

Multi-Factor Authentication in Cyber Physical System: A State of Art Survey

Sanjar Ibrokhimov*, Kueh Lee Hui**, Ahmed Abdulhakim Al-Absi*** hoon jae lee* and Mangal Sain*

*Division of Information and Communication Engineering, Dongseo University, Busan Republic of Korea

**Dept. of Electrical Engineering, Dong-A University, South Korea

***Department of Computer Engineering, Kyungdong University- Global Campus, Gangwondo, South Korea

ib.sanjar93@gmail.com, leehkueh@dau.ac.kr, absiahmed@kduniv.ac.kr, hjlee@dongseo.ac.kr and mangalsain1@gmail.com

Corresponding author: mangalsain1@gmail.com

Abstract—Digital Multifactor authentication is one of the best ways to make secure authentication. It covers many different areas of a Cyber-connected world, including online payments, communications, access right management, etc. Most of the time, Multifactor authentication is little complex as it require extra step from users. With two-factor authentication, along with the user-ID and password, user also needs to enter a special code which they normally receive by short message service or some special code which they got in advance. This paper will discuss the evolution from single authentication to Multi-Factor Authentication (MFA) starting from Single-Factor Authentication (SFA) and through Two-Factor Authentication (2FA). In addition, this paper presents five high-level categories of features of user authentication in the gadget-free world including security, privacy, and usability aspects. These are adapted and extended from earlier research on web authentication methods. In conclusion, this paper gives future research directions and open problems that stem from our observations.

Keywords—Authentication, Multifactor Authentication, Sensors, Cryptography, Face recognition

I. INTRODUCTION

Authentication is the case of verifying the claimed identity of an entity. The process involves the verification of one or more of some knowledge (like a parole), something in possession (like a RFID access card) or inherence (like the fingerprint) of the entity. Main authentication process verifies anyone of the above information. In theory, authentication is simple process where a user provides some sort of credentials like a password, smartcard, finger print, digital certificate-which identifies that user as the entity which it claims to be. There can be many ways and protocol that can be used to achieve this. Regardless of the method, the basic authentication process remains the same. Authentication is an absolutely essential element of any typical security model. Multi-Factor Authentication (MFA) is a form of strong authentication which uses more than one information among the above. Multi-factor authentication techniques operate multiple authentication programs to confirm the identity of the user and eliminate the risk of compromise of secret or token in basic authentication methods. Each authentication program is a basic authentication process. Thus, the overhead involved in a multi-factor authentication process is multiple times that of a

basic authentication process. This makes the process fewer flexible.

In cyber physical system digital multifactor authentication is one of the best ways to make secure authentication. It covers many different areas of a Cyber-connected world, including online payments, communications, access right management, etc. Most of the time, Multifactor authentication is little complex as it require extra step from users. With two-factor authentication, user also needs to enter a special code or key number which can be generated by mobile, Internet, or some special device or some special code which was generated at the time of registration. In some case these steps can be more than 2 where security level can be increase by adding special code or Token. By introducing additional authentication factors it greatly increases the level of security, but it could also become frustrating for end users. This paper surveys the already available and emerging sensors (factor providers) that allow for authenticating a user with the system directly or by involving the cloud. The corresponding challenges from the user as well as the service provider perspective are also reviewed.

Rest of the paper is organized as follow. In the first section we have discuss about the evolution from single authentication to Multi-Factor Authentication (MFA). In section III Multi – Factor Authentication using fingerprint and user specific random projection is explained. In section IV Shamir’s secret sharing scheme is explained. Multi-Factor authentication using threshold cryptography is explained in Section V. Moreover you will know about MFA-MB for Cloud Computing in Section VI, which is a solution aiming to enhance the security level at the authentication and access control process for the three cloud computing service models (SaaS, PaaS and IaaS). And lastly Cloud-based authentication infrastructure is discussed in section VII which is uses to accommodate an increasingly mobile workforce.

II. EVOLUTION FROM SINGLE AUTHENTICATION TO MULTI-FACTOR AUTHENTICATION

In the opening scene of Hamlet, Bernardo is asked to identify himself by reciting a password before he can take over his castle post from Francisco: —“ng live the king!” [1] This exchange, from Shakespeare’s prolific tragedy, is one of the most famous examples of passwords in literature. This

ancient collection of Arabic stories was officially published in English in 1706. In one of the most famous stories, a woodcutter named Ali Baba overhears a secret phrase used by a group of thieves to protect their treasure. While the thieves aren't watching, Ali Baba utters the phrase "Open sesame" and takes the treasure.

With the development digital technology devices are getting cheaper, smaller, more portable, and much more powerful. Due to advancements in network, connectivity is faster, easier, and wireless is available almost everywhere. However, one thing stills the same, the way we authenticate our device. We still using the same style of user names and passwords that was devised almost 50 years ago at MIT to control the amount of time students and professors could spend on the university's timeshare computer. In the beginning single password-based approach was enough to access to digital information and resources. Initially, only one factor was utilized to authenticate the subject. By that time, Single-Factor Authentication (SFA) was mostly adopted by the community due to its simplicity and user friendliness [1, 2].



Figure 1. Single Factor Authentication

But once we start sharing much more sensitive personal and financial information it was necessary to come up with alternative authentication solutions. In addition with the development of high speed computing device it was easy to use several algorithm like brute force to generate millions of passwords per second. To counter those attacks, Multifactor authentication (MFA) security systems come in to solve these problems. In MFA mechanism the user must present more than one credential in order to be authenticated. These credentials or authentication factors varies according to the security needs of the application. The user should submit several authentication factors to the security system consecutively. These factors must be independent to avoid breaking the whole security system in case of compromising one of these credentials. [3]

Biometric technology is among these new approaches validate identity. The move from passwords to fingerprint identification is already implemented in most of smart phones. For the first time PayPal and Samsung worked together to make the Galaxy S5 enables people to shop and pay in a store or on their mobile device using just a fingerprint for authentication. But it wasn't just a simple new authentication step, it open new window how digital commerce be safer and more secure. Up to now, using cryptic and hard to remember passwords were normal and it was always recommended to use maximum available symbols such as upper, lower case, special character, numbers etc. Now that we can begin to

move from passwords to biometric information like fingerprints, we're reaching the point where we won't have to make this kind of compromise any more.



Figure 2. Multi Factor Authentication

Fingerprints are not the only form of biometric information used for authentication today. There are many devices that use technologies such as voice impressions, iris scans, and personal physical signals such as unique heart rate information. Other types of advanced authentication technologies are also used. Organizations are already experimenting with various forms of "multifactor authentication" that combine different types of information, location, audio and gestures to verify that you are the one who claims to be you. With technological advances, we can have multi-level authentication that works in the background, so that the user does not even know what's going on.

To do that, you have to know what is needed in the future. Leading the way for these efforts is called Fast Identity Online or FIDO for short. Founded in 2012, FIDO What's new and what does it mean? PayPal is one of the founders of FIDO and now includes a large part of leading technology companies such as Google, MasterCard, Microsoft, RSA, Netflix and dozens of other companies. As it is so urgent to improve security and simplification, there are many companies working hard to offer new solutions. And while it's still too early to say which approach will ultimately replace the current system, I'm sure things are much safer and easier to use than the password-based approach,

III. MULTI-FACTOR AUTHENTICATION USING FINGERPRINTS AND USER-SPECIFIC RANDOM PROJECTION

The proposed multi-factor authentication method [11] (see Fig. 3), consist of two phases: the enrolment and verification phases. In the enrolment phase, the two inputs required are the fingerprint and the secret key (user-specific PRN). The PRN is used to generate a user-specific random matrix $R \in R^{m \times m}$, and it can be stored in a smartcard. A fixed length vector $x \in R^n$ is extracted from the fingerprint and subsequently projected onto a random subspace using the user-specific R , to generate a revocable and privacy preserving biometric template $t \in R^n$, which is then stored in template database. Random projection is a tool for dimensionality reduction. It can also be used to generate revocable and privacy preserving biometric templates.

In the verification phase, the user claims an identity and inputs a fingerprint and a PRN. Then, the same action for template generation carried out in the enrolment phase are

used to generate a template $t' \in R^n$. The similarity between t and t' is computed. The Euclidean range between two vectors was used. The users are verified to be who they claim to be if the Euclidean range between their query and enrolled templates are lower than a predetermined threshold.



Figure 3. Proposed Multi Factor Authentication System

IV. SHAMIR'S SECRET SHARING SCHEME

Shamir's Secret Sharing scheme [6] can be used to split an integer, s to n shares. The secret integer, s can be modernized successfully if a threshold number, t of shares are available. The algorithm to split the integer is known as the Dealing algorithm and the reconstruction algorithm is used to modernize the secret. The Dealing algorithm is given in Fig. 4 and Reconstruction algorithm in Fig. 5.

Algorithm 1 Shamir's Secret Sharing Scheme: Dealing Algorithm

Input: Number of shares n , Threshold value t , a prime number q and Secret integer $s \in \mathbb{Z}_q$
Output: A list of n shares, $\zeta = \{s_i\}$ where $1 \leq i \leq n$
 Randomly choose $t-1$ random integers $a_1, a_2, a_3 \dots a_{t-1}$
 $a_0 \leftarrow s$
 Build the polynomial
 $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_{t-1}x^{t-1}$
for $i \leftarrow 1$ **to** n **do**
 $s_i \leftarrow (i, f(i) \bmod q)$
end for
return ζ

Figure 4. Proposed Dealing algorithm

Algorithm 2 Shamir's Secret Sharing Scheme: Reconstruction Algorithm

Input: A list of shares, $S = (x_i, y_i) \forall i > 0$

Output: The reconstructed value, s'

for each $j \mid (x_j, y_j) \in S$ **do**
 $\ell_{j,0,S} \leftarrow \prod_{\substack{(x_m, y_m) \in S \\ m \neq j}} \frac{-x_m}{x_j - x_m} (\bmod q)$
end for
 $s' = \sum_{(x_j, y_j) \in S} y_j \ell_{j,0,S} (\bmod q)$
return s'

Figure 5. Proposed Reconstruction algorithm

V. MULTI-FACTOR AUTHENTICATION USING THRESHOLD CRYPTOGRAPHY

The concept behind the writers offered technique is to use Shamir's Secret Sharing scheme to generate the One Time Passwords (OTP) by splitting a random secret and to reconstruct the secret back when a threshold number of OTPs are fed back [7]. The process includes a secure authentication server that performs the authentication process using Shamir's secret exchange scheme. The process includes the following phases.

5.1 Registration

As with any authentication system, the users should register in the system with their credentials. The credentials should include a username to uniquely identify the user. The user should also provide the mobile phone number, email address, and other identifiers through which the OTPs are to be sent. If the user intends to use his/her own secret (PIN or password) as one factor of authentication, the secret should also be fed to the system in this phase.

5.2 Initialization

The initialization of the process starts when a user tries to authenticate to a system. The user may be either trying to login to an application or authorize a banking transaction which uses multi-factor authentication. Once the user indicates to get authenticated, the authentication server generates a cryptographically secure random numbers, and stores it securely in its database.

5.3 One Time Password Generation

In this step, the authentication server uses Shamir's Dealing Algorithm to split the random number to secret shares, following at (t, n) threshold scheme, where n is the number of authentication factors used and t is the threshold value. The server then sends each share to the user through the various channels viz., the smart phone program, SMS, and email. If the user has specified to use a secret (PIN or password), the shares are generated using a modified version of Shamir's dealing algorithm as given in Fig. 6. The algorithm splits the random number to n secret shares, out of which one share is set as the user's secret.

Algorithm 3 Modified Dealing Algorithm

Input: Number of shares n , Threshold value t , a prime number q and Secret integer $s \in \mathbb{Z}_q$, a predefined share S

Output: A list of n shares, $\zeta = \{s_i\}$ where $1 \leq i \leq n$ and $s_1 = S$
 Randomly choose $t-2$ random integers $a_2, a_3, \dots, a_{t-1}$
 $a_0 \leftarrow s$
 $a_1 \leftarrow S - (a_0 + a_2 + \dots + a_{t-1})$
 Build the polynomial
 $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_{t-1}x^{t-1}$
for $i \leftarrow 1$ **to** n **do**
 $s_i \leftarrow (i, f(i) \bmod q)$
end for
return ζ

Figure 6. Modified Dealing Algorithm

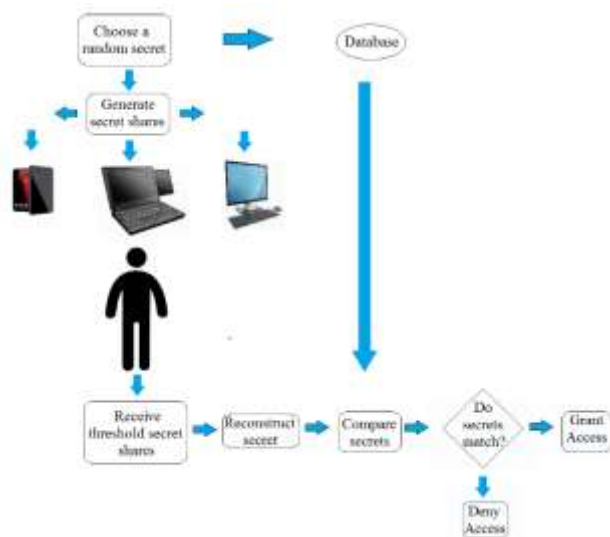


Figure 7. Illustration of multi factor authentication Proposed Reconstruction algorithm

5.4 Authentication

Once the user receives the threshold number of OTPs, he/she needs to send them back to the server. The server waits until it receives the threshold number of OTPs from the user. Upon receiving, the server tries to reconstruct the secret using the Reconstruction Algorithm of Shamir's scheme. The server then compares the reconstructed secret with the original secret random number stored in the database. The user gets authenticated if the comparison yields a match. The server denies authentication if the secret random number does not match with the reconstructed value. The process is illustrated in Fig. 7.

VI. MULTI-FACTOR AUTHENTICATION BASED ON MULTIMODAL BIOMETRICS (MFA-MB) FOR CLOUD COMPUTING

6.1 Proposed Solution

The A. Mansour et al. [8] present a Multi-Factor Authentication based on Multimodal Biometrics called MFA-

MB solution aiming to enhance the security level at the authentication and access control process for the tree cloud computing service models (SaaS, PaaS and IaaS). An authentication server is introduced in the authentication and access control process. The server provide an authentication response (Auth Response) to the user authentication request (Auth Request) for cloud PaaS or SaaS; and allow access to cloud resources for user's access demand for cloud IaaS.

5.1 FaMSL-MBS

Based on Ross et al. [9] observations and recommendations, that the fusion at the match score level is usually preferred as it is relatively easy to access and combine the scores presented by the different modalities. In this work, the authors suggest to use a MBS method integrating multiple biometric traits (Fusion) at the Match Score Level. The proposed system is called FaMSL- MBS, see Fig. 8 for detailed architecture. Depending on the number of traits, sensors, and feature sets used, a variety of scenarios are possible in a MBS. Hereafter, the authors have chosen to integrate multiple sensors and multiple biometric traits.

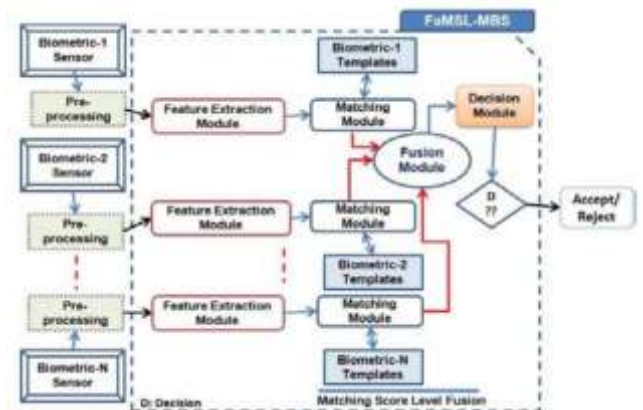


Figure 8. FaMSL-MBS scheme

6.2 Security of biometric templates

Having established the need for MFA and challenges involved in secure storage of authentication data; Khan et al. [10] have proposed a Keyed Random Projections and Arithmetic Hashing (KRP-AH) scheme for generating secure, efficient and renewable authentication templates (see Fig. 9). This scheme involves random projections of biometric data using a random key derived from a user's password, and arithmetic hashing of the resulted projections.

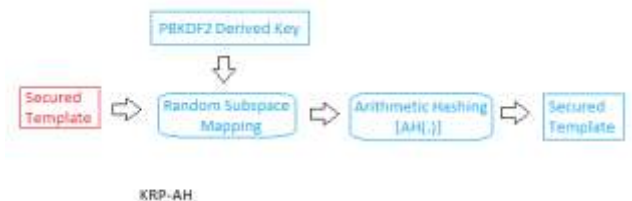


Figure 9. KRP-AH scheme for secure template generation

6.3 MFA-MB for Cloud SaaS or PaaS

For End-Users authentication in cloud SaaS or PaaS, the scheme in Figure 10 is proposed as a solution and privacy-preservation for cloud environments. Now, it is assumed that

the user has already registered in the database. Moreover, it is important to notice that the relationship between End-Users (cloud consumers) and cloud SaaS/PaaS providers takes place in a trusted environment introducing a Trusted Third Party (TTP); This is why they adopt the Secure Sockets Layer (SSL) security technology.

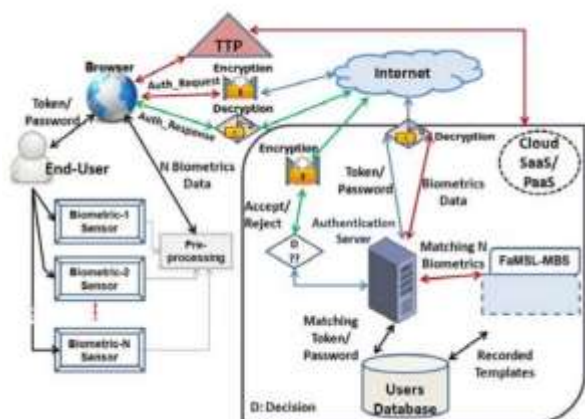


Figure 10. MFA-MB for authentication in cloud SaaS or PaaS

6.4 MFA-MB for Cloud IaaS

In order to control access of authorised or unauthorised users to the cloud infrastructure, it depicts in Fig. 11 solution to provide privacy and security for cloud consumers data-owners. Also, in the present case it requires that the user is already registered in the database. Thus, Fig. 11 presents the sequence diagram to allow access based on MFA-MB to cloud resources.

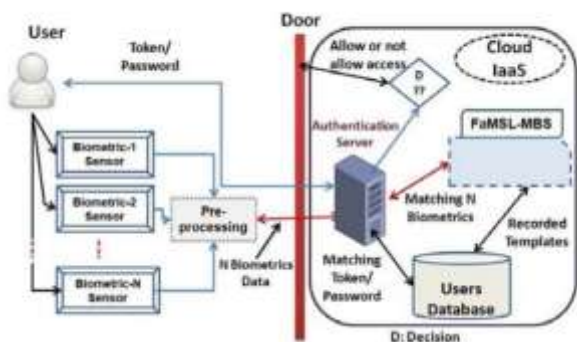


Figure 11. MFA-MB to allow access to cloud IaaS

VII. CLOUD-BASED AUTHENTICATION INFRASTRUCTURE

Users need to perform authentication whenever he tries to login from different application systems, for example input username and password to authenticate, one-time token authentication [11], or smart card authentication, etc.

Cloud terminals include personal computer, mobile phone, etc. Each terminal user is assigned a smart card with unique identity in this solution, including USB key, SD key, etc. These smart cards provide encryption and decryption functions. Users perform smart card authentication and password authentication while login application systems.

Cloud application systems provide service and need secure identity authentication for users [8]. A third-party authentication center can provide authentication and log service for different users. Encryption cards or encryption machine are adopted to provide encryption and decryption functions. Cloud application servers convey the strong authentication tasks to authentication servers, and deal with the users' access control according to the authentication result returned from authentication server. The proposed cloud-based authentication infrastructure is shown as follows:

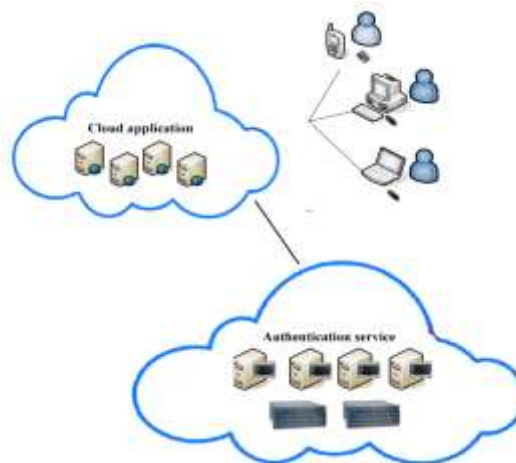


Figure 12. The cloud-based authentication infrastructure

7.1 Initialization

While initializing, authentication server updates user's smart key information, sets up the distribution system identity, user identity, key seeds and transmission key. Meanwhile, it sets up the related parameters of encryption cards or encryption machine at server, including transmission key, storage key, etc.

7.2 Registration

If a user needs to access cloud resources, a user should register firstly. When asking for a registration request, users enter a username and password, and select whether to use the proposed multi-factor authentication based on a smart key or not, and then send them to the cloud server.

After receiving the information, the cloud server checks the username. If it has been registered, the user needs to enter another username; if not, complete the registration process. For those multi-factor authentication users, the cloud server labels and stores their user identity, and carries out the multi-factor authentication protocol when authenticating.

7.4 Authentication Protocol

The proposed asynchronous challenge-response solution presents time factor as a challenge to the user when it tries to login to the cloud server. Each time the cloud server generates a new challenge for the user when it wants to login. This challenge is obtained and injected by the client software. Then the client software uses the smart card to generate a unique random number factor, and then uses the cryptography technique to generate a unique password according to the challenge and random number factor. The cloud server checks the username and password, and the authentication server checks the generated one-time password. Only the authenticated legal user can

access cloud resources at server. Consequently, the solution offers good security.

In table 1, we have compare most of popular multifactor authentication scheme which we discussed in this paper. After that we come to the conclusion that we still have a long way to go and specially to teach people about the difference between 2FA technologies and methods. People who are familiar with the knowledge of two factor they often use it, but they don't necessarily know about the different types of second factors, that can be the target of future.

Multi-factor is getting popular but still it's not that popular and as it needs extra step for authentication people often avoid that. Wang and et al [13] stated that it is not even possible to build an ideal two-factor authentication system and therefore research into this critical issue will continue. Designing a perfectly balanced authentication solution that fits all is probably infeasible. However, designing an authentication solution that is well suited for a particular application is certainly doable. Kumar et al. [15] proposed an efficient two-factor user authentication framework for wireless sensor networks, which is based on password and smart card and it uses one-way hash function. This scheme provides mutual authentication and gives user facility to change password at need. But the problem here is, it does not provide privileged insider attack as the password is sent to the base station in plain text. It also suffers from the synchronization problem as it uses the time stamp for avoiding replay attack.

TABLE I. MULTIFACTOR AUTHENTICATION COMPARISON

	Smart card	One time password	cryptographic technique	Multi-modal biometric systems	Token
MFA using fingerprint and user-specific random projection	✓			✓	
MFA using threshold cryptography		✓	✓		✓
MFA based on multimodal biometrics (MFA-MV) for Cloud Computing		✓	✓	✓	✓
Cloud based authentication	✓	✓	✓		✓

VIII. CONCLUSION

In this paper we discuss the evolution from single authentication to Multi-Factor Authentication (MFA) starting from Single-Factor Authentication (SFA) and through Two-Factor Authentication (2FA). In addition, this paper presents five high-level categories of features of user authentication in the gadget-free world including security, privacy, and usability aspects. These are adapted and extended from earlier research on web authentication methods. In conclusion, this paper gives

future research directions and open problems that stem from our observations.

REFERENCES

- [1] <http://shakespeare.mit.edu/hamlet/full.html>
- [2] Konoth, R.K.; van der Veen, V.; Bos, H. How anywhere computing just killed your phone-based two-factor authentication. In Proceedings of the International Conference on Financial Cryptography and Data Security, Christ Church, Barbados, 22–26 February 2016; Springer: Berlin, Germany, 2016; pp. 405–421.
- [3] Kim, J.J.; Hong, S.P. A method of risk assessment for multi-factor authentication. *J. Inf. Process. Syst.* 2011, 7, 187–198.
- [4] AJ Abboud "Multifactor Authentication for Software Protection", *Diyala Journal of Engineering Sciences* 8 (4), 479-492
- [5] E. T. Anzaku, H. Sohn and Y. M. Ro, "Multi-Factor Authentication Using Fingerprints and User-Specific Random Projection," 2010 12th International Asia-Pacific Web Conference, Busan, 2010, pp. 415-418. doi: 10.1109/APWeb.2010.44
- [6] A. Shamir, "How to Share a Secret." *Communications of the ACM* 22.11, vol. 22, no. 11, pp. 612–613, 1979.
- [7] V. Venkumar and V. Pathari, "Multi-factor authentication using threshold cryptography," 2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Jaipur, 2016, pp. 1694-1698. doi: 10.1109/ICACCI.2016.7732291
- [8] A. Mansour, M. Sadik and E. Sabir, "Multi-factor authentication based on multimodal biometrics (MFA-MB) for Cloud Computing," 2015 IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA), Marrakech, 2015, pp. 1-4. doi: 10.1109/AICCSA.2015.7507257
- [9] Arun Ross and Anil K Jain. *Multimodal Biometrics : an Overview*. In 12th European Signal Processing Conference (EUSIPCO), pages 1221–1224, Vienna, 2004. IEEE.
- [10] Salman H Khan, M Ali Akbar, Farrukh Shahzad, Mudassar Farooq, and Zeashan Khan. Secure biometric template generation for multi-factor authentication. *Pattern Recognition*, 48(2):458–472, 2015.
- [11] Sanjeet Kumar Nayak, Subasish Mohapatra, Banshidhar Majhi. An Improved Mutual Authentication Framework for Cloud Computing. *International Journal of Computer Applications* (0975-8887) Volume 52 No.5, August 2012. pp: 36-41.
- [12] G. Zhao, Y. Li, L. Du and X. Zhao, "Asynchronous Challenge-Response Authentication Solution Based on Smart Card in Cloud Environment," 2015 2nd International Conference on Information Science and Control Engineering, Shanghai, 2015, pp. 156-159. doi: 10.1109/ICISCE.2015.42
- [13] D. Wang, D. He, P. Wang, C.-H. Chu, Anonymous two-factor authentication in distributed systems: certain goals are beyond attainment. *IEEE Trans. Dependable Secur. Comput.*, 12(4) (2015) 428-442.
- [14] M Sain, HJ Lee, WY Chung, "Designing context awareness middleware architecture for personal healthcare information system" (ICACT), 2010
- [15] Kumar, P., Sain, M. and Lee H. J. "An Efficient TwoFactor User Authentication Framework for Wireless Sensor Networks" ICACT 2011

Mangal Sain received the M.Sc. degree in computer application from India in 2003 and the Ph.D. degree in computer science in 2011. Since 2012, he has been an Assistant Professor with the Department of Computer Engineering, Dongseo University, South Korea. His research interest includes wireless sensor network, cloud computing, Internet of Things, embedded systems, and middleware. He has authored over 50 international publications including journals and international conferences. He is a member of TIIS and a TPC member of more than ten international conferences.

