Client-Server Based Authentication Against MITM Attack via Fast Communication for IIoT Devices

M. Kara, and M. Furat

Abstract—**Security is an important issue that should be taken care of by every system. In recent years, however, attackers are constantly developing themselves with new techniques to obtain personal information on the network. As systems evolve, the data that needs to be protected is increasingly appreciated and carries a higher risk of attack. As with many attacks such as MITM, there are solutions against this attacks. Nevertheless, these safety measures must be developed continuously. For this reason, we have developed a new system architecture with user-defined authentication against the intruders for the systems having large amount of data transmission rate. To maintain integrity of data, over a reliable system is that all incoming data are authenticated when data send to the server, on the other hand, in this system, the user-defined authentication can provide fast communication and it can decrease authentication time. The proposed system introduced in the present study checks for any changes in our instantaneous data. Moreover, we control the data integrity on simple devices such as sensors and motors or other industrial devices. Instead of using encryption, basically client-server based authentication system is used to avoid complex operations and protect the big data.**

Index Terms—**Client-server based authentication, IIoT, MITM, Security**

I. Introduction

TODAY'S Internet of Things (IoT) technology world, we are trying to store and qualify the data that millions of sensors have produced. This situation occurs big data. Big data comes from the combination of thousands of sensors creates security risks for large scale network. We must take measures to protect big data and take precautions for the safety of these critical system clearly.

Along with the developing IoT device technology such as wireless sensors [1], attacks on the network system are increasing in recent years. It is vital to detect these attacks and protect our network system, especially in the industrial fields. IoT means Industrial Internet of Things (IIoT) in the industrial systems. If we examine them in detail, IIoT and IoT are absolutely different. IIoT technology includes networked smart power, factory and manufacturing. For this reason, IIoT devices require rapid communication between themselves and must be protected against harmful attack.

Intrusion Detection Systems (IDS) on a computer network is a first step of preventing the system to malicious use [2]. Sending to the main servers to analyze the information from various sensors is vital to large areas such as industrial areas. Therefore, intrusion detection systems have been developed. IDS may prevent many important damages for our system. IDS can be basically divided into two broad categories with respect to its architecture. [3]. Even then, a hybrid third one was developed by combining these two architectures. However, these architectures are basically similar in appearance to similar technologies in their application areas. Intrusion detection systems detect attacks made by instant analysis. The central server analyzes the events at different times with a base detection system.

We propose a new system architecture with user-defined authentication that simultaneously put on authentication and industrial field control at the same time. Besides we present a fast and secure client-server based system instead of encryption algorithms. In this study, the system architecture with user-defined authentications explained and the performance is discussed with popular encryption algorithms.

The IDS, which basically work with Host-based Intrusion Detection Systems (HIDS) concept, have turned into use Network-based Intrusion Detection Systems (NIDS) technology over time with different needs. HIDS are slightly different from the NIDS in that it is the technology in the protected computer. HIDS will not receive untrained traffic to the main computer under protection by itself. Instead, the HIDS tool monitors critical system file packages or files on the machine [4] and disconnects the network when there is an attack. It notifies a central management console. NIDS is deployed at strategic locations in the network system infrastructure (outside the firewall, especially in areas like the Demilitarized Zone, DMZ) to control traffic flow and compare known attack types against a database [5].

M. KARA, is with Department of Electrical Department, Mustafa Kemal University, Hatay, Turkey, (e-mail: mustafakara@mku.edu.tr)

✉ **M. FURAT**, is with Department of Electrical and Electronics Engineering Iskenderun University, Iskenderun, Turkey, (e-mail: murat.furat@iste.edu.tr)

Manuscript received August 11, 2017; accepted Nov 16, 2017.
DOI: 10.17694/bajece.419546

The intrusion detection systems, main server-based, are the focus of this article. In this paper, implemented with appropriate network connection is proposed to deal with intrusion detection problems using HIDS technology. Authentication system is designed to trigger instant attacks by performing key matching with specific functions. Thus, information obtained from instantaneous data generating devices such as sensors will be determined to have not undergone any changes during transmission.

