AN EFFECTUAL SECURED AUTHENTICATION APPROACH USING DYNAMIC ONE TIME PASSWORD AGAINST MiTM ATTACKS

I.Selvamani

Professor,Department of ECE, Malla Reddy College of Engineering for Women,Hyderabad,India.
Head(R& D), Malla Reddy College of Engineering for Women,Hyderabad,India.

Abstract: Numerous attacks on authentication of user have been launched against network-dependent companies, involving on-line financial services. To safeguard businesses as well as clients from security threats, there is a mighty need to build and introduce more reliable schemes for authentication. However, due to their security nature or excessive overheads, these systems have been shown to be ineffective. To solve this dilemma, a modified version of OTP termed as Dynamic One Time Password (DOTPass) is developed to make the networks more secure and to prevent MiTM attack. The calculation uses the dynamic combination of the user's secret key with the randomly generated OTP and the secret key is known only to the client. This approach generates an OTP that can be used to secure the sensitive association rules retrieved and shared with third-party users.
Keywords: OTP, DOTPass, MiTM Attack, Sensitive Rules, Security.

1 INTRODUCTION

Boosted by the revolution of information technology, computing with data has transformed as a promising area [1] with domains inclusive of economics, transportation, medical services, climate, social as well as urban planning [2]. Fortunately, the widespread use of big data poses new data protection challenges, especially when it deals with sensitive data like trade secrets, health data as well as personal information. There is a need to protect sensitive data from possible threats in order to get increased benefit out of this data [3-5]. With the growing number of Internet users as well as applications, it's more critical than ever to control user actions for effective access control and security monitoring. Because of the vast traffic data as well as broad variety of users, monitoring user activity characters of backbone or huge business networks is a difficult challenge [6, 7]. The collection of data must be delay-tolerant as well as exploiting strategies for secured storage acquired data locally, preserving users' privacy if sharing of computers by several users occur or stolen when holding few data [8-10]. The situation becomes much more complex when we consider network security. The additional protection devices make network configuration even more difficult. Furthermore, security systems provide a wide range of security features that can be used for a variety of purposes [11-13]. Cyber security risks, on the other hand, reach beyond the information infrastructure to the security system in networks. Various attacks can disrupt the normal functioning of the network, resulting in severe consequences for privacy [14, 15]. In order to combat these risks, networks must meet two essential security requirements: confidentiality and authentication. The sensitive messages cannot be read because of confidentiality. Authentication ensures that message recipients can determine the origin of a transmission and that no one can impersonate the message source [16, 17]. Most recent research on security network coding has focused on traditional encryption, which is based on computational security. The rapid advancement of hardware technology, on the other hand, might be able to crack the computational security nature. Furthermore, the complicated key management infrastructure makes the cryptographic security of incoming 5G applications less appealing [18, 19]. Numerous cryptographic authentication methods have been suggested to avoid unauthorized access. Since intruders cannot be authenticated, these approaches are based on the assumption that authenticated individuals can be fully trusted. Expanding attack tactics, like advanced persistent threats and social engineering attacks, however, are tearing the base apart [20]. Proposing a realistic OTP architecture is thought to aid in securing authentication to a wide range of services of network. One-time passwords (OTPs), enabling users to be authenticated with the acceptance to own a value which is pre-shared, are amongst the major common occupancy considerations in two-factor authentication [21, 22]. In OTP security scheme, secret keys are utilized for securing the data and an enhanced secrecy is obtained [23]. The fact that OTPs are chained is the key security problem with their validation. During the missing of OTP, the chain is split, and the authentication mechanism must re-negotiate an updated initial seed S and device number N due to the links among OTPs [24]. It provided a better solution to replay attack in which the unauthorized user intercept the password and replay it again and again. But it is vulnerable to MITM attack because these OTP's are the plain text randomly generated number. The hacker can in between intercept the OTP or through mobile sniffing these OTP can be

hacked. Considering these factors, an efficient algorithm is developed in this work which contributes,

- Generation of the unique passcode for user authentication that is the combination of secret key of the client and the generated OTP.
- Calculation of the dynamic OTP and its application in the field of data mining while data is shared between multiple users.

