iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** XII **Month of publication:** December 2017

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor :6.887
Volume 5 Issue XII December 2017- Available at www.ijraset.com

Developing a Security Model for VANET using cloud Computing

Rajapraveen.k.N[1], Dr.Tulika[2]
[1, 2] *Department of CS & IT, SHUATS*

Abstract: ***VANET (Vehicular ad-hoc networks) has become a significant research area due to its specific features and applications such as standardization and road safety. In VANET vehicles onboard units are deployed with computing facilities and storage systems for relatively free communication among the nodes. Hence several technologies are enhanced to promote intelligent transport system. We develop an application called vehicular cloud computing. Vehicular cloud computing is a new technology that has a remarkable impact on traffic management and road safety by instantly using vehicular resources, such as computing, storage and internet, in this we develop a security parameter in VANET using cloud computing technology.***
Keywords: **Cloud VANET, vehicular cloud computing, vehicular cloud, VANET Cloud, vanet cloud application Introduction**

I. INTRODUCTION

VANET (vehicular ad-hoc networks) is a communication technology developed for better traffic management. VANET is a set of moving vehicles in a dynamic environment, her we develop a safety application using cloud computing technology called cloud VANET, Cloud computing is an emerging IT environment that has significantly transformed everyone's vision of computing infrastructure, development models, and software distribution. The enhancement of cloud vanet application is to provide certain security parameters for authenticity of vehicle and user of the vehicle, development of cloud vanet(CV) is to travel securely in VANET environment, but not for the purpose of communication among the nodes or vehicles.

VANET Communication specifies certain standards, Here front vehicle can able to communicate with rear vehicle regarding maintains of distance, warning messages in case of any violation, The communication between vehicles to vehicle is exchanged via DSRC (Dedicated short range communication) Standards[1]. Each vehicle can communicate with other vehicle using short radio signals DSRC (5.9 GHz) for range can reach 1km.

A. Features of VANET & CLOUD Computing

Vehicular ad hoc network: are different from other ad hoc networks because VANETs are of their hybrid architecture, dynamic in nature and node movement. Vanet is the integration of ad hoc networks, wirelesses LAN, cellular technology for intelligent transport system –all work together in VANET, address routing is the most important of all. VANET can employ vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications for advanced notification of traffic events. In support of traffic-related communications, short-range communications [2].

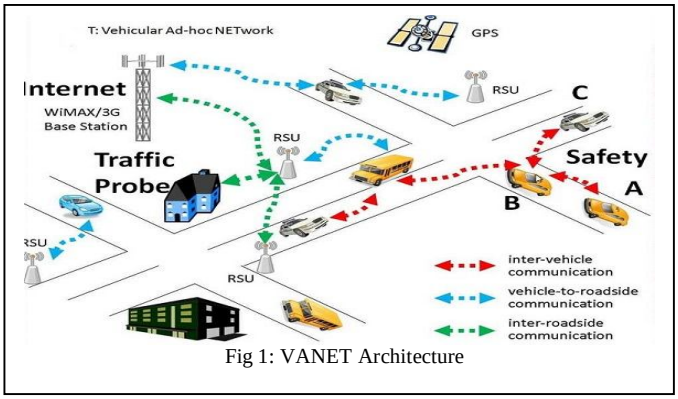


Fig 1: VANET Architecture

B. Vanet Characteristics

Highly dynamic topology: The high speed of the vehicles along with the availability of choices of Multiple Paths defines the dynamic topology of VANETs.

Frequent disconnected network: The high speed of the vehicles in one way defines the dynamic topology whereas on other hand necessitates the frequent requirements of the roadside unit lack of which results a frequent disconnections.

