A Secure Cloud Trading System with Third-Party Payments

Sue-Chen Hsueh, Shao-Tsong Lan*
Department of Information Management, Chaoyang University of Technology,
168, Jiefeng E. Rd., Wufeng District, Taichung, 41349 Taiwan, R.O.C.
*Corresponding Author: s10114622@cyut.edu.tw

ABSTRACT
Third party payment has been advocated and proliferated for e-commerce in recent years. The mechanism is especially important for both international trade and an honest exchange of a purchase. Various platforms such as PayPal and Alipay thus exist for the purpose. As more transactions are conducted in mobile commerce and the growing popularity of trading systems in cloud computing environments, confidential information might be disclosed by improper aggregations of trading data in a cloud-transaction platform. Therefore, a third-party payment mechanism that integrates multiple transaction parties, provides maximum convenience, and affords privacy protections under cloud computing environments is highly demanded. In this paper, we present a third-party trading mechanism under a cloud computing environment. The system uses independently-operated components to protect the complete information of a user from being compromised via partial data aggregations. The risk of repeated disclosure of information can also be reduced since registrations in various payment platforms are minimized in our cloud trading-system.

Keyword: E-commerce, Third-Party Payments, Information disclosure, Information security, Cloud service

1. Introduction
In the internet generation of vigorous development, people who use network engaged in e-commerce behavior increasing, including Business to Business (B2B), Business to Customer (B2C) and Customer to Customer (C2C). In addition to e-commerce activities involving trading services, automated processing of upstream and downstream business operations and workflow, solving customer problems through common experience and technology, but also social services among individuals and groups, recreational activities, information sharing, etc. Connected device to the Internet engaged in e-commerce also from desktop, ATM(Automated Teller Machine), evolved mobile devices such as mobile phones, tablets can use e-commerce services and application, the commerce we call m-commerce(Mobile Commerce) (S. Britto R. Kumar, S. Albert Rabara and J. Ronald Martin, 2009). In e-commerce people through mobile device immediately use in previous due to location of fixed equipment or
completed in time-bound restriction in the Internet environment, significantly enhance the user's convenience.

Although the nature of commerce unchanging, not only break the constraints of time and place can be more flexible so that users can use, but also change the commerce model and application to extend new commerce, such people will use mobile device to “check-in” or “thumb up”, in order to record life went, and businessman use the feature attract user through Facebook place display the store location, then the information about store will be known, thereby establish reputation. Another mobile commerce also emphasized personal usage scenario, user through mobile device obtain a friendly interface in commerce activities, in addition avoid information been stolen or tampered when using traditional computer sharing data, also increase account security by binding mobile device, these activities can demonstrate properties through holding mobile devices and using networks.

In the past, entrepreneurs attach great importance to trade secrets, for products or services such as materials, process, method of operation are not open to the public, in order to prevent confidential information been external attack or non-related person to steal, so use firewall or LAN topology formed quarantine (Demilitarized Zones, DMZ), the quarantine via firewall between the internal or external network must use network address conversion (Network Address Translation, NAT), enterprise information systems are also used by independent developers or ready-made, if enterprise want to perform maintenance or updates are quite difficult, coupled with the development of the internet is not mature, the cost of infrastructure is also quite expensive, enterprise cannot through internet quickly conduct business activities with upstream and downstream manufacturers, let while enterprise business system presents “Information Silo” status (Eric Yuan and Jin Tong, 2005). In pace with increasing age of advanced technology, cloud environment needs technical and cost gradually reduce, cloud service provider through infrastructure provide modular services, enterprise starting put the business activities on “cloud”, in order to reduce the enterprise internal aspects of the information technology related expenses (Takabi, H. and James BD Joshi, 2012), for example, the development of software and hardware equipment, maintenance and updating, retention and hiring of personnel training, business processes, such as modular and so on.

When business activities have appeared transactions, the buyer in order to obtain goods or services will give businesses as a reward through the payment methods, if there is no credible proof of the unit responsible for the supervision and then payment will be limited the specific process provided by the merchant, the buyer may not be able to track the flow of the amount of the transaction, there is no way the quality of the goods protected by the proposed test, even the risk of not receive the goods. there
is no way for merchants to receive goods security payments in the future needs to check if the transaction details and verify the identity of the buyer. Banks among financial services companies are also required in response to the needs of individual businesses to pay huge management and maintenance costs (Takabi, H. and James BD Joshi, 2012).

Therefore, when the conducting transactions between service providers and users, usually through a “Third-Party Payment” to witness the successful completion of the transaction. The Third-Party Payment can protect complete the transaction before the action will not have remittance, also protect providers to the exact amount received after the completion of the transaction, if the transaction is not completed that will no case of damage to the interests of both right. In the famous third-party payment website such as PayPal, Alipay, Google Wallet, they have own payment system operate independent. In the advanced e-commerce period, when user through internet carried out the business activities, need to apply for a third-party payment systems operate independently of each website, than will cause user’s personal information stored in a separate data of different websites database, these websites must create a considerable degree of database security mechanisms to protect, prevent misuse of user data or user operation been hacked or tamped. For login and transaction processing part also need to be carefully designed to increase the time for any action or transaction account aspects related to the application requesting its complexity to prevent illegal users or by malicious software attacks. On the part of the bank client's financial operators in addition to considering how to increase the security of personal account information, while also take into account the cash flow of the processing speed (Sean Marston et al., 2011). If same user respectively login to different business website proposed action in same time, bank client need to verify the legitimacy of the site and reviewing the user's identity is correct, these will make banks handle increased business content, also cause inconvenience when access different website to re-enter personal information for user, reduce the use of e-commerce will.

