the Iris and Fingerprint image using respective Sensors
   a. Capture two Iris images using IG AD100 and IKEMB220 each.
   b. Capture three Fingerprint images using essl ZK7500 and Startek FM220
2. Store the Iris and Fingerprint Images into Database Learning and Sensor Adaption
3. Training Iris Database
   a. Iris Images Preprocessing
      I. Localization
      ii. Segmentation
      iii. Normalization
   b. Extract Iris Features.
   c. Apply Neural Network algorithm and SVM algorithm on extracted features and save the adaption parameters in database.
4. Training Fingerprint Database
   a. Fingerprint Image Preprocessing
      I. Binarization
      ii. Thinning
   b. Extract minutiae from images using windowing technique

c. Apply Neural Network algorithm and SVM algorithm on extracted minutiae and save the adaption parameters in database.

VERIFICATION

5. Capture the Iris and Fingerprint image using respective Sensors
6. Image Preprocessing
   a. Apply step 3a and 3b on the captured iris image.
   b. Apply step 4a and 4b on the captured fingerprint image.
7. Compare Extracted Features
   a. Compare extracted iris features using selected method with the adaption parameters saved in database, found using Neural Network and SVM.
   b. Find image of minimum hamming distance (hd)

Match Found if hd< threshold
No Match if hd> threshold

c. Compare extracted minutiae using selected method with the adaption parameters saved in database, found using Neural Network
d. Find the image of minimum Euclidian Distance (ed)

Match Found if ed< threshold
No Match if ed> threshold

8. Find the result for Iris matching and Fingerprint Matching
9. Decision
   a. Check whether the identity of the person is same for Iris and Fingerprint
   b. Accept the identity if the result of Iris recognition and Fingerprint recognition is of same and claimed identity, otherwise reject the identity.

3. RESULT AND ANALYSIS

This system is developed in Matlab 2013b. For the Fingerprint enrolment we have used two different sensors, i.e. essl zk-7500 and Startek FM220. We have taken fingerprint data of 100 volunteer users. For the Iris enrolment we have used the CSIR train database, which is used for "The ICB Competition on Cross-sensor Iris Recognition"[12]. From this database we have taken images of 100 different eyes. Figure shows the images found during Iris features extraction.

Figure shows the images found during Iris features extraction.

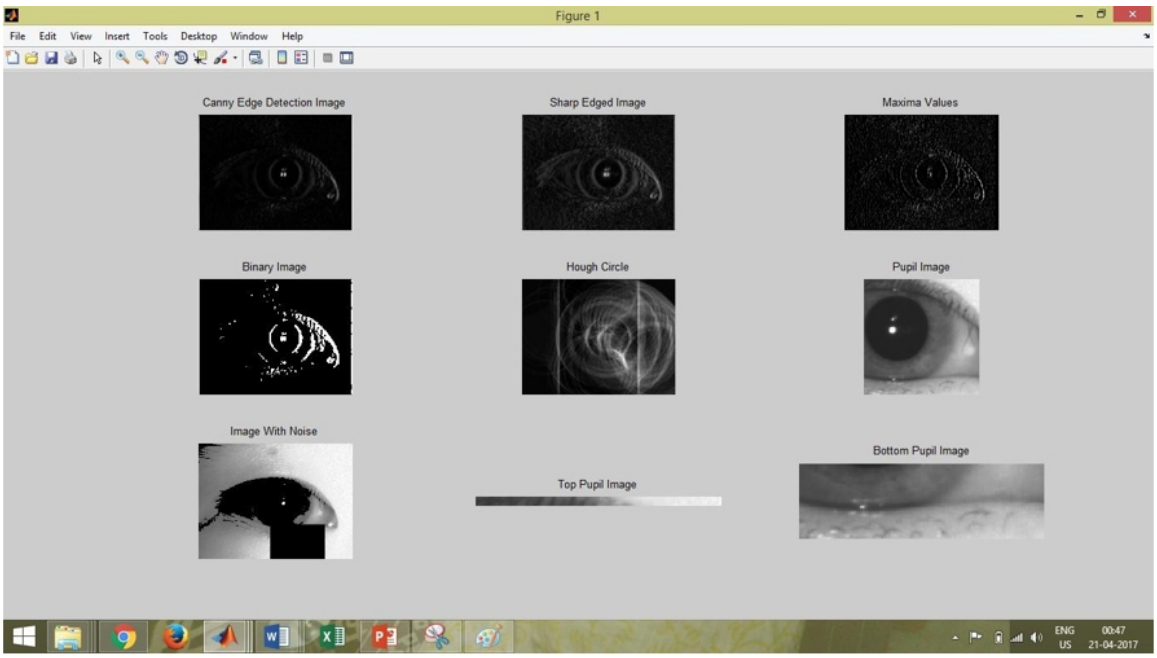


Figure 5: Iris pre-processing images

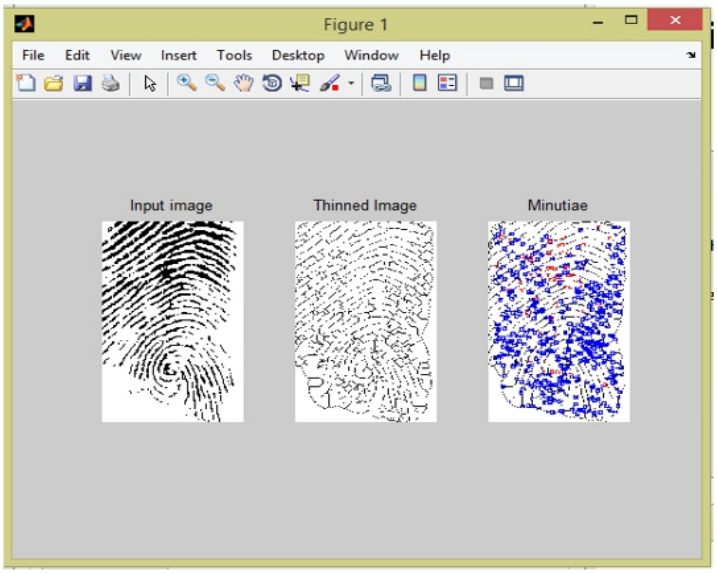


Figure 6: Fingerprint pre-processing and extracted Minutiae

The Figure shows the system input and result.

Verification Process is as follows:

FINGERPRINT

(a) Select the input Finger

(b) Select the Sensor from which the input is taken

(c) Select the verification method, i.e. Neural Network or SVM

(d) Click Finger Testing

(e) The result will be displayed.

IRIS

(a) Select the input Iris

(b) Select the sensor from which the input is taken

(c) Select the verification method, i.e. Neural Network or SVM

(d) The result will be displayed.

DECISION

(a) Click on the Result button, it will display whether the User is Authorised user or not.

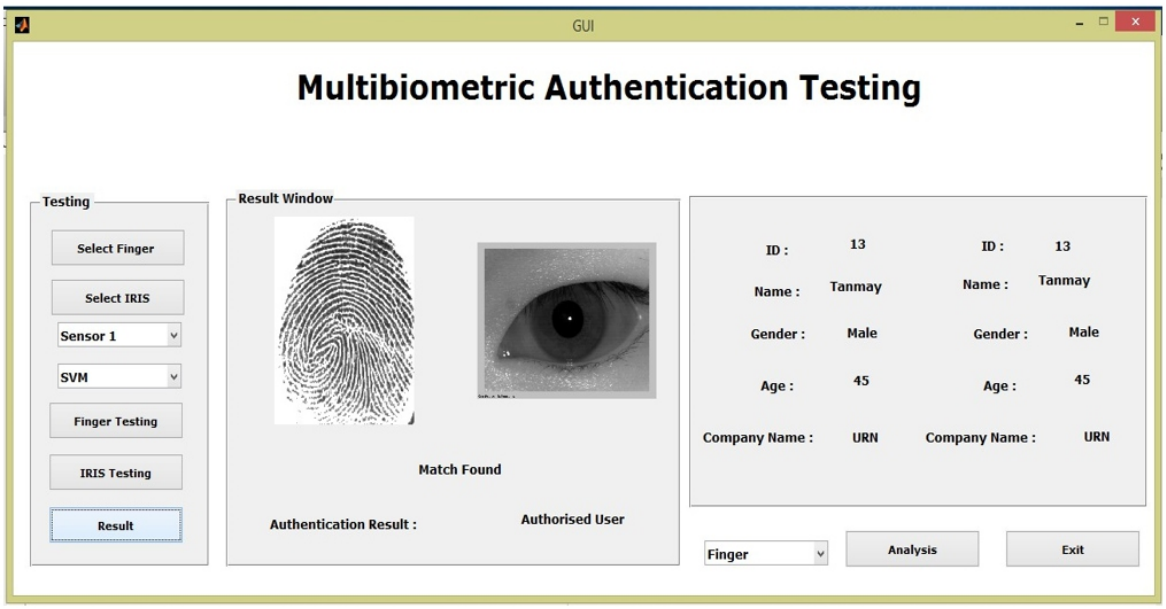


Figure 7: System Verification Module and Result

3.1 ANALYSIS

System is tested on various positive (registered user) and negative (non-user) samples. Below are the findings of Precision, Accuracy, Recall and other measuring factors.

TERMINOLOGY AND DEFINITIONS USED IN ANALYSIS

TPR= True Positive Rate= TP/(TP+FN)

TNR= True Negative Rate = TN/ (TN+FP)

FPR= False Positive Rate = FP/(FP+TN)

FNR= False Negative Rate = FN/ (TP+FN)

Pr. = Precision = TP / (TP+FP)

Acc. = Accuracy = (TP+TN) / (TP+FP+FN+TN)

Table 1 Fingerprint Analysis

Fingerprint Sensor	SVM						NN					
	TPR	TNR	Pr.	FPR	FNR	Acc.	TPR	TNR	Pr.	FPR	FNR	Acc.
Zk7500	0.8	0.9	0.888	0.1	0.2	0.85	0.8	0.9	0.888	0.1	0.2	0.85
FM220	0.6	0.6	0.6	0.4	0.4	0.6	0.9	0.6	0.692	0.4	0.1	0.75

Table 2 Iris Analysis

Iris Sensor	SVM						NN					
	TPR	TNR	Pr.	FPR	FNR	Acc.	TPR	TNR	Pr.	FPR	FNR	Acc.
AD100	0.9	0.9	0.9	0.1	0.1	0.9	0.9	0.9	0.9	0.1	0.1	0.9
IKEMB220	0.9	1	1	0	0.1	0.95	0.9	1	1	0	0.1	0.95

