Using Petri-Net for Modeling and Formal Verification of Crypto-security in Driverless Vehicles

S.Vijayalakshmi, J. Uma Maheswari, G.R. Karpagam, M. Visalakshi

Abstract: This paper presents a cryptography based approach for enforcing security mechanisms in driverless vehicles, used in the banking sector for transporting valuable assets. The proposed idea combines multi-factor authentication along with asymmetric encryption mechanism in order to ensure the required level of security. The system design is parallel and distributed; hence it is formally analyzed using Petri-net modeling technique.

Index Terms: Biometric Authentication, Elliptic curve cryptography, Integrity, Petri-Net and Privacy.

I. INTRODUCTION

Science and Technology has made human lives easier. Industry 4.0 is the next big industrial revolution that is expected to change the livelihood by a large margin. One important use case of Industry 4.0 that falls well within the boundary of cyber-physical systems and the Internet of things is the Driverless Vehicles, used for asset transportation in Banks and other concerned areas. Among many other difficulties involved in the construction and operation of driverless vehicles, security falls as a compelling issue to be dealt with, especially when requires applicability in the banking domain. The idea of using driverless vehicles for asset transportation has gained some practical applicability with the development of cyber security techniques. The Driverless vehicle is prone to many security attacks in the real world. The potential security attacks include:

- Loss of confidentiality when the asset is compromised.
- Loss of integrity when the contents of the asset (for eg. important files) are modified.
- Loss of availability when the asset is missing.
- Loss of access control when the contents of the asset are compromised by an external individual.

The idea presented in the paper involves a smart device housing the asset, which has a digital display, finger print sensor, processor module and a communication module. In addition, an ID card scanner is affixed to the doors of the vehicle, which remains to be the first level of authentication check to open the doors. The above mentioned security issues can be solved by locking the asset box using a password, which can be opened only by an assigned employee using his authentication credentials. However, this method is prone to many confidentiality issues, wherein the employee might leak his credentials to externals. This problem is solved by imposing cryptographic techniques such as hashing and asymmetric encryption into the process. This paper proposes such a solution that overcomes these identified security bugs. The basic concept of the proposed system is portrayed in the below figures Fig.1 and Fig.2

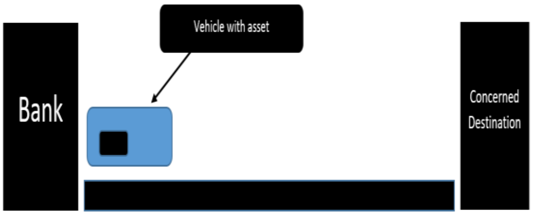

Fig.1. Set up of the asset by the concerned bank employee and transfer initiation with finger print locking.

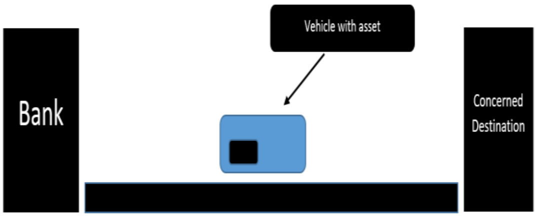

Fig.2. The vehicle stops during the transfer due to any problem. The authorized employee takes over the asset using his proper credentials.

II. RELATED WORK

[1] Studies the need for edge computing, possible challenges faced and opportunities. The authors present the issues related to latency and the user experience for time-critical applications. In [2] the authors emphasize on the scope of the Internet of Things (IoT) in our daily lives, involving Millions of sensors and devices are continuously producing data and exchanging important messages via complex networks. The paper analyzes how edge computing improves the performance of IoT networks.
[3] deals with the common threats to security issues faced in fog computing,

Revised Manuscript Received on February 05, 2020.

