Study of Enterprise Internal Control Based on Virtual Team and Cryptology Technique

[1]CHENGLIAN LIU, [2]SONIA C-I CHEN
[1]School of Computing, Neusoft Institute of Guangdong, Foshan 528225, CHINA
[2]School of Economics, Qingdao University, Qingdao 266061, CHINA

Abstract: The development in information technology, the widespread use of Internet and the fast movement of e-commerce has promoted the earlier realization of digital economy. Lots of enterprises use information technology inside the enterprise to reduce cost, shorten business deal time and achieve the largest production capability. Although digital technology brings convenience to people, crimes of information theft come after it too and the derived public security and financial issues are usually beyond our imagination. In this article, group signature technology is used to improve the operation of virtual team and to inspect the operation status within the enterprise; internet anonymous impeach function is provided through electronic internal control team mechanism so as to reinforce the mutual interaction rate between supervisor and employees, to enhance internal control efficiency within the organization and to enhance entire competitiveness.

Keywords: Group digital signature, Internal control, Virtual team, Electronic internal control team, Anonymous impeach.

Received: May 16, 2021. Revised: June 29, 2022. Accepted: July 25, 2022. Published: September 14, 2022.

1. Introduction

Technology product, no matter software or hardware, has now become the major competitive weapon for an enterprise to make strategies and create superiorities. Transaction time and cost can be greatly saved through the use of information and telecommunication technology and it is an unavoidable trend in such low profit time. However, under such trend, electronic transactions also brings new challenge and risk to this new era, for example, many illegal electronic transaction cases in recent years [1], [2] and the stock theft cases of Lee and Li Attorneys-at-Law [3]. Before the use of electronic transaction system, multiple steps have to be completed before a consumer can withdraw the money he/she needs. Moreover, the bank clerk has to confirm the identity and check to ensure that the identity of the consumer matches the check before the transaction can be completed; therefore, the entire process is very tedious and the cost is increased. Through the use of electronic medium, consumer only has to use ATM card and password to complete identity confirmation, money withdrawal and data registration within very short time and its accuracy and reliability is even higher than human processing [4]. However, when you enjoy the convenience, new risk must emerge. There is one special feature of transaction by using information and telecommunication technology, that is, electronic transaction can takes place at any places and such feature exposes electronic transaction under high risk. Only some digits need to be changed in the system and stranger out there thousands of kilometers away can vanish someone's savings which was accumulated by his/her entire life in very short time. What derived from the things we mentioned above is the internal control issues when dealing with electronic transaction procedures; the risk of electronic transaction not only comes from external environment, bad internal control is also an important factor. Enron scandal of USA occurred in the winter of 2001, however, on August one year before the occurrence of this scandal, vice president Sherron Watkin who was employed by Enron at Houston headquarter and was in charge of corporate development already discovered the illegal secret and reported and warned to upper management level and outer auditing company, Anderson, but not too much attention was paid to [5]. Therefore, it is very important how to, under known conditions, let internal control personnel to examine financial status of the company objectively and let the investors to get warnings from the financial report. The employee of Lee and Li Attorneys-at-Law, Mr. Wei-Chieh Liu (also call Eddie Liu), sells privately and illegally customer's custodial stocks for about three billions NT dollars brought an unprecedented risk to the company. This event reveals the internal control leak within an organization. A company must establish a good internal control system in order to let the company run stably and continuously. According to work place fraud

and infraction report made by Association of Certified Fraud Examiners in 2002, the result shows that the fraud in the work place could possibly happen no matter what the size is of an enterprise. In 2002, there is a loss of about 6% out of the corporate revenue, that is, about 60 millions US dollars, due to bad internal control. Of course, organization should have trust on its employee, but if the system does not have very effective operation of internal control, it could possibly lead to the motion and misconduct of fraud [6]. In this study, it proposes that a system such as electronic internal control team system can be installed in a company so that legal employees in the company can have a report and impeach mechanism to convey fast and fairly an impeach message to the top management level. In this study, digital signature mathematical model deduced previously is used to extend an electronic internal control system to provide a method of impeaching and auditing for the members of the organization; under this condition, the members of the organization do not have to worry anything, they will impeach any fraud occurred around them and do not have to worry about the exposure of their identity. In the second part of the literature survey, it includes the definition of internal control department, electronic internal control team and group digital signature in a company. In the third part, the electronic internal control team model is proposed and the application situation of each stage is set up. In the fourth part, discussion and analysis is made after the application and a complete model diagram is proposed. Conclusion and future study direction will be emphasized in the last part.

