International Journal of Engineering & Technology, 7 (4.12) (2018) 47-51
International Journal of Engineering & Technology
Website: www.sciencepubco.com/index.php/IJET
Research paper

Multifactor Authentication for Hospital Inventory access in Virtual Private Cloud

Gaurav deep[1], Paramroop Kaur[2], Rajni Mohana[3*]

[1]Research Scholar, Department of CSE & IT ,JUIT, Solan
[1]Assistant Professor, Department of CE, Punjabi University, Patiala
[2]Research Scholar , Department of CE, Punjabi University, Patiala
[3]Assistant Professor, Department of CSE & IT ,JUIT, Solan
**Corresponding author E-mail: rajni.mohana@juit.ac.in*

Abstract

In recent times, cloud computing has influenced every sector of life, from managing user database online on the cloud to access it on the cloud makes it more flexible to use. Cloud computing has its own security issues like privacy, integrity, confidentiality and authentication. In order to access data on the cloud Authentication majorly plays a very important role. This paper presents a secure multifactor authentication that can be used for Hospital Inventory access in Virtual Private Cloud. Virtual Private cloud is having the benefit of localization as all the data of cloud are accessible within the organization. To secure Hospital Inventory access in Virtual Private Cloud this paper proposes multifactor authentication technique using Biometric, MAC address via payload .The proposed a multifactor authentication protocol which is also validated by using a validation tool Scyther. The outcomes indicate that the proposed multifactor authentication is a robust technique.

Keywords: *Virtual Private cloud, Multi factor, Authentication, Media Access Control, Biometric*

1. Introduction

Modern healthcare services use new technologies to facilitate various activities of health care. Moving Hospital inventory control to the Virtual Private cloud (VPC) [1] provides the benefits of the cloud by saving time, reducing human errors and providing accessibility from any place within the vicinity. This provides Real time monitoring and connectivity between hospitals and vendors in VPC. This proposed infrastructure connects all components of the logistical and operational chain with real-time inventory accessible simultaneously to both hospital and vendor. Real time monitoring plays critical role in case of shortage of lifesaving medicines and at the time of epidemics. However, usage of cloud computing has its own risk also, unauthorized access to customer and business data, security attacks, data breach as managed by the third party may affect the performance of the overall system.

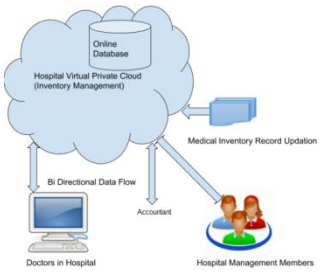

Fig. 1: Hospital medicine inventory with different supplier/vendors

In Figure 1 a scenario is presented where any physician of any department / Management of hospital can check the Medicine stock status from his desktop system via a cabled net. Doctors, Accountant and management can also check the Expiry date, manufacturer detail and price value of the medicine .The current status of medicine can be easily checked by the doctor whenever the crises arises.

Motivation

Private virtual 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 [2], etc. To reduce 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. The system can just not rely on features provided by the cloud service providers and existing cloud platform.

Key Highlights of this paper:-

Although many multi factor authentication schemes have been developed but there is a need of authentication method which provides more levels of security than existing ones. The proposed multifactor authentication technique uses Biometric, MAC address via payload to secure the system. The proposed multifactor authentication technique has following features:

i) It will not let the attacker to gain access into the system, as it is not possible for the attacker to get all the facts at the same time
ii) Prevents the system from insider attack
iii) Checks the authenticity of the user device also.

This paper has proposed multi factor authentication Protocol, in this Multiple factors said to be true to get access to the system. The verification of the protocol is shown by the Scyther tool.

Organization of the paper

The organization of the paper is as follows, Section 2 discusses various Authentication Techniques with their limitations discusses in existing work. Section 3 describes the proposed authentication. Section 4 includes the verification of the proposed methodology by scyther tool and finally the paper is concluded in Section 5.

2. Background

Any user who wants to use the services of the cloud has to be authenticated every time. The typical existing authentication techniques used are as follows:

1. Single factor authentication: In this 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 .As in the case of ATM, user swipes 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 to gain access [3].
3. Multi factor authentication: It is a method in which more than one authentication technique is applied. Multi factor has many factors 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 [3].
4. Single Sign on: -To take the benefit of single sign in on the cloud for accessing various service providers, or when accessing multiple services from the same service provider Single Sign-On authentication mechanism is available [5]. It prevents 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 physical (fingerprint, face, iris, ear, retina scan, hands, odor/scent, and voice) and behavioral traits (walking, signature, typing pattern,) [4] Biometric authentication helps in validation of legitimate users.
6. Location based authentication: It is a technique of authenticating a user by detecting his particular geographical location (latitude and longitude) [9]. The latitude and longitude are the coordinates of a place on the globe. Hence helps in authenticating the legitimate user.

2.1 Related study

Many research papers related to the cloud authentication domain have been published. Thomas et al [5], has implemented Single Sign on (SSO) mechanism on cloud federation scenario, results showed the proposed approach provides benefits in the reduction of execution time of the user requests when multiple services are accessed from CSPs in the cloud federation.

Amin et al [6] proposed a user authentication with smart card and key agreement protocol for a Telecare medical information system .It uses a cryptographic one way hash function, which achieves security protection on attacks and better complexities with login password change phase. Jiang et al [7] proposed a robust three factor authentication using ECC which provides security properties and from various attacks, preserve user privacy. Saha et al [8] presented the classification of pharmaceuticals to improve the performance of hospital inventory management based on the patient condition. Roy et al [10] proposed a multifactor authentication scheme which takes considerations the effects of various users, media, and environments to check whether the user is legitimate or not.

Tsai et al [11] proposed a scheme by which multiple access can be done from multiple service providers using a single private key only for distributed mobile cloud services environment. Jiang et al [12] talks about the vulnerability attacks on the wireless networks and proposed a two factor authentication protocol using ECC (elliptic curve cryptography). Their scheme achieves the security and usability features.

Nematollahi et al [13] has developed a Multi factor authentication by a combination of OTP (One Time Password), PIN and a speaker biometric through the speech watermarks. The proposed authentication scheme approves security against communication and spoofing attack. Xie, et al [14] proposed an Anonymous Two-Factor AKE (Authenticated Key Exchange) protocol scheme that provides security against a number of attacks and supports properties like perfect forward secrecy, un traceability. The protocol messages are short in length and do not require a large number of message flow.

Chandrakar et al [15] proposed a secure anonymous three factor based remote user authentication using ECC that can be used in the multi-server environment. This scheme also provides mutual authentication and session key agreement, and proves it to be efficient in smart card storage cost, communication cost, computation cost and estimated time to the existing schemes. Liu et al[16] proposed a User-Centered Design (UCD) data backup scheme by using multi-factor authentication, in this the user selects a key and it is divided into three shares and the key then is deleted .To regain it has to be combined from where its shares has been stored in the user smart card or in the system. Existing techniques are not able to prevent insider attack and are not able authenticate user device.

3 Proposed multi-factor authentication

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 the system as shown in Figure 2.

In the proposed work, the user enters the login id and password and the authenticator checks for the same in the database. If it matches, 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 the authenticator 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 as shown in Figure 3.

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 matches with the detail of the request. Different notations used in building Protocol are shown in table 1.

Table 1. Notations used

Description	Notation
User	U_i
User Identity	U_{ID}
Authenticator	A
User Password	U_{PW}
Biometric Trait	BT