The present paper is organized as follows. Section 2 describes the need for security, section 3 compares the methods of encrypting with the intrusion detection system, and explains why the IDS are preferred. Potential cyber threats are given in section 4 and the proposed system structure is presented in section 5. The conclusion can be found in the last section.

II. Big Data Needs Big Security

It's no secret that encryption is large proponents of data security. Attacks such as network misuse on the security side, data modification, data theft and unauthorized access to IoT devices should be avoided by taking security precautions. Data security is the most important factor in network construction. Because of this, industrial companies are trying to provide data security by making a monetary investment in a large amount.

Large scale systems depend on computers or servers to control field devices. By the nature of computer systems, important amount of data that is controlled and processed is very important and sensitive. Because of this reason, big data requires protection against intruders. In the light of this information, Big Data needs Big Security. For example, one the most important device of a plant could be seized and a different value is sent to the authentication server by changing the temperature, humidity or pressure sensor values and this will be a problem for large fields. Security for data integrity is vital for cyber physical system [6].

III. Comparison

A. Intrusion Detection Systems

Intrusion Detection System [3, 4] is a network security system designed to detect security vulnerabilities against applications that are likely to be attacked or computer systems. An IDS technology is used to detect explicit attacks and is out of bandwidth in the networking system; It finds no real-time communication between the server and the client as illustrated in Fig.1. Obviously, the IDS technology to be described here is just a listening device. The IDS monitors the network traffic instantly and reports its results to a system administrator, but cannot automatically take action to prevent a detected exploit from taking over the system.

To summarize, the three main functions of the IDS include controlling (evaluating), examining (detecting), and reacting (reporting) the attacking eyebrows in software systems and networks [7].

Intrusion detection system can be divided into three categories with respect to their architectures [3, 7] as shown in Table 1.

1) Host-based Intrusion Detection System

The host-based intrusion detection system allows critical incidents to be seen in transmission systems. One can also detect and respond to malicious attacks or unusual movements discovered in the network system. It checks data integrity and traces the network system.

2) Network-based Intrusion Detection System

A network-based intrusion detection system monitors the network traffic to protect a system from threats and analyzes it according to the information in its hand [4]. It reads all packages and examines the packages which detect as dangerous. The system categorizes dangerous packages and notifies IT (Information Technology) staff. It can also block the packets according to IP address.

3) Distributed Intrusion Detection System

Distributed Intrusion Detection Systems (DIDS) over a huge network [8], all of which communicate with each other, or with a central server that simplify developed network monitoring, event analysis, and instant attack data [9].

TABLE I
A COMPARISON OF DIFFERENT IDSS BASED ON THEIR ARCHITECTURE [7].

IDS Type	Deployment Location	Information source	Control domain
HIDS	Under-control system, software process	Local traffic (on OS level) and Log files	Local hosting system
NIDS	Isolated system on network traffic route, software process	Network traffic (raw data packets of the network)	Local segment or whole network
DIDS	Distributed and heterogeneous (host, network and central management system)	Host traffic and network traffic	Network wide (all hosts and different network segments)

B. Encryption

Encryption is a method that transforms the information on the computer into an unintelligible form. Hence, even if someone can access a network system with important data [10], it will not be able to do anything unless it is some special software or the original data key.

The main function of the encryption is to convert the not only a normal text into an encrypted text but also a binary data into an encrypted binary data. Encryption helps to ensure that the data is not readable by the unauthorized people.

There are three different basic encryption methods that have different advantages for themselves. Their properties are tabulated in Table 2. It is clearly seen from Table 2, encryption methods notice integrity, authentication and non-reputation.