1) *Cloud Computing:* Cloud computing is the pool of resources , notion of cloud computing started from the realization of the fact that instead of investing in infrastructure, businesses may find it useful to rent the infrastructure and sometimes the needed software to run their applications. One major advantage of cloud computing is its scalable access to computing resources. With cloud computing developers do not need large capital outlays in hardware to deploy their service for internet applications and services. Keeping the noble benefit of cloud computing, the idea of Vehicular Cloud (V-Cloud) comes into focus [2] Modern cars are equipped permanently connected with internet, featuring substantial on-board unit computational, storage, and sensing capabilities which can be thought as a huge farm of computers while their substantial amount of stay on the road[3]. As on the road most of these facilities remain idle, if we can able to use these computational facilities it will benefits the user(vehicle user)[4][5].

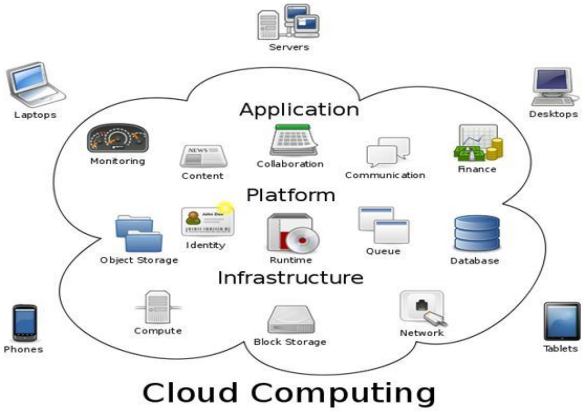


Fig 2: Cloud Computing

II. PROPOSED IDEA FOR SECURITY APPLICATION FOR VANET USING CLOUD COMPUTING:

In this proposed concept security application is developed for VANET, using cloud computing technology. in the enhancement of CLOUD VANET application the security features are established for authenticity, not for communication among the nodes or vehicles because Vehicular ad-hoc networks (VANET) is decentralized architecture and dynamic nature and it don't supports the centralized system for communication.

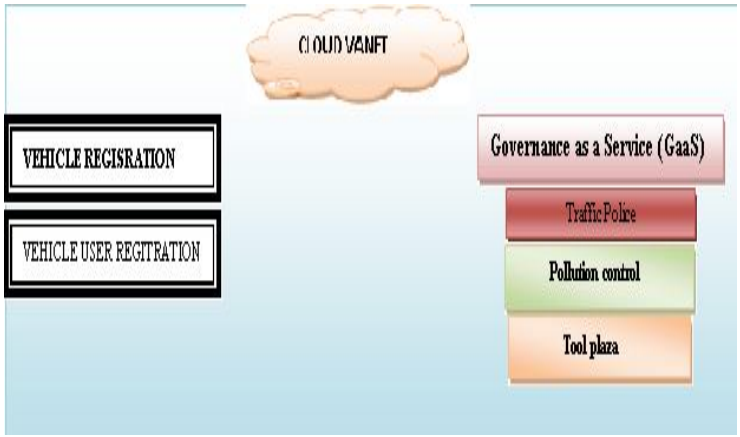


Fig 3: Functioning of Cloud Vanet

The development of secure vanet application introduces a model called cloud vanet. In cloud vanet(CV) centralized authenticating process is established, in this process a central traffic governing system is introduced called central governance as a service(GaaS).

A. Working Procedure Cloud vanet (Governance as a Service)Gaas

Cloud vanet (CV) is under the control of centralized governing system called governance as a service (Gaas).

1) Working Principals of (Gaas)

Location update information: Governance as a service (Gaas) or Admin updates the predefined information about every GPS location. For example: if the location is "1" GaaS will update the complete detailed information about the location "1" stating that Same scenario will continues in location 2, 3 etc..