Furthermore the way to connect mobile commerce due evolved from wired wireless on-line, about wireless network needs to be transmitted over a higher degree of safety channel (S. Britto R. Kumar, S. Albert Rabara and J. Ronald Martin, 2009), coupled with the current number of people using mobile commerce have increased, but most users are still limited to small business activities in locate consumption such as convenience stores payment(i-cash), traffic tickets, tickets, trafficking machine localization services, etc., if someone want to consume in large payments or distance will be used to more personal information such as credit card number, ID number, e-mail or contact address, these goods or services in a transaction will need to provide to businesses or a trusted third party to verify the unit, in the amount of information
provided, the more the case, the more it can ensure the normal completion of the transaction process, but also to verify the transaction object and the content is correct and legal. However, it also makes the user of doubt, the following problems faced by third-party payment:

1. Occult of third-party payment account
User conducted business behavior through a registered third-party payment identify account and bank account. If the third-party payment platform obtains some user’s sensitive information such as ID card number or bank card number in the process of transfer of funds, there may be internal staff or hackers to steal or cause user accounts to be the surrogate account. In addition, the currently registered third-party platforms way are mostly use e-mail or through mobile phone, user’s identity are still be virtual, so it is difficult to track the user’s identity.

2. Security of transfer account
There maybe have a risk form user to third-party payment custody account and the flow of funds from third-party payment to target account, for example, the flow suffer Man-in-the-middle Attack resulting funds transferred to the incorrect account or amounts being tampered. Due to different national legislation, there also have a risk when custody or defray the funds, that will may become some illegal group migration or cash tool.

3. Problem of temporary funds
Temporary user’s funds will begin from the third-party payment account, waiting store confirm payment, shipment until user receipt goods or service, user’s founds will transfer to the store’s target account. The process of the funds migrating be stranded for two days to a few weeks, the founds may be different from the original price because of some international situation let some cross-border transactions currency float.

4. Intense competition within the industry
In addition to PayPal and Alipay, there are many different circumstances of third-party payment platform currently on the market, but the main features are similar. For example, user need to transfer of funds or use other third-party payment services through Alipay, but the user only have a PayPal account, in this case user can’t use the services in Alipay. If user needs to use Alipay services, that user must to register a Alipay account. For the user, it increase complexity of the operation, but also exist the risk of leakage sensitive personal information, for third-party payment provider, this movement resulting loss of customers, reducing the profits of enterprises to obtain.

5. Issue of virtual currency
There are many business or entertainment sites unify the internal circulation of funds through the issuance of virtual currency in network services. The main source of
currency is divided into two categories, gaming manufacturers issued a medal and tokens issued by other service providers. In order to occurrence of money laundering or smuggling case, they review the flow of the legal amount entity and records transactions through tax in some countries. For example, China State Administration of Taxation (SAT) announcement:” Individuals income of trading virtual currency through the network made levy personal income tax.”, thus while the proposed property transfer of property, implementation ”virtual currency transaction tax” at the same time, the SAT will levy 20% personal income tax from sale of virtual currency revenues. Although SAT avoid money laundering, smuggling and auditing by law to regulate, but the virtual currency usually not limited to one area, there is still a way through transnational above happens, than will steal account and password, tampering virtual account, risk of virtual currency stolen or other illegal conduct through network.

Therefore, this paper use cloud technology proposes a third-party payment platform environment integrate user’s personal information, third-party payment systems and bank account to reduce user duplication grant the user sensitive personal information to other third-party payment platform, reducing the risk of leakage personal information, with cloud technology let businesses and individual user quickly and convenient operation completed business processes, improve user experience.

Through the hidden part way let between businesses and banks can only obtain the necessary information to protect the user’s sensitive information (Divyan Munirathnam Konidala et al., 2012), such as credit card numbers, purchase lists, and so on.

2. Related work

2.1 Cloud Environment

National Institute of Standards and Technology (NIST) defined the Cloud computing technology of 3 kind of modes, 4 deployment models, 3 service models and 5 essential features. As illustration 1:
2.1.1 Deployment Models

(1) Public Cloud
It is provided to general public and big enterprise groups of public cloud infrastructure, and owned by a selling cloud service of organization. It according to the using volume of resource to charge, user usually can use it free or by lower prices to use the open services. However, it will be limited of the save and load authority of some services. So that to prevent an illegal thirty party to data theft or tampering.

(2) Private Cloud
The difference between private cloud and the public cloud is it works for the only one organization or department, the programs and data are just flown and managed inside the organization, basically preventing over opened as public cloud. Though same as the public cloud has the advantages of flexible, and suitable for providing services, private cloud can make user won’t be limited by interviewing authority, law restriction influences. And have more authority to control the cloud infrastructure, use simple management to reduce risks.

(3) Community Cloud
Those organizations of same goal united the cloud infrastructure so to support some specific community. For example: the medical cloud, the educational cloud…etc. All these resources and equipment may located internal the organization or authorized to the third party to provide the assistance, and make users focus on the areas they need.

(4) Hybrid Cloud
An organization can adopt two or more different of cloud infrastructures. Though it’s isolated between these clouds, they can connect to each other via the same standard protocol or technology and increase the organization’s flexibility against to different demands. And make the data and the programs are interoperability and portability, so...
to grasp immediately the key services and data flows in the organization.

2.1.2 Service Models

(1) Infrastructure as a Service (IaaS)
Cloud Serves Provider (CSP) provides a completely outsourcing service of information equipment or resource, which provides the computing, storage spaces, internet frame-works…etc. All these infrastructures of resources are usually a dummy platform environment. The users don’t have to build up an expensive hardware facilities, just through renting to use these equipment and adjust the services contents as their demands. It provides the users the most flexibility and reduces the environment establishment of threshold.

(2) Platform as a service (PaaS)
A kind of an information development persons providing platform, the user through the Application Programming Interface (API) up load his writing program code on the platform provided by the could service provider to process the computing, storage, management, test and maintenance…etc. of service. During the whole constructing and developing program of life-period, the user only have to pay the resource used and don’t have to consider the environment development, management and upgrade. The daily system maintenance is all handled by the cloud service provider.

(3) Software as a Service (SaaS)
Sending data to the data center, process the storage or computing and make the payment according to the usage volume. By the dummy technology realized the multi-renters concept, let multiple users use on the same platform at the same time, and rapidly contribute resources or submit the services, hide the complex packet processing and reduce the user’s conduct burdens and low down the user relied on the Information Technology (IT) of professional knowledge.

2.1.3 Essential Characteristics

(1) Broad Network Access
Based on the rapid-changing of the hardware equipment and the network bandwidth, the user can operate many kind of equipment, for example the PC, smart phone, PAD and even the appliance which with the function of connect to the internet, so that to link to the internet and use every kind of the services provided by the cloud service providers.

(2) Rapid Elasticity
The cloud service providers can process the computing or storage according to the users’ demands any time. Its structure is really flexibility and scalability, and then charge according to the resources energy consumed and the hours used.

(3) Measured Service
Since the service is invisible, the cloud service providers will use the measurable data,
like the storage spaces, computing hours, network traffic volume…etc. to provide clear data flows units of report for users’ review, and through self-monitor of manner to ensure the optimal of resources applied.

(4) On-Demand Self-Service
The user can request the computing resources or the storage spaces from the cloud service providers according to his demands all the resources will be automatically allocated and, during the process, doesn’t need any purchasing, building, set-up, up-grade…etc. of preparing time costs, only use the network interaction surface and complete by himself.

(5) Resource Pooling
The cloud environment as to the users can be compared to a pool, which includes cloud service providers’ supplied computing resources, storage spaces, network frequency range…etc. infrastructure. By the dummy technology, it can allocate the resources to multiple users any time, and the users don’t need to know the real location of the resources and just use the service.

Since the cloud environment of resources all use the dummy technology to process the sharing resource of concepts, letting users to get the service more convenient is occurs by every kind of cloud services, hereby the required computing or storage resources are increased as well. Therefore in the cloud environment except consuming new real equipment, integrating computing environment inside the organization will require the most efficient and easy to management of methods to be the solution.

Google’s software of Google calendar, Gmail…etc. which are established in the cloud environment, so that to make the users can use the multiple services through internet any time anywhere. As per the Google Docs, it even makes multi-users to audit the same document in the same platform via the collaboration method, besides, Google also provides the development environment, such as the Google App. Engine, that makes the user can conduct the development or the test of services. In such convenient environment, relative to provide computing and storage resources are very impressive.

2.2 Mobile Commerce (M-Commerce)
In the rapid development of technology, engaged in electronic commerce is no longer confined to the fixed equipment such as desktop computer or ATM, the phone is not only call or send message, but also provide mobile related services in anywhere through linked to the network device, increase the perceived commerce environment, personal usage scenarios, real-time and convenience. In this paper, we can use the general fixed equipment and mobile device to login the system through proposed framework, currently the most popular mobile commerce applications issue is Near Field Communication (NFC), so we will introduce NFC in the following.
2.2 Near Field Communication (NFC)
NFC is a contactless communication technology by Philips joint Nokia, Sony and other manufacturers to promote wireless technology, using Radio Frequency IDentification (RFID) frequency band and Internet combined contactless card and reader into a chip for equipment identification and information exchange in close environment. The previous purpose is integrate RFID and network technology, now has developed a wireless communication standard, this function can be performed contactless peer to peer information transmission range of 4 centimeters through electronic devices, the frequency is 13.56MHz, and the transmission rate divided into 106-bit, 212-bit, 424-bit three kinds per second, the level of applications are extensive such as micro payment, access control system, Location-Based Service (LBS). The following are three kinds of NFC application mode introduced:

2.1.1 Card mode
Through simulate card way to make NFC device in a passive state, when the card close to reader can read the information, currently available to integrate a large number of IC card, travel card, tickets and so on. The card mode can be used also when the device is turned off. (Ugo Biader Ceipidor et al., 2012)

2.1.2 Peer to Peer mode
The two NFC-enabled devices use wirelessly liked manner like infrared connect together, use the faster transmission speed for data exchange or service in a close range, there is a significant effect for transmission of large amounts virtual files such as music, e-books.

2.1.3 RFID tag read/write mode
The NFC device can use as a reader, when the device near the card or tag and scanned to read the relevant information, for example, user through the smart phone scan the QR code than obtain the information.

2.3 Third-party payment
In the traditional trading platform, the buyer and the seller can negotiate a method with each other to confirm the payment or the receipt conditions and then process the delivery or the payment. The relationship must be built by mutual trust of situation. For the goods’ quality or the money source are not absolutely guaranteed and the users’ equity might be damages. In the meanwhile, what the former e-commerce used to trading is via credit card, debit card or the other signature payment tools. During the payment process both the buyer’s and the seller’s personal information, bank details, products information…etc. will be recorded by the none-relative parties. What if combine these information, the users’ sensitive information could be disclosed and caused to the security problems. In order to prevent this kind of problem, the third party payment of concept is created, through the process, the user usually deposit the
money to the third party after purchasing the goods or services, and approve the payment. After the seller/vendor confirmed, they will deliver the goods. Until the user received the goods, then the money will be assigned to the seller. In such transaction process, through monitoring the money flows by a trustable third party, it can secure both buyer and seller’s equity, and trade safely via the lowest data volume and protect users’ personal information. The following is the comparing of business contents and security between the biggest third payment party, the PayPal, and the most Chinese used, the Alipay.

3.1 PayPal
PayPal was an international trading payment platform merged by eBay in 2002. The active members so far is reach to one hundred thirty two million people, supporting more than 190 areas, and the currency is more than 20 kinds till 2012. Its main agent-based business is the payment, users only need an e-mail box to registered and then can process the money transaction. In the age of the smart phone and internet infrastructure so populated, PayPal also connect to the mobile payment function and make users conduct the payment by mobile phone through the application (APP) or the near field communication (NFC)…etc. related technologies. During registering at PayPal, account will be set-up by differently categories. Since the handlings and the transaction value and the members’ numbers are different, through these different account categories and reduce the risks of cash flow, improve the management of authority. In keeping with industry standards set by the Certification Authority/Browser (CA/B) Forum, PayPal will discontinue supporting 1024-bit key length certificates and will migrate to 2048-bit certificates before the end of 2013.

3.2 Alipay
The Alipay was established by Alibaba Group and as the most populate third payment platform in China, whose member is up to 8 hundred million. Till 2012, it accept over 25 kinds of currencies to pay. It agent-based business not only the payment function, but also the function of Tokens refill, payment of water, electric, coal and telecom of faire…etc. now it also open register to none Chinese users. Now it use the 2048-bits of SSL encryption on the payment. It registered of method is by the e-mail box and the mobile phone, as per the password is using the login and process of payment, so that to increase the safety of the payment process. As per the mobile payment part, now Alipay present one kind of sonic to conduct the data transmission via mobile phone and the receiver to conduct the NFC technology.

3.3 Google Wallet
The Google user can via a connect internet device to pay in web store, the main way usually through the mobile such as mobile phone and PAD, then the store can acceptable forms has credit cards, coupons and gifts… etc., the store also can use the
promotional activities to increase consumption at the same time, moreover the Google Wallet currently only supports specific U.S. network operator such as Virgin Mobile, Spring, US Cellular, this is why Google Wallet penetration is not universal. But the Google Wallet is security for mobile payment, there have three level protection mechanisms: ID and password, automatic turn off antenna, the Android NFC function code, the other way, Google do not allow the use of the password is entered again, regularly updated password, thereby reducing the risk of password theft, even the mobile device have been theft, the user can close the mobile payment function on Online Management Center, only leaving the online payment function.

3. Research Methods

In this paper, we propose a cloud trading system allows user can unified manage device, bank account, payment behavior and transaction details connected the network between store and bank. Cloud trading system component use minimal amount of information to reduce the risk of user’s sensitive information been leaked though the provision of part information to allow independent operation, the process when data transfer in each cloud trading system coupled the external and internal public key to increase security on transport, reduce possible when user information be revealed in a combined manner.

In this chapter, first we will introduce the cloud trading system architecture, shown in Figure 1, and descript each entity. Explain the flowchart for user though computer or own mobile device connect to the cloud trading system in certified environment, how user remit funds to target account through the part of information. We can see three steps in figure 2: login, register, remittances, required related symbols shown in table 1.

![Figure 1: Cloud Trading System Architecture](image-url)
When user log in to the cloud trading platform, user can stored their personal information and connected devices in database, depending on the needs of user beginning remit or receive, transferred the amount to another bank account.

3.1.2 Cloud Trading System
The main function for user is personal information and registered device management, request of remit, receives and transaction details, the cloud trading system component following described in detail:

(1) Service Interface: When user request service, user will connected internal cloud trading system interface conduct operation, avoid user direct access to the relevant information or external malicious attacks.

(2) Registration: Check and storage user’s personal information, bank account, device for duplicate registration and record new user.

(3) Certificate Authority: Before using cloud trading system services, user must verify the identity of the certificate authority, if the service needs higher level of security, certificate authority ask user conduct two-step security authentication to reduce cloud trading system load.

(4) Remittance: User can divide remittance and beneficiary, cloud trading system obtained the difference identities information by verifying the correctness of identity and then inform bank for remit to target account, via the transaction details to confirm the action is completed.

3.1.3 Bank
After trading platform cloud confirm user information, put the transaction information to the bank and then create a transaction detail return to cloud trading platform.

Figure 2: Cloud Trading System Flowchart

3.2 Flow
According to the needs of users, there have unregistered and registered two cases, in the case of unregistered the cloud trading platform will guide user into registration process, when the registration process have been complete, user can use remittance function, as shown in figure 2. The following is a description of the process:

3.2.1 Sign up
1a. login: User provides personal information for registration request to the service interface.
1b. register: Registration received information from the service interface, if the user information is not repeated then successfully registered.
1c. insert: Registered user information will be written to the database.

3.2.2 Remittance
2a. request AccBnf: After confirming the transfer target, user will request the beneficiary bank account.
2b. receive: Beneficiary gives the bank account to user and then submits the receive service for the service interface.
2c. auth.: When the service interface receives the user and the beneficiary’s request, both of the information will be sent to certificate authority for authentication.
2d. send information: Confirm the identity of user and beneficiary are correctly, service interface will send the transfer information to the remittance.
2e. remit: Remittance check the relevant information and then bank will complete the transaction.

<table>
<thead>
<tr>
<th>EU</th>
<th>User login information</th>
<th>Auth</th>
<th>Authentication of contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>UN</td>
<td>User name</td>
<td>PW</td>
<td>Password</td>
</tr>
<tr>
<td>CC</td>
<td>Communications code</td>
<td>IPK</td>
<td>Internal cloud trading</td>
</tr>
<tr>
<td></td>
<td>between user and device</td>
<td></td>
<td>system public key</td>
</tr>
<tr>
<td>DIDi</td>
<td>Device number</td>
<td>Cert</td>
<td>Certificate issued by CA</td>
</tr>
<tr>
<td>EXP</td>
<td>Expiration date</td>
<td>Sig</td>
<td>Signature issued by entities</td>
</tr>
<tr>
<td>H</td>
<td>Hash Function</td>
<td>Acc</td>
<td>Bank account</td>
</tr>
<tr>
<td>PSK</td>
<td>Pre-shared key</td>
<td>SV</td>
<td>Secret value</td>
</tr>
<tr>
<td>NewCA</td>
<td>New certification of contents</td>
<td>NewReg</td>
<td>New registration of contents</td>
</tr>
</tbody>
</table>
Table:

<table>
<thead>
<tr>
<th>request</th>
<th>Request service of contents</th>
<th>UID</th>
<th>System identify user’s number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ticket</td>
<td>The ticket between user and beneficiary</td>
<td>Token</td>
<td>User certificate</td>
</tr>
<tr>
<td>B</td>
<td>Bank</td>
<td>Bnf</td>
<td>Beneficiary</td>
</tr>
<tr>
<td>Rcv</td>
<td>Beneficiary request receive contents</td>
<td>Rmt</td>
<td>User request remit contents</td>
</tr>
<tr>
<td>IRcv</td>
<td>Internal cloud trading system request receive contents</td>
<td>IRmt</td>
<td>Internal cloud trading system request remit contents</td>
</tr>
<tr>
<td>TD</td>
<td>Transaction details</td>
<td>Acc</td>
<td>Bank account</td>
</tr>
</tbody>
</table>

3.3 Process Details

3.3.1 Login

Each time when user request cloud trading system service will enter service interface to verify user name and password, if the user was been successfully registered, then the user can login to use cloud trading system services by obtain certification.

Step 1: User enters UN and PW to login service interface.
Step 2: Service interface send the information to certificate authority.
Step 3: Certificate authority return the result for service interface.
Step 4: According the result award user login to cloud trading system.

Fig 3: Login

Service interface determine the user legality by verifying the result, if the user is
initial login, cloud trading system will request the user register, put the user’s browser into register component. So the user through the cloud trading system public key encrypt $E_U$ as follows: $E_U=PKSI(UN||PW)$. When service interface receive the information and sent to certificate authority by internal cloud trading system public key encrypt $Auth_U$ as follows: $Auth_U=IPKCA(UN||PW||DID_i)$. After the authentication is complete, certificate authority will award a $Cert_U$ to user by internal cloud trading system public key as follows: $Cert_U=IPKsi(SigCA||EXPCA||AC||CC)$. Service interface use the $Token_U$ to make sure the correct user login by service interface secret key as follow: $Token_U=SKSI(SigCA||H(Cert_U)||EXPSI)$.

3.3.2 Register

If user wants to use the internal cloud trading system service must to register the identity and device, when the registered device is more than one then will choose one to use.

Step 1: User enters UN, PW, Acci and DIDi to login service interface.

Step 2: When certificate authority check the user information are legitimate message then insert to registration.

Step 3: Registration verifies the user account is not registered and the device can be registered (there are two cases: one is the device has not been registered, another is the device has been registered and the original device holder awards sharing permission to the user), insert the information to Reg. DB, otherwise required to re-register.

Step 4: Registration inserts the UID and register date to certificate authority.

Step 5: According to the result return Token to user.

---

**Fig 4. Register**

User request a register service in cloud trading system, enter $request_{Reg}$ when user begging create the cloud trading system by service interface public key encryption such as follow: $request_{Reg}=PKSI(UN||PW||Acci||(DID_i||PSK(SVi)))$, if the device is not
the first time to register, then will through the pre-shared key secret value to proof the user holding the device competence. The service interface receives the register information will through the internal cloud trading system public key encryption such as follow: \( \text{Reg}_U = \text{IPK}_{\text{Reg}}(\text{UN} || \text{PW} || \text{Acci} || (\text{DID}_i || \text{PSK}(\text{SV}_U))) \), check out the account have not been register, let registration inserts the new user information to database and certificate authority such as follow:

\[
\text{NewReg}_U = \text{IPK}_{\text{RDB}}(\text{UN} || \text{PW} || \text{Acci} || (\text{DID}_i || \text{PSK}(\text{SV}_i)) || \text{EXP}_{\text{Reg}}), \\
\text{NewCAU} = \text{IPK}_{\text{CA}}(\text{Sig}_{\text{Reg}} || \text{UID} || \text{EXP}_{\text{Reg}}),
\]

Service interface response a token means the user can login to the cloud trading system through the registered device, when user login to service interface can check the token deadline by adding the expiration date, avoid the device repeat login, if the token expired then re-apply such as follow: \( \text{Token}_{\text{CC}} = \text{SKS}_i(\text{UID} || \text{DID}_i || \text{EXP}_{\text{SI}} || \text{CC}) \).

### 3.3.3 Remittance

Cloud trading system will create a transaction detail when user wants to transfer the funds to beneficiary, before this action need to obtain the beneficiary bank account. First, the user awards part of information to beneficiary by token format, when the beneficiary gets the token then request the receive to cloud trading system, at the same time the user also request the remit to cloud trading system. Cloud trading system will verify both of the user and beneficiary information correctness, if they are both correct then begging request remittance to bank and create a transaction detail after the transfer is completed.

**Step 1:** User requests the beneficiary bank account by token.

**Step 2:** Beneficiary transfer bank account to the user and request receive to cloud trading system.

**Step 3:** Service interface transfer user and beneficiary account information to certificate authority validated.

**Step 4:** Notice service interface both of user and beneficiary are legitimate account according to the results, otherwise require re-entering.

**Step 5:** Service interface send the both information to remittance.

**Step 6:** Remittance receive the information then notice the bank begging remit.

**Step 7:** After the end of the transaction, the bank return a transaction detail, if the transaction fail the return an error message.
User request beneficiary bank account information by adding the beneficiary signature, timestamp and the user login credential hash value to proof legality such as follows: TicketU=PKBef(SigU||TSRmt||H(TokenU)). When the beneficiary accepts the information will request receive to service interface such as follow:
RecvBnf=PKSI(ToeknBnf||TSRev||(H(TokenU))(AccBnf||Amount)). In the above same time, the user requests remit to interface such as follow:
RmtU=PKSI(TokenU||TSRmt||Amount||Bnf). Service interface accepts both information will verify identities legality by certificate authority such as follow:
AuthBnf/U=IPKCA(UIDBnf/U). After certificate authority confirmation will return the result to service such as follow: ResultBnf/U=IPKSI(UIDBnf/U). Service interface will sends the both of user and beneficiary trading information to remittance such as follow:
IRcvBnf=IPKRmt(UIDBnf||AccBnf||TSRmt),
IRmtU=IPKRmt(UIDBnf||AccU||TSRev||TSRev). After remittance receives information compared the beneficiary number to identify target account then transfer to bank remit such as follow:
RmtB=BPKmt(SigRmt||BC||TSRmt||AccU||TSRev||AccBnf||Amount). The bank will remits specified amount to the beneficiary account and creates a transaction detail return to remittance such as follow:
TDRmt=IPKRmt(SigB||TSRmt||AccRcv||AccRmt||Amount||Balance||MsgRmt). Remittance receives the transaction detail will response result to user and beneficiary the result.
4. Analysis

Through the following topics of: the required calculating efficiency of encryption, basic security of demands, potential attacks in each stages, we’ll analysis the cloud trading system in this research.

4.1 Efficiency Analysis

While the user operates this cloud trading system of this research, all the information transmitted is confidential, so it has to be in secured condition. Considering of the user’s mobile equipment of calculating ability, this section will analysis the user, the cloud trading system, and the bank transmit the information with each other of the encryption method to calculate how many times to encrypt. As illustrated in the table 2:

<table>
<thead>
<tr>
<th>Stage</th>
<th>Method</th>
<th>User</th>
<th></th>
<th></th>
<th></th>
<th>Bank</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Main user</td>
<td>Target (Remittance)</td>
<td>Service Interface</td>
<td>Registration</td>
<td>Certificate Authority</td>
</tr>
<tr>
<td>Login</td>
<td>Symmetric Encryption</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Asymmetric Encryption</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>One-Way Hash Function</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Register</td>
<td>Symmetric Encryption</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Asymmetric Encryption</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>One-Way Hash Function</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remittance</td>
<td>Symmetric Encryption</td>
<td></td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Asymmetric Encryption</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 2: Efficiency Analysis in Each Stage
From the table 2 to see that the user process the submitting in each stages will use the golden key provided by the cloud trading system of service interface to encrypt. Since the submitting contents are all the very important information like the user’s bank account or the connection code of equipment, it must ask to use a much complex Asymmetric Encryption and One-Way Hash Function to encrypt, and decrease information been intercepted or tampered of risks. While the user register the equipment, they’ll use the pre-sharing of method to establish the security value between the equipment owner and the user, and decrease the time that the user register the equipment and the owner confirm of sharing, so that to accelerate user register the equipment of speed. Besides, the user use 2 stage of encryption method while applying higher confidential activities will encrypt by using the open golden keys that from the service interface and the cloud trading system of internal components. Besides, use the Token provided by the certification center which is used to check up the user, reduce postpone when multiple users submitting system, and improve user’s operating speed and quality.

4.2 Security Analysis
4.2.1 Confidentiality

While the user submit service request to the cloud trading system, the certification center will according to the content requested to announce the certification and use the Token of format to conduct packing in the service interface. Let the user to get the authority according to the service content and process the operating in a short validity, and decrease the possibility of abuse on the competency. In order to reduce the cloud trading system components to be attacked, use an assembling manner to get completed user information, separate every action components of the system and isolate the components. If it needs to get the other internal components information, encrypt the internal open golden key (for example: IPKsi). To avoid the risk of information which is from the same component been theft all, and reach the goal of concealing the partial information. The bank will transfer the trading details to both the user and the beneficiary after receipt of the remittance order and completed the of the remittance, and also can reduce the thefts of the trading contents which user remit and transmit to the cloud trading system. If it needs to increase the security of the transmit contents, use the secret golden key to encrypt according to the specific sensitive information. For example: while a former user login is using $EU=PKsi(\text{TokenCC||UN||PW})$ of format to transmit to service interface, hereof according to user’s account and password use the secret golden key to encrypt, its
format is as below: \( E_U = \text{PKSI} (\text{Token}_{CC} || \text{SK}_U (\text{UN} || \text{PW})) \) therefore, only use the legal service interface to receive the inform, use its secret golden keys to decrypt, use the user’s open golden key to process the 2nd stage of decrypt and then get the completed information. If only get the \( \text{Token}_{CC} \), he cannot know who is the user and connecting to which equipment, and that will be just junk messages, so that can increase a higher security.

4.2.2 Authentication

In this research every individuals proceeding the information transmitting will all use the open golden key to ensure the receipt contents is correct, and the goal components can use his own secret golden key to decrypt and read the content. Besides, the user and the bank are the individuals that outside the cloud trading system, so to transmit the information will add extra signature to approve the message are sourced from legal parties. As per the cloud trading system of certification center and the service surface will transmit the information out of the system, it will be add certification and Token of method into the information content to approve the source corrections and avoid a tampering risks on the transmit contents.

Via the register unit establishing data base can manage users and its registering equipment, in order to check up whether the equipment has been registered, hereby use the Media Access Control Address (MAC Address), or the International Mobile Equipment Identity number (IMEI), to identify equipment as the unique code. If it happens the sharing, while the user transmit the equipment information to the certification center, connect a set of pre-sharing golden key value, that belongs to the equipment owner and the sharing user, after the equipment code. If this equipment doesn’t belong to sharing condition, it won’t shows the pre-sharing golden key of secret value, so that to prevent the thirty-party to forge legal equipment user to login. Therefore, successful applying user can own the sharing equipment authority of using, improve the sharing ability of equipment, and also pre-share with users’ golden key of method mutually and decrease the theft and tampering risks while apply sharing golden key in the internet. This procedure applies Asymmetric Encryption system to ensure users transmit register-required personal information to be secured, through the service interface of open golden keys to encrypt the user’s register information, besides, confirm the correct register user information via certification center secret golden key.

Regarding to the certification center issued of certification statements are clarified to 3 types: valid, aborted and expired. By indicating these 3 type condition of requests been receipt, the certification center can verify and confirm the content as approval or not. For the aborted of statement, even the certificated is not expired, it has to be waited till the certification been opened and then authorize the requested content. For
example: while the user’s Token been theft, it will aborted all the requests that relevant to that certification, avoid illegal request unit to use and decrease the user’s benefit been damaged. For the expired of statement, it will asks user to redo submit and get a new Token to process request. For example: the Token valid time is 5 minute, while the user submit request by this Token in the expired condition, the certification center will verify this Token as expired once received. It may not be the illegal user of submitting, therefore ask user to re-log to get new Token to continue the operation. So that to reduce the user ID been theft and avoid user repeat login via different equipment and ensure the user and the system ID are correct.

4.2.3 Non-repudiation
In the traditional internet environment, to verify and to authorize may be proceed in different server. For the information transmit more times, the risks of interception will increase, and the content can be theft and tampered. Therefore, while proceed the submitting, the information content will attached of the real signature. But the digital signature content is using that real information, combined to be produced by the trustable third party certification center. In this research, due to the submit request content are all process by the cloud trading system, use the system certification center to made the signature, while sending to outside, the service center will made the certification content according to the Token of format to send to users. While the user submit the request, the certification center can use this Token to process the 2dn stage of certification and ensure the request submitting subject is correct and it’s no tampering under the transmitting process, so that to guarantee the user with the legal source. And proof its submitting time according to the remittance and beneficiary of submitting time on the transaction content submitted by the remittance unit. To prevent the cloud trading system occurs repeating submitting, after the remittance, the bank will also transfer the trading details to both the remittance party and the beneficiary to proof the transaction situation.

4.2.4 Data Integrity
The only one that didn’t interact with the cloud trading system in this research is the process that the user asks to send the note to the beneficiary. Since there’s no certification info that from the cloud trading system certification center to verify it’s complete or not, use the method of submitting user’s Token One-Way Hash Function, and let the remittance party to process one-way hash by the original note. Using the one-way hash function to compare the original content and see if it was tampered.

4.3 Attack Analysis
Using cloud trading system will need to use the registered equipment to connect to the internet. If the equipment is lost, user can use the other equipment or the browser to connect to the cloud trading system and stop that login authority, so that to cancel the
service and prevent the lost equipment to be abused by others, when the equipment is get returned, it can be used by re-do the registration. Even the internal staffs of the cloud trading system cannot steal the user’s information since the user in the components of the system only have partial information, it must be requested by the user, the communication between each components can temporary get the required remittance information. After the remittance completed, the bank will directly send the trading details to both parties of trading, the cloud trading system has no mean to know completed trading information, thereby block the internal use of illegal workers.

While the user deliver the remittance note to the beneficiary, if it happen the Man in the Middle Attack, that intercept the user’s request, the content will be encrypted by the beneficiary’s open golden key as the first protection, and the 2nd is due to the one-way hash process on the submitting Token to login the cloud trading system, it cannot be available of the completed information to forge login ID, thereby protect user’s information not been abused.

5. Conclusion and future research

In the traditional transaction model, no matter the enterprise or the individual user all have to use the cash or the credit way to process the commercial behavior. That will usually increase the business process of time and decrease the service of quality. With the rise of the Internet, the e-commerce of concept is getting applied in the modern transaction environment. Under the browser and the server of applications, both the seller and the buyer of information can be established electronically. One can fast process the commerce activities even in different area is becoming nowadays business type. However, during the commercial activities of process, enterprise has to face the different demands from everyone to establish a system that secured the business secrets and personal information. Causing companies and users, other companies, and even inside-department are isolated as a funnel information environment. In the condition of information asymmetry, the user has to register in a specific system according to their demands. But while they conduct the real-name system adopted trading activities, it has to establish those sensitive information of their user account, personal information, and bank account…etc. As per user with various demands, to conduct various trading activities will all need to establish their personal data, that means to repeated exposure of personal data in the next work, and that will increase the leakage risk of personal data. If take the virtual account will cause more problems, for example: to conceal personal information from both sides each will not be able to recognize the legality, and have difficulty to chase the transaction details in the future, and abuse accounts problem…etc. so exist more risks.

Therefore, through this research of applying cloud trading system, and integrate
information from both sides of transaction and the bank will decrease risks of leakage for the personal sensitive information. While the user login the system by the equipment that is registered to connect the internet, so that to confirm as the legal user. By pre-share golden key will also increase the sharing ability on the equipment and let more users all can operating on the same equipment. After login, to guarantee the sending out each segment of information safely, add the target components of open golden key, especially on the internal use components, open golden key in the cloud trading system, this will increase the information transmit safety. Besides, while all the components exchange the information, only the partial inform will be received,( except the target components which can get the complete information), so that to meet the goal of concealing partial information. To avoid user information being intercepted in the transmitting process, use the way by put together combination and get the sensitive information. In the meanwhile, by using the cloud trading system can use the fewer steps to process the transaction, and greatly improve the user’s experiences.

In the future research will consider the user’s equipment of capacity. In the view of the smart phone in the market now, it has been able to bear a part of the computing requirement. Therefore, we’ll investigate how to increase the safety of the information delivered especial by the user in the future.

REFERENCES


