Adaptive and Dynamic Mobile Phone Data Encryption Method using Adaptive encryption algorithm selection and key generation

[1]**ASHOK BABU,** *Gandhi Institute of Excellent Technocrats, Bhubaneswar, India*
[2]**SNEHA JAISWAL,** *Gurukula Institute of Technology, Bhubaneswar, Odisha, India*

Abstract: To enhance the security of user data in the clouds, we present an adaptive and dynamic data encryption method to encrypt user data in the mobile phone before it is uploaded. Firstly, the adopted data encryption algorithm is not static and uniform. For each encryption, this algorithm is adaptively and dynamically selected from the algorithm set in the mobile phone encryption system. From the mobile phone's character, the detail encryption algorithm selection strategy is confirmed based on the user's mobile phone hardware information, personalization information and a pseudo-random number. Secondly, the data is rearranged with a randomly selected start position in the data before being encrypted. The start position's randomness makes the mobile phone data encryption safer. Thirdly, the rearranged data is encrypted by the selected algorithm and generated key. Finally, the analysis shows this method possesses the higher security because the more dynamics and randomness are adaptively added into the encryption process.

Key words: data encryption; mobile phone; cloud storage; pseudo-random number

I. Introduction

Nowadays, the mobile communication is the fastest growing industry in most countries in the world and plays an important role in daily life of people. Besides, using mobile phones for the fundamental telecommunication service such as voice and message service, more and more mobile users are employing their mobile phones to take pictures, record videos, even record their lives anywhere anytime because of the rapid function enhancement of the mobile intelligent terminal. Therefore, a mass of data is generated in user's mobile phone at all times. Although the local storage ability of mobile device has had a huger improvement than ever, it cannot meet the storage need of the mobile users. Cloud computing and wireless communication technique supply mobile users the ability to store remotely their data in the clouds to solve the above problem to perfection. This means that mobile users can upload and download their data in the clouds anytime and anywhere. In fact, it is equivalent to make the local mobile device possess the enhanced storage and computing ability on demand.

Although cloud storage brings convenience to mobile users, at the same time brings the certain risk to the security of their data because keeping data in the clouds means users will have to surrender the control of their data. The data security and confidentiality will completely be dependent on the cloud service provider. However, cloud service provider may not prevent the unauthorised access to the data. So it is essential and necessary to adopt the effective method to ensure the mobile user data security and privacy. Generally, there are two ways to guarantee user's data not to be spoiled: one is to encrypt user data by some popular encryption algorithms or standards [1-3] in user mobile terminal, the other is to enhance the safety of the storage devices in the clouds by all kinds of security mechanisms such as firewalls, virtual private networks and other security policies and technical ways [4-6]. But mobile user usually prefers to believe in himself than the cloud service provider for his private data security issue. Especially for an unreliable cloud service provider, it is the natural and safe way to encrypt the user confidential data in the user mobile device before uploading them to the clouds.

Encryption is the process of transforming the mobile user's useful and confidential data to the data which others cannot understand without the corresponding decryption algorithm and key. For protecting the data security, scientists had proposed lots of high-performance encryption algorithms based on the different purposes and application fields. Meanwhile, for acquiring the illegal profit, crackers from all over the world try to research the corresponding cracking algorithm to spy out mobile users' confidential data.

With the fast development of the mobile communication and intelligent mobile phone, the research about the data encryption becomes the current hotspot in mobile communication field. In the mobile phone data, there is lots of data containing some important information which the mobile user does not hope that the data is acquired or known by someone else, such as some important business files, some financial data or some privacy pictures. As usual, they are stored in a binary format on the mobile phone storage equipment. Especially for the private data generated by the mobile users in their mobile devices, scientists proposed a variety of effective encryption methods to protect them. Rohollah Karimi and Mohammad Kalantari proposed a location-based data encryption algorithms to make sure the cipher-text can only be decrypted when the coordinate acquired from GPS receiver matches with the target coordinate [7-8]. In Ref. [9], the algorithm "Elliptic Curve Cryptography for Image Encryption" was introduced to protect the image from unauthorised access. An efficient signature-encryption scheme tightly related to the trapdoor permutation in the random oracle models was proposed in Ref. [10] to ensure mobile user data safety. In addition, the self-encryption scheme for data security in mobile device [11] was also presented to complete mobile user data encryption.