Section 2 includes the related studies, Section 3 explains the proposed work, Section 4 includes conclusion and future work.

2 RELATED STUDIES

Jung et al [25] applied MITM attacks for learning with errors replacing search of exhaustive type. An algorithm was utilized for this approach and better analysis is performed. The resultant attack cost was dependent on the square root of the count of secret vector of the user, and was mildly sensitive regarding the absolute error size at the condition of minimal value of ratio between modulus and error.

Cheng et al [26] investigated the vigorous threats occurring in the Openflow control channel caused by Man-in-the-Middle attacks. A practicable stereotype was initially introduced in the framework, and further tasks for revealing the intrusions were implemented. In addition, a lightweight remedy utilizing Bloom filters was proposed and a prototype for monitoring stealthy packet change was introduced.

Qiao et al [27] described a methodology with minimal-latency, improved-reliability for avoiding the attack of MITM. Depending on this, authentication of access of device and communication service was demonstrated. Next, a methodology for the authentication of access which describes the influence of radio frequency was demonstrated.

Siavash et al [28] provided an updated search for obtaining appropriate attacks in a particular time. On examining, the proposed algorithm, offered automatic attack together with specific suggestions. The aim of this article was generalizing the MITM attack, and this attack was regarded as a common format of certain attacks which existed, in a manner that these attacks could be identified with the help of automatic search approach.

Fan et al [29] introduced a detection system for cyber-attack related to improve the cybersecurity, constructed on the defense-in-depth concept generated adopting estimated process parameters. This detection system for attack offers defence of various layers for gaining the valuable duration of the defender prior the occurrence of consequences which are unrecoverable considering the physical system.

Ibrahim et al [30] evaluated the functioning of the proposed framework regarding the detection of attacks as well as minimizing pseudo alarms. The obtained results were compared utilizing the configurations which are single-metric as well as multi-metric. The efficient chance for combining metrics to detect the performance was determined but these metrics were not efficient for all types of attacks.

3 PROPOSED METHODOLOGY

3.1 Procedure For Authentication

The authentication procedure comprises of four subtasks named as sign up duration, generation of OTP, transferring to server the facts of authentication, verification.

3.1.1 Signing up Duration

During signing up, user is provided with an account number as well as password which is stationary in nature which is further hashed to Password Digest, PD= W (password). The account number of the user along with its PD will be stored in the server database.

3.1.2 Generation of OTP

It is generated by the password of the user and the process flow is shown in figure 1. For achieving the dynamic property of OTP timing, a time factor is utilized in the generation process. The OTP is generated in the MAC address which is utilized for achieving spacing dynamism.

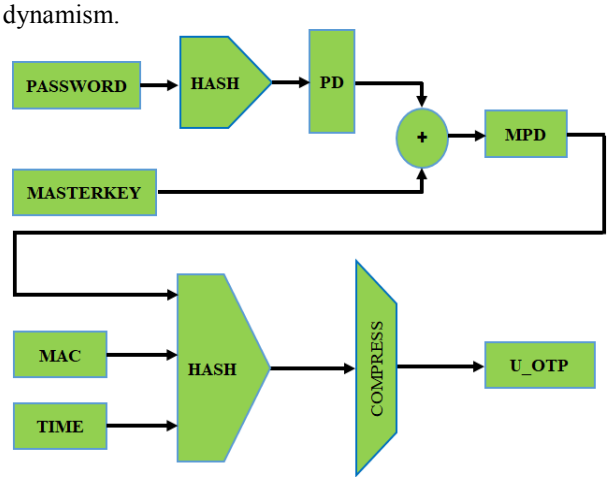

Figure 1 Generation of OTP

Initially, the password, user input will be hashed to obtain PD and then XORing with masterkey occurs for generating the masterkey password digest (MPD). This along with Media Access Control (MAC) and time compresses the message for generating the OTP. This

compression procedure is not mandatory and is required only during the handling of long OTPs. It is based on the security balance as well as the requirements of convenience. The result obtained will be the signature of the user at particular time and on particular machine.