* Correspondence Author
S.Vijayalakshmi,Department of CSE, PSG College of Technology, Coimbatore, India. Email:msvijipsg@gmail.com
J. Uma Maheswari, Department of CSE, PSG College of Technology, Coimbatore, India. Email: uma.cse@psgtech.ac.in
G.R.Karpagam, Department of CSE, PSG College of Technology, Coimbatore, India. Email: grk.cse@psgtech.ac.in
M. Visalakshi, Department of CSE, PSG College of Technology, Coimbatore, India, Email: salu.kumar.98@gmail.com

especially with respect to Location privacy and Data confidentiality. The main focus is on the fact that service providers as well as government can access users' data. The decoy technique is proposed as a solution to the issue. In [4] proposes the modified blind signature algorithm is appropriately efficient for online voting to achieve the privacy of the vote; in addition to anonymity and integrity of the vote.

[5] analyzes data security and privacy threats, protection technologies and countermeasures inherent in edge computing. It also suggests the use of attribute-based encryption, role-based encryption for providing access control and probabilistic public key encryption for providing privacy. In [6], the authors explore a range of security issues for IOT devices and then they present Multi-factor Authentication, Role-Based Access Control and Attribute/identity based encryption as a solution for security issues related to virtualization. [7] propose Identity and access management as a service in e-healthcare cloud. It enhances the security of identity along with the availability of resources in multitier cloud. [8] Suggests the certificate based strong authentication to achieve the identity of the user.

The analysis of the above papers shows that most Fog applications do not consider security as part of system, but rather focus on functionality, which results in many Fog platforms being vulnerable. Hence the need for cryptographic mechanisms comes into picture. Digging deeper into the various cryptographic algorithms for encryption and decryption, many researchers emphasize on the usage of Elliptic Curve Cryptography to fit in well for satisfying the security requirements in edge systems.

Khajehei in [9] aims to provide a highly secure communication between two Virtual Machines. With key length being a shortfall in most traditional cryptography algorithms like RSA, the author proposes the use of ECC algorithm that uses faster in speed, smaller in size, and more efficient cryptographic keys to provide the required level of security. [10] suggest Fingerprint with Fuzzy commitment Scheme. It is a strong authentication technique because Biometric information is unique to each user and secure against user impersonation Attack. It is easy to use separate passwords for different applications, and to change passwords on frequently. Akanksha Bansal and Arun Agrawal in [11] propose the use of ECC to maintain data privacy and integrity in cloud storage. Futher in [12], Srinivasan and Raju suggest an approach for image security by integrating image encryption with ECC. In [13], Dindayal and Dilip Kumar experiment a technique of enhancing the security of one-time password using Elliptic Curve Cryptography with finger-print biometric. This model also overcomes the necessity to create and store private keys, and thereby prevents the potential compromise of secret keys.

From the results of the above works, it may be concluded that ECC would be an optimal choice of asymmetric cryptographic algorithm to suffice the security requirement of the asset transportation problem. Next, the correctness of the proposed solution need to be verified either experimentally or by a formal verification mechanism. One such mechanism that can be used is the Petri-net modeling technique**.**

In [14] Petri-nets are used to model basic authentication procedure in two different ways and compare them both. In [15], the authors claim that the correctness of dynamic and autonomous protocols such as MAC cannot be verified using traditional testing techniques. Hence Petri-net formal description technique is used to generate performance-oriented simulation results and to determine more formal correctness properties. In [16], the complex modeling of communication systems having a large number of variables and dynamic behavior is done using Petri-Nets. The focus is to analyze the validity of an encryption scheme applied to Wireless Sensor Networks using Petri-net modeling. Petri nets can be used to model features like precedence relation, concurrency, conflict and mutual exclusion of real-time systems. Further, it can be used to test the Reachability, Liveliness, Boundedness, Safeness, Conservativeness and Reversibility properties of the system design. Hence Petri-net modeling can be used to verify the flawless applicability of the proposed solution.

III. PROPOSED SYSTEM

A. System Setup

Each employee is registered with his name, address and other personal details, along with his public key and finger-print data. A Bank Manager is an Employee with special privileges and responsibilities.