Although the above methods solve many problems to some extent in data encryption for mobile phones, they usually make use of the certain encryption algorithm to prevent the confidential data of mobile user from being decrypted. For all users, the encryption algorithms in these encryption systems of the mobile phones are static, uniform and invariant. This decreases the difficulty to decrypt the users' private data and results in a low safety for the mobile phone encryption system. For this reason, this paper designed an adaptive data encryption method for mobile user. By choosing adaptively the encryption algorithm based on the mobile phone personalization information and adding more randomness into the encryption process, the encryption intensity is highly enhanced. Moreover, the risk in cracking the data is greatly decreased.

The rest of the paper is organised as follows. Section II presents the adaptive encryption method for the user data of mobile phone. Section III provides the performance analysis of the data encryption method. Section IV concludes the paper with a discussion of the implications of the work.

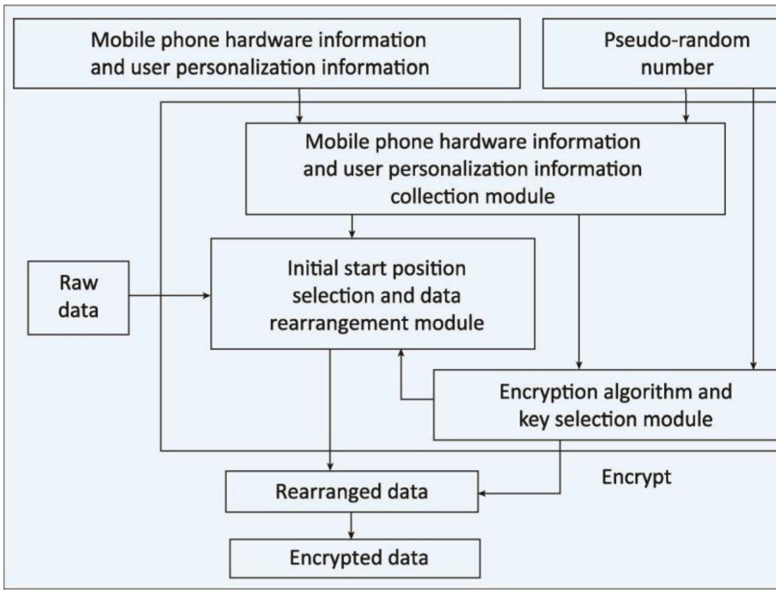
Mobile phone hardware information and user personalization information
Pseudo-random number
Mobile phone hardware information and user personalization information collection module
Raw data
Initial start position selection and data rearrangement module
Encryption algorithm and key selection module
Encrypt
Rearranged data
Encrypted data

Fig.1*The general function block diagram of the encryption method*

Table I*Notation table*

Symbol	Definition
U	The user's personalised information data
H	The mobile phone hardware information data
R	Pseudo-random number
A	The encryption algorithm ID in the algorithm set
K	The encryption key
P	The initial realignment position
N	The bits number of the encrypted data
M	The number of all algorithms in the encryption algorithm set
L	The biggest value of the encryption key
S	The bits number of the encryption key
F_R□$U\ H\ R,$, □	The user's personalized information data extraction function
V	The output value of F_R□$U\ H\ R,$, □
F_A□ □V	The encryption algorithm selection function
F_K□V□	The encryption key generation function
F_P□V□	The realignment initial start position selection function
P	The realignment initial start position
D_o	The user original data

D_r	The rearrangement data
F_r □$D\ V\ P_o$, , □	The rearrangement function
F_s □$A\ K\ D$,, $_r$ □	The encryption function
D_s	The data which had been encrypted
e	The selected encryption algorithm cracking computation cost
e_n	The encryption system's new cracking computation cost

II. Proposed Encryption Method

In this section, the proposed encryption method for the user data protection of mobile phone is presented. The system is installed on the mobile user's smartphone, and is composed from three main modules. The function block diagram is shown in Figure 1.

Mobile phone hardware information and user personalization information collection module is responsible for extracting the user's mobile phone hardware and personalization information from the user's smartphone. The detail extraction strategy is based on the input pseudo-random number which is randomly produced by the user mobile phone when the user makes an encryption request.

Initial start position selection and data rearrange module is responsible for looking for the initial start position for realignment based on the output from the user's mobile phone hardware information and user personalizationinformation collection module and encryption algorithm and key selection module.

Encryption algorithm and key selection module is responsible for dynamically and adaptively selecting the encryption algorithm and generating the encryption key based on the output from the mobile phone hardware information and user personalization information collection module and the input pseudo-random number.

All the symbols used in this paper are given in Table I.

2.1 Adaptive encryption algorithm selection and key generation

In this section, the adaptive encryption algorithm selection and key generation method is presented based on the mobile phone hardware information, user personalization information and pseudo-random number.

An obvious fact is that the illegal decryption will be very difficult when crackers do not know which encryption algorithm has been adopted. Therefore, for the encryption system of mobile phone, a series of high-performance encryption algorithms are in advance added into the encryption algorithm set. For ensuring the security, the different user's mobile phone has the different encryption algorithm ID for the same encryption algorithm in the encryption algorithm set. This ensures others cannot guess the adopted encryption algorithm even though the encryption algorithm ID for certain user's mobile phone is known. Meanwhile, with the constant appearance of new high-performance encryption algorithms, the encryption algorithm set will be further enriched and the difficulty in illegally decrypting the user data will be further increased.

When there are the data to be encrypted, the encryption algorithm will be adaptively and dynamically selected from the encryption algorithm set based on the mobile phone hardware information, user personalization information and a pseudo-random number. Similarly, the encryption key is also generated based on the above information.

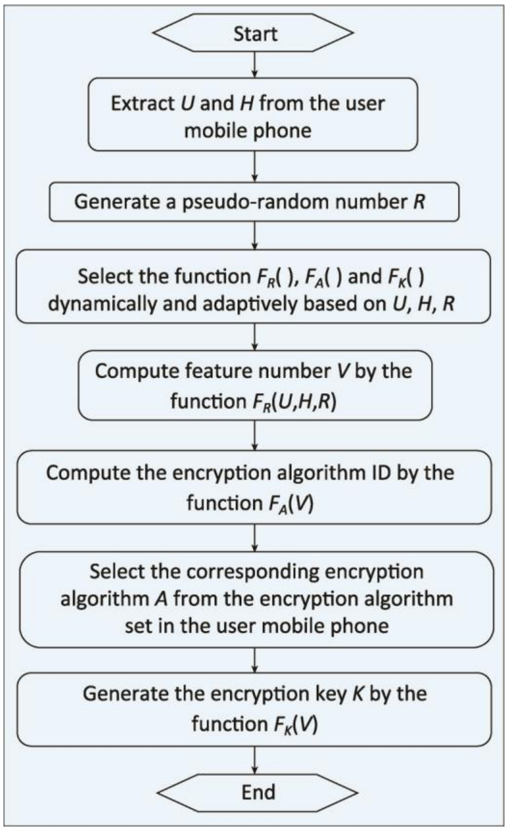
Start
Extract U and H from the user mobile phone
Generate a pseudo-random number R
Select the function F_R( ), F_A( ) and F_K( ) dynamically and adaptively based on U, H, R
Compute feature number V by the function F_R(U,H,R)
Compute the encryption algorithm ID by the function F_A(V)
Select the corresponding encryption algorithm A from the encryption algorithm set in the user mobile phone
Generate the encryption key K by the function F_K(V)
End

Fig.2*The encryption algorithm selection and key generation flow chart*

Here, V, which describes this time the encryption feature number for the user and his mobile phone, is the output value of function F_R □$U\ H\ R$, , □ . U is denoted as user’s ID and password, H is defined as mobile phone’s IMEI and IMSI number, R is a pseudo-random number, then have Eq. (1)

$$V F U H R\square _R \square , \qquad , \square \qquad (1)$$

For the convenience and security, here,

$F_R \square U\ H\ R, \ , \ \square$ is a function randomly selected from a series of functions which are designed to generate the different output value when there are the different input value of U, H and R. This ensures in a certain encryption process, the different mobile phone, different user or different encryption task will all produce the different feature number V.

Meanwhile, to add the difficulty of the illegal decryption, the encryption function is various for each encryption. The certain function $F_R \square U\ H\ R, \ , \ \square$can be defined or randomly selected in a serial of different functions.

For example, $V\ F\ U\ H\ R\square \ _R \square \ , , \ \square$may be defined as a certain 4-dimensional space curve. Certainly, $F_R \square U\ H\ R, \ ,$ $\square$may be defined as different function according to the different role or situation.

$F_A \ \square V \square$ and $F_K \ \square V \square$are randomly selected from a series of functions which are designed to generate the different output value when there are the different input value just like $F_R \square U\ H\ R, \ , \ \square$. So for the different V, F_A $\square \ \ \square V$ and $F_K \square V \square$ will have the different output value according to Eqs. (2) and (3),

$$A\square ^{F\ V}{}_A \square \ \square \qquad (2)$$

$$K\square ^{F\ V}{}_K \square \ \square \qquad (3)$$

Similarly, the function $F_A \ \square V \square$and $F_K \ \square V \square$, can be defined or randomly selected. For example, they may be defined as 2-dimensional space curve. The encryption algorithm selection flow chart is shown in Figure 2.

By the above ways, for each encryption of the different mobile user, the encryption algorithm and key are completely different and unpredictable because they are dynamically and adaptively decided. And, more randomness is added into the encryption process. At last, the encryption intensity of the system is highly enhanced and the risk in illegally cracking the data is greatly decreased.

2.2 Random initial start realignment position selection and data realignment

In this section, the random initial start realignment position selection and data realignment strategy based on the mobile phone hardware, user personalization information and a pseudo- random number are presented.

$$P\ F\ V\square \ _P \square \ \square \qquad (4)$$

$F_P \square V \square$ can be defined just like the function

$F_A \ \square V \square$ and $F_K \ \square V \square$. After that, every S bits data is rearranged based on the mobile phone hardware information, user personalization information and the pseudo-random number. Repeat the above rearrangement process until all data are rearranged. For N bits data, according to the original user data D_o, rearrangement data

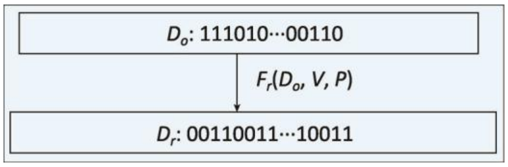

Fig.3*The rearrangement function block diagram*

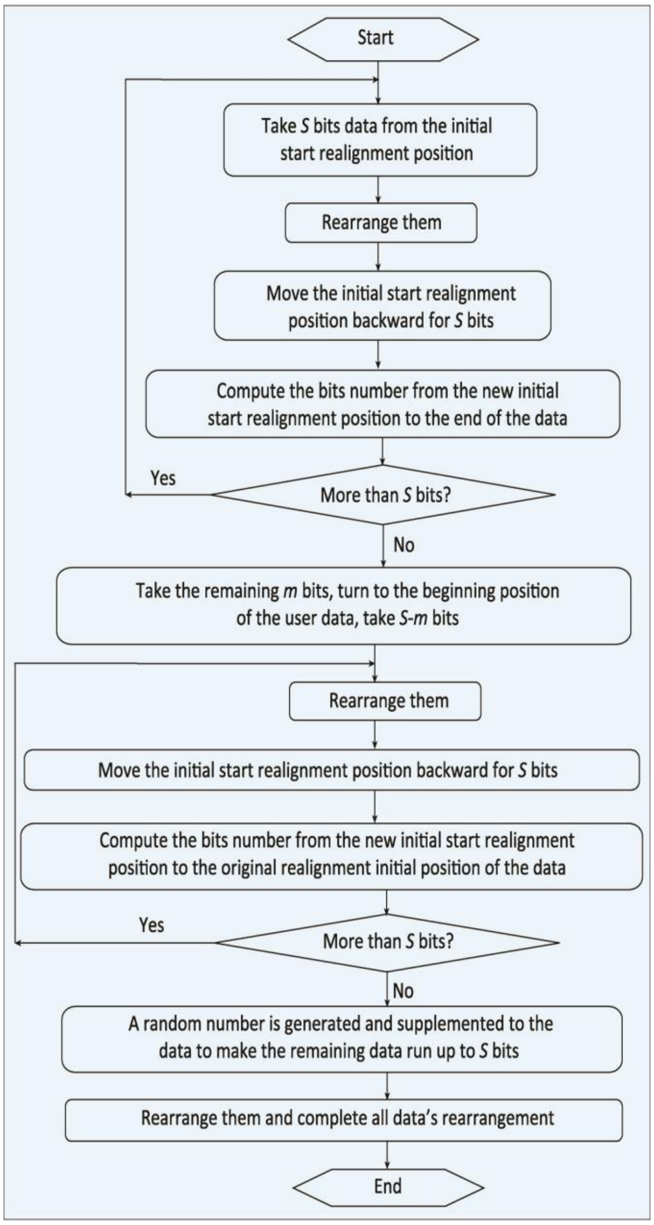
Start
Take S bits data from the initial start realignment position
Rearrange them
Move the initial start realignment position backward for S bits
Compute the bits number from the new initial start realignment position to the end of the data
Yes
More than S bits?
No
Take the remaining m bits, turn to the beginning position of the user data, take S-m bits
Rearrange them
Move the initial start realignment position backward for S bits
Compute the bits number from the new initial start realignment position to the original realignment initial position of the data
Yes
More than S bits?
No
A random number is generated and supplemented to the data to make the remaining data run up to S bits
Rearrange them and complete all data's rearrangement
End

Fig.4*The rearrangement flow chart*

D_r, and the rearrangement function F_r□D_o, V P, □ , we have Eq. (5),

$$D_r \square F\ D\ V\ P_r \square\ {}_o, \qquad (5)$$

According to different V and P, the special rearrangement algorithm is selected from a series of known rearrangement algorithms. The

rearrangement function block diagram is shown in Figure 3.

Firstly, the rearrangement process starts from the selected realignment initial start position, then rearranges and moves on subsequently. When the bits number of the remaining data to the end of the original data is less than S, the rearrangement process will turn to the beginning position of the original data. Then, continue the above rearrangement process until the bits number of the remaining data to the original realignment initial start position of the data is less than S. A random number is supplemented to make the remaining data run up to S bits to complete all user data's rearrangement. The detail rearrangement flow chart is shown in Figure 4.

2.3 Encrypting the rearranged data

In this section, the user data which is rearranged in advanced is encrypted using the above selected encryption algorithm.

For the rearrangement data D_r, according to the above selected encryption algorithm ID A, generated encryption key K, then we have Eq. (6),

$$D_s \square F\ A\ K\ D_s \square\ ,, \qquad {}_r \square \qquad (6)$$

Because more dynamics and randomness are introduced in the encryption process, the encrypted data D_s is very difficult to be cracked illegally.

III. Performance Analysis

In this section, the security performance of the proposed mobile phone data encryption method is analysed.

In this proposed encryption method, the system's security is greatly improved by the following four robust measures. These measures are respectively the uncertain high-performance encryption algorithm selection and adoption, the dynamic and adaptive encryption algorithm selection and encryption key generation, the realignment initial start position random selection and the adaptive data rearrangement tactics.

Firstly, the user data is encrypted not by the uniform and fixed encryption algorithm, but by certain a selected dynamic and adaptive encryption algorithm from the high-performance encryption algorithm set of the user mobile phone encryption system for each encryption.

□

The illegal decryption will be very difficult if crackers do not know which encryption algorithm has been adopted when the new high-performance encryption algorithms are introduced, the encryption algorithm set will be further enriched. With the constant growth of the encryption algorithm set, the difficulty in illegally decrypting the user confidential data will greatly be increased.

Secondly, the different user's mobile phone has the completely different encryption algorithm ID for the same encryption algorithm in their encryption algorithm sets.

And the encryption algorithm is dynamically and adaptively selected from the encryption algorithm set based on the mobile phone hardware information, user personalization information and a pseudo-random number. The adopted encryption algorithm by user mobile phone cannot be known by crackers because the above personalization data which the encryption algorithm is selected based on is distinct for the different mobile phone or different user or different encryption.

Thirdly, the data's initial start realignment position is not placed on the just beginning position of the user data as usual, but a random position which is decided based on the mobile phone hardware information, user personalization information and a pseudo-random number. Because the more randomness is added into the encryption process, the cost of the illegal decryption is further increased.

Fourthly, the data are rearranged not based on the fixed or static ordering strategy, but based on the special personalization information and varied pseudo-random number which is completely distinct for different mobile phones or different user or different encryption.

At last, quantitatively suppose there are M algorithms in the mobile phone encryption set, and the selected encryption algorithm's cracking computation cost is e, the possible start encryption position choice has N locations. Then, the new cracking computation cost e_n of the system's encryption algorithm is:

$$e_n \square e N \square \qquad (7)$$

The illegally decryption algorithm total computation cost is heightened N times. Moreover, the cracker will have to guess the exactly accurate algorithm from M algorithms. This is a small probability event when the value of M is very large. Especially, the value of M will be increased when some new good encryption algorithms are continuously added into the mobile encryption system. These means make crackers more difficult to extract privacy information from the mobile user data.

By the above measures, the more dynamics and randomness in the encryption process make this encryption method possess the higher complexity. At the same time, the algorithm overhead has no an apparent increment compared with the traditional fixed mobile phone encryption method because the encryption algorithm's dynamic selection dose not add the computing complexity of the selected encryption algorithm itself. In the same way, the data rearrangement algorithm's computing complexity does not increase even though the initial start realignment position random selection highly enhances the cost in illegally decrypting the data.

IV. Conclusion

In this paper, a method for the user data encryption in the mobile phone was provided, and three steps to realise this method were proposed. In addition to guaranteeing effectiveness, this method is safer than similar solutions in terms of the data decryption complexities because there are more randomness and dynamics introduced in the encryption process. The extensive performance analysis and evaluation demonstrate that the proposed privacy-preserving schemes are well suited to mobile phone user data encryption. Moreover, with the constant appearance of the new encryption algorithms, the encryption strength of the proposed encryption method will be increased by adding them into this encryption algorithm library of this encryption method. The encryption effective will also be heightened with the fast performance improvement of the mobile phone.

References

[1] RIVEST R. RFC 1321. The MD5 Message Digest Algorithm[S], 1992.

[2] DAEMEN J, RIJMEN J. The Design of Rijndael [M]. Berlin: Springer, 2002.

[3] KOBLITZ N, MENEZES A, VANSTONE S. The State of Elliptic Curve Cryptography[J]. Design, Codes, and Cryptography□Special Issue on Towards a Quarter-Century of Public Key Cryptography, 2000, 19(2-3): 173-193.

[4] MOLNAR D, SCHECHTER S. Self Hosting vs. Cloud Hosting: Accounting for the Security Impact of Hosting in the Cloud[C]// Proceedings of Workshop on the Economics of Information Security (WEIS 2010): June 7-8, 2010. Harvard University, MA, USA, 2010.

[5] CSA: Cloud Security Guide. Tech. Rep., Cloud Security Alliance[EB/OL]. [2009-04]. http://www.cloudsecurityalliance.org/csaguide.pdf.

[6] ENISA: Cloud Computing: Benefits, Risks and Recommendations for Information Security. Tech Rep., European Network and Information Security Agency[EB/OL]. [2009-11-20]. http://enisa.europa.eu.

[7] LIAO H C, LEE P C, CHAO Y H, *et al.* A Location- Dependent Data Encryption Approach for Enhancing Mobile Information System Security [C]// Proceedings of the 9th International Conference on Advanced Communication Technology: February 12-14, 2007. Gangwon-Do, Korea, 2007: 625-628.

[8] LIAO H C, CHAO Y. H. A New Data Encryption Algorithm Based on the Location of Mobile Users[J]. Information Technology Journal, 2008, 7(1): 63-69.

[9] SHANKAR T N, SAHOO G, NIRANJAN S. Image Encryption for Mobile Devices[C]// Proceedings of 2010 IEEE International Conference on Communication Control and Computing Technologies (ICCCCT): October 7-9, 2010. Ramanathapuram, India, 2010: 612-616.

[10] BAO Haiyong, WEI Guiyi, SHAO Jun, *et al*. Efficient Signature-Encryption Scheme for Mobile Computation[C]// Proceedings of 2011 International Conference on System Science and Engineering (ICSSE): June 8-10, 2011. Macao, China, 2011: 390-393.

[11] GASTI P, CHEN Yu. Breaking and Fixing the Self Encryption Scheme for Data Security in
Mobile Devices[C]// Proceedings of 2010 18th Euromicro Conference on Parallel, Distributed and Network-Based Processing (PDP): February 17-19, 2010. Pisa, Italy, 2010: 624-630.