Asian Journal of Computer Science and Technology
ISSN: 2249-0701 (P) Vol.7 No.2, 2018, pp.101-106

DOI: https://doi.org/10.51983/ajcst-2018.7.2.1862

Virtual Private Cloud and Authentication: A Review

GauravDeep[1], Rajni Mohana[2]and Paramroop Kaur[3]
[1]Assistant Professor, [3]PG Student
[1&3]Department of Computer Engineering, Punjabi University, Patiala, Punjab, India
[2]Assistant Professor , Jaypee University of Information Technology,Solan, Himachal Pradesh, India
E-mail: deepgaurav48@pbi.ac.in, rajnivimalpaul@gmail.com, paramroop17@gmail.com

(Received 12 July 2018; Revised 25 July 2018; Accepted 10 August 2018; Available online 16 August 2018)

***Abstract* - Cloud computing can be called as service through which computer resources could be used online. It helps to eliminate the need of usage of physical hardware rather it offers to use them on the cloud server. Different Types of cloud service models and deployment models make the cloud access to its users. The cloud supports characteristic such as on demand services, resource pooling, elasticity .While authentication plays important role in the security as it protects the data from the unauthorized people and helps to achieve trust between the service provider and the user. In this Paper, we've reviewed the existing work so as tounderstand the concept of cloud computing, virtual private cloud and proposed a multifactor authentication technique which uses biometric trait along with the identity password and MAC address as its factors.**

***Keywords:*Cloud Computing, Authentication, Encryption,Virtual Private Cloud and Validation Tools for security protocols**

I.INTRODUCTION

Cloud computing is a dynamic pool of computer resources which offers services to the user [1].And the data does not reside physically on your device or computer, but rather on the device of the cloud provider as cloud eliminates the need of storing data on hard drive or local storage devices. It delivers services to its user, from wherever the cloud can be accessed. The cloud should support characteristics as on demand services, high performance network access, resource pooling, rapid elasticity and metered services [4]. There are different cloud services as the public, private and hybrid clouds are provided by the cloud domains. It provides cloud users many benefits including availability, reduced costs, pay per use etc. The cloud services model is as below:

A. Cloud service models

Software as a service is a service (SaaS) provides software as a service through the internet. In SaaS, the user does not need to install and run the applications on his own computer [2]. Some of the examples of SaaS are CRM (Customer Relationship Management, Gmail, etc [1]. Platform as a service (PaaS) provide a platform environment for developing and managing applications and run them [2].The users are able to use resources like the hardware, storage, operating system on rent [3]. While some of the examples of PaaS are Microsoft's Azure, Google's App Engineetc. [1]. And the Infrastructure as a service (IaaS) provides users the capability to control the application, data, etc [2]. IaaS users are provided resources on demand [3].Some of the examples of IaaS are Eucalyptus,OpenStacketc [1].

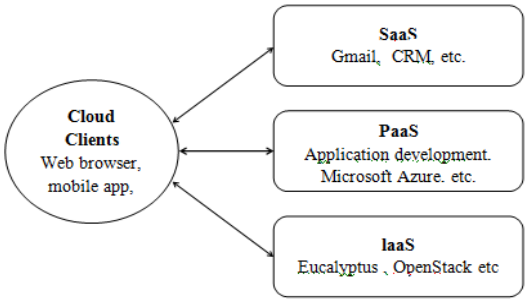

Fig. 1Cloud Service Models

B. Cloud deployment models are:Private cloud, Public cloud, Hybrid cloud, Community cloud

Private cloud: As its name implies private, is used by a single organization that is why called private cloud, so its resources or services are private to its organization only.The cloud infrastructure is monitored by the organization and its usage remain private to that organization only whereas its data remains secure with the organization[2]. While this model resembles Intranet which is used within an organization [1].

Public Cloud: A public cloud offers services that are open for the public use. In this cloud the data are sharedpublicly. Some of the examples are Google cloud platform, Microsoft Azure etc [2]. The nature of this deployment model resembles the internet which means services can be used where the internet is accessible [1].