Performance analysis graphs for Iris and Fingerprint are as follows

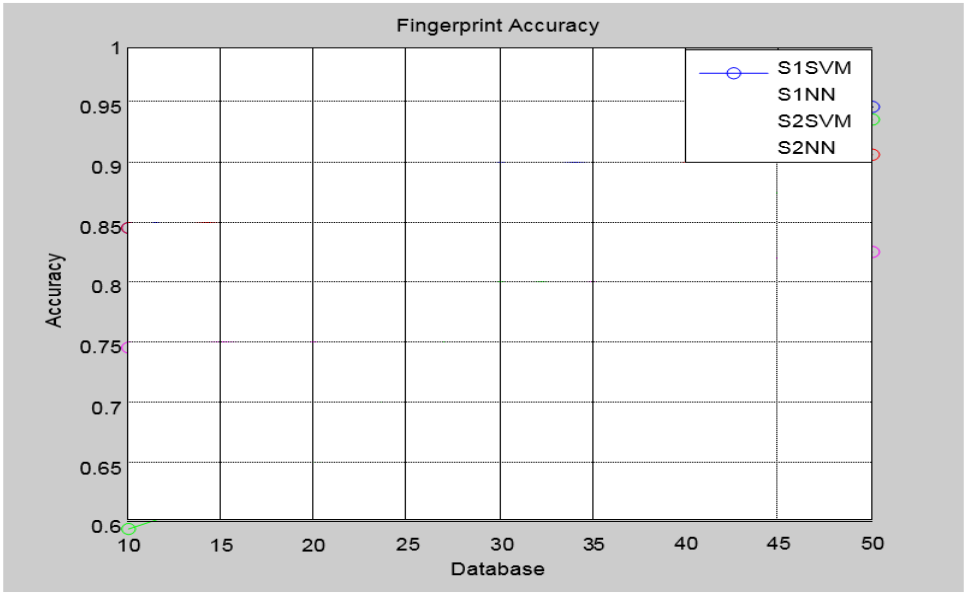


Figure. 8 Fingerprint Accuracy

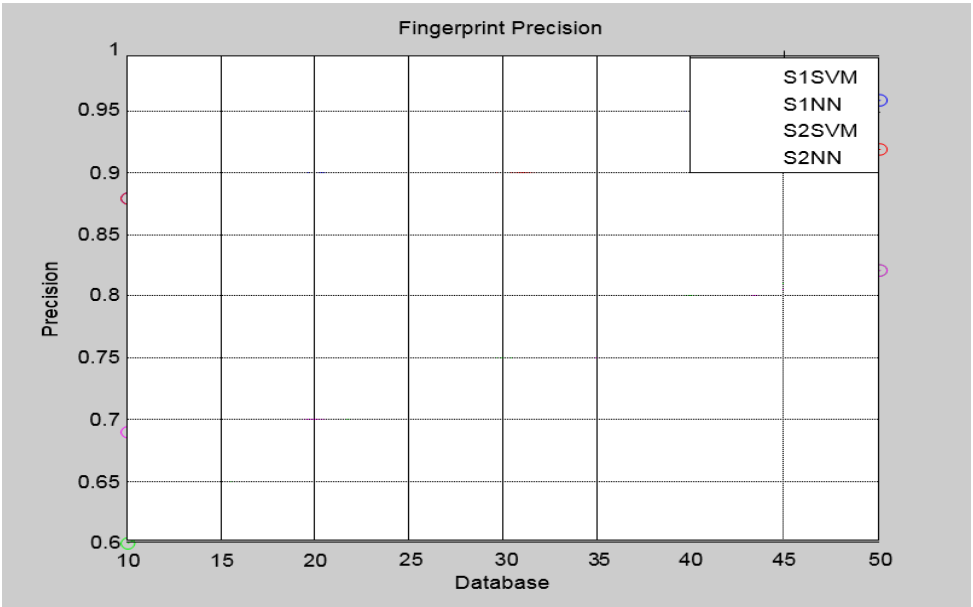


Figure 9 Fingerprint Precision

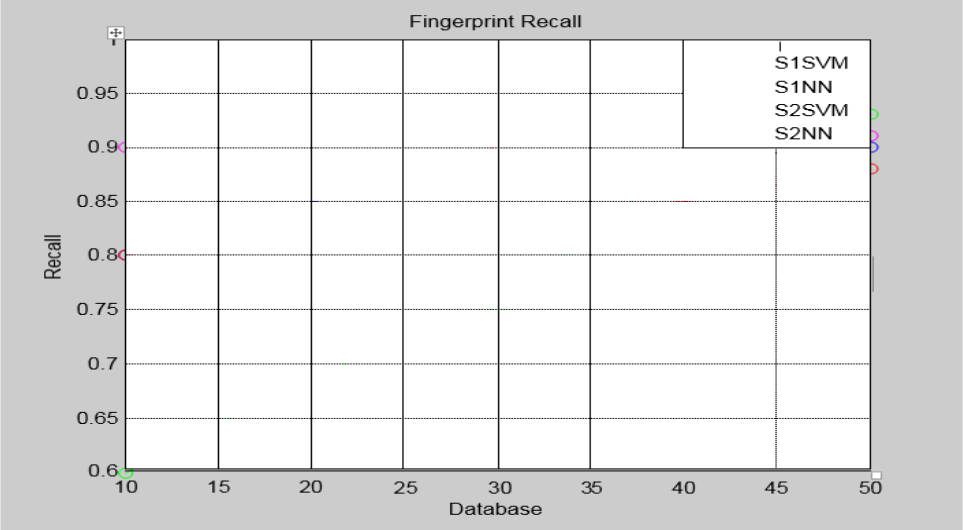


Figure 10. Fingerprint Recall

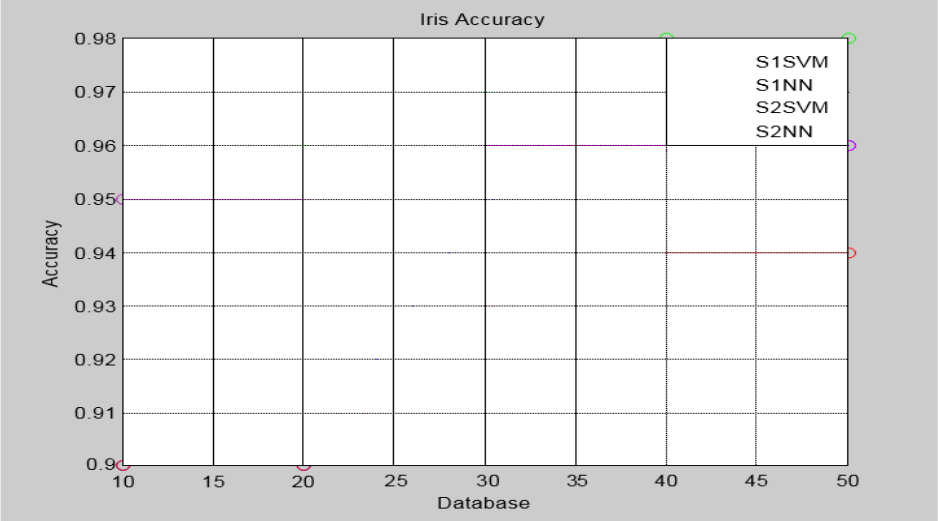


Figure 11. Iris Accuracy

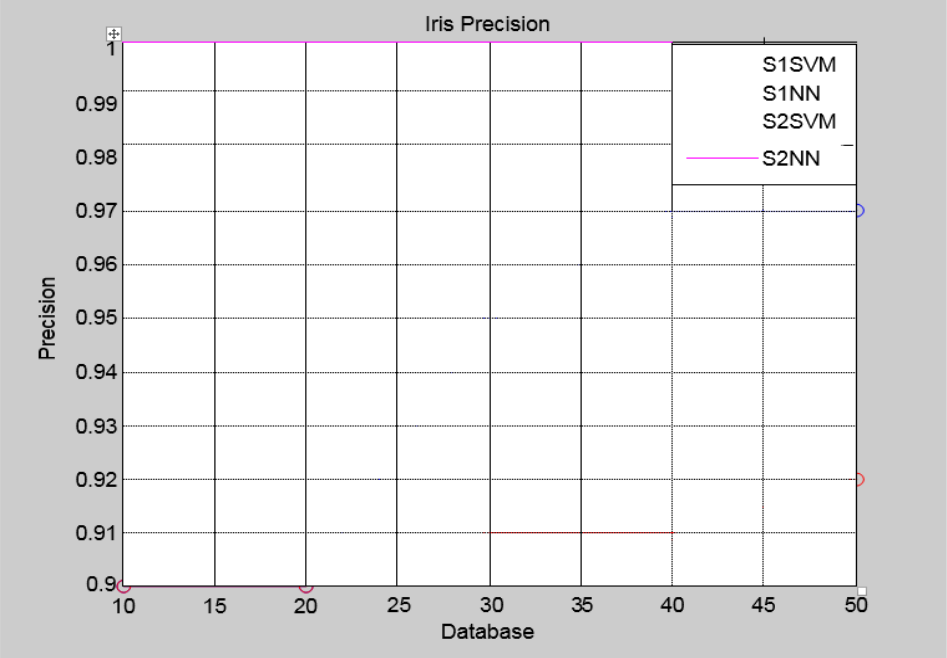


Figure 12Iris Precision

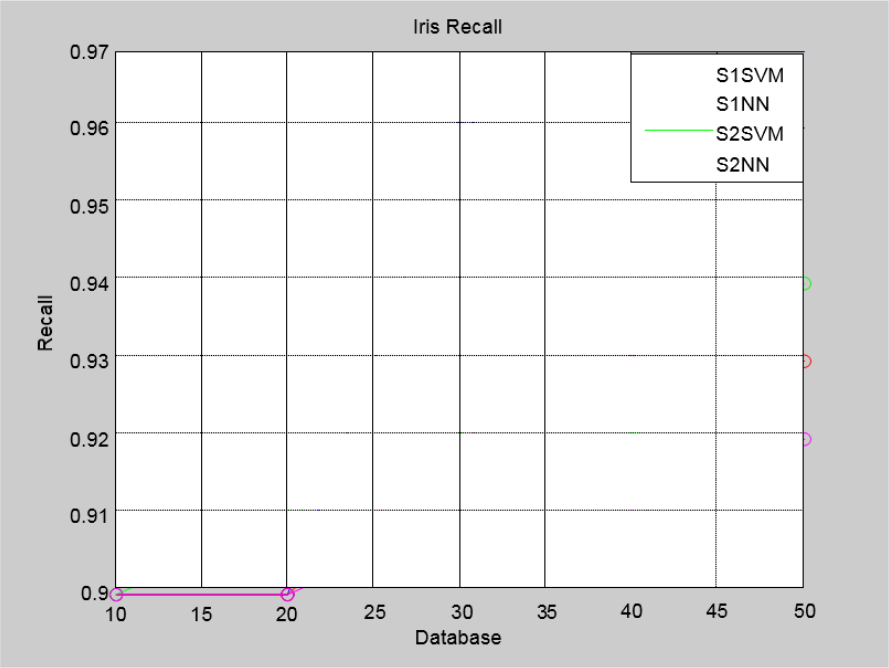


Figure 13.Iris Recall

3. CONCLUSION & FUTURE WORK

The Cross Sensor Multi Biometric Authentication Using Machine Learning is developed. The main focus revolves around the system adaption for cross sensor and using multi biometric to provide increased security. We presented the complete architecture for the development of cross sensor multi biometric system and several algorithms for this system.

