Application of Biometric Key in Practical Secret Sharing for DNSsec

Anneke Soraya Hidayat, Rosemary Koikara, Pyung-Han Kim, Kee-Young Yoo*
School of Computer Science and Engineering
Kyungpook National University
Daegu, South Korea
annekesoraya@gmail.com, rosekoikara@gmail.com, k2jbks90@gmail.com, yook@knu.ac.kr
*Corresponding Author

Abstract— Secret sharing is one of the branches of threshold cryptography. Secret sharing is intended to secure a secret key *s* among a group *G* with *n* participants. Thus, the secret key *s* can be reconstructed by collecting shares of *t* or more participants. Recently, the secret sharing concept has been applied in securing DNSsec root key. However, the idea of DNSsec root key security is based on Shamir's (*t*, *n*)-secret sharing scheme and has implemented a smart card as a media to store the share information. To improve the system, we have considered Yang et al.'s scheme, one of the earlier practical secret sharing, to apply in DNSsec. By combining these two systems, we propose a biometrics-based practical secret sharing for DNSsec to resolve the problem with the storage media used. Also, we improve the drawbacks of Yang et al.'s scheme by producing a more efficient and asynchronous reconstruction phase compared to other secret sharing. Furthermore, it is applicable to the DNSsec system.

Keywords—Practical, Secret Sharing, DNSsec, key protection

I. Introduction

Shamir [1] and Blakley [2] were the first scientists who introduced the scheme of secret sharing in 1979. Both the researchers proposed diverse mathematical approaches. Shamir's secret sharing scheme uses the polynomial interpolation and Lagrange interpolation. On the other hand, Blakley's secret sharing scheme takes the hypergeometric approach. Followed by Mignotte [3] and Asmuth-Bloom [4] in 1983, both of which use the Chinese Remainder Theorem (CRT). In 2009, Chao and Lin [5] proposed a secret image sharing scheme using Boolean operation, such as XOR operation. During the 35 years since secret sharing was first proposed, many mechanisms based on secret sharing schemes have been developed.

Most of the secret sharing concepts can distribute only one particular secret message. However, it is infeasible and inefficient to distribute more than one share for each additional message. Also, the share size will be larger than the actual message [6]. Thus, to solve the first problem, a multi-secret sharing scheme, which permits the dealer *D* to distribute more than one secret message in one distribution phase, was proposed [7-8]. Furthermore, it is possible for the participants to have given fake shares during the reconstruction which leads to the second problem. The verification procedure is needed to verify each participant's share before the reconstruction phase. Verifiable Secret Sharing (VSS) concept was introduced by Chor et. Al. [9] in 1985. Their scheme provides the additional verification stage before or during the reconstruction phase. Most of the secret sharing schemes have to be generated several times once the secret has been reconstructed. Thus, Jackson et al. [10] introduced the concept of multi-use also known as practical secret sharing, where participants can maintain their shares without updating even after the secret has been reconstructed. Also, this method requires its participants to create their shares. This method solved the third and fourth problems. More practical secret sharing schemes have been proposed since then [11-13].

Most of the secret sharing scheme are aimed at applying to the practical world. Until recent times, many types of research regarding the possibilities of application of secret sharing are data protection [24], server data protection against upcoming disaster [25], and so on.

A widely known secret sharing implementation in the real-world application is key protection among participants in the Domain Name System Security (DNSsec). DNSsec is aimed to replace the security problem in the previous Domain Name System (DNS). DNS is the system that maps the Internet domains to IP addresses. However, a third party can impersonate the DNS server and get information from a user computer such that it may confuse the node with another domain address [14-15]. DNSsec protects against attacks by digitally signing data to ensure that it is valid. The system does not encrypt the data. However, it gives the validity of the address, so it makes sure that the end user is connecting to the right address. The main root key in the DNSsec acts as the main key for rebooting the web under DNS server and initialize when there is a breakdown or threat to the internet. Among seven selected participants in the whole world, five participants can conduct the reboot ceremony in the assigned place somewhere in America. As told in [16-17], no one knows the exact secret sharing algorithm which being is used, except for the fact that it is based on Shamir's secret sharing scheme. However, it has been publicly known that they use a smart card for storing shares [18-19].

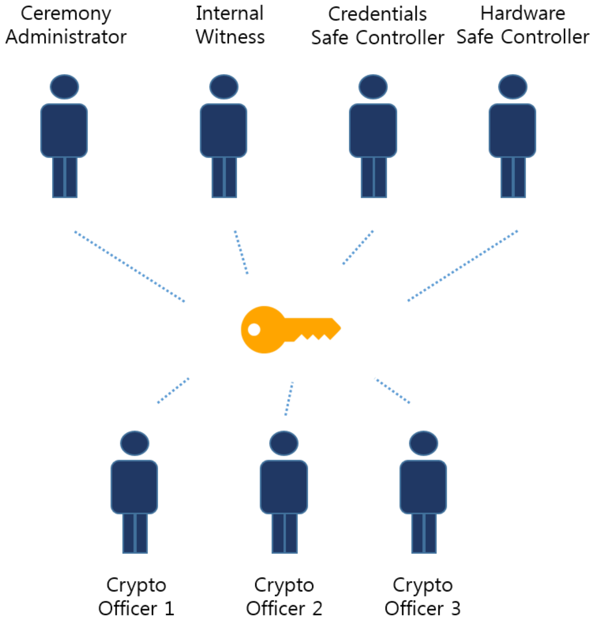

Figure 1 DNSsec Root Key System

This paper is organized as follows. Section II reviews the related work that has been done. Section III describes the proposed scheme of this paper. Section IV explains the security analysis made related between the proposed scheme and the related work. Finally, Section V concluded this paper.

II. Related Works

A. *DNSsec*

Domain Name Security (DNSsec) is a technology to protect the user against man-in-the-middle attacks by digitally 'signing' data to guarantee that it is valid. The whole process does not encrypt the data but authenticates the address of the user and the destination node [20-21]. The primary goal is to provide authentication and integrity for the data held in the DNS database. Here, confidentiality is the first priority, since the data are public data. However, this technology does not stop the attacker from making threats to the internet. Once the web becomes endangered, the role of the key holders is to get together and reboot the internet. These particular keys are generated in the key-signing ceremony.

The key signing ceremony involves ICANN staff, Trusted Community Representation (TCR) and representatives of the Root Zone Maintainer (Verisign). The TCR comprises of the seven volunteers from different countries and act as the key holders of the Root Zone Key. Thus, at least five of the key holders among the seven participants have to travel to the assigned location to present their share, thus allowing the internet to undergo DNS reboot and initialization, in case a cyber threat occurs. The illustration of the DNSsec root key system can be observed in Figure 1.

B. *Shamir's* (*t*,*n*)*-threshold secret sharing*

Given a set of secret messages $\mathcal{S} = \{s_i \mid s_i \in \mathbb{Z}_p, i \leq t-1\}$, the dealer D generates a polynomial $f(x)$ with the threshold value $t-1$ by using the Equation (1). Dealer calculates the share y and distributes the shares to a group of participants $\mathcal{P}$.

$$f(x) = s + a_1x + a_2x^2 \ldots + a_{t-1}x^{t-1}\ (mod\ p) \qquad (1)$$

Where p is a prime number, and x is each participant's ID. The dealer assigns the polynomial $f(x)$ into participant's share y_j, where $j = \{1, \ldots, n\}$, and distributes the shares to participants. When the participants wish to reconstruct the secret message, the dealer collects t or more shares from the participants and conducts the reconstruction by using the Lagrange's interpolation in the Equation (2).

$$f(x) = \sum_{j=1}^{t} y_j \prod_{\substack{k=1 \\ k\neq j}}^{t} \frac{x - x_k}{x_j - x_k}\ (mod\ p) \qquad (2)$$

$$f(0) = s \qquad (3)$$

This scheme assures the privacy and correctness features. The privacy parameter of this scheme lies in the proof of Lagrange's interpolation which guarantees that no less than t shares can yield the original secret message. Also, the privacy assures that any combination of $Y_T = \{y_{i_j} \mid y_i \in Y, j \geq t\}$ produces the same secret polynomial. The foundation of this research can be verified in [1].

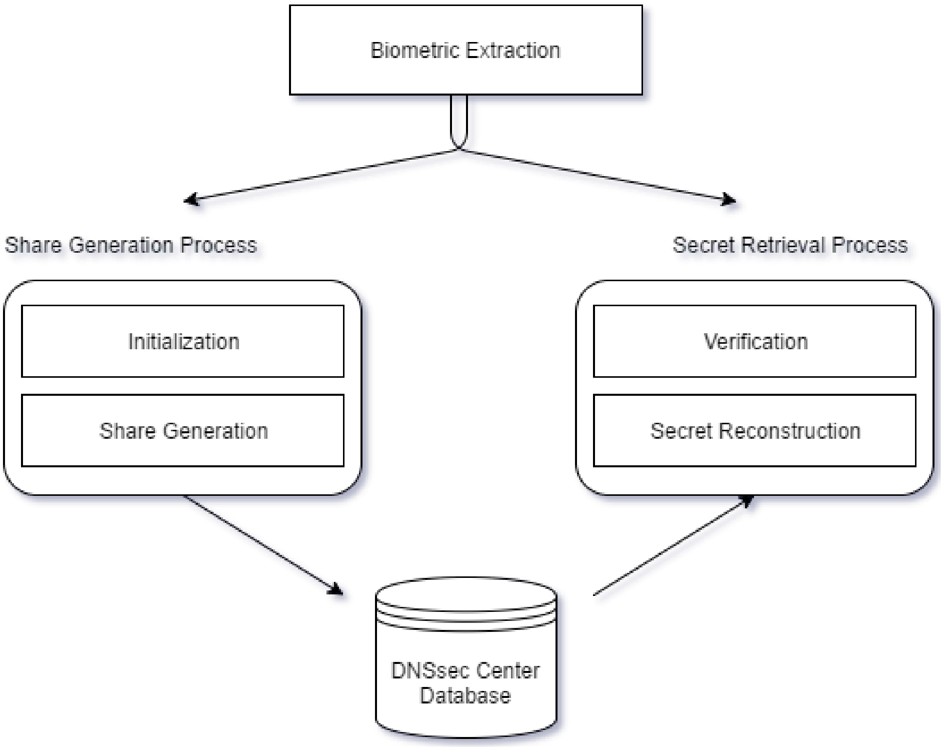

Figure 2 Proposed Scheme Model

C. *Yang et al.'s Practical Secret Sharing*

For the first time, Yang et al. proposed the practical secret sharing based on the one-way function [22]. This scheme consists of three phases: initialization phase, distribution phase and reconstruction phase.

1) *Initialization*

Given n participants $P_1, P_2, \ldots, P_n$ and a set with k elements of secret message A. Each of the participants chose n secret shadow $s_1, s_2, \ldots, s_n$ and sends it to the dealer D. The dealer D chooses random value r and computes and computes $f(r, s_i)$ for each $1 \leq i \leq n$ where f denotes a two-variable one-way function.

2) *Distribution phase*

Suppose the number of secrets is $k \leq t$, the dealer D performs the following steps.

Step 1: Chooses a prime number p and builds $(t-1)^{\text{th}}$ degree polynomial $g(x)$ as follows.

$$g(x) = a_1 + \cdots + a_k x^k + b_1 x^{k+1} + \cdots + b_{t-k} x^{t-1} \quad (4)$$

Step 2: Calculates $y_i = g\big(f(r, s_i)\big)$ mod p for $i = 1,2, \ldots, n$.

Step 3: Sends the variables $(r, y_1, y_2, \ldots, y_n)$ publicly.

3) *Reconstruction phase*

The dealer D collects the shares $f(r, s_j)$ for $j = 1, \ldots, m$ from a pool of participants, where $t \leq m \leq n$. Then reconstruct the polynomial $g(x)$ uniquely by using the following equation.

$$\begin{aligned} g(x) &= \sum_{i=1}^{t} y_i \prod_{\substack{j=1 \\ j \neq i}}^{t} \frac{x - f(r, s_j)}{f(r, s_i) - f(r, s_j)} \ (mod\ p) \\ &= a_1 + a_2 x + \cdots + a_k x^k + b_1 x^{k+1} + \cdots + b_{t-k} x^{t-1} \end{aligned} \quad (5)$$

III. Proposed Scheme

The proposed scheme consists of the following three phases: (1) Key extraction phase, (2) distribution phase and (3) reconstruction phase. The distribution phase also divided into two sections: initialization section and share distribution section. The overview of the proposed scheme model described in Figure 2.

A. *Key Extraction Phase*

The key extraction phase is conducted by the dealer D. The key is extracted from the biometric element of each participant and is always conducted in both phases, distribution phase and reconstruction phase. The biometric itself can be widely used, such as face prints, fingerprints, iris, etc. Later, the extracted key acts as participant's secret shadow.

In this key extraction phase, we applied the concept of Local Binary Patters (LBP) Operator [23] as shown in Figure 3. The process is conducted by each participant in the following steps.

Step 1: Each participant p_i collects their biometric prints by the scanner.

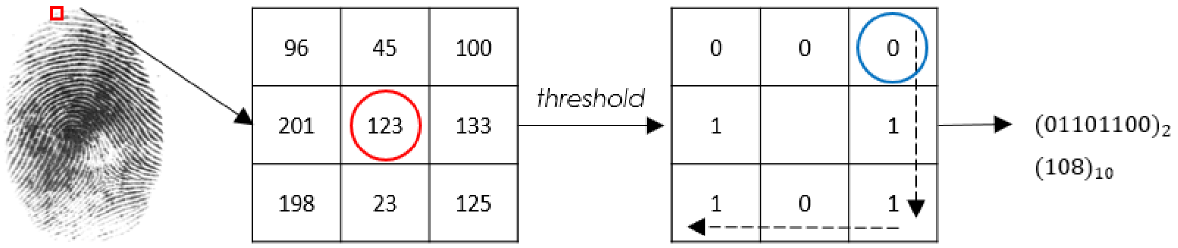

Figure 3 LBP Operator

Step 2: Convert the biometric print image into grayscale.

Step 3: For each pixel, choose 9×9 neighbour pixels to perform a Local Binary Patterns (LBP) as shown in the figure 3. One step produces 8-bit as output.

Step 4: Iterate the procedure and concatenate until it reaches the initial 56-bit.

Step 5: Iterate the rest of the pixels and XOR with the initial bits.

Step 6: Output the bits as participant's key pk_i.

B. Distribution Phase

After the dealer D extracts the key from the participant's biometric element, the distribution phase continues to be conducted. The distribution phase consists of three sections: Initialization, share distribution and reconstruction phases.

1) *Initialization*

Given a set with k elements of secret message A and the secret shadow. Each participant has their own extracted key pk_i and sends it to the dealer through a secure channel. The dealer D chooses a random value r and publishes it publicly. Each participant gives the ID and concatenates $pk_i = pk_i||ID$ which produces a 64-bits key. Then, pk_i computes $f(r, pk)$ for each I which f denotes a two-variable one-way function.

2) *Share Distribution*

Suppose there are up to t secrets available to be included in the share generation, the following steps show the share generation phase. Here, note that all the variables lie in the range of participant's extracted key $D(pk)$.

Step 1: Build $(t-1)^{\text{th}}$ degree polynomial $g(x)$ as follows.

$$g(x) = a_1 + a_2x + \cdots + a_kx^k + b_1x^{k+1} + \cdots + b_{t-k}x^{t-1} \quad (6)$$

Step 2: Calculate $y_i = g\big(f(r, pk_i)\big) \bmod p$ for $i = 1,2, \dots, n$.

Step 3: Send the variables $(r, y_1, y_2, \dots, y_n)$ publicly.

C. Verification and Reconstruction Phase

Suppose that m participants, where $t \le m \le n$, gather and wish to reconstruct the secret messages. After the dealer D extracts the key pk from each participant, the dealer calculates the share $f(r, pk_m)$. The dealer D compares the variable as follows.

$$y_i \overset{?}{=} f(r, pk_m)$$

To reconstruct the polynomial $g(x)$, the share has to be compute together by using the Newton polynomial show as follows. Note that $u_m = f(r, pk_m)$.

$$g(x) = g[u_0] + g[u_0, u_1](x - u_0) + g[u_0, u_1, u_2](x - u_0)\ (x - u_1) + \cdots + g[u_0 . u_1, \dots, u_n](x - u_0)(x - u_1) \dots (x - u_{m-1}) \quad (7)$$

where, coefficient $g[]$ is defined by the following equation.

$$g[u_j, u_{j+1}, \dots, u_{k-1}, u_k] = \frac{g[u_{j+1}, \dots, u_k] - g[u_j, \dots, u_{k-1}]}{u_k - u_j} \quad (8)$$

IV. Security Analysis

The proposed scheme presents a new approach in the reconstruction phase to counterpart the condition in the DNSsec environment based on the two variable one-way function and Newton interpolation. Both the variables are added for the purpose of improving the security and the time complexity of the secret sharing. The one-way function gives more hardness to guess for the third party. Also, the Newton interpolation enables the reconstruction to be conducted with less time complexity. This section is divided into two subsections: security and performance analysis and the time complexity analysis.

A. Security and Performance Analysis

Based on the (t, n) $-$threshold secret sharing scheme, the proposed scheme has the security parameters as follow.

1. ***Correctness***: The reconstruction algorithm has a security parameter correctness if and only if it computes a single interpolating polynomial with the mixture of any participant's $p_{i_j} \in P$ shares for at most t participants.
2. ***Privacy***: To demonstrate that no valuable information about the set of shared secrets is exposed to an adversary E corrupting at most $t - 1$ participant.

Security parameter performance evaluated by the comparison is shown in Table 1. Assume that there are m participants who already present and construct the secret together, there are $m + l$ participants, where $l = \{1, \dots, (n - m)\}$ which want to present their share. In the previous Shamir and Yang scheme, they have calculated the procedure from the beginning with the whole of $m + l$ participants. Meanwhile, our scheme can do the additional reconstruction with only l participants with the existing polynomial.

B. Time Complexity

The comparison of time complexity analysis is shown in Table 2. Here, we select the original Shamir secret sharing, Yang et al. scheme and our scheme. Considering that both Shamir and Yang et al.'s schemes were using the Lagrange interpolation in the reconstruction phase, the worst time complexity is $O(n^2)$ for one-time reconstruction phase. Here, we added the asynchronous reconstruction is which the scheme can reconstruct the secret even though the polynomial has been formed by adding the share into the reconstructed polynomial. The Lagrange interpolation has to compute the whole procedure when the new share has been inserted after the reconstruction phase is conducted. Here, the time complexity for both reconstruction phases is the same. However, the Newton interpolation can provide faster time complexity in the context of asynchronous reconstruction by $O(1)$. [26]

Table 1 Security Parameter Comparison

Security Parameter	Shamir's SS	Yang et al.'s SS	Ours
Asynchronous Reconstruction	No	No	Yes
Use of ID	Yes	No	Yes
Share Verification	No	No	Yes
Reuse of share (practical)	No	Yes	Yes
Reconstruct several secret	No	Yes	Yes

Table 2 Time Complexity Comparison

Security parameter	Shamir's SS	Yang et al.'s SS	Ours
Time Complexity	$O(n^2)$	$O(n^2)$	$O\left(\frac{n^2}{2}\right)$
Asynchronous Reconstruction	$O(n^2)$	$O(n^2)$	$O(1)$

V. Conclusion

The application of biometric key in practical secret sharing for DNSsec is proposed. The purpose of this research is to point out the key-handling drawbacks in DNSsec and provide a solution together with the security improvement of practical secret sharing. The research is motivated by the security awareness regarding the protection of the keys since the impact of the reconstruction leads to the rebooting of the whole internet under DNS. Moreover, some adversaries may take an advantage to breakdown the internet as one of a terror attack. After considering the security aspect of the DNSsec system, the Yang et al.'s practical secret sharing scheme is suitable for DNSsec implemented protection. Thus, we did explore the whole scheme and improve the scheme with several considerations for applying in DNSsec system.

Our proposed system gave three major improvements biometric based, practical and less time complexity. Biometric keys are more favourable to be implemented in a system since it does not require a storing system for each participant. Also, a biometric key, such as fingerprints, face prints, iris, are considered secure since it is unique for each person. In the real world system, conventional secret sharing requires a new share generation process after any reconstructions. Thus, practical secret sharing gives an advantage which the participants do not need to renew the share. Time complexity is also a consideration when it comes to a big system. The Our scheme takes $O\left(\frac{n^2}{2}\right)$, while the previous gives $O(n^2)$. Our scheme proved that these three aspects are applicable in DNSsec. Apart from these three issues, we also provide several improvements such as asynchronous reconstruction with $O(1)$ time complexity and double verification through consistency process.

Acknowledgment

This research was supported by the MSIP(Ministry of Science, ICT and Future Planning), Korea, under the National program for Excellence in Software supervised by the IITP(Institute for Information& communications Technology Promotion) and supported by the BK21 Plus project (SW Human Resource Development Program for Supporting Smart Life) funded by the Ministry of Education, School of Computer Science and Engineering, Kyungpook National University, Korea (21A20131600005).

References

[1] Shamir, Adi. "How to share a secret." *Communications of the ACM* 22.11 (1979): 612-613.

[2] Blakley, George Robert. "Safeguarding cryptographic keys." *Managing Requirements Knowledge, International Workshop on*. IEEE Computer Society, 1899.

[3] Mignotte, Maurice. "How to share a secret." *Cryptography*. Springer Berlin Heidelberg, 1983. 371-375.

[4] Asmuth, Charles, and John Bloom. "A modular approach to key safeguarding."*IEEE transactions on information theory* 30.2 (1983): 208-210.

[5] Chao, Kun-Yuan, and Ja-Chen Lin. "Secret image sharing: a Boolean-operations-based approach combining benefits of polynomial-based and fast approaches." *International Journal of Pattern Recognition and Artificial Intelligence* 23.02 (2009): 263-285.

[6] Capocelli, Renato M., et al. "On the size of shares for secret sharing schemes." *Journal of Cryptology* 6.3 (1993): 157-167.

[7] He, Jingmin, and Edward Dawson. "Multistage secret sharing based on one-way function." *Electronics Letters* 30.19 (1994): 1591-1592.

[8] Blundo, Carlo, et al. "Multi-secret sharing schemes." *Annual International Cryptology Conference*. Springer Berlin Heidelberg, 1994.

[9] Chor, Benny, et al. "Verifiable secret sharing and achieving simultaneity in the presence of faults." *Foundations of Computer Science, 1985., 26th Annual Symposium on*. IEEE, 1985.

[10] Jackson, Wen-Ai, Keith M. Martin, and Christine M. O'Keefe. "On sharing many secrets." *International Conference on the Theory and Application of Cryptology*. Springer Berlin Heidelberg, 1994.

[11] Hwang, Ren-Junn, and Chin-Chen Chang. "An on-line secret sharing scheme for multi-secrets." *Computer Communications* 21.13 (1998): 1170-1176.

[12] Zhao, Jianjie, Jianzhong Zhang, and Rong Zhao. "A practical verifiable multi-secret sharing scheme." *Computer Standards & Interfaces* 29.1 (2007): 138-141.

[13] Dehkordi, Massoud Hadian, and Samaneh Mashhadi. "New efficient and practical verifiable multi-secret sharing schemes." *Information Sciences*178.9 (2008): 2262-2274.

[14] Arends, Roy, et al. DNS security introduction and requirements. No. RFC 4033. 2005.

[15] Yang, Hao, et al. "Deploying cryptography in Internet-scale systems: A case study on DNSSEC." *IEEE Transactions on* Dependable *and Secure Computing* 8.5 (2011): 656-669.

[16] Ljunggren, Fredrik, et al. "DNSSEC Practice Statement for the Root Zone KSK Operator." ICANN, 2010.

[17] Del Sorbo, Aniello. "Network Security Sk-DNSSEC: an alternative to the Public Key scheme Syncfiles: a secure file sharing service for Linux." (2002).

[18] CommunityDNS CEO Holds Recovery Key Share for Root Zone. (2010, June 21). Retrieved March 9, 2016, from http://www.cdns.net/ROOT-DNSSEC.html.

[19] Dillow, C. (2010, July 28). An Order of Seel Global Cyber-Guardians Now Hold Keys to the Internet. Retrieved March 09, 2016, from http://www.popsci.com/technology/article/2010-07/order-seven-cyber-guardians-around-world-now-hold-keys-internet.

[20] Arends, Roy, et al. DNS security introduction and requirements. No. RFC 4033. 2005.

[21] Yang, Hao, et al. "Deploying cryptography in Internet-scale systems: A case study on DNSSEC." *IEEE Transactions on Dependable and Secure Computing* 8.5 (2011): 656-669.

[22] Yang, Chou-Chen, Ting-Yi Chang, and Min-Shiang Hwang. "A (t, n) multi-secret sharing scheme." *Applied Mathematics and Computation* 151.2 (2004): 483-490.

[23] Ahonen, Timo, Abdenour Hadid, and Matti Pietikainen. "Face description with local binary patterns: Application to face recognition." *IEEE transactions on pattern analysis and machine intelligence* 28.12 (2006): 2037-2041.

[24] Chang, Chin-Chen, Yeh-Chieh Chou, and Chin-Yu Sun. "Novel and practical scheme based on secret sharing for laptop data protection." *IET Information Security* 9.2 (2015): 100-107.

[25] Takahashi, Satoshi, and Keiichi Iwamura. "Secret sharing scheme suitable for cloud computing." *Advanced Information Networking and Applications (AINA), 2013 IEEE 27th International Conference on*. IEEE, 2013.

[26] Kogan, Noam, and Tamir Tassa. "Improved efficiency for revocation schemes via Newton interpolation." *ACM Transactions on Information and System Security (TISSEC)* 9.4 (2006): 461-486.