International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-3, September 2019

Enhanced Mutual Authentication Technique using Id (Matid) in Fog Computing

K.Sujatha,V.Ceronmani Sharmila

Abstract: ***The expanded development of cloud computing is emerging as a new paradigm is known as Fog Computing. The focus of the fog is to achieve fine data processing in the cloud. Apart from everything, authentication is the primary security guard to the system. Since fog is a booming paradigm, the traditional authentication techniques lacks in latency issues and fails to satisfy the requirements of fog computing. In this paper, a new Mutual Authentication Technique using ID (MATID) is introduced to entrust complete mutual authentication between fog users and fog nodes. In this technique, fog users and fog nodes have to register themselves in a common Identity Issuer (IDI) to get their authentication message respectively to collaborate in the network. Fog users and fog nodes have to perform only simple hash functions and XOR operations. Our technique mainly focuses on mutual authentication, trustworthiness and reduced computational and communication costs. It ensures higher security and easily adapted to the fog computing environment.***

Keywords : Mutual Authentication, Fog Computing, MATID.

I. INTRODUCTION

Cloud computing has so much possibilities for enterprises, by providing computing services like SaaS, PaaS and IaaS[1]. Obviously, Cloud computing model becomes a predominant power over handling of data for the customers. It makes easier way to the enterprises for their applications hold the better solution to some of the entities such as, resources for storage, communication cost and computation limitations.

Nowadays, the concepts of IOT are showing higher involvement in today's life. When it comes to cloud computing architecture, it barely supports their requirements of location awareness, support of mobility and low latency.

The perfect definition of the fog is an intermediate layer between users on the edge of the network and the cloud. Both cloud and fog services remain same in the details of data, storage, computation and application services.

Generally fog computing is defined as an expanded version of the cloud computing. End users of the edge network are highly influenced by the resources pool of fog computing, such as storage, computation and networking services [2].

Manuscript published on 30 September 2019
* Correspondence Author
K.Sujatha*, CSE, Hindustan Institute of Technology and Science, Chennai, India. Email: sujeekevi@gmail.com
Dr.V.Ceronmani Sharmila, SCS, Hindustan Institute of Technology and Science, Chennai, India. Email: csharmila@hindustanuniv.ac.in

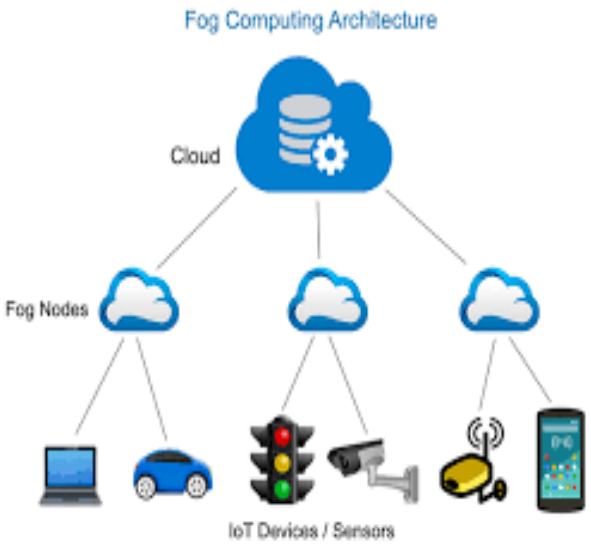

Fig. 1 depicts the infrastructure of the fog Architecture.

Fig. 1. Fog Architecture

Fog computing has more advantage over cloud due to direct connection with the edge location. With the low latency requirements, it may be able to support some similar applications. Location awareness is an important characteristic of fog computing. Fog node can target the devices of end users to manage transportability.

In Fog computing, the fog services are differentiated depends upon the choices of providers [3].

a. Internet Service Provider
   The fog infrastructure can be made by their legacy architecture. It may have control over home gateways or cellular base stations.
b. Cloud Service Provider
   It is a general fog infrastructure, who wants to extend the cloud services to the end users.
c. End Users
   They construct their provincial private cloud in order to minimize the cost of the ownership.

