An Optimization of Security and Trust Management in Distributed Systems

Alsharif Mohamed Y. Ahmed
School of Computer Science & Engineering
Beihang University (BUAA)
Beijing, China
sharif_younis@yahoo.com

Depei Qian
School of Computer Science & Engineering
Beihang University (BUAA)
Beijing, China
depeiq@buaa.edu.cn

***Abstract*—with the development of cloud computing, the security and trust management in distributed systems is changeable. This paper proposes an architecture and solution of security and trust management for distributed systems which use cloud computing. Since the solution requires future technologies, an optimization to the security and trust management, including multi-paths transmission, virtual personal networks and encryption, is proposed. This optimization will enhance the security and trust in distributed systems.**

Keywords—optimization; Security amd trust management; Distrubuted systems;multi-path transmission

I. INTRODUCTION

The security and trust management is critical to the information system, which includes the computing resources, transmission resources and storage resources. In a distributed system or networking system, contents and messages should be kept as a secret. This means the system should protect the private message. Most distributed system requires the trust computing or safe computing. The security and trust failure often occur in our society. We do not exactly know the underlying security architecture upon which those systems are built. In particular, the system often fails to address every layer of business, technology, and process.

According to the research issues [1][2][3], some algorithms, methods and technologies, including the encryption technology and evaluation methods are already taken into consideration. But some solutions use the future technologies, which are not available in recent time.

The network is an open distributed system and classified into transmission resources, computing resources and storage resources here. It provides packet transmission services, computing services and storage services. This paper proposes a fully secured solution (architecture) for the distributed system which would protect data from attacks which are from the local area, network area and remote area. According to the architecture which we expect as secure, we propose an optimization for distributed systems.

II. DEFINITION OF SECURITY AND TRUST ARCHITECTURE

Security architecture is defined as the distributed organization that describes how the security controls are positioned, and how they relate to the overall information technology architecture. These controls serve the purpose to maintain the system's quality attributes, among them including confidentiality, integrity, availability, accountability and assurance.

The objective of security architecture includes protection of information and property from theft, corruption, or natural disaster, while allowing the information and property to remain accessible and runnable to its users.

The term system security means the processes by which sensitive and valuable data and services are protected from publication, tampering or monitoring by unauthorized users or untrustworthy individuals and unplanned events respectively [4].

III. THE SOLUTION OF SECURITY AND TRUST SYSTEM

This paper proposes the architecture of security and trust system for networking and distributed computing. Fig. 1 shows the architecture of security and trust system (STS). STS is a distributed security and trust architecture that provides a suite of functions including login, authentication, and access control, encryption/decryption and encryption computing in a distributed system. It is different from other similar architectures; the STS architecture offers the ability to access all these functions without the trusted devices being active.

STS is consisted of the user end and server end. The connections between the user end and the sever end are formed by the internet, including routers, switches and fibers. The following gives a description to the user end and server end.

- The user end, called local end, consists of the input from keyboard, the output to the screen or printer, the local computer for computing and disks for storage.
- The server end, called remote end, has servers for computing and disks for storage.

978-1-4673-4529-3/12/$31.00 ©2012 IEEE

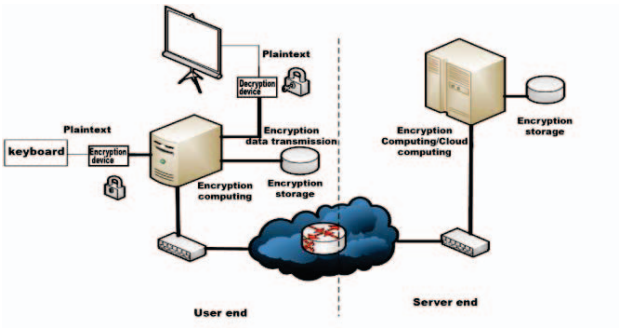

Fig. 1. Architecture of security trusted system

If STS is considered as a secure and trust system, there are some important hypotheses, descripted in the following, working in the system.

- Input protection: Nobody could see or know what you click on the keyboard, because most of information leak happens when you show your words.
- Output protection: Nobody could see or know what are showing on the screen or print pages.
- Encryption protection: The encryption algorithms, being active in the transmission, storage and computing, should not be decrypted by any organization or users [5].