2. Literature Survey

2.1. Study on the corporate internal control department

Internal control system originated in 1949 from a research report of American Institute of Certified Public Accountants (AICPA) named “Internal control- It integrates the key elements of control and is very important to management level and independent accountant.” [5]; later on, many related reports and discussions gave recognition of different levels on the definition, purpose and structure of internal control. The current definition originates from a report of ”internal control-integration architecture”, generally called COSO Report, presented by a Committee of Sponsoring Organization of the Treadway Commission in 1992 (abbreviated as COSO) with members include AICPA (American Institute of Certified Public Accountants), American Accounting Association, The Institute of Internal Auditors, Institute of Management Accountants, Financial Management Personnel Association. COSO Report has now become the newest guidance of internal control system. COSO Report thinks that internal control is a process and this process is designed for three major purposes such as: to achieve the reliability of financial report reasonably, to follow laws and regulations, to operate the business effectively and efficiently; moreover, this process is affected by is affected by the Board of Directors, management personnel and other personnel of the company. For the definition of internal control, there is an explanation in the article 7 (1998) of No. 33 of Audit Standard Annals announced by the Audit Standard Commission of Accounting Research and Development Foundation: “Internal control is a management process and is designed by management level personnel and approved by the Board of Directors (or equivalent decision-making unit) so as to ensure the achievement of the following goals reasonably.” [7]:

- Reliable financial report.
- Efficient and effective operation.
- The follow-up of related regulations and laws.

Internal control can usually be divided into internal accounting control and internal management control. The former is a control directly related to the accuracy and reliability of accounting record and financial report which emphasizes on the achievement of two goals of accurate accounting information and guarantee of property safety; the latter is a control to maintain operation efficiency and to check if the organization follow the regulations as specified, therefore, its main purpose it to enhance operation efficiency and to realize specified management policies.

Internal control can be divided into two parts, that is, structural internal control and operation internal control. The former is of planning and designing characteristic which includes the construction of organization system, responsibility division, management authorization, layered responsibility, setting of work standards, making of all kinds of management method and operation procedures; the latter is real work implementation such as: the use, incubation and management of the work personnel, the safety maintenance of property, the treatment of accounting affairs, the management and control of budget and the implementation, auditing, preparing and reporting of all kinds of business activities and operations. All the things mentioned above should be carefully watched in the work personnel’s usual daily work operation so as to achieve the final goal of internal control [8]–[13].

2.2. Study on the electronic internal control team system

The current trend is to use the computer equipment of enterprise resource planning project to assist the operation in every part of the enterprise. Among them, the planning and implementing right and responsibility and an objective auditing mechanism of internal control department is designed by information system. Furthermore, there is a derived need of electronic internal control team of low cost, low risk and of confidential-keeping capability. This design not only can achieve the corporate planning effect but also can keep the privacy of organization members.

Through the use of the architecture basis of virtual team in association with group digital signature, we can deduce management functions of electronic internal control team. The general definition of virtual team is a team formed because of common ideal, common goals or common interest [14]. Electronic internal control team is an independent operation team with members coming from employee of the company and the topmost manager can know the identity of the employee but other members of the organization cannot know the identity of members in the virtual team. Virtual team is built in the organization because of its confidential and fast report characteristic [14]. In this article, the auditing and examining function, confidential function due to network communication as well as fraud impeaching function of electronic internal control team system are investigated and used to design a special organization for internal control. The goals that an enterprise hopes to achieve during the application of such system are as in the followings:

Step 1. The internal personnel of the department impeaches in anonymous way so that the electronic internal control team cannot calculate its real identity. Additionally, if the member of the organization impeaches in anonymous and repeated way, the electronic internal control team can not judge how many documents are from the same impeacher through the content of the impeached document.

Step 2. After the reception of anonymous impeaching case by the electronic internal control team and if the inspection result is found to be mismatching the fact, the identity of the anonymous impeacher can be calculated through the approval of the topmost decision-maker and appropriate penalty can be given; however, the impeaching reception center still can not guess if the previous or subsequent documents of the anonymous document are coming from the same person who makes the false accusation.

Step 3. Although the topmost decision-maker in the organization can has the right to examine the identity of the anonymous impeacher, the decision-maker can not forge an identity of any member of the organization and perform anonymous impeaching and make false accusation on that personnel [15].

Step 4. When electronic internal control team is performing its job for monitoring and if the responsibility of correct transfer of cases is violated, the topmost decision-maker can track its real identity and give penalty to personnel who make false accusation.

For corporate organization, the members of the Board of Directors are the strategic core organization, since directors have many things to do; they thus apply the authorization mechanism in the personnel management and help them in monitoring the implementation status of the policies. The system mentioned in this article, in addition to helping the processing of daily things, can also avoid a decision made by medium level manager by exceeding his/her authorization scope so as to do illegal things. Moreover, if necessary, this system can help the topmost manager finding out bad guys who use this system to make false accusation which might lead to a management dilemma.