The design of the fog computing is based on some of the factors such as,

a. Persistent, unique and distinct ID achievement.
b. Deliberate and aleatory misbehaviour treatments.
c. Punishment and redemption of reputation management.

In Fog computing, we can refer some of the trusting models [3] which are given below,

a. Secure element
b. Trusted platform module
c. Trusted execution environment

Generally user data are outsourced and the users control over data is managed by fog node. It implies the similar security issues as discussed in the cloud computing. First of all, data integrity is the main concern since the data is outsourced. Secondly, abuse of uploaded data by unauthorized parties may bring another convolution in the system.

The new challenges in the fog computing have to be solved to support dynamic operation, achieve low latency and communication management between fog and cloud [4].

Fog nodes are propinquity nodes of users from edge network and can observe more delicate information. So, privacy preserving is also the major concern in the fog computing. To achieve the privacy of data, that is, dealing in between the fog nodes and end users, some methods such as homomorphic energy should be implemented.

Another privacy issue occurs, when the fog client utilizes the services of the fog. Fog nodes are easily approachable to the end user usage. Due to that, we have to analyze the applications to ensure the unshipped resource usages that do not reveal the private details. Next privacy issue falls on client's location privacy. It may reveal the complete track range to the fog nodes.

Fog computing satisfies some of the application requirements [5] such as Internet of Things, Smart grid applications, Wireless sensors and software influenced networks

II. RELATED WORKS

In this section, some of the related works regarding mutual authentication to the proposed mechanism have been reviewed.

Balfanz et.al[6] discussed the pre-authentication scheme over location limited channels. This scheme works on the demonstrative identification to perform pre-authentication over location limited channels. This scheme is based on Guy Fawkes protocol. The digital streams are authenticated by this protocol. This Guy Fawkes protocol ensures integrity protection and authentication that cannot provide encryption.

The simple mechanism of pre-authentication over location limited channel is given below:

A ---→B : Address (A), h(PK_A)
B ---→A : Address (B), h(PK_B)
PK_A - A's Public Key
PK_B - B's Public Key
h ( ) - Hash Function

This scheme has advantages over some of the details given below:

a. Use of location limited channels
b. Novel location limited channels
c. Concrete pre-authentication protocols
d. Group communication
e. No reliance on Public key infrastructure

Though it has many advantages over the system, still lacks in the complete achievement of mutual authentication, security issues and computational overheads. Moreover, this scheme does not fit into the fog computing environment.

Bouzefrane et.al [7] implemented an NFC based technique for the cloudlet authentication. This authentication mechanism guarantees the data integrity between the cloudlet and the mobile. This focuses mainly on mobile computing to enable a secure cloulets.

The general flow of authentication mechanism takes place between mobile devices, cloudlet, Trusted service manager and Mobile network operator. Fig. 2 describes the flow of authentication.

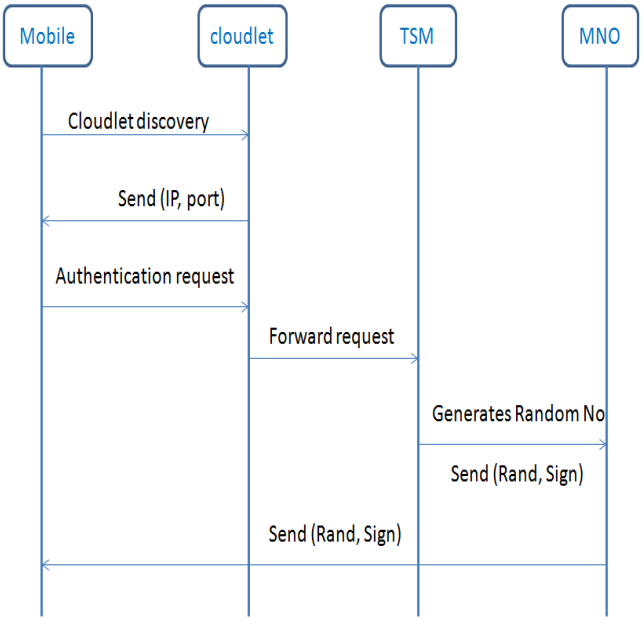

Fig. 2. Flow of Authentication

Manoj et. al[8] introduced a password based scheme for an authentication in a general network. This scheme implements the authentication by using two functions such as, Redirected function and Check digit function. The work of the system falls in the four phases like, Registration, Login, Verification and Password change.