An 'asset' can be any valuables like gold, cash, documents etc. that need to be transported physically across different branches of Banks. Each asset under a bank's control is assigned a unique system-generated password that is required to access the asset. This password is stored securely in the server's database and users can access only a hash-value computed over it (using MD5) and the actual password is not visible to users. By this way, leakage of password by the Bank personnel's will be prevented.

A vehicle used for asset transportation will have an ID-card scanner over the door and a box to hold the asset inside. The door of the vehicle can be opened only upon scanning the ID-Card by an authorized bank employee. The box is controlled by a processor module (Arduino or Raspberry Pi), installed with a wireless communication module and finger print sensor. The box will open upon providing the proper decryption credentials.

B. Workflow

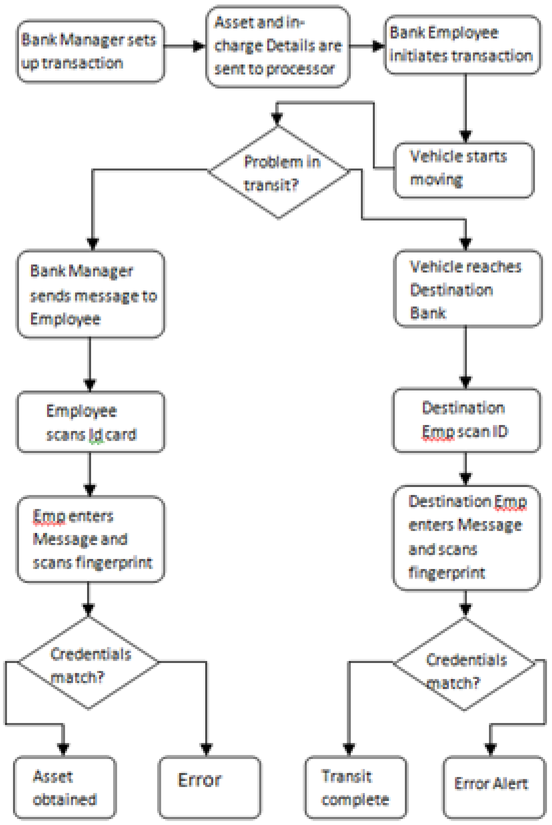
Bank Manager sets up transaction
Asset and in-charge Details are sent to processor
Bank Employee initiates transaction
Problem in transit?
Vehicle starts moving
Bank Manager sends message to Employee
Vehicle reaches Destination Bank
Employee scans Id card
Destination Emp scan ID
Emp enters Message and scans fingerprint
Destination Emp enters Message and scans fingerprint
Credentials match?
Credentials match?
Asset obtained
Error
Transit complete
Error Alert

Fig.3. The workflow of the proposed system

The above figure shows the workflow of the proposed system

1. The Bank Manager assigns the vehicle number, destination, travel route and a concerned Employee for the asset to be transferred, along with the transit date, time etc.
2. The asset password and fingerprint data of the Employee in-charge of the asset till it reaches the destination Bank are sent to the respective vehicle's processor.
3. The respective source Bank Employee places the asset in the vehicle's box and authenticates the transit using his finger print.
4. The vehicle starts moving towards the destination. The processor continuously monitors the current GPS location of the vehicle.
5. In case the vehicle is moving out of the route, or the vehicle stays idle for a particular amount of time or if there are any attempts to manipulate the box, the processor immediately sends an alert to the Bank Manager.
6. The Bank Manager retrieves the hash value of the password and encrypts it using the concerned Employee's public key, and sends it as a message to the Employee.
7. The Employee reaches the spot, opens the door by scanning his ID card, then enters the message and places his finger print - which acts as the private key for decryption by the processor.
8. The processor computes a hash over the original password received (from step 2) and compares it with the decrypted value received (from step 6). If they match, the box opens and the employee takes over the asset. Else, alerts are sent to the Manager and it gets time-locked after a few attempts.
9. If no problem occurs during the transit and the vehicle reaches the destination Bank safely, the source and destination Bank Managers are notified and the details of the destination Bank Employee assigned in-charge for opening the box are sent to the processor and message is sent to the concerned employee. The Employee uses his ID card, the received message and his finger print to unlock the device and take over the asset.