A. Data Stream in the Security and Trust System

The security and trust system (STS), described in the architecture, is a data stream process system, with the data input and output in the user end. STS is a closed security and trust system, which would be able to process, transmit, store and protect data. Data in STS could be described as the stream.

The data stream in STS can be described as following:

Input(data)→ Local encryption (data) → Local encryption computing (Local encryption (data))

→Transmission (Local encryption (data)) → Remote encryption computing (Local encryption (data))

→Transmission (Local encryption (data)) → Output(data).

Data in STS is encrypted in order to protect its privacy from the eyes of others and modifications to the data are not allowed. Technologies for protecting the privacy and for verification include the local encryption and remote encryption computing.

- The local encryption, encrypting data at user's computer, is the technology which would be used in the future security system. In contrast with the local encryption, the remote encryption, encrypting data at server, is considered as the fake security technology. Even though the remote encryption is easily implemented by the service providers, they will be not considered by customers [6].
- The remote encryption computing, computing on the encryption data in the server end is a future technology which is not available in recent time.

B. The Local Security and Trust

Most of work in the user end is to input data, locally pre-process data and output data. Unfortunately, data in the user end, (e.g. customer's computer, would be controlled by the malicious software, such as software virus) [7][8]. Especially, users are not using their own computers. The following gives analysis of attacks from the local side.

- Malicious software: Malicious software, e.g. virus, would be able to capture the sensitive data, e.g. the username and password, from the keyboard, disks and screen. Moreover, it can control customer's computer and could do what the customer can do [9].
- Computer security: If customers may not use their own computers, they would not be sure whether their sensitive data would be left on the computer or not [10].
- Location safety: The data input and output of the closed system are settled at the local (user end). No any technologies could protect the plaintext output and input except the location safety, which is controlled by customers and guards.

The local security and trust is the core idea in the closed system. The user end, local end, should have the capability for data protection. If the above measures are considered as safe, another two devices should be introduced to the user end. One is the encryption device between the keyboard and the computer, and another is the decryption device between the screen and the computer. STS only need such encryption devices and decryption devices to keep the whole system safe and trust. STS is considered as the safest and most trusted system. The data in computing resources, transmission resources and storage resources is encrypted and no users, software and virus could know user's information.

C. The Remote Security and Trust

The remote security and trust is the security and trust in the server end. Most of servers, hosted in carriers' internet data centers, which may not be owned by customers. The data encryption algorithms in the server end may be provided by customers themselves and third parties, e.g. carriers and service providers. However, customers may risk the following:

- If the encryption algorithms were provided by the third parties, including managers and administrators, the third parties would have the ability to know customer's data.
- If the encryption algorithms were provided by customers themselves and runs on the server, the encryption algorithms would be known to administrators.

As the data and encryption algorithms cannot be known to third parties, the encryption at the remote side is not safe, although they really run on servers recently. Fig. 2 shows safe streams and unsafe streams. All remote encryptions and decryption are not safe, because of the leak of encryption algorithms and data to administrators and managers. The only safe stream is the data encrypted at the local side.

STS proposes the local security and trust, accomplished by local encryption, would address the above security ant trust issues.

- Local encryption encrypts and decrypts data at customer's computer which is controlled by customer and customer could ensure whether his computer is secure or not.

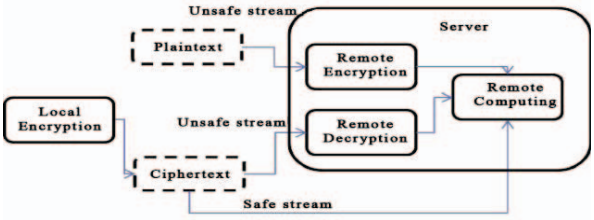

Fig. 2. Safe streams and unsafe streams

- Malicious users, sniffers and monitors have fewer opportunities to know the encryption Algorithm and plaintext from transmission resources, remote computing resources, and even the local resources [11].Table I describe the data stream and corresponded rank.