Hybrid cloud: It is a combination of two clouds that are joined together to give services (Private, Public) [3]. The example of this cloud is Microsoft Azure Stack [1].

Community cloud: It provides services to specific community sharing some concerns and which use same shared resource [4].

Virtual Private cloud: It is a private cloud, but located in the public cloud, Its users pay the fixed amount [1].

II. AUTHENTICATION IN CLOUD

Authentication play an important role in cloud security. Various attacks can be prevented if efficient authentication

schemes be implemented. To secure the cloud users data located in different parts of the world from the hackers or from the unauthorized access or theft of personal data. There is a need to develop secure and efficient authentication techniques that can provide security from the theft, leakage attacks etc.

The typical existing authentication techniques:

1. Single factor authentication (id, password based): In single factor authentication it is easy for the attacker to know the ID and password of the user. The single factor authentication system mainly depends on the id-passwords and the system make the data unprotected and attackable.
2. Two factor authentication: As its name implies two factors means two authentication levels are used such as in an ATM, users swipe card, then enters a PIN (Personal Identification Number) code for the transaction to be done. Here the attacker must have the user's ATM card and PIN code.
3. Multi factor authentication: It is a method in which more than one authentication technique is applied so called multifactor authentication. Multi factor has many factors or many levels of authentication like passwords, fingerprints, smart card, voice, location, etc. Now, if the attackers get any one factor of the listed above he cannot get to the user's information and it is not possible for the attacker to get all the factors. In this, there are more factors for authentication to increase the authenticity level to break.
4. Single sign on: —Single Sign-On (SSO) is an authentication mechanism in which a Cloud Service Consumer (CSC) take benefit of single sign on by accessing services from service providers, or multiple services from the same service provider [6]. Single sign on preventing the user to remember many passwords as it helps to decrease the amount of time to type many passwords.
5. Biometric authentication: This type of authentication uses physicality (fingerprint, face, iris, ear, retina scan, hands, odor/scent, voice) and behavioral traits (walking, signature, typing pattern,) Biometric authentication helps in validation of legitimate users.
6. Location authentication: This is a technique in which authentication of a user is done by detecting his particular geographical location (latitude and longitude). The latitude and longitude are the coordinates of a place on the globe. Therefore, any place on the earth can be specified by the geographical location. Hence helps in authenticating the legitimate user.

III. AUTHENTICATION ISSUES IN CLOUD

The major issue in cloud is security, all the personal information of users data is stored on the service provider's cloud so in case of any disaster the data is at the risk of unavailbilty . Now the privacy protection becomes important if the data is compromised. Also integrity of the stored data is a quite challenge. Data stored in the clouds is only accessible via the internet [25]. And there is no transparency in the cloud which can provide the user to monitor their own information in the cloud. When a user uses more multiple services, his information is stored on multiple servers and hence copy of the user's data will be on more servers. To secure the data more authentication process has to enforce.There should be isolation of the data among various virtual machines.

IV. ENCRYPTION

Encryption is the process of making messages, communication between parties secure by converting them in an unreadable format to the intruder and decryption is the process of converting the unreadable form back to the readable form. The only person who knows the encryption and decryption keys can read the message. The key which is known to the public is called public key and the key which is secret is called the private key.

This process saves data from the intruder unless he/she knows the way to hack confidential data. The sender sends message with encryption algorithm, the receiver gets the messages and decrypts the messages using the decryption algorithm. Or in other words, the process of sending messages from plain text to unreadable form (cipher text) and converting unreadable form (cipher text) back to plain text is called encryption and decryption respectively [4]. The method of encryption and decryption can achieve by many ways, i.e. symmetric encryption and asymmetric encryption and decryption.

A. Symmetric Encryption

This encryption uses only a single secret key (private key) for the encryption and decryption. The symmetric encryption has benefited over the asymmetric encryption is the speed of the symmetric encryption [5]. The sender and receiver has the same shared secret key and DES (Data encryption Standard), AES (Advanced Encryption Standard), 3DES (Data encryption Standard), Blowfish is the common examples of symmetric encryption [4].