2.3. The development of group digital signature system

What group digital signature means is, any member within the organization, can issue paper to outside bearing the name of the organization and the receiver only knows that the document is a formal document of that organization but does not know which member of that organization make the paper. Based on the cryptography, we develop a group digital signature system which can be used in the internal management of the company to enhance the safety of E-Commerce dealing [16]–[18]. Earlier, Chaum and van Heyet proposed in 1992 [19] simple research methods and Chen and Pedersen improved them in 1995 [20]; in another aspect, Camenisch and Stadler [21] create fast signature mechanism targeting at large organization; Lee and Chang proposed a strategy based on Discrete Logarithm; Chen and Liu [22] combine the method of Lucas [23] and the assumption of factorization to prepare a signature mechanism faster than Camenisch and Stadler. In the concern of information system security, the major part of the application of group signature emphasizes on the generation process of password and how to control the password and how to protect the password and enhance management

efficiency during the operation of business. However, in real analysis and application, whether the system has been thought in every detail and be tested in every aspect seems far more important than the complexity of the writing of programs [24]. In the system construction aspect, a good password system should possess secrecy, identification, completeness, un-deniability [25] as well as un-predictability [26], [27]. Targeting on the defects of group digital signature [19], some scholars propose to use the simple calculation formula existed in IC smart card accompanied with the use of simple password easy for the user to memorize in order to generate identity confirmation which is difficult to be solved by others. In the corporate internal management, the use of digital signature system can help the evaluation of performance objectively and be used as an internal communication tool.

3. Our Research Methodology

This paper extends the concept of information security technology and management, specifically introducing cryptography and information security mechanisms into the COVID-19 monitoring system, combining the two cryptographic algorithms of ElGamal [28] and RSA [29] to meet the requirements of the digitalization process of electronic medical records. In the process of patients using the medical insurance card, the information center can set the identity of the person who knows or does not know (double blind mechanism). Based on this design concept, the medical staff passively know or does not know the patient's identity. In this paper, we propose a conditional anonymity scheme. In the process of submission, patients and the system center have registered and issued account numbers, and patients, hospitals, doctors and the health insurance bureau are anonymous. In the process of the system, the patient has no direct contact with the health insurance bureau, so the health insurance bureau can not know the real identity of the patient at the initial stage; the role of the health insurance bureau has the right to supervise and inspect the doctor's visit content and inquire about the hospital information; the hospital has the responsibility to report the business to the health insurance bureau; the doctor has to report the visit situation to the hospital. This scheme of the algorithm consists of eight phases: registering phase, account issuing phase, medical treatment phase, diagnosis phase, data verification phase, data update phase, data response and final result return phase.

Step 1. Employee opens an account and register to company's system center.
Step 2. The system center issues an accounts to employee who applied an ID previously.
Step 3. Employee uses his anonymous ID to complaint or report to virtual team.
Step 4. The virtual team forward and check the record by system center.
Step 5. The system center received the record from virtual team before returned the verification.
Step 6. The virtual team forward the record to board.
Step 7. The board decodes the record when he received the parameters from virtual team.

The detailed information flow is shown in Figure 1.
Notation and **Significant**:
p_i: denote a large prime of RSA.
q_i: denote a large prime of RSA.
n_i: denote a modulo number of RSA.
e_i: denote the public key of RSA.
d_i: denote the secret key of RSA.
p_1: denote an other prime number of ElGamal, it different with p_i.
g: is the primitive root of prime number p_1.
x_i: is a private key in ElGamal-like algorithm.
y_i: is a public key in ElGamal-like algorithm.
m_i: digitized message.
Employee: The usually refers to the grass-roots level staffs or users in the organization or company.
System Center: We usually means the organization's information system center. Here, we use abbreviation 'ISC' or 'system'.
Virtual Team: We denote the staff who works in middle level such as manager or equivalent position.
Board: A person who is director, supervisor, chairman or president in high level of organization or company.

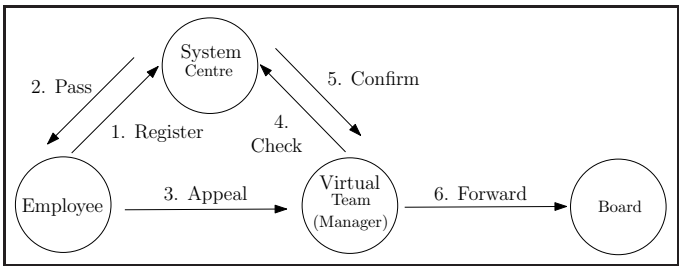

Figure 1. The concept of this system.

