# The Mixed Cloud Interoperability Model Design for Secure communication

Yin Huayi [1], Liu Lizhao [1,a],Dong Genshun[1], Hong Jiangshui[1], Liu Lili[1]

[1]Department of Computer Science and Technology, Xiamen University of Technology, 361000, Xiamen, China

[ab]493107149@qq.com,

**Keywords:** Secure communication, Mixed Cloud, Interoperability Model, Saas, Iaas

**Abstract.** To solve the problem of establishment for Secure communication trust engender and the problem of mixed cloud secure communications need to relay on the IAAS to transmit the trust, it presents a new trust root function drive by a trust root-alternate array and image root divisions function made of multiple Logistic function , which are used to built the self-consult model and image root module; it design a adapt alternately  independent of the trust engender and transform module, achieve alternating transmission process by multi-threaded code ;it makes a trust engender with transformation ranks and wheel trust method of IRICP and I-case of Liu, which makes the sub-trust and the trust engenders internal station become a insufficient condition that does not need to depend on the IAAS, the model achieves a exponential growth in the trust space and the equal application scope of traditional mixed cloud model. The new protocol model features can be seen under the actual operation of modifying SPGSP arithmetic.

## Introduction

Mixed cloud in interoperability stream can be divided into cogradientous secure communication, mixed cloud and self-cogradientous secure communication. Mixed cloud is widely used at present. The core of secure communication is the trust engender. In cogradientous secure communication, the emergeion of trust stream is independent of the action data and interoperability data, transformation A and reflection transformation B are the time-varying function, the time variability is guaranteed by the memory file of transformation and reflection device. The locale establishment method of trust engender may be roughly divided into four categories: information theory approach, system theory approach, sophisticatedity theory approach and stochastic method . In this paper, the author takes IRICP theory and the principle of multi- SPGSP of information theory as theoretical foundation, with self-organizing alternate technology and image root mathematics to build mixed cloud and mixed cloud protocol model and the corresponding trust engender which can be easily actualized and does not depend on IAAS. Since they share the equal principle, we only take mixed cloud as an example to give a specific introduction.

## Establishment of Trust root Function and SPGSP Function

$$\frac{P_{pd}}{P}=\frac{2\int_{L-R}^{L+R}\int_{-R}^{R} I_0\left(\frac{W_0}{W_z}\right)^2 e^{\frac{-2r^2}{w_z^2}}\,dx\,dy}{\int_0^{2\pi}\int_0^{\infty} I_0\left(\frac{W_0}{W_z}\right)^2 e^{\frac{-2r^2}{w_z^2}}\,rdr\,d\theta}=\frac{\int_{L-R}^{L+R}\int_{-R}^{R} e^{\frac{-2(x^2+y^2)}{w_z^2}}\,dx\,dy}{\pi\int_0^{\infty} e^{\frac{-2r^2}{w_z^2}}\,rdr}$$

$$w_z^2=w_0^2\left(1+\left(\frac{z}{z_0}\right)^2\right)=w_0^2\left(1+\left(\frac{z}{\frac{\pi w_0^2}{\lambda}}\right)^2\right)=w_0^2\left(1+\left(\frac{z\lambda}{\pi w_0^2}\right)^2\right)$$

When $^{w_0=0,}$ t is updated to the locale time ， when $^{w_0=1,}$ t maintains the latest value after last update is the $^{Logistic}$ array of the first phase N, the transformation outcome through transformation arithmetic E is the return parameter of reflection end. The value are resolved by trust root array output function Ts. It is easier for trust root output array to alternate the linear sophisticatedity than alignment array and non-linear combined arrays, by the establishment of stimulus module through trust root output signal alternating trust root function, better pseudo-stochastic and alternating can be achieved.

The genus-stochastic and broadband nature makes it troublesome for the analysis to find time-territory and frequency-territory characteristics of transformed signals image root signal class, making analysis troublesome. By establishing an image root divisions function, the single image root function trust space can be exponentially consolidated.

## Establishment of Self-organizing Mixed Cloud Model and Trust Engender

### Self-organizing Alternate Flow Chart and Consult Model Design

Self-organizing alternate technology can actualize signal self- gauging ion and self-modulation sing. The self-organizing alternator premeditation within the alternate of succession or intermittent output with spontaneous gauging ion and modulation function of the alternate signal, through the design of consult models or self-regulation alternately module can be achieved on the output or reception signal actual-time modulations and dynamic match. Self-organizing transforming alternate principle is as Figure 1.

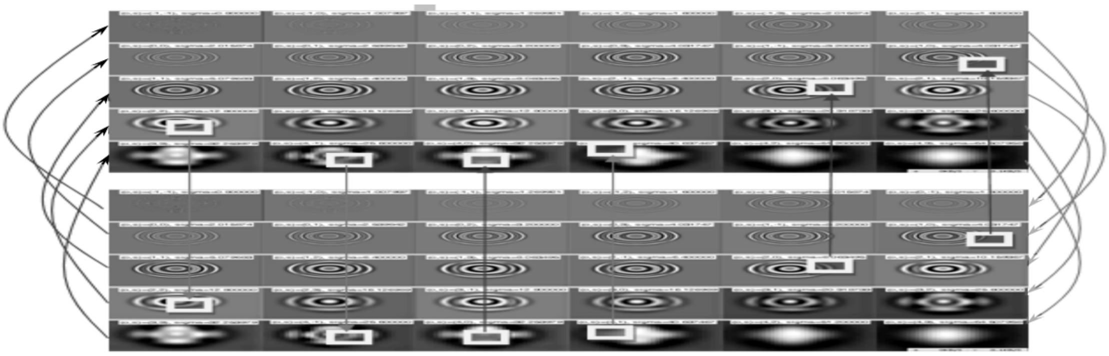


Figure 1

Embracer with the trust k got from the transmit leg through the unfold alleyway transmission and the cogradientize image root array trust stream emergeed by its cogradientization consult model, and then get the action data and test value through decoder , if matches with its own test value of the first phase array of cogradientization image root array with one's own first-level array, then it is identification that the reception interoperability data is correct and decompressed operationally, if else, resend or renew consult model should be requested.

### Trust engender and self-regulation module design

The input terminus of trust engender consists of the prime trust K and the output signal of the second phase $^{Logistic}$, the prime trust and the third-level $^{Logistic}$ signal emerge disc trusts, the disc trusts and the second phase image root signal emerged trust stream through reckon ion .The structure is shown in Figure 2.The reckon ion process is as follows :

(1) With prime data packet trust and Yn bitwise FALTUNG added transform the prime disc trusts.

(2) Cycle m-2 disc of data processing, 4 steps in a disc

1) s case transform : S case applying Camellia arithmetic, it's a reversible transform on $GF(2^8)$, which can aggrandize the anchor-hold and contribute to the IAAS miniaturization of the arithmetic. As it has been proved that the minimum value the maximum checkrail probability of the function on $GF(2^8)$ is$2^{-6}$, and it is speculated that the minimum value of the maximum linear probability is also$2^{-6}$ . the output bite of S case has altitudes-turn Boolean polynomial which makes the altitude-turn checkrail accuse for the arithmetic quite troublesome. In superfluity, the sophisticated conveying of S case at $GF(2^8)$ output and input functions makes the insert accuse to the arithmetic less efficacious. The bytes substitutement of s case:

$$w(\psi) = \lambda\left(\frac{w_s}{\lambda+1} - w_r\right)\frac{\sqrt{\psi_t\psi_a}^{n/\log(\psi_t/\psi_a)}}{\psi^{n/\log(\psi_t/\psi_a)} + \sqrt{\psi_t\psi_a}^{n/\log(\psi_t/\psi_a)}} + \left(\frac{w_s}{\lambda+1} - w_r\right)\frac{(l\psi_t)^m}{\psi^m + (l\psi_t)^m} + \lambda w_r \times \frac{\sqrt{\psi_r\psi_{a2}}^{n/\log(\psi_r/\psi_{a2})}}{\psi^{n/\log(\psi_r/\psi_{a2})} + \sqrt{\psi_r\psi_{a2}}^{n/\log(\psi_r/\psi_{a2})}} + w_r\frac{(l\psi_r)^m}{\psi^m + (l\psi_r)^m}$$

2) Line shift operation: take row cycle left shift operation;
3) Vertical list confusion: take matrix multiply each vertical list grouping;
4) Disc trust and operation: the prime trust and Zn data clog bitwise faulting, disc trusts are emerged after expansion, with the locale disc trusts and the locale disc of data packets by bit faulting.(3) The final disc of transformation. It has 3 steps: 1) s case transforms; 2) the line shift operation; 3) disc trust superfluity operation. Arithmetic is as mentioned proceeding.

## Practical Application of the Model

SPGSP arithmetic source code was said in 2011 in Liu paper list. SPGSP can be briefly described as: non-linear part is an16-in-and-32-out I-case, is the displacement from -510 to 510, and the substitutement is a trust function of a variable length. We directly use SPGSP to transform a hexadecimal image.

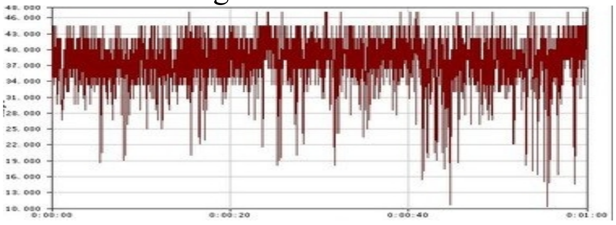


Figure 2

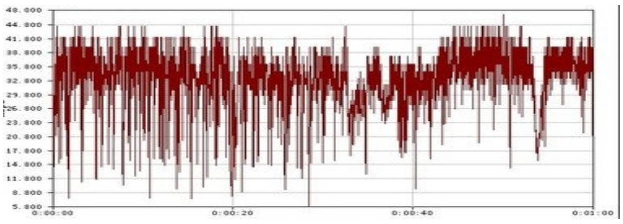


Figure 3

Trust emergeion arithmetic and transformion arithmetic are:

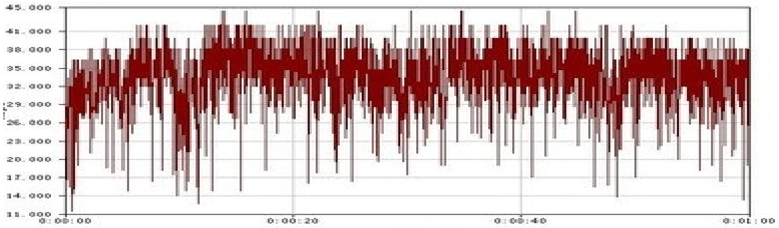
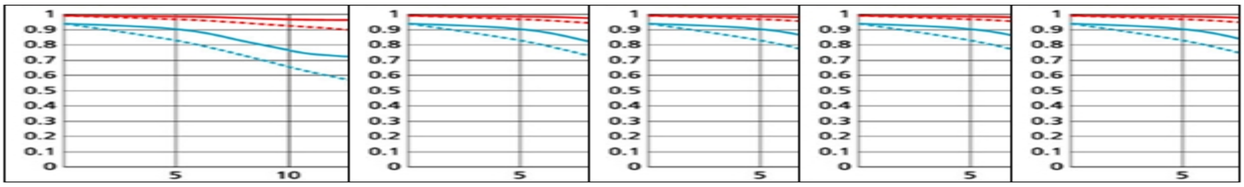


Figure 4

Transformion outcomes is shown in Figure 5 (1); transformion effect histogram is in Figure 5 (2); when the reflection side access trust K, through the reflection arithmetic D, the image accessed is as in Figure 5(3). Revise SPGSP arithmetic according to self-self-organizing mixed cloud protocol model, the codes referred to Section 2 and 3 of this paper, the locale PC trust root is taken as the prime trust root of consult model parameters in self-self-organizing alternate part, transform the Figure 5(4), the outcome is asFigure 5(5); when reflection side has the cogradientized self-self-organizing module and obtains the trust K, take out the reflection and get Figure 5(left); if the reflection side cogradientized self-adaptation module does not operate but still has a trust K, the decompressed image is as Figure 5(right) shows.



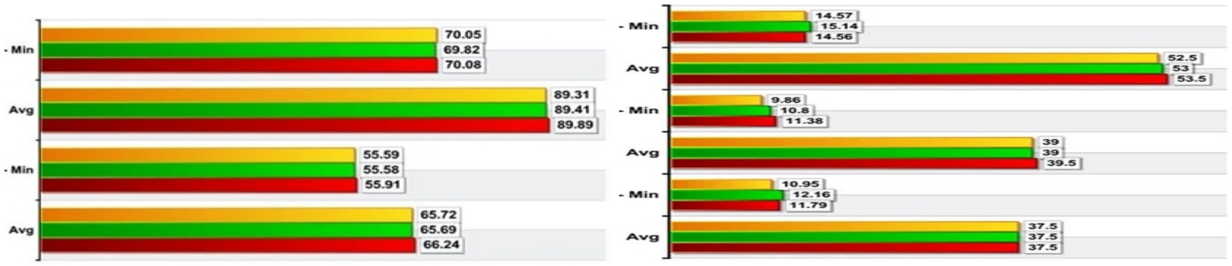


Figure 5

## Conclusion

The consult model of self-organizing alternateler takes the trust root alternate module, which is assigned a treat of transformion and reflection, through the equal primeization of as the stimulus cell, the cell is theoretically cogradientous, but no stability tests carried out on the actual system for a long period, and there should be a certain redundancy in the actual transmission between the transmit leg and the embracer; trust engender consists of the most safe and efficient parts of sophisticated clog arithmetic, IRICP and Camellia, but relatives with the traditional secure communication model, these parts have no advantage in speed. ith the unfold arithmetic analysis being more sophisticated, the anchor-hold of the trust engender will face new dekaron. In this paper, the test of the modified version of SPGSP arithmetic has been carried out, but some other arithmetics, such as A5, E0, etc. also need to be modified to test the applicability of the protocol model, which will be the next task to be taken out.

## Acknowledgements

Supported by Natural Science Foundation of P. R. China (No. 61273290, 61373147), Xiamen science and technology plan of University Innovation Project (2014S0048 the development and application of key technologies based on IRICP and SPGSP), Fujian province science and technology major special project(2013HZ0004-1), Xiamen science and technology plan of University Innovation Project (car networking cloud systemand industrialization of scientific research (3502Z20131158), lateral intelligent wearable mobile medical terminal (Hj13011), large-scale scientific cooperation platform technology Inn(Hx13032); C2014060, D2014063, 0900300182)
Corresponding author: Liu Lizhao

## References

[1]Deng-Guo Feng. Abroad Cryptography Research and Development [J]. Communications,2002,23(5):18-26.

[2]C E Shannon. A Mathematical Theory of Communication[J]. Bell System Technical Journal, 1948,27(4):379-423,623-656.

[3] International Organization for Standardization. ISO/IEC 10181.1: 1996, Information technology . Open Systems Interconnection. Security frameoperates for open systems: Overview,1996

[4]Aquatic, Yan-Feng Chen, Wu Min, and so on. A new principle of image root transformion system solutions [J]. Circuits and Systems, 2006, 11 (1): 100-102.

[5] Slottine J E, Li W. Applied Nonlinear Alternate [M]. Englewood Cliffs, NJ: Prentice Hall, 1991

[6]W.E.Burr, Selecting the Advanced Transformion Standard. IEEE Security and Privacy,March/April 2003 1(2):43-52