The Centrifuge of Cloud Service: Separated Cryptographic and Ciphered-storage Services

Zheng-Yun Zhuang[1,5], Yi-Chang Hsu[2], Hsing-Hua Liu[3], Chien-Hsing Wu[4*]

[1] Graduate Institute of Data Science, Taipei Medical University, [2] Department of Industrial and Business Management, Chang Gung University, [3] Head Office, Hivocal Technologies, Inc., [4] The Graduate Institute of Business Management, Chang Gung University, [5] Faculty of Science and Technology, Universidade de Macau

[1]zyzhuang@tmu.edu.tw, [2]ivan7219@yahoo.com.tw, [3]davidliu@hivocal.com.tw,

[4,*]kenhing.wu@gmail.com, [5]zyzhuang@umac.mo

Abstract

This study proposes a business model to provision a security-enabled cloud via splitting cryptographic and cipher-storage sub-services off from the main cloud service, being independently operated by other SPs. The security/privacy enhancements of the model over the existing approaches are proved progressively but cogently. As such, the model can alleviate the improper user data disclosure risk, raise the privacy preservation of sensitive user information and therefore, mitigate the two information-leaking threats. The interoperability (among the centrifuged services) and migration issues (i.e., seamless system transferring and SLA amending) are illustrated and studied by using the extremely security-sensitive e-banking cloud service example.

Keywords: service operation risk management, security service and privacy, distributed cloud systems organizing principle, database and storage security, management and querying of encrypted data, cryptography and key management

1. Introduction

Cloud computing has become popular by providing ubiquitous data access and

* Corresponding author: Chien-Hsing Wu, kenhing.wu@gmail.com

computing to users, making them get rid of setting up a robust storage. A user simply stores data and performs relevant computations on the cloud directly, as the computational resources of the cloud system have been well organized and utilized by the service provider. On the user side, only a low-speed Internet-enabled device, such as smartphone, desktop, or laptop, is required [14]. As such, many types of cloud service have been derived, e.g., utility computing service, grid computing service, data-center service, and etc.

However, the privacy protection level of and the security functions offered by a cloud system usually determines the degree to which a user can trust it, which will further affect the user willingness to access the service. In fact, these can be viewed as some major technology acceptance factors during cloud service adoption [1][20].

In order to alleviate relevant information-leak and security risks (as to enhance both privacy protection and security levels), this study advocates that the cryptographic and the cipher-storage functions can be separated from the main cloud service (i.e., the service with main functional purposes) and they can become services which are independently operated. According to this concept, a multi-service business model (MSBM) is established (i.e., the three separate services: ‘crypto’, ‘cipher-storage’ and ‘main’).

The security level enhancements brought by the model are proved, while the possible consequences upon taking this model to reorganize the cloud service are examined. In addition, the application scenario of this model is illustrated by an e-banking case, while security, user privacy preservation, system interoperability and the efficiency issues are addressed. These may draw implications for other cloud services in which the stored data is also highly sensitive.

Section 2 reviews the literature, addressing the important privacy and security concerns pertaining to a cloud service. Section 3 proposes the MSBM model, addresses its advantages over the existing cloud service operational models and proves the security/privacy enhancements brought by MSBM. In Section 4, the model is then illustrated by applying it to reorganize an e-banking cloud service, wherein the collaborations of the three isolated services are shown. Section 5 drafts the *N*-to-1 SLA and discusses the detail design issues about the model. Section 6 concludes this study.

2. Literature Review

2.1 Cloud Computing and Cloud Service

Cloud computing originated from *grid computing* [2]. It has been defined in several ways

[3]. Some researchers view it as *utility computing* because it offers public utilities [4][40], while others consider it as *autonomic computing*, because on the cloud the managed resources are automatically utilized and self-adapted [17][32]. The study by [36] took a *service-based view* and concluded that it refers to a service that involves a compilation of Internet resources, wherein the resources to meet user needs (i.e., hardware, system development platforms and various application systems) are combined dynamically and flexibly.

A well-known definition of cloud computing is in Special Publication 800-145 by NIST (The National Institute of Standards and Technology) [15], which states: "… Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released *with minimal management effort or SP interactions. ...*"

The above definition is based on a *resource-based view* [18]. By also taking the autonomic-computing views mentioned above, cloud computing performs its autonomous system functions by utilizing its resources, such as software, storages, processing functions, RAMs, network bandwidths and virtual machines, which constitute the resource pool. Resources in the pool are flexibly tuned to handle and catch up with a variety of user needs. The well-known hierarchical classifications of cloud service has been discussed in [15][37].

By taking the service-based view in addition, from a viewpoint of user, a cloud service offers common software for public use, computing platforms for general purpose (i.e., the storage and the computing facilities) and system development platforms for the application developers. As such, the cloud SP charges the user by meter-rating [22] the contents assessed or the time elapsed, or simply by the utility packages subscribed during a certain period.

2.2 Data Security and Privacy Concerns while Accessing a Cloud Service

In the past, user data was stored in an internal storage device of a computer. With some proper measures, saving data in this manner can be safe. To prevent company data from improper disclosure, except for locking the permanent memory physically, a user can install some software, which is secured by user passwords, to encrypt the document files saved in the permanent storage [23]. On the institution side, a company may set up a firewall or an intrusion detection system (IDS) to prevent the unauthorized accesses from cyber criminals [12][39], or introduce internal regulations to forbid information leaking by any privileged individual.

Nevertheless, the state-of-the-art cloud computing has changed the way in which data is stored. The hosted data on the cloud as well as the computation results are not always

trustworthy because of the lack of physical possession and control over the data for data owners [30][31][38]. With the trend of storing user data in the cloud, [33] have mentioned that service provider (SP) should take the responsibilities for ensuring data security and mitigating the improper disclosure risks. Encrypting user data when it is to be stored in the cloud is therefore suggested.

However, merely to encrypt the data can be still risky [24][30]. In any traditional security-enabled system, if some privileged individual can have the decryption key of the user and the encrypted user data at the same time, the plain data can be easily recovered, given the condition that the crypto algorithm is known [41]. Analogically for a cloud service, if the main SP operates both the crypto and the cipher-storage services at the same time, a privileged employee (e.g., a system operator employed by the SP) might access the user key and the encrypted user data simultaneously and would thus be fully capable of recovering all the user data (whether granted or not).

This may bring up the *improper disclosure (of user data) risk*, which will depress user's trust to the service. If any such security event occurred, existing users would lose their faith and this could also deter new users from signing up the service. In other words, *if both the crypto and the cipher-storage services are operated by one sole SP which also operates the main service, the SP must manage its employees perfectly; otherwise, the improper disclosure risk cannot be completely avoided or alleviated*.

Except for the abovementioned data security concern, which is about the data itself, *information privacy risk* becomes another concern of users to feel safe to host their profiles (e.g., contacts or credit card #s) on the cloud. In recent years, adversaries are more enthusiastic because they can use the organization's confidential information in order to earn the financial profit [11]. For the cloud SP organization, in addition to the internal information (e.g., the financial reports), user profiles are the most valuable assets, but so for the intruders. As the endless news have reported how the scammers can 'utilize' user privacy information, enhancing user privacy preservation level should become another spark light to attract new users, or at least to hold the old users.