3.1. Initializing System Phase

3.1 In the system initialization phase, all users such as employee, system center, manager and board set their own account numbers and passwords, and share primitive parameters g and a large prime numbers p_1 through the system.
The employee randomly selects a number x_a, as its

private key and satisfies $\gcd(x_a, p-1)$, then calculates his public key

$$y_a \equiv g^{x_a} \pmod{p} \tag{1}$$

The system center randomly selects its own private key x_b to calculates its own public key y_b, and then announces

$$y_b \equiv g^{x_b} \pmod{p} \tag{2}$$

The virtual team (or manager) randomly selects its own private key x_c to calculates its own public key y_c, and publishes it

$$y_c \equiv g^{x_c} \pmod{p} \tag{3}$$

The board will randomly select its own private key x_d to calculate his public key y_d, and then publishes

$$y_d \equiv g^{x_d} \pmod{p}. \tag{4}$$

Please see Figure 2. Every employees randomly select

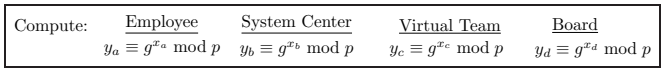

Figure 2. The System Initializing Phase.

two primes p_i and q_i to find:

$$n_i = p_i \cdot q_i, \tag{5}$$

since

$$\phi(n_i) = (p_i - 1) \cdot (q_i - 1). \tag{6}$$

Compute the public key e_i where it satisfied

$$\gcd(e_i, n_i) = 1 \tag{7}$$

and

$$e_i \cdot d_i \equiv 1 \pmod{n_i}. \tag{8}$$

The public key pairs are (e_i, n_i), although the secret key is d_i; we have destroyed some parameters such as (p_i, q_i and $\phi(n_i)$) based on security issue. From Equation (5) to (8), it is well-known RSA algorithm [29].

3.2.Registering Phase

3.2 The employee uses his ElGamal public key y_a and the RSA secret key d_a to calculate a temporary account by Equation (9).

$$S_a \equiv y_a^{d_a} \pmod{n_a}, \tag{9}$$

and register this account to system center, see Figure 3.

3.3. Getting Account Phase

3.3 When the system center receives S_a from employee, the system center approved and returned V_a since

$$V_a \equiv S_a^{e_a \cdot x_b} \pmod{n_a}, \tag{10}$$

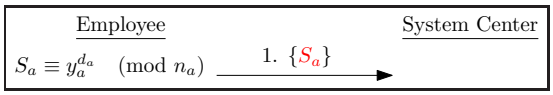

Figure 3. The Registration Phase.

see Figure 4.

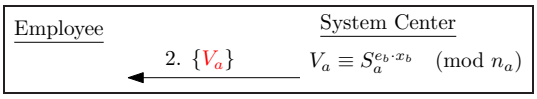

Figure 4. The Getting Account Phase.

3.4. Complaining Phase

3.4 The employee obtains a valid account and he then uses W_a and C_a before he complaint to virtual team. This operation has an anonymous feature:

$$W_a \equiv (V_a)^{d_a} \pmod{n_a}, \tag{11}$$

and

$$C_a \equiv y_d^{x_a} \cdot m_a \pmod{p}, \tag{12}$$

see Figure 5.

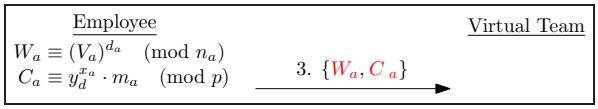

Figure 5. The Complaining Phase.

3.5. Checking Record Phase

3.5 When the doctor receives the patient's requirement, he will diagnose patient and sent the diagnostic record to system center for processing. The process is shown in Equation (13) and Figure 6.

$$F_a \equiv y_c^{W_a} \cdot W_a^{x_c} \cdot C_a \pmod{p}. \tag{13}$$

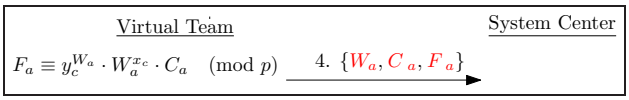

Figure 6. The Checking Record Phase.

3.6. Confirming Phase

3.6 The hospital received the diagnostics record by a doctor, he would check this identifier W_a firstly; if it is

hold, and then verified this message before returned to doctor. See Equation (14)-(15) and Figure 7.

$$W_a^{e_a} \stackrel{?}{\equiv} V_a \pmod{n_a}. \tag{14}$$

If holds, to calculate the Equation (15).

$$T_a \equiv (F_a)^{x_b} \cdot (W_a^{x_c})^{-x_b} \cdot C_a^{-x_b+1} \pmod{p}. \tag{15}$$

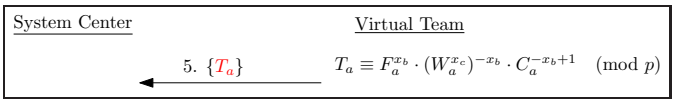

Figure 7. The Confirming Phase.

3.7. Reporting Business Phase

3.7 The system center has verified the effective identity of the informant. After the manager received the verification results, he signed or endorsed the verification results, and then submitted the results to the board of directors for processing. Please see Equation (16) and Figure 8.

$$Z_a \equiv (T_a)^{x_c^{-1}} \cdot C_a^{-x_c^{-1}+1} \bmod p. \tag{16}$$

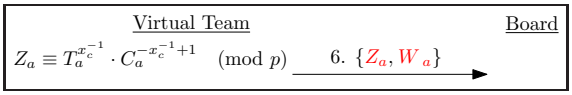

Figure 8. The Reporting Business Phase.