C. Private Key generation from Fingerprint

The incorporation of Biometrics to cryptography can be seen as a method of data hiding, which will introduce high level of strength to information security. The strength of most present day cryptosystems lies mainly in the key used for encryption. The problem to remember, protect and manage private key is a major issue in case of asymmetric ciphers. Biometrics is a form of inherent data, specific to the decrypter, and hence can be used as a means to solve the above mentioned issues.

In this paper, such a simple, stable secret key is maintained for each Employee of the Bank. The process of key extraction from the Employee's Fingerprint follows the baseline procedure suggested in [17]. The authors propose this novel approach after having implemented it in MATLAB and analyzing the generated key sizes and time complexities.

The basic idea is to derive minutiae coordinate points from fingerprint template and from that coordinate points elliptic curve is generated using elliptic curve algorithm. This process comprises of the following four steps:

i. Binarization

Image binarization is the process of turning a grayscale image to a black and white image. This can be done by applying a threshold comparison for each pixel.

ii. Thinning

The thickness of all ridge lines in the binarized image is reduced to a single pixel, while keeping constant the location and orientation of the minutiae.

iii. Minutiae extraction

The minutiae extraction step is of core importance in any finger print recognition system. The cross numbering approach over thinned binarized images is proposed in [18]-[20], wherein the neighborhood of each ridge pixel in the image is examined over a

DOI: 10.35940/ijeat.C6457.029320

3X3 window and the CN value is computed from the absolute value of the difference in the pixel values of neighboring points. Based on the CN value, the ridge point is categorized as an isolated point (CN=0), Ridge ending point (CN=1), Continuing ridge point (CN=2), Bifurcation point (CN=3) or a crossing point (CN=4).

iv. Elliptic curve points generation

The next step is to derive elliptic curve coefficients from minutiae. For each extracted minutiae point, the X and Y coordinates, orientation of the associated ridge segment (θ), and type of minutiae (ridge ending or bifurcation) are noted. Now, each minutiae is represented in three co-ordinate system as (x,y,θ).

Let p be a prime number, and let Fp denote the field of integers modulo p. An elliptic curve E over Fp is defined by an equation of the form

$$y^2 = x^3 + ax + b \qquad (1)$$

where a, b € Fp satisfy $4a^3 + 27b^2 = 0(mod\ p)$.A pair (x,y),where x, y € Fp, is a point on the curve if (x,y) satisfies the equation. The set of all the points on E is denoted by E(Fp). Find point of infinity n.

The source and destination banks agree on a Base point G on E for communication. The message which comprises of the Hash value of the asset password is encoded onto a point Pm on the elliptic curve. The Employee's private key Kpvt is generated from his finger print using the approach presented in [15] that makes use of the triplets (x,y,θ) representing the minutiae. The Employee's public key Kpub is computed as

Kpub = G*n Kpvt (2)

Now the message is transmitted according to the regular ECC encryption scheme, and at the edge device, it is decrypted using the private key computed from the scanned finger print of the employee.

IV. PETRI NET MODELING

Petri net, also known as Place/ Transition net is a mathematical modeling language that is best suitable to describe the design of dynamic and concurrent distributed systems. The model consists of a collection of directed arcs denoting arcs connecting places and transitions; Places represent possible states of the system; Transitions are events that cause change of states. Firing of a transition occurs based on input conditions and availability of tokens in the preceding places, and causes movement of tokens to the succeeding places, which denotes a change of state.

The Petri net model for the proposed system is shown in parts in Fig 4, Fig 5 and Fig 6. The places and transitions involved in the models are listed out with descriptions in Tables 1 and 2.