1) *Hashing Functions*

The way of summarization functions work is to show a shorter area by taking a long input. The goal is to reflect on the exit when there is a change in the ground. An encryption hash function [11] is a type of algorithm that can be applied on a piece of data, such as a single file or password, and produces a result called a checksum. The logic underlying the encryption hash function is to verify the authenticity of the data packet. For example, two files can be the same, but only if the checksums generated from each file use the same encryption burst function. Some of the summarization functions are MD5 (Message-Digest algorithm 5) and SHA1 (Secure Hash Algorithm 1).

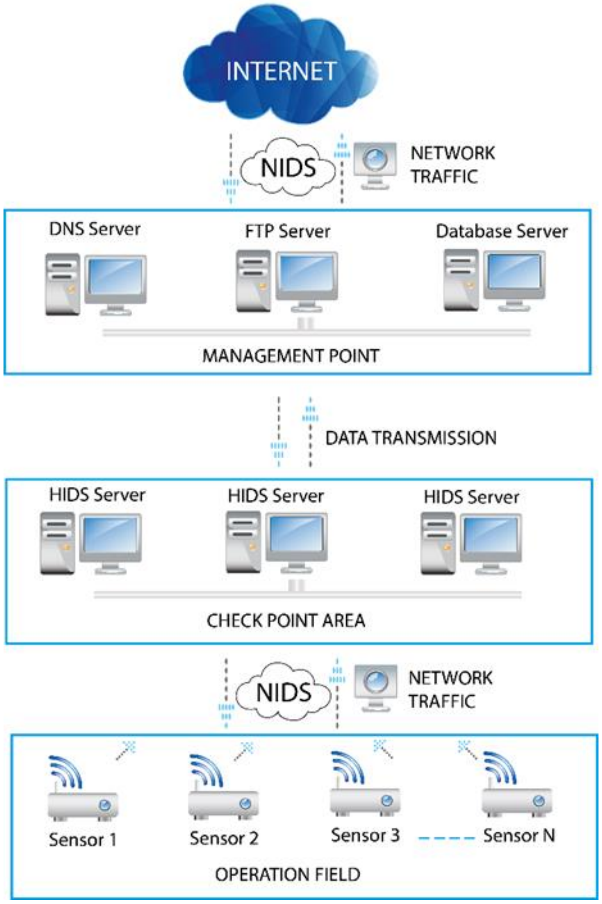

Fig 1. HIDS and NIDS are illustrated basically in the same picture in terms of how they work

TABLE II
CRYPTOGRAPHIC TECHNICS WITH KEY USAGE

Property	Hashing Functions	Symmetric Methods	Asymmetric Methods
Integrity	Yes	Yes	Yes
Authentication	No	Yes	Yes
Non-repudation	No	No	Yes
Key Usage	None	Symmetric Key(One key)	Assymmetric Key(two key)

2) *Symmetric Methods*

Symmetric methods care about integrity and authentication with a symmetric key. Essentially, symmetric algorithm means hash function with a key. Encrypt the whole data. AES (Advanced Encryption Standart) is a kind of symmetric key encryption [12].

3) *Asymmetric Methods*

Asymmetric encryption uses two keys for encryption or decryption. This method cares about integrity, authentication and non-reputation with the asymmetric key [13].

C. *Reason for IDS Selection*

Some systems, particularly networks that care about data coming from sensors, want to analyze whether only incoming information has been changed. Thus, they achieve both a faster system and a lower cost. Such systems in an industry can need to control the accuracy of instantaneous transmission by considering data integrity directly rather than encryption. Because symmetric [10] cryptosystems involve significant communication problems. The secret key is forwarded to the receiving system before sending the actual data. The system with the Internet connection is 99% safe so there is no guarantee that the hacker will not attack. For this reason, the only safe way to change the keys is to exchange them personally. There is no need encryption in some systems which care about data integrity to make process go faster.

In this paper, we developed a network system that allows verifying the identity of the sender. For this reason, we only care about data integrity during data transmission. We propose to select a user-defined authentication system in this network to determine if there is a change in the data package.