3.8. Board Processing Phase

3.8 The board of directors received the reporting $\{Z_a,\ W_a\}$ by manager. Since the content has been signed it digitally, if board of directors want to fetch the contents C_a. However, the content of the report is encrypted with the public key y_a of the board of directors and the private key x_a of the reporter (namely employee). Therefore, there are only two persons (employee and board) who can recovery (decode) the C_a into m_a after obtaining the ciphertext C_a, please see Equation (17).

$$C_a \equiv Z_a \cdot y_b^{-W_a} \pmod{p}. \tag{17}$$

Proof. As know from Equation (12), the C_a generated by employee, we can rewrite as

$$m_a \equiv y_a^x \cdot C_a \pmod{p}. \tag{18}$$

According to Fermat Little Theorem, we let

$$x = p - 1 - x_d, \tag{19}$$

namely

$$m'_a \equiv y_a^{p-1-x_d} \cdot y_d^{x_a} \cdot m_a \pmod{p} \tag{20}$$

□

From Equation (18) to (20), we finished the proof.

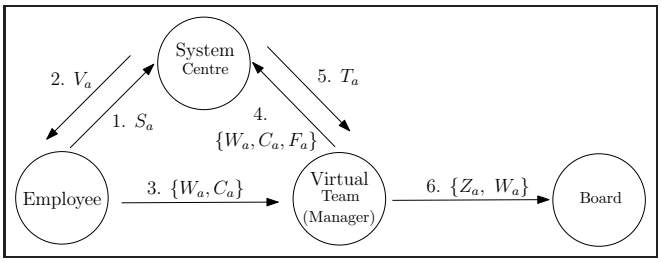

Figure 9. The protocol of this scheme.

3.9. The Experiment Example

We assume $p = 101, g = 18$ and the private keys as $x_a = 11, x_b = 49, x_c = 37, x_d = 71$ where public keys

$$\begin{aligned} y_a &= 59. \\ y_b &= 28. \\ y_c &= 86. \\ y_d &= 3. \end{aligned} \tag{21}$$

Suppose the RSA's parameters $p_a = 11, q_a = 13$, and $e_a = 19$, we find

$$\begin{aligned} n &= 143. \\ \phi(n) &= 120. \\ d_a &= 19. \end{aligned} \tag{22}$$

The result are

$$\begin{aligned} S_a &\equiv 58 \equiv 59^{19} \pmod{143}. \\ V_a &\equiv 124 \equiv 58^{19 \cdot 49} \pmod{143}. \\ W_a &\equiv 136 \equiv 124^{19} \pmod{143}. \end{aligned} \tag{23}$$

Let $m_a = 50$, responding to

$$\begin{aligned} C_a &\equiv 54 \equiv 3^{11} \cdot 50 \bmod 101. \\ F_a &\equiv 61 \equiv 86^{136} \cdot 136^{37} \cdot 54 \bmod 101. \\ 124 &\stackrel{?}{\equiv} 136^{19} \bmod 143. \\ T_a &\equiv 87 \equiv 61^{49} \cdot (136^{37})^{-49} \cdot 54^{-49+1} \bmod 101. \\ Z_a &\equiv 16 \equiv (87)^{37^{-1}} \cdot 54^{-37^{-1}+1} \bmod 101. \end{aligned} \tag{24}$$

According from Equation (18) and (19), we get

$$\begin{aligned} x &= 29 = 101 - 1 - 71. \\ m'_a &\equiv 50 \equiv 59^{29} \cdot 53 \pmod{101}. \end{aligned} \tag{25}$$

The authors gave an example of experiment flow from

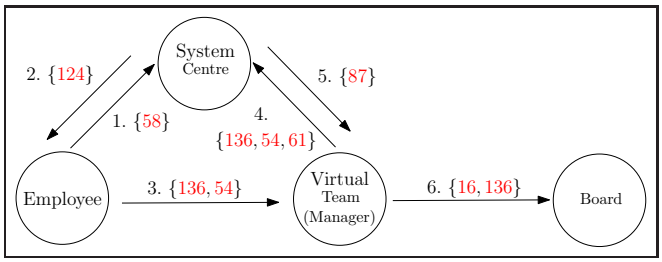

Figure 10. The Example of Experiment Flow.

Equation (21) to (25), and the diagram show in Figure 10.

4. Security Analysis

1312321

Definition 1. *Discrete Logarithm Problem (DLP)*
As known parameters $\{p,\ g,\ y_i\}$ *where the formula* $y_i \equiv g^{x_i} \pmod p$, *it is very hard to find the private key* x_i *while prime approaching infinite. Based on this assumption of computation and condition, it is called solving the discrete logarithm problem (Solving Discrete Logarithm Problem) [30]. The current public key cryptosystem based on discrete logarithm has value parameters that are greater than* 1024 *bit length or* 2048 *bit length.*

Definition 2. *Computation Diffie-Hellman Problem (CDHP)*
The Computation Diffie-Hellman Problem [31]is derived on the Diffie-Hellman key exchange principle (Diffie Hellman Key Exchange) [32]. The main ideas are described as follows: Given $\{g,\ g^x,\ g^y\}$ *to find* g^{xy}. *Here,* g *is known parameter, the* x *and* y *are unknown parameters.*

Definition 3. *Decisional Diffie-Hellman Problem (DDHP)*
The Decisional Diffie-Hellman Problem [33] is a variant of the Diffie-Hellman computation problem. Given $\{g,\ g^x,\ g^y,\ g^z\}$, *to find the* $\mathbb{Z}_p$ *is satisfied* $z = xy$. *Given* $\{g,\ g^x,\ g^y\}$, *to find* g^{xy}. *Here the parameter* g *is known, and the parameters* $\{x,\ y,\ z\}$ *are all unknown.*

4.1. Theoretical Security Level Analysis

Theoretical Security Level Analysis Analysis security of theoretical level

Lemma 1. *If user is honest, the Equation (14) would be correct, that is, the system center verified the employee.*

Proof. $W_a^{e_a} \stackrel{?}{\equiv} V_a \pmod{n_a}$.
As known from Equation (11), we get $W_a \equiv (V_a)^{d_a} \pmod{n_a}$ since Equation (14), according to RSA theorem; it becomes

$$\begin{aligned} W_a^{e_a} &\stackrel{?}{\equiv} (V_a^{d_a})^{e_a} \pmod{n_a}, \\ &\equiv V_a \pmod{n_a}. \end{aligned} \tag{26}$$

From above calculation, we connect the relationship between the Equation (11) and (14). The Equation (9) $S_a \equiv y_a^{d_a} \pmod{n_a}$ by employee, the Equation (10) $V_a \equiv S_a^{e_a \cdot x_b} \pmod{n_a}$ by system center. If employee is honest, the system center check Equation (27) holds.

$$\begin{aligned} V_a &\stackrel{?}{\equiv} y_a^{x_b} \pmod{n_a} \\ &\equiv (S_a)^{e_a \cdot x_b} \pmod{n_a} \\ &\equiv (y_a^{d_a})^{e_a \cdot x_b} \pmod{n_a} \\ &\equiv y_a^{x_b} \pmod{n_a}. \end{aligned} \tag{27}$$

Otherwise, it is a contradiction. □

Lemma 2. *If system center is honest, the Equation (10) holds, that is to say, the employee verified the system center.*

Proof. As known from Equation (10), the system center produced the V_a after employee transmitted his account S_a. We can rewrite the Equation (28) into

$$\begin{aligned} V_a &\stackrel{?}{\equiv} y_b^{x_a} \pmod p \\ &\equiv (g^{x_b})^{x_a} \pmod p \\ &\equiv (g^{x_a})^{x_b} \pmod p \\ &\equiv y_a^{x_b} \pmod p. \end{aligned} \tag{28}$$

Actually, from Step 1 to Step 2 (see Figure 1), the system center and employee both verified each other. It is stopped while one side failed. Otherwise, there is a contradiction. The Lemma 1 and 2 provide the evidences. □

Lemma 3. *If system center and manager are both interaction honestly, the Equation (13) and (15) holds, the system center and manager can verify each other.*

Proof. As known the Equation (14) and (21), the anonymous parameter W_a produced by employee and then via manager to system center. If manager is honest, the system center received the correct W_a; otherwise, he would got a wrong content. By Lemma (1) and (2), we prove employee and system center are honest. Hence, the system center can easily check the right or wrong of W_a based on the Step 1 to Step 3 without to check the F_a. This is to say, the manager honest to system center. On the other hand, the system center used his private key x_b to produce T_a after he received F_a by manager. If manager dishonest to system center who cannot produces

right T_a before received the F_a from manager. Although, the T_a was produce by system center, the manager can verify T_a such as Equation (29)

$$\begin{aligned} T_a &\stackrel{?}{\equiv} y_c^{w_a \cdot x_b} \cdot C_a \pmod p \\ &\equiv y_b^{w_a \cdot x_c} \cdot C_a \pmod p. \end{aligned} \tag{29}$$

As known $T_a \equiv (F_a)^{x_b} \cdot (W_a^{x_c})^{-x_b} \cdot C_a^{-x_b+1} \pmod p$ by Equation (15).

$$\begin{aligned} T_a &\equiv (F_a)^{x_b} \cdot (W_a^{x_c})^{-x_b} \cdot C_a^{-x_b+1} \\ &\equiv (y_c^{W_a} \cdot W_a^{x_c} \cdot C_a)^{x_b} \cdot (W_a^{x_c})^{-x_b} \cdot C_a^{-x_b+1} \\ &\equiv y_c^{W_a x_b} \cdot \cancel{W_a^{x_c x_b}} \cdot C_a^{x_b} \cdot \cancel{W_a^{-x_c x_b}} \cdot C_a^{-x_b+1} \\ &\equiv y_c^{W_a x_b} \cdot \cancel{C_a^{x_b}} \cdot \cancel{C_a^{-x_b}} \cdot C_a \\ &\equiv y_c^{w_a \cdot x_b} \cdot C_a \\ &\equiv y_b^{w_a \cdot x_c} \cdot C_a \pmod p. \end{aligned} \tag{30}$$

According from Equation (30), the (29) equal to (30), we finished the proof. □

4.2. Analysis of practical safety levels

Analysis security of practical levels

Doubts about cracking RSA and ElGamal cryptosystems: If the attacker intends to disguise the identity of the patient, the attacker must have the patient's key da to be able to calculate the corresponding pairing public key ea. In addition to being unable to disguise the patient, the attacker cannot disguise the system center, unless the attacker can crack the RSA cryptosystem. Obviously cracking the RSA cryptosystem is not realistic at the moment [34].

Key Compromise Impersonation attacks: The patient, system center, doctor and Health Bureau keep their own keys. Although their public keys are published, the hackers can not calculate the corresponding key through known public parameters. The discrete logarithm problem of the Definition 1 is defined and fully described. This study does not consider this assumption unless any party who owns the key divulges the key.

5. Conclusion

Under the fast development of E-commerce and the trend of technology leads the economic development, the past human resource internal audit is thus no longer an operation of black box. The network impeaching will become more transparent through the use of group signature system; therefore, the topmost decision-maker of the company can no longer affect the normal operation of the company intentionally due to private interest. Additionally, this can prevent the selective acceptance adopted by the audit or anti-corruption department because of their involvement in the case too. Moreover, this can also prevent the unnecessary conflict caused within the organization due to rank suppression.

This study proposes architecture for the setup of electronic team in the internal control department of a company so that the identities of employees, who are worrying about getting revenged when they impeach something and gets their identities exposed, will be protected. This architecture will encourage the members of the organization to impeach illegal things bravely and protect their identities. In the system of the current study, if necessary and under the agreement of the decision-maker of the organization, the identity of the original electronic impeacher can be tracked and this has threatening effect and can prevent any conflicts caused by persons who make false accusation. Moreover, the system can also perform monitoring and management on medium level managers and employees of the basic level, which is thought to be the greatest contribution of this study. However, the insufficient part of this study is the lack of consideration on humanity, which will be future direction of study.

References

[1] BBC News, "Taiwan ATMs 'robbed of $2.5m by European hackers'," http://www.bbc.com/news/worldasia36824507, July 18 2016.

[2] Ivana Kottasova, "Hackers steal millions from ATMs without using a card," http://money.cnn.com/2016/07/14/news/bankatmheisttaiwan, July 14 2016, CNN News.

[3] Y.-Y. Chiang and W. G. Rowe, "Lee and Li, Attorneys-at-law and the Embezzlement of NT$3 Billion by Eddie Liu (A)," College of Commerce, National Chengchi University and Ivey Management Services, Tech. Rep., January 16 2009, Case: 9B08M079.

[4] J. C. Tsui and J. J.-R. Chen, "A study of group signature implanted to network with impeachment system," in 2003 Proceedings of Electronic Commerce and Digital Life Conference, April 11-13 2003, pp. 1500–1510.

[5] K.-F. WU, "The study of the business for build internal control system and internal audit system cases representative in the far eastern group," Master Thesis, Department of Business Administration, College of Management, National Dong Hwa University, Taiwan, 2005.

[6] Taipei District Prosecutors Office, Taiwan, "Record of serious financial cases," https://www.tpc.moj.gov.tw/media/187386/%E5%8C%97%E6%AA%A2%E9%87%91%E8%9E%8D%E9%87%8D%E6%A1%88%E5%AF%A6%E9%8C%84-010-a-law-firms-3-billion-dollar-lesson.pdf, June 22 2021, a law firm's 3-billion-dollar lesson.

[7] Yiyun Wang, Principles and methods of internal control, 1st ed. Wu-Nan Culture Enterprise, Taipei, Taiwan, October 2009, Chinese edition.

[8] S.-I. Chang, L.-M. Chang, and J.-C. Liao, "Risk factors of enterprise internal control under the internet of things governance: A qualitative research approach," Information and Management, vol. 57, no. 6, p. 103335, 2020.

[Online]. Available: https://www.sciencedirect.com/science/article/pii/S037872062030272X
[9] X. Chen and H. Nie, "Research on the internal control of small and medium manufacturing enterprises under comprehensive risk management," in Proceedings of the 8th International Conference on Innovation and Management, 2012, pp. 680–684.
[10] J. Feng, "Research on enterprise internal control based on accounting computerization," in Proceedings of the 2016 International Conference on Education, Sports, Arts and Management Engineering. Atlantis Press, 03 2016, pp. 356–360. [Online]. Available: https://doi.org/10.2991/icesame-16.2016.75
[11] F. GAO, "A study of the internal controls of accounting information systems in the network environment," International Journal of Simulation Systems, Science and Technology, vol. 17, no. 18, pp. 91–95, 2016.
[12] C. Qin, "Literature review and prospect of enterprise internal control," American Journal of Industrial and Business Management, vol. 8, pp. 2120–2132, 2018.
[13] E. M. Akhmetshin, V. L. Vasilev, D. S. Mironov, E. I. Zatsarinnaya, M. V. Romanova, and A. V. Yumashev, "Internal control system in enterprise management: Analysis and interaction matrices," European Research Studies Journal, vol. 21, no. 2, pp. 728–740, 2018.
[14] S. Stough, S. Eom, and J. Buckenmyer, "Virtual teaming: a strategy for moving your organization into the new millennium," Industrial Management and Data Systems, vol. 100, no. 8, pp. 370–378, 2000.
[15] N. Barić and B. Pfitzmann, "Collision-free accumulators and fail-stop signature schemes without trees," in Advances in Cryptology–EUROCRYPT '97, W. Fumy, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 1997, pp. 480–494.
[16] W. Diffie and M. Hellman, "New directions in cryptography," IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644–654, 1976.
[17] L. Lamport, "Constructing digital signatures from a one way function," Tech. Rep. CSL-98, October 1979, this paper was published by IEEE in the Proceedings of HICSS-43 in January, 2010. [Online]. Available: https://www.microsoft.com/en-us/research/publication/constructing-digital-signatures-one-way-function/
[18] K. Tu, "Comment: Public-key cryptosystem design based on factoring and discrete logarithms," vol. 143, no. 1, p. 96, January 1996.
[19] D. Chaum and E. van Heyst, "Group signatures," in Advances in Cryptology–EUROCRYPT '91, D. W. Davies, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 1991, pp. 257–265.
[20] L. Chen and T. P. Pedersen, "New group signature schemes," in Advances in Cryptology–EUROCRYPT'94, A. De Santis, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 1995, pp. 171–181.
[21] J. Camenisch and M. Stadler, "Efficient group signature schemes for large groups," in Advances in Cryptology-CRYPTO '97, B. S. Kaliski, Ed., 1997, pp. 410–424.
[22] Jonathan Jen-Rong Chen and Y. Liu, "A traceable group signature scheme," Mathematical and Computer Modelling, vol. 31, no. 2, pp. 147–160, 2000. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0895717799002290
[23] D. Bleichenbacher, W. Bosma, and A. K. Lenstra, "Some remarks on lucas-based cryptosystems," in Advances in Cryptology–CRYPT0' 95, D. Coppersmith, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 1995, pp. 386–396.
[24] U. Feige, A. Fiat, and A. Shamir, "Zero-knowledge proofs of identity," Journal of Cryptology, vol. 1, no. 2, pp. 77–94, Jun 1988. [Online]. Available: https://doi.org/10.1007/BF02351717
[25] D. Chaum, E. van Heijst, and B. Pfitzmann, "Cryptographically strong undeniable signatures, unconditionally secure for the signer," in Advances in Cryptology–CRYPTO '91, J. Feigenbaum, Ed., 1992, pp. 470–484.
[26] D. Chaum, J.-H. Evertse, and J. van de Graaf, "An improved protocol for demonstrating possession of discrete logarithms and some generalizations," in Advances in Cryptology–EUROCRYPT' 87, D. Chaum and W. L. Price, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 1988, pp. 127–141.
[27] S. Goldwasser, S. Micali, and R. L. Rivest, "A digital signature scheme secure against adaptive chosen message attack," D. S. Johnson, T. Nishizeki, A. Nozaki, and H. S. Wilf, Eds.
[28] T. ElGAMAL, "A public key cryptosystem and a signature scheme based on discrete logarithms," IEEE Transactions on Information Theory, vol. 31, no. 4, pp. 469–472, 1985.
[29] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Communications of the ACM, vol. 21, no. 2, pp. 120–126, Feb. 1978.
[30] Wikipedia, "Discrete logarithm," https://en.wikipedia.org/wiki/Discrete_logarithm.
[31] ——, "Computational Diffie-Hellman assumption," https://en.wikipedia.org/wiki/Computational_Diffie-Hellman_assumption.
[32] ——, "Diffie-Hellman key exchange," https://en.wikipedia.org/wiki/Diffie_Hellman_key_exchange.
[33] ——, "Decisional Diffie-Hellman assumption," https://en.wikipedia.org/wiki/Decisional_Diffie-Hellman_assumption.
[34] ——, "RSA factoring challenge," https://en.wikipedia.org/wiki/RSA_Factoring_Challenge.