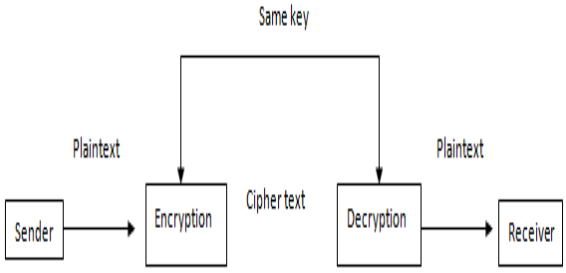

Fig. 2 Symmetric encryption/Decryption

B. Asymmetric Encryption

This encryption uses two keys as public key and secret key (private key) for encryption and decryption respectively. Asymmetric encryption compared to symmetric encryption

is slow [5]. RSA (Rivest, Shamir, Adelman), Diffie-Hellman are examples of asymmetric algorithms [4].

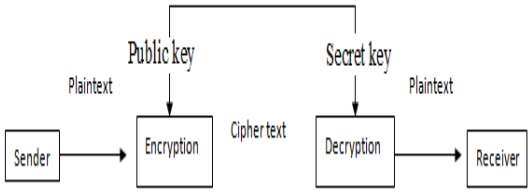

Fig. 3 Asymmetric encryption/Decryption

V. A VIRTUAL PRIVATE CLOUD (VPC)

A Virtual Private Cloud (VPC) is called the pool of resources of which are shared in the cloud combined with the infrastructure of VPN (Virtual private Network) [7] .Whereas A VPN is a method by which a private network is connected to a public network, i.e. the internet. To access securely a private network or company network, a virtual private network is used [6]. It is called virtual because the infrastructure is not shared with other VPC users and provide an isolated environment to VPC users. It is isolated, secure and stable environment. The data is stored on a public cloud, but it is isolated from the other users. It may include user defined IP address range and can be connected securely to data centers.

In Virtual Private server, the webmaster is responsible for the working of the website or the application in use. The webmaster has the control to look out for the working on the server, if the webmaster is unable to do so it can create a mess and unmanageable. The hardware is shared by users, so the VPS cannot use the full capacity of the RAM.

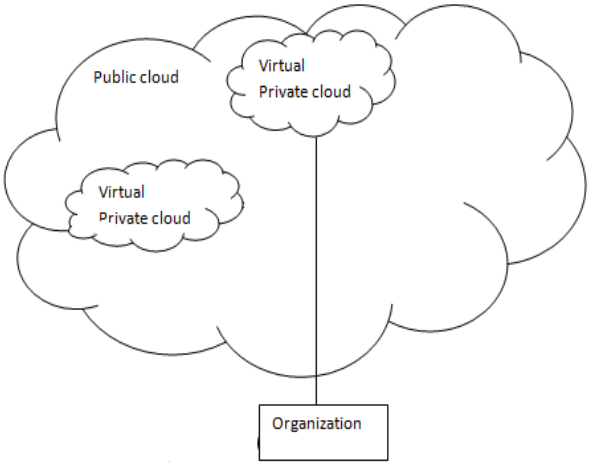

Fig. 4 A virtual private cloud

Virtual private cloud is considered as safest type of cloud among public and Hybrid cloud but it is also prone to various types of attacks such as Insider attack, DoS , Data Breach etc. In order to minimize the security challenges of a Cloud based Medicine Inventory System, there is a need to develop a robust secure system by using number of secure platforms and technologies that can encrypt the data and mutual authenticate between various parties like Doctors, Hospital management members, vendor, Accountant etc. this will lead to improvement of system privacy and security.

VI. RELATED STUDY

Many research publications have been published in this area while some of them are considered. Martial Michel *et al.* [2] talks about the cloud computing and tells the reason for using cloud computing in big data applications. While comparing public and private cloud, private cloud offers additional pros.

Majed Almubaddel*et al.* [3] has surveyed cloud computing concepts and giving examples of service usage in applications. Furthermore, cloud computing usage threats are also addressed. Description of the concepts of cloud, its service models, deployment models along with characteristics is addressedto.