TABLE I. DATA STREAM AND SECURITY RANK

No.	User end (Local)	Server end (Remote)	Security Rank
1	*Encryption*	*Encryption*	*1*
2	*Encryption*	*Decryption*	*3*
3	*Encryption*	*Decryption/Encryption*	*2*
4	*Plaintext*	*Encryption*	*4*
5	*Plaintext*	*Plaintext*	*5*

The remote encryption stream is rank less secure than the local encryption stream.

In the following we are going to propose some security and trust methods, approaches and technologies for the architecture, STS which we expect to work is the user end and server end.

IV. SECURITY AND TRUST METHODS AND TECHNOLOGIES

All the resources, including computing resources, storage resources and transmission resources, are not secure and trusted yet because of the following reasons:

- The first attack to user data is from the computer at the user end, which directs connects to the keyboard. The computer at the user end, considered as the computing resource, is not safe because of the intrusion of virus and malicious applications.
- The transmission resources, such as routers, switches, fibers and links, are also not safe, because their physical locations are not safe and trusted, and all routers, links and switches are not controlled by users.
- The computing resources and storage resources at the server end, such as servers and disk racks, are not safe and trusted also, because their physical locations are not safe and not controlled by users from the user end. Moreover, they may be also intruded by viruses and malicious applications.

A. Attacks and Attacker Areas in the System

All attacks are shown in Fig. 3. Attackers would have three areas to attack resources, local area, network area and remote area. Malicious users in the local area would be able to attack the local screen, keyboard, local computer and local storage. Sniffers in the network area like to monitor routers and fibers [11][12]. Attackers in the remote area have opportunities to attack servers and their storage.

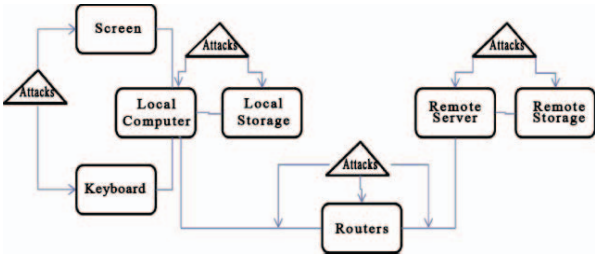

Fig. 3. Attacks to the distributed system

Table II shows attacks and attackers in the distributed system. Attackers include men's eyes, malicious software, sniffers and administrators.

TABLE II. ATTACKS AND ATTACKERS

No.	Area	Attacks	Attackers
1	Local area	*Screen attack*	*Eyes*
2		*Keyboard attack*	*Eyes*
3		*Local storage attack*	*Software*
4		*Computer attack*	*Software*
5	Network area	*Router attack*	*Monitor*
6		*Fiber attack*	*Sniffer*
7	Remote area	*Remote server attack*	*Administrator*
8		*Remote storage attack*	*Administrator*

The encryption/decryption strategies or technologies can keep the data safe, when the data is in computing resources, storage resources or transmission resources. The encrypted data would not care what location the data stay and what kind of resource the data is with. The encryption/decryption technologies are easy to deploy in transmission resources and storage resources, but there is no actually better solution for computing encryption.

B. Trusted Computing Approaches

Trusted computing (TC) is a technology which is promoted by the Trusted Computing Group (TCG) [13]. With trusted computing, the computer will consistently behave in an expected way, and those behaviors will be enforced by computer hardware and software [14].

Trusted computing proponents such as International Data Corporation, the Enterprise Strategy Group and Endpoint Technologies Associates claim the technology will make computers safer, less prone to viruses and malware, and thus more reliable from an end-user perspective [15]. In addition, they also claim that trusted computing will allow computers and servers to offer improved computer security over that which is currently available [16].The trusted computing

includes the trusted hardware, trusted operating system and trusted applications.

Chip manufacturers such as Intel and AMD, hardware manufacturers such as Dell, and operating system providers such as Microsoft all plan to include trusted computing in coming generations of products. The first challenge is the hardware controlling.TC is controversial as the hardware is not only secure for its owner, but also secure against its owner. Such controversy has led opponents of trusted computing, such as free software activist Richard Stallman, to refer to it instead as treacherous computing, even to the point where some scholarly articles have begun to place scare quotes around "trusted computing". The following will illustrates a trusted computing based on encryption computing.

C. *Encryption computing technology in the system*

Encryption computing is called "blind computing". The encryption computing allows a user to encrypt his data and transmit the data to a computing server [17]. The server stores the encrypted data and processes the encrypted data; even the server doesn't know what it's processing [18]. Fig. 4 is the architecture of encryption computing. Data from the user, such as data A and data B must be encrypted firstly before transmitting over the internet and entering into the server, whose hardware is not controlled by the user. So the encrypted data A and the encrypted data B are not clear to the server. Moreover, the server uses the encryption computing, whose intention is not clear to the server owner or other users, especially the virus or malware except, the user itself.

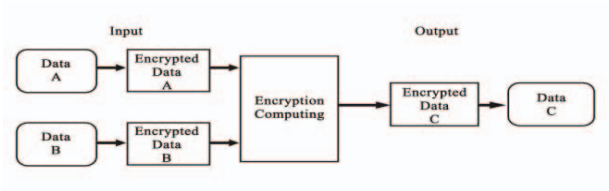

Fig. 4. The architecture of encryption computing

Encryption computing technology are fairly welcomed, but they are not mature and far from being usable. The typical examples, published over the internet or in the journals, are the quantum computing and the homomorphic encryption (HE) method [7]. They can offer the encrypted computing for distributed systems, such as the cloud computing systems, which have the big challenge in the trust and security issues [19].

Encryption computing is like something out of a spy novel. Scientists like Broadbent are trying to develop quantum computers that would revolutionize information processing. They use the mysterious nature of quantum mechanics to create the super-secret information that cannot be decoded by cloud computing systems. The breakthrough, published recently in the journal Science, is a crucial step toward perfectly secure cloud computing, a growing industry providing computer processing and data storage over the internet and other networks.

The HE method is a kind of encryption method, which uses the traditional data encryption algorithms, such as the RSA algorithm [20].It is considered as an encryption method for computing, when the IBM scientist begun to show their research results over Internet. In our solution, we suggest to use the HE method.

The HE methods include two types, partially HE methods and fully HE methods. Partially HE methods are efficient, but they can carry out all computing issues. Fully HE methods can calcite use all operators, but they are less efficient. Others see the potential of. HE Recently, Defense Advanced Research Projects Agency (DARPA) announced a 20-million-dollar research project to solve the cryptographic problems, already awarding the research company Galois five million dollars [21].

V. Optimization of Trust System

The typical trust distributed system is full secure system, where nobody can know the exact data and the computing process. However, this full secure system is an ideal system, because most of technologies for this system are not available now, especially the encryption computing algorithms. For the real world, the encryption computing is not available. Most of the engineers or scientists have to keep servers staying in secure locations or controllable locations in order to protect servers avoiding the intrusion. However, the physical location secure is not a critical issue, because companies may have their own internet data centers (IDCs). Intrusions come from malware over the Internet cause most of security accidents. Some passwords or encryption keys may be lost or leak, when servers are intruded by the malware or virus. In such situation, the computing resources are not secure and trustable. All we want to do is to keep encryption keys or password in a relative secure state and avoid the data capture.

This is a typical distributed system. The resources in the Internet are classified into computing resources, storage resources and transmission resources. The security trust challenges are how to protect data in the computing resources, storage resources and transmission resources. In order to avoid the data capture, the whole system must be changed according to the requirements of security. Fig. 5 gives an optimization of the trust system. The architecture shown in Fig. 5 does not consider the security of computing resources, where servers have not used the encryption computing and data stored in disks are plain text. Moreover, the personal computer at the user end also does not use the encryption computing. The encryption technology is used in the transmission resources, from the personal computer to the server.

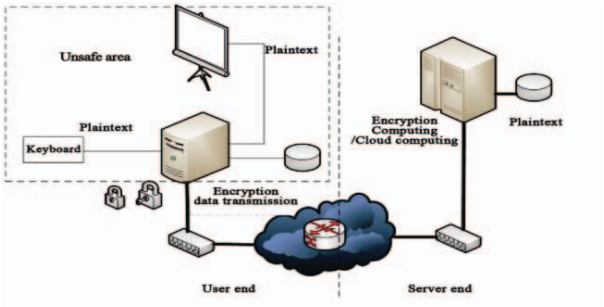

Fig. 5. An optimization of the trust system

The challenge of such system is how to keep encryption keys, passwords and encrypted data safe, and avoid the malware intrusion. Although the encryption computing is the best solution for this issue, most of efforts will be focused on the system protection, location security and device control. With the transmission resources, we introduce the dynamic transmission strategies, which we will not discuss in details in this paper (it is not our main topic here).