This password based scheme achieves mutual authentication. It establishes the secure communication and message confidentiality. It overcomes more security flaws like a replay attack, denial of service attack, password guessing attack, stolen verifier attack and smart card loss attack.

Even though it baggage more advantages still it lacks in computational complexity since this password based scheme is implemented using smart cards. Finally the requirements of the system does not fit for the fog computing.

Generally in password based scheme [9], [10], low entropy is the factor which decides the password portray. In the process manifesting the session key by amplifying the entropy, some substantial modular arithmetic computations are essential. The most familiar attack on the weak password is the offline dictionary attacks.

In fog computing, many fog servers in different fogs are inadequate to keep the password with each server.

To keep a common password in the fog computing for all the nodes is also not an effective method to achieve the mutual authentication.

M.H.Ibrahim[11] proposed a mutual authentication scheme (Octopus) in the fog computing. This is the entry point to all the researchers in fog computing, which implements the complete mutual authentication in fog computing. Fig. 3 depicts the general network model of the system.

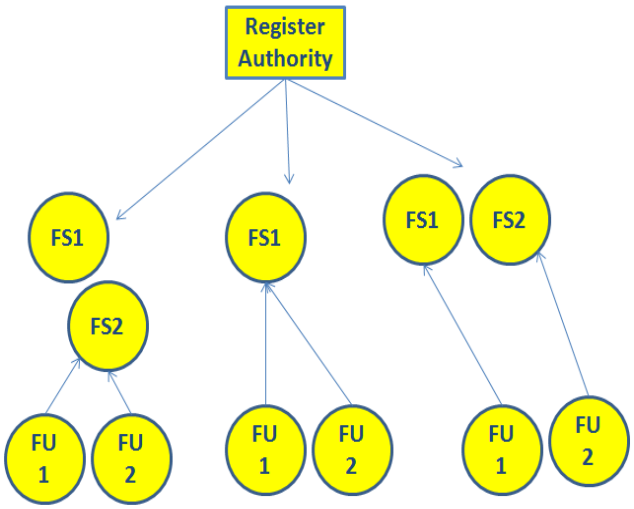

Fig. 3. General network model

This scheme does not rely on any public key infrastructure to authenticate mutually to each other. The fog user is responsible to maintain a single master key. They must be able to authenticate with other fog server without need to enroll again and without any extra added aloft. This model has to perform only some hash functions and symmetric encryption or decryption.

The efficient implementation of smart cards is done by the process which includes three phases are Initialization, Registration and Authentication. It achieves mutual authentication, confidential communication session, and overcomes security threats like replay attacks, MITM attack and session key guessing attack. Still, it lacks in computational complexity and some threats against smart card issues.

Youcef et.al [12] proposed a novel, efficient authentication technique to implement a mutual authentication in fog computing. This scheme ensures the registration of fog nodes and fog users at the cloud level. It follows the eventual authentication between fog nodes.

The concepts used in the scheme are block chain technology and secret sharing technology. Block chain technology is maintained in the fog nodes and considered as resource consuming technology.

The phases of the system are Set up phase, Fog registration phase, User registration phase and Mutual authentication phase.

Fig. 4 explains the flaws of authentication between fog users and fog node.

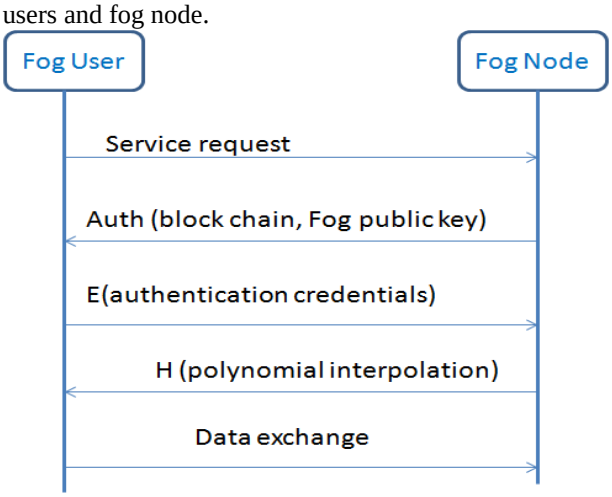

Fig. 4. Authentication between fog user and fog node

This scheme is so dynamic and scalable while in the registration phase of the system. It is considered as a secure and fully distributed authentication scheme. It has low latency, adaptive and portable scheme which does not require any public key infrastructure. Even though it achieves mutual authentication efficiently still, it is time consuming due to block chain technology and carries computational overheads.

Some of the existing system focuses on mutual authentication but not in the fog computing environment. If the system focuses on fog computing then lacks in security issues and computational overheads.

III. MATERIALS AND METHODS

In related works, rarely focuses on the environment fog computing. Our proposed system concentrates more on mutual authentication using ID in fog computing to overcome the issues such as, security threats, computational and communication overheads.

The proposed system is having three roles like, Fog User, Fog node and Identity Issuer (IDI). The initial registration is done at IDI for fog users and fog nodes by using their ID. The phases of the system are Fog registration and Mutual authentication.

The general model of the system made up of fog users from the networking side, Fog nodes or servers from the fog computing environment and the cloud network. The IDI is connected in between fog users on the networking side and fog nodes or servers from the fog computing environment.

Notations:

ID_{FU} - Identity of the fog user
ID_{FN} - Identity of the fog node
RAN_{FU} - Random number adopted by user
RAN_{FN} - Random number adopted by node
SK_{IDI} - Secret key of the IDI
H(.) - One way hash function
XOR - XOR operation
TS - Timestamp

Fig. 5 represents the general network model of the system.

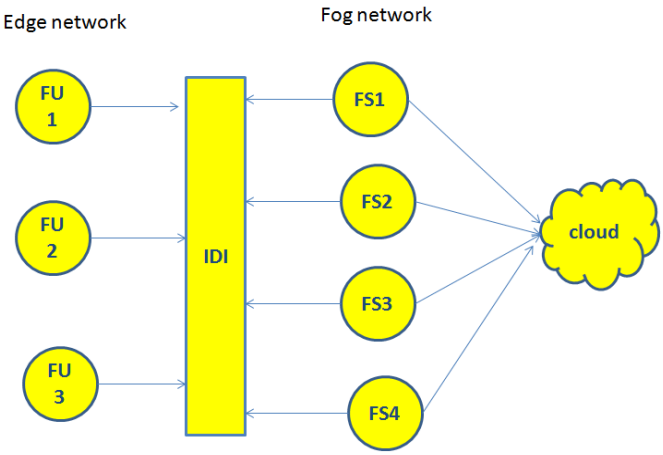

Fig. 5. Model of the system

1. Fog Registration

In the fog registration phase, the IDI acts as an intermediate between the fog user and the fog nodes. They have to register them in the IDI to get their authentication message while starting their collaboration.

i. Fog users send their request to IDI with Identity of them and identity of the fog node (ID_{FU}, ID_{FN}) to which they want to collaborate.

FU ----- (ID_{FU}, ID_{FN}) ---→ IDI

ii. After encountering the request from the particular fog user, the IDI computes fault message which consists of hash function of identity of fog user and secret key of IDI. This FU_{Auth} message is given to the fog user. To the fog node, the IDI computes FN_{Auth} that is hashed function of FU_{Auth} and is sent to the fog node.

$$FU_{Auth} = H (ID_{FU} (XOR) SK_{IDI})$$

$$FN_{Auth} = H (FU_{Auth})$$

Fig. 6 explains diagrammatic representation of the fog registration phase.

