Securing and Hiding the Destination of Confidential Medical Information with Domain Fronting

Gulara Muradova
Azerbaijan Technical University
Baku, Azerbaijan
gulara.muradova@gmail.com

Mehran Hematyar
Azerbaijan Technical University
Tehran, Iran
m.hemmatyar@outlook.com

Abstract— **E-Health is a developed infrastructure, which usage becomes important to control access to personal patients' data, as well as to various medical resources. The need for confidentiality of personal medical data and control of access is necessitated by the safety concerns. This paper shows Domain Fronting technology application method that significantly decreases unauthorized accesses and illegal actions into the E-health system. It uses a method of hiding visits to a resource by redirecting received requests to arbitrary addresses.**

Keywords— E-Health; personal medical data; information security; illegal access; hiding data; safety; privacy; HTTP; HTTPS ; DNS; CDN; Domain Fronting

I. INTRODUCTION

The public importance of the problem of protecting personal data is in the focus of attention of all countries. International practice shows that the vulnerability of confidentiality and security of personal data of patients is a major obstacle to the effective development of e-medicine [1,2]. At present, medical organizations generate and store large volumes of data. Information regarding the personal data of patients plays an important role in conducting clinical, epidemiological, environmental and other scientific studies that improve the quality of health care. However, the disclosure of health information to researchers raises concerns about privacy breaches. This is due to the fact that not only medical professionals who are responsible for maintaining medical confidentiality, but also other agents such as the Internet and hosting providers, cloud service operators are involved in this process [3].

The protection of personal data can be considered as a single complex (object) of regulation or as a set of problems, each of which is regulated within various legislative, normative and regulatory frameworks (contextual inviolability). The Convention of the Council of Europe on the Protection of Individuals is developed with regard to automated processing of personal data. The organizations that we share our personal data with are responsible for the nondisclosure of those [4-10].

The cloud-based network covers medical and statistical information about the health status of the population and the activities of various types of medical organizations. The network covers all aspects, both technical and organizational, including legislative, of health information exchange aspects. After connecting to the cloud, one can control this data flow to obtain information on population groups, territorial, medical and demographic indicators of fertility, morbidity, disability, and mortality. Here one is able to find extensive information about the physiological features of a person, namely - the structure of her body, fingerprints, palms, retina as well as DNA analysis [11,12]. However, the public dissemination of information can cause sizable physical or moral suffering. There emerges the need to eliminate the illegal access, risks of unwanted disclosure of personal medical data of public people. It is required to regulate the possibility of using electronic personal medical data for scientific research and use of private information in statistical activities of the government. [13,14]. An unauthorized access to computer information results in the unlawful receipt, disclosure and use of patient personal data. Crimes in the area of breach of confidentiality of personal health information is one of the most urgent issues [15].

II. CONFIDENTIALITY ISSUES OF PERSONAL MEDICAL DATA

Unauthorized access to the network infrastructure of a medical information system by outsiders, former employees, patients, hackers, etc. is the penetration to an organization's network system from outside to gain access to patient information or render the system inoperable. Hackers use their intellectual abilities to develop methods of criminal attacks on computer information, mainly "hacks" of computer protection and security systems. Attackers seize control of resources hacking into a computer system for the purpose of theft and gaining access to confidential information. Protection of personal data is an obstacle to the realization of public interests or the national security. There exist numerous ways to use information with malicious intent and it should be protected accordingly. The proliferation of a variety of monitoring and control technologies requires the development of a whole set of policy tools to protect personal data, determine the coordinates of the synchronization of new technologies and organizational practices, and their impact on the protection of personal data [16]. The paper proposes to use personal data protection methods through built-in confidentiality technology policy and by hiding the ultimate goal of the connection, as currently there is not sustainable countermeasure against this method. [17].

The modern-day Internet is an enormous and complex system consisting of a set of intermediate nodes that can be controlled by various people, organizations, or government structures. In modern conditions, a patient receives treatment and is being examined in different institutions depending on the specialization of medical institutions, insurance programs, criteria for the cost of services, etc. In particular, the images taken at the diagnostic center are in demand both at the outpatient clinic that sent for examination and at the hospital where the patient will be treated. Upon completion of treatment, they should be available in other clinics for the rehabilitation phase. Clinics that participate in the exchange of medical data can be completely independent and operate on the basis of different information systems and receive information about all integrated databases. Dozens of specialized regional health information organizations comprise government regulators, hospitals and clinics of various size, medical communities, insurance companies, major payers, and other structures. Medical companies should take care of the safety of their patients at clinics as well as online [18]. When integrated into a single information space, the introduction of secure communication channels is required for data transmission. Remote servers without the consent of the patients can record any information on their own local disks. Public information about personal data may be detrimental to their patients [19]. There are many different technologies that allow you to hide the contents of the transmitted data [20-23]. But in most cases, the transmission channel is not encrypted, and therefore, the identity of a sender to the IP address of the sender, the location of the sender to the resource IP address and the sent content is known. There is a need to ensure the establishment of a control point of the authorized body through which all messages will pass. Thus, the task of hiding not only the transmitted data, but also the very fact of their transmission arises. To achieve this goal, it is necessary to hide the fact that the data resource is being accessed [24]. The broad use of various monitoring and control technologies required the development of a whole set of policy tools for protecting personal data in order to determine the coordinates of synchronization of new technologies and organizational practices as well as their impact on the protection of personal data [25-27]. Literature review shows that method Domain Fronting is currently used in government organizations where strict control of data transmission is required to detect and prevent any criminal and non-authorized activities. [24,28] We propose to establish global standards for data protection in e-medicine.

III. Domain Fronting a Useful Technique for E-Health System

Domain Fronting - method for entangle circumvention traffic with other traffic. Domain Fronting is a new masquerading technique we can use to censor Internet censorship with traffic visibility, as it relates to unlimited web domain but here we try to use it in order to securing the sensitive information. All information sent to the Internet is directed to the recipient in the form of packages, and the protocols for the sending and security of these packets are used [17]. We can provide examples of several Internet protocols, but Hyper Text Transfer Protocol (HTTP) and Secured HTTP protocol (HTTPS) are more commonly used. HTTPS executes almost the same function as other protocols, but it also has a distinction that it differs from other protocols, using cryptographic encryption such as (Secure Sockets Layer) SSL and Transport Layer Security (TLS) encryption. This protocol has the capability to encrypt everything else except Host Domain. Generally, Domain Fronting is based on address delivery networks (CDNs) that have multiple domains. CDN is a content delivery network or content distribution network geographically serves as a distribution network of proxy servers and their data. While CDN is managed by a company like Akamai, Amazon, Microsoft Azure, or CloudFlare, a CDN can contain thousands of different types of domains [29,30]. Because of the features of CDNs, mobile providers and censorship-proxies cannot simply block them, as it will block many web sites and services without their knowledge. In this technique the main purpose is to hide the destination IP address or Domain Name, in this way we can hide the end-point Domain name for some goals include censorship or filtering the Website or hiding data from hackers based on destination addresses. We think that this technique can be used as a security service or security solution to hide the destination site from Hackers, in other hand it means to decrease the rate of attacks to the main server according to unknown destination address. In this technique a request sent to middle server such as Amazon Web Service and try to create a HTTPS. Other configurations allow a content delivery network's CDN common HTTPS certificate and infrastructure to act as a reflector through to the target server behind. Domain fronting generally is a way to bypass censor, filters and locks by hiding the End-Point of a connection using the features of a CDN. This method is possible and usable in modern CDNs because of containing two principal parts that exist independently of each other and, in another hand, interact with each other only in terms of establishing a TCP/IP connection with each other:

- External part that is responsible for establishing a secure connection between start (clinics, users and etc., and End point by E-Health Domain Front Servers with SSL certificate data transmission.
- Internal part that is responsible for fast processing the immediately sent request after decryption. Usually – HTTP/HTTPS request.

A main (general)-purpose circumvention tool - technique based on HTTPS Protocol that hides the actual destination of a medical website or medical web server from a filter. Generally, in this method we want to advice a security solution based in E-Health purpose to secure and hide the destination of medical information on Domain Fronting. The fig. 1 illustrate that:

1) A user' computer sends a HTTP(S) / TLS request to CDN servers such as Google, Amazon etc.

2) The server responds and picks the header and send the packet to real /main server.

3) Main server receives and respond the request to CDN server.

4) CDN server respond to user as edge server.

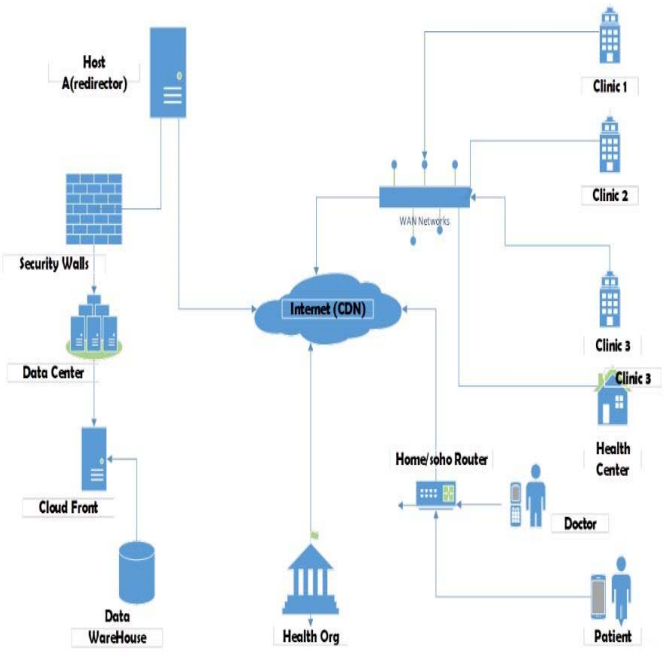

Fig. 1. Protect of confidential information in medical resources with Domain Fronting

Domain fronting server in this method receives the requests and after encryption passes it to the main server, the connection uses the Domain Fronting server to send, receive and encrypting E-Health data (fig. 1). In this method the medical data transmission endpoint will be hide due to hide the data under HTTPS protocol in application layer by E-Health Domain Front Servers.

IV. Using teleclinic.az as a Real the Template

The domain fronting bases on internet's HTTP and HTTPS protocols, using the TLS standard, and using CDNs, to manipulate and change the way in which firewall rules and deep packet inspection are processed or handled. As a typical web request, domain names processing as explain:

- As a part of a Domain Name System (DNS) sending a query for the IP address of the Destination site.
- In the Server Name Indication (SNI) session extension of Transport Layer Security.
- In the HTTP "host" header of the Web request.

For standard HTTP data traffic, all three instances of the domain name are visible to an internet / government censor's or "man in the middle" attack machinery – but and under the HTTPS protocol, the HTTP header is really encrypted. This makes it possible for owner or developer to substitute the name of their favored destination under the HTTP header – and this destination is a proxy server, Tor bridge, Freegate, Psiphone or VPN gateway which uses this technique. To anyone monitoring the connection between the web client and the CDN such as MITM (Man in the Middle attack), data shows to be streaming towards an approved site, while it's really being re-directed to another destination address [30].

This **Wget** command describes to check how to domain fronts on Amazon, one of big fronting-capable services.

There are plenty of other CDNs that could be used but Amazon has the easiest setup. Here is a HTTPS request has a Host header for aws.amazon.com, even as the DNS query and the SNI (Server Name Indication) custom SSL. SNI stands for Server name Indication and is an extension of TLS protocol which allows a server to host multiple hostnames under the same IP. Nowadays SNI is supported by most modern internet browsers and provides an efficient and secure way to deliver content over HTTPS using our own domain with or without SSL certificate in the TLS handshake specify www.amazon.com. Here it's clear that the response comes from https://aws.amazon.com/

```
$ wget -q -O - https://www.amazon.com/ --header 'Host:
aws.amazon.com' | grep -o '<title>.*</title>'
<title>Amazon AWS</title>
```

Here's how you can do it manually in your shell using Openssl's client:

```
$ openssl s_client -host www.teleclinic.az -port 443
CONNECTED (00000009)
depth=1 C = US, O = Let's Encrypt, CN = Let's Encrypt
Authority X3
verify error:num=19:
NET:ERR_CERT_COMMON_NAME_INVALID
verify return:0
---
Certificate chain
0 s:/CN=www.teleclinic.az
i:/C=US/O=Let's Encrypt/CN=Let's Encrypt Authority X3
…
<snip>
```

That's all it takes to reach the main page of **www.teleclinic.az**

If it sent the server a host header that it isn't responsible for it happens as follows:

```
$ openssl s_client -host www.teleclinic.az -port 443
---
GET / HTTP/1.1
Host: www.facebook.com

HTTP/1.1 403 Forbidden
Date: Sun, 1 May 2019 17:34:18 GMT 4+
Server: Apache/3.4.10
Content-Length: 325
…
```

Let's to see how Domain Fronting works. In Amazon's CDN, that's **megamed.cloudfront.net**. If you would just connect to this domain in the usual way, it could be easily reviewed by tracing that domain in the DNS, SNI or in many other ways. But if we connect to another domain of Amazon's CDN and set **playforce.cloudfront.net** as our host header we can give the correct answer.

```
$ openssl s_client -host megamed.cloudfront.net -port 443
---
GET / HTTP/1.1
Host: playforce.cloudfront.net

HTTP/1.1 180 OK
Date: Sun, 1 May 2019 17:34:18 GMT 4+
...
```

Now we could able to hide destination server address from censored or under supervision connections to www.teleclinic.az

CONCLUSION

Protection of patients' personal data in E-health systems integrated into a single information space requires an introduction of secure communication channels for data transmission. The quality of information protection depends on the technology used. Domain Fronting technology successfully deals with the increasingly large-scale problem of identity theft on the Web. It is important to maintain a complex balance between the confidentiality of patients' personal data and the openness of this data for medical workers of clinics, and modern information protection technologies should take care of this. Domain Fronting can be used to build hidden channels for the transmission of patients' personal data, as well as to identify and block information leakage channels. Domain fronting is a tool-technique that hides actual destination of a medical website that hackers are trying to connect to from network monitors. The technology contributes to hiding patients' or doctors' present addresses and the confidentiality of the transmitted data between them. Domain Fronting method facilitates a special control of access to the module of genealogical records, including information about patient's relatives' state of health. If a doctor requests access to a patient record without having a permission using Domain Fronting method, then the doctor's access will be denied because the domain fronting technology is hidden behind the public domain. We have presented Domain fronting method that uses different domain names at different communication layers in order to hide confidential information in medical resources.

REFERENCES

[1] G. Greenleaf, "Global Data Privacy in a Networked World," 2011. [Online]. Available:http://ssrn.com/abstract=1954296.

[2] D. Schoeman, Philosophical Dimensions of Privacy: An Anthology, Cambridge University Press, 1984, pp.403-412.

[3] M. Duplaga, "The Impact of Information Technology on Quality of Healthcare Services," Lecture Notes in Computer Science, Springer, Berlin, vol 3039, 2004, pp.1118-1120.

[4] Y.B.Choi, K.E. Capitan, J.S Krause, M.M. Streeper, "Challenges Associated with Privacy in Healthcare Industry: Implementation of HIPAA and Security Rules," Journal of Medical Systems, vol.30, no.1, 2006, pp.57–64.

[5] D. Schoeman, Philosophical Dimensions of Privacy: An Anthology, Cambridge University Press, 1984, pp.403-412.

[6] J.G. Hodge, L.O Gostin, P.D Jacobbson, "Legal Issues Concerning Health Information: Privacy, Quality, and Liability," Journal of American Medical Association, vol.282, no.15, 1999, pp.1466–1471.

[7] S. D. Warren and L. D. Brandeis, "The right to privacy," Harvard Law Review,vol.4,no.5,pp.193–220,1890.[Online].Available: http://www.jstor.org/stable/1321160.

[8] Paul Craig and Grainne De Burca, "Chapter 11 Human rights in the EU," EU Law: Text, Cases and Materials (4th ed.). Oxford: Oxford University Press, 2007, pp.15.

[9] E.P. Mikhaylova, A.N. Bartko, Biomedical ethics: theory, principals and problems. - M.: Publishing house of Moscow Museum of Modern Art, 1996, pp120-139.

[10] Paul de Hert and Vagelis Papakonstantinou, "Three scenarios for international governance of data privacy: Towards an international data privacy organization, preferably a UN agency," Journal of Law and Policy, vol.9, no.2, 2013, pp.279-311.

[11] C. Sibona, S.Walczak, J. Brickey, M. Parthasarathy, "Patient perceptions of electronic medical records: physician satisfaction, portability, security and quality of care," International Journal of Healthcare Technology and Management, 2011, vol. 12, pp. 62-84.

[12] P. Datta, A. Siami Namin, M.Chatterjee, "A Survey of Privacy Concerns in Wearable Devices," 2018IEEE International Conference on Big DataDec, Seattle,WA, 2018, pp.4536-4538.

[13] D. Bates and A. Gawande, "Improving Safety with Information Technology," New England Journal of Medicine, vol. 348, 2003, pp. 2526-2534.

[14] R.S. Magnusson, "The Changing Legal and Conceptual Shape of Health Care Privacy," Journal of Law, Medicine & Ethics, vol.32, 2004, pp.685-689.

[15] E. Omran, T Grandison, D.Nelson, A.Bokma, "A Comparative Analysis of Chain-Based Access Control and Role-Based Access Control in the Healthcare Domain," International Journal of Information Security and Privacy, 2015, pp. 36-43.

[16] M. Mammadova "Information security of personal medical data in electronic environment," Problems of information technology, no.2, 2015, pp.15–25.

[17] D. Fifield, C. Lan, R. Hynes, P. Wegmann, V. Paxson, "Blocking-resistant communication through domain fronting," Proceedings on Privacy Enhancing Technologies, no.2, 2015, pp.1–19.

[18] Yue Shi, "Data Security and Privacy Protection in Public Cloud," IEEE International Conference on Big Data, Seattle,WA, 2018, pp.4805-4808.

[19] I. Y. Kuchin, "Protection of confidentiality of personal data using de-identification," Journal of Astrakhan State Technical University, 2010, no. 2, pp. 158-162.

[20] G. Muradova, "Security of personal medical data for the Redis concept," Problems of Information Technologies, no.2, 2018, pp. 71–80.

[21] Soon Ae Chun , V. Atlur, "Risk-Based Access Control for Personal Data Services Statistical Science and Interdisciplinary Research: Architectures and Information Systems Security," vol.3, 2008, pp. 263-280.

[22] L.Sweeney, "K-anonymity: A model for protecting privacy," International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, vol.10, no.5, 2002, pp.557–560.

[23] V.I. Vasiliev, N.V Belkov, "Decision making support system for personal data security," Ufa State Aviation Technical Univesity Journal, vol.15, no.5 (45), 2001, pp.54–57.

[24] C. Diaz, S.J. Murdoch, C. Troncoso, "Impact of Network Topology on Anonymity and Overhead in Low-latency Anonymity Networks," Proceedings of the 10th International Conference on Privacy Enhancing Technologies, 2010, pp.184—201.

[25] P. Winter, R. Köwer, M. Mulazzani, M. Huber, S. Schrittwieser, S. Lindskog, E. Weippl, "Spoiled onions: Exposing malicious Tor exit relays," PETS. Springer, 2014, pp.304-331.

[26] B. Greschbach, T. Pulls, L.M. Roberts, P. Winter, N. Feamster, "The Effect of DNS on Tor's Anonymity," Network and Distributed System Security Symposium, 2017. [Online]. Available: https://nymity.ch/tor-dns/tor-dns.pdf

[27] A. Fogelson, "Protecting data on file servers.Intrusion detection systems based on sensory traps," Business & Information technologies, 2011, no. 102, pp.45-47 (rus.)

[28] C. Wright, S. Coull, F. Monrose, "Traffic morphing: An efficient defense against statistical traffic analysis," In Proceedings of the 16th Network and Distributed Security Symposium. IEEE,2009. [Online]. Available: https//www.internetsociety.org/sites/default/files/wright.pdf

[29] C. Ross, "Empire Domain Fronting" [Online].09.01.2017 Available: https://www.xorrior.com/Empire-Domain-Fronting/

[30] A. Fortuna, "Domain Fronting in a nutshell" [Online]. 07.05.2018 Available: https://www.andreafortuna.org/2018/05/07/domain-fronting-in-a-nutshel