Agent based Enterprise Security and Authentication System

Yin Nyein Aye , Nang Kay Thi Hlaing
Computer University, Hinthada
yinnyeinaye.ptn@gmail.com, nangkthi.23@gmail.com

Abstract

Organizations in both public and private sectors have become increasingly dependent on electronic data processing. It is essential to protect the communication channels and the interfaces of any system that handles information that could be the subject of attacks e.g. personal mail, electronic commerce and other financial transactions. Protecting the important data is of utmost concern to the organizations and cryptography is one of the primary ways to do the job. Public Key Cryptography is used to protect digital data going through an insecure channel from one place to another. This paper will implement a secured architecture for the various medical records by using RSA public key encryption algorithm and different authentication levels with the help of Agent Technology. RSA algorithm, asymmetric public key algorithm, is used to encrypt and decrypt the data. Agent Technology is used to retrieve required data efficiently and effectively. Since, medical records are confidential; it needs to be secured over the communication channel. So that security agent encrypts the requested data before sending to the target user. Personal agent is responsible for requesting data, carrying user preferences and user authentication to the remote server and bringing data back to the user. Data agents are used for generating the relevant data to the user (Personal) agent through security agent.

1. Introduction

A trusted framework must be established to preserve the privacy of patient information. The future of the healthcare industry lies in the ability of organizations to share critical information throughout the enterprise, across the continuum and among consumers and patients. While access to critical information must be increased, patient privacy must be preserved. Before this can be realized, reliable and secure infrastructures must be established and adopted so healthcare organizations can share confidential medical information over the Internet.

An agent is a software entity that applies Artificial Intelligence techniques to choose the best set of actions to perform in order to reach a goal specified by the user. It should react in a flexible, proactive, dynamic, autonomous and intelligent way to the changes produced in its environment. A multi-agent system may be defined as a collection of autonomous agents that communicate between themselves to coordinate their activities in order to be able to solve collectively a problem that could not be tackled by any agent individually.

This paper includes the following sections. Section 2 has discussed the previous work and how this scheme is proposed. In section 3, agent based architecture is presented. Public key encryption is in section 4 and Section 5 has the design of proposed system. Experimental results are in section 6 and section 7 is the conclusion.

2. Related Work

Security for information resources has three components: confidentiality (protection against disclosure to unauthorized individuals); integrity (protection against alternation or corruption) and availability (protection against interference with the means to access the resources) [14]. In this system, clients send requests to access data managed by servers, which involves sending information in messages over a network. A doctor might request access to his patient's data to other (remote) hospital or make changes to that data. The challenge is to send sensitive information over a network in a secure manner. But security is not just a matter of concealing the contents of messages – it also involves knowing for sure the identity of the user or other agent on whose behalf a message was sent. The second challenge is to identify a remote user or other agent correctly. Both of these challenges can be met by the use of encryption techniques developed for this purpose. Secure channels use cryptographic techniques to ensure the integrity and privacy of messages and to authenticate pairs of communicating principals [3].

Electronic information retrieval is becoming a necessity for most businesses, including medical practice [14]. Agent technology promises to provide a facile means for intelligently searching the Internet. However, any agent or other electronic information

placed onto the Internet poses a security risk. Encryption and firewalls are traditional methods for increasing Internet information security, but are these techniques sufficient to protect adequately electronic information carried by Internet agents? [5] Need to know and partial information strategies are discussed as methods for improving information security for Internet agents.

The current state-of-the art solution is to establish, in an access level manner, a system to issue public key certificates, in which the principal's public key (as well as some other information) is included and signed by an authority, and the authority may hold a certificate issued by a super authority, and so on up the hierarchy. This system is the so called public key certificate management infrastructure, or PKI (Public Key Infrastructure) [3].

With the increasing use of agents for different applications, increasing agent decentralization and need for agent communication and interoperation, such flexibility is essential [4]. This has been recognized in recent security literature. This flexibility in PKI implementation requires that multiple types of certificates, definition of name space, and management protocols tailored for various applications must be developed [8].

This system will present a practical agent-base scenario for mobile communication which can be made secure by using existing techniques. These techniques are used in such a way that the entire scheme becomes efficient and feasible to be deployed. Moreover, taking into account the advantages of mobile agents (able to travel autonomously from host to host to perform one or more tasks on behalf of a certain user) with the use of public key cryptology, leads to retrieve required data over a communication channel securely and efficiently.