IV. CYBERSECURITY THREATS

The ever-evolving world of the internet is becoming the focus of hackers. As IoT technology evolves, attacks are increasing in species. In particular, aggressive tools such as botnets take advantage of the exploits in the system to capture the network. Security systems often catch many attackers on the network. However, imagine that an attacker has captured a system such as an industry or a large hospital. Let's consider a production site that works with very sensitive sensors. The risk of mortal accidents is very high when cameras and sensor devices are seized. As a real example, we have come to the conclusion that by the end of 2015, cyber-attacks [14] were a serious threat when Ukraine seized large portions of the electricity grid and proved to be dark in the middle of winter [15].

Currently, IoT technology brings a great deal of connectivity and convenience to modern day-like. However, the benefits created by IoT technology require manufacturers and users to be alert throughout the product life cycle. Protection against such danger must be provided by improved algorithms.

Today, the types of attacks are increasing. Some attacks can get some information between two computers that are in direct communication. The type of attack we are handling in this study is the man-in-the-middle attack (MITM). The MITM intercepts communication between the two network devices such as router, key server and switch etc. and this attack can change, modify or filter data [16].

The purpose of network security is to provide information security. This information security is based on 3 basic reasons: confidentiality, integrity and availability.

In some cases, the network's data may change because the data is gone through the intruder’s computer. In this cases, we need to know if there is an attack for changing the data. Otherwise, we cannot secure communication. So, IoT technology can never be passed in industry or any other huge systems.

Such attack as man-in-the-middle attack on confidentiality and integrity or Denial of Service Attack [17] on availability [18]. Compromised credentials, cross-site scripting, man-in-the-middle attack, data breach, denial-of-service attack, malicious insiders, arp-poisoning, malware, ransomware and spear phishing etc. There are many kinds of attacks that can be performed by intruders for capturing. There is too much danger in the transmission phase from device to device. That’s why, some attack detection algorithms should be developed to take precautions while transmitting the data.

Intrusion detection systems such as Firewalls, Network IDS, SNORT, Firestorm, Host IDS are developed to prevent the attacks [19]. However, these systems have the advantages of intrusion detection but have some disadvantages also. To explain some of them; Firewalls have legitimate user restriction, diminished performance, vulnerabilities, internal attack and high cost. For this reason, we use the firewall together with IDS to avoid many attacks. SNORT is an important system which rules define new attacks can easily be written and added. On the other hand, a kind of system which encrypted communications (VPNs, SSL, SSH, etc.) cannot be monitored, it cannot keep up with high volume traffic, network infrastructure requires change/editing and produce false alarms very intensely. Firestorm logs the data regularly every day using the administration console. But this brings overload to the system on the network. Our system removes the overload of computers. Because the network system is very simple. It just cares about data integrity and detects the intruders.

V. Client-Server Based Authentication System

The most important purpose of our system is to evaluate this big data obtained by IIoT devices with sensors in the industrial field. As the amount of data increases, attackers are regularly trying to change this files and logges. For this reason, we propose a system via HIDS. This intrusion system is a technology that works like a central server and scans its own systems for activities. Typically, HIDS scans daily or weekly files in the operating system, application log files, or files in the database to find attack traces. For this reason, HIDS only works depending on the daily or weekly received file. As a result of this dependent situation, HIDS cannot detect the occurrence of an attack on the network by itself if the data of the weekly database files are bad or the information is changed by the attacker.

When controlling the data coming from the sensors, we must move with an advanced algorithm by controlling the server entrance, taking filtering precautions, monitoring the events instantly and activating the warning system.

The result of the control scan performed by the host-based intrusion detection system is filed and logged securely and compared with logs to detect any malicious attempt. As a result of this situation, we propose a new system architecture with user-defined authentication. This is a kind of instant detection system for intruders.