Neural training algorithm and SVM are used to train the iris and fingerprint database for cross sensor adaption. Which reduces the efforts of features comparison while verification or identification. The goal of developing such an authentication system is to provide increased security where required, with sensor adaptability

.

Neural Network and SVM both are good classifiers. For this system, SVM gives the better results than Neural Network.

For more efficient system we can take more samples of iris and fingerprint images of single user at the time of enrolment, which can result in more efficient learning and adaption parameters.

4. REFERENCES

[1] Geethu S Kumar &C Jyothirmati Devi "A Multimodal SVM Approach for Fused Biometric Recognition" (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3, 2014, 3327-3330)

[2] Gajendra Singh Chandel&Ankesh Bhargava "Identification of People by Iris Recognition"International Journal of Science and Modern Engineering (IJISME) ISSN: 2319-6386, Volume-1,Issue-4, March 2013

[3] P.U.Lahane&Prof.S.R.Ganorkar "Fusion of Iris & Fingerprint Biometric for Security Purpose" International Journal of Scientific & Engineering Research Volume 3, Issue 8, August-2012 1 ISSN 2229-5518

[4] Mohamad Abdolahi, Majid Mohamadi& Mehdi Jafari "Multimodal Biometric system Fusion Using Fingerprint and Iris with Fuzzy Logic" International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-6, January 2013

[5] Anil Jain, Lin Hong and Yatin Kulkarni "A multimodal biometric system using Fingerprint, Face and Speech"

[6] S. Sangeetha & N. Radha (2012) "A new Framework for Iris and Fingerprint Recognition Using SVM Classification and Extreme Learning Machine Based on Score Level Fusion" Intelligent Systems and Control (ISCO), 2013 7th International Conference

[7] Jaishanker K. Pillai, Maria Puertas and Rama Chellappa (2014) "Cross-Sensor Iris Recognition through Kernel Learning" IEEE Transactions on Pattern Analysis And Machine Intelligence, Vol. 36, NO. 1, January 2014

[8] Ryan Connaughton, Amanda Sgroi, Kevin Bowyer, and Patrick Flynn "A Multi-Algorithm Analysis of Three Iris Biometric Sensors" IEEE Transactions on Information Forensics And Security 2012

[9] Sunpreet S. Arora, MayankVatsa, Richa Singh and Anil Jain (2012) "On Iris Camera Interoperability" 978-1-4673-1228-8/12/2012 IEEE

[10] Samir Nanavati, Michael Thieme, Raj Nanavati"Biometrics Identity Verification in a Networked World" Wiley Computer Publishing, 2002

[11] S.N. Sivanandam and S.N. Deepa "Principles of Soft Computing" Wiley India Publication

[12] http://biometrics.idealtest.org/2015/csir2015.jsp

Framework For Authenticate The Message In Vechular Ad-hoc Network

Madhavi Sinha[1], Ankit kumar[2]

[1]Associate Professor, Department of Computer Science &Engineering, Birla Institute of Technology, Mesra, Jaipur campus, Jaipur

[2] Research scholar, Dept. Department of Computer Science &Engineering, Birla Institute of Technology, Mesra, Jaipur campus, Jaipur

A B S T R A C T

Vehicular Ad- Hoc Networks (VANET) is a special kind of ad- hoc wireless networks that include wireless communication devices with short range, each representing a road vehicle or a static device. Networks VANET (Vehicular Ad- Hoc Networks) represents an area of research interest because of the advantages they bring in development Application traffic optimization , improve road safety , reduce pollution in major urban and more. Many experts consider that this form of ad- hoc network Mobile will become increasingly important in coming years. The development of applications and protocols for VANET networks pose problems unique security induced by devices used for vehicle or sporadic connectivity need to protect the identity of the users. Information which is passed in the VANET network frequently require increased measures to ensure the security of the message. This paper proposes a security protocol to ensure proper submission particular characteristics of VANET systems. The proposed solution is shown to be adequate to protect messages sent between participants traffic. Overall, this paper shows an experiment that wants to turn the compromise between advantages and disadvantages in a step forward in what concerns security in vehicular networks ad- hoc.

I. INTRODUCTION

VANET Vehicular Ad- hoc Network provides a communication protocol between nearby vehicles or between a vehicle and infrastructure. It is expected that to it use the wireless communication baseband 5.9Ghz technology using Dedicated Short -Range Communications (DSRC) .Cars are used to create a mobile ad- hoc network in which they communicate with each other. Each node is actually a wireless router that allows other nodes to connect to the network, expanding the range. It is estimated that the first systems that implement this technology will be designed for police and firefighters, so that the vehicle can communicate with each other for safety reasons. Vehicular ad- hoc network can be seen as a component of Intelligent Systems Transportation (ITS). The main purpose of these networks remains occupant safety and convenience of traffic. By equipping vehicles with communication equipment, and organizing them in ad-hoc networks, we do not remain just a step for the design of services and applications that improve vehicle driving experience. Vehicular ad- hoc networks (VANETs) provide infrastructure less, rapidly deployable, self-configurable network connectivity. The VANET network is

the collection of vehicles interconnected by wireless links (Roadside Unit, OnBoradUnit) and willing to store and forward data to the other vehicles. As vehicles move in VANET and arrange themselves randomly, routing of message is done dynamically based on network connectivity and speed. Like the other network VANET network are particularly very important due in part to the vehicles' high rate of mobility and the many different signal- weakening barriers, such as buildings, in their geographical position.

Due to their huge potential, VANET have gained a huge attention in both industry and academic world. Research activities range from lower layer protocol design to safety applications and implementation of them is covered by all the country and universities. We need a safe and reliable VANET system, while exchanging information protect the VANET network against unauthorized message modification, message injection, eavesdropping. The security of VANETs is one of the most significant issues because their information transmission is transmitted in open access (wireless network) environments. It is essential that all transmitted data should not be injected or altered by users who have malicious goals or objective. Last few years VANET have usual increased attention as the potential technology to promote the active and defensive safety on the road and the drivers, as well as travel ease. Trust and privacy are compulsory in vehicular communications for successful approval and deployment of such a technology.

2. STATE OF ART

Research on VANET security is abundant and demonstrates, PKI encryption and decryption are very complicated and create a large calculation overhead during communication to provide the security. The method which is used by Choi JY, Jakobsson M, Wetzel S (2005) Balancing auditability and privacy in vehicular networks. They use the RSA and MAC to provide message security and RSUs to authenticate message integrity. The method in assumes that each vehicle has a black box that generates the vehicle's public/private key. However, each key is very long because it is based on the continued product of two numbers, and this imposes a huge burden during message transmission.

Zhang C, Lin X, Lu R, Ho P-H, Shen X (2008) An efficient message authentication scheme for vehicular communications. (IEEETrans Veh Technol 57(6):3357–3368) proposes a security mechanism for excessive calculation burden during message authentication. When a vehicle enters an RSU's communication range, it negotiates with the RSU for a common secret key to send the hello message. When the vehicle requires to transmit a message to other vehicles, it calculates an HMAC value using with well known hash function, in combination with a secret key which is used to validate

the message. When the RSU receives the message, it announces the result of message authentication within a fixed time interval to help the vehicle confirm the message's integrity. These announcements are sent at fixed time intervals to conserve network resources. Because the hash functions perform this calculation, the HMAC can provide quick authentication and decrease the burden of encryption and decryption.

As mentioned by the above two author there are two problems with their methods:-

1. Vehicles in different RSU communication ranges cannot authenticate with each other the message-receiving vehicle cannot confirm message integrity because it does not know the common secret key of the source vehicle.
2. Message handoff when a vehicle moves between different RSUs is problematic. When a vehicle moves from one RSU range to another, the new RSU must obtain the vehicle's certificate for source authentication before negotiating a new common secret key. This authentication method is not only inefficient but also dangerous, because it frequently exposes certificates.

3. DIFFERENT SECURITY REQUIREMENT FOR THE VANET SYSTEM.

- **Confidentiality:** is the assurance that the data could not have been accessed by any other vehicles than the designated recipient for whom it was meant; thus insuring that the data was untouched in anticipation of reception. Confidentiality is generally obtained by cryptography techniques in VANET network.

- **Availability:** It is the section of time that a system is in a functioning tenure. In safety applications like post-crash warning in the wireless channel has to be available, so that forthcoming vehicles can still gets the warning messages. If the radio channel goes out (e.g. jamming by an attacker), then the warning message can never be broadcast and the application used itself becomes abject. Hence high availability of communication systems is obligatory.

- **Authentication:** It is the authentication of a vehicle to identity prior to granting access to the VANET network. It can be composed as the first line of defense against intruders in the VANET network... In safety application, where trust plays a prominent role. Authentication declares that the given message is trustworthy by correctly identifying the originator of the message. With ID authentication the receiver becomes worthy to have a unique ID of the sender. The ID could be the license plate or chassis number of the vehicle. In other cases receivers are not concerned with the actual identity of nodes. They are gratified if they are able to verify that the sender has a certain property with related

to the vehicle authenticity. Property authentication is a security requirement that permits the verifying properties of the sender, e.g., a colored traffic sign. For applications using location information, location authentication allows to authenticate that the sender is essentially at the claimed position, or that the message position claim is valid.

- **Data integrity:** It is the declaration that the content of the data was not modified while in transit. It differs from privacy trust and authenticity in the sense that it verifies that detection of data modifications.

- **Non-repudiation:** It is the process of authentication that the data was sent with vehicles credentials and other information so that without denial or repute the datacan be related to the sender vehicles. Non-repudiation aims to avoid one entity to deny having done some action. The most common examples in computer networks are related to sending some information (NRO, Non- repudiation of Origin) or receiving it (NRR, Non-repudiation of Receipt). However, both services are different by nature and so are their implementing mechanisms in VANETs.

4. PROPOSED METHODOLOGY

Security protocol is designed and implemented for vehicular ad-hoc networks with property as existing OBU (on board unit) which can communicate with each other and with existing infrastructure. T he aims to ensure the transmission of messages between different vehicle to securing vehicle communication in traffic .The method is designed for heavily traffic which suffers from high dynamicity of the connecting the nodes in the network.

The main components considered in protocol design are Vehicle and Road Side Unit (CityTrafficLight). The component on which our framework work are Messaging secured between vehicles in traffic is based on the existence of a third party certification authority present in that geographical area, The distance between road side unit and vehicles who want to communicate, The path on which they are moving, that the vehicle destination is in transmission range, or the need to select a route that includes several hops in the transmission of messages.

Communication between vehicles in a network characterized by a high degree of dynamism, geographical positioning, and sporadic connectivity between automobile securities problems unique. This protocol is aims to solve these issues, covering the following general issues relating to safety:

Vehicle is considered a mobile entity that exchange messages with other vehicle well with existing infrastructure (i.e. traffic road side unit at crossroads secure). The purpose Protocol is to provide a solution for securing messages between vehicles so that the entity to be able to check the validity of incoming messages. Secure traffic road side unit (part of infrastructure) have the role to verify the message and signed the message with third parties certification authority entities that help prove the authenticity of messages. Certifying Authority will knows that the road side unit can communicate with each other if they want to validate certain data. The main aspects that rely solution the sending ofmessages, timing of car existing certification authority in the geographical area when communication happen. Protocol is modular, scalable, structured seen in the figure below.

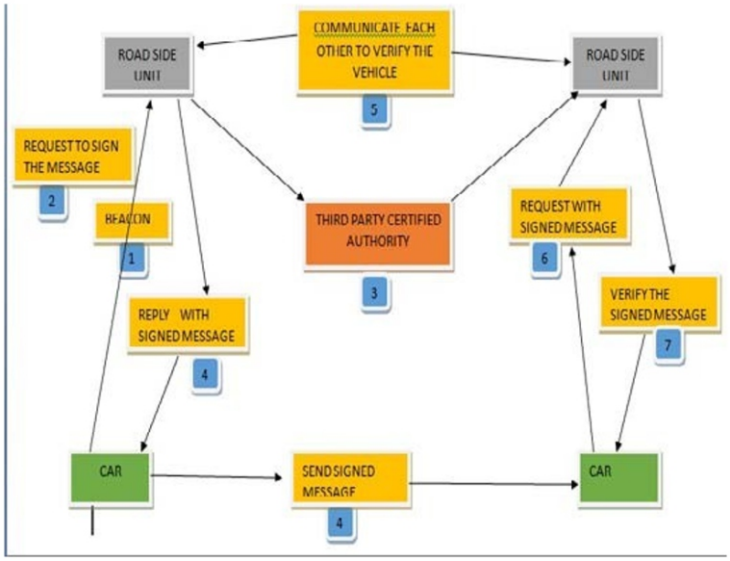


Fig: 1.0 new protocol design for secure VANET

The proposed method is structured in many states. Range of transmission of a car is less than the range of transmission of Road side Unit to Signing a secure message by Road side unit when a vehicle wants to send information to another vehicle, first Road side unit the beacon waits in whose coverage area is. Beacon message is transmitted periodically by all vehicle of zero coverage in a message broadcast (vehicle will transmit a data packet traffic light containing information that must signed by them .Considering the specific mobility transmission that has a vehicle, sending the message to be signed by the message that can be achieved in two ways: The protocol is structured in several states. Communicating vehicle place only when the car has a message that is in coverage) of a Roadside unit. Transmission range of a vehicle is less than the transmission range of secure Road side unit. Signing a secure message by third party When a vehicle wants to send information to another vehicle, first road side unit has the beacon message waits in whose coverage area is .Beacon message is transmitted periodically by all vehicle of a message (broadcast) . Upon receipt Beacon vehicle will transmit a data packet traffic road side unit containing information that must considering the specific mobility in VANET networks and restricted area of transmission.

- When a vehicle wants to send information to another vehicle, first traffic road side unit the beacon waits in whose coverage area is. Beacon message is transmitted periodically by all OBU in the area of
- If the traffic light is in the range of the car, the message will be sent directly semaphore for signature
- If the traffic light is not in range of the car, the message will be routed, hop by hop through intermediate cars to reach the issuing beacon lights.

Important information contained in the package are the timestamp for the moment is the message, the current location and the actual message. All this information will be signed by the issuing beacon lights. When the message gets back from the road side unit message with signature there on, vehicle will convey this message to the destination. If issued periodically beacon message is sent as a secure broadcast, the signed message to be sent back car is sent in the form of unicast, as the vehicle is in the range of the light. Message transmission to the destination vehicle can be done in two ways: target vehicle is in the range of the source vehicle, so the message is routed directly. Destination vehicle is not in range of the source vehicle, so the message is routed using existing intermediate cars to their final destination. When the message reaches the destination, the destination vehicle must validate that message before processing it. The way they could check a message on destination is sending it to a stop in the immediate neighbor. Road side unit communicate with each other so that the message can verify the signature. sending the message to the road side unit in the neighbor can be made directly, if it is within range (transmission) the car or routed through multiple hops (intermediate cars), if not in range. Data validation can be done only at the road side unit, this message and signature checking related fields which was established signature. Verification results will sent to the car who called validation for the message. If the answer is yes, then the message can be processed further, or otherwise it is discarded the message.

Geographical Location is a very important field that certifies that the message transmitter located in a specific geographic area. Footstep on the geographical position (latitude, longitude) requires network users to probing site. The easiest and safest way to check the appearance of terms location is existent route infrastructure require validation infrastructure (road side unit secure) so when a car receives a message, all the infrastructure can decide whether to accept the message geared location.

At a high level, the location is a metadata component emitted from a wireless infrastructure (road side unit) for a mobile device. To use fingerprint positioning a application must trust infrastructure for validation geographical position. For any type of communication infrastructure require cars to sign those messages. Role infrastructure is only to sign and validate messages automotive transmission range.

6. STRUCTURE AND DETAIL OF SAFETY MESSAGES - DIGITAL SIGNATURES

Generating keys has two phases. The first phase of the algorithm is in choosing parameters:

1. Choose a hash function H. output hash function application can be truncated to size chosen pairs of keys.
2. Choose the key length L and N.
3. Choose a prime number of N bits. N must be less than or equal to the length of g. The result of applying the hash function.
4. choose a prime number p of L -bit mode so that p -1 to be a multiple of q
5. g is chosen , a number whose multiplicative order modulo p is q. It is set by choosing g =h(p-1)/q mod p for arbitrary h (1 < h <p -1) (check again if the result is equal to1) Usually h = 2.

The second phase of the algorithm computes the public key and private key for a uses specifically:

1. Choose a random number x with the property 0 < x < q.
2. calculate y = pow(g,x)mod p
3. The public key is (p , q , g, y) .
4. Private Key is x.

6.1 SIGNING THE MESSAGE CONSISTS OF THE FOLLOWING:

Consider the hash function H and m message

1. generate a random value K for each post 0 <k <q
2. compute r = (pow(g,k)mod p) mod q
3. calculate s = (K-1(H (m) + x*r)) mod q
4. recalculate signature if r = 0 and s = 0 the signature is ®, s)
5. Signature accepting if at least one of the conditions 0 <r <q and 0 <s <q is not is satisfied
6. compute w = (s)-1mode q

7.compute u1 = (H (m)*w) mod q

8. calculate u2 = (r*w) mod q
9. compute v = ((pow(g u1)* y u2) Mod p) mod q signature is valid if v = r

The proof of correctness of the algorithm can be done as follows: first time, if g = h (p-1) / q mod p then it follows that g q ≡ h (p-1) ≡ 1 (mod p) according to Little Fermat Theorem Fermat. How g> 1 and q is prime, g have the same order of q.

ALGORITHM USED FOR CREATING THE DIGITAL SIGNATURE:

1. Choose two large distinct primes p, q. Calculate n=pq.
2. Calculate • (pq). This happens to be (p−1)(q−1).
3. Choose e such that gcd(e,• (pq))=1 and 1<e<•(pq).
4. Compute d such that de=1mod• (pq).
5. Do some crypto; c=te mod n and t=cd mod n.
6. . Fermat's little theorem states that ap=amod(p) An alternative, equivalent definition is that ap−1=1mod(p).
7. a• (n)=1 mod n
8. • (x) function, it's the number of numbers less than or equal to x which are also coprime to it. For any given prime p, every number less than itself is coprime to it, which means • (p)=p−1. If you're wondering about why • (1)=1, well, gcd(x,1)=1 is the definition of coprimality, including for 1 itself.
9. Now, it's also possible to get the value of • (xy)=• (x)• (y).
   n=pq⇒• (n)=• (p)• (q)⇒• (n)=(p−1)(q−1).

IMPLEMENTATION ISSUES

1. Only Road side unit have the authority to verify the signature .so there is no any such method by which vehicle can verify the message.

2. Each vehicle have the on board unit through which they can send and receive the message from road side unit or from the other vehicles.

3. A representation of a certifying authority which issue the certificate to each vehicle who want to join the VANET network.

4. A certificate which is issued by the certifying authority is valid up to one region of issue.

5. Relocation new certificate won't required in nearby location.

7. CONCLUSION:

In this paper, we have proposed the new secured model for VANET system for vehicle communication using public key cryptography which has very less overhead than other cryptography technique .Here we focus only why vehicular networks need to be secured, and this problem requires a specific approach to get the security in VANET network. We have proposed a model that identifies the most appropriate communication aspects. We have also identified the major threats and security flaw which is possible in VANET. The security framework along with the related protocols has been proposed which shows how and to what extent it protects availability, authorization, privacy, trust. We have been proposed that public key cryptography is suitable as solution for the considered problem. In terms of future work, we intend to further develop this Proposal. In particular, we intend to explore in more detail the respective

merits of key distribution by the manufacturers or by governmental bodies; we will also perform additional numerical evaluations of the solutions.

REFERENCES:

[1] Carlos J. Bernardos, Ignacio Soto, Maria Calderon, "VARON: Vehicular Ad hoc Route Optimisation for NEMO, "Computer Communication 30(2007) 1765-1784

[2] D.Boneh, M.Franklin, "Identity-based encryption from the Weil pairings, "Advances in Cryptology-Crypto 2001, LNCS 2139, pp.213-229.

[3] Manik Lal Das, Ashutosh Saxena, Ved P. Gulati and Deepak B. Phatak, "A novel remote user authentication scheme using bilinear pairings, "Computers & Security, Volume 25, 2006, pp.184-189.

[4] Chun-Ta Li, Min-Shiang Hwang, Yen-Ping Chu, "A Secure and Efficient Communication Scheme with Authenticated Key Establishment and Privacy Preserving for Vehicular Ad Hoc Networks, "Computer Communications 31 (2008), pp.2803-2814.

[5] Chih-Yin Lin, Tzong-Chen Wu, Fangguo Zhang, Jing-Jang Hwang, "New identity-based society oriented signature schemes from pairings on elliptic curves, "Applied Mathematics and computation 160 (2005) 245-260

[6] Yi-Wei Lu , L Wu, "Electronic payment systems by group blind signatures, ". ethesys.yuntech.edu.tw, 2003.

[7] KG Paterson, "ID-based signatures from pairings on elliptic curves, "Electronics Letters, Volume 38, Issue 18, 29 Aug 2002 Page(s): 1025 – 1026

[8] Klaus Plößl, Hannes Federrath, "A privacy aware and efficient security infrastructure for vehicular ad hoc networks, "Computer Standard & Interfaces, Volume 30, Issue 6,
August 2008, Pages 390-397

[9] M. Raya, J. P. Hubaux, "Security aspects of inter-vehicle communications, "Proceedings of the 5th Swiss Transport Research Conference (STRC), 2005.

[10] M.Raya, J. P. Hubaux, "The security of vehicular ad hoc networks, "Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks, 2005, pp.11-21.