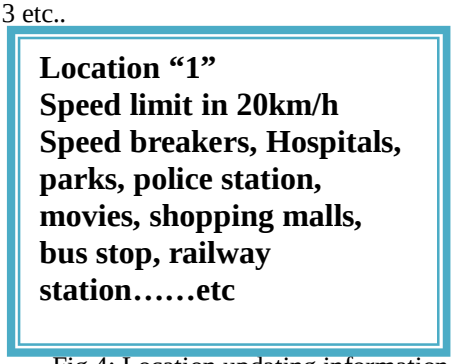


Fig 4: Location updating information

B. Block/Release Vehicle ID: Admin can able to block/release the vehicle ID

A.If the vehicle is thiefted, the user of the vehicle will pass a complaint to block the vehicle ID. Due to the reason the cloud vanet resources (GaaS) got disabled until the block released.

B.If any vehicle found misbehaving in the cloud VANET environment Admin will block the Vehicles ID.

1) *Block/Release User ID:* Admin can able to block/release the vehicle ID If Admin found any misbehaving user in cloud vanet environment the user id will be blocked, to disable the resources of cloud vanet.
2) *Complaints list:* admin will get complains from various users regarding the problem faced by them in the vanet environment. The list of complaints will be displayed in the complaint box
3) *Vehicle Authenticity:* vehicle will get registered in to cloud vanet with its vehicle unique identity number + vehicle number +vehicle engine number.
4) *User Authenticity:* user will get registered with his user unique identity number + biometric key, user driving license and bank account details.User login into cloud vanet to avail governance as a service (GaaS) resources, authenticity of every user is established through biometric key, and with the help of driving license number the entire information about the user is linked with cloud vanet , user bank account details linked with cloud vanet(GaaS) if any fault tolerance happens with concern user the fine will be imposed immediately through GAAS and amount from linked bank account will be reduced or debited. Google maps for navigation and gps location are established to know the information about location and navigation.
5) *Resource request message:* Resource request message will sends to GaaS or Admin from user to get predefined information from cloud vanet regarding GPS specific location.
6) *For example:* if user wants to retrieve predefined information from cloud vanet, user enters the Concern GPS location name. The predefined information will be retrieved.
7) *Location information update:* user "1" found any accidents occurrences in the location "A", user "1" will update the information to the cloud vanet notification center.
8) *Notification Center:* notification center is nothing but the information hub, the information regarding road status and postcrush, precrush and road conjunction information is displayed in notification center with user id and time stamp, this can be accessible by every cloud vanet user. If user wants to know the information about the location"A" in notification center, updated information will be displayed.
9) *Complaint to (GAAS):* if user "2" found any false information updated by user "1" in the notification center about the concern location "A", the user "2" will file a complaint to cloud vanet(GAAS) , necessary action will be taken by GAAS.
10) *Traffic Police (GAAS):* traffic police governance as a service, if any user going against to traffic rules, traffic police can able to impose fine immediately. The fine amount will be debited from user bank account automatically.
11) *Pollution control Authority (GAAS):* pollution control authority governance as a service, if any vehicle emitting huge pollution more than the limit and the vehicle is out dated, then pollution control authority will impose fine to concerned user, the fine amount will be debited from user bank account automatically. PCAGAAS can able to block the vehicle identity to stop the cloud vanet resources.

III. DEVELOPING A SECURITY PARAMETERS USING CRYPTOGRAPHIC ENCRYPTION & DECRYPTION PROCESS

The above security model is developed for vanet using cloud computing is enhanced by strong cryptographic encryption and decryption process.

To deploy the security parameters we enhanced visual cryptography technology. Visual cryptography is a cryptographic technique that enhances the encryption of images

Here we propose the model of encryption of both images and text information as well, Here we enhance , 2 out of 2 visual cryptography schemes based on pixel expansion m=2 in detail. Visual cryptography enables the secure transmission of images in open and insecure environment; Scheme explained in this paper is based on k out of k visual cryptography scheme. To prevent the discloser of the information by forming copy of the first share randomization of sub pixel is performed on the shares. One single share cannot reveal the information. To extract the confidential information both the shares are needed to superimpose one on another. We provide (2, 2) Visual Cryptography (VC) in detail for black and white image based on pixel expansion scheme.