Akashdeep Bhardwaj *et al.* [4] have presented a comparison of the security algorithms and has given special attention to the symmetric algorithms for the considerations in security.

Vincent Lozupone [5] has presented the description of cryptographic systems along with the analysis of symmetric an asymmetric encryption and the pros, cons of PKI i.e. Public Key Infrastructure.The difference of the symmetric and asymmetric encryption is also addressed.

Daniel Palomares*et al.* [6] proposed a scheme that provided reliability and the elasticity for the virtual private clouds based on the IP Sec. It was shown the way to improvise VPN infrastructures in terms of traffic management and high availability through the sharing of IP session. They measured the impact of traffic management and high availability through simulation of phone conversation.

Timothy Wood *et al.*[7] have proposed a method which includes the abstraction of the virtual cloud pool and have presented a way of VCP that uses the combined technology of controllers with VPN, and described the challenges in setting the VCP abstraction. Their VCP is quite similar to the product of the Amazon private cloud.

Luigi Coppolino *et al.* [8] has presented an analysis of threats in the way of adoption of the cloud computing and tells that the paper is a navigation tool for the industry personnel as they can understand the risks to the cloud usage.

Rad*et al.* [9] has presented the analysis on cloud with their challenges in the adoption and issues. The benefits of clouds, security issues like privacy, confidentiality have also been mentioned in this paper.

Robert Birke*et al.* [14] has presented a study on the concept ofvirtualization and shows the working of the VM including their patterns of migration, frequency of migration across the servers which are physically different.It was also shown

that how the data centers use the virtualization techniques in the private cloud.

F. John Krautheim [15] has proposed a model for the security and management of the cloud namely, Private Virtual Infrastructure.Owner of the data has control over the data center while the structure of the cloud is under the service provider. It says that the a secure structure is the responsibility of the vendor while protection of the data is in the hands of owners of the information.

Bhatia *et al.* [16] a comprehensive study has been done on the cryptographic, biometric multifactor solutions for the security of data in the clouds. It also highlighted the security issues in the environment of the mobile cloud along with the future research issues.Roy *et al.* [17] proposed a method of multifactor authentication, which takes consideration effects of various users, media, environments to check whether the user is legitimate or not.

Tsai*et al.* [18] a scheme is proposed by the authors which provides multiple access using a single private key from multiple service providers that can be used only for distributed mobile cloud services environment. This scheme uses a cryptographic system of bilinear pairing with the usage of nonce generation (dynamic). In addition, this scheme proposed by the authors supports mutual authentication, key exchange, the anonymity of the user and the traceability of the user. The scheme has eliminated the need for the verification tables for the smart card generators (SCG). It also reduces the memory consumption and authentication processing time between the service providers and trusted third party service.

TABLE 1 COMPARISON OF EXISTING WORK

S No.	Name of the paper	Method	Advantages	Limitations
1	Tsai *et al* (2015)	Bilinear pairing cryptosystem and dynamic nonce generation.	i) The scheme supports mutual authentication, key exchange, user anonymity, and user untraceability. ii) In this scheme verification tables are not required.	Time consumed by hash operations is not considered in this Scheme.
2	Nematollah*et al*(2017)	Multipurpose speech watermarking and online speaker recognition	Proposed Multi factor Authentication model helps in Enhancing the security of the systems against attacks	1. The proposed model is proof-of-concept only. 2. In this model adversary can affect the working of model by destroying the watermark.
3	Roy *et al*(2017)	Genetic algorithm, NSGAII algorithm	It is capable of handling the uncertainty which arises due to the availability/unavailability of different trusted levels of authentication modalities	The scheme does not cover the influences of other surrounding conditions in the selection process.
4	Fan Wu *et al*(2017)	Wireless sensor network for the health applications using two factor authentication	The scheme is secured authentication and can be used practically when compared to other existing WSNs.	The cost of time of login and authentication is higher than the comparable schemes on the gateway side.
5	Shehzad Ashraf Chaudhry *et al* (2017)	Authentication scheme to preserve privacy for the SIP(session Initiation Protocol) based on the ECC	The scheme supports mutual authentication and resists attacks.	The proposed scheme takes more memory in the smart card and overhead in the communication with some of the schemes compared to purposed.
6	Azeem Irshad *et al* (2017)	Authentication scheme based on the biometric over the server	The scheme provides perfect forward secrecy, password can be modified and also is able to verify the user authenticity .	The scheme costs slightly higher than some of the compared schemes and lacks the overhead communication cost .
7	Zhangbing Li *et al* (2016)	RFID scheme for mutual authentication	The scheme is resistant to many attacks and offers privacy protection.	Storing the tag is quite difficult because of its size is larger and there is more computational loads on the tag.
8	Prosanta Gope *et al* (2018)	RFID authentication scheme	The schemes gives forward secrecy, user anonymity , secure localization and RFID tag untraceabililty	1.The scheme is not secured from the physical and cloning attacks. 2.The server can be compromised and forgery attacks can be performed. 3.The scheme ha more computational cost and takes tomes to compute fourteen hash operations.