A. Proposed System Architecture

Reliability of data integrity always needs security via observation. For this reason, the system must be installed with some rules on network system with actuator and sensors as follows:

- Monitor and check access to the variables instantaneously.
- Abnormal sensor data should be detected and attempted attack should be prevented.
- Real-time intrusion must be detected and alerted.
- After the attack, check the system and analyze the output event.
- Give a report to IT staff after alarm against the possibility of changing big data environments.

The proposed client-server based authentication system in an industrial plant network is illustrated in Fig. 2. In this network system, large amount of data produced instantly by thousands of sensors in an industrial field are supposed. In the context of IIoT, owing to the instant transmission in the proposed system is carried out through smart devices, the emerged large data is naturally in the network environment. This system requires the data transmission between industrial devices to be controlled and secure. For this reason, we propose an architecture for this system consisting of 3 layers. These are Sensor and Actuator Layer, Transmission Layer and Administrator and Management Layer.

First, the data produced by the field sensors data is sent from Sensor and Actuator Layer to Transmission Layer. The data reaching the Transmission Layer is collected by the Sensor Unit. The Sensor Unit transmits this data to the Authentication Server. The Authentication Server updates the sensor data depending on the functions defined by the system user. For example, these functions can be adapted to be able to authenticate within an algorithmic rule. After this process, the data is sent to the Administration and Management Layer. Within the Administration and Management Layer, Management Points or IT Staff departments make the necessary assessments. The evaluated data is sent to the Authentication Client Server in the Transmission Layer again. The Authentication Client Server controls the authenticity of these data with respect to the previously defined authentication rules. After control by the Authentication Client Server, if there is no attack trace in the coming data, it sends these new inputs to the controller unit. The Actuator Unit sends these control inputs to actuators in the industrial field. As a result, the proposed system works in a secure structure.

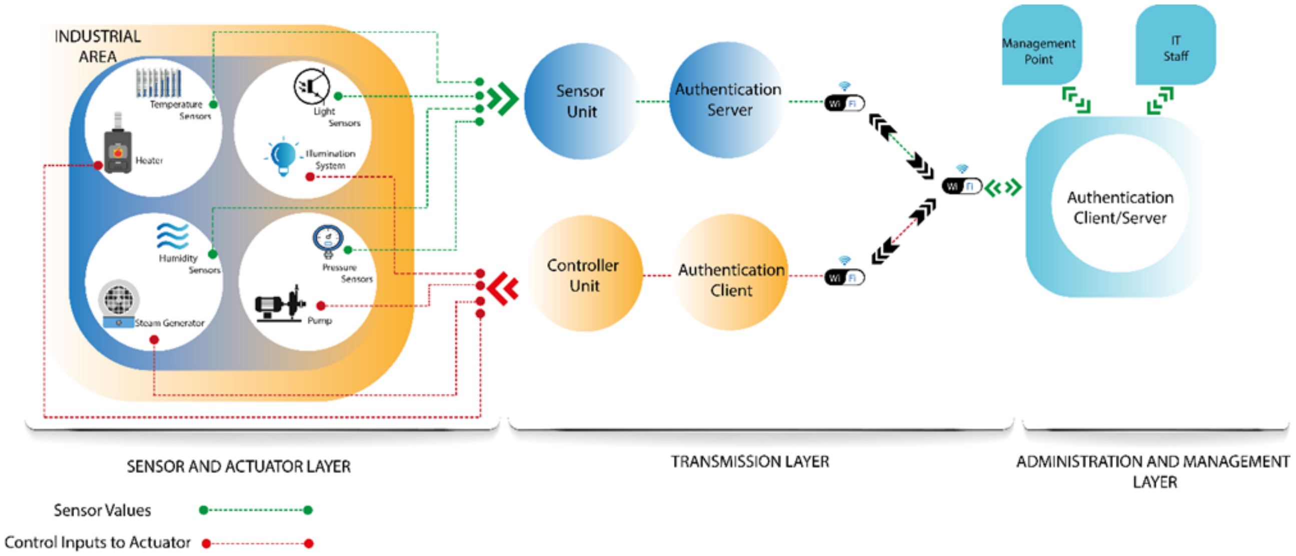

Fig.2. Proposed client-server based authentication system in an industrial plant network.