In day to day life internet and World Wide Web plays very important role in facilitating and sharing of information over the network. In this open environment the transfer of information should be authentic to prevent hacking of information from unknown source. Researchers have proposed and implemented several security parameters. Various text security methods and algorithms are proposed for secure communication. Likewise RSA, Asymmetric Encryption System, Data Encryption Standard (DES), and Triple Data Encryption Standard (3DES) all these algorithms hold lot of encryption and decryption computation.

A. Basic Model Of Visual Cryptography

Each and every pixel of image 'I' is denoted by 'm' (m =2) and each sub pixels of 'n' ("n=2 in each case") two shared images.

The structure of each and every shared image is enhanced by Boolean matrix 'S',

where S=[Sij] an [n x m] ([2 X 2])matrix Sij=1

if "Jth" sub pixel in the "Ith" share is black "Sij=0"

if the Jth sub pixel in the Ith share is white.

Shares are completely stacked together with confidential images; size can be increased by 'm' times. Here grey level of each and every pixel in the reconstructed image is proportional to the hamming weight H(V) of the OR – ed Vector 'V',

Vector 'V' is the stacked sub pixels [5] for each and every original pixel.

black pixel matrix is denoted by "C0", to encrypt a black pixel randomly select one of the matrices from "C0", white pixel matrix is denoted with"C1" , encrypt a white pixel and randomly select one of the matrices from C1 where C0 = {all the matrices obtained by permuting the columns of [1 0; 1 0]} C1 = {all matrices obtained by permuting the columns of [1 0; 0 1]}; difference in image contrast of the original confidential image, confidential image enhanced after overlapping of the shares is given by 'α', relative difference in the white and black pixel of the reconstructed image.

IV. TWO-BY-TWO VISUAL CRYPTOGRAPHY SCHEME WITH PIXEL EXPANSION

Visual cryptography is a cryptographic technique scheme based on pixel expansion. Image 'I' the confidential image will be encoded as a binary string, where "0" denotes a white pixel; "1" denotes a black pixel.

Here each and every pixel from the confidential message ("That the information to be encrypted") will be sub- divided into more than one pixel, where that is "2" to represent the pixel of the confidential message, that is each and every single pixel from the confidential image is greater than one.

Here Pixels in generated shares ">, greater than" pixels in original image number of columns in constructed image equal to= 2 * no. of columns in original image Size of the Constructed image = 2 * Size of Original secret image, the increase in pixels in (2, 2) "visual cryptographic schemes" for pixel expansion "m=2", two sub pixel for each pixel in the confidential message. Here each and Every single pixel in confidential image is encrypted with random selection of possible permutation approach, for each and every sub pixel combinations. There is very less chances of possibility to retrieve any kind of information by visualizing at single "share 1" or "share 2", in the case of stacking the both shares there will be a loss of "50% percent", contrast in the overlaid image as compare to loss of "50%", contrast in the overlaid image as compare to the original image.

It is stated that, the black pixel in original confidential image, will get "2" black sub pixels and in the case of a white pixel we get "1" black sub pixel & white sub pixel, grey level of "1" pixel is black & a grey level of ½ if the pixel is white. There will be 50% of loss in contrast in constructed image and the confidential information is clearly visible. Marinating the clarity of the image to avoid image distortion aspect the ratio of the pixels to the sub pixels has to be maintained carefully.

Pixel	Probability	Share1	Share2	Share1 × Share2
	50%			
	50%			
	50%			
	50%			

Fig 5: Pixel Expansion Scheme

To denote a white pixel of the confidential information one of the two rows under white pixel is selected from fig1, and for a black pixel one of the two rows under black pixel is selected from Fig 1 [3] i.e. a white pixel is shared into two identical blocks of sub-pixels.

A black pixel shared into two complementary blocks of sub-pixels. Permutation of the pixel combination is performed such that no information can be reconstructed from any single share. Selection of the permutation combination is based on random selection of the pixel pairs. Random selection of the pixel pair combination prevents shares constructions based on the previously generated shares.