This subsection reviewed the two main concerns of the cloud service users: the security concern about user data and the privacy concern about user information. For a cloud SP, let us examine back the interesting definition by NIST, which states that a cloud service should be managed with a 'minimal management effort'. With the above two user concerns, this is perhaps difficult just because of the existence of the improper disclosure risk, which is induced by bundling the security-relevant sub-services all together and being unable to manage the employees perfectly. Although bundling the involved services can lead to 'minimal SP interactions', it becomes hard to totally control the improper disclosure risk, and

therefore the information privacy risk.

2.3 The Modern Cryptography Aspect

In Section 2.2, user concerns about the adoption of a security-enabled cloud system and the main drawbacks of bundling all the sub-services together were addressed, calling for the need to separate the security-relevant sub-services. As a supplement to these, this subsection reviews the threat matters from the perspective of modern cryptography. Refer to Appendix A for a review of the modern cryptographic methods which have successfully supported the commercial application scenarios.

However, in spite of the effort that modern cryptography has made, methods or algorithms present in modern cryptography may appear insufficient for cloud service. As mentioned previously, both user data and user profile are to be stored on the cloud, but current service-centralized cloud system may induce improper disclosure risk and personal information privacy risk. And to prevent from these, a recent trend is to encrypt user data before it is stored [21] in the cloud. Nevertheless, from the perspective of network security (than information security) and management, merely encrypting user data is still insufficient and insecure, because of the following possible threats:

— *The "winner takes all" threat*. Consider that an adversary has intruded the SP cloud system. As he/she can obtain the encrypted data, there should be ways to retrieve the user keys further, if the SP cloud system covers both the cipher-storage and the key management functions. As all the services are bundled together, the user data could be at risk. This is analogical to, but not identical to, the problem of the old firewall architecture which bundles all the functions (e.g., packet filtering, content screening, NAT, and etc.) together, and if once this sole bastion was vulnerable, the adversary would gain control over everything.

— *The "privileged individual theft" threat.* Any intentional privileged individual inside the SP might obtain both a copy of the decryption key and a copy of the encrypted data, while the SP may not be able to manage all the employees perfectly, as discussed in 2.2. More critically, if this sole SP also stored the user profiles (e.g., user name, contact information, account information, and etc.), the privileged individual would be able to recover a full range of privacy information and to perform more things harmful (e.g., extortion), than merely to decrypt and just to know the user data. If such a security event occurs, the SP will have no chance to regret, although it is a management problem due to internal failures, rather than intrusions. The "2008 Data Breach Totals Soar" published by the Identity Theft Resource Center [34] has

indicated that ‘theft of data by internal personnel’ is one of the top five reasons for leaks.

As can be seen, analysing the ‘threats’ from these perspectives yields similar observations of the possible security/privacy vulnerabilities of a contemporary, centralized cloud service, which are thus harmful to any security-sensitive cloud service provisioning.

3. The Multi-service Business Model (MSBM)

3.1 The Concept of Multi-service Business Model

With improper disclosure risk present and with the increase in user awareness of information privacy, this study proposes the multi-service business model, wherein both the crypto and the cipher-storage sub-services are isolated from the main cloud application service. It is a ‘business’ model because the separated sub-services become individual services that can be owned and operated by other SPs (business parties), while their roles are defined as follows:

— *Crypto service*. Key management and the en-/decryption functions are centrifuged from the main service and they are performed by a separate ‘crypto service’. It encrypts and decrypts data, manages the cryptographic keys and holds in memory only the necessary information for algorithmic computations (i.e., the memory keeps only the keys in use for the encryption/decryption, while other keys must be saved securely). In other words, temporary information such as the plain text (the unencrypted information), the encrypted data, or the decrypted data, is erased right after its life cycle is due.

— *Cipher-storage service*. The storage function that reads and writes the encrypted data is also isolated from the main service and the crypto service. A separate ‘cipher-storage service’ serves this purpose and in this subsystem, key management is not allowed.

Such design is mainly based on two ideas: 1) separating the encryption/decryption functions and making them as a separate crypto service [10]; 2) cross-cloud service composition [6]. And since by following (1) the cipher-storage service is also isolated, the two centrifuged services are independent not only from the main service, but also from each other. With this model, the user concern about improper disclosure risk should be resolved, and it has the following advantages:

— Since the main service stores the user profiles and the crypto service stores only the keys without any user information, once any key in the crypto service system is leaked, user profiles in the main service system will remain secure, because their association is unknown. This is a reverse thought in contrast to digital certificates, wherein user information and the public key are bundled.
— If the data stored in the cipher-storage media is leaked incidentally, the key would not be exposed along with the data, i.e., it has been stored in the crypto service system. Therefore, the ciphered data remains secure.
— Since the power of cloud service is decentralized, relevant services can be performed by individual systems which are operated by different SPs. Each SP operates its individual cloud service and manages the dedicated job only. As the SPs operate different services and as one cannot serve two companies at the same time, a major part of the improper disclosure risk can be avoided, because any intentional employee has merely some 'partial clue' to recover the plain message.
— The migration to the MSBM model (which is to split off the services) can be performed seamlessly and transparently to the users. This will be shown in later sections.
— After the migration, the whole MSBM model will be transparent to the users when they are accessing the cloud service, although there are, in fact, multiple SPs. In other words, a running MSBM model will be transparent in that a user will, still, face with and access the main service system as usual and won't be aware of such change.

However, when the MSBM model is applied, 'multi-SP' becomes a fact. This implies that within the service level agreement (SLA) [8], the '1-to-1 relationship between the sole SP party and the user' has to be changed to '*N*-to-1 relationship among the three individual SPs and the user'. Therefore, the responsibilities of the *N* involved SPs must be re-stipulated in the new SLA and the SLA must be resigned. This will be illustrated in 5.1.

3.2 Service Decompositions to MSBM: An Elaboration

In order to better illustrate the advantages of the proposed MSBM model, the sequential reasoning process of MSBM is examined, which is to derive all possible business models coupling the three services (as defined below) in different manners.

— *AS*. The main application service.
— *ES*. The encryption/decryption crypto service.
— *CS*. The cipher storage service.

Based on these definitions, different cloud service business models can be derived, as

follows:

— *The 'ACE-aaS' approach.* This approach bundles the AS, the ES and the CS all together as an entire service. The dashed triangle in Figure 1 shows this coupling relationship. This is defined as 'AS-CS-ES as a service', or simply 'ACE-aaS'. As can be observed in current service operations, most non-security-enabled cloud SPs adopt the 'ACE-aaS' solution. The possible drawbacks of this approach were discussed in previous sections.

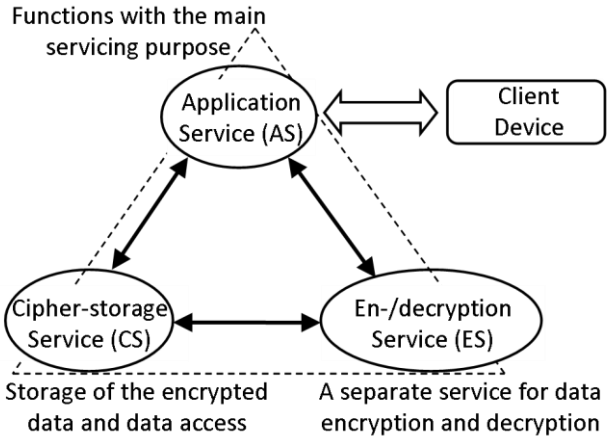


Figure 1: The service separation conceptual model and the usual 'ACE-aaS' approach.

— *The 'CS-aaSS (and AS-ES-aaS)' approach*. Making CS as a separate service (CS-aaSS) was perhaps the first work to spin off a security-relevant service from the main cloud service. In this manner, the cipher data generated by the AS are stored in an independent storage facility, which is owned by the SP itself or owned by a third-party SP that provides storage hosting service. In either way, the stored data is encrypted and the latter option is shown in Figure 2. In the industry, the cloud system structure of Salesforce.com's CRM [27] or SAP's ERP [28] accords with the CS-aaSS approach.

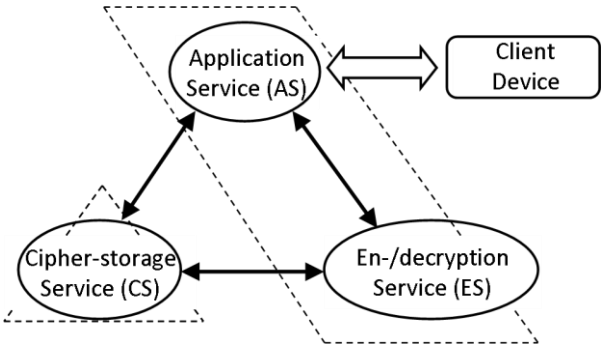


Figure 2: The 'AS-ES-aaS and CSaaSS' approach.

— *The 'ES-aaSS (and AS-CS-aaS)' approach*. Making ES as a separate service (ES-aaSS) is another approach. This is also defined as the 'AS-CS-aaS' approach and is as shown in Figure 3, wherein the AS and the CS are still bundled. In the paper by [10], the idea of ES-aaSS was first disseminated and the importance of separating the ES from the main service was emphasized: the keys and the encryption/decryption functions can be independently managed. However, to the authors' best knowledge, this approach is rarely mentioned, let alone its applications. In addition, as mentioned in that paper, before ES-aaSS was proposed in 2011, most cloud services were organized by taking the ACE-aaS approach or the CS-aaSS approach.

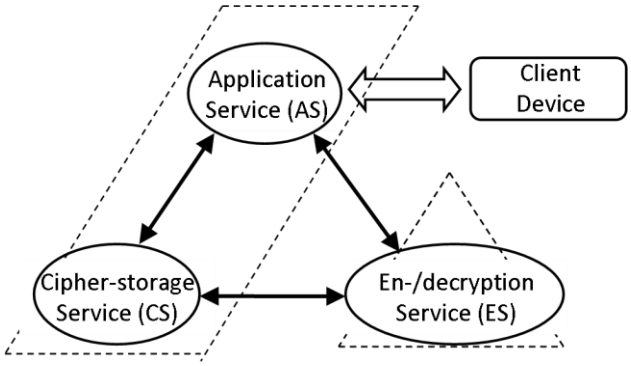


Figure 3: The 'AS-CS-aaS and ESaaSS' approach.

— *The 'AS-aaSS (and ES-CS-aaS)' approach*. Another approach is to bundle ES and CS as a service and leave AS as an isolate one. For space reason, the figure to illustrate this approach is omitted. In this manner, the AS provider company merely operates its main service but shifts all the cryptographic-relevant burdens to the other SP party where both ES and CS are hosted. However, from the view of risk management, this is only a policy of the AS provider to shift part of its risks to some other SP party. As can be figured out, this approach does not effectively prevent improper data disclosure from happening because 'the other' SP company is operating both ES and CS. Any intentional employee in 'the other' SP can retrieve both a key and the ciphered user data, which is the condition to decrypt it. In addition, this approach cannot meet the data-privacy requirement: because the AS still stores the complete user-profile information, it could not avoid the theft events of user profiles.

— *The 'AS-aaSS, ES-aaSS and CS-aaSS' approach*. Based on both 'ES-aaSS' and 'CS-aaSS', the 'AS-aaSS, ES-aaSS and CS-aaSS' approach can be derived. In Figure 4, the ES is in charge of managing the keys, encrypting the data received from the AS and sending the ciphered output to the CS. The ES is also in charge of decrypting the cipher data received from CS and passing the data back to the AS. As such, this approach involves three separate services, each of which can be operated by an SP.

The framework shown in Figure 4 is exactly the MSBM model proposed based on the last 'ASaaSS, ESaaSS and CSaaSS' approach, which is the final product of the above reasoning process. Based on the security/privacy advantages brought by MSBM (see 3.1), a part of sensitive user profile information can be taken out from AS and stored in the CS.

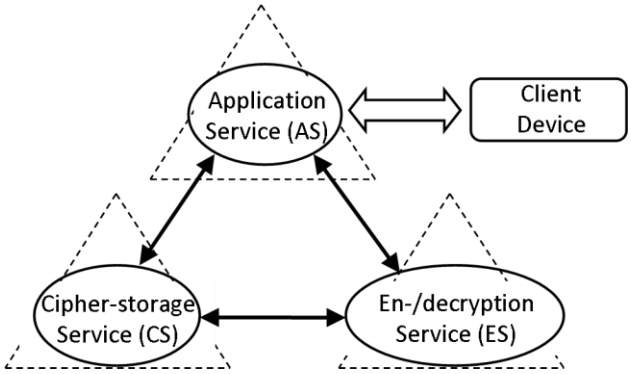


Figure 4: The 'ASaaSS, ESaaSS and CSaaSS' approach (the proposed MSBM model).

3.3 The Security/Privacy Enhancements and Proofs

The first salient feature of the MSBM model is that it separates the functional responsibilities of ES and CS. It thus *avoids the improper disclosure risk of the 'AS-aaSS (and ES-CS-aaS)' approach* because the data key and the ciphered data for a user are separately stored. And, since a part of the sensitive user profile information (e.g., user–account association information, as will be shown in the example) is not saved by the AS, any intentional employee may not associate a user with his/her sensitive profile. Therefore, *the protection level of user privacy is enhanced*.

Next, the model also *resolves similar problems which the 'CS-aaSS (and AS-ES-aaS)' approach will encounter*. By taking the CS-aaSS approach, the CS is nothing but a storage SP who can save the user data in a very secure way. Encryption, decryption and key management are still performed by the main SP. This means that any intentional employee can see the plain data already decrypted by the decryption function and match it further with the user profile based on their known association relationship. This is akin to the residential infectious software, which can watch the memory blocks that contain the decrypted data directly, rather than trying to perform any crypto-analytic tasks.

Thirdly, based on the above two points, it should be obvious that the proposed model also *alleviates the improper disclosure risk of the traditional ACE-aaS approach*.

The above three discussions also form a cogent proof about improper disclosure risk improvement and user privacy protection level enhancement, from existing approaches to MSBM. The ontology behind this proof is shown in Figure 5.

From Figure 5, relevant proofs can be read as follows.

— (1): CS-aaSS has improved the security level of ACE-aaS by saving the user data in a very secure way. It is still insecure because the encryption/decryption and the key management functions are performed by the main SP.

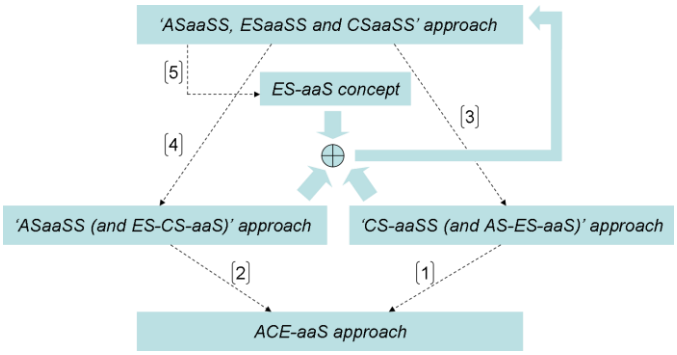


Figure 5: The enhancement relationships and the ontology behind the proofs.

— (2): AS-aaSS has improved the security level of ACE-aaS, whereas the main SP has submitted all the security-relevant works to another SP, which handles both the cryptographic and the cipher-storage functions. With this approach, data security risk will be shifted to the latter SP, while information privacy preservation level is identical to ACE-aaS. They will still be at risk.

— (3): the MSBM model (i.e., the top one) can improve the security level of the CS-aaSS approach, with drawbacks stated in (1).

— (4): the MSBM model can improve the security and privacy level of the AS-aaSS approach, with drawbacks stated in (2).

— (5): the model can improve the security level of ES-aaSS because the storage function of user data has been centrifuged from the main service functions, avoiding the complete associations between the user profile and the decrypted user data.

Based on the above proofs, it can be asserted that the security/privacy level of the MSBM model is higher than the security/privacy levels of the other models wherein the three studied sub-services are not totally decomposed. This should be the main result of this study.

As a supplemental discussion to this section, perhaps the MSBM model can reflect a frequently-mentioned concept in business management: avoiding the risk of power concentration. For example, every company has two financial departments, the accounting department and the cashier department. The accounting department is in charge of book-keeping and sorting the financial records, while the cashier department is in charge of the payments and the receipts. Such design prevents from the improper expenditure of company funds. This concept is readdressed by MSBM again: the centrifuge of the

security-relevant services can prevent the improper disclosure risk and enhance the privacy protection level!

4. Illustrative e-Banking Cloud Service Example

Internet banking (e-banking) has been proved to be an efficient way to overcome the spatio-temporal restrictions of face-to-face banking. In the past two decades, many common bank services were designed and shifted to e-banking. As a customer can go online to check the account status (e.g., the balance) and make the allowed transactions, it unloaded the clerks' burdens. When moving an e-banking service onto the cloud, the bank can take the ACE-aaS approach and operate all the services by itself. However, since e-banking is highly security-sensitive, the bank can consider the MSBM model and outsource the crypto service and the cipher-storage service, as to enhance its security/privacy-preservation level.

Figure 6 is an E/R model [5] for the data stored in an e-banking system. It is a simplified version because the purpose here is to illustrate the MSBM model with a few involved processes. Five major entity classes, i.e., customer, account, sub-account, transaction and transaction entry, are defined as follows:

— *Customer*. A 'customer' entity in Figure 6 is a profile for an e-baking customer. It includes, for example, customer ID in the system, name, date of birth, gender, social security number, contacts and the possible data for data association, e.g., the account(s) owned by a customer, and other necessary data. Note that a customer can own more than one account in a bank.

— *Account*. An 'account' entity is the account information of the bank accounts owned by a customer. The basic types of account include, for example, the savings, fix deposit and cheque accounts in domestic currency. The extended account types include, for example, the saving account in foreign currencies, the mutual fund account, the stock exchange account and the mortgage account. The fields for an account includes, for example, customer ID, account ID, balance, account opening date, last-invoked date, other required information and possibly, the sub-account IDs.

— *Sub-account*. Some accounts have sub accounts, but some does not, e.g., the savings or cheque accounts. An account such as the savings account in foreign currencies can have multiple sub accounts. A foreign currencies saving account is further stratified into many sub accounts by the different currencies exchanged and deposited.

— *Transaction*. A 'transaction' entity records an authorized transaction that a user has made. Today, the fruitful e-banking functions not only cover a wide variety of the

traditional transactions that one can make at the counter, but also become a tool for a bank to expand its market share. A transaction made by a user often involves more than one account. For example, the purchase of a deposit certificate involves a deduction of the savings account and an addition to the fix deposit account. Such transaction will involve two accounts and it will produce two 'transaction entry' records in the database. The situation of foreign currency purchase is analogous. See the following for 'transaction entry'.

— *Transaction entry*. Most transactions may induce two or more than two transaction entries, while some induce only one. For example, if the transaction is to wire some monetary amount out from the savings account, for this transaction, only one transaction entry is recorded by the transferring bank, while the other entry is recorded by the receiving bank and thus is not the business of the transferring bank. The possible fields for a transaction entry includes, for example, transaction date and time, serial number, ID of the account, amount of transaction, transaction remark, other details about the transaction, and possibly, the ID of the sub-account.

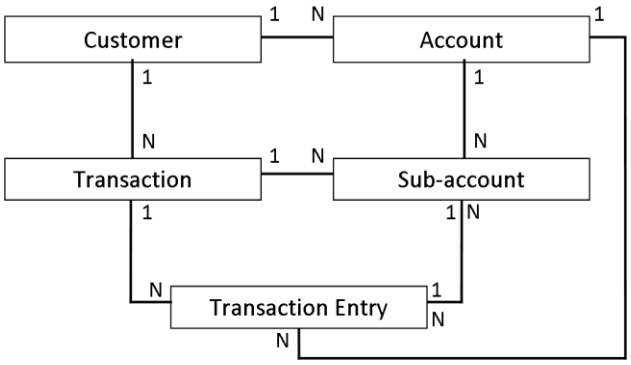


Figure 6: The simplified E/R model of an e-banking service.

In each instance of the above entity classes, a sequentially numbered *unique ID* must be assigned. With the MSBM model, any such ID is also encrypted before it is stored, since it can be recovered with a decryption process by calling the crypto service. To avoid the possible conflicts, unique IDs are encrypted by a discrete logarithm function that ensures a 1-to-1 mapping property between the plain-text field and the encrypted-data field, so that any encrypted ID is also unique in the encrypted-data field. An *encrypted unique ID* is defined as a '*substitute ID*' in this study.

4.1 Model Application

This section explains the collaborations among the three independent but relevant

services when the MSBM model is applied.

4.1.1 User Login and Account Status Inquiry

Figure 7 illustrates the process in which a customer logs in the e-banking service and checks the status of the major account. Note that a password security scheme discussed in Appendix A, e.g., challenge and response, can be incorporated with the login process.

After logged in, the AS obtains the 'customer ID' and sends it to the ES for encryption. The ES retrieves the 'user key' associated with this customer ID and the 'substitute customer ID' is obtained by using its encryption function. This substitute ID is then sent to the CS so that the customer's 'substitute major account(s) IDs' can be retrieved. Within the CS, the 'substitute customer ID' is the index to look up the specified data entry in the 'major substitute accounts table'.

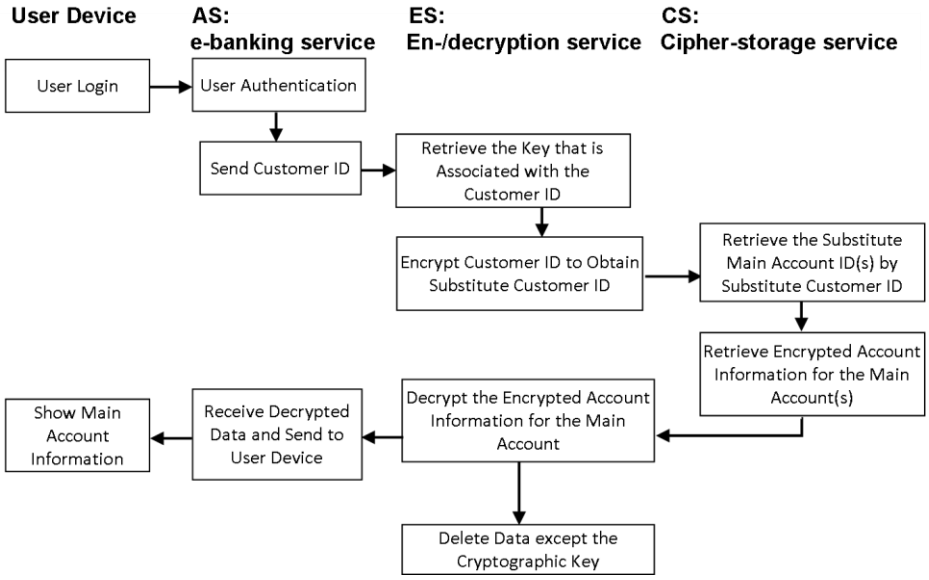


Figure 7: User login and account status checking flow of MSBM-based e-banking service.

Subsequently, each 'substitute major account ID', in an encrypted form, is used to retrieve the 'encrypted account status information' in the 'accounts' table. Together with the 'substitute major account ID', the 'encrypted account status information' is then sent to ES for decryption. As a result and finally, the ES sends back the plain text to the AS and the AS forwards the decrypted information (e.g., account number and the account balance) to the user.

After the above process, the ES immediately deletes all data received or produced so far because of the expiration of data lifecycle, except the user key. The user key is kept until the session is expired some time. Also note that the secure transmission from the AS to the client, e.g., via the established secure (e.g., SSL) channel, is irrelevant to this process. It is another

security issue and is out of the scope of this study.

4.1.2 Transaction History Lookup

Figure 8 illustrates the process in which a customer is asking for the transaction history of some savings account further, restricted by a certain user-specified period. As a common scenario of using an e-banking service, this possible process usually immediately follows the account information inquiry process in 4.2.1 and is triggered by a user click (on a hyperlink displayed in the browser). Figure 8 begins with a status that the customer has logged in and the account information has been retrieved after the login process in Figure 7.

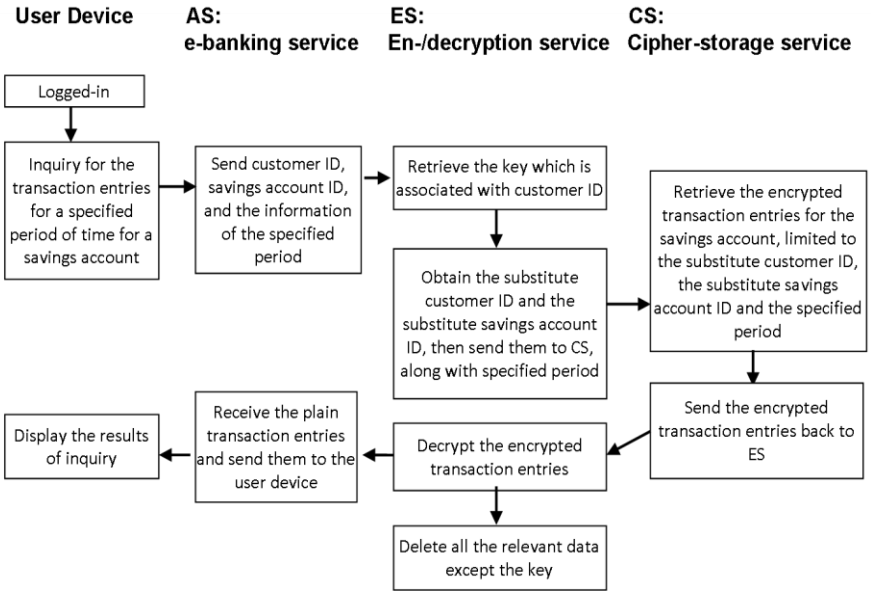


Figure 8: The transaction history lookup flow for a savings account.

At the beginning, the ‘customer ID’ obtained previously and the ‘account ID’, which has been obtained from the previous account status retrieval process, are sent to the ES for encryption.

Next, the ES encrypts the account ID and will have the ‘substitute account ID’. This ‘substitute account ID’ is passed to the CS for looking up the ‘encrypted transaction entries’, which is then passed back to the ES.

Finally, the ES decrypts these entries and sends the ‘decrypted transaction entries’ back to the AS. The AS can then forward them to the user side.

4.1.3 Foreign Currency Exchange Transaction

Figure 9 illustrates the process in which a customer is making a foreign currency exchange. The customer is trading-in Euro with the local currency savings. Therefore, a

decrease in the local currency savings account balance and an increase in the Euro foreign currency savings sub-account balance are both expected.

Based on this transaction, the update of relevant account balances is more complicated. As can be seen in Figure 9, the initial steps are similar to those in Figure 7 and 8, which is in a 'CS →ES→AS' order. The information retrieved from the CS for both involved accounts, in the original form, are ciphered and they will require decryptions by the ES.

In addition, while the plain account information of the two involved accounts should be passed to AS so that the AS can perform the business logic for this transaction (i.e., computes the two updated balances and composes the two transaction entries, one for each account), the result information (about the new status of the involved accounts and the composed transaction entries) must travel through a reverse order to the CS, which is 'AS→ES→CS', before their ciphered information can be stored.

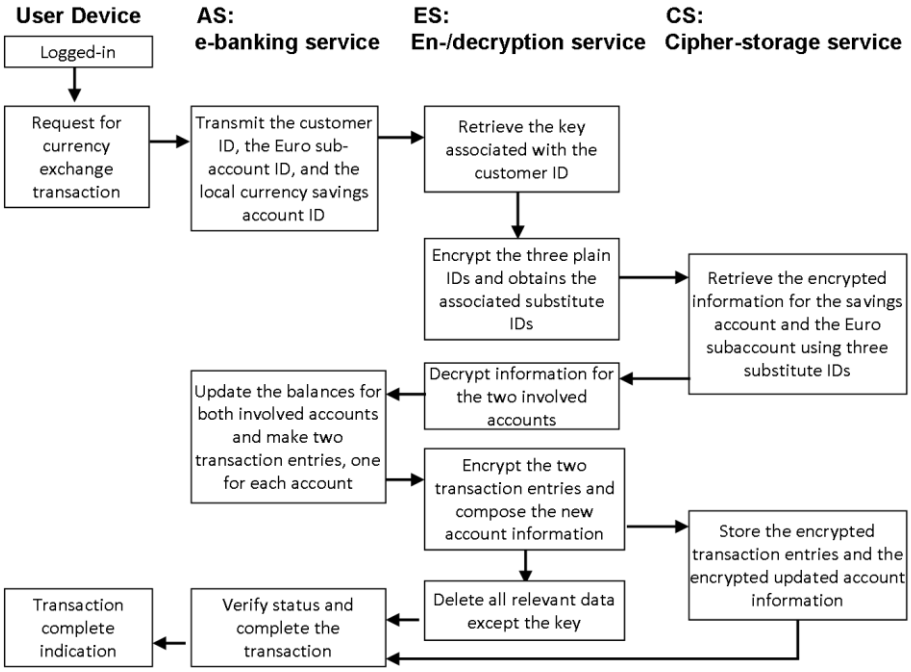


Figure 9: The flow of foreign currency exchange between two savings accounts.

Note that before the third step of Figure 9, usually, whether to make such a transaction is reconfirmed. This is often done by the password security methods, such as SMS OTP, which is out of the scope of this study.

5. Discussions

5.1 Amendments of SLA and the New SLA

As discussed earlier, SLA, a contract, is usually signed between the cloud SP and the user. A SLA may include the service application procedure articles, terms of use, services offered, information protection disclaimers, compensational terms (for any damage), and contract renew/termination conditions. Different business services may have different additional terms or appendices in the SLA. But the fundamental part of the SLA should be an intersection of the statements listed above.

For an e-banking cloud service which applies the proposed MSBM model, the new SLA should take into account user privacy improvements. It should also reflect the new operational facts and in particular, the enhancement of avoiding the improper disclosure risk. In addition, it is required to clearly stipulate the rights and the responsibilities of the involved SP parties to the user.

SLA for Internet Banking Cloud Service

Before applying for Internet banking services (Our service), please read the following service level agreement (Agreement) carefully. By signing up for our services, you acknowledge that you have read and understood, and agree to be bound by, the terms and conditions as set forth in this Agreement.

I. Our service

(The e-banking services provided, such as transfers, investments, bill pay, and etc.)

II. Service providers (SPs)

A. Internet banking service: _____. Provides all services listed under article I (Services).

B. Encryption and Decryption Service Provider (Crypto SP): _____. Provides encryption and decryption services to encrypt and decrypt information and manage the cryptographic key used in encryption and decryption.

C. Storage Service Provider (Cipher-storage SP): _____. Provides storage equipment and system to store the information required for this service. Provides information while necessary. All data except those stated below is encrypted by the crypto SP before storage. [Some data, including the transaction date and serial number, may be stored in the plaintext form in consideration of computing efficiency. The disclosure of these data would not be to the detriment of information privacy.]

III. Storage

With that the Crypto SP encrypts data, the encrypted data is stored on the system provided by the Cipher-storage SP; data will be stored for ___ years.

IV. Data security

The Cipher-storage SP will not store data which has not been encrypted by the Crypto SP (except those specified in Article II, C.). Once the Crypto SP has completed an encryption or a decryption, the non-encrypted (unencrypted), encrypted and decrypted data will be erased immediately. The cryptographic key required for encryption and decryption is managed by the Crypto SP.

V. Privacy

Unless required by law, the cryptographic key managed by the Crypto SP is not disclosed to any party other than the Crypto SP, in particular, not to ‘Our service’ or to the Cipher-storage service. Any information obtained from the use of the service, by User, by ‘Our service’, by the Cipher-storage SP, or by the Crypto SP, shall not be disclosed to any third party or used for any purpose which is not stated in this SLA. If a third party is given the permission to access the data, the third party is also bound by this Agreement.

VI. (Other non-information privacy related articles)

Figure 10: The renewed SLA for an e-banking cloud service appropriating the MSBM model.

A new SLA that serves these purposes is drafted in Figure 10. In this SLA, the statements for data storage, data security and privacy reflect the core architecture of the MSBM cloud service model (i.e., the separation of AS, ES and CS). Responsibilities of the different SPs are stated. As is shown, the crypto SP is responsible for key management, information en-/decryption and the proper erasing of all the unencrypted, encrypted and decrypted user data in time. The cipher-storage SP is only allowed to store and retrieve the encrypted information. Note that in this SLA, articles that are irrelevant to privacy protection or data access security were omitted.

5.2 Discussions: Practical and Compromise Issues

In Figure 8, the user-specified period, limited by a start date and an end date, is used to select out from the database a proper range of encrypted transaction entries for the clicked account. This can be semantically expressed as a non-formal SQL command which is executed by the CS, as the following:

```
SELECT *
FROM TranscationEntries
WHERE S_CustomerID = $Substitute_CustomerID AND
        S_AccountID = $Substitute_AccountID AND
         (Time_Transaction>=$SpecifiedStartDate AND
          Time_Transaction<=$SpecifiedEndDate)
ORDER BY Time_Transaction.
```

As can be seen, the ‘Time_Transaction’ field in the ‘TransactionEntries’ table must be stored plainly. If this field is also ciphered, the CS system could have no way to perform a fast period-limited transaction lookup based on the given customer account (which is indexed by the ‘S_CustomerID’ substitute customer ID field and the ‘S_AccountID’ substitute account ID field), since the ‘Time_Transaction’ field will lose its order. Analogically, the ‘SerialNum_Transaction’ field in the same table must be stored plainly, too.

In other words, the flow in Figure 8 should work under the condition that both the ‘Time_Transaction’ and the ‘SerialNum_Transaction’ fields are not encrypted. This is because leaving these fields plain will make the MSBM model efficient and thus able to be produced. In addition, doing so does not affect the privacy protection level. Therefore, with the application of MSBM, in the CS only those sensitive fields (e.g., the customer IDs, account

IDs, account balance information, the amounts of transactions, and etc.) are encrypted and saved.

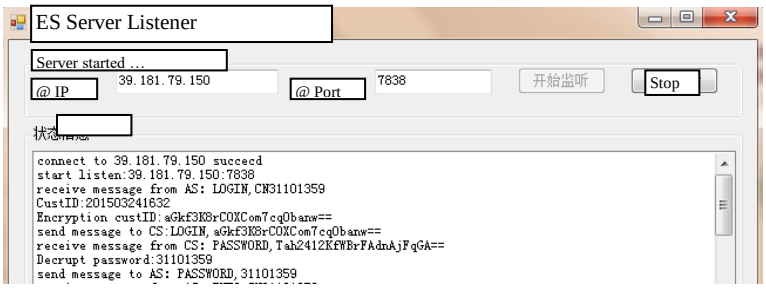
The new SLA in Figure 10 also reflects this fact. The terms have shown the fact that a part of user information, while not violating any privacy protection policy, will not be ciphered when it is stored (e.g., the tail part of article and term II.C. in Figure 10). This means that if a new SLA is signed, the user has already acknowledged this and for the SPs, the relevant legal problems can be avoided.

In summary, these are designed based on the practical concerns. The terms in the new SLA which matches these concerns are a compromise between efficiency and security, when the proposed MSBM model is to be applied.

5.3 Validation and System Prototyping

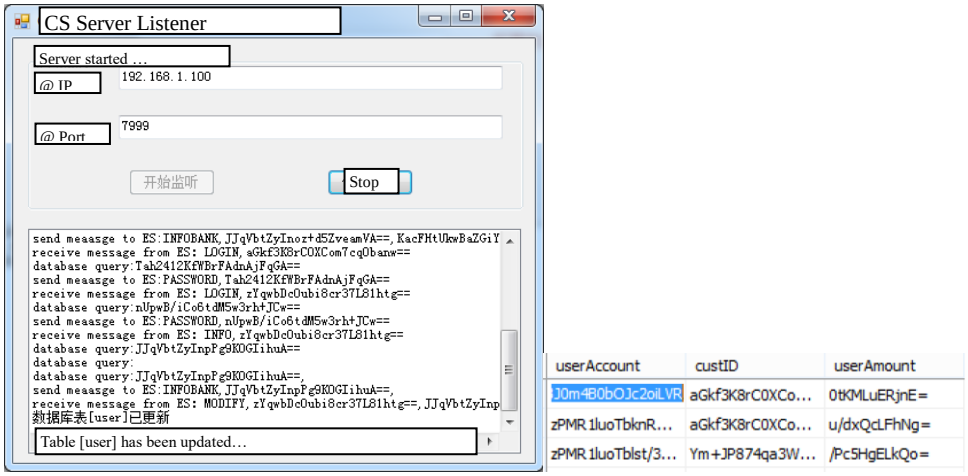
To validate the proposed MSBM model, a prototype system which simulates the interactions of the three separated services for the e-banking service are implemented in C# with Microsoft Visual Studio. The system is still under developing. Some screenshots are captured and shown in Figure 11. Note that for better presentation, without losing the meanings, in the figures some displayed Chinese words are overwritten by the corresponding English terms, as shown in the text boxes.

(a) User-side software interface and login



(b) ES server

(c) CS server



(d) Database snapshot: customer-account mapping (user table) and CS-side modification

Figure 11: Screenshots of the prototype system.

6. Conclusion

This paper advocates separating both the crypto and the cipher-storage sub-services out from the main service (being two independent services operated by other third-party SPs) and proposes the MSBM business model to reorganize or provision a security-enabled cloud service (Sub section 3.1). The model takes the 'AS-aaSS, ES-aaSS and CS-aaSS' approach, which is derived from two existing 'CS-aaSS (and AS-ES-aaS)' and 'ES-aaSS (and AS-CS-aaS)' approaches (3.2). Some immediate advantages and the relevant changed/unchanged matters upon taking this model were examined and outlined in 3.1, while the security/privacy enhancements of the model over the existing approaches were proved in a progressive and cogent manner in 3.3. As such, the possible threats, i.e., winner-takes-all and privileged-individual theft (2.3), are mitigated, and therefore, the improper user data disclosure risk and the privacy of the sensitive user profile (2.2) are alleviated and preserved. These are reflexive to some security issues in the data management field of cloud computing [42].

In particular, the idea of isolating crypto service (ES) is readdressed and designed, because such idea lacks a scrutiny after it was proposed. In the ES, user keys are only hold by the ES program during an active session, while the other keys are secured carefully. If there is any improper disclosure risk on the ES side, let us say that with MSBM, a privileged individual of the ES operator would still be able to look inside the memory for the decrypted plain data. However, it should be difficult to recover full information from the piecewise plain jigsaws.

With the proposed model, the role of the cipher-storage service (CS) is also redefined. Because CS does not store any key, this again alleviates the improper disclosure risk of user data: when the CS is vulnerable, only ciphered data without keys are present (to the outside adversary or the internal theft)! In addition, storing the part of sensitive user profile information (e.g., the user-account association table) in the CS can also mitigate the two possible kinds of threat (due to any vulnerability of AS or CS).

Future works include the full implementation of the MSBM model to the e-banking case, the reapplication of the model to other security-sensitive cloud services (than e-banking) and a better design compromise to satisfy the efficiency criterion without decreasing the privacy protection level.

Appendix 1: Modern Cryptography Methods

Modern cryptography lends supports to the relevant information security measures taken by the companies. It ensures confidentiality of the stored data. It ensures the authenticity of the negotiating parties, the integrity of the transmitted information and the non-repudiation of the communication behaviours or transactions made.

Symmetric cryptography and asymmetric cryptography are the two main streams of studies. *Symmetric cryptography* involves using a shared key for both encryption and decryption and is thus adequate for efficiently dealing with the session contents, which is to be ciphered and deciphered [35].

Asymmetric cryptography involves a pair of exchangeable public and private keys [16][25]. But since the algorithms usually take longer time for encryption and decryption, it is often used to transmit the symmetric key and the parameters of a session, in a secure manner. With the use of digital certificate and digital signature, data integrity and confidentiality can be guaranteed and the authenticity of the remote party can be validated. Besides, a made transaction or communication session cannot be denied.

Another effort of modern cryptography is *password security*. Many improved password

mechanisms have been proposed and applied to modern information systems. One of them is the popular challenge and response scheme [29]. One-time password is the other scheme [13][26] and SMS-based one-time password (SMS OTP) has been increasingly popular for the e-banking service [19].

Modern cryptography has been widely applied for e-commerce (EC). In EC, to transfer the data securely and to negotiate safely, both a secure client/server channel and a deliberately designed protocol to ensure a transaction flow for all parties to rely upon are both required. Relevant standards such as SSL and SET have been utilized [7]. For example, most banks are offering e-banking service now and have become e-banking SPs. They use SSL to realize a confidential user-assess channel and ensure that the data being transferred is neither corrupted nor lost (i.e., integrity). They also use SET to ensure the holistic transaction flow among the multiple banks/user/shop parties. Besides, they always keep their security protocols up to the standard [9]. In other words, modern cryptography has, already, done a lot: it would be difficult to recover the plain text from the cipher without the decryption key. In addition, it has ensured a secure access channel from a user client to the SP. Moreover, it has ensured a safe flow among multiple transaction parties.

Acknowledgment

We have utmost respect for Prof. Dr. Jing-Jang Hwang, who passed away on March 2015. He coached all authors of this study, either directly or indirectly. In 2011, he initiated the foremost idea to isolate the encryption/decryption service out from a main service. The concept of this study, which is the centrifuge of two security-relevant services in the cloud context, takes his idea. For this work, he also made considerable instructions when reviewing it in 2014 autumn.

We are grateful for the funding supports from National Science Council, Taiwan (project # NSC 99-2410-H-182-025-MY2), from UM Research Fund, Macau (project # CPG2015-00017-FST) and from Tri-service General Hospital Research and Planning Fund, Taiwan (project # TSGH-IM-R160228).

References

[1] A. Ajili, S. Salehi, K. Rezaei-Moghaddam, D. Hayati and F. Karbalaee, “Estimating the model of investigating attitude and intention in the usage of variable rate irrigation

technology," *American Journal of Experimental Agriculture*, vol. 2, no. 3, pp. 542–556, 2012.

[2] M. Baker, R. Buyya and D. Laforenza, "Grids and grid technologies for wide-Area distributed computing," *Software: Practice and Experience*, vol. 32, no. 15, pp. 1437-1466, 2002.

[3] R. Buyya, C.S. Yeo, S. Venugopal, J. Broberg and I. Brandic, "Cloud computing and emerging IT platforms: vision, hype and reality for delivering computing as the 5th utility," *Future Generation Computer Systems*, vol. 25, no. 6, pp. 599-616, 2008.

[4] N. G. Carr, "IT doesn't matter," *Harvard Business Review*, vol. 81, no. 5, pp. 41-49, 2003.

[5] P. Chen, "The entity-relationship model — Toward a unified view of data," *ACM Transactions on Database Systems*, vol. 1, no. 1, pp. 9-36, 1976.

[6] W. Dou, X. Zhang, J. Liu and J. Chen, "HireSome-II: Towards privacy-aware cross-cloud service composition for big data applications," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 2, pp. 455-466, 2015.

[7] A. Elgohary, T.S. Sobh and M. Zaki, "Design of an enhancement for SSL/TLS protocols," *Computers & Security*, vol. 25, no. 4, pp. 297-306, 2006.

[8] S. K. Garg, S. Versteeg and R. Buyya, "A framework for ranking of cloud computing services," *Future Generation Computer Systems*, vol. 29, no. 4, pp. 1012-1023, 2013.

[9] N. Hawthorn, "Finding security in the cloud," *Computer Fraud & Security*, vol. 2009, no. 10, pp. 19-20, 2009.

[10] J. J. Hwang, Y.C. Hsu, C.H. Wu and H.K. Chuang, "A business model for cloud computing based on a separate encryption and decryption service," *in Proc. 2011 International Conference on Information Science and Applications (ICISA)*, pp. 1-7.

[11] M. Jahanirad, Y. AL-Nabhani and R.M. Noor, "Comprehensive network security approach: security breaches at retail company – A case study," *International Journal of Computer Science and Network Security*, vol. 12, no. 8, pp. 107–112, 2012.

[12] J. Kim, P.J. Bentley, U. Aickelin, J. Greensmith, G. Tedesco and J. Twycross, "Immune system approaches to intrusion detection - A review," *Natural Computing*, vol. 6, no. 4, pp. 413-466, 2007.

[13] L. Lamport, "Password authentication with insecure communication," *Communications of the ACM*, vol. 24, no. 11, pp. 770-772, 1981.

[14] P. McFedries, "The Cloud is the Computer," *IEEE Spectrum, Online Electronic Magazine*, http://spectrum.ieee.org/computing/hardware/the-cloud-is-the-computer, (2008).

[15] P. Mell and T. Grance, "The NIST definition of cloud computing," *NIST Institute of Standards and Technology Special Publication*, no. 800-145, 2011.

[16] V. Miller, "Uses of elliptic curves in cryptography," in *Lecture Notes in Computer Science (Advances in Cryptology - CRYPTO '85)*, vol. 218, pp. 417-426, 1986.

[17] V. Nallur and R. Bahsoon, "A decentralized self-adaptation mechanism for service-based applications in the cloud," *IEEE Transactions on Software Engineering*, vol. 39, no. 5, pp. 591-612, 2013.

[18] S. Nevo and M.R. Wade, "The formation and value of IT-enabled resources: Antecedents and consequences of synergistic relationships," *MIS Quarterly*, vol. 34, no. 1, pp. 163-183, 2010.

[19] R. Oppliger, R. Rytz and T. Holderegger, "Internet banking: client-side attacks and protection mechanisms," *IEEE Computer Security*, vol. 42, no. 6, pp. 27-33, 2009.

[20] N. Opitz, T.F. Langkau, N.H. Schmidt and L.M. Kolbe, "Technology acceptance of cloud computing: Empirical evidence from German IT departments," *in Proc. 45th Hawaii International Conference on System Sciences (HICSS 2012)*, pp. 1593-1602.

[21] A. Parakh and S. Kak, "Online data storage using implicit security," *Information Sciences*, vol. 179, no. 19, pp. 3323-3333, 2009.

[22] P. Peter and O. Ekabua, "Implementation of novel accounting, pricing and charging models in a cloud-based service provisioning environment," *in Proc. International Conference on Electrical and Electronics Engineering, Clean Energy and Green Computing 2013 (EEECEGC'13, The Society of Digital Information and Wireless Communication)*, pp. 1-9.

[23] F.A.P. Petitcolas, R.J. Anderson and M.G. Kuhn, "Information hiding – A survey," in *Proceedings of the IEEE (1999, special issue on protection of multimedia content)*, vol. 87, no. 7, pp. 1062 -1078.

[24] C. Rong, S.T. Nguyen and M.G. Jaatun, "Beyond lightning: A survey on security challenges in cloud computing," *Computers and Electrical Engineering*, vol. 39, pp. 47-57, 2013.

[25] R. 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, 1978.

[26] RSA Laboratories, "PKCS #11 V2.3 Cryptographic token interface standard," *RSA Security Inc. Publication*, 2009.

[27] Salesforce.com Inc., "Force.com platform," http://www.salesforce.com/tw/ (2010)

[28] SAP AG, "SAP services: maximize your success," http://www.sap.com/services/index.epx (2010)

[29] B. Schneier, *Applied Cryptography (2nd ed.)*, John Wiley & Sons, New York, 1996.

[30] M. Sookhak, A. Gani, M. K. Khan and R. Buyya, "Dynamic remote data auditing for

securing big data storage in cloud computing," *Information Sciences*, available online 10 Sep 2015. (doi: 10.1016/j.ins.2015.09.004)

[31] M. Sookhak, H. Talebian, E. Ahmed, A. Gani and M. K. Khan, "A review on remote data auditing in single cloud server: Taxonomy and open issues," *Journal of Network and Computer Applications*, vol. 43, pp. 121 – 141, 2014.

[32] R. Sterritt, "Autonomic computing," *Innovations in Systems and Software Engineering*, vol. 1, no. 1, pp. 79-88, 2005.

[33] S. Subashini and V. Kavitha. "A survey on security issues in service delivery models of cloud computing," *Journal of Network and Computer Applications*, vol. 34, no. 1, pp. 1-11, 2011.

[34] The Identity Theft Resource Center, "2008 data breach totals soar," *ITRC Surveys & Studies*, 2009.

[35] US National Institute of Standards and Technology, "Advanced encryption standard," *Federal Information Processing Standard (FIPS) Publication*, no. 197, 2001.

[36] L.M. Vaquero, L. Rodero-Merino, J. Caceres and M. Lindner, "A break in the clouds: Towards a cloud definition," *ACM SIGCOMM Computer Communication Review*, vol. 39, no. 1, pp. 50-55, 2009.

[37] C. Weinhardt, A. Anandasivam, B. Blau, N. Borissov, T. Meinl, W. Michalk and J. Stößer, "Cloud computing: a classification, business models, and research directions," *Business & Information Systems Engineering*, vol. 1, no. 5, pp. 391-399, 2009.

[38] M. Whaiduzzaman, M. Sookhak, A. Gani and R. Buyya, "A survey on vehicular cloud computing," *Journal of Network and Computer Applications*, vol. 40, pp. 325 – 344, 2014.

[39] H. Yang, T. Li, X. Hu, F. Wang, and Y. Zou, "A survey of artificial immune system based intrusion detection," *The Scientific World Journal*, Art. No. 156790, 2014. (doi: 10.1155/2014/156790)

[40] C.S. Yeo, S. Venugopal, X. Chu and R. Buyya, "Autonomic metered pricing for a utility computing service," *Future Generation Computer Systems*, vol. 26, no. 8, pp. 1368-1380, 2009.

[41] Z.M. Yusop and J. Abawajy, "Analysis of insiders attack mitigation strategies," *Procedia—Social and Behavioral Sciences*, vol. 129, pp. 581-591, 2014

[42] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," *Future Generation Computer Systems*, vol. 28, no. 3, pp. 583-592, 2012.

Biography

本篇論文承蒙方主編之邀稿，謹此致謝。文中內容若有不周之處，敬請見諒。最後感謝讀者的寶貴時間，請隨時不吝提出建議以便改進。