[11] M Raya, D Jungels, P Papadimitratos, I Aad, JP, "Certificate Revocation in Vehicular Networks, "Laboratory for Computer Communications and Applications (LCA), School of Computer and Communication Sciences, EPFL, Switzerland, LCA-Report- 2006-006

[12] Maxim Raya, Jean-Pierre Hubaux, "Securing vehicular ad hoc networks, "Journal of Computer Security, 15, 2007, pp.39-68

[13] Narn-Yih Lee, Chien-Nan Wu, Chien-Chih Wang , "Authenticated multiple key exchange protocols based on elliptic curves and bilinear pairings, "Computers and Electrical Engineering, Volume 34, Issue 1, January 2008, Pages 12-20.

[14] Neng-Wen Wang, Yueh-Min Huang, Wei-Ming Chen, "A novel secure communication scheme in vehicular ad hoc networks, "Computer Communications, Volume 31, Issue 12, 30 July 2008, Pages 2827-2837

Feedforward Neural Network: A Review

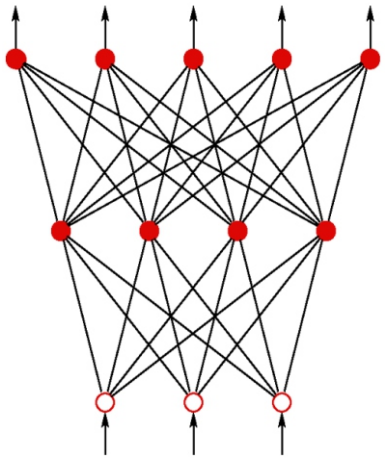
**Pankaj Sharma, Naveen Malik,
Naeem Akhtar, Rahul, Hardeep Rohilla**

Student, CSE, Dronachraya College of Engineering, Gurgaon

ABSTRACT

Precise identification of claimed identity is very important to the operation of our increasingly electronically interconnected information society. As a rapidly evolving technology Biometrics has been widely used in forensics, such as identifying criminals and prison security, and has the good potential to be adopted in a very broad range of civilian applications. The proposed system is trained using neural network (NN) algorithm and support vector machine (SVM) to achieve sensor adaptability. The result of training gives the adaptive parameters which will be stored into database. These stored adaptive parameters will be used at the time of matching for verification. The output of the system will be whether to accept the claimed identity or to reject A feedforward neural network is an artificial neural network where connections between the units do not form a directed cycle. This is different from recurrent neural networks. The feedforward neural network was the first and simplest type of artificial neural network devised. In this network, the information moves in only one direction, forward, from the input nodes, through the hidden nodes (if any) and to the output nodes. There are no cycles or loops in the network.

A feedforward neural network is a biologically inspired classification algorithm. It consist of a (possibly large) number of simple neuron-like processing units, organized in layers. Every unit in a layer is connected with all the units in the previous layer. These connections are not all equal, each connection may have a different strength or weight. The weights on these connections encode the knowledge of a network. Often the units in a neural network are also called nodes. Data enters at the inputs and passes through the network, layer by layer, until it arrives at the outputs. During normal operation, that is when it acts as a classifier, there is no feedback between layers. This is why they are called feedforward neural networks.



In the following figure we see an example of a 2-layered network with, from top to bottom: an output layer with 5 units, a hidden layer with 4 units, respectively. The network has 3 input units. The 3 inputs are shown as circles and these do not belong to any layer of the network (although the inputs sometimes are considered as a virtual layer with layer number 0). Any layer that is not an output layer is a hidden layer. This network therefore has 1 hidden layer and 1 output layer. The figure also shows all the connections between the units in different layers. A layer only connects to the previous layer.

I. INTRODUCTION

Feedforward neural networks (FF networks) are the most popular and most widely used models in many practical applications. They are known by many different names, such as "multi-layer perceptrons."

Figure 2.5 illustrates a one-hidden-layer FF network with inputs $x^1,...,x^n$ and output $\hat{y}$. Each arrow in the figure symbolizes a parameter in the network. The network is divided into layers. The input layer consists of just the inputs to the network. Then follows a hidden layer, which consists of any number of neurons, or hidden units placed in parallel. Each neuron performs a weighted summation of the inputs, which then passes a nonlinear activation function , also called the neuron function.

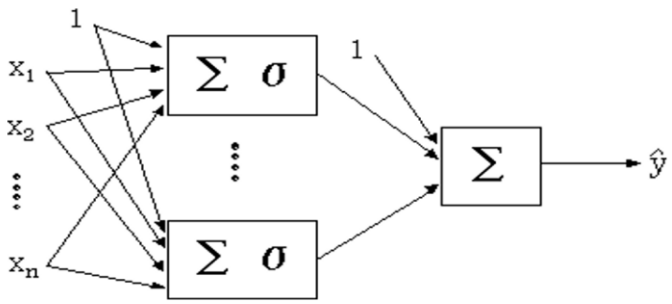


Figure 2.5. A feedforward network with one hidden layer and one output.

Mathematicallv the functionality of a hidden neuron is described by

$$\sigma\left(\sum_{j=1}^{n} w_j x_j + b_j\right)$$

where the weights $\{w_j, b_j\}$ are symbolized with the arrows feeding into the neuron.

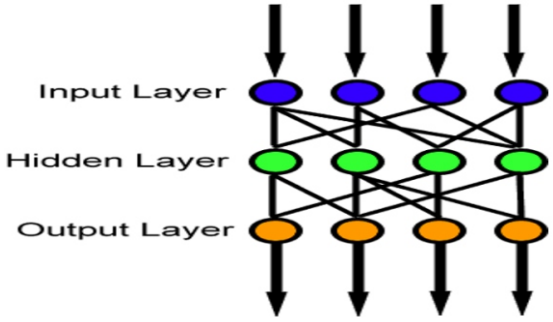
The network output is formed by another weighted summation of the outputs of the neurons in the hidden layer. This summation on the output is called the output layer. In Figure 2.5 there is only one output in the output layer since it is a single-output problem. Generally, the number of output neurons equals the number of outputs of the approximation problem.

The neurons in the hidden layer of the network in Figure 2.5 are similar in structure to those of the perceptron, with the exception that their activation functions can be any differential function. The output of this network is given by

$$\hat{y}(\theta) = g(\theta, x) = \sum_{i=1}^{nh} w_i^2 \sigma\left(\sum_{j=1}^{n} w_{i,j}^1 x_j + b_{j,i}^1\right) + b^2$$

where n is the number of inputs and nh is the number of neurons in the hidden layer. The variables $\{w_{i,j}^1, b_{j,i}^1, w_i^2, b^2\}$ are the parameters of the network model that are represented collectively by the parameter vector$^{\theta}$. In general, the neural network model will be represented by the compact notation g (θ ,x) whenever the exact structure of the neural network is not necessary in the context of a discussion.

2. BRIEF HISTORY:-



In a feed forward network information always moves one direction; it never goes backwards.

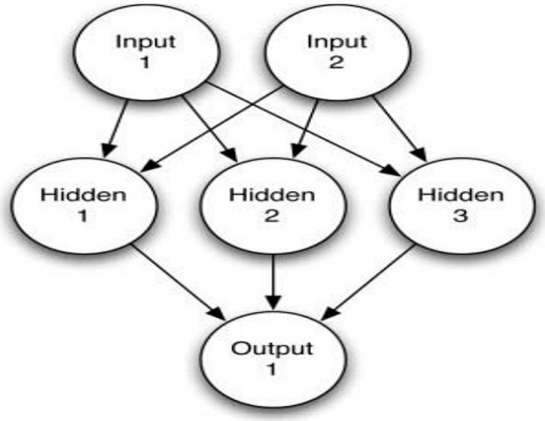
3. FEEDFORWARD NEURAL NETWORK

3.1 Definition

The term, "feed foreword" describes how this neural network processes the pattern and recalls patterns. When using a "feed forward neural network" neurons are only connected foreword. Each layer of the neural network contains connections to the next layer (for example from the input to the hidden layer), but there are no connections back. Feedforward neural network is an interconnection of perceptrons in which data and calculations flow in a single direction, from the input data to the outputs. The number of layers in a neural network is the number of layers of perceptrons.

4. STRUCTURE OF FEEDFORWARD NEURAL NETWORK

In a feedforward neural network, data enters at the inputs and passes through the network, layer by layer, until it arrives at the outputs. During normal operation, that is when it acts as a classifier, there is no feedback between layers. This is why they are called feedforward neural networks. Following figure shows a typical feed forward neural network with a single hidden layer.



4.1. CHOOSING THE NETWORK STRUCTURE

There are many ways that feedforward neural networks can be constructed. The user must decide how many neurons will be inside the input and output layers, and also decide how many hidden layers it is going to have, as well as how many neurons will be in each of these hidden layers. There are many techniques for choosing these parameters. There are some of the general "rules of thumb" that can be used to assist making these decisions. In nearly all cases some experimentation will be required to determine the optimal structure for feedforward neural network.

4.2. THE INPUT LAYER

The input layer to the neural network is the conduit through which the external environment presents a pattern to the neural network. Once a pattern is presented to the input later of the neural network the output layer will produce another pattern. In essence this is all the neural network does. The input layer should represent the condition for which the neural network is trained for. Every input neuron should represent some independent variable that has an influence over the output of the neural network.

4.3. THE OUTPUT LAYER

The output layer of the neural network is what actually presents a pattern to the external environment. Whatever pattern is presented by the output layer can be directly traced back to the input layer. The number of output neurons should directly related to the type of work that the neural network is to perform. To consider the number of neurons to use in output layer one must consider the intended use of the neural network. If the neural network is to be used to classify items into groups, then it is often preferable to have one output neurons for each group that the item is to be assigned into. If the neural network is to perform noisereduction on a signal then it is likely that the number of input neurons will match the number of output neurons.

4.4. THE NUMBER OF HIDDEN LAYERS

There are really two decisions that must be made with regards to the hidden layers. The first is how many hidden layers to actually have in the neural network. Secondly, how many neurons will be in each of these layers. Neural networks with two hidden layers can represent functions with any kind of shape. There is currently no theoretical reason to use neural networks with any more than two hidden layers. Further for many practical problems there's no reason to use any more than one hidden layer. Problems that require two hidden layers are rarely encountered. Differences between the numbers of hidden layers are summarized in following table:

Number o f Hidden Layers	Result
none	Only capable of representing linear separable functions or decisions.
1	Can approximate arbitrarily while any functions which contains acontinuous mapping from one finite space to another.
2	Represent an arbitrary decision boundary to arbitrary accuracy with rational activation functions and can approximate any smooth mapping to any accuracy.

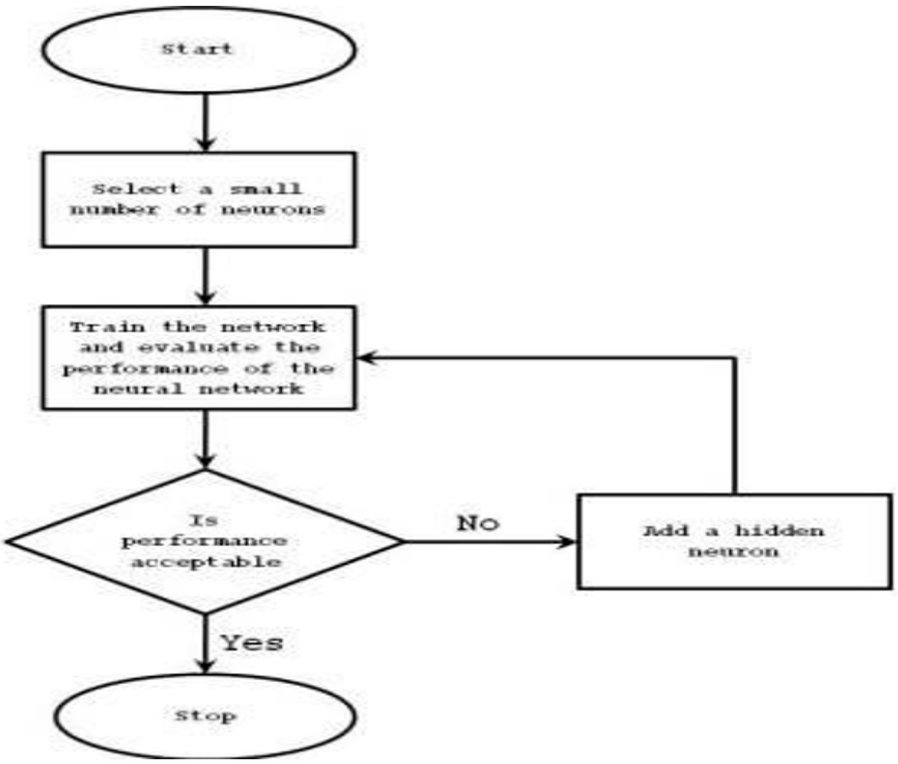
4.5. THE NUMBER OF NEURONS IN THE HIDDEN LAYERS

Deciding the number of hidden neurons in layers is a very important part of deciding the overall neural network architecture. Though these layers do not directly interact with the external environment these layers have a tremendous influence on the final output. Both the number of hidden layers and number of neurons in each of these hidden layers must be considered. Using too few neurons in the hidden layers will result in something called underfitting. Underfitting occurs when there are too few neurons in the hidden layers to adequately detect the signals in a complicated data set. Using too many neurons in the hidden layers can result in several problems. First too many neurons in the hidden layers may result in overfitting. Overfitting occurs when the neural network has so much information processing capacity that the limited amount of information contained in the training set is not enough to train all of the neurons in the hidden layers. A second problemcan occur even when there is sufficient training data. inordinately large number of neurons in the hidden layers can increase the time it takes to train the network. The amount of training time can increase enough so that it is impossible to adequately train the neural network. Obviously some compromise must be reached between too many and too few look neurons in the hidden layers. There are many rule-of-thumb methods for determining the correct number of neurons to use in the hidden layers. Some of them are summarized as follows

- .The number of hidden neurons should be in the range between the size of the input layer and the size of the output layer.

- The number of hidden neurons should be 2/3 of the input layer size, plus the size of the output layer.
- The number of hidden neurons should be less than twice the input layer size.

These three rules are only starting points to consider. Ultimately the selection of the architecture of the neural network will come down to trial and error. But what exactly is meant by trial and error? Nobody wants to start throwing random layers and numbers of neurons at the network. To do so would be very time-consuming. There are two methods that can be used to organize the trial and error search for the optimum network architecture. There are two trial and error approaches that one may use in determining the number of hidden neurons are the "forward" and "backward" selection methods. The first method, the "forward selection method", begins by selecting a small number of hidden neurons. This method usually begins with only two hidden neurons. Then the neural network is trained and tested. The number of hidden neurons is then increased and the process is repeated so long as the overall results of the training and testing improved.The "forward selection method" is summarized in following figure.



The second method, the "backward selection method", begins by using a large number of hidden neurons. Then the neural network is trained and tested. This process continues until about the performance improvement of the neural network is no longer significant. One additional method that can be used to reduce the number of hidden neurons is called pruning. In the simplest sense pruning involves evaluating the weighted connections between the layers. If the network contains any hidden neurons which contains only zero weighted connections, they can be removed. Pruning is a very important concept for neural networks.

5. OPERATION

The operation of this network can be divided into two phases:

5.1. THE LEARNING PHASE

The feedforward network uses a supervised learning algorithm: besides the input pattern, the neural net also needs to know to what category the pattern belongs. Learning proceeds as follows: a pattern is presented at the inputs. The pattern will be transformed in its passage through the layers of the network until it reaches the output layer. The units in the output layer all belong to a different category. The outputs of the network as they are now are compared with the outputs as they ideally would have been if this pattern were correctly classified: in the latter case the unit with the correct category would have had thelargest output value and the output values of the other output units would have been very small. On the basis of this comparison all the connection weights are modified a little bit to guarantee that, the next time this same pattern is presented at the inputs, the value of the output unit that corresponds with the correct category is a little bit higher than it is now and that, at the same time, the output values of all the other incorrect outputs are a little bit lower than they are now. (The differences between the actual outputs and the idealized outputs are propagated back from the top layer to lower layers to be used at these layers to modify connection weights. This is why the term backpropagation network is also often used to describe this type of neural network. The time for learning phase depends on the size of the neural network, the number of patterns to be learned, the number of epochs, the tolerance of the minimizer and the speed of your computer, how much computing time the learning phase may take.

5.2. BACKPROPAGATION

Backpropagation is the most commonly implemented training procedure for feedforward neural networks. Its primary objective is to provide a mechanism for updating connected neurons based upon minimization of error. To accomplish this, gradient descent is generally used to determine the steepest path toward the minimum of

$$E(\vec{w}) = \frac{1}{2} \sum_{d \in D} (t_d - o_d)^2$$

where d is a training instance in D, td is the target value, od is the output value, and $\vec{w}$ is the weight vector.

Backpropagation requires determining an error by first feedfowarding inputs into the network and subtracting the result from some target output. This difference is then multiplied by the derivative of the neuron's activation function -- in the case of the sigmoid, this is f'(net) = o(1 − o) -- and stored for

reference by the update at the preceding layer. We can now proceed to make error calculations layer-by-layer by traversing backward through the network and performing the neuron's error computation, which is the derivative of the neuron activation function multiplied by the sum of each output weight's multiplication with the forward neuron's error term. After each error term is calculated, we update the weights by the multiplication of each branch's output with the forward node's error and the learning rate. [Charles Nugent]

5.3.THE CLASSIFICATION PHASE

In the classification phase, the weights of the network are fixed. A pattern, presented at the inputs, will be transformed from layer to layer until it reaches the output layer. The classification can occur by selecting the category associated with the output unit that has the largest output value.In contrast to the learning phase classification is very fast.

6. APPLICATIONS

Feedforward neural network, part of artificial neural network, has broad applicability to real world business problems. In fact, they have already been successfully applied in many industries. Since the network is best at identifying patterns or trends in data, it is well suited for prediction or forecasting needs including: sales forecasting, industrial process control, customer research, data validation, risk management, target marketing.

It is also used following specific paradigms: recognition of speakers in communications; diagnosis of hepatitis; recovery of telecommunications from faulty software; interpretation of multi meaning Chinese words; undersea mine detection; texture analysis; three- dimensional object recognition; hand-written word recognition; and facial recognition.

It is a 'hot' research area in medicine and it is believed that it will receive extensive application to biomedical systems in the next few years. It is ideal in recognising diseases using scans since there is no need to provide a specific algorithm on how to identify the disease. It learns by example so the details of how to recognize the disease are not needed. What is needed is a set of examples that are representative of all the variations of the disease. The quantity of examples is not as important as the 'quantity'. The examples need to be selected very carefully if the system is to perform reliably and efficiently.

REFERENCES

[1]. http://www.wikipedia.org/neuralnetwork
[2]. http://www.studymode.com/neuralnetwork
[3]. http://www.fon.hum.uva.nl/praat/manual/Feedforward_neural_networks.html.Retrieved
[4]. Jeff Heaton,2008. Introduction to Neural Networks for Java, 2nd Edition,Heaton Research, Inc. ISBN:1604390085 9781604390087

"Implications Of Network Neutrality In The Light Of Make In India Digital Drive"

Ms. Ankita Jain[1], Ms. Vandana Gablani[2]

[1]Assistant Professor, Delhi School of Professional Studies & Research, New Delhi

[2] Assistant Professor, Delhi School of Professional Studies & Research, New Delhi

ABSTRACT

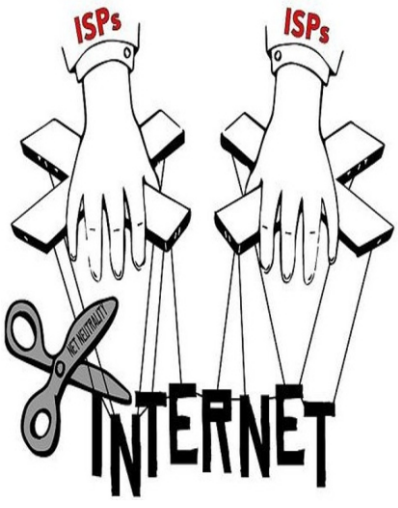
Internet is everywhere, without it no organization can think of business in this fast moving world where survival of the fittest in the world market finds itsnichewith the delivery of not only right information to right person at right time and place but also the dissemination of information over the internet should be impartial i.e. Network Neutrality or Net Neutrality.[1] Network neutrality is the principle that all Internet traffic should be treated equally.[2] According to Columbia Law School professor Tim Wu, the best way to explain network neutrality is as when designing a network: "that a public information network will end up being most useful if all content, sites, and platforms are treated equally."[3]

This paper discusses about the implications of the network neutrality in the light of the Make in India digital drive. In other words, the objective is to discuss whether the dream of making India, truly a digital India as part of Make in India project will be successful if all theinternet service providers in India give their customers equal access to all lawful websites and services on the Internet, without giving priority to any website over another.

Keywords: Digital India, Net Neutrality, Make in India, Internet for all, Save the Internet

I. INTRODUCTION

Should the Net Be Neutral?



This very hot debate took its very first flight when a survey of operator practices in US was conducted in 2002.[4] In that year, evidence of a discrimination problem became clear from several sources, including consumer complaints about operators who ban classes of applications or equipment, like servers, Virtual Private Networks, or Wi-Fi devices[5], and in filings at the Federal Communications Commission by application developers.[6]The survey advised that operators indeed

had implemented significant contractual and architectural limits on certain classes of applications. Operators showed an unfortunate tendency to ban new or emerging applications or network attachments, like Wi-Fi devices or Virtual Private Networks, perhaps out of suspicion or an (often futile) interest in price discrimination. On the whole the evidence suggested that the operators were often pursuing legitimate goals, such as price discrimination and bandwidth management. The problem was the use of methods, like bans on certain forms of applications, which were likely to distort the market and the future of application development[7]

GLOBAL THREATS TO NET NEUTRALITY

In the light of the foregoing facts and the possible threat to the Internet with regards to its unbiased use globally, many rules were made and adopted but the latest rules adopted by the Federal Communications Commission[8] on February 26, 2015 – the FCC's Open Internet rule gave strongest ground as far as legal foundations are concerned. The new rules will protect no matter how they access the internet-over mobile or desktop computer.

FEW OF THE GLIMPSES OF ABOVE SAID RULES[9]

No Blocking:
Broadband providers may not block access to legal content, applications, services, or non-harmful devices.

No Throttling:
Broadband providers may not impair or degrade lawful Internet traffic on the basis of content, applications, services, or non-harmful devices.

No Paid Prioritization:
Broadband providers may not favor some lawful Internet traffic over other lawful traffic in exchange for consideration of any kind—in other words, no "fast lanes." This rule also bans ISPs from prioritizing content and services of their affiliates.

To ensure an open Internet now and in the future, the Open Internet rules also establish a legal standard for other broadband provider practices to ensure that they do not unreasonably interfere with or disadvantage consumers' access to the Internet. The rules build upon existing, strong transparency requirements. They ensure that broadband providers maintain the ability to manage the technical and engineering aspects of their networks. The legal framework used to support these rules also positions the Commission for the first time to be able to address issues that may arise in the exchange of traffic

between mass-market broadband providers and other networks and services. But policy makers in other regions of the world like Europe and India are on the track of making new rules that could threat the net neutrality. Few months back, the European Council, which is made up of the 28 national governments of European Union members, adopted a proposal that would allow telecom companies to charge Internet businesses like Google fees to deliver their content to the users faster as compared to smaller companies that could not afford to pay that preferential payment.

NET NEUTRALITY: THE INDIAN AMBIENCE

The topic of "net neutrality" came to spotlight in India in December 2014 when Airtel, a mobile telephony service provider announced the additional charges for making voice calls from its network using apps like Watsapp, Facebook, Skype etc[10] . However, the issue of net neutrality started creeping in 2006 itself when TRAI published a paper on it by inviting options from stakeholders whether regulatory inventions are required or left to market force.[11] Bharti Airtel's Director of Network Services, Jagbir Singh in July 2012, recommended that large Internet companies like Facebook and Google should contribute a part of their revenues to telecom companies. According to him, Internet companies were enjoying huge profits from small investments, whereas the telecom companies were actually investing in building networks. This move of Airtel faced harsh criticism on social networking sites due to which later on 29 December 2014, Airtel announced that it would not be implementing planned changes, pointing out that TRAI would be soon releasing a consultation paper on the issue.[12] On 27 March 2015, TRAI released a consultation paper on over-the-top services (OTT) and net neutrality for public feedback.[13][14] The last date for submission of comments was 24 April 2015 and TRAI received over a million emails.[15] Another scheme that violates net neutrality is launching of Internet.org in India with Reliance Communications by Facebook in February 2015 that aims to provide free access to 38 websites through an app.[16] To add to this list in April 2015, Airtel announced "Airtel zero" scheme under which if an app sign contract with them then Airtel will provide that app free of cost to it's customer.[17] Flipkart decided to join the scheme but again due to negative response from the public and being criticized for its action it pull out its hand from this scheme. All these schemes time and again has breached the net neutrality in India.

LITERATURE REVIEW

Bruce M. Owen has enlightened in his paper on "The Net Neutrality Debate" [18] that regulator and regulations have time and again been obstacle in the path of technological innovation as it gives power to the present producers by preventing entry of new competitors, which in turn reduces incumbent's

own enticement to innovate. According to him, sad history of failure of attempts to regulate old AT&T under traditional utility regulation principle should be an eye opener for us that the "net neutrality" remedy is a cure far worse than the feared disease.

Robin S. Lee and Tim Wu in their paper on "Subsidizing Creativity through Network Design: Zero-Pricing and Net Neutrality"[19] emphasized on the theory of two-sided market which suggests the de-facto ban on termination fees on the content providers by the Internet service Providers and hence supports the zero- pricing aspect of net neutrality. The theory of two-sided markets provides bedrock for the skyscraper building of new content and spurs innovation while avoiding crumbling of the Internet.

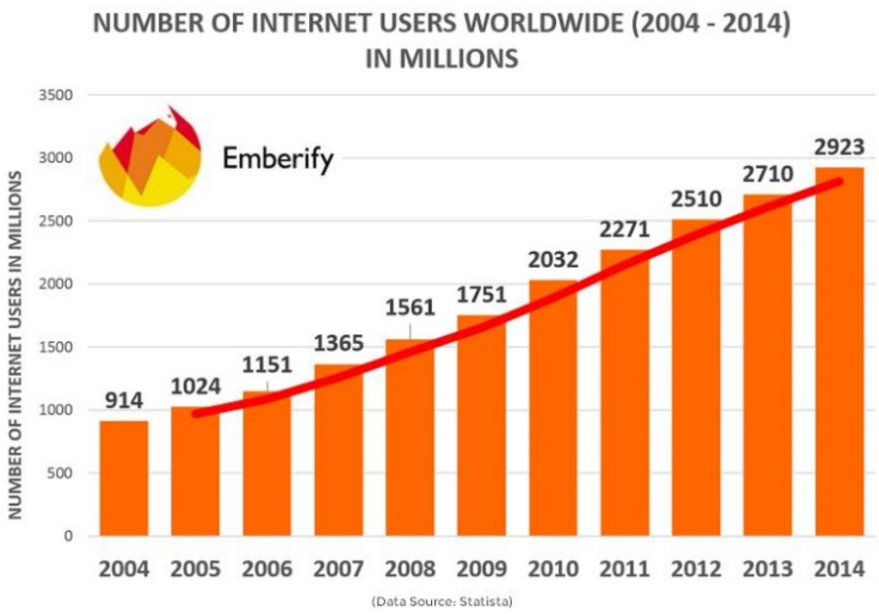
H.Kenneth Cheng, Hong Guop and Subhajyoti in the paper "The Debate on Net Neutrality: A Policy Perspective"[20] found that if the net neutrality concept is removed the broadband service providers will be on gaining side because they will be able to extract preferential fees rom the content providers. Also, incentive to expand infrastructure capacity for broadband service provider under the umbrella of net neutrality are higher than the no neutrality regime as under net neutrality broadband service provider always invest in broadband infrastructure at socially optimum level but either under-or –over invests in infrastructure in absence of it.

Not much research has been conducted in this so far because it is one of the latest issue that has come into limelight, thus having a great scope of further studies with the suggestions of its implementation and its impact over the Indian Economy.

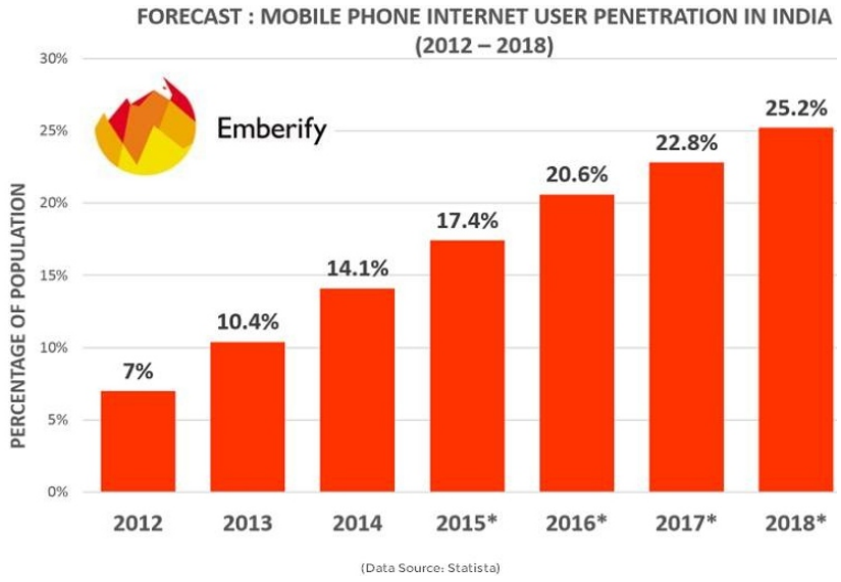
NET NEUTRALITY: THE REAL STAKEHOLDERS

A THREAT TO THE START-UP ECOSYSTEM

Startups are taking India by storm and galvanizing the picture of India in global market. All this is because of the vast customer that they can pitch through the internet. Beauty of internet is that anyone with a computer and an internet connection can start his own business and reach the new heights in Business world. Firstly, the number of Internet users in the world is on a steady rise. If we look at the statistics from 2004 up to 2014, we see that the number of users has been growing at a tremendous pace. As of 2014, the number of Internet users worldwide stood at 2.92 billion people, up from 2.71 billion in 2013. [21]



Shifting the focus to India now, where the topic of net neutrality is still trending, there's been a rise in the mobile phone Internet user penetration share. From a statistic of 7% in 2012, a figure of 14.1% was attained in just two years. It is projected that in 2015, 17.4% of the total population in India will use mobile Internet, and this number will grow to about 25.2% by 2018.[21]



To sum it up, we can see that world is embracing internet like never before, which signifies its importance for the small business and start-ups to make their online presence vital. Without net neutrality all the innovation will take back seat and ideas will no longer be turned into reality resulting into crushed ambitions of millions of young entrepreneurs. Net Neutrality is of the utmost importance for small business owners, startups and entrepreneurs, who can simply launch their businesses online, advertise the products and sell them openly, without any discrimination on the basis of cost or speed.As India's vibrant entrepreneurial ecosystem is emerging, it would do well to understand the role of startups and create support for them to succeed with first and foremost requirement of providing them a fair playing field which is possible only through net neutrality.

A THREAT TO DIGITAL MARKETING

Digital marketing is so powerful because the Internet has removed the middle man. Earlier, with traditional marketing medium; the evil media company was in the middle of the business owner and the customers. Business owners had to pay the media companies an advertising fee to reach the audience. The medias – TV, Radio, Newspaper and Magazines had access to the audience and they guarded it well. The Internet enabled the business owner to reach the customer directly for free using content marketing or at a very low cost using Marketing. Now the middle man wants to come back. This time it is not the media companies but the ISPs who control access to the audience. They are going to set the rules. With such an ecosystem only the people who already have the money will be able to have the reach they want. A group of 3-4 people wanting to innovate from a small room in Bangalore cannot compete with the big giants. The playing field will not be level again. Without innovation from small timers, there is no competition. Without competition, there is no innovation in big companies. In the end, we will end up paying more for mediocre products and services and disruptive innovation which has been improving our lives will come to a grinding halt.

A THREAT TO DIGITAL INDIA PLAN

Honorable Prime Minister Mr. Narendra Modi spoke extensively of his vision for Digital India, a program to transform India into digital empowered society and knowledge economy It would ensure that government services are available to citizens electronically. It would also bring in public accountability through directive delivery of government's services electronically. This will be for preparing the India for the knowledge based transformation and delivering good governance to citizens by synchronized engagement with both Central Government and State Government. Digital India's main objective is to provide an equal platform of opportunities and bringing citizens to same level by digitally connecting them and creating a digitally empowered society which can be possible only through unbiased internet.

The main ongoing highlights of Digital India campaign are: [22]

1. The programme aims to widespread the use of internet to each nook and corner of India by providing the coverage to 2.5 lakh Gram panchayats by the end of December 2016 and by turning 1.5 lakh post offices into multi-service centers. At the same time, it will be ensured that 2.5 lakh schools get facilitated with the free wifi services and there are web-based platforms to encourage “2-way communication” between government and public.

2. Mobile coverage is being provided for 42,300 remote villages of India for supporting the ongoing effort of increasing network coverage in the country and to fill the gaps.

3. The era of "e-governance" is being introduced with this campaign by implementing methods like "online applications and tracking", "use of online repositories", "use of Payment gateway platforms" and using IT to automate different government processes and reduce paper work.

4. Other small projects under this campaign which are being run are wi-fi in universities, free wi-fi spots at tourist centers and in cities with population greater than 1 million,etc.The question arises, is all this possible without net neutrality???

As we can see that for all these objectives of "Digital India" campaign internet is the prime requirement. And internet without net neutrality is handicapped in fulfilling the above goals. The net neutrality can only ensure the success of "Digital India" drive. If all the 2.5 lakh Gram panchayats have the internet provision but they have to pay the price for accessing websites on it then what's the use of such facility made available to them??? We have to ensure net neutrality so that each and everyone should be able to get benefitted from the internet services and be able to freely explore the world of internet for his use.Almost all of the above have net neutrality as their backbone. Digital India campaign depends on "high-speed" internet for its success as it is the core utility with which National Telecom Policy 2012 envision providing affordable and reliable broadband on demand by 2015 and 175 million broadband connections by 2017. A web economy that will enhances affordability and increased access and delivery of multiple services at reduce cost is not possible without a neutral internet.

CONCLUSION

Technology, in both its evolutionary form and in its revolutionary form, has changed our lives drastically. India is on the path of development wherein with the campaign like Digital India its image is being projected as one of the emerging superpower country in the world. Today there is much excitement and expectation about the advent of Digital India—a major initiative of the government to transform the country into a digitally empowered society—which is centered on three key areas of digital infrastructure as a utility to every citizen, governance and services on demand, and digital empowerment of citizens. However, where are we today? Voice connectivity is only about 60% and data penetration far lower at about 20%. Digital India is closely connected to Net Neutrality. Net neutrality can only ensure the fulfillment of the dream of Digital India which aims taking India forward on the path of development.Net neutrality framework promotes and protects the innovation. In recent times, some of the products and services that have transformed the way we live, such as Tablets, smart

phones, the Internet, social media etc., have been a result of revolutionary innovation. Innovation is the backbone of start-ups and they are in turn one of the major role player in the development of Indian Economy. Net neutrality will facilitate Digital India plan.

REFERENCES

[1] The term coined by Columbia University media law professor Tim Wu in 2003, as an extension of the longstanding concept of a common carrier.

[2] Honan, Matthew (12 February 2008). "Inside Net Neutrality: Is your ISP filtering content?"

[3] Wu, Tim. "Network Neutrality FAQ"

[4] Wu, Tim (23 April 2005). "Network Neutrality, Broadband Discrimination"

[5] Complaints about restrictions on broadband applications like filesharing applications or VPNs are common on discussion forums like DSL Reports. See, e.g., broadband reports,at http://www.dslreports.com /forum/remark,3775421;mode=flat;root=sware(July2002)-Retrieved June 07, 2015.

[6] See Comments of the High Tech Broadband Coalition, In re: Inquiry Concerning High-Speed Access to the Internet Over Cable and Other Facilities (filed June 18, 2002), available at http://www.itic.org/policy/fcc_020618.pdf; see also FCC Ex Parte Letter, Aug. 22 2003, available at http://faculty.virginia.edu/tim wu/wu_lessig_fcc.pdf.

[7] Wu, Tim (23 April 2005). "Network Neutrality, Broadband Discrimination"

[8] An independent U.S. government agency overseen by Congress, the commission is the United States' primary authority for communications law, regulation and technological innovation.

[9] https://www.fcc.gov/openinternet Retrieved on June 08, 2015

[10] " What Net Neutrality?". NDTV. 24 December 2014. Retrieved 24 December 2014.

[11] "What is net neutrality and why it is important". The Times of India. 20 January 2014. Retrieved29 September 2014.

[12]" Airtel drops plans to charge extra for internet voice calls". The Hindu. 29 December 2014. Retrieved1 January 2015.

[13] " TRAI seeks views on net-neutrality". The Hindu. 27 March 2015. Retrieved 27 March 2015.

[14] " Consultation Paper On Regulatory Framework for Over - the - top (OTT) services" (PDF). Telecom Regulatory Authority of India. 27 March 2015. Retrieved 27 March2015.

[15] " Trai publishes email IDs of netizens, site hacked". Deccan Chronicle. 28 April 2015. Retrieved4 May 2015.

[16] Union minister Ravi Prasad tweets about net neutrality, says committee to look into matter". DNA India. 8 April 2015. Retrieved 8 April 2015.

[17] "Airtel Zero: Another blow to net is net neutrality is only for airtel users..?/?neutrality". The Times of India. 6April 2015. Retrieved 6 April 2015.

[18] The Net Neutrality Debate: Twenty Five Years after United States v. AT&T and 120 Years after the Act to Regulate Commerce Bruce M. Owen

[19] Subsidizing Creativity through Network Design: Zero-Pricing and Net Neutrality Journal of Economic Perspectives—Volume 23, Number 3—Summer 2009—Pages 61–76

[20] The Debate on Net Neutrality: A Policy Perspective Department of Decision and Information SciencesWarrington College of Business Administration University of Florida Gainesville, FL 32611-7169 U.S.A.

[21] Net Neutrality and its Impact on Startups | Emberify Blog

[22] http://www.youthkiawaaz.com/

Instructions for Authors

Essentials for Publishing in this Journal

1 Submitted articles should not have been previously published or be currently under consideration for publication elsewhere.

2 Conference papers may only be submitted if the paper has been completely re-written (taken to mean more than 50%) and the author has cleared any necessary permission with the copyright owner if it has been previously copyrighted.

3 All our articles are refereed through a double-blind process.

4 All authors must declare they have read and agreed to the content of the submitted article and must sign a declaration correspond to the originality of the article.

Submission Process

All articles for this journal must be submitted using our online submissions system. http://enrichedpub.com/ . Please use the Submit Your Article link in the Author Service area.

Manuscript Guidelines

The instructions to authors about the article preparation for publication in the Manuscripts are submitted online, through the e-Ur (Electronic editing) system, developed by **Enriched Publications Pvt. Ltd**. The article should contain the abstract with keywords, introduction, body, conclusion, references and the summary in English language (without heading and subheading enumeration). The article length should not exceed 16 pages of A4 paper format.

Title

The title should be informative. It is in both Journal's and author's best interest to use terms suitable. For indexing and word search. If there are no such terms in the title, the author is strongly advised to add a subtitle. The title should be given in English as well. The titles precede the abstract and the summary in an appropriate language.

Letterhead Title

The letterhead title is given at a top of each page for easier identification of article copies in an Electronic form in particular. It contains the author's surname and first name initial .article title, journal title and collation (year, volume, and issue, first and last page). The journal and article titles can be given in a shortened form.

Author's Name

Full name(s) of author(s) should be used. It is advisable to give the middle initial. Names are given in their original form.

Contact Details

The postal address or the e-mail address of the author (usually of the first one if there are more Authors) is given in the footnote at the bottom of the first page.

Type of Articles

Classification of articles is a duty of the editorial staff and is of special importance. Referees and the members of the editorial staff, or section editors, can propose a category, but the editor-in-chief has the sole responsibility for their classification. Journal articles are classified as follows:

Scientific articles:

1. Original scientific paper (giving the previously unpublished results of the author's own research based on management methods).

2. Survey paper (giving an original, detailed and critical view of a research problem or an area to which the author has made a contribution visible through his self-citation);

3. Short or preliminary communication (original management paper of full format but of a smaller extent or of a preliminary character);

4. Scientific critique or forum (discussion on a particular scientific topic, based exclusively on management argumentation) and commentaries. Exceptionally, in particular areas, a scientific paper in the Journal can be in a form of a monograph or a critical edition of scientific data (historical, archival, lexicographic, bibliographic, data survey, etc.) which were unknown or hardly accessible for scientific research.

Professional articles:

1. Professional paper (contribution offering experience useful for improvement of professional practice but not necessarily based on scientific methods);
2. Informative contribution (editorial, commentary, etc.);
3. Review (of a book, software, case study, scientific event, etc.)

Language

The article should be in English. The grammar and style of the article should be of good quality. The systematized text should be without abbreviations (except standard ones). All measurements must be in SI units. The sequence of formulae is denoted in Arabic numerals in parentheses on the right-hand side.

Abstract and Summary

An abstract is a concise informative presentation of the article content for fast and accurate Evaluation of its relevance. It is both in the Editorial Office's and the author's best interest for an abstract to contain terms often used for indexing and article search. The abstract describes the purpose of the study and the methods, outlines the findings and state the conclusions. A 100- to 250-Word abstract should be placed between the title and the keywords with the body text to follow. Besides an abstract are advised to have a summary in English, at the end of the article, after the Reference list. The summary should be structured and long up to 1/10 of the article length (it is more extensive than the abstract).

Keywords

Keywords are terms or phrases showing adequately the article content for indexing and search purposes. They should be allocated heaving in mind widely accepted international sources (index, dictionary or thesaurus), such as the Web of Science keyword list for science in general. The higher their usage frequency is the better. Up to 10 keywords immediately follow the abstract and the summary, in respective languages.

Acknowledgements

The name and the number of the project or programmed within which the article was realized is given in a separate note at the bottom of the first page together with the name of the institution which financially supported the project or programmed.

Tables and Illustrations

All the captions should be in the original language as well as in English, together with the texts in illustrations if possible. Tables are typed in the same style as the text and are denoted by numerals at the top. Photographs and drawings, placed appropriately in the text, should be clear, precise and suitable for reproduction. Drawings should be created in Word or Corel.

Citation in the Text

Citation in the text must be uniform. When citing references in the text, use the reference number set in square brackets from the Reference list at the end of the article.

Footnotes

Footnotes are given at the bottom of the page with the text they refer to. They can contain less relevant details, additional explanations or used sources (e.g. scientific material, manuals). They cannot replace the cited literature.
The article should be accompanied with a cover letter with the information about the author(s): surname, middle initial, first name, and citizen personal number, rank, title, e-mail address, and affiliation address, home address including municipality, phone number in the office and at home (or a mobile phone number). The cover letter should state the type of the article and tell which illustrations are original and which are not.

Notes: