Attribute-based pseudonymity for privacy-preserving authentication in cloud services

ABSTRACT

Attribute-based authentication is considered a cornerstone component to achieve scalable fine-grained access control in the fast growing market of cloud-based services. Unfortunately, it also poses a privacy concern. Users attributes should not be linked to the users identity and spread across different organizations. To tackle this issue, several solutions have been proposed such as Privacy Attribute-Based Credentials (Privacy-ABCs), which support pseudonym-based authentication with embedded attributes. Privacy-ABCs allow users to establish anonymous accounts with service providers while hiding the identity of the user under a pseudonym. However, Privacy-ABCs require the selective disclosure of the attribute values towards service providers. Other schemes such as Attribute Base Signatures (ABS) and mesh signatures do not require the disclosure of attributes; unfortunately, these schemes do not cater for pseudonym generation in their construction, and hence cannot be used to establish anonymous accounts. In this paper, we propose a pseudonym-based signature scheme that enables unlinkable pseudonym self-generation with embedded attributes, similarly to Privacy-ABCs, and integrates a secret sharing scheme in a similar fashion to ABS and mesh signature schemes for attribute verification. Our proposed scheme also provides verifiable collusion, enabling users to share attributes according to the service providers policies.

CHAPTER 2

2. SYSTEM ANALYSIS

2.1 EXISTING SYSTEM

- Anonymous authentication provides zeroknowledge proof of identity, allowing data to be securely decoupled from provenance for enhanced privacy.
- Prior work has also explored decoupling document content from format and structure for more secure cloud storage and processing.
- In contrast, information-centric approaches imbue data with self-protecting properties, such as by representing it in a form amenable to direct computation on cyphertexts without decryption.
- AnonymousCloud's approach of decoupling private data from its provenance information can be viewed as an instance of the last of these approaches.

2.1.1 DRAWBACKS OF EXISTING SYSTEM :

- Attribute-based cryptography is suitable for addressing fine-grained access problem for cloud computing.
- In recent research works on authentication for cloud environment, many studies focus on addressing the problem of users' privacy disclosure.

- By using attribute-based signature, their authentication approach could address anonymity and user revocation problems.
- To address the above mentioned problems, this paper introduce an efficient privacy-preserving authentication scheme for cloud computing.
- In addition to users' privacy protection, fine-grained authorized access is another challenging issues for cloud computing.

2.2. PROPOSED SYSTEM

- In this paper we proposed an approach to improving data privacy in the cloud by decoupling private data content from metadata concerning its provenance and semantics.
- Our system, Anonymous Cloud, employs Tor onion routing inside cloud providers for customers to anonymously communicate computations and data to the system.
- Anonymous authentication based on publickey cryptography safely links jobs and data to customers for billing purposes without revealing these associations to untrusted computation nodes.
- To maintain a pay-per-use business model, clouds must inevitably track ownership information at some level for billing and auditing purposes.

2.2.1. ADVANTAGES OF PROPOSED SYSTEM

- We conduct theoretical security analysis, and carry out experiments to prove that the proposed scheme has good performance in terms of computational, communication and storage overheads.
- We also carry out comprehensive performance evaluation and further perform simulation experiments on both Intel and smart phone platforms.
- To address the challenge, this paper proposes an efficient attribute-based authentication scheme.
- In this paper, we consider achieving authorized access and attribute privacy preserving with high efficiency simultaneously.
- In this paper, we provided an efficient privacy preserving attribute-based authentication scheme for secure cloud computing.

Literature Survey:

TITLE	AUTHORS	DESCRIPTION
Cloud computing security: The scientific challenge, and a survey of solutions	Ryan M D,	The fact that data are shared with the cloud service provider is identified as the core scientific problem that separates cloud computing security from other topics in computing security.

Dynamic Data Operations with Deduplication in Privacy-Preserving Public Auditing for Secure Cloud Storage	Wu, Yulin, et al.	Cloud storage service has been increasing in popularity as cloud computing plays an important role in the IT domain.
A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data	Xia Z, Wang X, Sun X, et al.,	In this paper, we present a secure multi-keyword ranked search scheme over encrypted cloud data, which simultaneously supports dynamic update operations like deletion and insertion of documents.
Addressing cloud computing security issues	Zissis, Dimitrios, and D. Lekkas,	The recent emergence of cloud computing has drastically altered everyone's perception of infrastructure architectures, software delivery and development models.

2.3 FEASIBILITY STUDY

The feasibility Analysis is an analytical program through project manager determines the project success ratio and through feasibility study project manager able to see either project. The key considerations involved in the feasibility analysis are:

- Economic Feasibility
- Technical Feasibility
- Operational Feasibility
- Environmental Feasibility

2.3.1 ECONOMICAL FEASIBILITY

Hence this project is economically feasible there is no need to involve any cost for this project.

2.3.2 TECHNICAL FEASIBILITY

Software Technologies used are PHP and MySql. In the educational institutions, it is possible to update the system in future. No special hardware is required for the purpose of using this system. Hence it is declared that this project is technically feasible.

2.3.3 OPERATIONAL FEASIBILITY

As the admin work mainly to maintain the Patient and Doctor .Doctor will predict patient cancer disease. Hence it is easy to operate with training. Therefore it is operationally feasible for implementation.

2.3.4 ENVIRONMENTAL FEASIBILITY

This project environment is correct as a admin has developed this system and no expenditure is involved under any head and this process is part of admin document management, this project environment is accessible.

2.4 SYSTEM REQUIREMENTS

- System : Pentium IV 2.4 GHz.
- Hard Disk : 40 GB.
- Monitor : 15 inch VGA Color.
- Mouse : Logitech Mouse.
- Ram : 512 MB
- Keyboard : Standard Keyboard

2.4.1 HARDWARE REQUIREMENTS

The Hardware of the computer consists of physical component such as Input Devices, Storage Devices, Processing & Control units and Output Devices. Computer includes external storage unit to store data in programs.

The Hardware Configuration involved in this project

- System : Pentium IV 2.4 GHz.
- Hard Disk : 40 GB.
- Monitor : 15 inch VGA Color.
- Mouse : Logitech Mouse.
- Ram : 512 MB
- Keyboard : Standard Keyboard

2.4.2 SOFTWARE REQUIREMENTS

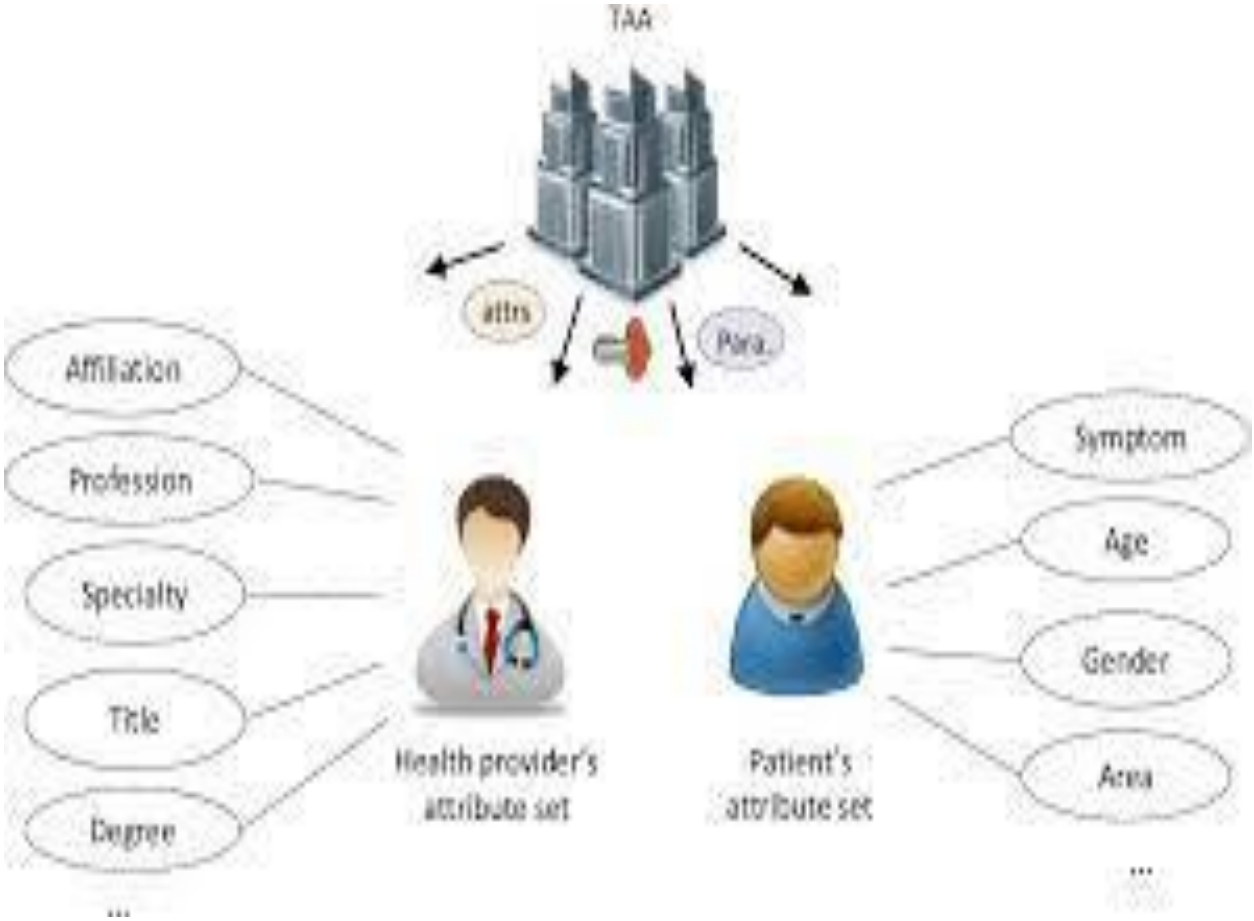
Software is a group of programs that computers need to do a particular task. It is an essential requirement of Computer System. The Software used to develop the project is

- Operating System : Windows XP.
- Platform : DOT NET TECHNOLOGY
- Front End : ASP.Net 3.5
- Back End : SQL SERVER 2005

CHAPTER 3

SYSTEM DESIGN AND DEVELOPEMENT

SYSTEM ARCHICTURE



CHAPTER 4

TESTING AND IMPLEMENTATION

4.1 TESTING

Implementation is the stage of the project when the theoretical design is turned into a working system. This is the final and important phase in the system life cycle It is actually the process of converting the new system into a operational one.

4.1.1 Unit Testing

Unit testing comprises the set of tests performed by an individual programmer prior to integration of the unit into a larger system. The module interface is tested to ensure that information properly flows into and out of the program unit. The local data structure is examined to ensure that data stored temporarily maintains its integrity during all steps in an algorithm's execution. Boundary conditions are tested to ensure that the module operates properly at boundaries established to limit or restrict processing. All independent paths through the control structure are tested. All error-handling paths are tested.

4.1.2 Block Box Testing

Black-box testing is a method of software testing that examines the functionality of an application without peering into its internal structures or workings. This method of test can be applied virtually to every level of software testing: unit, integration, system and acceptance. It is sometimes referred to as specification-based testing.

4.2 SYSTEM IMPLEMENTATION

Implementation is the stage of the project when the theoretical design is turned into a working system. This is the final and important phase in the system life cycle It is actually the process of converting the new system into a operational one.

CHAPTER 5

CONCLUSION:

In this paper, we provided an efficient privacy preserving attribute-based authentication scheme for secure cloud computing. The proposed scheme achieved two objectives, i.e. privacy preservation and fine-grained access to patients' personal health records. Through detailed security analysis, the proposed solution was shown to be secure and resisted various attacks including forgery attack, replay attack, and collusion attack, etc. The experimental simulation was further conducted to prove that our scheme was efficient in computational and communication overheads.

CHAPTER-6

REFERENCE

- [1] Ryan M D, " Cloud computing security: The scientific challenge, and a survey of solutions, Journal of Systems & Software, 2013, 86(9):22632268.
- [2] Wu, Yulin, et al. " Dynamic Data Operations with Deduplication in Privacy-Preserving Public Auditing for Secure Cloud Storage," IEEE International Conference on Computational Science and Engineering IEEE, 2017:562-567.
- [3] Xia Z, Wang X, Sun X, et al., "A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data, IEEE Transactions on Parallel and Distributed Systems, 2016, 27(2): 340-352.
- [4] Zissis, Dimitrios, and D. Lekkas, "Addressing cloud computing security issues," Future Generation Computer Systems, 28.3(2012):583-592.
- [5] Lu, R., Lin, X. and Shen, X., "SPOC: A secure and privacy-preserving opportunistic computing framework for mobile-healthcare emregency," Parallel and Distributed Systems, IEEE Transactions on, Vol. 24, pp. 614-624, 2013.
- [6] Pise P D, Uke N J, "Efficient security framework for sensitive data sharing and privacy preserving on big-data and cloud platforms, International Conference on Internet of Things and Cloud Computing. ACM, 2016:38.

- [7] Farash MS, Attari MA, “An efficient client-client password-based authentication scheme with provable security,” Journal of Supercomputing, 2014, 70(2):10021022.
- [8] Chen TY, Lee CC, HwangMS, Jan JK, “Towards secure and efficient user authentication scheme using smart card for multi-server environments,” Journal of Supercomputing, 2013, 66(2):10081032.
- [9] Wang D, Wang N, Wang P, et al., “Preserving privacy for free: Efficient and provably secure two-factor authentication scheme with user anonymity”, Information Sciences, 2015, 321:162-178.
- [10] Jiang Q, Khan M K, Lu X, et al., “A privacy preserving three-factor authentication protocol for e-Health clouds,” Journal of Supercomputing, 2016, 72(10):3826-3849.