3.1.3 Transfer of Authentication facts to the Server

The inputting of user in hand typing or replicating the user's password is done. The user's MAC address is transferred to server with information about authentication. The transfer of authentication details to server occurs only when the authentication and OTP generation is implemented by the user on the same machine. The process flow is given in figure 2.

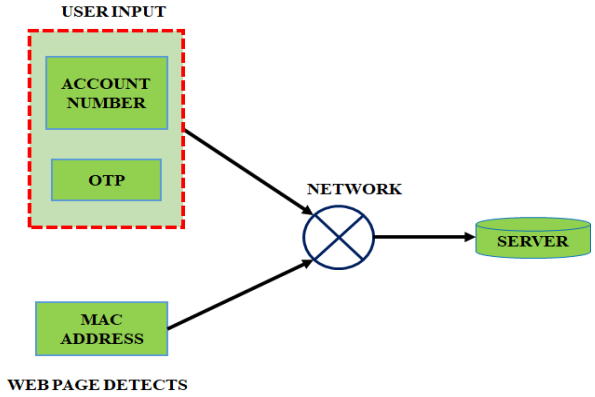

Figure 2 Transfer of authentication details to the server

3.1.4 Verification

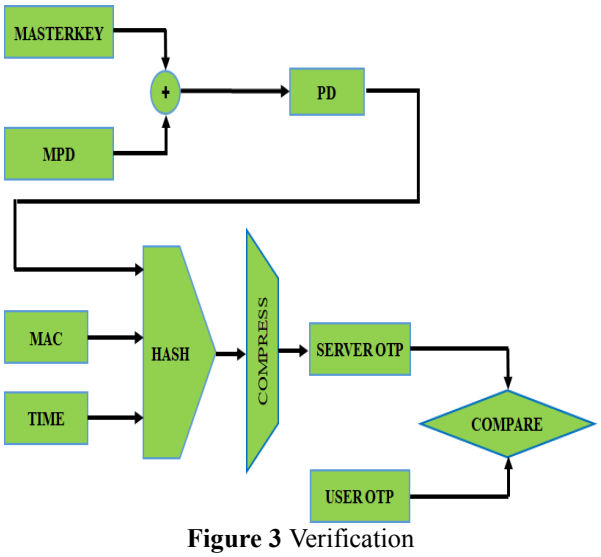

Figure 3 Verification

On receiving the details of authentication, the verification is implemented by the server consisting of the extraction of the user's MAC address, generation of OTP and comparison of details of authentication. The PD of the user can be extracted from the database and the MAC of the user is available easily. When the OTP of the server is similar to the OTP of the user, then the user is referred to be legitimate. The process flow is illustrated in figure 3.

3.2 Synchronization of Time

There is a need for server in implementing generation of OTP utilizing time factor similar to the user for the generation of OTP which is identical. For achieving synchronization of time, two concepts to be adopted are introduced.

3.2.1 Addition of Time Factor to OTP

A general conclusion for the synchronization is the addition of information about time to OTP. Hence the concluded dynamic password comprises of two portions named as user OTP and time information. The structure of the dynamic password is shown in figure 4.

User OTP	Time

Figure 4 Structure of dynamic password

Through this way, the server receives the information about time from the dynamic password received. The addition of information leads to increased OTP length, adding inconvenience to the user input. When the information about time demands encryption because of requirements of security, the resultant dynamic password length will be long.

3.2.2 Server Guess Methodology

In this methodology, the server is granted with the access to permit the user in guessing the time for the generation of OTP. Consider the duration of valid time of OTP is VT, the time for the generation of OTP by the user is UT. The time factor utilized for the generation of OTP is given by,

$$Time\ factor = UT - UT\ mod\ \frac{VT}{2}$$

When the authentication time is received by the server, two guesses will be performed by the server. Initially, the server will utilize $ST - ST\ mod\ \frac{VT}{2}$ as time factor for generating OTP. If the initially guessed OTP is similar to the OTP of the user, the process of guessing will be stopped the user obtains successful

authentication. If the initially guessed OTP is not similar to the OTP of the user, the server will utilize $ST - ST\ mod(VT)$ for implementing the generation of second OTP and second comparison.

3.2.3 Comparison of Methodologies

Both the addition of time factor to OTP and server guessing methods contribute the synchronization of time. The addition method is simpler and efficacious for application when compared to the other. The former performs addition of length of dynamic password when the guessing method is opted. The user's system duration must be steady but not easier because of various durations or invalid duration. Hence, network time protocol is adopted for achieving consistency within the user and server. The generation of OTP will adopt network time protocol for grabbing the time of internet replacing the user's system time.

3.2.4 Spacing Dynamism

It is implemented utilizing MAC address and every machine possess a specific address of MAC. With combining the address of MAC and generation of OTP, OTP is applicable. If the hacker uses the OTP of the user to login, the authentication cannot be successful since the MAC address of the PC of the hacker is not similar to the PC of the user.

3.2.5 Encoding

Since the result of the hash function is in the form of a binary string, encoding approach is utilized for presenting a readable as well as type-able to the user. Prior to encoding process, the data is to be restricted to a specific range. During encoding, the actual binary string is converted into binary bits of finite length. These systems for encoding possess a key distribution problem as well as issues related to security of the operator. The encoding in generation of OTP is widely utilized due to its ability to protect data efficiently and is performed with the bit strings. The data, $d \in \{0,1\}^n$ for values of n and encoding is performed with the secret key $s \in \{0,1\}^n$ for values of n. The function for encoding , F performs mapping of the OTP key which is secret as well as the text message with the ciphertext, $t \in \{0,1\}^n$ for values of n.

3.2.6 Decoding

Following the encoding of data, decoding is performed for recovering the representation of actual OTP which is encoded. The obtained OTP is compared with the user OTP which is encoded by the user at the registration of account. For recovering the data, the mapping of key is performed with the ciphertext, t and the plaintext message is recovered.

4 RESULTS AND DISCUSSION

The analysis of the security offered by the proposed approach includes the following parameters.

4.1 Utilization of Hash Function

The password of user is stored in the database utilizing a hash function in a cypher fashion. Through doing so, the hacker would be unable to obtain the password of the user due to attacks. The hacker receives the password through the server's master key but the OTP generation is difficult. The output of the hash function generates the OTP which is fed to the network and hackers would not be able to deduce the stationary password of the user.

4.2 Time Factor

To achieve timing dynamism, a time factor is introduced in the process for generating OTP. The updation of OTP is performed in a minimal duration of time. The amount of reasonable time is customised with the choice of user.

4.3 Address of MAC

The use of space factor by MAC denotes the manner of utilization of space factor for solving the spacing dynamism problem. Since each machine's MAC address is unique, MAC addresses can be used to demonstrate the use of "what you have" in authentication techniques. There is no way for a hacker to successfully authenticate even though he gets all of the authentication information and perform its implementation in the reasonable OTP time. The MAC of the hacker is utilized for creating OTP, and is completely variable considering the user . The combination of spacing as well as timing dynamism ensures that the strategy is safe against Perfect-Man-In-The-Middle attacks.

4.4 Generation of OTP

Unlike other two-factor authentication schemes, the OTP is generated using software, and is cost-effective as well as simpler. The benefit of the proposed concept is that it is more comprehensible, since the calculation of OTP is not requird by the user.

The proposed system is tested for various inputs and the response time for the corresponding inputs are evaluated as in table 1. The table clearly indicates that

the time of response for the generation of OTP is quicker due to the minimal information which is to be hashed.

Table 1 Response time for various tests

Test number	Response time
1	0.005
2	0.006
3	0.014
4	0.007
5	0.006
6	0.005

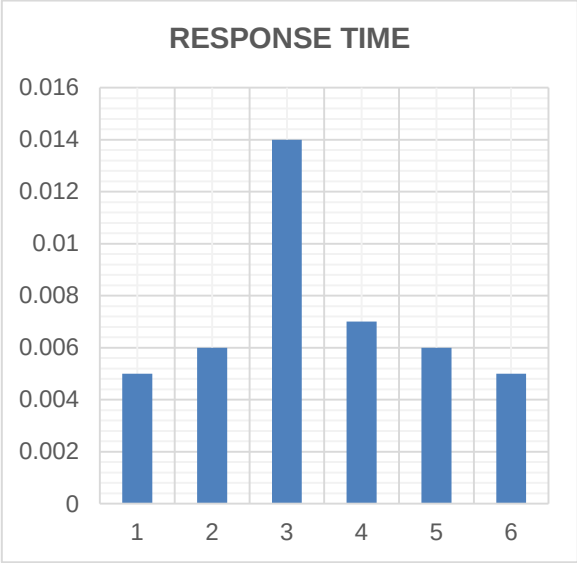

Figure 5 Plot for response time

On the server side, the time it takes to retrieve the account number of the user and password from the database would have the greatest impact on results, rather than the time it takes to generate an OTP and compare authentication information. The characteristic plot for table 1 is indicated in figure 5.

The proposed methodology for the generation of dynamic password is tested with the help of 150 participants with varied genders and ages. This selected population comprised of 100 men as well as 50 women. These candidates' ages were within the range of 15 to 65 and the corresponding distribution is shown in figure6.

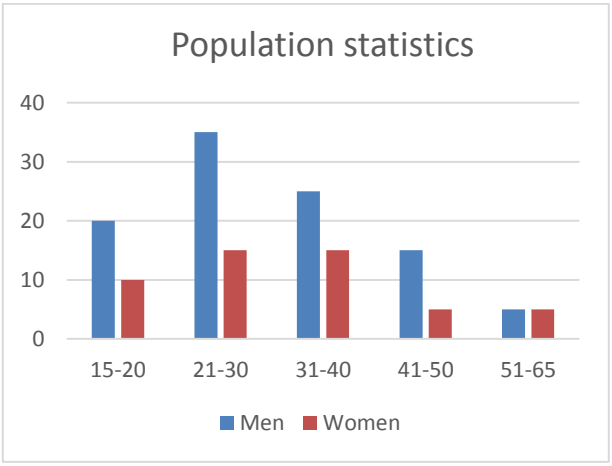

Figure 6 Statistics of population

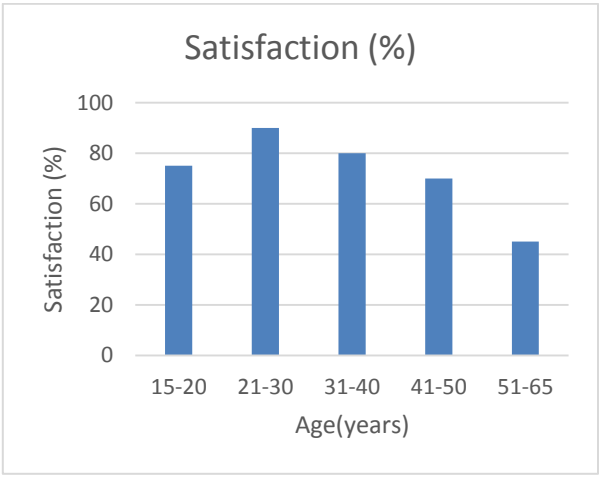

Figure 7 Satisfaction percentage

Prior the utilization of authentication the satisfaction of the proposed approach is analysed among the users and the results are obtained as given in figure 7. From the graph it is clear that the age group 21-30 showed improved satisfaction while the age group 51-65 showed decreased satisfaction.

6 CONCLUSION AND FUTURE WORK

OTP is the two-factor authentication approach that safeguards several online applications from critical threats and attacks, providing authentication of real time. Even so, since these OTPs are plain text randomly generated numbers, they are prone to MITM attacks.

In this article, a novel concept is presented for developing DOTPass by incorporating the user secret key with the OTP that adds an extra layer of security and a solution to the MITM attack. After the mining processes,

these rules are retrieved and shared with third parties for good decision making. This dynamic OTP technique makes it extremely difficult for unauthorized users to obtain the rules; even if they do, the OTP will only be active for 5 minutes, and the user should have legitimate instructions in order to generate the correct OTP. As a result, even to gain unauthorized access to the system, an individual must be available in the same room. Future works may concentrate on methodologies against phishing attacks.

References

[1] Rong Jiang, Mingyue Shi,Wei Zhou, "A Privacy Security Risk Analysis Method for Medical Big Data in Urban Computing", IEEE Access, Vol. 7, pp. 143841 – 143854, 2019.

[2] Nicholas Jing Yuan,Yu Zheng, Xing Xie, Yingzi Wang, Kai Zheng, HuiXiong,"Discovering Urban functional ones using latent activity trajectories", IEEE Transactions on Knowledge and Data Engineering, Vol. 27, no. 3, pp. 712 – 725, 2015.

[3] Ismail Hababeh, Ammar Gharaibeh, Samer Nofal, Issa Khalil, "An Integrated Methodology for Big Data Classification and Security for Improving Cloud Systems Data Mobility", IEEE Access, Vol. 7 , pp. 9153 – 9163, 2019

[4] Victor Chang, Muthu Ramachandran, "Towards Achieving Data Security with the Cloud Computing Adoption Framework", IEEE Transactions on Services Computing, Vol. 9, no. 1, pp. 138 – 151, 2016

[5] Julio Moreno, Eduardo B, Fernandez, Manuel A. Serrano, Eduardo Fernández-Medina, "Secure Development of Big Data Ecosystems", IEEE Access, Vol. 7, pp. 96604 – 96619, 2019.

[6] Tao Qin, Xiaohong Guan, Chenxu Wang, Zhaoli Liu, "MUCM: Multilevel User Cluster Mining Based on Behavior Profiles for Network Monitoring", IEEE Systems Journal, Vol. 9, no. 4, pp. 1322 - 1333, 2015.

[7] Chen, Min, Yongfeng Qian, Shiwen Mao, Wan Tang, and Ximin Yang, "Software-defined mobile networks security", Mobile Networks and Applications, Vol. 21, no. 5, pp. 729-743, 2016.

[8] Marcos A. Simplicio, Leonardo H. Iwaya, Bruno M. Barros, Tereza C. M. B. Carvalho, Mats Näslund, "SecourHealth: A Delay-Tolerant Security Framework for Mobile Health Data Collection", IEEE Journal of Biomedical and Health Informatics, Vol. 19, no. 2, pp. 761 – 772, 2015.

[9] Shi-Cho Cha, Kuo-Hui Yeh, "A Data-Driven Security Risk Assessment Scheme for Personal Data Protection", IEEE Access, Vol. 6, pp. 50510 – 50517, 2018.

[10] Fanyu Kong, Yufeng Zhou, Bin Xia, Li Pan, Limin Zhu, "A Security Reputation Model for IoT Health Data Using S-AlexNet and Dynamic Game Theory in Cloud Computing Environment", IEEE Access, Vol. 7, pp. 161822 – 161830, 2019.

[11] Seungwon Shin, Haopei Wang, Guofei Gu, "A First Step Toward Network Security Virtualization: From Concept To Prototype", IEEE Transactions on Information Forensics and Security, Vol. 10, no. 10, pp. 2236 – 2249, 2015.

[12] Alireza Shameli-Sendi, Yosr Jarraya, Makan Pourzandi, Mohamed Cheriet, "Efficient Provisioning of Security Service Function Chaining Using Network Security Defense Patterns", IEEE Transactions on Services Computing, Vol. 12, no. 4, pp. 534 – 549, 2016.

[13] Jun Wu, Kaoru Ota, Mianxiong Dong;J ianhua Li;Hongkai Wang, "Big Data Analysis-Based Security Situational Awareness for Smart Grid", IEEE Transactions on Big Data, Vol. 4, no. 3, pp. 408 – 417, 2018.

[14] Vijay Varadharajan, Kallol Karmakar; Uday Tupakula, Michael Hitchens, "A Policy-Based Security Architecture for Software-Defined Networks", IEEE Transactions on Information Forensics and Security, Vol. 14, pp. 897 – 912, 2019.

[15] Tanja Zseby, Félix Iglesias Vázquez, Alistair King, K. C. Claffy, "Teaching Network Security With IP Darkspace Data", IEEE Transactions on Education, Vol. 59, no. 1, pp. 1 – 7, 2016.

[16] Liu, Yiliang, Hsiao-Hwa Chen, and Liangmin Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges", IEEE Communications Surveys & Tutorials, Vol. 19, no. 1 , pp. 347-376, 2016.

[17] Yuanyuan Kong, Bin Lyu, Feng Chen, Zhen Yang, "The Security Network Coding System With Physical Layer Key Generation in Two-Way Relay Networks", IEEE Access, Vol. 6, pp. 40673 – 40681, 2018.

[18] Sarika, S., A. Pravin, A. Vijayakumar, and K. Selvamani, "Security issues in mobile ad hoc networks", Procedia Computer Science, Vol. 92, pp. 329-335, 2016.

[19] Fang, Dongfeng, Yi Qian, and Rose Qingyang Hu., "Security for 5G mobile wireless networks", IEEE Access, Vol. 6 , pp. 4850-4874, 2017.

[20] Shuaishuai Tan, Xiaoping Li, Qingkuan Dong, "TrustR: An Integrated Router Security Framework for Protecting Computer Networks", IEEE Communications Letters, Vol. 20, no. 2, pp. 376 – 379, 2016

[21] Emir Erdem, Mehmet Tahir Sandıkkaya, "OTPaaS—One Time Password as a Service", IEEE Transactions on Information Forensics and Security, Vol. 14, no. 3, pp. 743 – 756, 2019.

[22] Bartłomiejczyk Maciej, El Fray Imed, Mirosław Kurkowski, "Multifactor Authentication Protocol in a Mobile Environment", IEEE Access, Vol. 7, pp. 157185 – 157199, 2019.

[23] Ahmed El Shafie, Asma Mabrouk, Kamel Tourki, Naofal Al-Dhahir, Ridha Hamila, "A Secret-Key-Aided Scheme to Secure Transmissions From Single-Antenna RF-EH

Source Nodes", IEEE Wireless Communications Letters, Vol. 7, no. 2, pp. 238 – 241, 2018.

[24] Tong Xu, Deyun Gao, Ping Dong, Chuan Heng Foh, Hongke Zhang, Victor C. M. Leung, "Improving the Security of Wireless Communications on High-Speed Trains by Efficient Authentication in SCN-R", IEEE Transactions on Vehicular Technology, Vol. 68, no. 8, pp. 7283 – 7295, 2019.

[25] Cheon, Jung Hee, Minki Hhan, Seungwan Hong, and Yongha Son, "A hybrid of dual and meet-in-the-middle attack on sparse and ternary secret LWE", IEEE Access, Vol. 7, pp. 89497-89506, 2019.

[26] Li, Cheng, Zhengrui Qin, Ed Novak, and Qun Li. "Securing SDN infrastructure of IoT–fog networks from MitM attacks" , IEEE Internet of Things Journal, Vol. 4, no. 5, pp. 1156-1164, 2017.

[27] Tian, Qiao, Yun Lin, Xinghao Guo, Jinming Wen, Yi Fang, Jonathan Rodriguez, and Shahid Mumtaz, "New security mechanisms of high-reliability IoT communication based on radio frequency fingerprint", IEEE Internet of Things Journal, Vol. 6, no. 5, pp. 7980-7987, 2019.

[28] Ahmadi, Siavash, and Mohammad Reza Aref., "Generalized meet in the middle cryptanalysis of block ciphers with an automated search algorithm", IEEE Access, Vol. 8, pp. 2284-2301, 2019.

[29] Zhang, Fan, Hansaka Angel Dias Edirisinghe Kodituwakku, J. Wesley Hines, and Jamie Coble, "Multilayer data-driven cyber-attack detection system for industrial control systems based on network, system, and process data", IEEE Transactions on Industrial Informatics, Vol.15, no. 7, pp. 4362-4369, 2019.

[30] Ibrahim Ghafir, Konstantinos G, Kyriakopoulos, Francisco J, Aparicio-Navarro, Sangarapillai Lambotharan, Basil Assadhan, Hamad Binsalleeh, "A Basic Probability Assignment Methodology for Unsupervised Wireless Intrusion Detection", IEEE Access, Vol. 6, pp. 40008 – 40023, 2018.