Int. J. Nonlinear Anal. Appl. 13 (2022) No. 1, 765-771
ISSN: 2008-6822 (electronic)
http://dx.doi.org/10.22075/ijnaa.2022.5583

# Medical data encryption in private cloud based on MAR

Ahmed Dheyaa Radhi[a,*], Baqer A Hakim[b], Fuqdan AL-Ibraheemi[c]

[a]College of Pharmacy, University of Al-Ameed, Karbala PO Box 198, Iraq
[b]College of Dentistry, University of Al-Ameed, Karbala PO Box 198, Iraq
[c]Department of Computer Engineering and Information Technology, Faculty of Engineering, Razi University, Kermanshah, Iran

(Communicated by Madjid Eshaghi Gordji)

## Abstract

It's easy to exchange files, folders, and emails in a private network with the aid of a private cloud (PriCld). However, the most common attack with this sort of system is the guessing of the password. The unencrypted connection makes it potential for a man-in-the-middle attack (MaMiAtk) to occur at times. Scanners used to discover vulnerabilities in the system and exploiting them are also a major issue. Therefore, a system that can withstand assaults such as MaMiAtk, Denial of Service Attack (DoS attack), and password guessing is required. In the presented study, a log-based analysis approach has been recommended to guard the system against assaults such as DoS attack, password guessing, and automated scanners. We also use encrypted channels to prevent attacks such as MaMiAtk.

*Keywords:* Denial of service (DoS attack); Medical Record Analysis (MAR); Private Cloud (PriCld); man-in-the-middle (MaMiAtk).

## 1. Introduction

PriCld make it easier to exchange information, but like any technology, they come with their own set of advantages and disadvantages. There are four key requirements for a security system: privacy, authenticity, integrity, and non-repudiation (P.A.I.N) [2]. According to privacy, medical data or files that are sent cannot be viewed by uninvited third party. Access to medical data should be restricted

*Corresponding author
*Email addresses:* ahmosawi@alameed.edu.iq (Ahmed Dheyaa Radhi), h.bagher@alameed.edu.iq (Baqer A Hakim), fuqdan@razi.ac.ir (Fuqdan AL-Ibraheemi)

*Received:* August 2021 *Accepted:* September 2021

to the verified individuals only. Integrity refers to the fact that unauthorized parties cannot alter medical data during transmission. Non-repudiation implies that the sender cannot dispute that they transmitted the communication. As a result of security concerns, files are now delivered encrypted [2, 9]. Many cryptographic methods had been created to safeguard the private system.

On the basis of key distribution method, cryptographic systems may be divided into two main categories. The most often used encryption systems are those that employ symmetric key encryption, which encrypts and decrypts files and communications using the same key. That's because anyone with the key can decode it [9]. The main difficulty with this sort of cryptographic technique is that the key is shared between many parties. As a result, an additional communication channel is employed to transmit the key securely. A brute force assault or a MaMiAtk can easily crack this password [12]. Symmetric key cryptography has the benefit of providing more anonymity, but it is unable to address concerns such as authenticity, integrity, and non-repudiation [5]. An authentication system that can verify that the client (patient) is allowed, maintains the integrity of files, and ensures non-repudiation will be needed. An asymmetric key based encryption system with digital certificate and digital signature is the appropriate option for P.A.I.N [1]. It is common for servers to authenticate clients using SSL signature. Services such as SSL and TLS are the most common. The creation and distribution of the key [6] are the primary issues in this sort of system. Despite hardware-based solutions are available, they are not scalable. Using asymmetric key cryptography, we have developed a system for the transmission of medical files that is scalable for big users (or specialists) and uses software-based key generation. For security reasons, this technology transmits medical records in encrypted form, preventing unauthorized parties from accessing them [1, 7].

