An Evaluation to Security of Distributed System

Alsharif Mohamed Y. Ahmed and Qian Depei

***Abstract*—The distributed system is consisted of transmission resources, computing resources and storage resource. The construction, evaluation and testing of trusted distributed system are challengeable for users and administrators. This paper proposes several methods to evaluate performance and protection technologies in order to enhance the security of transmission resources, computing resources and storage resources. The evaluations include the performance of security, security level and security logics.**

***Index Terms*—Distributed system, security value, security logic, security evaluation.**

I. Introduction

The network is an open distributed system, including transmission resources, computing resources and storage resources. However, some technologies, such as the encryption computing technologies are future technologies and not available in recent time [1]. We can't evaluate these future technologies. Regarding recent technologies, they are not able to address all security issues, especially the encryption storage technologies. As a solution, we combine several recent technologies to address such issue, and then we give evaluations to them.

We setup the following environment as shown in Fig. 1 for evaluation, which has user personal computers (PCs), servers and network (routers, links and switches) with the following assumptions:-

The distributed system is consisted of user end and server end. The user end includes PCs, storage and transmission resource. The server end includes servers, storage and transmission resource.

The encryption algorithm for transmission is equipped both in the user side and server side in order to enhance the transmission security.

PCs in the user side would be able to use the encryption technologies [2], but the key board and screen shows the plaintext. Suppose PCs in the user side should have the location safe environment.

Servers in the user side would be able to use the encryption technology. Two situations should be taken into consideration. That is severs may be in location safe environment or location unsafe environment.

All security technologies and environment can be combined. They are either encryption technologies or location safe technologies.

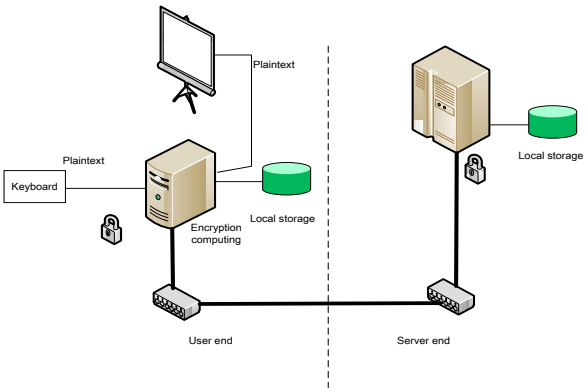

Fig. 1. Environment for evaluation.

II. Security Value and Security Logic

At first, what customers concerned is whether the distributed system is secure or not. If the distributed system is secure, the value '1' is given to evaluate the system security. Otherwise, the value '0' is given to evaluate the system security [3].The value for evaluating whether, the distributed system is secure or not, is referred to as 'security logic'.

But, sometimes customers want to know the degree of security the distributed system they are going to use. Researchers tend to give a value to indicate or to show how secure the distributed system is. Such value is referred as 'security value'. The security value is the value in the range between: 0.0-1.0, such as 0.5, 0.71, 0.87, 0.9 and 0.94 etc...

We can apply these two values, security logic and security value, to any distributed systems. If the distributed system is secure, the security logic is assigned to '1' and nobody will care what the security value is, because when security logic is assigned to '1' that means security value will also will be absolutely 1.0.On the other hand, if the distributed system is not secure, the security logic is assigned to '0' In this case customers are still interested to know how secure the distributed system is. That means they want to know the security value of this distributed system, it could be high enough.

If the security of distributed system is described as 'security logic = '0' and 'security value = 0.9', such distributed system is considered as a good secure system, which also better than (more secure) the system described as 'security logic = "0' and 'security value = 0.1', which has the critical fault in the system. We can also combine the security logic and the security value in a way that can reflect security degree of the system according to conjunction of the two values, we combine the security logic and the security value as (security logic, security value) = (L, S).

Manuscript received November 9, 2012; revised January 14, 2013.

Alsharif Mohamed Y. Ahmed is with the School of Computer Science and Engineering, Beihang University (BUAA), 37 Xueyuan Road, 100191 Haidian District Beijing ,China (e-mail: sharif_younis@yahoo,com).

Qian Depei is with Sino-German Joint Software Institute Beihang University (BUAA), 37 Xueyuan Road, 100191 Haidian District, Beijing, China (e-mail:depeiq@buaa.edu.cn).

If L=1, then S=1.0.

If L=0, the S<1.0.

where L and S represents Security Logic & Security value.

