

A Survey on the Security in Cyber Physical System with Multi-Factor Authentication

Mangal Sain*, Oloviddin Normurodov*, Chen Hong** and Kueh Lee Hui***

*Division of Information and Computer Engineering, Dongseo University, South Korea

**Department of Linton School of Global Business, Hannam University, Daejeon, Republic of Korea

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

mangalsain1@gmail.com, oloviddinnormurodov52@gmail.com, prof.chenhong@hnulinton.org and leehkueh@dau.ac.kr

Abstract—Cyber-physical Systems can be defined as a complex networked control system, which normally develop by combining several physical components with the cyber space. Cyber Physical System are already a part of our daily life. As its already being a part of everyone life, CPS also have great potential security threats and can be vulnerable to various cyber-attacks without showing any sign directly to component failure. To protect user security and privacy is a fundamental concern of any kind of system; either it's a simple web application or supplicated professional 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 requires extra step from users. 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). This paper seeks to analyze and evaluate the most prominent authentication techniques based on accuracy, cost, and feasibility of implementation. We also suggest several authentication schemes which incorporate with Multifactor authentication for CPS.

Keywords—Authentication, Multifactor Authentication, Cyber Physical System, Sensors, Cryptography, Face recognition

Manuscript received January 10, 2019. This work is a follow-up the invited journal to the accepted & presented paper of the 20th International Conference on Advanced Communication Technology (ICACT2018),” This work was supported by Hannam University, Daejeon and Dongseo University, "Dongseo Cluster Project" Research Fund of (20200007).

Mangal Sain is with the Division of Information and Computer Engineering, Dongseo University, South Korea. (Corresponding author phone: +8251-320-2009, e-mail: mangalsain1@gmail.com)

Oloviddin Normurodov is with the Division of Information and Computer Engineering, Dongseo University, South Korea. (Corresponding author phone: +8251-320-2009, e-mail: oloviddinnormurodov52@gmail.com)

Chen Hong is with the Department of Linton School of Global Business, Hannam University, Daejeon, Republic of Korea. (e-mail: prof.chenhong@hnulinton.org)

Kueh Lee Hui is with the Dept. of Electrical Engineering, Dong-A University, South Korea (e-mail: leehkueh@dau.ac.kr)

I. INTRODUCTION

We live in a world that is changing at a much faster pace than ever before. More than any other time in our history, there is a pressing need for a new way of looking at science, technology, and social phenomena to help us understand our planet, ourselves, and how we can take control of our collective destiny. Without a doubt, our knowledge in the areas of science, technology, and social sciences has played a key role in shaping the modern world. In simple words Cyber-Physical Systems (CPS) is an engineered system in which a physical system or a process is augmented with cyber components such as computational hardware and communication network. All these components are tightly integrated with each other that's the reason functionality of one component is dependent on the functionality of other component. each other. CPS are systems of collaborating computational entities which are in intensive connection with the surrounding physical world and its on-going processes, providing and using, at the same time, data-accessing and data-processing services available on the internet. With other words, CPS can be generally characterized as “physical and engineered systems whose operations are monitored, controlled, coordinated, and integrated by a computing and communicating core” [1].

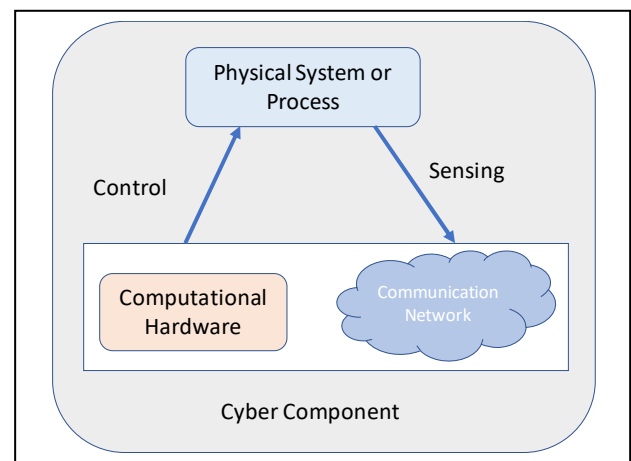


Fig. 1. Cyber Physical System Architecture

The interaction between the physical and cyber elements is of key importance: “CPS is about the intersection, not the union, of the physical and the cyber. It is not sufficient to

separately understand the physical components and the computational components. We must understand their interaction". [2]

Population and our consumption of the Earth's resources are soaring. Estimates put the world's population beyond 7 billion, and annual per capita energy consumption at about 20 MWh/year or 1,800 kg oil equivalent. Fortunately, with the development and availability of powerful communications infrastructure, our awareness of the state of the world and our ability to influence it are also improving: It is remarkable, for example, that the number of smartphones on the planet has already topped one billion. Some of the most exciting innovation these days are from cyber physical system. Some of the examples of CPS include smart grid, autonomous automobile systems, medical monitoring, process control systems, robotics systems, and automatic pilot avionics.

With the recent development and exponential growth of CPS, new security challenges have emerged. New type of security threats, attack and controls have been introduced for the new generation of CPS. However, there lack a systematic study of CPS security issues. In particular, the heterogeneity of CPS components and the diversity of CPS systems have made it very difficult to study the problem with one generalized model. [3]

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 requires 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 several Multi -Factor Authentication scheme are discussed. In section 4 we have done some comparative analysis and finally in section 5 describes about the conclusion and future work.

II. CONCEPT OF 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: "Long live the king!" [4] 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-bases approach was enough to access to digital information and resources. Fig 2 shows 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 [5, 6].



Fig.2. 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 algorithms 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. Fig 3 shows 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. [7]

Biometric technology is among these new approaches validates 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.



Fig.3. 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 METHODOLOGIES

3.1 A Cyber Situational Awareness Framework Based on Digital Twins

Proposed Solution

To improve the cyber defense capabilities of CPS, A cyber situational awareness framework based on Digital twins were

developed. As we know staff who operated these systems need better and need more accurate situational awareness, as they have to be ready to intervene in the case of any cyber threat. In As can be seen in Fig. 3, the virtual environment, which hosts the digital twins, lies at the heart of the proposed framework. Data (e.g., system logs, network traffic, sensor measurements) is passively collected from the physical environment to mirror the program states of real devices to digital twins [6].

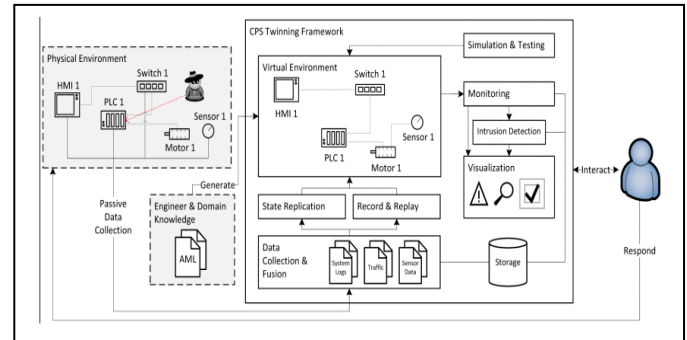


Fig.4. the architecture of the proposed digital-twin cyber situational awareness framework

From the Fig.4's architecture, the behavior of digital twins can be monitored on the program and network layer and potential intrusions can be detected. In this case, digital twins should show the correct, benign behavior of other physical counterparts, because they are generated from the CPS's specification. It also possible that they not show actual state of real devices, but they will still able to spot the deviations that could indicate malicious activity. If there are some vulnerability or if there are some errors, digital twins will show malicious behavior similar to their physical counterparts. Above proposed framework provides enough veracity to advance cyber situational awareness. As a result, the functionality of devices (i.e., programs, network communication) can be emulated or simulated.

3.2 Multi-Factor Authentication based on multimodal Biometric (MFA-MB) for Cloud Computing

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 provides 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.

3.2.1 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. 5 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.

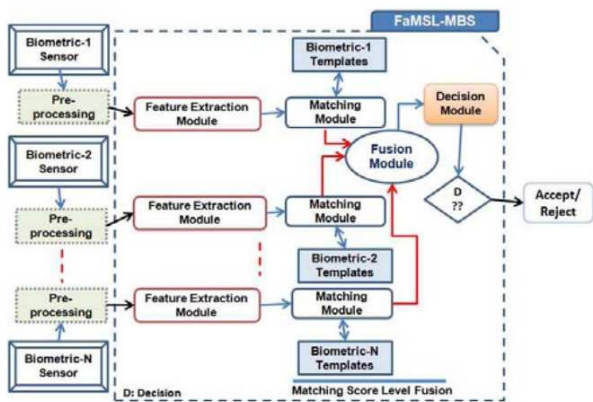


Fig. 5. FaMSL-MBS scheme

3.2.2 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. 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.

3.2.3 MFA-MB for Cloud SaaS or PaaS

For End-Users authentication in cloud SaaS or PaaS, the scheme in Fig.6 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.

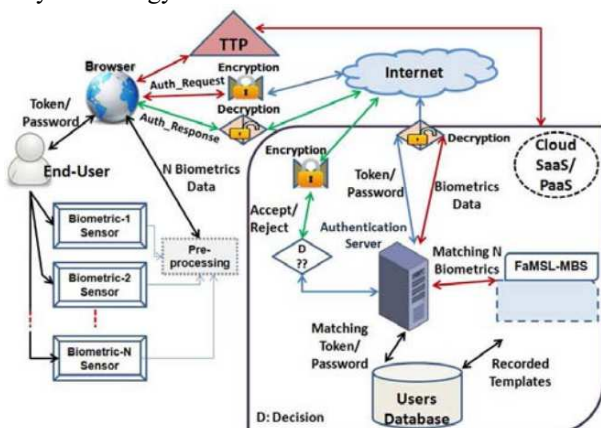


Fig.6. MFA-MB for authentication in cloud SaaS or PaaS

6.4 MFA-MB for Cloud IaaS

In order to control access of authorized or unauthorized users to the cloud infrastructure, it depicts in Fig. 7 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. 7 presents the sequence diagram to allow access based on MFA-MB to cloud resources.

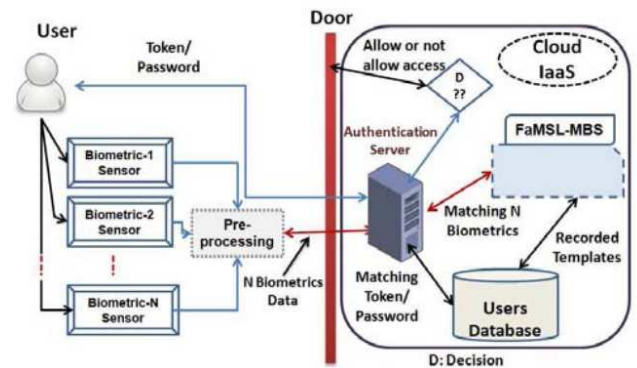


Fig. 7. MFA-MB to allow access to cloud IaaS

3.3 Prioritized access control enabling weighted, fine-grained protection in CPS

The public report from the National Electric Sector Cybersecurity Organization Resource (NESCOR) project highlighted the importance of access control. [11] This report identifies possible cybersecurity failure scenarios in six domains of smart grid applications; they are Advanced Metering Infrastructure (AMI), Distributed Energy Resources (DER), Wide Area Monitoring, Protection, and Control (WAMPAC), Electric Transportation (ET), Demand Response (DR), and Distribution Grid Management (DGM). As shown, the top four action groups relate to access control as follows:

1. Control access: block unauthorized access;
2. Authenticate only qualified users;
3. Detect abnormal or unauthorized activity;
4. Verify that systems operate as they should (audit).

A security policy addressing the prioritization is to distinguish and prioritize access operations and strengthen protection level for highly prioritized ones. However, MFA increase the security level with most of the application but it does not work well in CPS environment, specially when it comes to smart grid. An access control mechanism must be able to adjust protection level accordingly that MFA cannot do.

Proposed Solution

To overcome the security weakness in smart grid, Lee et al. introduces a priority-based access control, find grained protection in cyber physical system. [12]

a) Attribute-based identification

In CPS, there are number of devices are connected which generate a large amount of data and that data makes it more difficult to manage communication a non-trivial task. With the help of attribute-based identification, each user does not remember the ID of partners. Instead, it describes data of interest using keywords and/or attributes and communicates with any users who store contents matching the description.

b) Attribute-based encryption

In attribute-based encryption (ABE), a user encrypts data using a set of descriptive attributes, not using a specific user's public key.[13,14] It also creates an access policy tree, representing a Boolean formula defining the combination of attributes. Any user who can present credentials that correspond to the attributes, that is, satisfying the tree, can decrypt the ciphertext.

c) Decentralized access control entry

In Access Control Entry (ACE), each file (object) maintains an ACE that predefines three user classes (owner, group, and others) and determines which privileges (read, write, and execute) are assigned to each class. The privilege for each class is represented by a three-digit code so that a user is authorized to read from, write to, or execute the file. DeACE decentralizes ACE by exploiting ABE and capability-based security. That is, a user is granted a capability "object_1 = 101" by an authority. When the user accesses the object_1, he or she is authorized to read and execute, but not to write. The capability is realized by number-assigned attributes using ABE.

Access Control Decision

In a MFAC system, there exist three types of entities—authorities $CA \in \mathcal{CA}$, users $u \in \mathcal{U}$, and objects $\tilde{u} \in \mathcal{U}$. An authority CA_j maintains its own set of attributes, L_j , that can be in various forms. Fig.8 illustrates a protocol for access control in MFAC.

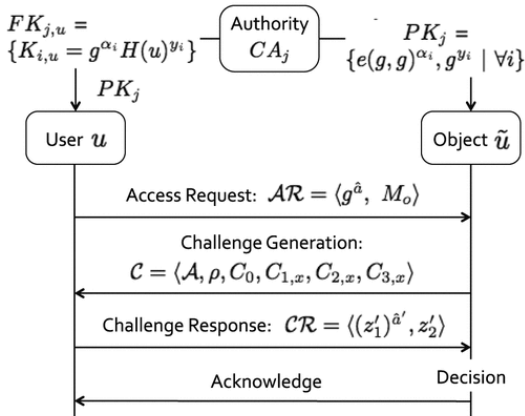


Fig.8. Authentication and authorization protocol. A protocol for an access control decision in MFAC

The proposed MFAC can be applied to various situations in many CPS applications as prioritization occurs everywhere. This article considers a fine-grained access control in a smart building context as a sample scenario. As introduced in section

“Prioritization in access control,” people perceive the access operations of “reading” and “controlling” with different priorities. The use of additional channel strengthens the level of verification independence. In MFA, a factor represents a very low computation complexity; numbers of 4–6 bits are generated and matched. This simplicity is mainly attributed to human being’s involvement in the verification process. This article adopts PBC, LSSS matrix, and DeACE, which represent expensive computation costs. Unlike in MFA, qualification of factors and independence between factors are defined and verified via more complicated mathematical computation processes in MF authorization.

3.4 Anonymous and Efficient Message Authentication Scheme for Smart Grid

In smart grid, network communication forms the core of the electric system automation applications. The deployment of one-way information flow communication networks is similar to that in the traditional smart grid. But when it comes to two-way information flow communication network, it involves a neighborhood gateway which collects the electricity consumption records from corresponding consumers via wireless network connections [15]. In next step, neighborhood gateway sends its collected data to the control center for detailed consumption analysis via a wired network connection. Finally, the control center sends the electric control information to relieve the burden of electricity demand peak or responds with real-time pricing information to the smart grid consumers.

It is necessary to select the internet Protocol based communication to enable network communications in the smart grid. Unfortunately, such networks are prone to a number of external attacks, such as impersonation attack, tracking attack, and denied of service (DoS) attack [16]. Most recently, Li et al. [17] proposed a provably secure message authentication scheme with high efficiency for smart grids. However, this scheme fails to provide mutual authentication and cannot mitigate the impersonation attacks and DoS attacks. [18] To overcome the weakness of Li et al.’s scheme, they have proposed an improved anonymous message authentication scheme for the smart grid. Similar to Li et al.’s scheme, proposed scheme also has three phases: the initialization phase, the authentication and key agreement phase, and the message transmission phase.

3.4.1 Security Initialization Phase

In this phase, the registration center (RC) generates the system parameters and private-public key pair for each registered entity user (i.e., HAN_{GW_i} and NAN_{GW_j})

Step 1. The RC chooses a multiplication cyclic group G with order q , and the generator is g . Next, the RC selects a secure one-way hash function $h'(\cdot): \{0,1\}^* \rightarrow \{0,1\}^{* \log_2 q + |D|}$ and a secure hash function $h(\cdot): \{0,1\}^* \rightarrow Z_q^*$.

Step 2. For each registered entity, RC generates a distinct random number x as private key and compute g^x as the

corresponding public key. Here, let $x_i \in Z_q^*$ be the i -th HAN-GW's private key, and $P_i = g^{x_i}$ be i -th HAN-GW's public key.

Step 3. The RC sends the key pair (x_i, P_i) to HAN_{GW_i} (i.e., the i -th HAN-GW) via a secure channel, where P_i can be revealed to others.

Similarly, the j -th NAN_{GW} can obtain its own key pair as $(y_j, Q_j = g^{y_j})$ from the RC as described in Step 3.

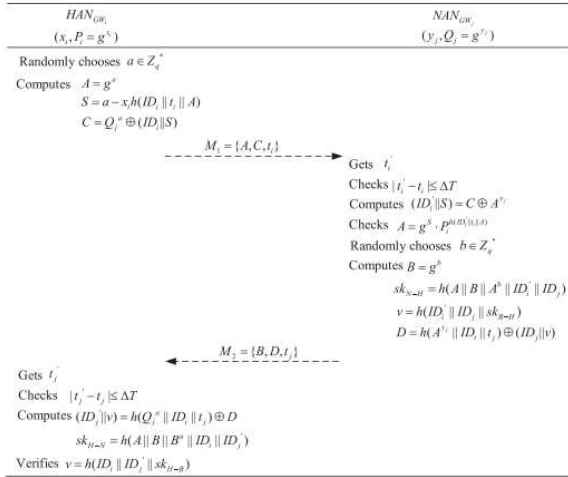


Fig.9. Authentication phase of the proposed scheme

3.4.2 Authentication Phase

In this phase, HAN_{GW_i} and NAN_{GW_j} authenticate with each other. In addition, a temporary session key is created and used for encrypting subsequent transmitted messages, as depicted in Fig. 8.

3.4.3 Message transmission phase

In this phase, a secure symmetric encryption algorithm (i.e., Advanced Encryption Standard, AES) and a secure one-way hash function are used to guarantee the message's confidentiality and integrity.

This paper also demonstrates how their improved scheme achieves the mutual authentication, session key agreement, user anonymity, perfect forward secrecy, and resistance to several attacks [19-23].

3.5 Cloud-based Authentication Infrastructure

Users need to perform authentication whenever try to login from different application systems, for example input username and password to authenticate, one-time token authentication [24], 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[25]. 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 in Fig. 10 as follow:

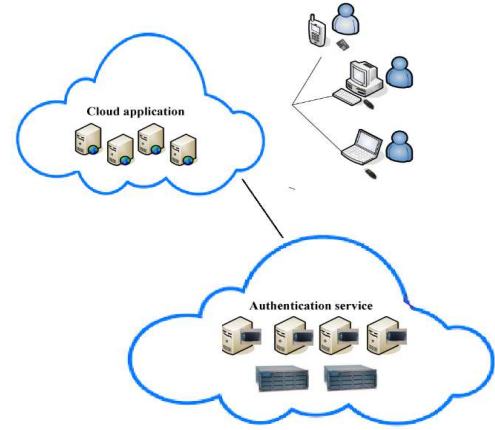


Fig. 10. The cloud-based authentication infrastructure

7.1 Initialization

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

7.2 Registration

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

After receiving the information, cloud server checks the username. If it has been registered, the user need enter another username, if not, complete the registration process. For those multi-factor authentication users, cloud server label and storetheir user identity, and carry 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 cloud server. Each time cloud server generates a new challenge for 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 use the cryptography technique to generate a unique password according to challenge and random number factor. The cloud server checks 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.

IV. SECURITY ANALYSIS AND COMPARISONS

In the following section we will discuss and compare some of popular and improved Multifactor authentication schemes which we discussed in this paper. in Cyber Situational Awareness Framework Based on Digital Twins provide an advanced monitoring, inspection, and testing capabilities. They also introduced technical use cases illustrate how these features support operations staff in gaining situation perception, comprehension, and projection. But it still needs lots of improvement as author suggested that for further development effort is required to improve the visualization of digital twins and to bring the record-and-replay feature to completion.

In Multi-Factor Authentication based on multimodal Biometric (MFA-MB) for Cloud Computing authors first discuss about security issues (authentication, identity and access management) of cloud computing as well as an overview of biometrics-based solutions were presented. Next, they propose FaMSL-MBS which is a multimodal biometric fusion system at the Match Score Level. Later, they present a multimodal biometric authentication scheme for CC systems aiming to enhance and to increase the security level in terms of authentication and access control. The proposed approach is more efficient as it overcome all the drawbacks related to Tokens and Passwords authentication technologies based on single factors and the limitations imposed by UBS.

In Prioritized access control enabling weighted, fine-grained protection in CPS author presented a novel access control mechanism, MFAC, that employs an MF technique to solve the prioritization problem. In addition, it is implemented using an ABAC model working well in a large-scale CPS network. implemented and applied MFAC to a fine-grained access control scenario in our smart building testbed. The experiments measured its computation cost and showed reasonable performance. They also develop an automated, prioritized smart building control in which protection levels changed along with real-time power price.

In Anonymous and Efficient Message Authentication Scheme for Smart Gridauthor first address the weaknesses in Li et al.'s scheme, and later proposed an improved message authentication scheme which does not incur additional computation and communication costs. A security analysis demonstrates that our proposed scheme can satisfy various security requirements for the smart grid. demonstrate how their improved scheme achieves the mutual authentication, session key agreement, user anonymity, perfect forward secrecy, and resistance to several attacks.

After going through with all above example, we conclude that Multi-factor is getting popular but still it's not that popular and as it needs extra step for authentication people often avoid that. Although some defense mechanisms have been proposed/deployed, new and systemspecific solutions are still expected in response to the newlyidentified threats and vulnerabilities [26-28]. Wang and et al [29] 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. [30] 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 timestamp for avoiding replay attack.

TABLE 1.

MULTIFACTOR AUTHENTICATION COMPARISON

	Mutual Authentication	Session Key Agreement	cryptographic technique	Resistance to Several Attacks	User Anonymity
A Cyber Situational Awareness Framework Based on Digital Twins	✓	✓	✓	✓	
Prioritized access control enabling weighted, fine-grained protection in CPS	✓	✓	✓		✓
MFA based on multimodal biometrics (MFA-MV) for Cloud Computing	✓	✓		✓	
Anonymous and Efficient Message Authentication Scheme for Smart Grid	✓	✓	✓	✓	✓
Cloud based authentication	✓	✓	✓		

V. CONCLUSION

With the exponential growth of cyber-physical systems (CPSs), new security challenges have emerged. Various vulnerabilities, threats, attacks, and controls have been introduced for the new generation of CPS. In this paper we discuss the evolution of security from single authentication to Multi-Factor Authentication (MFA) starting from Single-Factor Authentication (SFA) and through Two-Factor Authentication (2FA). In addition, this paper also presents some of the latest multifactor authentication scheme available for different part of Cyber Physical System which demonstrate several features 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, we compare all these methodologies available and try to compare with some key attributes such as mutual authentication, Session Key Agreement, cryptographic technique, Resistance to Several Attacks and User Anonymity. this paper gives future research directions and open problems that stem from our observations.

REFERENCES

- [1] Rajkumar R, Lee I, Sha L, Stankovic J (2010) Cyber-physical systems: the next computing revolution. In: *Proceedings of the design automation conference* 13–18 June 2010, Anaheim, pp 731–736
- [2] Lee EA, Seshia SA (2014) Introduction to embedded systems – a cyber-physical approach, LeeSeshia.org., Edition 1.5. <http://LeeSeshia.org>
- [3] 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.
- [4] <http://shakespeare.mit.edu/hamlet/full.html>
- [5] Kim, J.J.; Hong, S.P. A method of risk assessment for multi-factor authentication. *J. Inf. Process. Syst.* 2011, 7, 187–198.
- [6] AJ Abboud "Multifactor Authentication for Software Protection", *Diyala Journal of Engineering Sciences* 8 (4), 479-492
- [7] 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.
- [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.
- [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] Electric Sector Failure Scenarios and Impact Analyses . *NESCOR*, <http://www.smartgrid.epri.com/nescor.aspx> .
- [12] Lee, E.-K., Lim, J.-H., & Kim, J. (2017). Prioritized access control enabling weighted, fine-grained protection in cyber-physical systems. *International Journal of Distributed Sensor Networks*.
- [13] Bethencourt, J, Sahai, A, Waters, B. Ciphertext-policy attribute-based encryption. In: *IEEE symposium on security and privacy*, Berkeley, CA, 20–23 May 2007. New York: IEEE.
- [14] Goyal, V, Pandey, O, Sahai, A. Attribute-based encryption for fine-grained access control of encrypted data. In: *CCS'06 Proceedings of the 13th ACM conference on computer and communications security*, Alexandria, VA, 30 October–3 November 2006. New York: ACM.
- [15] H.Li,R.Lu,L.Zhou,B.Yang,and X.Shen, "AnefficientMerkletree-based authentication scheme for smartgrid," *IEEE Systems Journal*, vol.8, no.2, pp.655–663, 2014.
- [16] A. O. Otuoze, M. W. Mustafa, and R. M. Larik, "Smart grids security challenges: classification by sources of threats," *Journal of Electrical Systems and Information Technology*, vol. 5, no. 3, pp. 468–483, 2018.
- [17] X. Li, F. Wu, S. Kumari, L. Xu, A. K. Sangaiah, and K.-K. R. Choo, "A provably secure and anonymous message authentication scheme for smart grids," *Journal of Parallel and Distributed Computing*, 2017.
- [18] Libing Wu, Jing Wang, Sherali Zeadally, and Debiao He, "Anonymous and Efficient Message Authentication Scheme for Smart Grid," *Security and Communication Networks*, vol. 2019, Article ID 4836016, 12 pages, 2019.
- [19] D. He, N. Kumar, S. Zeadally, A. Vinel, and L. T. Yang, "Efficient and privacy-preserving data aggregation scheme for smart grid against internal adversaries," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2411–2419, 2017.
- [20] D. He and D. Wang, "Robust biometrics-based authentication scheme for multiserver environment," *IEEE Systems Journal*, vol. 9, no. 3, pp. 816–823, 2015. View at Publisher
- [21] Q. Feng, D. He, S. Zeadally, N. Kumar, and K. Liang, "Ideal lattice-based anonymous authentication protocol for mobile devices," *IEEE Systems Journal*, pp. 1–11, 2018.
- [22] C. Lin, D. He, X. Huang, K. R. Choo, and A. V. Vasilakos, "BSeln: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0," *Journal of Network and Computer Applications*, vol. 116, no. 1, pp. 42–52, 2018. View at Publisher
- [23] D. He, N. Kumar, H. Wang, L. Wang, K.-K. R. Choo, and A. Vinel, "A provably-secure cross-domain handshake scheme with symptoms-matching for mobile healthcare social network," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 4, pp. 633–645, 2018.
- [24] 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.
- [25] 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
- [26] A. Humayed, J. Lin, F. Li and B. Luo, "Cyber-Physical Systems Security—A Survey," in *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1802-1831, Dec. 2017. doi: 10.1109/JIOT.2017.2703172
- [27] P. Kumar, A. Gurtov, M. Sain, A. Martin and P. H. Ha, "Lightweight Authentication and Key Agreement for Smart Metering in Smart Energy Networks," in *IEEE Transactions on Smart Grid*, vol. 10, no. 4, pp. 4349-4359, July 2019. doi: 10.1109/TSG.2018.2857558
- [28] N. Bruce, M. Sain and H. J. Lee, "A support middleware solution for e-healthcare system security," 16th *International Conference on Advanced Communication Technology*, Pyeongchang, 2014, pp. 44-47, doi: 10.1109/ICACT.2014.6778919.
- [29] 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.
- [30] P. Kumar, M. Sain and H. J. Lee, "An efficient two-factor user authentication framework for wireless sensor networks," 13th *International Conference on Advanced Communication Technology* (ICACT2011), Seoul, 2011, pp. 574-578.



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.



Normurodov Oloviddin received the bachelor degree from Tashkent University of Information Technologies named after Muhammad Al-Khwarizmi in 2018 (Uzbekistan). At the moment he is doing MS at Dongseo university, South Korea. His area of interest is cyber security, Computer vision, Computer graphics and Network security.



Chen Hong has been an Assistant Professor with the Department of Linton School of Global Business, Hannam University, Daejeon, South Korea from 2015. She received her MA in International Trade, GSIS, Pusan National University, South Korea and BA E-Business in Management, Xiang Tan University, China



Kueh Lee Hui is working as an assistant professor at the department of Electrical Engineering, Dong-A University since 2012. She completed her PhD Degrees from Department of Electrical Engineering, Dong-A University, Korea. In 2009 she completed her BS degree in Electronic and Communication, Department of Electronic Engineering, University Malaysia of Sarawak, Malaysia. She also did MS in 2007 from Malaysia.