## 2. Medical Records Analysis (MAR)

In layman's words, MAR is a thorough search, examination, assessment, and interpretation of medical records. It is carried out by experts with a thorough understanding of medicine and expertise analyzing medical data, such as doctors, registered nurses, pharmacists, and other healthcare workers. MAR, permits user the following:

- Retrieve indexed, paginated, and date-stamped medical records that are arranged by facility, provider, date, document type, or customizable data fields.
- Keep a record of all medical occurrences.
- Make a list of all medical professionals.
- Examine your injuries.
- Determine what circumstances contributed to the reported injury.
- Examine and compare witness statements.
- Determine the minimum standards of care and the legal obligations.
- Receive medical material that has been carefully studied and summarized.

## 3. The Proposed Algorithm Authentication

To overcome the problem of the PriCld, we have proposed a more secured cloud based file sharing system framework that is more resistant to different attacks. Figure1 shows the flow of the security system. The basic work flow is given below:

- Browser based file sharing system or cloud
- To create a secured transmission channel
- Minimize the attack possibilities by differentiating between legitimate traffic and automated traffic.
- To create a secured authentication system
- Server side encryption

As shown in the flowchart 1, when the user (patient) wants to access or share the medical file with specialists, he/she will send the request through the browser. The system will check whether the traffic is HTTPS or not, if the traffic is not https then it will provide an SSL certificate and converts it to https. Due to this, the client will receive an SSL certificate which will provide the authenticity of the server to the client and the channel will be encrypted so that the medical data is safe in transmission [11].
Next step is to find whether the traffic is legitimate or not. To this end, we suggest a log based method. If the scanners like NMAP is trying to scan the cloud server than the logs like given in figure 2 is generated. So, if we make any script that can automatically detect this type of attack than this host can be banned [8]. We are using the same methods to protect the system from the DoS attack. We can limit the attacker that if its requesting more than predefined attempts than it will be blocked [13]. We can define DoS attack by searching the text "$\%(_prefix_line)s$Did not receive identification string from $< HOST > \backslash s^*\$$" and by modifying firewall rules we can ban that IP address [4].

To find the authenticity of the user (patient), a database in which the patient name and hashes of passwords were saved was made. Password is generated through the asymmetric key-based password generation and authentication technique which cannot be breakable. To protect the system from the password guessing attack, we can monitor the logs of failed attempts and if the failed attempts are above the predefined limit then ban the host. There should be a system by which automatic log monitoring is possible, so that if there is any intrusion is detected than it can be banned. Like if any attacker tries to send many request at a time, tries to scan the website than it should be banned [13, 4].
Our next step is to validate the user (patient) so that there is a database created in the server which stores the users (patients) and their passwords hashes. When clients (users) want to access their account they have to enter the correct user name and password. As shown in the flowchart, total number of failed login attempts are counted, so that if the number of failed attacks are increasing than the predefined limit then that user (not a real patient) should be banned, and only authorized user can able to take access [10]. To protect the medical file in a way that administrators (specialists) can also not view the data, we can use the same asymmetric key-based encryption method by using the user's password (patient's password) as a key and encrypting files on the server. Therefore, users (patients) having the correct key can only view the sensitive data [3].

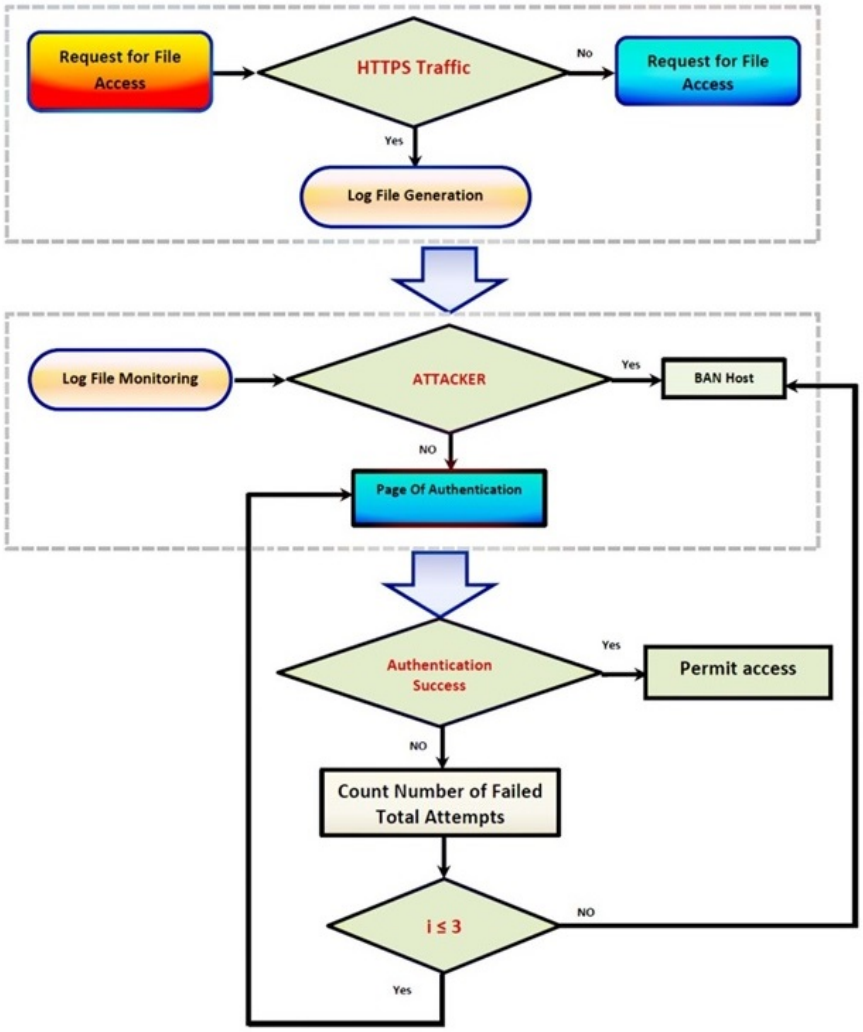


Figure 1: The flowchart of the proposed system

```
192.168.1.1 - - [11/Oct/2018:11:36:24 +0200] "GET /index.php/apps
192.168.1.1 - - [11/Oct/2018:11:36:25 +0200] "GET /index.php/apps
192.168.1.1 - - [11/Oct/2018:11:36:25 +0200] "GET /index.php/apps
192.168.1.1 - - [11/Oct/2018:11:36:27 +0200] "GET /index.php/apps
192.168.1.1 - - [11/Oct/2018:11:36:28 +0200] "GET /index.php/apps
192.168.1.1 - - [11/Oct/2018:11:36:29 +0200] "GET /index.php/apps
192.168.1.1 - - [11/Oct/2018:11:36:31 +0200] "GET /index.php/apps
192.168.1.1 - - [11/Oct/2018:11:36:32 +0200] "GET /index.php/apps
192.168.1.1 - - [11/Oct/2018:11:36:32 +0200] "GET /index.php/apps
192.168.1.1 - - [11/Oct/2018:11:36:34 +0200] "GET /index.php/apps
192.168.1.1 - - [11/Oct/2018:11:36:35 +0200] "GET /index.php/apps
192.168.1.1 - - [11/Oct/2018:11:36:35 +0200] "GET /index.php/apps
192.168.1.1 - - [11/Oct/2018:11:36:37 +0200] "GET /index.php/apps
192.168.1.1 - - [11/Oct/2018:11:36:39 +0200] "GET /index.php/apps
192.168.1.1 - - [11/Oct/2018:11:36:39 +0200] "GET /index.php/apps
192.168.1.1 - - [11/Oct/2018:11:36:40 +0200] "GET /index.php/apps
192.168.1.1 - - [11/Oct/2018:11:36:42 +0200] "GET /index.php/apps
192.168.1.1 - - [11/Oct/2018:11:36:42 +0200] "GET /index.php/apps
192.168.1.1 - - [11/Oct/2018:11:36:44 +0200] "GET /index.php/apps
192.168.1.1 - - [11/Oct/2018:11:36:46 +0200] "GET /index.php/apps
192.168.1.1 - - [11/Oct/2018:11:36:46 +0200] "GET /index.php/apps
192.168.1.1 - - [11/Oct/2018:11:36:47 +0200] "GET /index.php/apps
```

Figure 2: A strange log file access

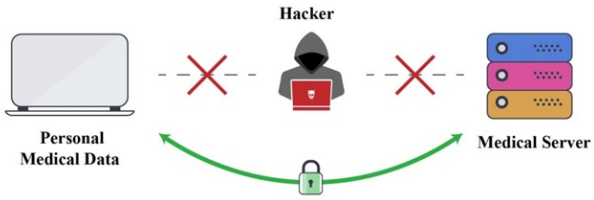


Figure 3: MaMiAtk scheme

## 4. A Man in the middle Attack (MaMiAtk)

MaMiAtk is a phrase that describes a situation in which a hacker intercepts communication between two parties, either to surreptitiously eavesdrop or manipulate the data being sent between them. These attacks are used by hackers to steal login credentials or personal information, spy on the target, damage data, or sabotage communications in general. Most of its consumers are financial apps and cloud services users as well as early adopters of e-commerce sites. MaMiAtk is shown in figure 3:

## 5. A Denial-of-Service Attack (DoS)

As a DoS attack aims to push a system / network into a dead end, making it inaccessible for the future users, it floods the target with traffic / provides data that causes it to crash. In all cases, a DoS attack prohibit open users (i.e. workers, members, or account holders) that they had hoped for. A denial of service attack is depicted in Figure 4.

## 6. Results and Analysis

### *6.1. Attack 1: Password guessing*

For the implementation purpose, we are using OwnCloud as public cloud system and the Fail2Ban for automatic log analysis. IP of OwnCloud is 192.16.224.130. 172.16.224.1 is an attacker's IP address

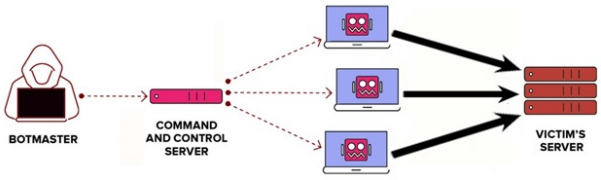


Figure 4: DoS attack scheme


Figure 5: Attack work scheme

which tries to enter different password and username to get the correct username (patient's name) and password. Figure 5 shows the attacker's machine trying to add different passwords. Figure 6, shows the service of the attacker machine is banned.

### *6.2. Attack 2: Scanning of server's IP*

Figure 7 shows that the automated scanners will give the information about ownCloud server hosed on IP 192.168.86.139.

### *6.3. Attack3: MaMiAtk*

The medical data traveling between the machines is encrypted so that cannot be disclosed to the middlemen or intruder. Figure 8 shows the encrypted traffic. Now, if the user is legitimate (i.e. real patient), he/she will allow using the service like shown in figure 8 which shows the admin panel.

## 7. Conclusions

PriClds are very useful in sharing the files and mails easily but it is not secure due to improper configuration and security loopholes. These vulnerabilities make the system unauthorized access to the file that can be very harmful for organizations. We tried to give a log based solution to prevent the attacks like password guessing, DoS attack and scanning with automated tools. In addition, the secured channel will not allow passive attack like information gathering through channel.

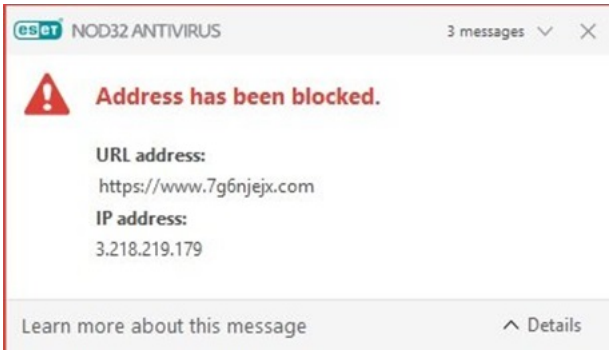


Figure 6: IP banned-attackers

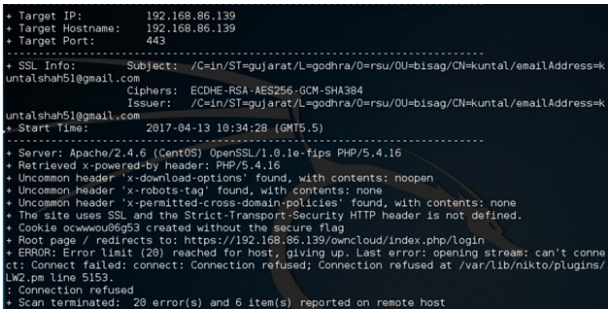


Figure 7: A strange access log file

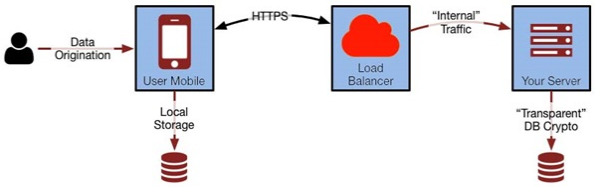


Figure 8: Transmitting encrypted data

## References

[1] A.S. Abdulbaqi, A.A. Abdulhameed and A.J. Obaid, *Cardiopathy symptoms diagnosis based on a secure real-time ECG signal transmission*, Int. J. Nonlinear Anal. and Appl. 12(2) (2021) 1353–1370.

[2] A.S. Abdulbaqi and R.H. Mahdi, *Biometrics detection and recognition based-on geometrical features extraction*, In 2018 Int. Conf. Adv. Sustainable Engin. Appl. IEEE, (2018) 59–63.

[3] A.S. Abdulbaqi, A.J. Obaid and A.H. Mohammed, *ECG signals recruitment to implement a new technique for medical image encryption*, J. Discrete Math. Sci. Crypt. (2021) 1–11.

[4] J.M. Beaver, C.T. Symons, R.E. Gillen, *A learning system for discriminating variants of malicious network traffic*, 8th Annual Cyber Security and Information Intelligence Research Workshop, (2012) pp. 1–4.

[5] D.S.A. Elminaam, H.M.K. Abdual and M.M. Hadhoud, *Evaluating the performance of symmetric encryption algorithms*, Int. J. Network Secur. 10(3) (2010) 216–222.

[6] N. Gura, A. Patel, A. Wander, H. Eberle and S.C. Shantz, *Comparing elliptic curve cryptography and RSA on 8-bit CPUs*, M. Joye and J.J. Quisquater (eds), Cryptographic Hardware and Embedded Systems - CHES 2004, 3156 (2004) 119–132.

[7] A. Khalique, K. Singh and S. Sood, *A password-authenticated key agreement scheme based on ECC using smart cards*, Int. J. Comput. Appl. 2(3) (2010) 26–30.

[8] G. Lakshmi, M. Ghonge and A.J. Obaid, *Cloud Based IoT Smart Healthcare System for Remote Patient Monitoring*, EAI Endorsed Transactions on Pervasive Health and Technology, 2021.

[9] P. Mell and T. Grance, *The NIST Definition of Cloud Computing, Computer Security Division*, Inf. Tech. Lab. Nat. Inst. Stand. Tech. 800(145) (2011).

[10] J. Owens and J. Matthews, *A study of passwords and methods used in brute-force SSH attacks*, USENIX Workshop on Large Scale Exploits and Emergent Threats (LEET), 2008.

[11] R.L. Rivest, A. Shamir and L. Adleman, *A method for obtaining digital signatures and public-key cryptosystems*, Commun. ACM Magazine 21(2) (1978) 120–126.

[12] S.P. Singh and R. Maini, *Comparison of data encryption algorithms*, Int. J. Comput. Sci. Commun. 2(1) (2011) 125–127.

[13] M. Strebe, *Network Security Foundations: Technology Fundamentals for IT Success*, Wiley, 2004.