Nematollahi*et al.* [19] has developed a scheme called Multi factor authentication by a combination of OTP (One Time Password) and PIN (Personal Identification Number) and a speaker biometric through the speech watermarks. The proposed authentication scheme approves security against communication and spoofing attack. It also improves the recognizing performance.

VII. AVAILABLE SECURITY PROTOCOL VALIDATION TOOLS

There are many validation tools available in the market through which the process of validating is performed. Some of the tools are:

*Avispa:*Automated Validation of Internet Security Protocols and Applicationsfor the specification security of protocols and properties it gives away, expressive formal language[10]. It also provides the integration of different back-ends, which implements automatic analysis technique from attack finding on the input protocol called protocol falsification to the verification based on abstraction methods that are used for the finite and infinite number of sessions.

ProVerif:it analyzes an unbounded number of sessions. It has two types of input as a Horn clause or of Pi-calculus. Through the use of ProVerif, an attack can be classified as active or the passive attack. It is able to support the public channel and private channel. A trace is produced by the tool and does not produce a trace of counter example. Because of the over approximation, it sometimes we get false positive attacks[11].

FDR: provides a time based analysis of using the tool for analyzing a large collection of existing protocols. It is not able to do the verification of the knowledge proof of the non interactive zero and is an expressive tool [11].

*MATLAB:*It is a programming language stands for MATrix LABoratory which supports object oriented and includes data structure, and built in editing tools to debug. It is used for teaching and research. The basic data element is an array, commands are MATLAB specific and designed for scientific computing [13].

Scyther: It is used for the falsification, verification and the analysis of security protocols [12]. Scyther provides a graphical user interface and can verify protocols with an unbounded or bounded number of sessions. It uses a language to write protocols called SPDL (Security Protocol Description Language). The tool can prove the correctness, classification of attacks, protocol behaviors that are for an unbounded number of sessions of a protocol. It gives 80 percent unbounded verification or falsification cases and 20 percent cases of bounded verification.Verification is easy in Scyther as it provides a graphical user interface and can verify protocols with an unbounded or bounded number of sessions. When an attack is found by the tool, it produces an attack graph. All possible protocol claims can be verified through the Scyther on a protocol. It is a pattern refinement algorithm based that gives the brief and to the point representation of (infinite) sets of traces [12]. For Scyther it is possible to generate claims if the protocol does not hold any security claim. It helps users assess the properties and to verify or falsify them easily. The representation of the protocol has small number of patterns that can be executed.

VIII. PROPOSED METHDODLOGY

As the name implies Multi-factor authentication, it means the authentication process where two or more possible factors of authentication are combined. To secure the user information while preventing the attackers to gain access is the purpose of the multi-factor authentication as it provides defense in a layered mechanism and it requires the attacker to break levels to get access into a system.