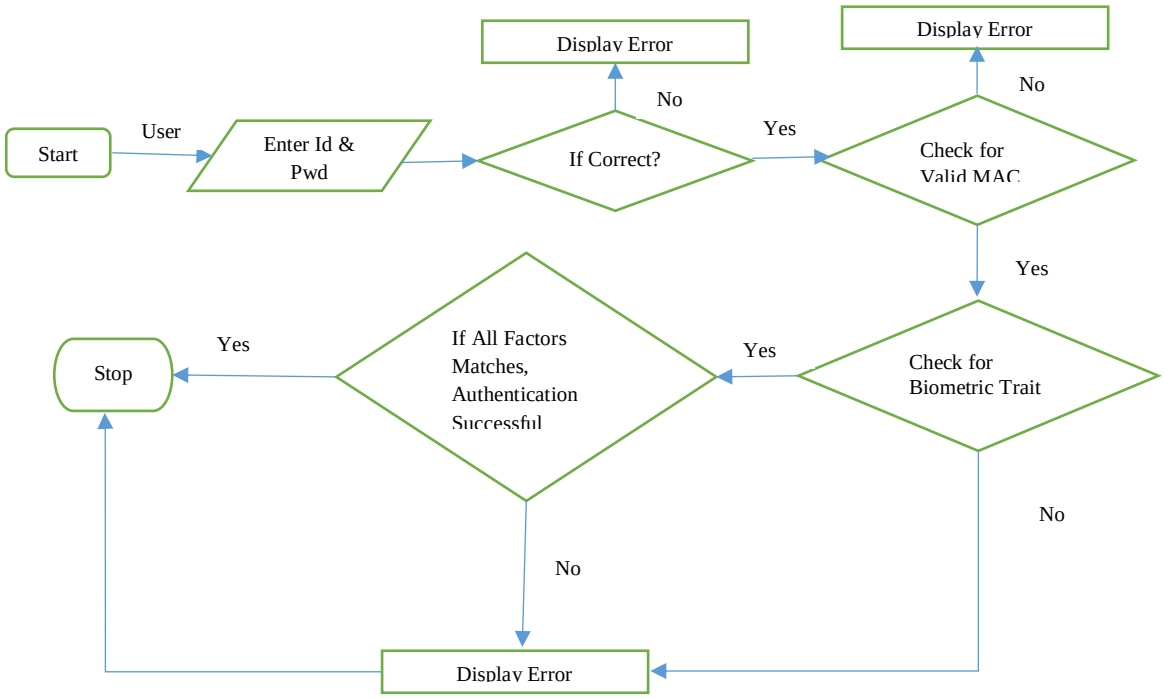

Fig. 2: Proposed multi-factor authentication

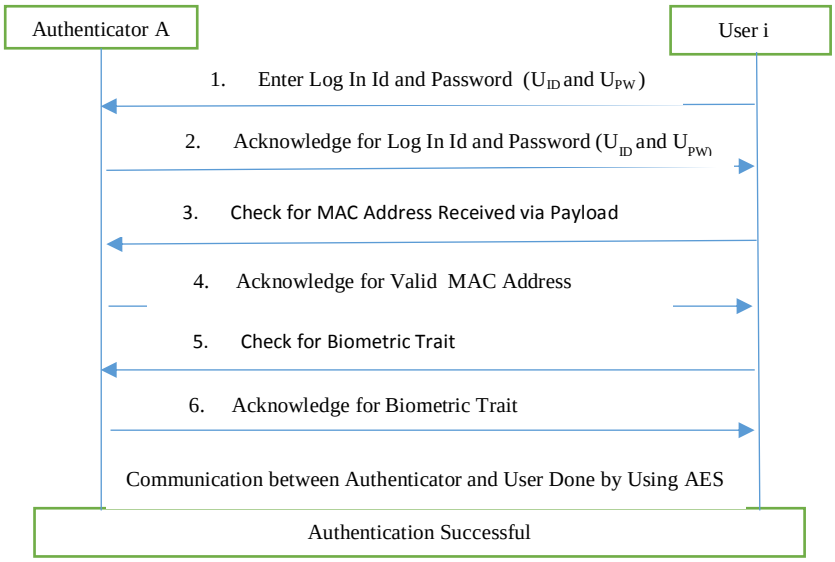

Fig. 3. Flow of data between Authenticator A and User Ui

Algorithm: Multifactor Authentication for Virtual Private Cloud.
Input: User Identity, User Password, Mac address (accessed via payload), Biometric Trait of user
Output: Authentication Granted:-Yes / No
Procedure:
Step1: If Entered Ui= =Stored Ui
Then Match Entered Psw= =Stored Psw
If Outcome is Yes Go To Step 2:
Else Give error message "user detail doesn't Exist/Match"
Go To Step4:
Step 2: If System Mac address (accessed via payload) = =stored Mac Address
Then fetch Biometric Trait of user= =Stored Biometric Trait
If Outcome is Yes Go To Step 3:
Else Give error message "user detail doesn't match"
Go To Step4:
Step3: If all parameters match
Then Grant authentication
Else Deny authentication.
Go To Step4:
Step4: Quit authentication phase
End Procedure
Once all the factors are true only then accessing is allowed, otherwise access is denied. At the same time, a hacker cannot get all the components at the same time and hence multi factor authentication provides security to the user data.

4. Verification by the Scyther tool

Scyther 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 [17][18].

The output of scyther in Figure 4 shows the protocol test results in which the status is ok meaning, there are no attacks within the bound. The use of nonces ensures that the old communications cannot be reused as nonce is an arbitrary number that is used once.

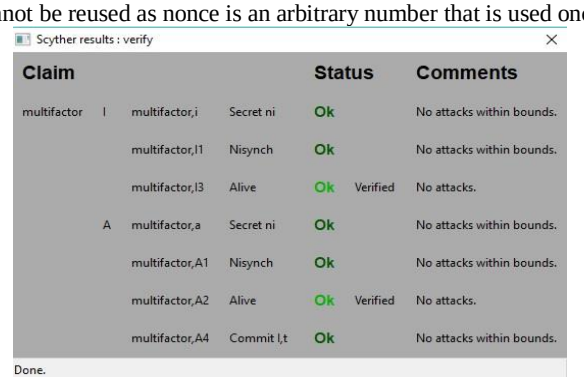

Fig. 4: Output for scyther claim test for I and A

Secret shows the secrecy of the data and confidentiality of the data to the user. Aliveness means that the role in the protocol (I, A) is alive and available at any time. Nisynch stands for Non-injective Synchronization and ensures the successful synchronization between the parties and commitment describes the promise made one party to the other. So from the scyther results it can be concluded that the protocol can withstand attacks like replay attacks, DOS attacks, impersonation attack etc. It also ensures the confidentiality and secrecy.

Fig. 5: Verify automatic claim results

As we can see that in figure 5 Automatic claims were verified and no attacks were found within bounds.

5. Conclusion

Security is undeniably an important concern for everyone. The data should be protected from being accessed by unauthorized persons; that is why cloud should provide more security to its users. In the proposed work medicine inventory system too needs to be protected from the unauthorized access, theft or alteration of the data on Virtual Private cloud. Multi-factor authentication in medicine inventory control will secure the system by allowing only authenticated user which includes all the conditions to be met for the secure authentication, to fill up the details for the medicine inventory. To remove the limitations of single factor authentication and two factor authentication there is need of multi factors to be included in authentication schemes. In the future Multi factor Authentication IP trace back and asymmetric keys can also be used.

References

[1] Farrukh Nadeem and Rizwan Qaiser, "An Early Evaluation and Comparison of Three Private Cloud Computing Software Platforms", Journal of Computer Science and Technology, Volume 30, Issue 3, May 2015, pp 639–654, https://doi.org/10.1007/s11390-015-1550-1

[2] Tatiana Galibus, Viktor V. Krasnoproshin, Robson de Oliveira Albuquerque and Edison Pignaton de Freitas," Elements of Cloud Storage Security", Springer International Publishing,2016, XII, 101, https://doi.org/10.1007/978-3-319-44962-3_2

[3] Nils Fleischhacker, Mark Manulis and Amir Azodi," A Modular Framework for Multi-Factor Authentication and Key Exchange", Security Standardisation Research,2014, pp 190-214 , https://doi.org/10.1007/978-3-319-14054-4_12

[4] Qi Jiang, Zhiren Chen, Bingyan Li, Jian Shen, Li Yang and Jianfeng Ma," Security analysis and improvement of bio-hashing based three-factor authentication scheme for telecare medical information systems", Journal of Ambient Intelligence and Humanized Computing, pp 1–13, https://doi.org/10.1007/s12652-017-0516-2

[5] Manoj V. Thomas, Anand Dhole and K. Chandrasekaran ," Single sign-on in cloud federation using cloud sim.",International Journal of Computer Network and Information Security, Vol. 7, No. 6, May. 2015, PP.50-58, DOI:10.5815/ijcnis.2015.06.06

[6] Ruhul Amin and G. P. Biswas," A Novel User Authentication and Key Agreement Protocol for Accessing Multi-Medical Server Usable in TMIS", Journal of Medical Systems, Volume 39 Issue 3, March 2015 Pages 1-17, https://doi.org/10.1007/s10916-015-0217-3.

[7] Qi Jiang , Muhammad Khurram Khan , Xiang Lu , Jianfeng Ma and Debiao He ," A privacy preserving three-factor authentication protocol for e-Health clouds ",The Journal of Supercomputing , Volume 72 Issue 10, October 2016 ,Pages 3826-3849 https://doi.org/10.1007/s11227-015-1610-x

[8] Esha Saha and Pradip Kumar Ray," Inventory Management and Analysis of Pharmaceuticals in a Healthcare System", Healthcare Systems Management: Methodologies and Applications , pp 71-95 https://doi.org/10.1007/978-981-10-5631-4_7

[9] Yusuf Albayram, Mohammad Maifi Hasan Khan, Athanasios Bamis, Sotirios Kentros, Nhan Nguyen and Ruhua Jiang," Designing challenge questions for location-based authentication systems: a real-life study", Human-centric Computing and Information Sciences, 2015, https://doi.org/10.1186/s13673-015-0032-3

[10] Arunava Roy and Dipankar Dasgupta," A fuzzy decision support system for multifactor authentication", Soft Computing, Volume 22, Issue 12, June 2018, pp 3959–3981 https://doi.org/10.1007/s00500-017-2607-6

[11] Jia-Lun Tsai and Nai-Wei Lo," A Privacy-Aware Authentication Scheme for Distributed Mobile Cloud Computing Services ", IEEE Systems Journal , Volume: 9 Issue: 3, 805-815. DOI: 10.1109/JSYST.2014.2322973

[12] Qi Jiang ,Neeraj Kumar ,Jianfeng Ma ,Jian Shen ,Debiao He and Naveen Chilamkurti," A privacy-aware two-factor authentication protocol based on elliptic curve cryptography for wireless sensor networks",.International Journal of Network Management, 2016, https://doi.org /10.1002/nem.1937

[13]Mohammad Ali Nematollahi , Hamurabi Gamboa-Rosales , Francisco J. Martinez-Ruiz , Jose I. De la Rosa-Vargas , S. A. R. Al-Haddad and Mansour Esmaeilpour," Multi-factor authentication model based on multipurpose speech watermarking and online speaker recognition", Multimedia Tools and Applications, Volume 76, Issue 5,2017, pp 7251–7281,https://doi.org/10.1007/s11042-016-3350-1.

[14] Qi Xie , Duncan S. Wong , Guilin Wang , Xiao Tan , Kefei Chen and Liming Fang ," Provably Secure Dynamic ID-Based Anonymous Two-Factor Authenticated Key Exchange Protocol With Extended Security Model ",IEEE Transactions on Information Forensics and Security, Volume: 12 Issue: 6,2017,pp-1382-1392. DOI: 10.1109/TIFS.2017.2659640

[15] PreetiChandrakar and Hari Om," A Secure and Robust Anonymous Three-Factor Remote User Authentication Scheme for Multi-Server Environment Using ECC", Computer Communications. Vol 110,2017, pp 26-34,https://doi.org/10.1016/j.comcom.2017.05.009

[16] Yining Liu , Qi Zhong , Liang Chang , Zhe Xia , Debiao He and Chi Cheng ," A secure data backup scheme using multi-factor authentication.".IET Information Security,Vol 11,Issue 5,2017.pp250-255, DOI: 10.1049/iet-ifs.2016.0103

[17] Cas J. F. Cremers," The Scyther Tool: Verification, Falsification, and Analysis of Security Protocols. ",Computer Aided Verification, Lecture Notes in Computer Science, vol 51232008,pp 414-418 https://doi.org/10.1007/978-3-540-70545-1_38

[18] Reema Patel , Bhavesh Borisaniya , Avi Patel , Dhiren Patel , Muttukrishnan Rajarajan and Andrea Zisman ," Comparative Analysis of Formal Model Checking Tools for Security Protocol Verification.", Recent Trends in Network Security and Applications,vol 89,2010,pp152-163, DOIhttps://doi.org/10.1007/978-3-642-14478-3_16