3. Agent-based Security Architecture

"Agent based computing has already transformed processes such as automated financial markets trading, logistics, and industrial robotics" [1]. Now it is moving into the mainstream commercial sector as more complex systems with many different components are used by a wider range of businesses. Agents are capable of operating in dynamic and open environments and often interact with other agents - including both people and software [4]. Agents are a way to manage interactions between different kinds of computational entities and to get the right kind of behavior out of large-scale distributed systems.

The agent-based security architecture enables both static and runtime application-aware reconfiguration [10]. Adaptation allows the security provisions of the network to meet specific individual security requirements within different application scenarios. This agent security research includes agent schemes to solve node-related security problems and mechanisms for the secure transfer of agents between nodes. It exploits the unique flexibility and expressiveness of the agent-based paradigm to provide security solutions for wide-area dynamic distributed applications.

Existing PKI implementations began with specifying their certificate formats and the name spaces through a pre-defined access level [7]. In this system, instead of specifying the format certificates, it uses agent concepts and technology to authorities of authentication service and developing a security agent.

In this paper, we implement the different kinds of agent over the network to get the data. These agents are data agent, personal (user) agent, security agent and interface agent respectively.

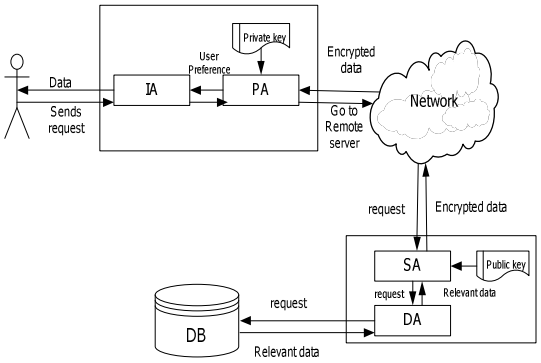

Figure 1. Agent based Security Architecture

3.1 Personal Agent

Personal agent provides a graphical interface to the user that facilitates the access to the services offered by the system. It is the only agent that can execute outside the main container of the platform and make remote requests through user interfaces. The user has a personal and confidential information area that keeps his/her personal data and health record. Different kinds of access levels have different personal agents. It goes to remote hospital in order to fulfill the user requirements carrying user request and authentication information and bring the required data back to the user.

3.2 Security Agent

This agent provides a flexible framework where different applications can specify their own certificate formats. From a user point of view, the security agent can be thought as a kind of configurable facilitator that can be employed by any group of users, organization, community, etc. to construct their own authentication verification service system. A security agent could potentially provide additional capabilities, such as retrieve, transfer, or exchange credentials among different

hierarchy systems, or introduce one agent to another, or delegate one agent to act on another's behalf, etc.

3.3 Data Agent

It sits at the host data site and has the responsibility to get data from the database on user request and got the request redirected by security agent. Relevant query is generated based on the user request. Then data is retrieved according to that query and returns the results to the Security agent for Data Encryption.

3.4 Interface Agent

Generate appropriate interfaces based on user level. Different kinds of access levels in our system can be seen in **Figure 2.**

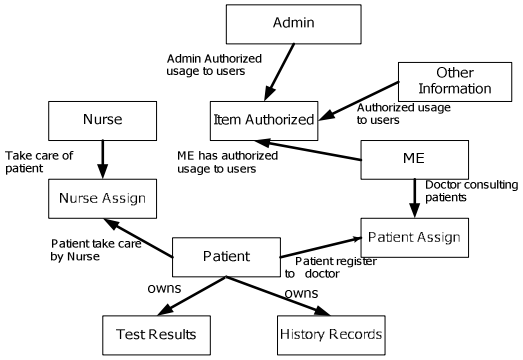

Figure 2. User Access Level Diagram

In this system, there are three kinds of user levels - Admin, Patient Care and Patient. A user may be assigned with the combination of above levels, for example, Admin with Patient care. Admin level has authority to view and manage employee (Physicians, Nurses and Staffs) of the hospital. Patient Care level has access to Patient's information and for the Patient Level, he / she can only view his medical records.

