iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** II **Month of publication:** February 2022

DOI: https://doi.org/10.22214/ijraset.2022.40497

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue II Feb 2022- Available at www.ijraset.com

Shielded Identity Based Data and Contour Sharing for Mobile Healthcare Through Cloud Computing

Narotam Kumar[1], Prof. Dr. Bhuvana J[2]
[1]*MCA 3rd Year Jain University*
[2]*Jain University*

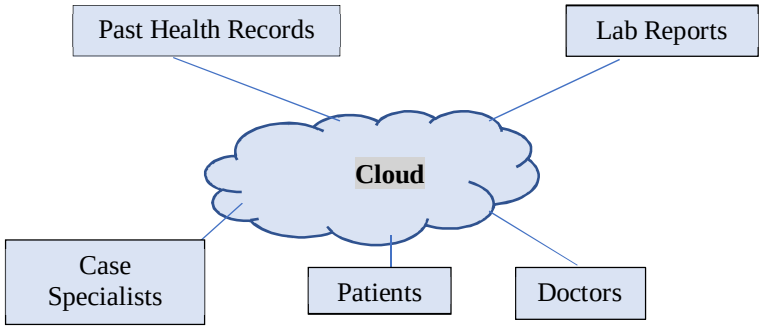
Abstract: ***Cloud computing and social networks are changing the way healthcare provides by providing real-time data sharing in a cost-effective way. However, the issue of data security is one of the key barriers to the widespread use of social networking services (MHSN), as health information is considered extremely sensitive. In this paper, we introduce a secure data sharing and MHSN profile matching scheme on a cloud computer. Patients can extract their encrypted health records from cloud storage via identity-based broadcast encryption (IBBE), and share them with a team of physicians in a safe and effective manner. Then we introduce a conditional data-based encryption component, which allows physicians who satisfy the pre-defined conditions in ciphertext to authorize cloud platform to convert ciphertext into a new ciphertext-based encryption system. without disclosing any sensitive information. The paper will also provide insight into data security policies that may authorize certain administrators to have read-only capabilities for all device parameters and read / write specific set of commands. Each administrator may have a different access profile introduction.***

I. INTRODUCTION

Cloud computing is the latest technology that plays important roles in public and private organization. The main concern of the health care provider is to reduce errors during treatment of patients. Quick access to Cloud allows a member to view patient information and without having to spend time processing its information as in Fig 1. to a third party without the patient's content. Health care systems are primarily divided into two categories of personal and community services and teaching and research activities. Personal health care such as hospital services, patient housing and various departments. Public health care services include medication, diet and safety measures to maintain a friendly environment. Similarly, treatment of infectious diseases is done through educational and research institutions. MOBILE health care is an innovative combination of mobile devices and communication technologies, as it can provide much-needed health information, improvements in general care, potential prevention of infectious diseases, health interventions, etc. It is becoming increasingly cold to use emerging computer technologies. in the portable health sector. Using a portable health care system, an electronic health record (EHR) can be transmitted over the network to a cloud service provider (CSP) for remote storage. In addition, healthcare providers can read it from the end. However, it does not guarantee complete data security and privacy, as many organizations are not qualified enough to add all the layers of security to sensitive data. This paper is a study of data protection strategies used to protect and secure data from clouds around the world. Discusses potential threats to data in the cloud and its solutions adopted by various service providers for data protection. The rest of the paper is arranged as follows. Phase 2 is a review of the literature that provides insight into the work that is already being done in this area. Section 3 discusses the types of threats in the data in the cloud. Section 4 examines some of the data security methods used worldwide. The final section concludes with a summary of this study.

Patients have better knowledge of their health care; they are well educated about their illnesses and are increasingly accessing the latest technology that provides greater information about health care.

Patients want the best care at the lowest cost and are willing to investigate their own options. As a result, access to patient records is increasing and organizations are required to provide patient record information.



A. Fig .1. Health Care Architecture

It is difficult for patients to understand why they do not have access to their secure global health information such as how a banking system allows customers to withdraw money and access other services anywhere in the world. But health care providers need to be more efficient in terms of cost-effective procedures compared to others, so cloud computing would be a good platform for such a situation. A large number of connected systems, in order to cost and increase the use of automated resources to reduce costs and data usage. In this way hospitals can only provide information if it is needed by a single user without the knowledge of a third party.

B. Cloud Computing Features Especially Like

1) *Shared Services:* Clients can share resources simultaneously. According to the providers the required resources are distributed but the customer is not fully aware of the areas of demand for services.
2) *Extensive Network Access:* By using the cloud we can have wider network access using the internet from any devices, anywhere in the world.
3) *Extension:* Clients can get unlimited usage resources because the cloud is loud and flexible which is free to use. *On-demand self-service:* A customer can configure the cloud automatically without help of service technicians.

II. AUTHENTICATION

With the important policy of today's LANs, businesses cannot afford to have their data networks compromised by unauthorized users. To date, the primary protection device or network access implementation has been a firewall or router-based access control list. Providing a link between unreliable networks (such as the Internet) and internal, trusted networks is important but not limited to. Security experts today warn that while the external threats to the networks are real, the biggest threats usually come from within the company.

Internal user authentication has long been established as a key defense tool for file servers, network applications, and large frames. There are also verification requirements for router tables (RIP, OSPF, BGP4), change holes, router and change configuration files, and web servers, to name just a few.

Traditional authentication - the user ID and password sent in clear text - are often inadequate for most security policies. People often use simple passwords or write them down because of a potential perpetrator. Passwords can be stolen, sniffed, guessed, attacked using free dictionary tools or forcibly attacked, corrupted by unprotected password files, and obtained through social engineering. Some passwords do not expire. Some expire every 60 to 90 days without allowing the user to reuse the old password. Some are short, simple alphabet letters only. Some are a combination of alphabet letters, numbers, and special characters. Some password files are stored in clear text; some were crucified. Many are conveyed in plain text; others as a cipher text.

III. AUTHORIZATION

Authorization is the granting of rights related to an authorized user, device, or host. The standard authorization method is provided by standard operating systems such as UNIX. The main user is the omnipotent system owner or controller. That person has the authority to grant rights to other users. These rights can be "read," "write," "add," "lock," "use," and "save" - individually or in combination. Very unusual though similar to the rights given to network administrators - those in charge of network infrastructure. The network is made up of many different devices - from hosting machines to application, file, web, DNS, and communication servers; from remote access servers to hubs and edge-shift work group; and from WAN-focused routers to LAN- or ATM-based key switches and routers.

There is a growing need to grant rights to these programs according to their need.

To allow this, network devices must be able to support a given management framework. Rights that may be granted may be limited to devices, services, and repair parameters.

Device access protection is similar to a traditional access control list or security program rules. The security controller creates certain rules that limit access to network devices based on device features requesting access, for example, source and / or destination IP address or MAC source address. This traditional concept of access control retains all authorization on the device itself. The proposed administrative structure here includes device authentication and authorization rules for external directory server. Access is granted as long as the policy allows. For example, an IP source (host or network) is trying to access an IP (host or network) location. The network device detects that the existing policy for this application - has the same rule. It asks the bibliography to determine what to do with it. The correct policy is restored to the device and used properly. In addition to this ambiguous application, policy may also be associated with explicit information such as the time of day or month.

IV. POLICY MANAGEMENT

The capabilities of this provided administrative structure are enhanced when validation and authorization are integrated with a central directory or policy server. Ideally, when a administrator verifies a network, you are given the ability to access all pre-authorized devices, services, and configuration parameters. Each time the administrator tries to access a network device, that device will ask the policy server. The policy server will send the approval to the device that provides the requested service authorization.

Policy-based network management uses a directory, centralized repository of policies. This is done for a very good reason. Instead of setting up each device with specific permissions, devices interact with the central directory for this information. This makes management easier - instead of changing authentication and authentication information on multiple or larger devices, it is done in a central location.

Implementation-based management implementation, that term reference and policy servers, is provided by a number of vendors including Alcatel, Cisco, Lucent, and Nortel. They all share the same design. It is all based on the concept of a policy console, a policy server or repository, a policy decision area (PDP), and a policy consolidation point (PEP).

These policy management structures are a two-phase or three-phase design. The two-phase approach integrates PDP and PEP into the same network device. The three-phase approach consists of PDP and PEP working on different devices. The rules used to communicate policies will depend on new products. For example, with the new gear, a separate PDP communicates with PEP via the Common Open Policy Service (COPS) protocol. In an integrated PDP / PEP, policy is transferred to a policy repository through LDAP. In the old communications gear, policy communication may be SNMP or CLI.

A. System Model

Our proposed data-based secure sharing of data and MHSN profile model on cloud computing is shown in Fig. 1, which includes five organizations: central authority, CSP, patient, physician and specialist.

1) *The Central Authorities:* The central authority is trusted by launching the system and generating attribute keys and private keys for participating users.
2) *CSP (Cloud Service Provider):* CSP is responsible for archiving data and can be made a proxy as it is less trustworthy. In addition, CSP performs patient profile matching.
3) *Patient:* The patients register the system to obtain their secret keys with their identities. They encrypt the electronic health record using AES cryptography techniques and the encryption key *K* will be encrypted by an Identity-based broadcast encryption algorithm and outsource the ciphertexts and encryption key to CSP, hence only authorized doctors could decrypt them. Simultaneously, patients with the same symptom can generate trap doors and form social relationships according to their wills.
4) *Doctor:* Authorized physicians can encrypt patient ciphertext stored in CSP. The authorized doctors can decrypt the patients' ciphertext that stored in the CSP. When encountering a problem that needs to negotiate with a specialist, the doctor can generate a re-encryption request, thus the CSP converts the ciphertext into an IBE-encrypted data for specialist if the doctor satisfies the pre-defined conditions in the ciphertext.
5) *Specialist:* An expert may remove encrypted ciphertext encryption and help doctors find advice. The specialist could decrypt the re-encrypted ciphertext with the secret key and then assist doctors for advice

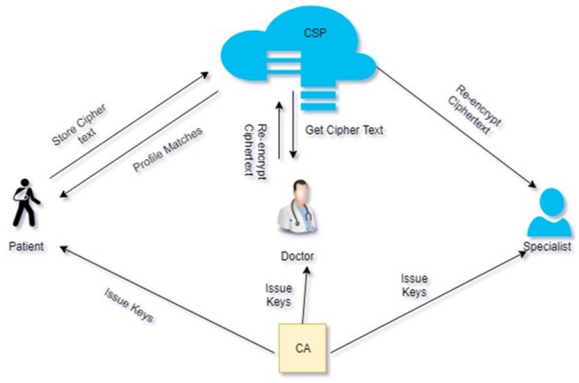


Fig. 1. System model

B. Flexible Authorization

In order to withstand the keywords guessing attack and strengthen the privacy protection, flexible authorization is considered in our scheme. We describe three types of authorization as follows:

1) User to user authorization. Nitin and Ravi generate trapdoors on their all ciphertexts respectively.

2) User to ciphertext authorization. Nitin generates a trapdoor on her all ciphertext, while Ravi generates a trapdoor on his specific ciphertext. Suppose that Ravi suffers from headache and stomachache, but he only wants to find a social friend who has a stomachache. Then he will generate a trapdoor on the stomachache and send it to the CSP.

3) Ciphertext to ciphertext authorization. Nitin and Ravi may have more than one symptom. They generate a trapdoor on one of their ciphertexts according to their inclinations. It also means that they may prefer to find some social friends with part of their symptoms.

REFERENCES

[1] C. Delerablée, “Identity-based broadcast encryption with constant size ciphertexts and private keys,” in Proc. 13th International Conference on the Theory and Application of Cryptology and Information Security, Kuching, Malaysia, 2007, pp. 200-215.

[2] J. Bethencourt, A. Sahai and B. Waters, “Ciphertext-policy attribute-based encryption,” in Proc. 2007 IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 2007, pp. 321-334.

[3] M. Green, G. Ateniese, “Identity-based proxy re-encryption,” in Proc. the 5th International Conference on Applied Cryptography and Network Security, Zhuhai, China, 2007, pp. 288-306. M. Li, S. Yu, Y. Zheng, K. Ren and W. Lou, “Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption,” IEEE Trans on Parallel and Distrib. Syst., vol. 24, no. 1, pp. 131-143, Jan. 2013

[4] M. Wegmuller, J. P. von der Weid, P. Oberson, and N. Gisin, "High resolution fiber distributed measurements with coherent OFDR," in Proc. ECOC00, 2000, paper 11.3.4, p. 109

[5] J. Breckling, Ed., The Analysis of Directional Time Series: Applications to Wind Speed and Direction, ser. Lecture Notes in Statistics. Berlin, Germany: Springer, 1989, vol. 61

[6] Secure Identity-Based Data Sharing and Profile Matching for Mobile Healthcare Social Networks in Cloud Computing,Qinlong Huang, Member, IEEE, Wei Yue, Yue He, Yixian Yang, Jul. 2018

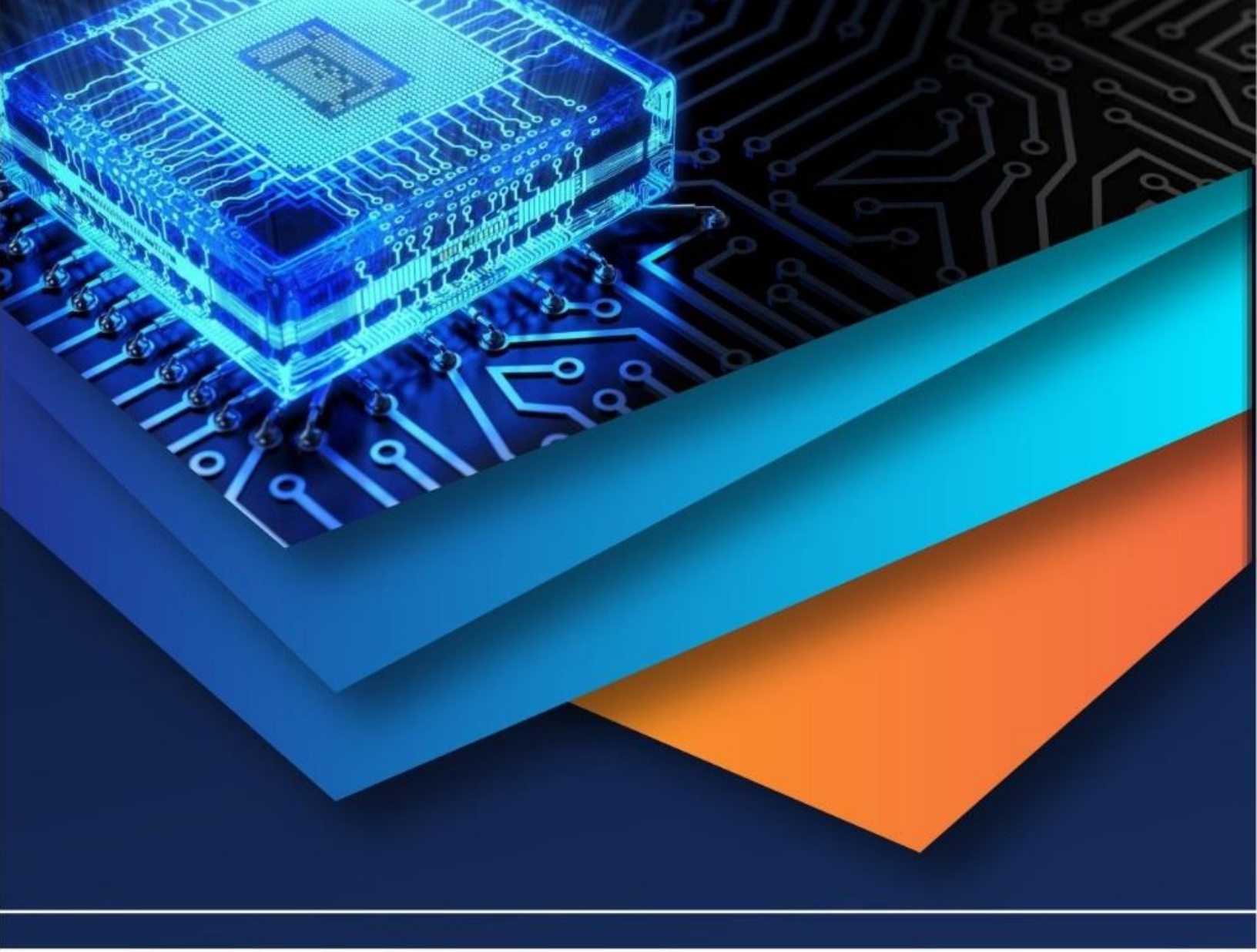
[7] A. Abbas and S. Khan, “A Review on the state-of-the-art privacy-preserving approaches in the e-Health clouds,” IEEE Journal of Biomedical and Health Informatics, vol. 18, no. 4, pp. 1431-1441, Jul. 2014.

[8] M. Li, S. Yu, Y. Zheng, K. Ren and W. Lou, “Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption,” IEEE Trans on Parallel and Distrib. Syst., vol. 24, no. 1, pp. 131-143, Jan. 2013

[9] M. Li, N. Cao, S. Yu and W. Lou, “FindU: Privacy-preserving personal profile matching in mobile social networks,” in Proc. 2011 IEEE International Conference on Computer Communications, Shanghai, China, 2011, pp. 2435-2443.

[10] R. Zhang, J. Zhang, Y Zhang, J. Sun and G. Yan, “Privacy-preserving profile matching for proximity-based mobile social networking,” IEEE J. Sel. Areas Comm., vol. 31, no. 9, pp. 656-668, Sept. 2013.

[11] L. Wu, Y. Zhang, K. Choo and D. He, “Efficient and secure identity-based encryption scheme with equal



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY