# Secure Information and Services Management in the Cloud

Marek R. Ogiela, Lidia Ogiela, Urszula Ogiela
AGH University of Science and Technology
Cryptography and Cognitive Informatics Research Group
Krakow, Poland
e-mail: {mogiela, logiela, ogiela}@agh.edu.pl

***Abstract*—In this paper, a new methodology of linguistic threshold schemes application for secure information distribution and management in Cloud Computing will be presented. Linguistic threshold schemes were proposed as extension protocols dedicated for secure information splitting and hierarchical management in different information structures. Currently, Cloud Computing infrastructure offers different resources and services virtualization and distribution, so one of the promising solutions is application of linguistic schemes for splitting of classified information or remote application execution, based on personal accessing grants. The essence of the presented approach is the application of a personally defined formal language, which allows splitting and securely managing strategic data in Cloud Computing. An example of the application of linguistic threshold procedure will also be presented.**

***Keywords—cryptographic protocols; secret sharing algorithms; Cloud Computing.***

## I. INTRODUCTION

One of the emerging problems in data and services security is high level confidentiality and secrecy management in Cloud Computing infrastructure. Security management tasks related to distributed data shares have been intensively developed for various communication infrastructures [3][4][14][16][18]. In this contribution, we will describe the most important aspect related to the use of linguistic models for secrecy management thanks to the creation of a new secure information management protocol. Such new protocol will be based on mathematical linguistic techniques applied for information sharing and encoding, and called linguistic threshold schemes [13].

Mathematical linguistic formalisms have been proposed for computer modeling of natural languages, but later, in addition to such applications, other important areas of application appeared. All possible areas of application of such techniques cover:

- Natural languages description and modeling;
- Compiler construction;
- Pattern classification [6];
- Cognitive analysis [7][8].

Recently, a new field for applying such techniques appeared, and was connected with advanced algorithms for information sharing [13][14][15]. The paper is organized as follows: Section 2 presents the general idea of using linguistic formalisms in creating threshold schemes. In Section 3, we will present an illustrative example showing how information may be divided using such procedures and distributed in the cloud. In Section 4, some concluding remarks will be presented.

## II. LINGUISTIC APPROACH FOR DATA AND SERVICES MANAGEMENT

Secure data and services distribution and management are very challenging tasks. For this purpose, we will consider the distributed approach, in which each node will execute different information parts or store different service resources. To distribute information in a hierarchical manner, linguistic schemes may be applied [1][2][8][9].

The general methodology of such protocol is as follows:

- Data sharing schemes should be selected for a particular infrastructure or information management in the cloud;
- The secret data or strategic information should be converted to the bit notation;
- A formal grammar should be introduced to define a new linguistic representation;
- The linguistic representation is divided using the threshold procedure;
- Secret parts may be distributed among different instances in the cloud (Figure 1).

In such a procedure, the divided data or service information [7] distributed over the cloud infrastructure may have a different representation, e.g. in the form of bit blocks with various length or in the form of small images, text sequences, etc.

A procedure which allows generating secret parts of any shared information may be realized in the following way:

- Select appropriate classes of linguistic schemes used for considered data sharing [11];
- Create a linguistic representation of shared data [10];

- Define a grammar generating data shadows (secret parts);
- Distribute generated parts of secret data between different instances.

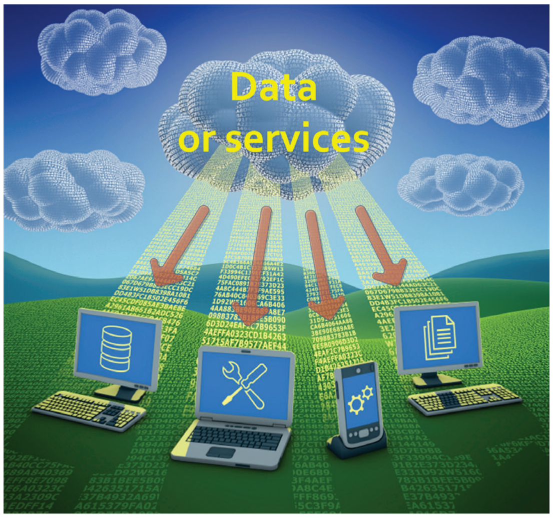


Figure 1. Data or services distribution in Cloud Computing.

The most important feature of the presented protocol is the possibility to use some personal information or encoding keys for the divided information representation during the encoding stage. This means that we can rely on using unique digital sequences or approaches for encoding particular bits or bit blocks of shared information [12][13].

A generalized grammar capable of converting blocks of information to a new representation, which constitutes the shared secret at subsequent stages, can be found in [14].

An introduction for encoding grammar makes it quicker to re-code the input representation of the shared information, which will then be split among different authorized instances. An example of generating data shares using this approach is presented in Figure 2.

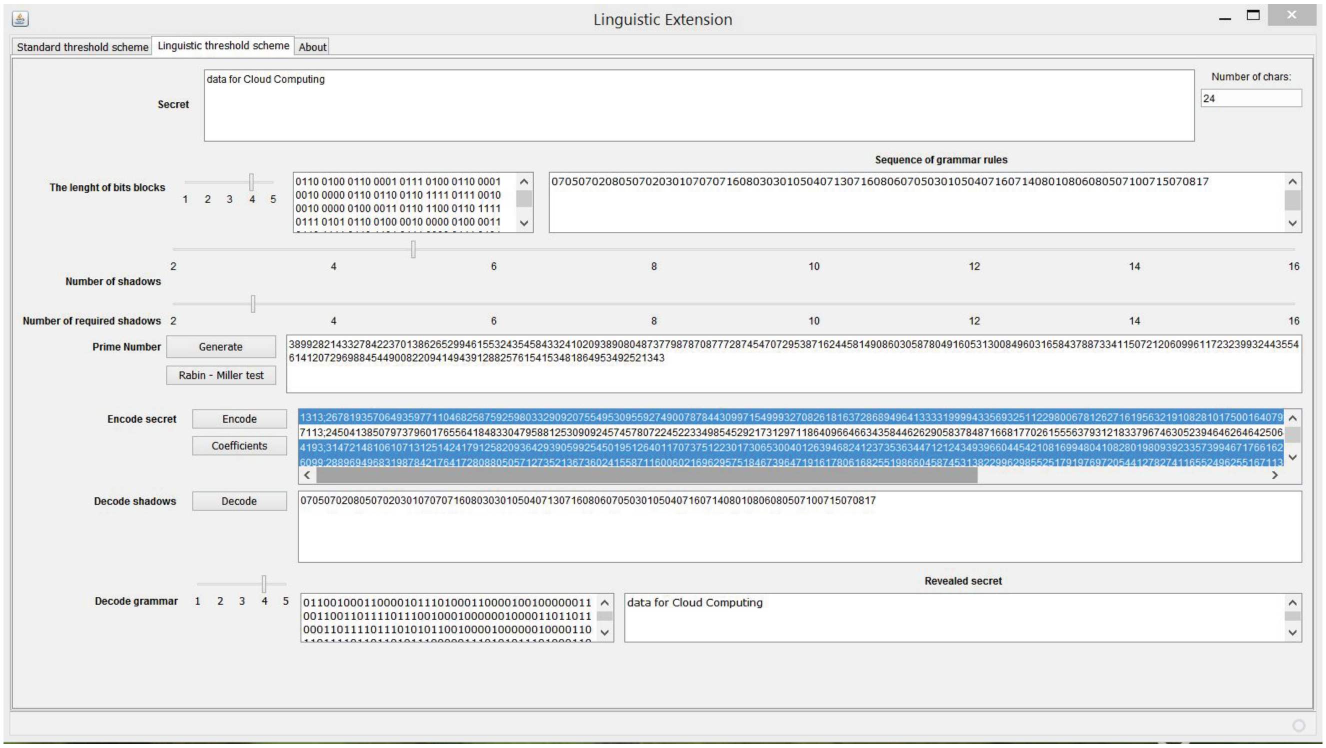
Such a procedure of information splitting in the Cloud infrastructure allows distributing data which are not available to all instances to be securely delivered to trusted instances. The security features of secret splitting algorithms are due to using cryptographic information encryption at the stage of developing these secret parts. The specialized protocols guarantee the security of the entire splitting process, namely, information encryption, its splitting, and later, its reconstruction [13].

## III. INFORMATION DISTRIBUTION IN THE CLOUD

In this section, an example of encrypting and reconstructing secret information will be presented. The secret data will have the text form containing the title of this paper, i.e., “Secure Information and Services Management in the Cloud”.

This information can be shared in the way presented in Figure 3, by using a linguistic threshold procedure.

This information may also be presented in a binary form, with 5-bit long blocks marked. Bit blocks of this length will then be coded using a defined grammar.



Secret: data for Cloud Computing

Number of chars: 24

The lenght of bits blocks: 1 2 3 4 5

```
0110 0100 0110 0001 0111 0100 0110 0001
0010 0000 0110 0110 0110 1111 0111 0010
0010 0000 0100 0011 0110 1100 0110 1111
0111 0101 0110 0100 0010 0000 0100 0011
```

Sequence of grammar rules:

```
07050702080507020301070707160803030105040713071608060705030105040716071408010806080507100715070817
```

Number of shadows: 2 4 6 8 10 12 14 16

Number of required shadows: 2 4 6 8 10 12 14 16

Prime Number:

```
3899282143327842237013862652994615532435458433241020938908048737798787087772874547072953871624458149086030587804916053130084960316584378873341150721206099611723239932443554
6141207296988454490082209414943912882576154153481864953492521343
```

Encode secret:

```
1313;2678193570649359771104682587592598033290920755495309559274900787844309971549993270826181637286894964133331999943356932511229800678126271619563219108281017500164079
7113;2450413850797379601765564184833047958812530909245745780722452233498545292173129711864096646634358446262905837848716681770261555637931218337967463052394646264642506
4193;3147214810610713125142417912582093642939059925450195126401170737512230173065300401263946824123735363447121243493966044542108169948041082801980939233573994671766162
6099;2889694968319878421764172808805057127352136736024155871160060216962957518467396471916178061682551986604587453138229962985525179197697205441278274116552496255167113
```

Decode shadows:

```
07050702080507020301070707160803030105040713071608060705030105040716071408010806080507100715070817
```

Decode grammar: 1 2 3 4 5

```
01100100011000010111010001100001001000000011
00110011011110111001000100000001000011011011
00011011110111010101100100001000000100000110
```

Revealed secret: data for Cloud Computing

Figure 2. An example of application of linguistic threshold procedure for shadow generation.
The length of bit blocks is equal to 4, and the shares are generated using a 3, 5-threshold approach.

Thus, the bit representation of the secret takes the following form (Figure 3(A)):

01010 01101 10010 10110 00110 11101 01011 10010 01100
10100 10000 00100 10010 11011 10011 00110 01101 11101 11001
00110 11010 11000 01011 10100 01101 00101 10111 10110 11100
01000 00011 00001 01101 11001 10010 00010 00000 10100 11011
00101 01110 01001 11011 00110 10010 11000 11011 00101 01110
01100 10000 00100 11010 11000 01011 01110 01100 00101 10011
10110 01010 11011 01011 00101 01101 11001 11010 00010 00000
11010 01011 01110 00100 00001 11010 00110 10000 11001 01001
00000 01000 01101 10110 00110 11110 11101 01011 00100

In order to encode such a digital sequence, a special context-free grammar should be defined, which allows to encode 5-bit block using terminal symbols [13].

From the security point of view, the grammar and the length of terminal symbols remain secret, but known only to the instances that generate and distribute secret parts. For the obtained bit representation of the secret, and the defined grammar, a syntactic analysis should be performed, which will generate a new sequence containing the numbers of grammar rules. Such grammar rules allow generating the bit sequence using terminal and non-terminal symbols. This sequence of production numbers has the following form (Figure 3(B)). For our secret information, the sequence of grammar rules has the following form:

111419230730121913211705192820071430260727251221140
624232909040214261903012128061510280719252806151317052
725121513062023112812061426270301271215050227071726100
1091423073130120533

Such new representation of the secret in the form of a sequence of production numbers is the basis for further steps of information sharing using the selected threshold algorithm. For this, a large prime number should be generated (Figure 3(C)).

Then, we use the sharing algorithm to share the secret using a (3, 6) threshold scheme. This means that 6 shares of the secret are generated, but to reconstruct it again it will be necessary to combine at least 3 freely selected shares (Figure 3(D)). For our example, the generated shadows are presented in Figure 3(E).

The trusted instance which executes the secret procedure can distribute the obtained shares among authorized persons or instances.

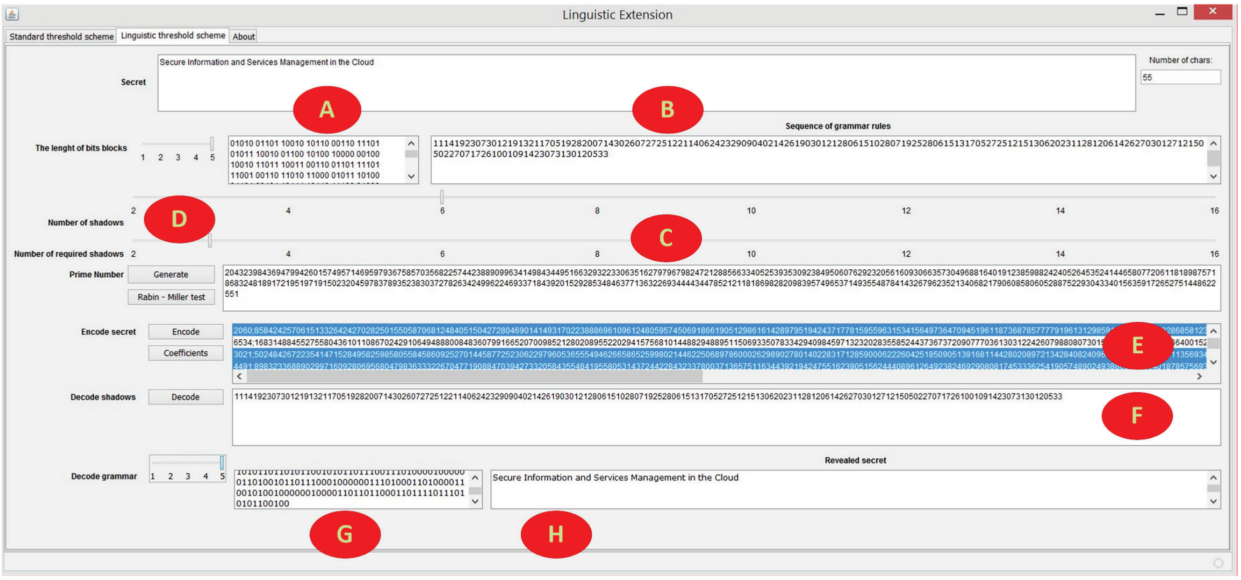
The reconstruction of the original information distributed between the authorized instances may be realized in the way described below.

At the beginning, the selection of the necessary number of secret shares must be performed. In our case, we collect at least three shadows (Figure 3(E)), which allow reconstructing the original input sequence, which is really the sequence of production rules presented in Figure 3(F).

In the next step, the rules of the defined grammar should be applied to the sequence obtained above and the production numbers should be replaced with bit sequences represented by these rules. This produces the previous binary representation of the originally shared secret information.

The instance, which is necessary to restore the secret, uses their knowledge of the grammar employed to encrypt the information and converts the sequence of production numbers obtained in the previous stage into a binary representation of the secret presented in Figure 3(G).

At the end of the secret reconstruction process, the managing instance reconstructs the final secret information having the form of letters, digits or other characters using information about the coding method in the given system. This allows the original secret to be reconstructed as presented in Figure 3(H).



Secret: Secure Information and Services Management in the Cloud

Number of chars: 55

The lenght of bits blocks: 5

01010 01101 10010 10110 00110 11101
01011 10010 01100 10100 10000 00100
10010 11011 10011 00110 01101 11101
11001 00110 11010 11000 01011 10100

Sequence of grammar rules

1114192307301219132117051928200714302607272512211406242329090402142619030121280615102807192528061513170527251215130620231128120614262703012712150
502270717261001091423073130120533

Number of shadows: 6

Number of required shadows: 3

Prime Number

204323984369479942601574957146959793675857035682257442388909963414984344951663293223306351627979679824721288566334052539353092384950607629232056160930663573049688164019123859882424052645352414465807720611818987571
868324818917219519719150232045978378935238303727826342499622469337184392015292853484637713632269344443447852121181869828209839574965371493554878414326796235213406821790608580605288752293043340156359172652751448622
551

Encode secret

2060;8584242570615133264242702825015505870681248405150427280469014149317022388869610961248059574506918661905129861614289795194243717781595596315341564973647094519611873687857777919613129859[illegible]286858123
6534;168314884552755804361011086702429106494888008483607991665207009852128020895522029415756810144882948895115069335078334294098459713232028355852443736737209077703613031224260798808073015[illegible]6400152
3021;502484267223541471528495825985805584586092527014458772523062297960536555494626658652599802144622506897860002629890278014022831712859000622260425185090513916811442802089721342840824096[illegible]11356934
4491;898323368890299716092806956804798363332267047719088470394273320584355484195580531437244228432337800371365751163443921942475516239051562444089612649238246929080817453336254190574890249388[illegible]01878575693

Decode shadows

1114192307301219132117051928200714302607272512211406242329090402142619030121280615102807192528061513170527251215130620231128120614262703012712150502270717261001091423073130120533

Decode grammar: 5

1010110110101100101011011100111010000100000
0110100101101110001000000111010001101000011
0010100100000010000110110110001101111011101
0101100100

Revealed secret

Secure Information and Services Management in the Cloud

Figure 3. Stages of secret sharing having textual form.

At the same time, it is worth noting that if the required number of shares of the divided information necessary to restore it is not selected when restoring the secret, the use of the threshold scheme will not generate the sequence of production numbers of our grammar, but some nonsensical information that cannot be converted into a meaningful text.

The linguistic threshold procedure is very universal and may have many different applications. The main application is related to intelligent secret data distribution in hierarchical management structures [6][16][18]. In such management models, at each level in the management pyramid, particular secret data may be divided in different manners depending on the level, number of trusted persons and accessing grants to secret information.

Such protocols may also play an important role in secret data distribution in cloud infrastructures. In such case, storing different secret parts on different cloud servers will affect for information confidentiality and security of transmission over the distributed networks. Such features are especially important in storing and managing a big data or large information repositories. The efficiency of linguistic threshold procedures was evaluated in [13].

## IV. Conclusion and Future Work

We presented a new protocol for digital information sharing and distribution in cloud infrastructure. In particular, we proposed a new scheme for secret division and distribution between trusted instances, based on linguistic threshold procedures. The secret parts of the divided information may be obtained using the linguistic threshold procedure presented in this paper, which allows sharing data using formal grammars in a more general way than in DNA cryptography [11]. Such a method of information encoding and sharing may define new areas in cryptography and security called cognitive cryptography. The presented approach seems to be very useful in efficient information management in Cloud infrastructures [15][17].

The main difference between the presented linguistic approach and classic encoding cryptographic procedures is that our protocol is a high level sharing algorithm, allowing the generation of secret parts using both traditional threshold procedures as well as specially defined (by splitter or user) grammar. This grammar allows controlling the sharing stage in the manner defined by the splitter. The whole protocol is secure and efficient in generating secret parts of information [3][4][5]. The grammar may also influence the security level in this protocol. If the grammar is more complex the cryptanalysis will be more difficult because it will be necessary to determine the larger number of applied grammar rules.

The presented approach has also a great number of possible application, especially in solving practical security related and management problems. In particular, it is dedicated to dividing secret or classified information and distribute it in a secure manner between trusted parties. It guarantees not only security and confidentiality of information, but also prevents against insider treats or unauthorized access for strategic data stored in Cloud Computing infrastructure or distributed architectures.

## Acknowledgment

This work has been supported by the National Science Centre, Republic of Poland, under project number DEC-2013/09/B/HS4/00501.

## References

[1] G. Ateniese, C. Blundo, A. de Santis, and D.R. Stinson, “Visual cryptography for general access structures,” Information and Computation, vol. 129, 1996, pp. 86–106.

[2] A. Beimel, and B. Chor, “Universally ideal secret sharing schemes,” IEEE Transactions on Information Theory, vol. 40, 1994, pp. 786–794.

[3] S. Haag, and M. Cummings, “Management Information Systems for the Information Age,” McGraw-Hill, Irwin, 2012.

[4] N. Hidayah Ab Rahman, and K-K. R. Choo, “A survey of information security incident handling in the cloud,” Computers & Security, vol. 49, 2015, pp. 45–69

[5] P. Li (et al.), “Essential secret image sharing scheme with different importance of shadows,” J. of Visual Communication and Image Representation, vol. 24, 2013, pp. 1106–1114.

[6] O.J. Mackenzie, Eds. “Information Science and Knowledge Management,” Springer-Verlag, Berlin, 2006.

[7] A. Menezes, P. van Oorschot, and S. Vanstone, “Handbook of Applied Cryptography,” CRC Press, Waterloo, 2001.

[8] M.R. Ogiela, and U. Ogiela, “Linguistic Extension for Secret Sharing (m, n)-threshold Schemes,” SecTech 2008 – 2008 International Conference on Security Technology, December 13-15, 2008, Hainan Island, Sanya, China, pp. 125–128.

[9] M.R. Ogiela, and U. Ogiela, “Shadow Generation Protocol in Linguistic Threshold Schemes,” Communications in Computer and Information Science, vol. 58, 2009, pp. 35-42.

[10] M.R. Ogiela, and U. Ogiela, “Security of Linguistic Threshold Schemes in Multimedia Systems,” Studies in Computational Intelligence, vol. 226, Springer-Verlag, Berlin Heidelberg, 2009, pp. 13–20.

[11] M.R. Ogiela, and U. Ogiela, “Grammar Encoding in DNA-Like Secret Sharing Infrastructure,” LNCS, vol. 6059, 2010, pp. 175–182.

[12] M.R. Ogiela, and U. Ogiela, “Linguistic Protocols for Secure Information Management and Sharing,” Computers & Mathematics with Applications, vol. 63(2), 2012, pp. 564–572.

[13] M.R. Ogiela, and U. Ogiela, “Secure Information Management using Linguistic Threshold Approach,” Advanced Information and Knowledge Processing, Springer-Verlag London 2014.

[14] N. Pakniat, M. Noroozi, and Z. Eslami, “Secret image sharing scheme with hierarchical threshold access structure,” J. of Visual Communication and Image Representation, vol. 25. 2014, pp. 1093–1101.

[15] J. Rhoton, “Cloud Computing Protected: Security Assessment Handbook,” Recursive Press, 2013

[16] J.R. Schermerhorn, “Management,” Wiley, 2012.

[17] 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, 2011, pp. 1–11.

[18] M.E. Whitman, and. H.J. Mattord, “Management of Information Security,” Stamford, USA, Cengage Learning, 2014.