4. Public Key Encryption

Public key algorithms are based on mathematical functions rather than on substitution and permutation. Public key cryptography is asymmetric, involving the use of two separate keys, in contract to symmetric encryption, which uses only one key. The use of two keys has profound consequences in the areas of confidentiality, key distribution and authentication. They rely on one key for encryption and a different key related for decryption. The concept of public key cryptography evolved from an attempt to attack two of the most difficult problems associated with symmetric encryption. The first problem is the key distribution under symmetric encryption requires (1) two communications share a key or (2) the use of a key distribution center and the second problem is digital signatures.

4.1 RSA Algorithm

RSA (Rivest, Shamir, Adelman) is an asymmetric algorithm and plays a key role in public key cryptography. It is widely used in electronic commerce protocols. It is extensively used in the popular implementations of Public Key Infrastructures .One advantage of using RSA is that it can be used for encryption and digital signatures. Using its one-way function, RSA provides encryption and signature verification and the inverse direction performs decryption and signature generation.

Following steps should be taken to generate a public key and a private key:

1. Choose two large prime numbers. In mathematics, a prime number or prime for short is a natural number whose only distinct positive divisors are 1 and itself; otherwise it is called a composite number. Hence a prime number has exactly two divisors. The number 1 is neither prime nor coprime $p \neq q$ randomly and independently of each other. Compute $N = p\,q$.
2. Choose an integer $1 < e < N$ which is coprime to $(p-1)\,(q-1)$.
3. Compute d such that $d\,e \equiv 1 \pmod{(p-1)\,(q-1)}$.

4.2 RSA Key Generation

Each entity creates an RSA public key and a corresponding private key. Each entity A should do the following:

1. Generate two large random (and distinct) primes p and q, each roughly the same size.
2. Compute $n = pq$ and $Ø = (p - 1)\,(q - 1)$.
3. Select a random integer e, $1 < e < Ø$, such that $\gcd(e; Ø) = 1$.
4. Use the extended Euclidean algorithm to compute the unique integer d, $1 < d < Ø$, such that $ed \equiv 1 \pmod{Ø}$.
5. A's public key is (n; e); A's private key is d.

Definition The integers e and d in RSA key generation are called the encryption exponent and the decryption exponent, respectively, while n is called the modulus.

5. Proposed System

This system has developed security and authentication service for the medical information system. There are different types of users: Admins,

Medical experts, Nurses, Workers and patients. For the security service, there are various types of items like hospital information, researches, patient's information and test results, etc. Each item has its own security control, for example, test results of patient's A cannot be seen to every physicians, except his own, and the same way in other items. The security service has been implemented with public key encryption with RSA algorithm. The proposed system design is presented in Figure 3.

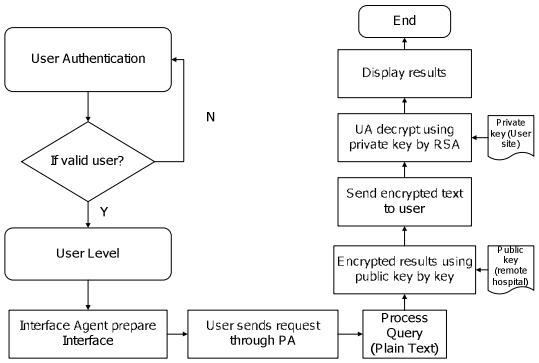

Figure 3. Proposed System design

Security agents control access level of the medical data, Personal agents request data and Interface agents provide a graphical interface to the user that facilitates the access to the services offered by the system. This system is the so called public key certificate management infrastructure, or PKI. **Figure 4** is an explanation of system architecture.

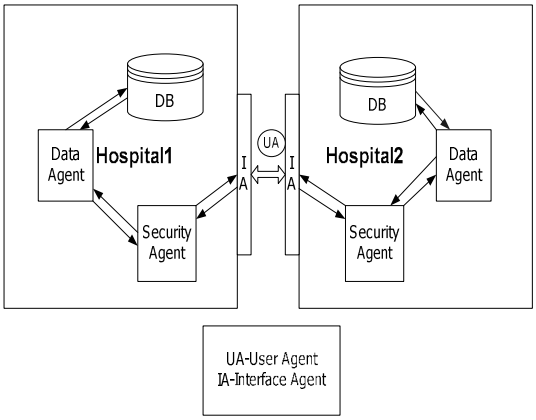

Figure 4. System Architecture

6. Experimental Results

This system is an implementation of Agent based security architecture. It uses multi-agent technology to efficiently and effectively get requested data. Asymmetric Algorithm, RSA is used to get the data in the secured manner. With the use of agent technology, there is less work will be performed by user and get the data in the secured way. Following **Figures 5, 6, 7** show how data is requested, encrypted and decrypted in the secured way.

In **Figure: 5**, a user makes remote request through user interface. If his access level is patient care and administration, this level can see employee information and patient information. So, personal agent goes to remote hospital in order to fulfill the user requirements by carrying user request and authentication information and brings the required data back to the user. Data agent sits the host site and responsible for getting data from the database based on user request. And then it got the request redirected by security agent.

In **Figure 6**: Security agent is responsible for encrypted data by using RSA algorithm with public key in remote site.

In **Figure 7**: Personal (User) agent decrypted data by using private key in user site. So, the user can see the confidential information of the remote hospital.

7. Conclusion

This paper discussed the implementation of authentication system for medical information system using RSA public key encryption. Records in the medical information system are encrypted when they are requested. Different kinds of users have different kinds of public keys based on their authorization level to get the access the electronic medical records. In this system, with the use of Agent Technology, helps the user in ease of getting what data he/she wants.

Figure 5: User request data with user level

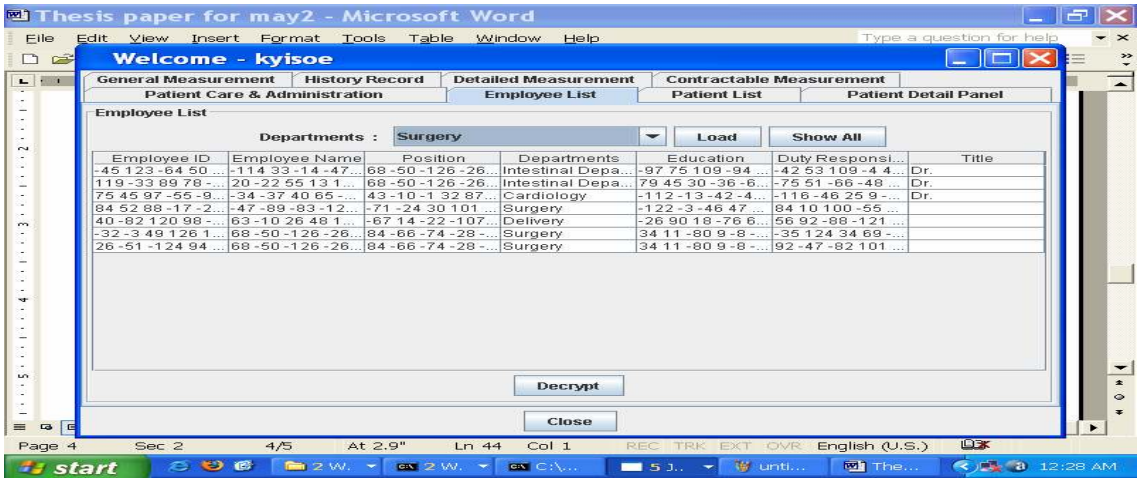

Figure 6: Encrypted data by using RSA

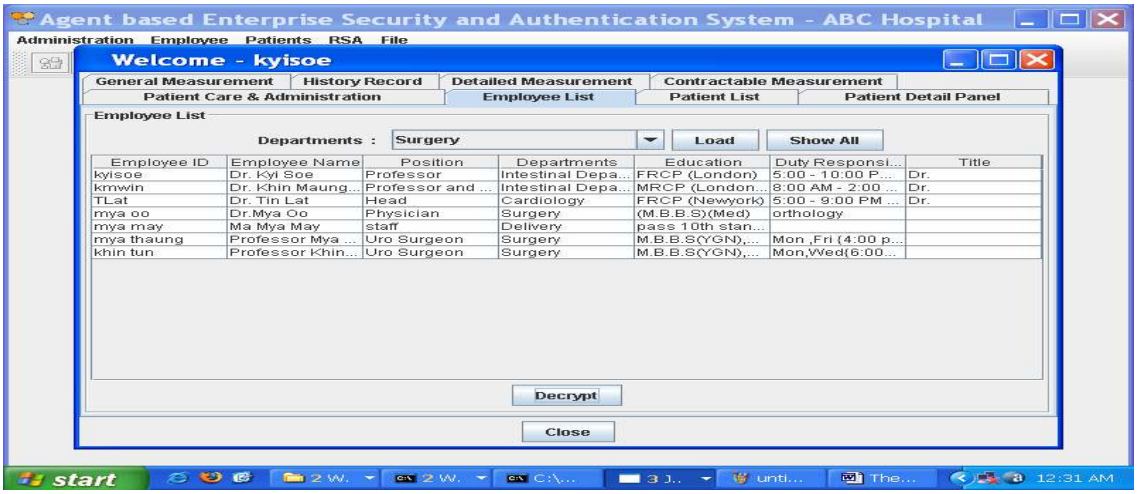

Figure 7: Show relevant data

8. References

[1] Antonio Moreno, *Medical Applications of Multi-Agent Systems*, 2003.

[2] Antonio MORENO(1), David SÁNCHEZ, David ISERN(2).
(1) Research Group on AI, Multi-Agent Systems Group (GruSMA).
(2)Dept. of Computer Science & Electrical Engineering University of Maryland Baltimore County Baltimore, MD 21250*:KQML-Based PKI* ,2006.

[3] G. Alan Khoheinm, *Computer Security and Cryptography*, 2007.

[4] Charlie Kaufman, Radia Perlman,Mike, Speciner, *Network Security*, 1997.

[5] D. Isern, D. Sanchez, A. Moreno, and A. Valls, HeCaSe: *An Agent-Based System to ProvidePersonalised Medical Services*, 2000.

[6] George Colouris, Jean Dollimorc, Tim Kindberg, *Distributed System Concepts and Design*, third edition ,2001.

[7] He,Qi(1); P.Sycara, Katia(1); W.Finin,Timothy (2)
(1)The Robotics Institute Carnegie Mellon University Pittsburgh.
(2)Dept. of Computer Science & Electrical Engineering University of Maryland Baltimore County Baltimore, *Personal Security Agent:KQML-Based PKI* ,2006.

[8] H. Mouratidis, P. Giogini, G. Manson, "Modeling Secure Multiagent Systems", *in the Proceedings of the 2nd International Joint Conference on Autonomous Agents and Multiagent Systems*, July 2003.

[9] James Riordan and Bruce Schneier, *Environmental Key Generation Towards Clueless Agents,* In Giovanni Vigna, editor, *Mobile Agents and Security*, Lecture Notes in Computer Science, LNCS 1419, Springer-Verlag, 1998, pp. 15–24.

[10] Kostaszotos, Andreas LitkeDept. of Applied Informatics, University of Macedonia 4006 Thessaloniki, GREECE, *Cryptography and Encryption*, 1997.

[11] Leonard N. Foner, *A Security Architecture for Multi-Agent Matchmaking*, *Proceeding of Second International Conference on Multi-Agent System*, Mario Tokoro, 1999.

[12] A. Moreno, D. Isern, D. Sánchez, *Provision of agent-based health care services, AI-Communications*, 2003.

[13] M. Wooldridge, *An introduction to Multi-Agent Systems*. John Wiley and Sons, 2002. ISBN 047149691X.

[14] J. Nealon, A. Moreno, *Agent-based health care systems*. In Applications of Software Agents Technology in the Health Care Domain, J. Nealon and A. Moreno Eds., Whitestein series in software agent technology, 2003.

[15] D. Russell, and G. T.Gangemi, *Computer Security Basics*, July 1991.

[16] M. Robshaw, *Security Estimates for 512 bit RSA*, June 1995.

[17] W. Staillings, *Cryptography and Network Security Principles and Practice* ,Third Edition. Upper Saddle River, NJ:Prentice Hall, 2003.

[18] U. Cortés, J. Fox, A. Moreno, Lyon, Klusch, M. *Proceedings of the Workshop on Agent Applications in Health Care*, at the 15th European Conference on Artificial Intelligence, ECAI 2002. *Information agent technology for the Internet: a survey. Data and KnowledgeEngineering* , Vol. 36 (3), (2001), pp. 337-372.

[19] V. ShankararamanBarcelona, *Proceedings of the Workshop on Agents in Health Care*, at the 4th International Conference on Autonomous Agents, AA 2000. Spain, (2000).

[20] W. Stallings, *Cryptography and Network Security: Principles and Practice*, Second Edition, Prentice-Hall 1999.

[21] www.rsasecurity.com