B. Proposed System Algorithm

The intrusion detection algorithm works within the proposed system can be summarized step by step as follows:

Step 1: The measurements of the sensors are collected in the sensor unit at each sampling time.

Step 2: The authentication server directly connected to the sensor unit adds a specific key to the sensors' data and sends the corresponding clients.

Step 3: The clients validates the data at first and then transmits the unit connected to itself.

Step 4: The tasks defined in Step 2 and 3 are valid for the Authentication Server/Client in Administration and Management Layer.

Step 5: If the validation is completed with success, then the data is proceeded.

Step 6: If the validation fails, then alarm is set to the IT staff and the data is logged.

Step 7: Stop

The flowchart of the algorithm is illustrated in Fig. 3.

C. User Defined Authentication

Authentication mechanism is one of the most effective ways to determination attacks. The proposed user-defined authentication technique has a lot of advantages over traditional encryption schemes.

First, the user-defined authentication procedures can be determined much simpler, and consequently. Then, it is much faster as compared to the encryption and decryption systems.

Second, the data traffic level can be reduced to very low levels in the industrial fields while sending data due to the authentication control based method here, together with the instantaneous comparison operations performed in the algorithm.

Third, the computation time is potentially reduced depending on the user-defined authentication function.

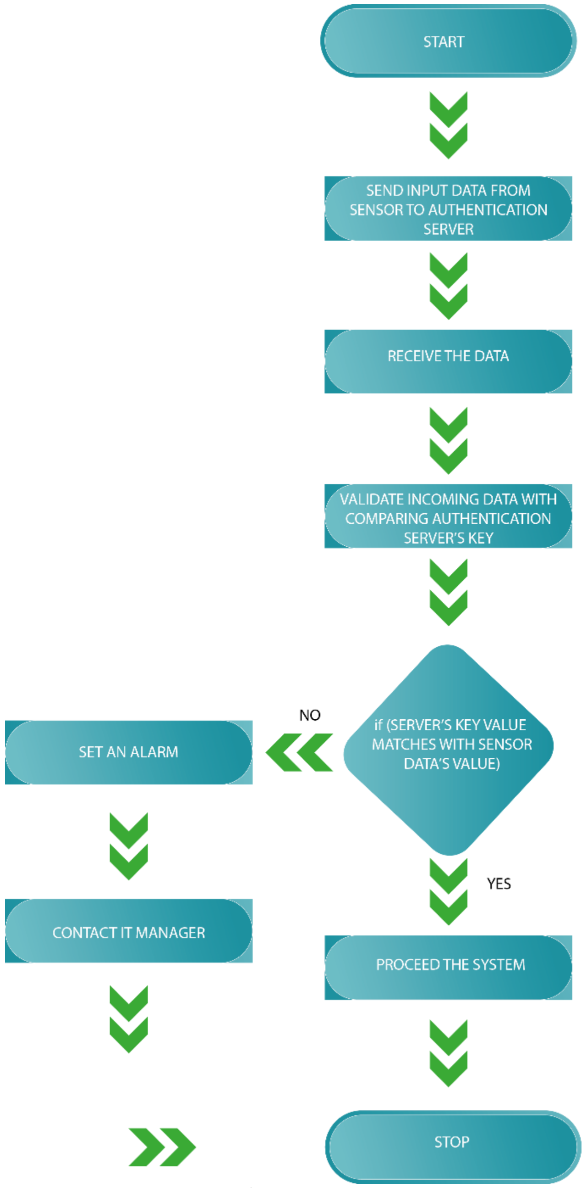
START
SEND INPUT DATA FROM SENSOR TO AUTHENTICATION SERVER
RECEIVE THE DATA
VALIDATE INCOMING DATA WITH COMPARING AUTHENTICATION SERVER'S KEY
if (SERVER'S KEY VALUE MATCHES WITH SENSOR DATA'S VALUE)
NO
SET AN ALARM
CONTACT IT MANAGER
YES
PROCEED THE SYSTEM
STOP

Fig 3. Flowchart of the proposed system algorithm.