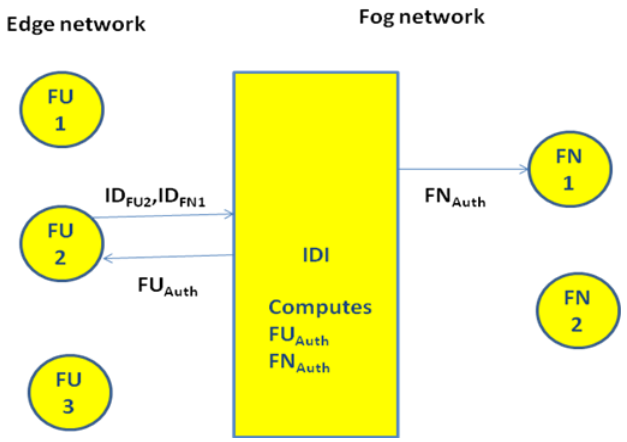

Fig. 6. Fog Registration

2. Mutual Authentication

In mutual authentication phase, the users from the edge network and the fog nodes from the fog network authenticate themselves to consequently by using authentication message which is received from the IDI. They made some calculations made from the random number chosen by fog users and fog nodes at the time of request made. The two stages of the phase are Fog user authentication and Fog node authentication.

a. Fog user authentication

i. Fog user computes concatenation of the user authentication message, Identity of the fog node and time stamp. Next, they perform a hash function of the computed value and perform an XOR operation with random number which is selected by the fog user at the time of request.

$$C = H (FU_{Auth}||ID_{FU}||TS) XOR (RAN_{FU})$$

ii. Fog user computes hash function of the random number which is chosen by the fog user.

$$M = H (RAN_{FU})$$

iii. After computation the fog user sends the request to the particular fog node which contains C, M, Identity of the user and timestamp.

iv. Initially, the fog node checks the timestamp whether it is valid or not. It will reject the request if it is not fresh.

v. At the fog node side, compute the random number value by using received C value. Then, the computed random number will fall in the process of hash computation. If the computed value matches with the received value, then, the fog node ensures the user as the valid user.

b. Fog node authentication

i. Fog node computes concatenation of the user authentication message, Identity of the fog node and time stamp. Next, it performs the hash function of the computed value and performs the XOR operation with a random number of the specified fog node at the time of computation.

$$D = H (FU_{Auth}||ID_{FN}||TS) XOR (RAN_{FN})$$

ii. Fog user computes hash function of the random number which is chosen by the fog node.

$$A = H (RAN_{FN})$$

iii. After computation the fog user sends the request to the particular fog user which contains D, A, and a timestamp.

iv. Initially, the fog node checks the timestamp whether it is valid or not. It will reject the request if it is not fresh.

v. At the fog user side, compute the random number value by using received D value. Then, the computed random number will fall in the process of hash computation. If the computed value, matches with the received value, then the fog user also ensures the node as the valid node.

Fig. 7 represents the overall view of the phase 2 mutual authentication.

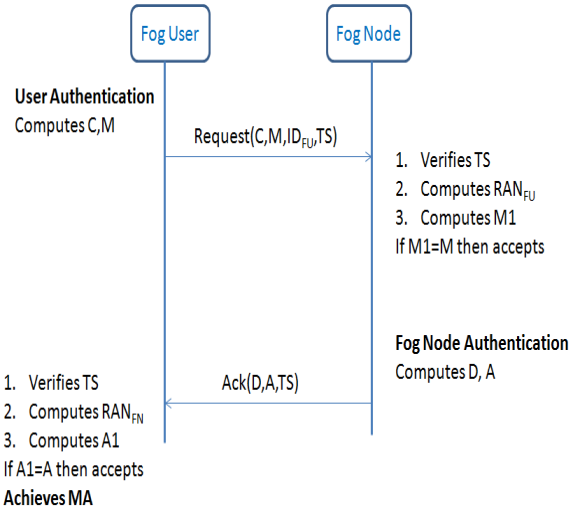

Fig. 7. Flow of Mutual Authentication

In real time, the proposed system is a perfect fit for fog computing environment with complete mutual authentication, trustworthiness, highly efficient with reduced computational cost.

IV. EVALUATION OF PROPOSED SCHEME

The proposed system implemented by Node JS for high level logic in server side, front end by angular, mongodb for storage purposes.

1. Security analysis

a. Mutual Authentication

The fog user sends the request to any one of the fog nodes contains computed value C, hash function of random number chosen by fog user, M, identity of the fog user and timestamp.

On the fog node side initially it will check the freshness of the request. While it is fresh then it computes a random number from his side. If it matches with the received request, then it will authorize the fog user as a genuine user. The same process will take place from the fog node to the fog user.

b. Stolen verifier attack

This proposed technique does not contain any table for passwords either at the IDI or at the fog node. At the request time, depends upon the random number the values are computed and sends the request. So the stolen verifier attack is impossible.

c. Replay attacks

If an attacker succeeds to get the request message from the fog user to the fog node (C, M, ID_{FU}, TS) then he cannot hit the fog node as an authorized person. Because random number will vary every time of the request and timestamp also added in the request. The initial stage of verification is to check the freshness of the request.

d. Password based attacks

The proposed scheme does not base on the password authentication scheme. Either the fog node or IDI does not contain any table to store the passwords. So this scheme is not vulnerable to the password based attacks.

Table I exhibits the comparison of security threats over legacy techniques to the proposed scheme.

Table I. Comparison over security

System / Factors	Octopus	MASFOG	Proposed
Mutual Authentication	Yes	Yes	Yes
Stolen verifier Attack	Yes	Yes	Yes
Replay Attack	Yes	Yes	Yes
Smartcard Attack	No	NA	NA
Computational Overhead	High	High	Low

*yes - Problem is resolved
No - Problem not resolved

2. Complexity evaluation

a. Storage evaluation

Fog User: for every fog user, it has to maintain only FU_{Auth} message for the entire process.

Fog Node: for every fog node, it has to maintain only FN_{Auth} message for the entire process.

IDI: It has to maintain only secret key of IDI.

b. Computation evaluation

Fog User: for every fog user, only in the mutual authentication phase, he has to compute some XOR operations and hash functions. In the registration phase, no computation takes place.

Fog Node: for every fog node, only in the mutual authentication phase, he has to compute some XOR operations and hash functions. In the registration phase, no computation takes place.

IDI: It has to execute some hash functions and XOR operations only in the registration phase. The IDI will keep idle in the mutual authentication phase.

Table II depicts the complexity evaluation based on the factors storage and computation.

Table II. Complexity evaluation

Members	Storage	Registration	Mutual Authentication
Fog User	One Authentication Message (FU_{Auth})	-	1. Hash Function (C) 2. XOR Operation 3. Hash Function (M)
Fog Node	One Authentication Message (FN_{Auth})	-	1. Hash Function (D) 2. XOR Operation 3. Hash Function (A)
IDI	Secret Key of IDI	1. Hash Function (FU_{Auth}) 2. XOR Operation 3. Hash Function (FN_{Auth})	-

Fig. 8 shows the result of fog users registration over the short period of time when the request is increasing enormously.

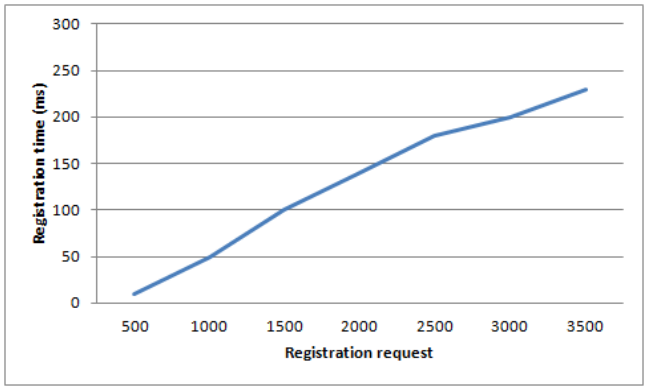

Fig.8. Registration

V. CONCLUSION

An enhanced mutual authentication scheme using ID is introduced in this paper for the fog computing environment. Both the fog users and fog nodes themselves register in IDI using ID to get the authentication message. This scheme eradicates the flaws of traditional authentication scheme. It is very efficient, trustworthy and easily adaptable to the fog computing. It resolves most of the security flaws of the system. In the result, it yields low computational and communication overheads. The primary objective of the system mutual authentication is achieved in an efficient and easy way. This scheme does not bags any overhead, which is related to storage factor for mutual authentication. This scheme is the perfect fit for the fog computing to achieve mutual authentication in an efficient method.

REFERENCES

1. M.Armbrust, A.Fox, R.Griffith, et.al., "A view of Cloud Computing" Communications of the ACM, Volume 53, pp.50-58, 2010.
2. Bonomi, Flavio,et.al. "Fog computing and its role in the internet of things", proceedings of the first edition of the MCC workshop on mobile cloud computing. ACM, 2012.
3. Shanhe Yi, Zhengrui Qin, Quan Li, "Security and privacy Issues of Fog Computing: A Survey", WASA, 2015.
4. Saad Khan, Simon Parkinson, Yongrui Qin, "Fog Computing Security: a review of current applications and security solutions" Journal of cloud computing, Advances, Systems and Applications" 2017, 6:19.
5. I.Stojmenovic and S.Wen, "The fog computing paradigm:Scenarios and security issues", IEEE Federated Conference on Computer Science and Information Systems, pp. 1-8, 2014.
6. Balfanz, Dirk et.al, "Talking to strangers:Authentication in Ad-Hoc wireless networks", NDSS, 2002.
7. Bouzefrane, Samiaet al., "cloudlets authentication in NFC based mobile computing", Mobile cloud computing, Services and Engineering (Mobile cloud), 2014 2nd IEEE International Conference on IEEE, 2014.
8. Manoj Kumar, "A new secure remote user authentication scheme with smart cards", International journal of Network Security11.2, 2010, 88-93.
9. R.Lu, Z.Cao,Z.Chai and x.Liang, "A simple user authentication scheme for grid computing", International journal of Network Security, volume 7, no. 2, pp. 202-206, 2008.
10. J.L.Tsai, "Efficient nonce based authentication scheme for session initiation protocol", International journal of Network security, volume 9, no. 1, pp. 12-16, 2009.
11. Ibrahim, Maged Hamada, "Octopus:An Edge-fog Mutual Authentication Scheme", International Journal of Network Security, 18.6, 2016.
12. Yousef Imine, Djamel-eddine kouicem, Ahmed Lounis, Abdelmadjid bouabdallah, "MASFOG: An Efficient Mutual Authentication Scheme for Fog Computing Architecture", 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering, 2018.

AUTHORS PROFILE

K.Sujatha, joined as a lecturer in the year 2007 in Anjalai Ammal Mahalingam Engineering College, Thiruvarur. She joined as an Assistant professor (O.G) in SRM University, Chennai in the year 2010. She received M.E degree in Software Engineering from Anna University in the year 2008. In 2015, joined as a research scholar in Hindustan Institute of Technology and Science, Chennai. She has5 years of experience in teaching. Published 1 research paper in scopus indexed journal. Presented 5 research articles in conferences. Research areas are Cloud and Fog Computing.

Dr.Ceronmani Sharmila, Joined as a Lecturer in the year 2003 in Hindustan College of Engineering and currently working as Associate Professor in Dept. of Information Technology, School of Computing Sciences, Hindustan Institute of Technology and Science. She received PhD degree titled "Strategic Connected Dominating Sets for Mobile Ad Hoc Networks" in Information Technology from Hindustan Institute of Technology and Science in the year 2016. She received M.E. Degree in Communication Systems from Anna University in the year 2007. She has 3 years of Industrial Experience in the field of VLSI and 16 years of Teaching Experience in Hindustan Institute of Technology and Science . Published 38 research papers in journals and conferences (including SCI & Scopus Indexed Journals). Received Best Faculty of the year 2017 at IIT Mumbai from Computer Society of India . Received Best Cyber Security Education Award of the year 2017 from Data Security Council of India (DSCI) at New Delhi. Received CLN Promotional Award from IET Professional Society in the year 2014. As a Convener organized DRDO Sponsored National Conference on Intelligent Information Systems. Attended and organized many workshops and seminars. FCE certified from Cambridge. D-Link Certified Trainer. IBM-ICE Trainer for the courses IT Infrastructure & Landscape, Cloud Computing Architecture and Cloud Deployment Model. Professional membership in IET and Lifetime Membership in CSI. Member of Elsevier Community and Research Innovation Explorers. Reviewer of Advances in Science, Technology and Engineering Systems Journal (ASTESJ). Research Areas are Computer Networks and Graph Theory.