According to the security logic (L) and security value(S), we can rank the security of any system as the following:
(L, S)= (1, 1.0) > (0, 0.9) > (0, 0.7) >… > (0, .00)

The best case is that the security logic is '1'. That is the system is absolutely secure.

The second case is that, even though the security logic is'0', the security value can still be in a high value, which can keep the distributed system secure enough.

The final case is that, the security logic is '0'; the security value is also approach to 0.0 values which is the worst case that means the distributed system is absolutely not secure.

III. Security Evaluation

The security evaluation is a technology to compute the value of trust and security. The trust and security include the computing resource security, the transmission resource security and the storage resource security. The storage resource security is the basic resource security in this case [4]. However, the distributed system has more than one resource; for example, a distributed system commonly includes the local computing resource, local storage resource, transmission resource, remote computing resource and remote storage resource [5]. Such system is referred as multi-resources system. For the multi-resources system, the evaluation for the security of such system is more complex than the single-resource system. The following gives the solution for security evaluation of multi-resources system.

A. Importance Value for Multi-Resources System

As the security importance is defined according to the importance of the resources, such as computing resources, storage resources and transmission resources, we can give an expression for an importance value $imp_i \in [0, 1]$ for each resource in the system.

- Where is the resource number

We give the importance value for each resource in the tested system as depicted in the following table (Table I) for testing.

TABLE I: The Importance Values for Resources

Resource Number(i)	Resource Name	Importance value(imp_i)
1	Computing resource	0.20
2	Storage resource	0.50
3	Transmission resource	0.25
4	Keyboard	0.001
5	Screen	0.001
6	Printer	0.0001
7	Com1	0.0001
…	…….	….
	Total	1

The importance value denotes the importance of resources. As we can see in Table I, the importance value is ranked as: $imp_2 > imp_3 > imp_1 \ldots$ Hence, the storage resource is the most important resource regarding the security value. The importance value depends on the importance to the security with resources. With regards the importance value, we take following facts into consideration in order to understand the effect of some resources in the distributed system:

Most security issues happen on the storage resources. Most malicious users archive their target by attacking servers' disks. Moreover, server administrators and managers could easily access server disks. Hence, the storage resources, especially server storage resources, are most important resources (security value) to users compared with other resources in the system.

At the user end, the keyboard, screen, COM1, and COM2 are controlled by customers and hosted in a secure location, home or office (private use only). Such resources have less opportunity to leak information or being attacked by malicious users. Hence, they are less important than storage resources.

The computing resources, such as central process units (CPUs) in servers' computers, are provided by the third party companies and hosted in carries' internet data centers (IDC). Administrators could know the computing resources and users' private data. Hence, the computing resources are important resources as well.

The transmission resources, such as fibers, routers and switches, provided by carries, are deployed in the country side, streets and buildings, where anybody can access the network. Even though they are in an unsafe location, information in transmission resources is not so easy to be known by malicious users. So a transmission resource is less important than storage resources and more important than other resources.

B. Security Value Calculation for Multi-Resources System

Multi-resources systems, such as the distributed system, would have more than one resource, including storage resources, computing resources and transmission resources [6]. Even though we can define the importance and security value for resources, we should create a formula to calculate the security value for multi-resources systems as a whole. The security value for multi-resources systems is the total security values of the whole system.

When dealing with individual resource, such storage resource, transmission resource and computing resource, we can simply give a security value to the resource by the following notations:

- Si $\in$ [0, 1] Denotes the security value for the ith resource.
- impi $\in$ [0, 1] Denotes the importance value for the ith resource.
- impi $\times$ Si $\in$ [0, 1] Denotes the security value for the ith resource occupied in the system.

According to the above definition, we can derive a general formula to calculate the total security value as following:

$$S = \Sigma_1^n (imp_i \times S_i) / \Sigma_1^n (imp_i) \ldots\ldots\ldots\ldots (1)$$

where
n denotes the total number of resources.
i is the resource number, or the i_{th} resource.

If the system includes all resources, then:

$$\Sigma_1^n (imp_i) = 1$$

else

$$\sum_1^n (imp_i) \neq 1$$

The security value for the system is calculated by using (1) and defined as the interval values from 0.0 to 1.0. The value is viewed as the total security situation for the distributed system. The following section will give an illustration by an example of evaluating the multi-resources systems.

C. Evaluation of Multi-Resources Systems

According to Table I, the security of storage resource is the most important resource in our tested system in terms of security, where data is well arranged and easy to handle and get, when the storage system is in uncontrolled situation. The computing and transmission resource are less important than the storage resource. At last, the peripheral devices, such as keyboards and screens resources, are not important compared with the other parts of the distributed system.

In order to understand the calculation of security value of multi-resources system, Table II give importance values and security values to every resource in the multi-resources system.

TABLE II: SECURITY VALUES AND IMPORTANCE VALUES FOR RESOURCES

Resource Number	Resource Name	Importance value	Security value
1	Computing resource	0.20	0.5
2	Storage resource	0.50	1.0
3	Transmission resource	0.25	0.9
4	Keyboard	0.001	1.0
5	Screen	0.001	1.0
…	…….	….	
	Total	1.0	

According to the security values and importance values in Table II, we can calculate the security value of the multi-resources system by using (1) we get the following result:

$$S = (imp_1 \times S_1 + imp_2 \times S_2 + imp_3 \times S_3 + imp_4 \times S_4 + imp_5 \times S_5) / (imp1 + imp_2 + imp_3 + imp_4 + imp_5)$$
$$= (0.20 \times 0.5 + 0.5 \times 1.0 + 0.25 \times 0.9 + 0.001 \times 1.0 + 0.001 \times 1.0) \div (0.20+0.5+0.25+0.001+0.001)$$
$$= 0.827 \div 0.952$$
$$\approx 0.87$$

If the multi-resources system only includes two resources, computing resource and transmission resource, labeled in Table II as resource number 1 and 2, we can use the same formula to calculate the security value of the system and get the following result:

$$S = (imp_1 \times S_1 + imp_2 \times S_2) / (imp1 + imp_2)$$
$$= (0.20 \times 0.5 + 0.5 \times 1.0) / (0.20+0.5)$$
$$= 0.6/0.7$$
$$\approx 0.86$$

Similarly, we can calculate the security value of the systems with an arbitrary numbers of resources (individual, dual and multi-resources) by means of (1). The security value for the multi-resources system is the total security value of all resources in that system. The security value may vary in different multi-resources system. The security value of the sub-system could be larger or smaller than the security value of the total system. As we can see, in the previous examples the second multi-resources system is a sub-system of the first multi-resources system and its security value is less than the first multi-resources system.

D. An Evaluation to Transmission Resources

Transmission resource is consisted of routers, switches and links [7]. Unauthorized users could capture packets from routers, switches and even links. Packets in the transmission resources can be classified into two categories. The first category refers to the packets whose contents are encrypted, and the other category is that the contents of the packets are not encrypted (included the plaintext). The security value and security logic for transmission resources are defined as follows:

The security value for transmission resource indicates or shows to the users how safe the transmission is by giving a dedicated value that ranges from 0.0 to 1.0.

The security logic for transmission resources indicates or shows to the users whether the transmission is absolutely safe or not, by giving only two dedicated Boolean value '0' or'1'.

The next two sections will explain the way of evaluation of security value and security logic for transmission resources.

1) The security value for transmission resources

The security value for transmission resources depends on some conditions that will be described in the following status:

- Status 1: Whether the encrypted contents of the packets [8] could be decrypted or not.
- Status 2: Whether the contents in the packets are encrypted or not.
- Status 3: How many packets the intruder can capture during packet transmission.

Suppose that the content of the packets can be decrypted as soon as all packets including its content are captured, when the malicious users or the intruders know the decryption algorithm [9]. In status 1 the security value is: where S can be one of the following cases:

- Case 1: S =0.0, (if the intruder or malicious knows the decryption algorithm and captures all the packets).
- Case 2: S is between 0.0 and 1.0, (if the intruder or malicious user knows the decryption algorithm but cannot capture all the packets).
- Case 3: S =1.0, (if the intruder or malicious do not know the decryption algorithm).

For example, if the malicious knows the decryption algorithm and capture 50% of packets that the user sends. The security value of this transmission will be about S=0.5.

When the contents of the packets are in status 2 (contents of the packets are not encrypted), i.e., in the plaintext form, we should use the physical policy, like multi-paths transmission. Then the security value is: where S in this case will be one of the following cases:

- Case 1: when S =0.0, (if the intruder or malicious captures all the packets)
- Case 2: when S is between 0.0 and 1.0, (if the intruder or malicious captures some of the packets).

2) The security value for transmission resources

The security logic for transmission resources highly depends on the decryption algorithm and the location where the network is hosted. Since formulas could give us a direct view of security, we analyze the security logic by using discrete mathematics expressions. The following gives the security logical value and expressions. Let

- *P*: The logical sentence: "the content can be decrypted". That has only one of the Boolean values '0' or '1'.
- *Q(x)*: Packet x would be captured. The value also is one of the Boolean values '0' or '1'.
- *R*: The content is known to unauthorized users.

We can give the expression for the transmission crack logical value in the first case as follows:

$$C=P \rightarrow \forall\, xQ(x) \rightarrow R$$

While the expression for the transmission crack logical value in the second case as follows:

$$C= \forall\, xQ(x) \rightarrow R$$

where:

$\forall$: denotes for all, and $\rightarrow$: denotes for the logical "imply".

E. Evaluation to the Multi-Paths Transmission

In private connections applications [10], for instance, users connected to a bank server have already data encryption in transmission, and their servers are protected and blocked physically by locked building and even guards. We need also an encryption connections using multi-paths transmission in such case [11].

As the security value depends on how many packets the unauthorized user can capture, we can transmit packets to many paths in order to avoid the packet capturing due to monitoring of unauthorized users [12], [13]. We can calculate the security value *S* according to the following formula, when the unauthorized user can decrypt some or all packets he captured from the monitored path:

$$S=m/(L/n) \quad (2)$$

where:

L: is the length of content in bytes.

m: is the number of packets the unauthorized user can't capture.

n: is the packet length, and *S*: is the security value.

Suppose a customer has a file which has 20000 bytes to transmit over the internet. The file is encapsulated into 200 packets. The customer forward 200 packets via 4 paths and each path has 50 packets to pass through. However, 2 paths are monitored by malicious users. We get the following security value by using (2):

Given = 2000; $m = 2 * 50 = 100$; $n = 20000/200 = 100$;
$S = 100/(2000/100) = 0.5$.

1) Security value for the multi-paths transmission

The following scenario is given to research on the packet encryption and multi-path transmission, which have both the real and most effects on the security value. In this scenario we are going to consider only the transmission resources. We are also going to calculate the security values in each situation and compare it with other situation in order to find what transmission resources is really affected by. The scenario we given here has a content of 20000 bytes and want transmit such content to the destination using the plaintext and encryption technologies. We also give 6 solutions for each composition transmission policies. The following values for packet lengths and paths will be used:

- The packet length can be one of two different lengths: the smallest packet length is 64 bytes, and the largest packet length is 1400 bytes.
- Paths: We use both 2 paths and 6 paths to transmit the content of the packet to its final destination in order to avoid paths monitoring and then packet capturing.
- Capture packets: As a consequence of path monitored by unauthorized users, packets could be captured.

The following Table shows the transmission solutions for different packets lengths and different paths used:

TABLE III: TRANSMISSION SOLUTIONS FOR PACKET LENGTH AND PATHS USED.

Solution number	Packets length	Used Path	Monitored paths(captured packet)
1	64	2	1
2	64	6	1
3	64	6	2
4	1400	2	1
5	1400	6	1
6	1400	6	2

With solution 1, 2 and 3 the content has: 20000/64 =313 (packets) , and with solution 4, 5 and 6 the content has only: 20000/1400 =15 (packets). In order to enhance the security in the transmission, multi-paths technology is used. Since one or more paths may be monitored as, some packets following these paths could be captured by unauthorized users. Suppose that all unauthorized users can decrypt the content in one or more packets according to the packets which are captured from the paths. If more packets are captured, the security value becomes smaller and if fewer packets are captured the security value will be higher. According to this policy, we get the total packets and captured packets results as shown in Table III.

TABLE IV: THE TOTAL PACKETS AND CAPTURED PACKETS

Solution number	Total packets	Captured packets (Less)	Captured packets (More)
1	313	156	157
2	313	52	53
3	313	102	103
4	15	7	8
5	15	2	3
6	15	4	6

Packets are evenly transmitted over different paths. For instance, with solution 1, 313 packets are divided into two paths before transmitted i.e. (313/2) = (156 and 157) small packet labeled as (less) and longer packet labeled as (more), respectively. Solution 2 has six paths (52, 52, 52, 52, 52, and 53), so that the malicious user could capture either 52 packets or 53 packets, labeled as 52 (less) and 53 (more). Solution 3

has two paths monitored so that the malicious user could capture 104 packets or 105 packets. In the same way, solution 4 has two paths with 7 packets or 8 packets which could be captured. Solution 5 has six paths with packets (2, 2, 2, 3, 3, and 3) and one path is monitored, the malicious user could capture 2 packets or 3 packets. And finally solution 6 has six paths with packets distribution (2, 2, 2, 3, 3, and 3) and two paths monitored; the malicious user could capture 4 or 6 packets. We are going to use the following formula for calculating the security values for different solution (scenario):

$$S=1-(\textit{captured packets}) / (\textit{total packets}) \quad (3)$$

For example, with solution 1, the security value will be:

$$=1-156/313$$
$$\approx 0.5016$$

With all solutions in Table IV, we achieved the following results of security values in Table V.

TABLE V: SECURITY VALUES WITH MULTIPATH TRANSMISSION

Solution No.#	Total packets	Captured packets (Less)	Captured packets (More)	Security value (Less)	Security value (More)	Difference
1	313	156	157	0.5016	0.4984	0.0032
2	313	52	53	0.8339	0.8307	0.0032
3	313	102	103	0.6741	0.6709	0.00317
4	15	7	8	0.5333	0.4667	0.0667
5	15	2	3	0.8667	0.8000	0.0667
6	15	4	6	0.7333	0.6000	0.1333

With results we getting from Table V, we can easily calculate security values for these solutions. The security values are shown in Fig. 2. Each solution (one of 6 solutions) has two security values. One is calculated depending on the situation that the unauthorized user captures fewer packets (Labeled as 'Less' in Fig. 2), while the other is depending on the situation that the unauthorized user captures more packets (Labeled as 'More' in Fig. 2).

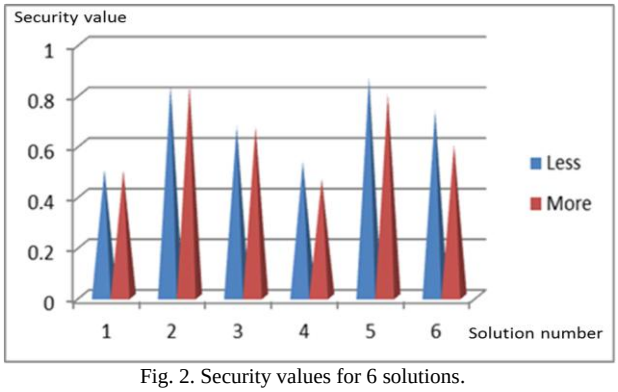

Fig. 2. Security values for 6 solutions.

With the result we get from Table V and Fig. 2 we can come to the following conclusion:

- When fewer paths are monitored, then as consequences fewer packet are may be captured by unauthorized user, the security value will be higher.
- When more paths are used in the multi-paths transmission, the system will be more secure and the security value will be higher.
- Compared with other security value, packet size has little effect on security value in such model. The 'less' and 'more' will give a view of influence difference on the packets length.

2) Security logic for the multi-paths transmission

The security logic is a method to know how such kind of system is secure [14]. The security logic value is, '0' or '1'. If the security logic is '0', that means the system is not secure. Otherwise, the system is secure. There are some conditions considered as not secure, we are going to define some rules in order to calculate the security logic value for those conditions.

Suppose the security value is: L, which can be an expression: $0 \le L \le 1$, then:

- $L=L1=0$; when the contents of the packet are using one path and each packet can be decrypted
- $L=L2=1-x/p$; when multi-paths transmission is used but some packets could be captured due to the monitoring of some paths

where p: is the number of packets in the multi-paths transmission, x denotes the number of packet in the paths the unauthorized user can monitor and then capture.

- $L=L3=1$; when *the* contents of the packet cannot be decrypted and multi-paths transmission is used.

Now let's consider the following assumptions as well:

$P1$ denotes the use of one path transmission.

$P2$ denotes the use of multi-path transmission.

By using the above security values and what kind of path transmission used, we can find out the security logic for each expression as listed in Table VI.

TABLE VI: CONDITIONS FOR SECURITY LOGICS

Security expression	Security description	Security Logic
L1	The decryption is done by capturing every encrypted packet, or plaintext, on the path.	0
L2	The decryption depending on the full content of all packets captured from different paths.	[1-X/P]; where X is number of packet captured, P is number of packets used in multi-path transmission.
L3	Packets can't be decrypted	1
P1	One path transmission is used	0
P2	Multi-paths transmission is used	1

When we consider the above situation and conditions, we can simply get the security logic for different combinations as shown in Table VII.

TABLE VII: THE SECURITY LOGIC BASED ON CONDITIONS

Conditions or scenarios	Security Expression	Paths used	Security logic
1	L1	P1	L1 ×P1= 0
2	L1	P2	L1 ×P2= 0
3	L2	P1	L2 ×P1=[(1-1/1)]×0.0= 0
4	L2	P2	L2 ×P2=([1-X/P]) ×1= { 1, when X □ P; 0, when X=P}
5	L3	P1	L3 ×P1= 0.0
6	L3	P2	L3 ×P2= 1.0

As we can see clearly from Table VII, the best policy is that the encryption algorithm cannot be known by anyone or

cannot be decrypted by unauthorized users. Otherwise, with the multi-paths transmission or other policies, we need to control the physical locations of the resources, such the locations of routers, links and switches. When we use the plaintext and simple encryption algorithm to transmit data, the security logic is not known to users.

IV. Conclusion

This paper proposes several methods to evaluate performances and protection technologies in order to enhance the security of transmission resources, computing resources and storage resources. The evaluation technologies include the evaluation of multi-paths transmission, the security logics, security levels and security combinations. With the evaluation of multi-paths transmission, the paper can address the issue of transmission security.

Acknowledgment

Alsharif Mohamed Y. Ahmed, thanks and deep gratitude to my advisor Prof. Dr. Qian Depei, he taught me to work hard is the way to succeed. He guided me and encouraged me to develop my skills as researcher.

References

[1] R. Anderson, "Cryptography and competition policy - issues with 'trusted computing'," *Advances in Information Security*, vol. 12, pp. 35-52, April, 2006.
[2] W. Stallings, *Cryptography and network security principles and practice*, 2nd ed., New Jersey: Prentice Hall, 1998.
[3] Theory and Practice of Model Risk Management. [Online]. Available: http://www.quarchome.org/ModelRisk.pdf
[4] J. P. Hughes, S. Plotkin, and F. Maino, "Standard architecture for encrypted shared storage media," *IEEE Project*, pp. 1619.
[5] R. C. Daley and P. G. Neumann. "A general-purpose file system for secondary storage," in *Proc. Fall Joint Computer Conference*, 1965, pp. 213-229.
[6] *Implementation of the federal information security management*, FY 2008, Report to Congress.
[7] *President forms national team to evaluate transportation safety, security*, ANTARA News Obtained January 20, 2007.
[8] *Datagram Transport Layer Security*, RFC 4347.
[9] T. Jordan, P. A. T. Hacktivism, and W. Cyber, *Rebels with a Cause*, U.K.: Routledge, 2004, pp. 133-134.
[10] *Sockets API Extensions for the Stream Control Transmission Protocol (SCTP)*, RFC 6458.
[11] L. Mark, *Comparing, designing, and deploying VPNs*, 1st ed., Ind.: Cisco Press, 2006, pp. 5-6.
[12] K. J. Connolly, *Law of Internet Security and Privacy*, U.S: Aspen Publishers, 2003, pp. 131.
[13] Sniffing Tutorial part 1, *Intercepting Network Traffic*, NETRESEC Network Security Blog, March 11, 2011.
[14] IEEE Grid 2007 Fine Grained Access Control Using Sec PAL. [Online]. Available: http://www.cs.virginia.edu/~humphrey/papers/GridFTP_SecPAL_2007.pdf.

Qian Depei was born in Shanghai, China, August 1952. He graduated from Xi'an Jiaotong University in 1977 computer professional, a master's degree from North Texas State University in the U.S. state of Texas in May 1984. June 1991 to 92 March as a senior visiting scholar of Computer Science, University of Hannover, Germany, the system structure and education work of the Institute of the operating system. Professor since 1992 was hired as a doctoral supervisor in 1996. Since 1996, deputy head of the current national "Eleventh Five-Year Plan 863 IT members of the Group in the field, 863 high-performance computer and grid service environment overall project group long, the Chinese Computer Society. Prof. Depei, DIRECTOR of the Sino-German Joint Software Institute at Beihang University (BUAA), He has been working on computer architecture and computer networks for many years.

Alsharif Mohamed Y. Ahmed was born in July 22 1970. He received the Bachelor's degree in Computer science & Engineering in Computer Security at "Engineering Academy Tajoura" Tripoli Libya since 1993. He was enrolled as a Master candidate in the School of Computer Science & Engineering "Computer Architecture & Networking" at Beihang University (BUAA) in March 1999, Beijing, China and Graduated in March, 2003. He is currently a PhD candidate at Beihang University (BUAA) since May 2008. His current research work focused on (Trust and Security Management in Distributed Systems).