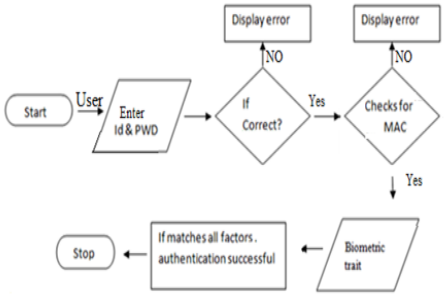

Fig. 5 Proposed multi-factor authentication

The proposed method; the user enters the login id and password and the authenticator checks for the same in the database if matches proceed next step, then authenticator checks for the registered Desktop system (MAC Address Via Payload) which should send data access request from within the Hospital Boundary. After checking the required MAC Address, at next step it demands the biometric authentication of the user. By doing so it can be decided whether the user is authorized or not. All the communication that takes place between the Authenticator and user is done by using AES.

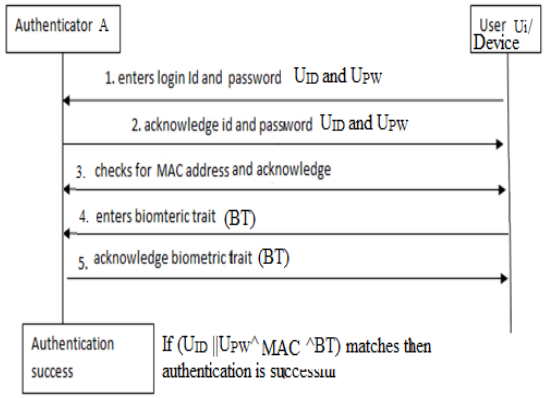

Fig.6 Flow of data for desired Authentication between Authenticator A and User Ui

For the process of authentication in the proposed methodology following conditions are taken into

considerations: identity password, MAC address and Biometric trait. Authentication will be given by authenticator when all the conditions are matched. It will work only when all the details stored on the database server in the Virtual Private cloud match with the detail of the request.

IX. CONCLUSION

With the advent in the area of cloud computing and usage of internet by so many people, the network comes under the attack by attackers. The attacks on security of cloud put pressure on the service provider to provide more security to the data. So authentication is an essential component that can decrease a certain level of security breach.Authentication is the way to secure the confidential and personal data on the cloud servers which adds one stepmore to securityof the data.

REFERENCES

[1] S. K. Naresh and P.C.P Bhatt, " Cloud Computing: Concepts and Practices", *Springer*, 2018.

[2] M. Michel, Serres, O., Anbar, A., Golden, E. J., and El-Ghazawi, T.,"Open Source Private Cloud Platforms for Big Data", In *Big Data Analytics for Sensor-Network Collected Intelligence*, pp. 63-80, 2017.

[3] M. Almubaddel, and Elmogy, A. M.,"Cloud computing antecedents, challenges, and directions", In *Proceedings of the International Conference on Internet of things and Cloud Computing*, ACM,p. 16, *2016*.

[4] Bhardwaj, Subrahmanyam, G. V. B., Avasthi, V., and Sastry, H.,"Security algorithms for cloud computing", *Procedia Computer Science*, vol*85*, pp: 535-542, 2016.

[5] V. Lozupone, "Analyze encryption and public key infrastructure (PKI)", *International Journal of Information Management*, vol. 38, no. 1, pp. 42-44, 2018.

[6] Palomares, D., Migault, D., Hendrik, H., Laurent, M., &Pujolle, G.,"Elastic virtual private cloud", In *Proceedings of the 10th ACM symposium on QoS and security for wireless and mobile networks* (pp. 127-131).ACM, 2014.

[7] T.Wood, Shenoy, P. J., Gerber, A., van der Merwe, J. E., and Ramakrishnan, K. K, "The Case for Enterprise-Ready Virtual Private Clouds", In *HotCloud*.2009.

[8] L.Coppolino, D'Antonio, S., Mazzeo, G., andRomano, L.,"Cloud security: Emerging threats and current solutions", *Computers & Electrical Engineering*, vol*59*, pp-126-140, 2017.

