A Framework of High-Confidence e-Healthcare Information System[†]

SHUN-CHIEH LIN[1,*], SHIAN-SHYONG TSENG[1,2], WEN-GUEY TZENG[1], AND SHYAN-MING YUAN[1]
[1]*Department of Computer Science, National Chiao Tung University , Taiwan*
[2]*Department of Information Science and Applications, Asia University, Taiwan*

ABSTRACT

In this paper a framework for a high-confidence e-healthcare information system which meets five criteria including availability, reliability, security, survivability and restorability is proposed. The function of this framework is to prevent the destruction from malicious intentions by integrating the technologies of information hiding, encryption, monitoring, self-adaptation and fast inference. This framework contains proactive-VPN, efficient e-anamnesis transmission, e-anamnesis protection, and intelligent monitoring components. The proactive-VPN, combining with the efficient e-anamnesis transmission component to provide the secure network environment, is designed for handling large-sized e-anamnesis. The e-anamnesis protection component is designed to protect the e-anamnesis by ensuring confidentiality. The intelligent monitoring component is designed for monitoring all users' behaviors in the framework. Finally, some experiments have been done to demonstrate the performance of our framework.

Key words: high-confidence system, message transmission, security, information hiding, monitoring.

1. INTRODUCTION

In this paper a framework of high-confidence e-healthcare information system which meets the five criteria of security, availability, reliability, survivability and restorability, is proposed. This framework consists of a proactive-VPN (Proactive Virtual Private Network), an efficient e-anamnesis transmission, an e-anamnesis protection and an intelligent monitoring component. By integrating the advanced technologies of information hiding, encryption, monitoring, self-adaptation and fast inference the destruction by malicious intent will be prevented. The proactive-VPN component is used to actively ensure the secure network environment. The efficient e-anamnesis transmission component can transfer large-sized e-anamnesis image data and achieve high availability, reliability and survivability. The e-anamnesis protection component makes use of e-anamnesis sharing and content fidelity technologies to achieve security and reliability of the e-anamnesis image data. Finally, an intelligent monitoring component makes use of fast inference and data mining technologies to ensure the security of the system. Moreover, it can also provide the function of dynamic key updating of the proactive-VPN component to achieve restorability. Finally, some experiments have been done to demonstrate the performance of our framework.

[†] This work was supported partially by the NSC Project Advanced Technologies and Applications for Next Generation Information Networks (II) with Project No. NSC 95-2752-E-009-015-PAE.

[*] Corresponding author. E-mail: jielin@cis.nctu.edu.tw

The remainder of this paper is organized as follows. In Section 2, the related works and issues for constructing a high-confidence e-healthcare system are described. In Section 3, the proposed framework based upon the above issues is presented. In Section 4, some experimental results are shown. Finally, some conclusions are made in Section 5.

2. RELATED WORKS

As is well known, in most traditional hospitals, the anamnesis is handwritten by doctors and the medical images are produced by medical appliances. The cost of well-managed anamnesis is often expensive without using computers. Due to a dramatic increase in e-healthcare applications, the anamnesis of hospital patients is usually digitized and the cost can then be reduced. However, most hospital information systems (HIS) (Global Care Solutions Ltd, 2003; Ohe et al., 1995), are mainly concerned with the management of the e-anamnesis and the sharing of medical knowledge to improve patient care within or between hospitals. As for the security issue, some kinds of access control, e.g., account and password, to the HIS has usually been implemented. Due to the requirements to protect the privacy of patients, a security mechanism to protect e-anamnesis including the names, diagnoses, and social security numbers, should be implemented. Therefore, a high-confidence e-healthcare information system which consists of a high secure e-anamnesis protection component, an efficient e-anamnesis transmission component, a secure network component, and an intelligent monitoring component, is designed and implemented in this study, based upon the following five criteria.

Security: The ability of a mission critical information system to protect its environment and not be damaged; and to secure the information and services and prevent them from being stolen or cracked. In other words, this ability, which is especially important for a high-confidence e-healthcare information system, ensures the integrity and confidentiality of the protected system, defends against attacks, and avoids dangerous operations.

Availability: The ability to perform the major functions of a mission critical information system at any given time. In other words, no matter how busy this system is, the response time of the user's request should be short.

Reliability: The ability to perform the functions of a mission critical information system at some specific time, e.g. to produce a correct output at peak network traffic times.

Survivability: The ability to perform the functions of a mission critical information system when some network component has crashed or failed. In other words, this ability ensures that the essential functions degrade gracefully when the system is under attack.

Restorability: The ability of a mission critical information system to recover the essential functions after the system has failed to operate. In other words, this system must be able to backup the status before an attack and restore the system automatically after an attack.

3. FRAMEWORK OF HIGH-CONFIDENCE E-HEALTHCARE INFORMATION SYSTEM

In recent years, the e-healthcare system has become common in many countries in the world. Many policies in medical care such as health prevention, clinical care, hospitalization, resident care and social rehabilitation are promoted in many countries. For example, the British National Health Service uses information technology and information systems for the benefit of patients and clinical processes (Wright, 1992). Due to the digitalization of anamnesis, the privacy issue needs to be considered to prevent malicious attacks which may crash an entire service. Also, in the e-healthcare environment, in order to refer the e-anamnesis for some referral patients, the e-anamnesis transmission issue needs next to be considered. Finally, the issues of the transfer and storage of secured information needs to be considered in the high-confidence e-healthcare information system. In Figure 1 we propose a framework of high-confidence e-healthcare information system in a distributed network environment to solve these issues.

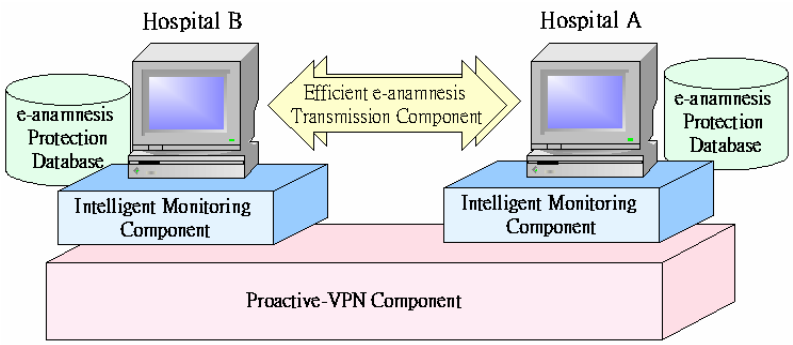

Figure 1. The framework of high-confidence e-healthcare information system.

Our proposed framework includes four components: a proactive-VPN component, an efficient e-anamnesis transmission component, e-anamnesis protection component, and an intelligent monitoring component. Since hospitals record patients' information on their medical server, protection for e-anamnesis and the whole system is urgently needed. In this distributed network environment, the proactive-VPN component combines with the efficient e-anamnesis transmission component to provide a secure network environment between hospitals. The proactive-VPN adds the proactive key server on traditional VPN gateways to provide more security and a reliable network environment. When transferring large-sized e-anamnesis image data from one hospital to another, the data can be transferred through the efficient e-anamnesis transmission component, which provides a unique interface and APIs for e-healthcare applications. In order to ensure the privacy of patients the e-anamnesis data stored in the appropriate

database can be protected by the e-anamnesis protection component, which achieves the security and reliability of the e-anamnesis. In each hospital client, each process and action can always be monitored by our intelligent monitoring component, which provides a fast response capability, to ensure the security of the high-confidence e-healthcare information system.

In following sections, the mechanisms used in the high-confidence e-healthcare information system will be introduced, and the benefits of using these mechanisms will be analyzed.

3.1 The Proactive-VPN Component

For Internet security, we provide a highly secure and reliable proactive-VPN that employs proactive cryptography to guard the long-term data of a traditional VPN system against mobile attackers.

3.1.1 Key sharing

Although proactive-VPN is an effective cryptographic tool to provide Internet security, the VPN's key is of most importance. If the key is stolen, the VPN becomes insecure. Therefore, we use the key sharing technology to improve the security of key protection instead of keeping it in only one place. However, we cannot assume that a security server is secure during its lifetime. On the other hand, we can assume that in a short period of time a set of coordinated attackers can break into at most *t*, a user-defined threshold, security servers and obtain the secret values in the servers.

3.1.2 Key updating periodically

Based on the above observation, proactive cryptography (Canetti & Herzberg, 1994; Herzberg, Jarecki, Krawczyk, & Yung, 1995; Ostrovsky & Yung, 1991) refreshes the secret values of servers periodically, say, once a day. The old secret values become useless in the new time period. Therefore, even though an attacker may have broken into all secure servers, the system is secure as long as they cannot break in t+1 security servers in the same time period. It provides a more secure environment than traditional VPN technology. A proactive-VPN system designs and implements a proactive mechanism for the key management module to provide "strong" protection for secret keys against frequent break-ins. We provide a library of proactive utilities that implement various proactive algorithms and protocols. Therefore, a high security and reliable network environment is provided by the high-confidence e-healthcare information system.

3.2 Efficient E-anamnesis Transmission Component

In our proposed e-healthcare framework, the efficient e-anamnesis transmission component provides high reliability and survivability. Since image data are the largest portion of the e-anamnesis, a complete message-oriented middleware (MOM) solution including a fast messaging system and an easy integration engine on the e-healthcare system is designed to transfer large-sized information.

3.2.1 Distributed architecture with multicasting

We proposed a distributed architecture with a multicasting technique in the efficient e-anamnesis transmission component to achieve reliability. This transmission component offers a publish/subscribe API java message service (JMS) and provides an efficient and reliable message delivery service, the so called fast java messaging system (FJM), for e-healthcare applications (Hsiao, Perng, Lo, Chang, & Yuan, 2003; Sun Microsystems, 1999). This component provides efficient, low bandwidth, multiple-to-multiple transmission. Moreover, it is built on the reliable IP multicast-based group communication protocol (Whetten, Montgomery, & Kaplan, 1995) in order to reduce message transmission overhead.

3.2.2 Unified interface

We developed a development and integration engine, called Ghostwriter, to help us integrate heterogeneous technologies in a quick and easy way (Hsiao et al., 2003). The Ghostwriter engine contains a runtime library-supported application to communicate over networks. Application programmers need only concern themselves with the data logic and how messages are sent and received in their programs. They do not have to know about event-based programming APIs or models. More detailed information of the Ghostwriter will be discussed in Section 4.

3.3 E-anamnesis Protection Component

Since the e-anamnesis usually contains large-sized image data, it is the most private information of patients in the high-confidence e-healthcare information system. Therefore, we propose a novel (k, n)-threshold scheme for sharing secret e-anamnesis image data, with multi-level security protection, in order to avoid the leaking out the e-anamnesis of patients and achieve the security and reliability of keeping e-anamnesis image data. An additional content authentication mechanism is also included to ensure the fidelity of the secret e-anamnesis.

3.3.1 E-anamnesis sharing

A well-known technique for secret sharing is the (k, n)-threshold method proposed by many researchers (Chang & Lee, 1993; Shamir, 1979; Stinson, 1992; Sun & Shieh, 1994), but these researches mostly concentrated on text data. Since medical images in hospitals are important and need to be kept private, we propose a novel approach suitable for large-sized medical image information, which is a new e-anamnesis image sharing approach with the capability of steganography effects. The proposed scheme as a whole thus provides a high secure mechanism for data sharing for any type of e-anamnesis images that is difficult to achieve by traditional secret sharing techniques. Also, it will be advantageous to check the fidelity of secret data after they are transmitted over networks.

3.3.2 Content fidelity

One way to ensure the fidelity of the secret e-anamnesis image data is to use fragile watermarks (Adelson, 1990; Wu & Tsai, 1998), which is a kind of signal designed to be embedded in an image and that can be easily destroyed if the

watermarked image is manipulated in the slightest manner. By inspecting the existence of the embedded signal in an inspected secret e-anamnesis image, the aim of authentication can be achieved. A technique of fragile image watermarking is adopted for e-anamnesis image authentication after secret transmission.

3.4 Intelligent Monitoring Component

In order to achieve the security of the proposed system, we design an intelligent monitoring component (Lin, Tseng, & Kuo, 2002b), which combines high efficiency for users' behavior monitoring and accuracy for knowledge expression of rule base systems (Lin, Tseng, & Tsai, 2003), to monitor each event occurring in the system. In this component, users' behaviors will be monitored in different layers, including the fundamental network layer and the customized application layer.

3.4.1 Misuse behaviors monitor

In the proposed system, a misuse behaviors monitor (MBM) is designed to be responsible for the real-time monitoring of abnormal behaviors in large amounts of users' activities. It is used for a signature based monitoring process, which is widely used for online behavior monitoring, to achieve system security. The monitoring of the general misuse behavior, which is defined in most signature based monitoring systems, is one main purpose of the MBM. Statistic network information is also generated for further analysis. All of these results can be represented using the IDML (Intrusion Detection Markup Language) which is an XML-based expression format (Lin, Tseng, & Lin, 2001).

3.4.2 Anomaly behaviors monitoring

Based on the above results, an anomaly behavior monitor (ABM) using rule base inference technology is proposed in the system to discover possible anomalistic behavior. Moreover, the ABM is also responsible for monitoring the abnormal events occurring in the components of the e-healthcare system, such as the proactive-VPN component, the e-anamnesis protection component, and the efficient e-anamnesis transmission component. For example, the ABM can trigger the process of key updating dynamically to achieve restorability of the e-healthcare system by monitoring dangerous events occurring in proactive-VPN gateways. The ABM also uses data mining technologies to discover possible users' behavior patterns, which can then be taken as feedback to an intelligent monitoring component for further monitoring and management (Lin, Tseng, Lin, & Chou, 2002a).

With the intelligent monitoring component, not only misuse behaviors can be monitored, but also anomaly and varied behaviors in applications in the system can be identified.

4. THE EXPERIMENTAL HIGH-CONFIDENCE E-HEALTHCARE INFORMATION SYSTEM

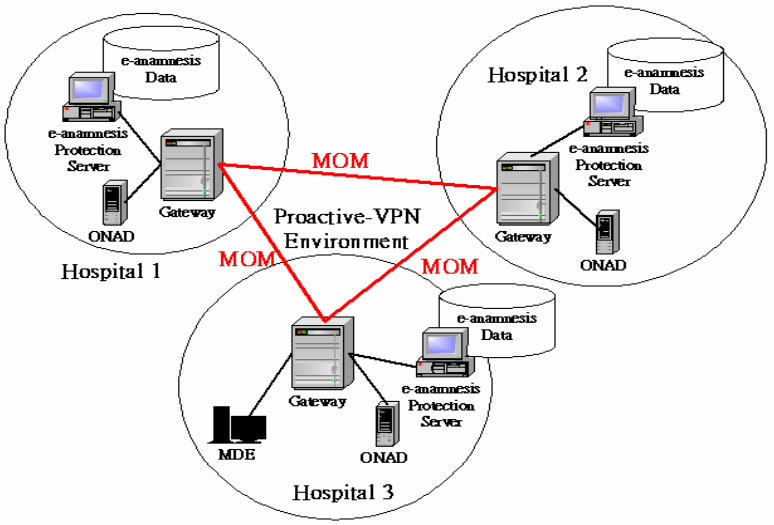

Figure 2. Illustration of the experimental high-confidence e-healthcare information system.

Since the Bureau of National Health Insurance (BNHI) in Taiwan was formed in 1995, many national policies in medical care such as health prevention, clinical care, hospitalization, resident care and social rehabilitation have been promoted. In 2002, the BNHI promoted the health insurance IC card and e-anamnesis for providing more convenient healthcare services and easier maintenance of the resources of medical care. However, many issues still need to be solved to provide a desirable e-healthcare information system.

In this section, a high-confidence e-healthcare information system, as shown in Figure 2, is a prototype of our four-year project of "high-confidence information systems" which was supported by the Ministry of Education Program, from January 2000 to March 2004, under the scheme for "promoting the academic excellence of universities." To simplify our discussion, only three different hospitals in this e-healthcare environment are included in Figure 2. Each hospital has one e-anamnesis protection server to be responsible for protecting e-anamnesis data stored in e-anamnesis database, a proactive-VPN gateway to construct the proactive-VPN network environment, and a misuse behaviors monitor (MBM) to monitor any abnormal behavior which occurs in the hospital. In some hospitals, there is an anomaly behavior monitor, a so-called Meta-Detection Engine (MDE), which is responsible for receiving the reported events from the MBM and other components in this e-healthcare system.

In the network environment the proactive-VPN gateway, which is the proactive-VPN component in the e-healthcare system, is used to transmit real raw data with encryption across the Internet. This can lead the e-healthcare information system to have an essential security network environment, which separates the private network from the public Internet and so avoid sniffing and modifying to ensure security and reliability.

In applications the e-anamnesis stored in the e-anamnesis database of one hospital is transmitted to another through the efficient e-anamnesis transmission component, which is here called Message-Oriented Middleware (MOM), when the referral patients need to refer to their anamnesis. The MOM is also used to communicate with the other components (applications) in the e-healthcare information system. In this environment, only the send () and receive () functions, which are provided by Ghostwriter in the MOM, need to be defined and implemented specifically in each application. Application programmers define an event Markup Language (Event ML) which is XML-based expression description file and implement the send() and receive() functions for each application and then the applications can communicate with each other by specific channels defined in event ML. In our prototype, each communication channel represents one kind of information type, such as the e-anamnesis of each patient and each different abnormal event. As mentioned in Section 3.3, a novel e-anamnesis sharing technology with content fidelity technology is also implemented for protecting and ensuring the fidelity of each e-anamnesis stored in e-anamnesis database.

In order to secure the e-healthcare information system, abnormal events occurring in the MBM and other components are also defined in the IDML format and reported to the MDE for analysis through each different kind of monitoring channel. For example, the malicious intentions, such as information gaining and abnormal connections, are defined to monitor these anomaly events. These events may occur in a proactive-VPN gateway, and the key to the proactive key server may be stolen. If such events reported through proactive-VPN monitoring channel are detected by the MDE, the key updating procedure in the proactive key server can be triggered dynamically through the same channel. In the e-anamnesis protection server, we also define abnormal events by an e-anamnesis verification failure monitoring channel when the e-anamnesis fails in the content fidelity process. The high-confidence e-healthcare information system is able to easily achieve the security, survivability, and restorability through the intelligent monitoring component cooperating with other components.

Some experiments have been done to evaluate the computation performance. When a picture (for example, a private anamnesis) needs to be stored at an e-anamnesis database, an operator can choose the picture and then the secret sharing process will be done automatically. These generated secret keys can be stored at VPN key sharing servers in a safe way. After doctors receive the images in an e-anamnesis database, the e-anamnesis protection component can determine whether the e-anamnesis is valid or not. Figure 3 shows one example of hiding and verifying an e-anamnesis, and the experimental results show that security, reliability and restorability of e-anamnesis can be achieved.

Since computation performance may be dominated by efficient e-anamnesis transmission components, only the experimental result of transmitting a large-sized e-anamnesis is shown as follows. Our test bed includes one AMD Athlon of 1GHz with 256MB SDRAM as the sender, and seven PentiumIII-600 hosts with 128MB SDRAM as the receivers. Figures 4 and 5 show the results of performance testing based on the average 1000 round trip time of variant data sizes where the average

round trip time is one-to-one (1-to-1) and one-to-seven (1-to-7) (sender-to-receivers). Our measurement of the JMS includes SonicMQ (2000.1 Release) (Sonic Software, 2000), iBus (version 4.1.2) (Softwired Inc., 2001), and open JMS (version 0.7.3) (Alateras, Anderson, & Mourikis , 2002).

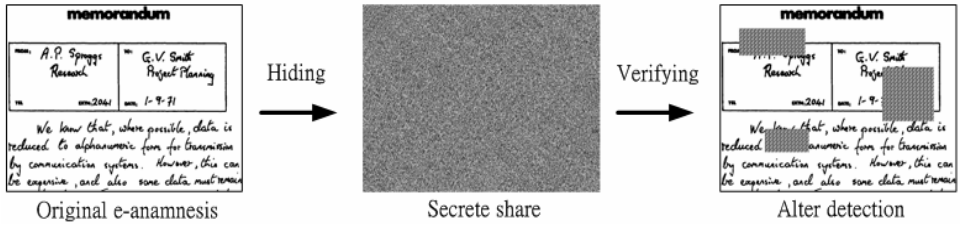

Figure 3. The process of E-anamnesis sharing and content fidelity.

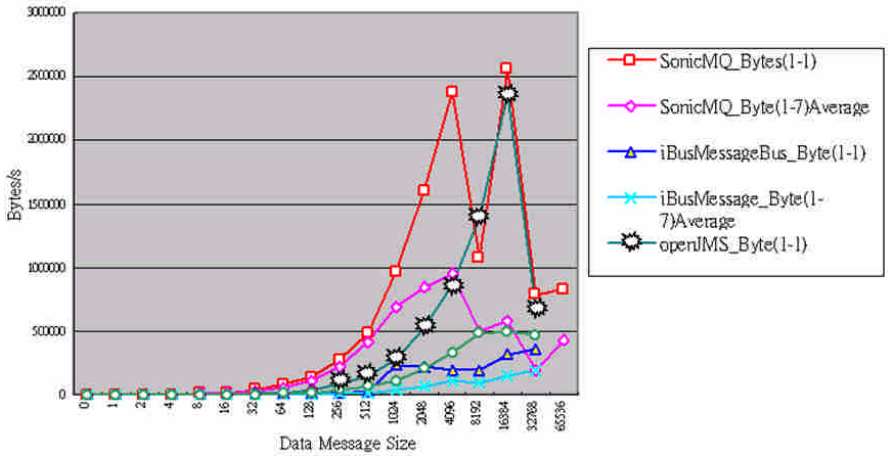

Figure 4. Throughput of other JMS products.

As shown in Figure 4, all of the other JMS's performances decrease dramatically when the data size is large than 32KBytes. Moreover, OpenJMS and iBus cannot finish 1000 times of measurement. Besides, all of the products' performances decrease rapidly in the 1-to-7 model. For example, SonicMQ's throughput is below half of the average throughput in 1-to-1 in comparison with the 1-to-7 model when the data size is 16KB~64KB. As shown in Figure 5, our FJM's performance increases steadily. Even when the data size is 64KB, the FJM has a better performance in comparison with the other products. Therefore, the computation performance of our proposed e-healthcare information system is more efficient than the other products in transmitting e-anamnesis.

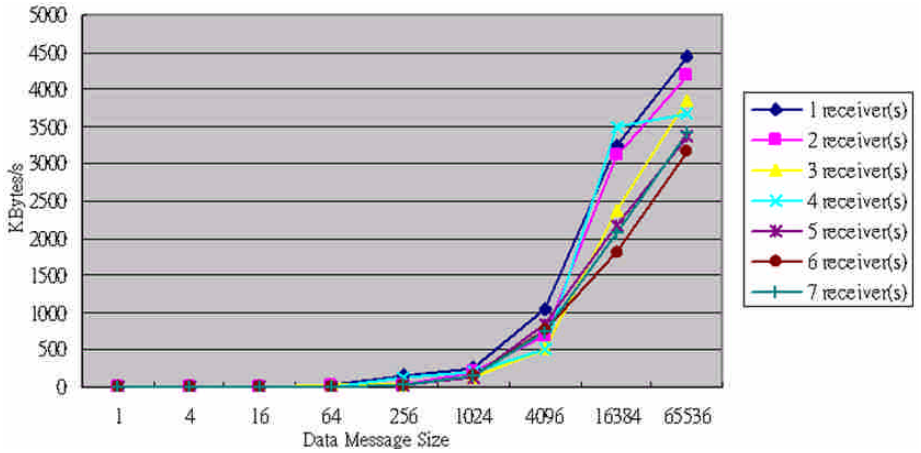

Figure 5. Throughput of fast java messaging system.

In our prototype system, an SNMP information collector was designed and implemented to pull information from the SNMP hardware or software according to the network address settings and the OID information and send the information with the IDML event format to an MDE server. With this SNMP collector, SNMP information can be used as the source of events for the MDE to detect, and enhance the detection ability of this prototype. The experimental result shown in Figure 6 illustrates the survivability of our high-confidence e-healthcare information system.

Figure 6. The network statistics information.

5. CONCLUSION

In this paper, a framework of high-confidence e-healthcare information system has been proposed to meet five criteria including security, availability, reliability, survivability, and restorability. An experimental high-confidence e-healthcare information system has also been implemented to demonstrate the performance of our framework. In our experiment, even when the data size is 64KB, the FJM is more efficient than the other products in transmitting e-anamnesis. Now, we have implemented an e-healthcare information system by integrating the technologies of information hiding, efficient encryption, self-adaptation, and auto-reconfiguration.

REFERENCES

Adelson, E. (1990). *Digital signal encoding and decoding apparatus*. U.S. Patent, No. 4939515.

Alateras, J., Anderson, T., & Mourikis, J. (2002). *OpenJMS User Guide*. Retrieved June 13, 2006 from http://www.openjms.org/

Canetti, R., & Herzberg, A. (1994). Maintaining Security in the Presence of Transient Faults. *Proceedings of 14th Annual International Cryptology Conference (CRYPTO '94)*, Santa Barbara, California, USA, 425-438.

Chang, C. C., & Lee, H. C., (1993). A new generalized group-oriented cryptoscheme without trusted centers. *IEEE Journal on Selected Areas in Communications*, *11*(5), 725-729.

Global Care Solutions Ltd. (2003). *Hospital 2000 and Amalga PACS*. Retrieved June 13, 2006 from http://www.hospital2000.com

Herzberg, A., Jarecki, S., Krawczyk, H., & Yung, M. (1995). Proactive secret sharing or: how to cope with perpetual leakage. *Proceedings of 15th Annual International Cryptology Conference (CRYPTO'95)*, Santa Barbara, California, USA, 339-352.

Hsiao, T. Y., Perng, N. C., Lo, W., Chang, Y. S., & Yuan, S. M. (2003). A new development environment for event-based distributed system. *Computer Standard and Interface*, *25*(4), 345-355.

Lin, S. C., Tseng, S. S., Lin, Y. T., & Chou, J. M. (2002a). A new mechanism of mining network behavior. *Proceedings of PAKDD'02*, Taipei, Taiwan, 218-223.

Lin, Y. T., Tseng, S. S., & Lin, S. C. (2001). An intrusion detection model based upon intrusion detection markup language (IDML). *Journal of Information Science and Engineering*, *17*(6), 899-919.

Lin, Y. T., Tseng, S. S., & Kuo, T. T. (2002b). Two layer network intrusion detection system. *Proceedings of 2002 International Computer Symposium*, Hualien, Taiwan.

Lin, Y. T., Tseng, S. S., & Tsai, C. F. (2003). Design and implementation of new object-oriented rule base management system. *In Expert System with Applications*, *25*(3), 369-385.

Ohe, K., Kaihara, S., Ishikawa, K. B., Hishiki, T., Nagase, T., & Sakurai, T. (1995). Hospital information system and the Internet. *Proceedings of International Networking Conference (INET'95)*, Honolulu, Hawaii, USA.

Ostrovsky, R., & Yung, M. (1991). How to withstand mobile virus attacks. *Proceedings of 10th Annual ACM Symposium on Principles of Distributed Computing*, Montreal, Quebec, Canada, 51-59.

Shamir A. (1979). How to share a secret. *Communications of the Association for Computing Machinery*, *22*(11), 612-613.

Softwired Inc. (2001). *iBus/MessageBus Version 4.1 – Datasheet*. Retrieved June 13, 2006 from http://www.softwired-inc.com

Sonic Software (2000). *SonicMQ programming guide 2000.1*. Retrieved June 13, 2006 from http://www.sonicsoftware.com/products/enterprise_messaging/sonicmq/index.ssp

Stinson, D. R. (1992). An explication of secret sharing schemes. *Designs, Codes, and Cryptography*, *2*, 357-390.

Sun Microsystems (1999). *Java message service, Version 1.0.2*. Retrieved June 13, 2006 from http://java.sun.com/products/jms/

Sun, H. M., & Shieh, S. P. (1994). Construction of dynamic threshold schemes. *Electronics Letters*, *30*(24), 2023-2024.

Whetten, B., Montgomery, T., & Kaplan, S. (1995). A high performance totally ordered multicast protocol. *Proceedings of International Workshop on Theory and Practice in Distributed Systems*, London, UK.

Wright, D. J. (1992). Strategic impact of broadband telecommunications in insurance, publishing, and health care. *IEEE Journal on Selected Areas in Communications*, *10*(9), 1369-1381.

Wu, D. C., & Tsai, W. H. (1998). Data hiding in images via multiple-based number conversion and lossy compression. *IEEE Transactions on Consumer Electronics*, *44*(4), 1406-1412.

Shun-Chieh Lin received his Ph.D. degree from the Department of Computer Science, National Chiao Tung University in 2006. Currently, he holds a post doctoral position at the Computing Center, Academia Sinica in Taiwan. His current research interests include network security, knowledge engineering, knowledge acquisition, and data mining, etc.

Shian-Shyong Tseng received his Ph.D. degree in Computer Engineering from National Chiao Tung University in 1984. Since August 1983, he has been on the faculty of the Department of Computer and Information Science at National Chiao Tung University, and is currently a professor there. From 1988 to 1991, he was the Director of the Computer Center National Chiao Tung University. From 1991 to 1992 and 1996 to 1998, he acted as the Chairman of Department of Computer and Information Science. From 1992 to 1996, he was the Director of the Computer Center at the Ministry of Education and the Chairman of Taiwan Academic Network (TANet) management committee. In December 1999, he founded Taiwan Network Information Center (TWNIC) and was the Chairman of the board of directors of TWNIC from 2000 to 2005. He is now the Dean of College of Computer Science, Asia University. His current research interests include data mining, expert systems, computer algorithms and Internet-based applications.

Wen-Guey Tzeng received his B.S. degree in Computer Science and Information Engineering from National Taiwan University, Taiwan, 1985, and M.S. and Ph.D. degrees in Computer Science from the State University of New York at Stony Brook, U. S. A., in 1987 and 1991, respectively. He joined the Department of Computer and Information Science (now Department of Computer Science), National Chiao Tung University, Taiwan, in 1991, where he continues to work. Dr. Tzeng's current research interests include Cryptology, Computational Complexity and Network Security.

Shyan-Ming Yuan received his B.S.E.E. degree from National Taiwan University in 1981, his M.S. degree in Computer Science from University of Maryland, Baltimore County in 1985, and his Ph.D. degree in Computer Science from the University of Maryland, College Park in 1989. Dr. Yuan joined the Electronics Research and Service Organization, Industrial Technology Research Institute as a Research Member in October 1989. Since September 1990, he has been an associate professor at the Department of Computer and Information Science, National Chiao Tung University, Taiwan. He became a professor in June 1995. His current research interests include distributed systems, Internet and education technologies, and software system integration. Dr. Yuan is a member of ACM and IEEE.