A. *Secure Transmission and Challenges*

The IP network includes links, routers and computers. Links and routers transmit packets from the source computers to the destination computers only. Computers in the IP network can store data (such as databases, pictures and text files) and computing for users, which are called applications. Fig. 6 depicted typical public IP network.

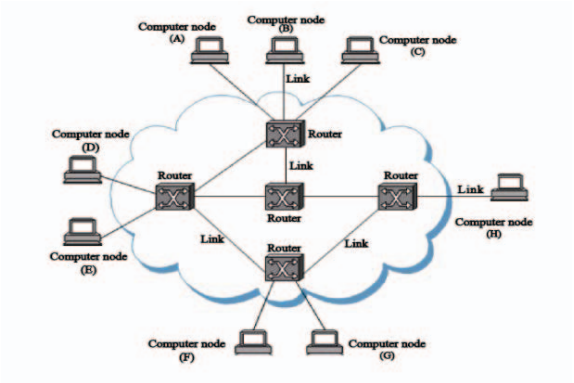

Fig. 6. Typical public IP network

We find two challenges in the existing IP network. The first challenge is how to protect data in the packet transmission. That is how to keep links and routers safe. The second challenge is how to protect data in computers. Some computers want to know the data from the source computers, while others only want to compute data, especially in the cloud computing.

Most applications use virtual private networks (VPNs) [22] to protect data in the packet transmission. A virtual private network is a secure virtual network that uses primarily public IP networks to transmit the private data or provide remote users an access to their office networks.

B. *Fixed Virtual Private Networks*

Virtual Private Networks (VPNs) provide security connections between users and servers, or from one local network to another. With the VPNs, firewall and encryption technology are used to prevent disclosure of sensitive data to unauthorized users. VPN also provides users who are not on that internal network, secure access to resources inside it. This is done by creating tunnels (IPSec Tunnel) that wrap data packets destined for the internal network and then encrypting those packets to send them across the Internet. IPSec functions through encrypting and encapsulating an IP packet inside an IPSec packet. De-encapsulation happens at the end of the tunnel, where the original IP packet is decrypted and forwarded to its intended destination Fig. 7 shows the existing virtual private network. Computers communicate over private virtual connections, marked by black dashed line. Some of VPNs use the multicasting technologies to construct the multicasting tree.

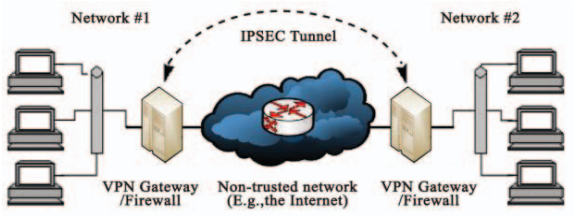

Fig. 7. The virtual private network

Although the VPNs are considered as the secure infrastructure for communications, but the sensitive data is not safe, when the computer is not safe, where the encryption keys or authentication passwords could be disclosed by the malware or virus. When the unauthorized users get keys or passwords, they want to decrypt sensitive data. In such way, only one thing we want to do is to protect the data.

Data is not easy to be assembled in the destination computers, if some applications do received their data and assemble data by themselves. Most of data is captured from the transmission resources. As a reason, the transmission resources should be protected as the final breakthrough line. With the fixed virtual private networks, unauthorized users can capture encrypted data or plain data from the routers, optical lines or listeners, when they know the actual connections between computers or local networks. However, unauthorized user must get whole encrypted data, when they want to decrypt data. Hence, we have another method to destroy the idea of unauthorized users, which is to cut data to pieces and transmit different pieces by different transmission technologies or different connections. The following section will explain the solution for such method.

C. *Dynamic Transmission Method*

Dynamic transmission is a method to destroy the data integrity by transmitting data using different connections, transmission technologies, strategies and physical networks. Fig. 8 is an example of the dynamic transmission method. The nodes denote computers in the internet; others are routers for forwarding data only. As we can see, data is divided into packets or segments, and packets are forwarded to the

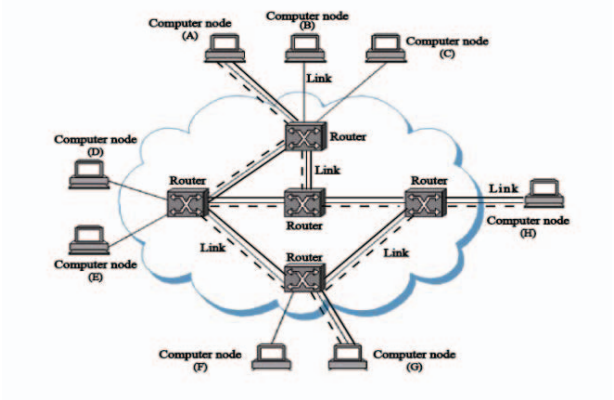

Fig. 8. an example of dynamic transmission method

destination computers over several paths, such as the black thick paths and dash paths. Although data finally reach to destinations; packets can avoid being fully captured by using one technology or listening to one path. With the dynamic transmission, it increases the difficulty for unauthorized users to fully capture all packets. That is the case to destroy the data integrity. In some case, data is encrypted before the transmission. The destination computer will decrypt data only depending on the computer's receiving all packets from the source computer. Data, with its integrity, can be known to the destination computer. If unauthorized users capture some pieces of encryption data, they are impossible to know the actual data, when the destination computer has the location safe and has no malware, virus or computer loopholes. This system can be safe, when the computing resources are safe and the transmission resources are also safe [23].

The dynamic transmission method includes the multi-paths transmission technology and the data assemble technology. The multi-paths transmission technology arranges the packets from data and forward packets to multi-paths in order to avoid the packet capturing. The data assemble technology is used to assemble packets to data. Both of the technologies would provide protection for data.

D. Multi-paths Transmission

The multi-paths transmission technology is a transmission technology which separates and forwards packets two different paths in an unsafe area [24]. We divide networks into safe areas and unsafe area. A safe area is a place where devices, such as computers, routers, switches and fibers, software and passwords can be controlled by users or administrators. Moreover, the malware or virus should be removed by a kind of software. An unsafe area is a place, where the switches, routers, and fiber belong to service providers or any companies. Users have no ability to control their condition, intrusion and anything ever, but all over the resources are only for packets transmissions. Fig. 9 depicts the safe areas and the unsafe area. For the safe area, on the user side, the computers and routers are controlled by users, so that such area is considered to be safe. On the server side, servers and storages are controlled by trusted companies or user's own Internet data center (IDC). The unsafe area may be owned by telecommunication companies, where telecommunication companies could not control fibers and routers by themselves, because most of fibers are in the outside and anyone can touch them.

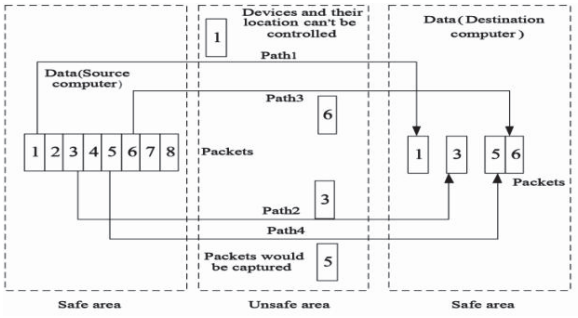

Fig. 9. Multi-paths transmission and safety

With the unsafe area, packets would be captured from routers, switches, or even fibers, assembled and analyzed by unauthorized users. Tools may be applied to decrypt packets and data. The multi-paths transmission forwards packets via more than one path. The source computer forwards packet 1,3,5,6 with path 1, path 2, path 4 and path 3 over the unsafe area in Fig. 9. Unauthorized users in the unsafe area may capture packets from one path. For example, once unauthorized user capture packet 5 from path 4, but they lost packets from path 1, path 2 and path 3.Once unauthorized users capture some packets, such as packet 5 and packet 3, and they cannot decrypt data because the captured data (packets) lost its integrity. Such data cannot be decrypted to plaintext. The purpose of the multi-paths transmission technology is to destroy the integrity of data, avoiding data decryption. Fig. 10 shows a packet capture area, where path 2 and path 4 are both listened by unauthorized users. Packet 2, 3, 5, 7 are forwarded over path 2 and path 4. Unfortunately, they are all captured by unauthorized users. With packet 2,3,5,7, unauthorized users cannot decrypt the plaintext, because data in packet have lost it integrity.

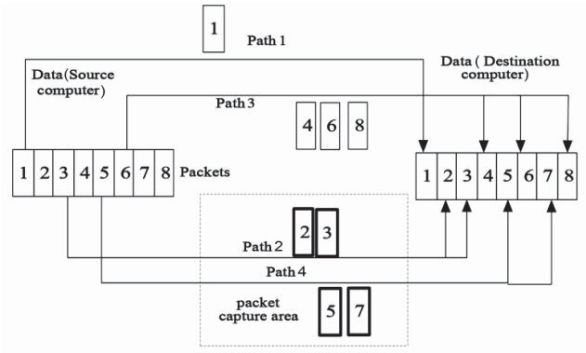

Fig. 10. Packet capture area and packets analysis

However, some clever listeners can capture all of packets from the source computer to the destination computer. We must introduce new scheme to protect data and packets in such situation. The data assemble technology would help us to protect data decryption.

E. Data Assemble Technology

The data assemble technology is carried at the destination computer when the destination computer received all packet from the source computer. Such thing will be carried also by unauthorized users. The data assemble technology is authorized to the destination computer or software running on the destination computer. Listeners, who capture packets from the unsafe area, are unauthorized users, and they don't know the actual assemble method and technology. Fig. 11 depicts the assemble technology which can protect data from the source computer. When the listener capture all packets from the source computer, packets are in disorder, data in the packets use multi-encryption algorithms, and the data integrity is based on multi-assemble method. So the assemble technology includes the disorder method, multi-encryption algorithms and the multi-assemble method.

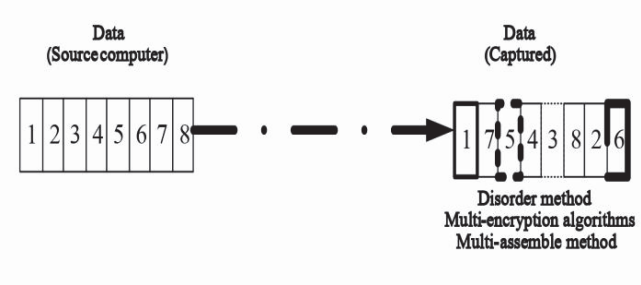

Fig. 11. Data protection using the assemble technology

The disorder method somehow already exists in the Transportation Control Protocol (TCP), but the packets over TCP are labeled by order number. That is, unauthorized users can assemble the TCP packets according to the protocol and order number. The disorder technology used in the assemble technology are implied by the software in the destination computer instead of inserting order number in packets, when the destination decrypt data.

The multi-encryption and multi-assemble method are also implied by the software in the destination computer. No method or encryption algorithm will be labeled in the packets, in order to avoid the decryption and the data assemble by listeners.

In such situation, anyone, who captures all of the packets, can't order them, decrypt them and assemble them. All strategies will keep transmission resources in the network safe.

VI. CONCLUSION

The distributed system includes transmission resources, computing resources and storage resources. The private information protection and computing require security technologies in transmission resources, computing resources and storage resources. But the encryption computing technology is under research and not available till now. An intermediate solution should be considered to overcome the unsafe computing. The location safety and software control should be enhanced to guarantee the safety of computing.

In order to enhance the computing safety, the dynamic transmission technology should be used as the transmission resources. The dynamic transmission technology includes the multi-paths method and the assemble technology. The multi-paths method enhances the safety in the unsafe area, such as the Internet. The assemble technology would enhance the safety when all packets are captured by unauthorized users or listeners.

REFERENCES

[1] Y.-H. Chu et al., REFEREE: Trust Management for Web Applications, 1997, AT&T Research Labs, http://www.research.att.com/~jf/pubs/www6-97.html.

[2] A. Vilmos and S. Karnouskos, SEMOPS: Design of a new Payment Service, International Workshop on Mobile Commerce Technologies & Applications (MCTA 2003), In proceedings of the 14th International Conference (DEXA 2003), September 1-5, 2003, Prague, Czech Republic.

[3] M. Blaze, J. Feigenbaum, and J. Lacy, "Decentralized Trust Management," IEEE Conf. Security and Privacy, 1996, Oakland, California, USA, http://www. crypto.com/papers/policymaker.pdf

[4] Simmonds, A; Sandilands, P; van Ekert, L (2004). "An Ontology for Network Security Attacks". Lecture Notes in Computer Science. Lecture Notes in Computer Science 3285: 317–323. doi:10.1007/978-3-540-30176-9_41. ISBN 978-3-540-23659-7.

[5] Biham, Eli and Shamir, Adi (1991). "Differential Cryptanalysis of DES-like Cryptosystems". Journal of Cryptology 4 (1): 3–72.

[6] William Stallings, 1998. Cryptography and Network Security Principles and Practice, Second Edition. Prentice Hall, Upper Saddle River, New Jersey.

[7] Burger, Ralph, 1991. Computer Viruses and Data Protection, pp. 19-20.

[8] Szor, Peter (2005). The Art of Computer Virus Research and Defense. Boston: Addison-Wesley. ISBN 0-321-30454-3.

[9] Ludwig, Mark (1993). Computer Viruses, Artificial Life and Evolution. Tucson, Arizona 85717: American Eagle Publications, Inc. ISBN 0-929408-07-1.

[10] J. C. Willemssen, "FAA Computer Security". GAO/T-AIMD-00-330. Presented at Committee on Science, House of Representatives, 2000.

[11] Kevin J. Connolly (2003). Law of Internet Security and Privacy. Aspen Publishers. pp. 131. ISBN 978-0-7355-4273-0.

[12] P. England, B. Lampson, J. Manferdelli, M. Peinado, and B. Willman. A trusted open platform. IEEE Computer, 36(7):55–63, 2003.

[13] Oltsik, Jon (January 2006). "Trusted Enterprise Security: How the Trusted Computing Group (TCG) Will Advance Enterprise Security" (PDF). White Paper. Enterprise Strategy Group. Retrieved 2007-02-07.

[14] Ross Anderson, "Cryptography and Competition Policy - Issues with 'Trusted Computing' ", in Economics of Information Security, from series Advances in Information Security, Vol. 12, April 11, 2006.

[15] Rau, Shane (February 2006). "The Trusted Computing Platform Emerges as Industry's First Comprehensive Approach to IT Security" (PDF). IDC Executive Brief. International Data Corporation. Retrieved 2007-02-07.

[16] Kay, Roger L. (2006). "How to Implement Trusted Computing: A Guide to Tighter Enterprise Security" (PDF). Endpoint Technologies Associates. Retrieved 2007-02-07.

[17] N. Ahituv, Y. Lapid, and S. Neumann. Processing Encrypted Data, In Comm. of the ACM, vol. 20, pages 777-780, 1987.

[18] E. Bach and J. Shallit. Algorithmic Number Theory, Volume 1, 1996.

[19] E. Brickell and Y. Yacobi. On Privacy Homomorphisms. In Proc. of Eurocrypt '87, LNCS 304, pages 117-125. Springer, 1988.

[20] B. Ptzmann and M. Waidner. Attacks on protocols for server-aided RSA computation. In Proc. of Eurocrypt `92, LNCS 658, pages 153-162. Springer, 1993.

[21] DARPA Invests 5 Million Towards Solving Homomorphic Encryption, http://www.thehostingnews.com/darpa-invests-5-million-towards-solving-homomorphic-encryption-17158.html.

[22] Metz, C. (Jan/Feb 2003). "The latest in virtual private networks: part I". IEEE Internet Computing (IEEE Computer Society) 7 (1): 87-91.

[23] Zhi Li and Yu-Kwong Kwok, "A New Multipath Routing Approach to Enhancing TCP Security in Ad Hoc Wireless Networks," Proc. ICPP Workshops, pp. 372-379, June 2005.

[24] S.-J. Lee and M. Gerla, "Split Multipath Routing with Maximally Disjoint Paths in Ad Hoc Networks," Proc. ICC 2001, vol. 10, pp. 3201–3205, June 2001.