[9] B.Rad, B., Diaby, T., and Rana, M. E,"Cloud computing adoption: a short review of issues and challenges", In *Proceedings of the 2017 International Conference on E-commerce, E-Business and E-Government*, ACM, pp. 51-55,2017.

[10] A.Armando, Basin, D., Boichut, Y., Chevalier, Y.,Compagna, L., Cuéllar, J., and Mödersheim, S.," The AVISPA tool for the automated validation of internet security protocols and applications". In *International conference on computer aided verification* (pp. 281-285). Springer, Berlin, Heidelberg, 2005.

[11] M.Moran, and Wallach, D. S.," Verification of STAR-Vote and Evaluation of FDR andProVerif", In *International Conference on Integrated Formal Methods*, Springer, Cham, pp. 422-436, 2017.

[12] C.J. Cremers, "The scyther tool: Verification, falsification, and analysis of security protocols", In *International Conference on Computer Aided Verification*, Springer, Berlin, Heidelberg.(pp. 414-418), 2008.

[13] D.Houcque,"Introduction to Matlab for engineering students", *Northwestern University*, pp. 1-64, 2005.

[14] R.Birke, Podzimek, A., Chen, L. Y., and Smirni, E.,"Virtualization in the private cloud: State of the practice", *IEEE Transactions on Network and Service Management*, vol13, no. 3,pp. 608-621, 2016.

[15] F. J. Krautheim,"Private Virtual Infrastructure for Cloud Computing", In *HotCloud*,2009.

[16] T.Bhatia, and Verma, A. K.," Data security in mobile cloud computing paradigm: a survey, taxonomy and open research issues", *The Journal of Supercomputing*, vol. *73*, no. 6,pp. 2558-2631, 2017.

[17] Roy,andDasgupta, D.," A fuzzy decision support system for multifactor authentication", *Soft Computing*, pp.1-23, 2017.

[18] J. L.Tsai, and Lo, N. W., "A privacy-aware authentication scheme for distributed mobile cloud computing services", *IEEE systems journal*, vol. *9*, no. 3,pp. 805-815,2015.

[19] M. A.Nematollahi, Gamboa-Rosales, H., Martinez-Ruiz, F. J., Jose, I., Al-Haddad, S. A. R., and Esmaeilpour, M.,"Multi-factor authentication model based on multipurpose speech watermarking and online speaker recognition", *Multimedia Tools and Applications*, vol. *76*, *no.* 5,pp. 7251-7281, 2017.

[20] Wu, F., Xu, L., Kumari, S., and Li, X.,"An improved and anonymous two-factor authentication protocol for health-care applications with wireless medical sensor networks", *Multimedia Systems*, vol. *23*, no. 2, pp. 195-205, 2017.

[21] S. A.Chaudhry, H.Naqvi, Sher, M., Farash, M. S., and Hassan, M. U.," An improved and provably secure privacy preserving authentication protocol for SIP", *Peer-to-Peer Networking and Applications*, vol. *10,no.* 1,pp. 1-15, 2017.

[22] P.,Gope, R. Amin, Islam, S. H., Kumar, N., and Bhalla, V. K.,"Lightweight and privacy-preserving RFID authentication scheme for distributed IoT infrastructure with secure localization services for smart city environment", *Future Generation Computer Systems*, vol . *83*,pp: 629-637, 2018.

[23] A.Irshad,S.Kumari, Li, X., Wu, F., Chaudhry, S. A., andArshad, H. ,"An improved SIP authentication scheme based on server-oriented biometric verification", *Wireless Personal Communications*, vol. *97*, *no.* 2,pp. 2145-2166,2017.

[24] Z. Li, X. Zhong, Chen, X., and Liu, J.,"A lightweight hash-based mutual authentication protocol for RFID", In *International Workshop on Management of Information, Processes and Cooperation*, Springer, Singapore, pp. 87-98, 2016.

[25] P.Spanaki, and N.Sklavos,"Cloud Computing: Security Issues and Establishing Virtual Cloud Environment via Vagrant to Secure Cloud Hosts",In *Computer and Network Security Essentials*, Springer, Cham,pp. 539-553, 2018.