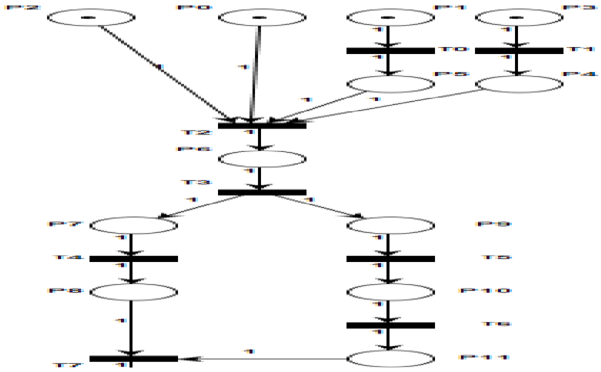

Fig. 4. Petri net – Initial phase.

Fig.4. shows the modeling form system start state till the vehicle is started. Initially, the places P0, P1, P2 and P3 are seeded with tokens, since these represent nominal assumptions required for the system workflow to begin. Once the entities involved in the transaction are ready, the processor in the edge device is setup with the required authentication constants and the employee assigned in-charge of the transaction triggers the vehicle to start moving.

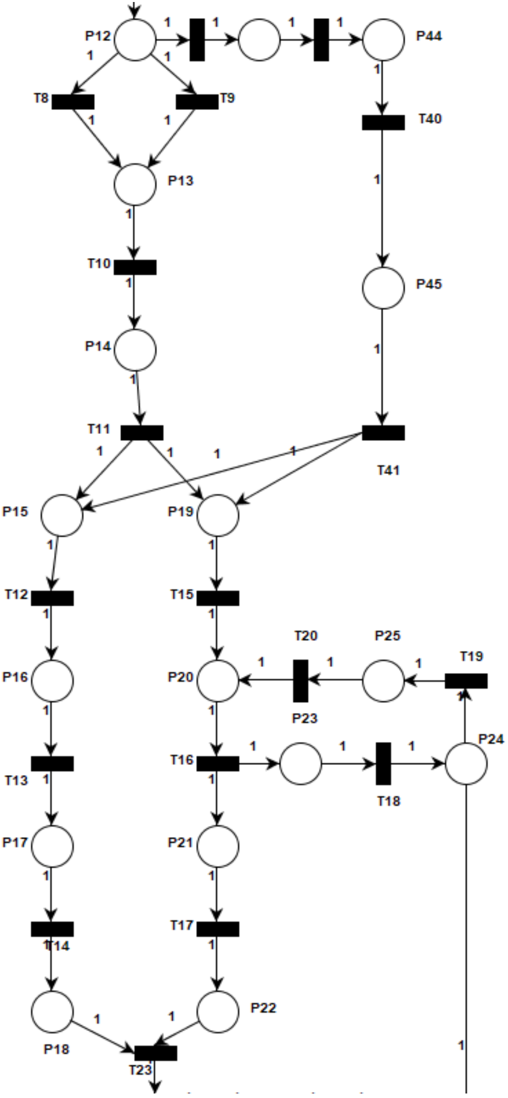

Fig.5. Petri net – First level Authentication (ID card scanning)

The occurrence of a transaction issue or arrival at the destination location is detected. Following the notification, the password of the respective asset is hashed and encrypted with the respective source or destination bank employee's public key and employee receives the message. Then the first level of authentication to open the door is done by an ID card scan. Once the scan is successful, the employee shall access the device display and enter the message.

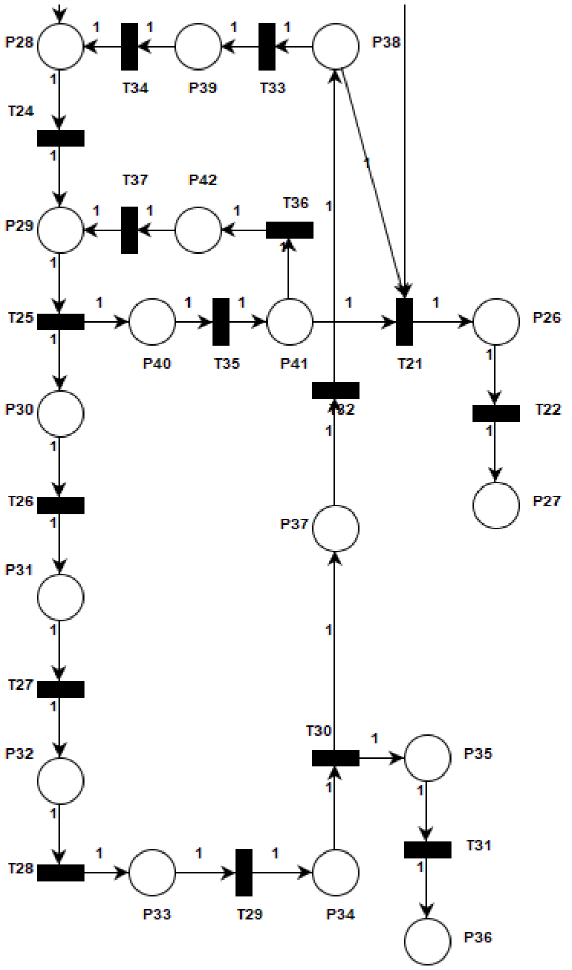

Fig.6. Petri net – Second and third levels of Authentication

The employee scans his/her fingerprint, which is verified as the next level of authentication. Then, the fingerprint image is processed to generate the ECC private key, using which the message is decrypted. The decrypted value is compared against the actual password Hash received. This forms the last level of authentication to disclose the asset.

Table- I: Places description of Petri nets in Fig.4, Fig.5 and Fig.6

Place	Description
P0	Asset Ready
P1	Bank Manager wants to transfer
P2	Destination bank Manager accepted transfer
P3	Employee to be assigned
P4	Employee ready
P5	Transaction details updated
P6	New transaction
P7	Processor receives details
P8	Processor initialized
P9	Employee assigned task
P10	Asset with Employee
P11	Asset in Box
P12	Vehicle moving
P13	Problem state
P14	Server receives alert
P15	Password for asset retrieved
P16	Hash (password) computed
P17	Message created
P18	Employee has credentials
P19	Employee reached vehicle location
P20	ID scan
P21	ID matched
P22	Employee can access display
P23	ID not matched
P24	Next scan attempt
P25	Allow rescan
P26	No more attempts
P27	System Locked
P28	Message entered
P29	Fingerprint obtained
P30	Fingerprint match
P31	Clean image of Fingerprint
P32	Minutiae co-ordinates obtained
P33	Private key generated
P34	Received hash obtained
P35	Hash values match
P36	Asset obtained
P37	Hash values mismatch
P38	Next credential attempt
P39	Allow reentry of message
P40	Fingerprint mismatch
P41	Next fingerprint attempt
P42	Allow rescan of finger
P43	Asset at destination Bank
P44	Source and Destination BM notified
P45	Box ready to open

Table- II: Transitions description of Petri nets in Fig.4, Fig.5 and Fig.6

Transition	Description
T0	Select transaction details
T1	Employee free to accept
T2	Create transaction
T3	Send message to Employee and processor
T4	Store details in edge device
T5	Employee gets asset
T6	Employee places asset inside box
T7	Employee authenticates vehicle to start
T8	Vehicle idle for long time
T9	Vehicle moving out of route
T10	Send problem alert to server
T11	Retrieve password and send location to Employee
T12	Compute Hash
T13	Encrypt with public key
T14	Send message to Employee
T15	Employee scans ID card
T 16	Check ID match
T 17	Open door

T 18	Increment scan attempts
T 19	Scan attempts less than four
T 20	Rescan ID card
T 21	Otherwise
T 22	Send Lock Notification
T 23	Enter message
T 24	Place fingerprint
T 25	Validate finger print
T 26	Preprocess finger print
T 27	Extract minutiae
T 28	Map to Elliptic curve point
T 29	Decrypt message
T 30	Compare with original hash
T 31	Open box
T 32	Increment message entry attempts
T 33	Message attempts less than three
T 34	Re-enter message
T 35	Increment fingerprint attempts
T 36	fingerprint attempts less than 3
T 37	Re-scan finger
T 38	Vehicle reached destination
T 39	Send reached notifications
T 40	Server gets opener details form Destination BM
T 41	Server sends message to destination Employee and Employee details to device

V. EXPERIMENTAL RESULTS

A Reachability graph of a Petri net is the state space representation of the system, where nodes correspond to reachable markings and edges correspond to relations. The properties of the Petri net may be analyzed by construction the reachability graph, however the reachability graph may be practically huge: exponential in the number of places. Structural analysis enables us to prove some properties without constructing the reachability graph.

Some of the essential properties to be verified include boundedness and liveliness. A Petri net is live if all the represented transitions can be fired and bounded if the number of reachable states if finite. More formally,

Live: A Petri net (PN, M) is live iff for every reachable state M' and every transition t there is a state M'' reachable from M' which enables t.

Bounded: A Petri net (PN, M) is bounded iff , there exists a natural number n such that for every reachable state and every place p the number of tokens in p is less than n.

PIPE2 (Platform Independent Petri Net Editor 2) tool has been used to visually analyze the designed Petri net model by the animated firing of transitions for all possible test situations. From the observations, it can been justified that every transition in the model is triggerable, hence the net is live. Every possible test flow will terminate after a finite number of states, hence the net is bounded. Further, it has been observed that the system will not enter any deadlock state.

VI. CONCLUSION

A multi level authentication solution for the security problems in edge devices has been proposed and designed. The suggested method is implied to provide:

- Authentication – Proving one's identity in order to access the asset
- Confidentiality – The details of the asset being transported is out of other's knowledge
- Integrity – The asset cannot be modified during transit by any means
- Non-repudiation – The employee cannot refuse his action of handling the asset, since there is biometric verification

REFERENCES

1. Weisong Shi , Jie Cao , Quan Zhang , Youhuizi Li and Lanyu Xu, “Edge Computing: Vision and Challenges,” IEE Internet of Things Journal, Vol.3, no.5, 2016.
2. Wei Yu , Fan Liang and Xiaofei He , William Grant Hatcher , Chao Lu , Jie Lin and Xinyu Yang, “A Survey on the Edge Computing for the Internet of Things,” IEEE Access. Vol.6, ISSN: 2169-3536, 2017.
3. Praveen Kumar , Nabeel Zaidi and Tanupriya Choudhury, “Fog computing: Common security issues and proposed countermeasures,” International Conference System Modeling & Advancement in Research Trends (SMART), 2016.
4. Vijayalakshmi, S and Karpagam, GR, “An Agent Based Online Voting System in Cloud using Blind Signature”, Asian Journal of Information Technology, vol. 15, no. 19. pp. 3826-3834, ISSN: 1682-3915, 2016.
5. Jiale Zhang , Bing Chen , Yanchao Zhao , Xiang Cheng and Feng Hu,” Data Security and Privacy-Preserving in Edge Computing Paradigm: Survey and Open Issues,” IEEE Access, Vol. 6, ISSN: 2169-3536, 2018.
6. Saad Khan, Simon Parkinson and Yongrui Qin,” Fog computing security: a review of current applications and security solutions,” Journal of Cloud ComputingAdvances, Systems and Applications, 2017.
7. Dhanabagyam, SN and Karpagam, GR, “Identity and access management as a service in e-healthcare cloud,” International Journal of Biomedical Engineering and Technology, vol. 26, no. 3-4,pp 250-265, 2018.
8. Vijayalakshmi, S and Karpagam, GR, ”Secure Online Voting System in Cloud,” Electronic Government. An International Journal, vol. 14, no. 3, pp. 276-286, ISSN: 1740-7494, 2018.
9. Kamyab Khajehei, “Secure Communication in Cloud by Using ECC Algorithm,” International Journal of Engineering Research & Technology (IJERT), Vol. 3 no. 1, ISSN: 2278-0181, 2014.
10. Vijayalakshmi, S and Karpagam, GR, “Authentication as a service in cloud from a fuzzy perspective,” International Journal of Enterprise Network Management, vol. 9, no. 3/4, pp. 352-362, ISSN: 1748-1260, 2018.
11. Akanksha Bansal and Arun Agrawal,” Providing security, integrity and authentication using ECC algorithm in cloud storage,” International Conference on Computer Communication and Informatics (ICCCI), 2017.
12. Srinivasan Nagaraj and G. S. V. P. Raju,” Image Security using ECC Approach,”Indian Journal of Science and Technology, Vol. 8, no. 26, 2015.
13. Dindayal Mahto and Dilip Kumar Yadav,” Enhancing security of one-time password using Elliptic Curve Cryptography with finger-print biometric,” second International Conference on Computing for Sustainable Global Development (INDIACom), 2015.
14. J. Capek, M. Hub and R. Myskova,” Basic authentication procedure modelled by Petri nets,” International journal of computers and communications, Vol. 4, no. 4, 2010.
15. R.J. Haines , G.R. Clemo and A.T.D. Munro,” Petri-nets for formal verification of MAC protocols, ”. IET Software.Vol.1, no.2 , 2007.
16. Hugo Gustavo Rodriguez, Ismael Soto and R.A. Antonio Carrasco, ” Using Petri Net for Modeling and Analysis of a Encryption Scheme for Wireless Sensor Networks,” 11th IEEE-IET Intern. Symposium on COMMUNICATION SYSTEMS, NETWORKS AND DIGITAL SIGNAL PROCESSING, 2018.
17. Dindayal Mahto and Dilip Kumar Yadav,” Network Security Using ECC with Biometric,” Quality, Reliability, Security and Robustness

in Heterogeneous Networks. Vol. 1, no.15, 2013.

18. Roli Bansal , Priti Sehgal and Punam Bedi, " Minutiae Extraction from Fingerprint Images - a Review, " International Journal of Computer Science Issues, Vo. 8, no.5, ISSN:1694-0814, 2011.
19. B.Raja Rao, E.V.V.Krishna Rao, S.V.Rama Rao and M.Rama mohan rao, " Finger Print Parameter Based Cryptographic Key Generation," International Journal of Engineering Research and Applications (IJERA), Vol. 2, no. 6 , ISSN: 2248-9622, 2012.
20. M Sreemathi, K Thangavel and K Sasirekha, " Elliptic Curve Cryptography based key generation from the fusion of ECG and Fingerprint," International Journal of Computational Intelligence and Informatics, Vol. 4, no. 3, 2014.

AUTHORS PROFILE

Ms. S. Vijayalakshmi obtained her ME Computer Science and Engineering in PSG College of Technology, Tamil Nadu and pursuing her PhD in Information and Communication Engineering from the Anna University.Currently she works as an Assistant Professor (Senior Grade) in Department of Computer Science and Engineering, PSG College of Technology. Her research interest includes network security, computer communication network and Blockchain. She is a Life Member of Indian Society of Systems for Science and Engineering (ISSE). She has published her research papers in peer reviewed international journals and conferences.

Dr. J.Uma Maheswari is an Assistant Professor(SG) with 12 years of experience in Computer Science and Engineering in PSG College of Technology. She completed her BE Computer Science and Engineering in Sri Krishna College of Engineering and Technology, Coimbatore from Bharathiar University in 2003 and ME Computer Science and Engineering in JJ College of Engineering and Technology, Trichy from Anna University in 2006. Her areas of research include Computing and Semantic web services

Dr. G.R. Karpagam is a Professor with 23 years of experience at Computer Science and Engineering in PSG College of Technology. She obtained her BE, ME and PhD in Computer Science and Engineering. Her area of specialisation includes database management systems, data structures and algorithms, cloud computing, network security and machine learning. She serves as a reviewer and editor for peer reviewed national and international conferences and journals. She possesses h-index 10 and i10-index 10.

Ms. M. Visalakshi obtained her BE Computer Science and Engineering in PSG College of Technology, Tamil Nadu.