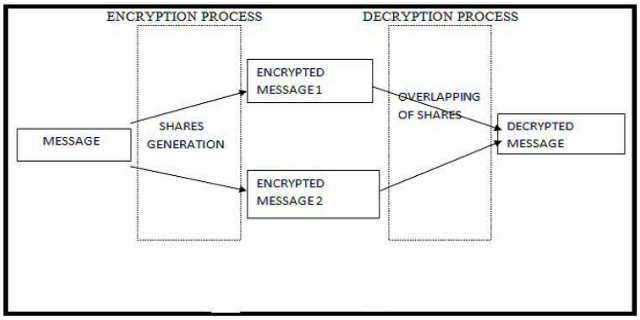


Fig 6: Schematic Layout of Visual Cryptography Scheme

V. FACTORS EFFECTING IMAGE QUALITY IN VISUAL CRYPTOGRAPHIC SCHEAMS

"m" – Higher the value of 'm' higher is the loss in resolution. To reduce loss in image resolution reduces the number of 'm'. 'α'- Greater is the image resolution greater is the image resolution. higher relative difference gives good and best in quality resolution. 'k out of n' - In "k out of n", Visual Cryptography scheme more is the number of k more clear is the reconstructed image, lesser is the number of k higher is the resolution loss. 'Aspect ratio' - [2] number of pixel expansion will be taken into consideration to avoid image distortion

VI. IMAGE ENCODING AND DECODING

To encrypt a text information using visual cryptography initially the text information should be converted in the form of image now take a black and white text image as an input to encode.

In case of color image binaries it to get a binary image. A black pixel is represented by "1" & white pixel "0". For a it is better to take large font for text images for best visualization. Encode the text image, encoding each black & white pixel. For each and every black pixel "1" in the confidential image replace it by two sub pixels, for black pixel the sub pixels distribution will be different in one shares different in other.

Either [1 0] in "share1" and [0 1] in "share2" or by randomly permuting it.Where [0 1] for "share1" and [1 0] for "share2". In case of white pixel "0" in the secret image pixel the sub pixels distribution will be same in both the shares, either [1 0] in "sahre1" and [1 0] in "share2".

white pixel in the confidential image is replaced by a half white & half black sub pixels for constructing a 100% pure white pixel a 50% white pixel, it will be half black & half white.

White pixel in the confidential image becomes a gray pixel in the final overlapped image. Due to the reason reconstructed image loses its contrast when compared to its main original image. For decoding the original image, stacking of both the shares and the confidential information will be reconstructed.

If (int==1)

share1= share2= {

{

Else if(int==0)

share1= share2=

{

{

End

The share combination to encode a 2 out of 2 scheme is -

Prepare matrix based on black or white

s0 = [1 0 ; 0 1];

s00= [0 1 ; 1 0];

s1 = [1 0 ; 1 0];

s11 =[0 1 ; 0 1];

Algorithm

1) Start
2) Take any confidential information (text, picture etc.) In image format.
3) If it is text message convert it into image form
4) Perform visual cryptography encryption technique,
5) Perform Pixel expansion
6) Generate shares,
7) Save all the generated shares,
8) Stack all or the defined number of shares.
9) Stop.

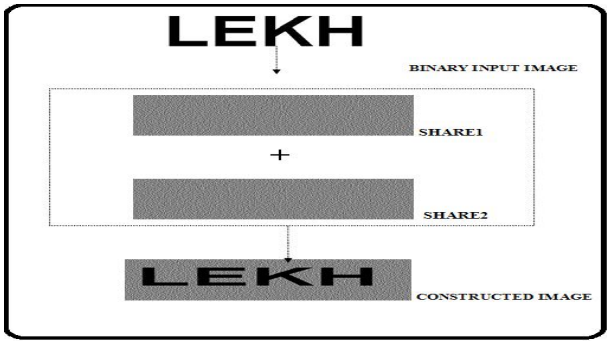


Fig 7: Experimental result of (2,2) Visual Cryptography Scheme

Original Pixel	Probability	Share 1 Sub-Pixel	Share 2 Sub-Pixel	Share 1 || Share 2
	0.5			
	0.5			
	0.5			
	0.5			

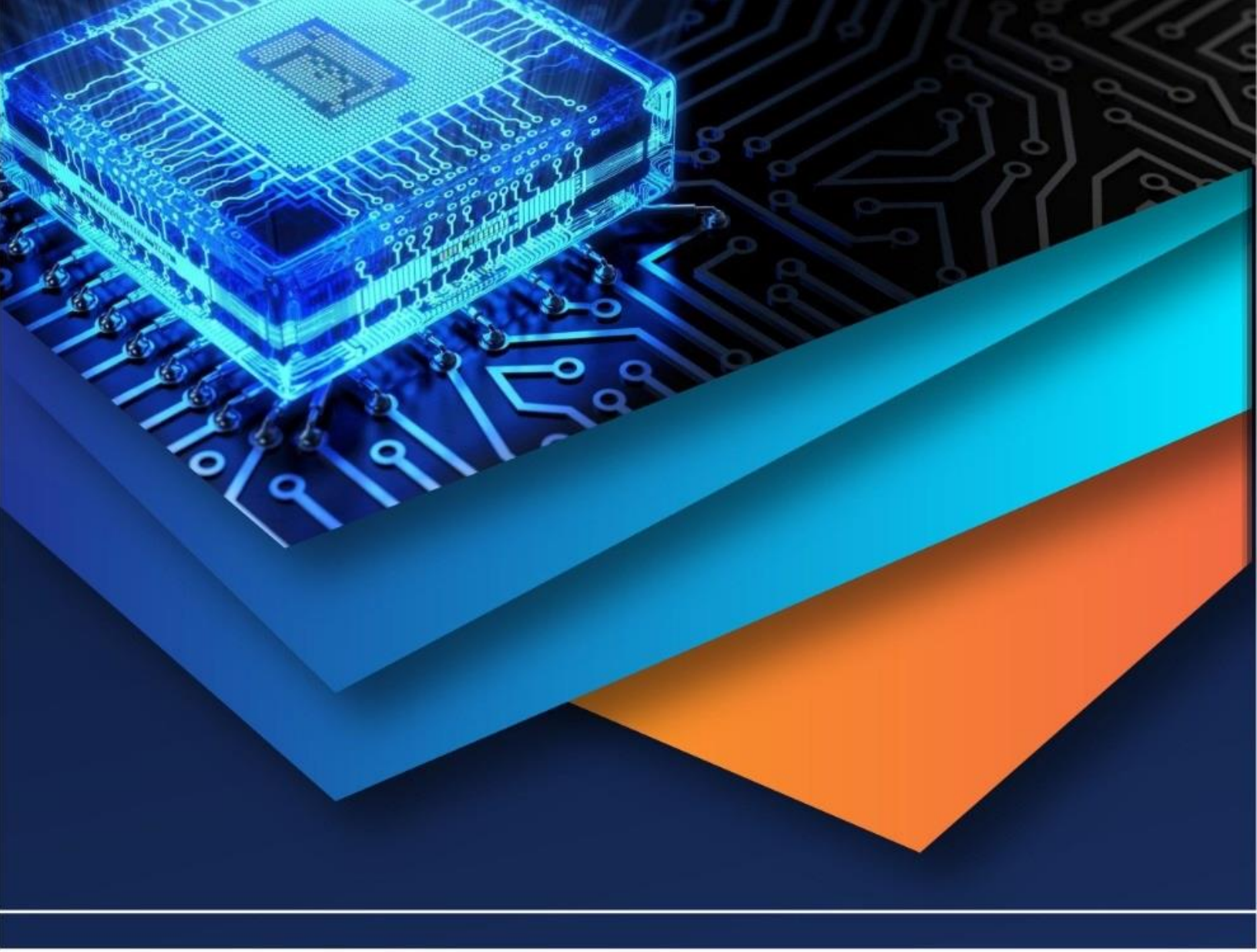
Fig 8: Pixel Expansion Scheme for (2,2) VCS for m=4

VII. CONCLUSION

In this paper we proposed an idea and there is lots of work needs to be done on this mode by implementing this concept more practically. The security for the node & secure traffic control can be established due to GaaS, managed by Government traffic control authority, they can generate income using this model. The vehicle will be in, secure mode it cannot be stolen by any one, if it happens tracing will be in fraction of seconds, and fast moment of nodes will be traced and action will be taken by concern traffic governing authority, and vehicles emitting more co2 and more pollution causing vehicles are easily traced. Due to incorporation of cloud computing technology the infrastructure cost will be reduced. We incorporated lots of security features using cryptography, using visual cryptographic technology and most of the research has needed for more improvement

REFERENCE

[1] Dedicated short range communication standards (DSRC),intelligent transport system ITS http://www.standards.its.dot.gov/
[2] Chenxi Wang,(2002)."Security issues and requirements for Internet-scale publish-subscribe systems Full "System Sciences. HICSS. Proceedings of the 35th Annual Hawaii International Conference on.
[3] jorjeta G. jetcheva, Yih-Chun Hu, santashil PalChaundry, Amit Kumar Saha,Davidd B. Johnsohn, “Design and evaluation of a metropolitan area Multitier wireless ad-hoc Network Architecture”, WINET, ACM & Springer,January 2005
[4] Muhl, G.Berlin,(May-Jun 2004)."Disseminating information to mobile clients using publish-subscribe",Internet Computing, IEEE (Volume:8 , Issue: 3).
[5] M Raya, J Pierre Hubaux, (2005). “The Security of Vehicular Ad Hoc Networks “, Proc. of the 3rd ACM workshop on Security of ad hoc and sensor networks.
[6] M Raya, P Papadimitratos, JP Hubaux, (October 2006).“Securing Vehicular Communications”, IEEE Wireless Communications, Vol 13.
[7] Jungels,P Papadimitratos, I Aad,JP Hubaux, (2006).”Certificate Revocation in Vehicular Networks“ , Laboratory for computer Communications and applications (LCA) School of Computer and Communication Sciences ,EPFL, Switzerland.
[8] ORaya, D Jungels, PPapadimitratos,I Aad, JPHubaux,(2006)”Certificate Revocation in Vehicular Networks “ , Laboratory for computer Communications and applications (LCA) School of Computer and Communication Sciences ,EPFL, Switzerland.
[9] P Papadimitratos, L Buttyan, JP Hubaux, F. Kargl, Raya, (2007). “Architecture for Secure and Private Vehicular Communications”, 7th International Conference on ITS.
[10] Stephan Olariu, Ismail Khalil, Mahmoud Abuelela, (March 2005). “Taking VANET to the clouds”, International Journal of Pervasive Computing and Communications, Vol. 7 Iss: 1 pp. 7 – 2.
[11] 1. Cimato, R. De Prisco, and A. De Santis, ‘Probabilistic visual cryptography schemes’. The Computer Journal, 49(1):97{107, December 2005.
[12] M. Naor and A. Shamir, "Visual cryptography," Advances in Cryptograhy: EUROCRYFT'94, LNCS, vol. 950, pp. 1- 12,1995.
[13] Sokratis K. Katsikas (2006), "Information security", 9th international conference, Springer Publications, pp. 548.
[14] John Blesswin, Rema, Jenifer Josel, “ Recovering Secret Image in Visual Cryptography”, Karunya University,538
[15] Chandramathi S., Ramesh Kumar R., Suresh R. and Harish S., “Anoverview of visual cryptography” , Volume 1, Issue 1, 2010, PP-32
.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY