International Journal of Engineering & Technology, 8 (1.4) (2019) 630-639

SPC

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper



A Study on Digital Signature Authentication Algorithm Based on Multi-Factor and Public Key Infrastructure

Yoon-Jae Park [1], Yong-Hoon Lim [2], Myung-Sin Chae [3]*

[1] *Seoul Venture University*
[2] *GCOD Innovation Inc.*
[3] *Seoul Venture University*
**Corresponding author E-mail: mlee31@naver.com*

Abstract

Today most people have connected each other with information communications technology (ICT) under Internet of Things (IOT) environment. It is not awkward to have more interactions with someone they never knew. The security has become very critical in IT systems, for the security most of services rely solely on password-based authentication that has made little technological progress over past decades. The password-based authentication is exposed directly to security vulnerabilities in IOT environment, thus leading to constant increase in security incidents. The research developed an innovative authentication method, called PASSCON, as a new digital signature authentication algorithm. It explains the algorism and explain why its users would feel comfortable and secure by using it. It also suggestion proof to verify its effectiveness. It does not use text-based authentication, which causes security flaw in password-based authentication. It works only on the user's dashboard. This can block SQL Injection Attack or Brute Force Dictionary Attack. In addition, the digital ink is used only on the specified device. It also prevents other device from generating an electronic signature even if it is a correct icon key. That is, even if the key of the user's information is leaked, the user's account is protected

Keywords: *Digital Signature, Information Security, PASSCON, Password free authentication, Verification Technology*

1. Introduction

Due to rapid advances in information and communications technology, people use information communication technology (ICT) in their everyday life. Most of them use password for their security on ICT-network. However, password-based security is vulnerable on the network. Thus, accidents due to information leakages of companies and individuals increase continuously. For an example, JAVILEN strategic analysis in US found that a falsified identity authentication caused damages to 17.7 million people at the cost of 17 trillion won in 2014. To overcome such shortcomings, researchers have worked hard developing block chain, FIDO technology and other methods for alternative ways of password. However, the password-based authentication has increased rather than decreasing. Even more threatening accidents such as biometric data leakage have occurred because all data regarding personal information are concentrated on server as far as password-based methods. FIDO technology provides only password free user experience, but it is not as robust as to be the alternative to password method.

In particular, despite the use of OTP, biometrics, and multi-factor authentication technologies for strengthening authentication security, they are not robust or effective to be a countermeasure against internet hacking. Currently under Internet of Things (IOT) environment the security becomes more vulnerable thus requires more nimble and robust way of user authentication. However, those such means do not serve as completely satisfying authentication methods. The information on user biometrics specified in FIDO standard specification, for example, would be for convenience rather than authentication purpose because it registers biometric data after users finish a login session. Accordingly, FIDO is not suit for password free authentication. OPT authentication method is also an additional authentication used after performing password authentication. Thus, this sequential two-factor authentication cannot be a true multi-factor authentication for the same reason. It rather makes users more inconvenient due to the two vulnerable steps [5].

With various trial for the password-free authentication technique to overcome such inconvenience and security vulnerability. PASSCON has been developed. In this study, we are to analyse its user authentication technique and verify its effectiveness.

The composition of this thesis is as follows. Chapter 2 includes current user authentication technique, and theoretical review of regarding their algorithms, and Chapter 3 explains how the PASSCON work: its algorithms, process, and components. It also provides verification details of authentication technique, and simple & safe procedure for replacing passwords. In Chapter 4, we will explore effectiveness, key functions and features of password-free authentication technique of this PASSCON technology. in Chapter 5 provides conclusion with suggestion on usage of the technology.

2. User Authentication

2.1. User Authentication Technique

What is authentication? It is an easy and difficult question. Some people think it is an encryption technology, and others say it as a software technology. Authentication is an algorithm that uses encryption and software technology. The algorithm is also called

Copyright © 2018 Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

as a procedure. Authentication technology aims to prevent third-parties from stealing accounts or identities, using password and software technologies in predefined procedure. Before designing algorithms to achieve the goal of preventing theft, it is necessary to understand the authentication is classified into two types. One is a user credential authentication and the other is an identity authentication. For example, in order to access any WEB or APP service, user presents ID and password, and credentials, and then server verifies for approval. This series of process is called a credential. It differs from identity authentication. The identity of requester would not be verified at this time.

On the other hand, some services would require verifying requestor identity. Showing ID cards for medical service in hospitals can be an identity authentication procedure. However, it is difficult to present the identity in non-facing online environments. The solution to the problem is to use something like electronic identification that can be stored on computers or removable storage devices. A public electronic "Certificate" issued by authentication authorities has functions to identify users with electronic signature functions. In other words, it includes electronic ID cards in. In fact, number of cases has shown that users were verified using the "Certificate", electronic signature authentication to subscribe particular WEB/APP services. For WEB-APP services, which verify applicant's identity at time of sign up, has advantage of being cost-effective as well as providing users with comfortable and satisfying experience. Without this means of identification, it would be inconvenient to visit the customer centre of concerned authority [3].

Then, it is necessary to explore how the authorization by (public) Certificate includes identification functions. The reason is quite simple. To obtain initial (public) Certificate, it is required to visit the customer center, present an identification card, and sign the application directly, which is the issuance procedure. In other words, the procedural nature of linking applications and issuance is the basis for electronic non-face-to-face identification methods. Afterwards, to maintain sustainable stability of the "Certificate" issued through secure procedures, public key-based asymmetric encryption technology is integrated.

Ultimately, it makes sense to view that it consists of user credentials and identity authentication as two basic bodies of authentication. It is only natural that any of these accounts should be safe and secure after the issuance. It is not reasonable to allow lower level of security for user authentication and require higher level of security for identification. That is, the issuance process of account may vary depending on needs, and as a result, authentication method divided into the two types. Any particular authentication technique may apply for both authentications.

2.2. Authentication Technique Algorithm

A service provider applies the account issuance procedure based on its purpose and legal regulations to customers. At the time of account issuance, user can identify availability of authentication technology and usage. When users sign up Internet portal or SNS, they are almost forced to use their ID and password. In addition, for certain financial transactions or blockchains, private keys are supposed to be used as core authentication technique and much effort has been made to learn how to use such technology. Nevertheless, it is difficult to identify and follow safe management methods, and user experience tends to be further away from their satisfaction. It is because such phenomenon is based on the use of different algorithm for each authentication technique. The technique mainly consists of procedures of identification, and creation & verification of factors.

2.2.1. Identification

From the viewpoint of service provider (server), identifying requester is a top priority. The server is a computer that holds customer information in database and software that makes decisions based on established protocols. In other words, it extracts information from a particular customer in the database, and then makes judgment based on programed steps. This requires unique keys that determine which factors would be extracted from the database. Typically, WEB/APP service servers use IDs as identification values. Of course, ID can be made with a combination of letters, numbers. Email address, unique ID numbers, digital ID can be used as well. Digital ID has not been generalized so far, but can be the unique ID value given to each person. For instance, a key feature is that it is very long strings for individuals to remember and store in digital devices for use. In short, service server should be a passive system that initiates identification process only upon customer requests. So the identification value can be passed to server by direct entering when requester makes authentication request, or by transmitting pre-stored values and then server can easily identify the authentication requester.

Users prefer to present identification values in the most convenient way. Nevertheless, for the forced identification by third parties, instead of their voluntarily presented identification values, it can become a serious privacy issue. Of course, as the act of being identified itself does not complete authentication process, some security problems may still exist. However, in light of extended concept of security, the privacy of individual should be protected. Not only for security goal of authentication, but for privacy protection of individuals and upkeep of authentication system with more robust security, identification without user's own intent should be prevented if possible. Biometrics can be the most typical example of the concern for involuntary identification. It is divided into server and local authentication. FIDO biometrics is not associated with privacy issues, as it compares the information stored on devices with the biometric input entered from local device. However, storing biometric information on server can be very problematic. So biometric information is stored in the server. Then corresponding information, which user device extracts, send to the server, and then server compares both information. While it provides outstanding functionality from user convenience point of view, but there are many issues worrisome from security perspective. Most of all, body itself is exposed all the time, and therefore, illegal and malicious filming or scanning by third parties is possible. If information from server is leaked due to unalterable nature of (living) body, people constantly put themselves at risk of privacy breaches identified by third parties, or at risk of their own accounts or identities being stolen [6].

2.2.2. Factor Creation and Validation

If authentication requestor accurately performed an identification task voluntarily, then the authentication provider (server) should determine if the requestor who presented identification key has legitimate rights. Authentication requesters and authentication providers are actually forced to perform authentication based on information transmitted among computers when they interact with each other over the network. It means that software and counterpart software determine judgment based on its own criteria while sending and receiving information according to established protocols. Any information exchanged at this time can be an authentication factor, and authentication technology is like a series of processes for creating and validating these factors A factor can be created or entered solely by authentication requester, or created through interaction with authentication provider. Typically, the process of entering and encrypting passwords by authentication requester can be a factor creation. Password authentication verifies that the password received from authentication provider matches the password value extracted from authentication provider database. So it is what we call a single factor authentication. The security risks of password authentication are also due to this dependence on single factor and the creation of factor that uses keyboard/keypad to enter character strings. Nevertheless, passwords are the technology most appropriate for basic authentication re-

quirements since authentication requester remembers and presents factor values voluntarily only when necessary.

As mentioned earlier in 2.1. Certification and authentication technique, “authentication technique aims to prevent third parties from stealing account or identity by using encryption and software technologies in the context of predefined protocol." Thus, factor creation and verification algorithm is the key to achieving certification objectives. In fact, authentication technique identifies what might be the motive of a factor, applies encryption technology in a sophisticated manner, and finally specified as a technology by blocking the seizure or theft of factors by third parties. By blocking theft of factors, account or identity theft can be blocked in efficient manner.

2.3. Desirable Authentication Technique

What is a good authentication technique? It is a universal technique that minimizes additional burden on users, makes easy for anyone to learn and use, and with almost no administrative burden on confidential factors. Up until now, many experts have been trying diligently to create such technology. It has been more than 50 years since password was used for the first time in online networks. 50 years of advancement in IT technology have been truly a remarkable success. However, the security limitations and inconvenience of password authentication technique have rarely been improved, and users’ stress and security threats are becoming more intense [4].

Despite various problems of password authentication, password authentication continues to increase in use without disappearing or being replaced by other technologies, and we identified such reasons as follows. New and universal authentication technique that can resolve the problem requires the identification and reflecting of those important factors that enable password authentication technique still controls the world. Based on our consideration, it can be organized in five possible reasons.

First, the technology is inexpensive. Second, it is a fixed user habit. Third, it feels safe because it involves voluntary intents. Fourth, additional authentication is required. Fifth, even biometrics requires a password.

Even the best technology cannot be applied to the world if the cost of introducing is too expensive. In addition, it is unlikely that most WEB/APP services realize significant revenue successfully. The process of communicating information about new technologies and educating users also takes time and money. If password authentication is used as it is, it will become a common service following user's habits faithfully. Accordingly, there is no concern of customer resistance. Password authentication, which obtains certification by presenting facts known only by myself, may feel safer intuitively. Furthermore, new authentication techniques are not the technologies that can replace passwords, but the secondary authentication method with another authentication added. Secondary authentication refers that one-time password authentication, such as OTP is required once more, upon successful password authentication.

Although some use the secondary authentication mixed with a two factor authentication, this is not strictly a multi-factor authentication. Therefore, it does not provide the confidence that the security value offered by new authentication technologies is large enough to offset the inconvenience. Even with the recent increase of biometrics, password authentication is required most of the time, when users actually register their accounts. It is because validation process for biometrics is performed in local devices and permit to the biometrics registration of certification requester cannot be determined. Other authentication methods are essential when the server is unable to verify the biometrics of authentication requester. This means that passwords should be kept and managed for use. In such sense, desirable authentication would then be a technology that incorporates voluntary expression of intent but completes with a single authentication process, while maintaining already habitual user experience at low cost. In addition, it is reasonable requirement for the technology that can provide the highest level of security to prevent theft of accounts or identities.

2.4. Status of Account and Identity Theft

Before analyzing the innovative "PASSCON" certification technology addressed in this study, we would like to examine the damage caused by the theft of individual cyber accounts or identities by criminals. Therefore, we intend to identify the criterion determining how much new value this research will bring by examining the extent and frequency of the damage based on objective research data.



Fig. 1: Identity Fraud Hits All Time High With 16.7 Million U.S. Victims in 2017, According to New Javelin Strategy & Research Study

As shown in the chart above, according to a report, the US, an advanced country in IT industry showed a tendency of increase in IT since 2015, with a huge toll of 16.7 million people and 17 trillion won in damages in 2017 alone. For the scale of damage across global market, it is difficult to obtain accurate statistics, but it can be assumed that the amount can surely be dozens of times [9]. Clearly, there must be a huge side effect growing constantly along with internet and mobile innovations. Vulnerable authentication technology should be pointed out as part of the cause.

3. PASSCON Authentication Technique

There are three main ways to authenticate users. The first is ID / PASSWORD, the second is the method of verifying the fingerprints and DNA using the user's characteristics, and the ID cards based on SW token activation. PASSCON, the third method is as same as the SW token method. The owner of the PC or smartphone does not store the authentication information directly. Passcon language has the same characteristics. Because it has evolved from HSM (Hardware Security Module) method it is capable of ensuring enhanced security in the event of loss, automatic blocking, device-to-device pairing, and fingerprint recognition control tools [10].

3.1. The Need for PASSCON Technology

PASSCON technology defines the digital signature as follows. A digital signature refers to a specific person's digital data that is created and attached to with an electronic method that can only be used by a specific person. Therefore, the minimum requirement for digital signatures should be designed so that the digital signature generation information should be exclusively occupied by the user. it also must be only available to legitimate users. Unfortunately, the PKI (Public Key Infrastructure) certificate-based digital signature, up to now, does not guarantee the exclusive occupancy of digital signature generation information. Therefore, the fraudu-

lent use of the digital signature by the third party cannot be sufficiently blocked. This is because most PKI certificate-based digital signatures depend on passwords and private keys. Here our PASSCON will provide a new algorithm that overcomes the security limitations of passwords and guarantees exclusive occupancy of the signature generation information so that can secure the certificate and the digital signature authentication.

In particular, with the development of Internet of Things (IOT) technology, the disadvantages of user authentication approaches are growing as the cyber physical systems (CPS), where objects and things are connected, are being transformed into a highly selective society. Hacking to utilize such vulnerabilities has steadily occurred on businesses information leakage incidents, such as financial, insurance, or general business leakage incidents.

In addition, technologies for alternative authentication methods are required in the device industry domains where it is difficult to use authentication tools, such as existing passwords, authentication certificates and OTP [1]. In addition, Table 1, which is being adopted by financial institutions such as card issuers, has also taken risks and disadvantages [2]. To address these shortcomings, more advanced certification techniques are needed, which supplement PASSCON certification techniques [10].

Table 1: Comparison of alternate authentication services

Section	ARS/SMS certify	Phone certify	Phone OTP Certify	IC Tagging certify	Bio Certify
Status	provided	provided	provided	provided	To be provided
Conditions of use	N/A	Smart Phone	Process for supporting security domains	Smart phones with NFC functionality	Certification Module (Finger-Prints / iris Recognition, etc.)
Subscription information	(ARS) Authentication number (SMS) Name, date of birth, telephone number	Payment secret number	Payment secret number	IC Touch card	Biometric information (Fingerprints, iris, Voices, etc.)
Certification body	Mobile	Mobile	Financial company, Mobile	Financial company	Financial company (cellphone)
Credential Create subject	Mobile	cellphone	cellphone (Security area)	IC, Card (+cellphon)	cellphone (Security area))
Danger	Forward Rogue code Operation of Communication Equipment	Remote control, reverse engineering	Vulnerability Intermediator Attack	IC chip replication, memory dump, intermediate attack	Forged retransmission attacks
Issue	SMS authentication is not used alone due to risk	IPhone requires direct text messaging	Require relevant function module (secure area, NFC, biometrics, etc.), therefore, more recent terminal usage conditions are necessary		

3.2. PASSCON Technology Overview

3.2.1. Overview

Authentication and Digital Signature Technology using the user-specified digital signature creation information and icon dashboard. PASSCON provides very easy and simple UI / UX for initial installation and configuration. Users select a photo from the gallery and select the security icon from the icon dashboard to complete the security setup. The user can complete the authentication simply by touching the security icon.

3.2.2. Deployment

In the application example of Figure 2, 1 channel or 2 channel authentification can be selected and applied. For PCs, 2 channels are recommended, but if you do not have a mobile app, you can apply 1 channel authentication with a Windows-based APP. In this case, apply PASSCON Windows app to share. You only need to install the shared app once. Mobile 1 channel is not based on a separate app but is applied based on App in App. Option may be given to the user in parallel with password authentication.

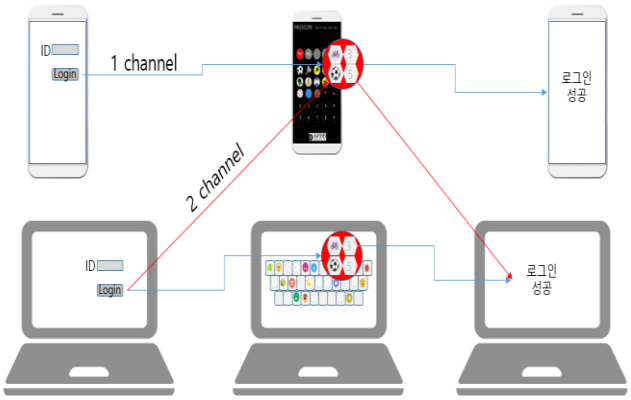


Fig. 2: Application example

In the 1 User Multi-Device & 1 Device Multi-User of Figure 3, Users often use more than one smart device. In addition, home computers are shared by multiple users at the same time. Therefore, supporting 1 User Multi-Device & 1 Device Multi-User environment is very important, and PASSCON fully satisfies these demands.

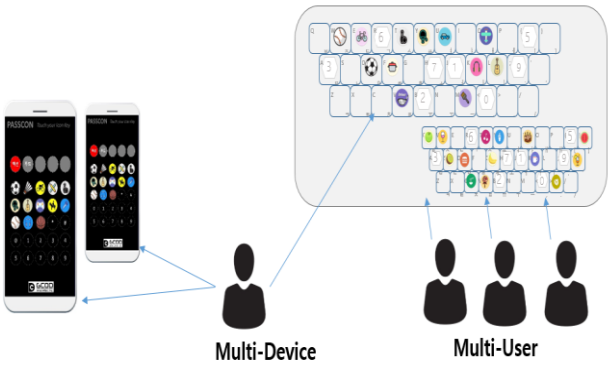


Fig. 3: 1 User Multi-Device & 1 Device Multi-User

3.2.3. Concept of PASSCON Authenticator

You need a pen and ink to sign. It should also be your own ink. So it is a digital ink that is invented. This is a true digital transformation. Here, the pen should not be stolen. There must be a way to prevent third parties from using it if it is stolen. Inks must be

manufactured in such a way that they cannot be reproduced by applying reverse engineering using only unique materials. So I decided to use some photos that the user kept in the gallery as the raw material of the ink. Photographs can satisfy uniqueness and confidentiality. We also use dashboards that consist of icons instead of keyboards to keep the pen safe from malicious code or peeking

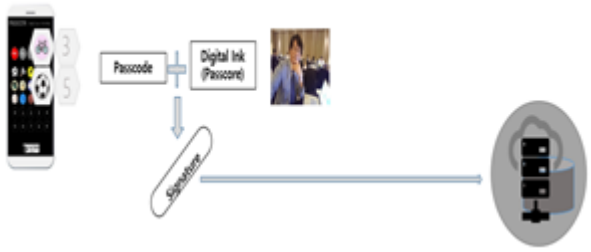


Fig. 4: Signature, Pen and Ink

The next challenge is how to keep safe these digital inks and use them when needed. For this purpose, we adopt a method of generating and verifying digital signatures using PKI asymmetric encryption technology. Digital ink is securely encrypted / decrypted using PKI, and the device-specific information is combined so that it cannot be used by third party devices even if it is stolen.

The next challenge is how to keep safe these digital inks and use them when needed. For this purpose, we adopt a method of generating and verifying digital signatures using PKI asymmetric encryption technology. Digital ink is securely encrypted / decrypted using PKI, and the device-specific information is combined so that it cannot be used by third party devices even if it is stolen.

PASSCON's unique and creative authenticator creation, management and verification algorithms provide unprecedented and innovative results in terms of convenience and security.

3.2.4. Algorithm of Setup and Factor Generation

The user selects a photo in the gallery to create the digital ink. and Select the security icon to be used for authentication and complete the set and then the authentication factor is stored in the device and the server. At this time, the security passcode corresponding to the user security icon is not stored anywhere.

The process of setting up PASSCON by the user is as follows. PASSCON is an application-based authentication technology. The process consists of five steps. Installation, Membership, Photo selection and digital ink creation, Dashboard selection and security icon selection. In the process of setting up, the user has to consider, and the only part to decide is the easy and quick process of two steps: photo selection and security icon selection.

First, Users can download and install the PASSCON application program from the service provider's Web site, the APP store, or the Play Store. This PASSCON application can be embedded in other applications in one modular type. PASSCON is also available for iOS, Android and even Microsoft Windows systems.

Second, Membership is required to identify customers. KYC (Know Your Customer) is a very important issue in recent online business. Therefore, all users are identified by ID.

Third, Digital ink is PASSCON's very unique and innovative technology. This allows unique and confidential elements to be entered into the signature generation function. The user can create one's own digital ink by selecting one of the photos in his gallery and change it at any time.

Finally, PASSCON offers many kinds of dashboards. The user selects his or her dashboard and selects the security icon. This dashboard is completely different from the keyboard / keypad. This means that we do not use ASCII codes as input to the computer system. Therefore, all keyboard hacking tools and malicious malware will automatically become useless. The Passcode matched to the security icon is another unique secret factor that is entered into the signature generation function.

In the installation process, what the server does is create a "passcode" and securely store the necessary factors in the user directory table. The step-by-step procedure for setting up PASSCON can be easily expressed in the diagram below Fig 5.

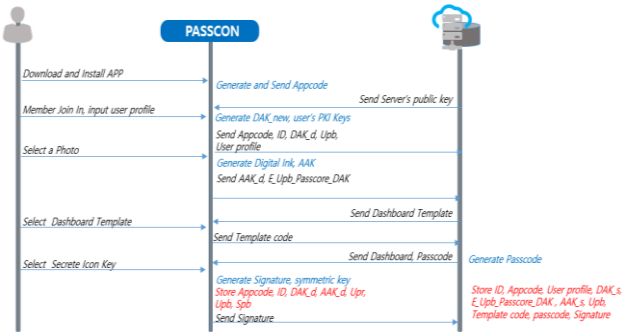


Fig. 5: Setup Process Diagram 1

The application of each process and factors can be summarized as Setup Process Diagram 1 (Fig 5.) and Setup Process Diagram 2 (Fig 6.) See the Generation Algorithm Description page below for a specific algorithm for each element[7].

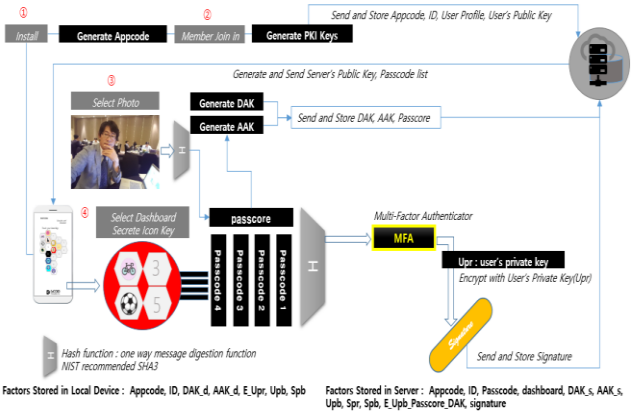


Fig. 6: Setup Process Diagram 2

Most of the setup process is performed in the PASSCON application to create, store and send the required authentication elements. These elements are generated step by step by a very secure algorithm. The PASSCON application generates Appcode, DAK, user's PKI key, digital ink, AAK, symmetric key and digital signature. A very special point of the generation algorithm is that one element is combined with the other. For some elements, a secret black box algorithm is applied. Several factors are stored on the user's device and some factors are transmitted to the server for storage on the server only. But especially important is that security icons and secret passcodes are not stored anywhere. The specific factor storage architecture is shown in the diagram below.

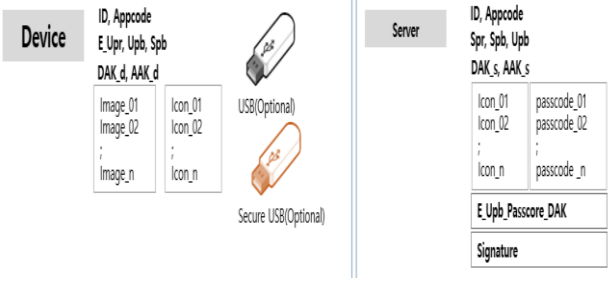


Fig. 7: Architecture Diagram

As seen in this architecture, the server does not have information about the user's security credentials. Therefore, the Zero Knowledge Proof (ZKP) is satisfied[8]. ZKP is inevitably required in the non-repudiation security environment. Users can also store

important user elements on separate media such as USB sticks. It is optional for customers who want to deploy PASSCON in service PASSCON generates application code for identification of installed applications.

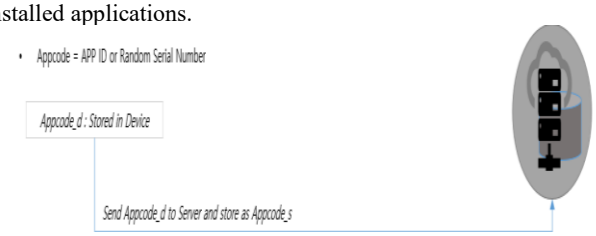


Fig. 8: Generate Appcode

PASSCON generates a DAK for device identification. Unique device information can be used as input data. The DAK generation involves a black box algorithm, which is not a simple hashing process. It can also be changed according to the way the server provides.



Fig. 9: Generate and Store Device Key

By designing the user's PKI key to be created on the local device, even the server will not know about the user's private key at all. This is the basic theory of PKI digital signatures. The user's private key is encrypted with a special symmetric key (S_Key). The algorithm that generates S_Key uses Passcode as input value as hidden logic, i.e. a black box algorithm. The private key (E_Upr) can be decrypted only when the user touches the correct security icon. This private key is also used to generate a digital signature and decrypt the encrypted passcore.

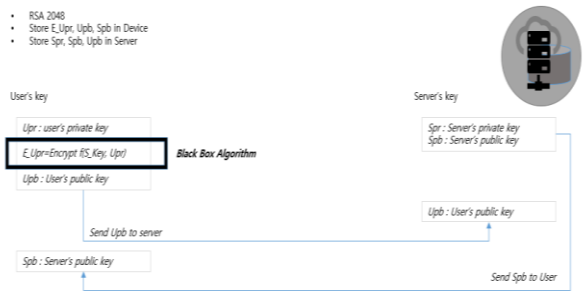


Fig. 10: Generate and Store PKI Key

The PASSCON application enters the user-selected picture into the hash function and obtains the digital ink as the result. It is defined in this white paper as "Passcore". There are no same pictures in this world except for copy files. Even if the same subject is photographed, it is impossible to obtain the same photograph due to the change of light. So the photos in the gallery are very suitable as an authentication factor. However, using the picture itself consumes so much computing power. So PASSCON uses the hash result of the picture. The hash function reduces the size of the image file to a short character set that retains its own properties. Theoretically, mp3 and doc files can be used instead of photos.

PASSCON manages and applies Passcore in a very unique and secure way. First, the black box algorithm combines the passcore value with the DAK. Next, the combined values are encrypted with the user's public key and transmitted to the server for archiving. Therefore, even if it is stored in the server, the server cannot know the value of the passcore. This is because only the user's private key can decrypt the archived passcore. This is an important feature that PASSCON satisfies ZKP.



Fig. 11: Generate and Store Passcore(Digital Ink)

AAK is a non-regenerable factor. This is because it is designed to include a timestamp value. The time stamp value is the time point at which the PASSCON generates the AAK in the setting step. After creating the AAK, the timestamp is permanently deleted and is not stored anywhere. Therefore, a hacker must steal an AAK to try to hack someone's ID. Passcore is included as one of the input data of AAK. That is, when the user changes the digital ink, the AAK is also changed. This provides the effect of neutralizing the stolen AAK by altering the digital ink.



Fig. 12: Generate and Store Application Key

Passcodes matching the icons are randomly generated for each user. This personalized Passcode set provides the ability for all users to own their own dashboards and use them as UIs and input devices. This makes it impossible for an attacker to infer a security icon from a randomly acquired security passcode and at the same time to infer a security passcode from a randomly acquired security icon.

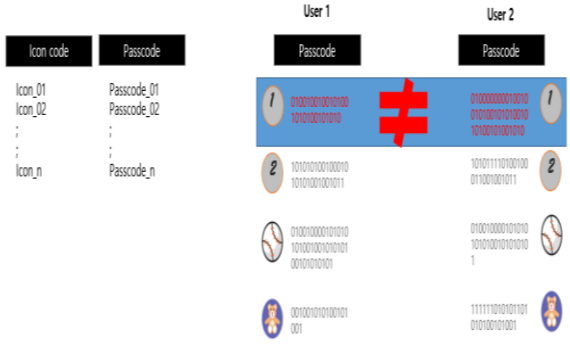


Fig. 13: Generate and Store Passcode

The key process of signature generation is the creation of mutifactor authenticators (MFA) and the application of private keys. MFA is a result obtained by processing Passcore and Passcode by using a black box algorithm as a hash function. At this time, first, a security passcode is obtained from the security icon touched by the user, and a symmetric key S_Key used for decrypting the private key is generated from the security passcode using the black box algorithm.

The passcore is obtained by decrypting the E_Upb_Passcore_DAK received from the server using the user private key Upr. After creating the MFA, it encrypts the MFA

with the user's private key, generates the digital signature, and sends it to the server for storage.
S_Key is a symmetric key that encrypts or decrypts Upr. This key is generated by the black box algorithm from Passcode and is not stored anywhere. The creation algorithm is generated only when the user touches the correct security icon, and the algorithm can be updated by the server from time to time. Also, since the user does not have to remember or input this value, the length of the applied key can be made very large. Since the passcode obtained by touching the security icon is an alphabet which is already over 100 digits, the symmetric key is very difficult to be cracked by extracting about 30 digits as a rule in a predetermined black box and applying it as a key. This makes the private key more secure for the user.

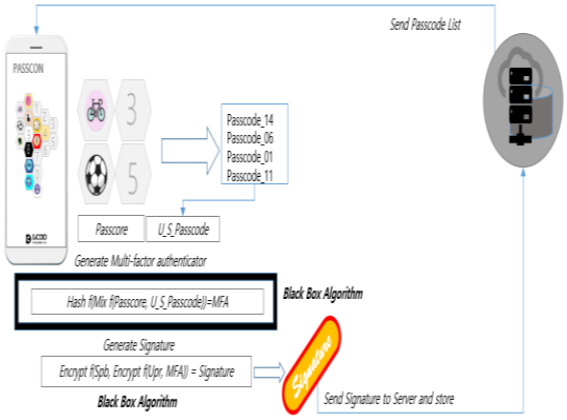


Fig. 14: Generate and Store Signature

3.2.5. Authenticate Algorithm

When the user selects the security icon, authentication is complete. and then when PASSCON is executed, it first carries out its own device verification, transmits information on devices and applications to the server, and the server performs the secondary device verification. If successful, the digital ink is sent to PASSCON.
PASSCON again perform the verification of combined digital ink and device together. If the verification is successful, the digital signature is generated using the security passcode, the digital ink, and the private key corresponding to the security icon selected by the user, and transmitted to the server to perform the final verification.
As shown in Figure 5, PASSCON certification techniques are automatically performed by the program when the user requests certification and touches the security icon. Verification is performed in a four-stage chain of procedures, and if any of the verification steps fail, the request for certification is rejected.
During the verification phase, communication between the device and the server is enabled by complicated verification techniques with digital ink. In particular, the pass-core shall be read first. The re-criminate key S_key used can only be created by touching the correct security icon. If all of these processes are successful, you can finally generate a digital signature. Digital signatures combine Passcore with secure Passcode to create a hash function and encrypt the results with a private key.

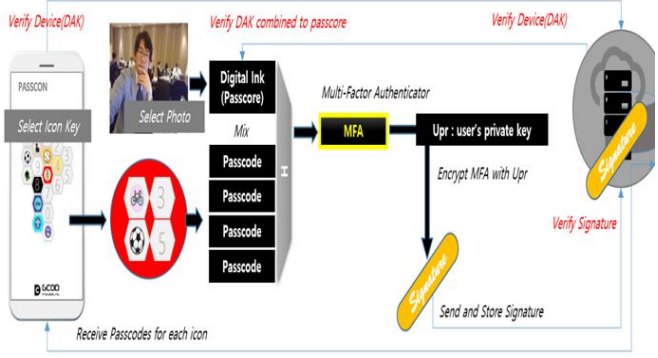


Fig. 15: Signature=Encrypt Private key (Hash f (Digital Ink + Passcodes)

As shown in Figure 5, PASSCON certification techniques are automatically performed by the program when the user requests certification and touches the security icon. Verification is performed in a four-stage chain of procedures, and if any of the verification steps fail, the request for certification is rejected.
During the verification phase, communication between the device and the server is enabled by complicated verification techniques with digital ink. In particular, the pass-core shall be read first. The re-criminate key S_key used can only be created by touching the correct security icon. If all of these processes are successful, you can finally generate a digital signature. Digital signatures combine Passcore with secure Passcode to create a hash function and encrypt the results with a private key.
Once the signature is sent to the server, the server will then validate the electronic signature and decide whether to grant the authorization for the authentication request. Every important factor used in PASCON is encrypted, and each factor is combined with the other factor and shared property.
Therefore, if a certain factor is changed, it is effective to modify several factors at the same time. It provides the security effect that makes stolen factors obsolete by the user's simple manipulation even if the attacker steals a particular factor from a device, server, or memory. In addition, PKI key changes can be automated periodically. This flexible and complete assurance of control over the factor has the effect of costing the attacker an enormous amount of money to launch the attack itself. These technical specifications in PASSCON provide sufficient requirements to replace the password completely. Such PASSCON authentication techniques are the choice of a fully password-free authentication technique[10]. The following description is part of a more detailed Authentication Process procedure.
The final approval decision for the user's authentication request is performed by the server. The server determines whether to accept the user request according to the result of the confirmation of the combined element through a step-by-step procedure. A special feature of PASSCON is that the PASSCON application also plays an important role in validating a few elements to distinguish legitimate user authentication requests from attackers' attempts.
If it is not the registered device at this time, the process will be aborted immediately and an approval rejection will be notified. Of course, in order for an authentication request to be approved, it is natural that ultimately the correct security icon should be touched as well as the device that has passed the verification. The authentication process is very simple compared to the installation process. The user simply requests authentication and touches his secret icon. All other processes are run automatically by the PASSCON application and server.

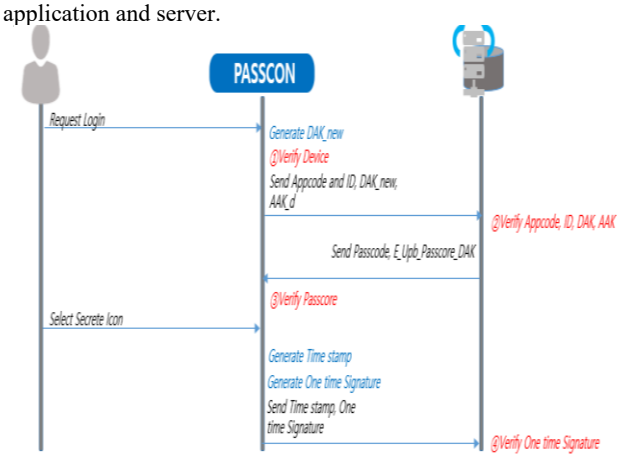


Fig. 16: Authentication Process Diagram 1

Authentication Process Diagram 1, Authentication Process As shown in Diagram 2, there are four verification procedures to complete the execution of the authentication process. This four-step verification should be passed sequentially. If any step fails, the process is aborted and the authentication request is rejected.

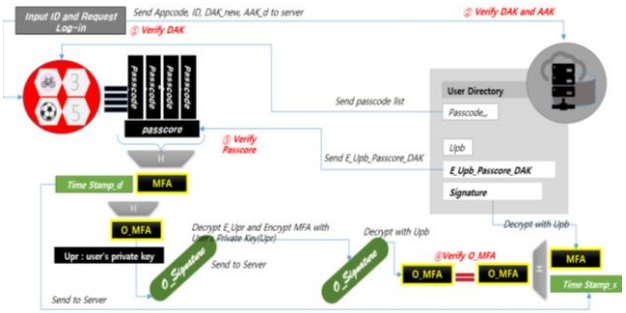


Fig. 17: Authentication Process Diagram 2

first verification step is a process of comparing DAK_new newly created by the PASSCON application with the stored DAK_d. This step makes the stolen DAK_d useless. The second step is to compare DAK_s and DAK_new by the server. This dual verification makes it almost impossible for an attacker to cheat the server into thinking that the hacker's device is the right user's device. AAK is the result of processing the value obtained by combining Passcore, DAK, and time stamp with the black box algorithm by using a hash function.

So even any genius hacker cannot regenerate the same AAK. The timestamp is not stored anywhere. This AAK makes it difficult for an attacker to steal an AAK from a device or server if he intends to hack the user's identity. This security logic plays a big role in harassing hackers because of the changeable digital ink. If the user changes the Digital Ink, the stolen AAK will immediately become garbage.

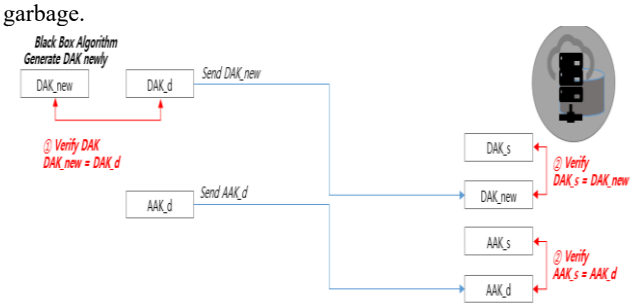


Fig. 18: Verification of Device and Application

Digital ink is a very important authentication factor. This is one of the key information for generating digital signatures. Apply the verification of the device to protect Passcore from attacker's theft. The server sends the passcore and passcode to the user application only if the device verification of ① and ② succeeds. So, if some genius hacker cheats the server as if the device is the correct user's device, the server sends E_Upb_passcore_DAK to the hacker It is possible.

Nevertheless, this is not the end. This is because the hacker must pass the device verification once more and touch the correct security icon in order to steal the passcore. Passcore is designed to be combined with DAK, so the verification procedure of ③ verifies the DAK with nes DAK. Also, to decrypt E_Upb_passcore_DAK, you must first decrypt E_Upr. The S_Key for decrypting E_Upr can only be created by correctly touching the security icon. As a result, the device must be the correct device and know the correct security icon to attempt to steal someone's identity.

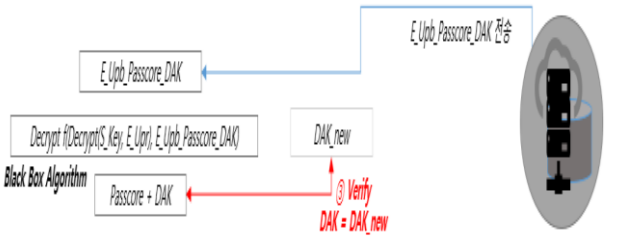


Fig. 19: Verification of Passcore

When the device is verified and you are ready to generate a signature by touching the correct security icon, the PASSCON application generates a digital signature with the user's private key, Passcore and Passcode. In this procedure, the timestamp is combined with the MFA to use the signature only once. The signature is then encrypted with the server's public key before being sent to the server. This last encryption protects the signature from intermediate attacks between the server and the device network.

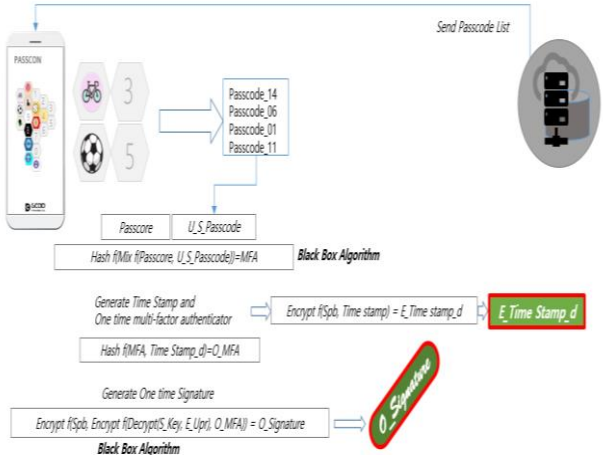


Fig. 20: Generation of One time Signature

When the server receives the signature, it decrypts the signature using the server's private key and the user's public key to obtain a disposable MFA (O_MFA). The server then decrypts the stored signature to obtain the MFA and puts the MFA and the received timestamp value into the hash function to obtain the O_MFA. Finally, the server compares the two O_MFAs to see if they are equal. If no application programs are falsified, the device is from a registered user, and the requestor is correct and touched the security icon, then the previous validations and signature verification will pass successfully. The server then notifies that the authentication request has been approved.

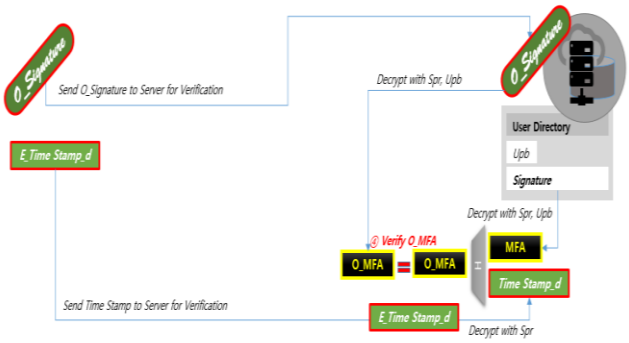


Fig. 21: Verification of One time Signature

3.3. PASSCON Main Technology

PASSCON is a method of touching a security icon using an icon dashboard instead of a keyboard. It is easy to hack using a keyboard, but PASSCON is safe from this danger. It is also user-friendly technology that can remember interesting ways, such as " 3 hours of bike time, 3 hours of soccer, 5 hours of soccer, " and use simple touch. PASSCON provides a technology that meets the convenience of users as well as the superior security. Figure 1 below and PASSCON PKI System Architecture.

As PASSCON advanced, it provides a higher probability of randomness, so even if the security icon is configured with only four of the 24 icons, it is more likely to be more random than the sixth digit PIN. It is almost impossible to locate a security icon through repeated attempts, so it is safe to lose the device. In addition, if there are five failures, the server can block the request. . Today, traditional PKI digital signatures rely only on the user's personal key for security



Fig 22: PASSCON PKI System Architecture

PASSCON, however, applies new digital signature creation information and algorithms that improve authentication and security. Users randomly select a picture in a gallery and convert it into digital ink to use it as information about creating digital signatures. A matching key, S_key is created using a secure pass code to encrypt and decode individual keys. And only the digital signature is stored on the server, so PASSCON meets Zero Knowledge Proof (ZKP). That is, security is very high, since even servers do not know a user's confidential information[10].

We propose a new advanced concept for digital PKI based digital certificates and digital signature authentication. Our PASSCON PKI does not verify only the ownership of the private key. The PASSCON PKI guarantees the validity, integrity and confidentiality of the signature, including the uncrackable knowledge authentication factor and digital signature generation information. This feature of PASSCON is sufficient to meet non-repudiation requirements.

4. Effectiveness of PASSCON

4.1. PASSCON Key Value

4.1.1. Simple, Easy, Fast, Accurate

The user simply touches four or more different security icons. It is easy to remember, easy to use. Easy to remember and use. A user-friendly usage environment provides benefits to both users and service providers.

4.1.2. Compatibility and Flexible Device Management

PASSCON is compatible with all kinds of HW or OS, even all kinds of application SW. PASSCON is suitable for all kinds of industries: Finance, Fintech, Block Chain, IOT, Cloud, Internet Portal, SNS, Groupware, ERP, Military, Public, Education and Healthcare. The user can add multiple devices as needed, and the user can securely use the same device with other users.

PASSCON is an authentication technology tightly coupled with devices. This is how the device information is combined with the various authentication factors. Therefore, nobody can use PASSCON unless it is a properly registered device. This is critical to security in today's environment where mobile is commonplace. However, if a user can only use one device, it can be very inconvenient and can lead to the loss of many customers. Therefore, PASSCON provides users with the ability to register and use multiple devices. Also, it provides a function that many users can use PASSCON while maintaining security even in the environment where the same computer is shared by a family member or the like. This 1 User Multi-Device or 1 Device Multi-User environment is a very powerful service function of PASSCON. However, this may optionally limit the application as needed.

4.1.3. Safety

Using the same icon key for all WEB / APP service certificates is still safe. This is because even if the server is hacked, the attacker cannot find the security icon in the server's database, and even if the attacker finds the security icon, he must steal the device to try to steal the identity of the legitimate user. PASSCON can identify the stolen factor because it confirms in a special way whether it is a registered correct device, and if the stolen factor is found in another device, PASSCON will automatically terminate the user's authentication request process.

The most common security problem in authentication and digital signatures is that an attacker steals someone's secret authentication element. Protecting authentication elements from theft, leaks, or many other hacking techniques in computerized digital systems is really difficult and incomplete. So you need to find a way to prevent an attacker from using the stolen element or causing it to cost very much. PASSCON satisfies this task successfully.

PASSCON does not require user's troublesome effort. At the same time, it guarantees complete user rights to change Factor very simply. For example, you can change the secret icon, digital ink, or PKI key at any time. In addition, one Factor change automatically amplifies the effect by simultaneously changing multiple Factors connected. Even if you change the digital ink or PKI key, you do not need to memorize or add any additional procedures. This unpredictable change in Factor makes every effort by the attacker useless at once.

4.1.4. Security without Password

Users can safely use PASSCON on all online services with the same security icon without having to follow password management guidelines. This means that users do not have to find complex combinations of icons, change security icons on a regular basis, and create different combinations of icons for different services in APP / WEB. Therefore, PASSCON can completely replace the password.

PASSCON needs to remember only one security icon. Nevertheless, you may forget. Fortunately, PASSCON provides a safe recovery method using hints even in the rare case of forgotten secure icon. The feature of the hint algorithm that PASSCON provides is how to engage a trusted third party in the hinting process. The hint for the security icon can be defined and registered by the user on a text basis and can be received from the server through a third party.

When you want to repair the PASSCON after changing or adding the device or initializing the device, you should submit the photo used as digital ink material. At this time, the photographs can hardly be remembered or found, and may even have been deleted. In this case, the hint function can be used to search and download the pictures stored in the server. In this way, PASSCON can be used at all times with safe account recovery while avoiding the stress to remember in any case.

4.2. PASSCON Key Features

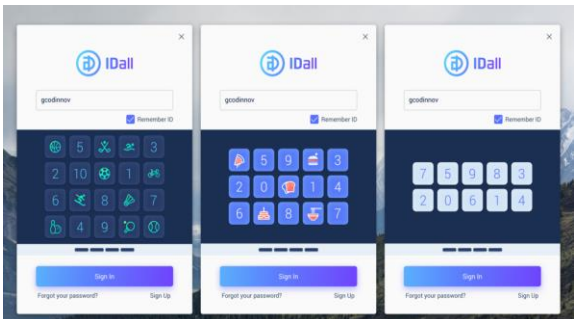


Fig 23: Password Icon (PASSCON) Dashboard

5. Conclusion

Security vulnerabilities in passwords and their consequences have been addressed for decades and many efforts and investments have been made. However, even now that biometrics has become a hot topic, this problem has not been solved. It is because there is also the advantage of the password. So it's time for everyone to understand it like a password, apply it everywhere, and at the same time need very secure authentication technology.

PASSCON is very easy to use and easy to understand and use by icon dashboard. It also offers high availability and compatibility that is applicable everywhere. In addition, it is a technology designed with a very secure and unique algorithm that cannot be used by attackers immediately, even if all authentication factors are stolen. Even the user can change most of the authentication factors with a simple touch without burdensome additional memory or effort to easily block stolen factors from being used by a third party.

The new digital signature authentication algorithm we propose works only on the user's dashboard as shown in Fig 23. Therefore, the text-based authentication factor is not allowed being entered arbitrarily at the endpoint, which is an important security flaw in password authentication. This can essentially block SQL Injection Attack or Brute Force Dictionary Attack.

In addition, Fig. 19. the digital ink (Passcore) is designed to be used only on the specified device, as it required by the verification of Passcore. Therefore, it prevents other devices from generating an electronic signature even if it is a correct icon key. That is, even if the key of the user credential is leaked, the user's account is protected.

Therefore, PASSCON is the best technology for safe and easy user authentication and digital signature, effectively replacing password input method.

References

[1] D. H, Choi, S. J. Kim, & D. H Won. One-Time Password Technology Ananlysis and its Standization Trend, Review Korea Institute of Information Security and Cryptology (2007)., Vol. 17, No. 3, pp. 12-17.

[2] Financial Security Institute Comparison of Credit Card Alternative Authentication Technology, Dept. Security Research, Team of Security Technology, (2016), pp.1-11

[3] H. B. Ahn, Status of Adaptation of FinTech in Korea, Communications of the Korean Institute of Information Scientists and Engineers (2016), Vol. 34, No. 4, pp. 29-33

[4] J. M. Sung, S. M. Lee, B. N. Noh, & S. H. Ahn, Extensional End-to-End Encryption Technologies to Enhance User's Financial Information Security and Considerable Security Issues. Journal of the Korea Institute of Information Security and Cryptology (2010), Vol. 20, No. No. 4, pp. 145-154

[5] Y. J. Shin. (2017). A Study on the Personal Information Protection for Improvement of Personal Identification: Focusing on the alternative means of resident number for users, Journal of Korean Regional Information (2017), Vol. 20, No. 2, pp. 1-2

[6] Seungjin Han. (2018). A Secure Decentralized Storage Scheme of Private Information in Blockchain Environments. Journal of Computer Information Society, 23(1), pp. 111-116.

[7] TSUDIK, Gene. Message authentication with one-way hash functions. In: INFOCOM'92. Eleventh Annual Joint Conference of the IEEE Computer and Communications Societies, IEEE. IEEE, 1992. pp. 2055-2059.

[8] GRZONKOWSKI, Slawomir; CORCORAN, Peter M.; COUGHLIN, Thomas. Security analysis of authentication protocols for next-generation mobile and CE cloud services. In: Consumer Electronics-Berlin (ICCE-Berlin), 2011 IEEE International Conference on. IEEE, 2011. pp. 83-87.

[9] McMahon, R., Bressler, M. S., & Bressler, L. (2016). New global cybercrime calls for high-tech cyber-cops. Journal of Legal, Ethical and Regulatory Issues, 19(1), pp.1-3.

[10] Y. J. Park, Y. H. Lim, M. S. Chae, A Study on Passwordless Authentication Technology and Its Effects, International Journal of Reliable Information and Assurance (2018), 6(1), pp.1-5