VI. CONCLUSION

In recent years, IT staff in industrial systems want to detect the changes from the sensors during the instantaneous data transmission process. Taking this into account, the proposed system architecture with user-defined authentication works to ensure the confidentiality, accessibility and security integrity of the data transmission system. Our presented system, especially for IIoT technology, detects the modification of the packet at the moment of data transmission. This system provides high performance and efficient technology when compared with existing encryption techniques. This is very important if large amount of data transmissions exists in a system. Transmitted and stored correct data directly effects the reliability of the large systems, i.e. IIoT based large networks.

REFERENCES

[1] K. Hewage, S. Raza, and T. Voigt, "An experimental study of attacks on the availability of glossy". Computers & Electrical Engineering, V.41, 2015, pp. 115-125.

[2] B. Daya, "Network security: History importance and future", http://web.mit.edu/~bdaya/www/Network%20Security.pdf

[3] S. Parveen and C. Sharma. "A Survey: Intelligent Intrusion Detection System in Computer Security", International Journal of Computer Applications, Vol.151, No.3, 2016, pp.18-22.

[4] K. Nesreen, N. Hamdy and S. H. Ahmed, "A Proposed Intrusion Detection System for Encrypted Computer Networks", Third International Conference on Informatics and Systems, Giza, Egypt, 2005.

[5] K. A. Varunkumar, M. Prabakaran, A. Kaurav, S. S. Chakkaravarthy, S. Thiyagarajan, P. Venkatesh. "Various Database Attacks and its Prevention Techniques", International Journal of Engineering Trends and Technology, Vol. 9, No. 11, 2014, pp. 532-536.

[6] C. Shire. "Advanced mobile security in silicon". Secure Mobile Communications Forum: Exploring the Technical Challenges in Secure GSM and WLAN. The 2nd IEE, London, UK , 2004.

[7] H. Jadidoleslamy. "Weaknesses, Vulnerabilities and Elusion Strategies Against Intrusion Detection Systems", International Journal of Computer Science and Engineering Survey, Vol. 3, No. 4, 2012, pp. 15-25.

[8] R. Robbins. "Distributed intrusion detection systems: An introduction and review", SANS Reading Room, GSEC Practical Assignment, 2002.

[9] N. Einwechter. "An Introduction to Distributed Intrusion Detection Systems", 2002, https://www.symantec.com/connect/articles/introduction-distributed-intrusion-detection-systems

[10] K. T. Nguyen, M. Laurent, and N. Oualha. "Survey on secure communication protocols for the Internet of Things", Ad Hoc Networks Vol. 32, 2015, pp. 17-31.

[11] D. Wang, Y. Jiang, H. Song, F. He, M. Gu and J. Sun. "Verification of implementations of cryptographic hash functions", IEEE Access, V. 5, 2017, pp. 7816 - 7825.

[12] Advantages and Disadvantages of Asymmetric and Symmetric Cryptosystems, www.uobabylon.edu.iq/eprints/paper_1_2264_649.pdf

[13] M. Vigil, J. Buchmann, D. Cabarcas, C. Weinert and A. Wiesmaier. "Integrity, authenticity, non-repudiation, and proof of existence for long-term archiving: a survey". Computers & Security, Vol. 50, 2015, pp. 16-32.

[14] J. Jang-Jaccard and S. Nepal. "A survey of emerging threats in cybersecurity". Journal of Computer and System Sciences, Vol. 80, Issue. 5, 2014, pp. 973-993.

[15] K. Zetter. "Inside the cunning, unprecedented hack of Ukraine's power grid", 2016, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack -ukraines-power-grid.

[16] Thuc, N. D., Phu N.C., Bao T.N., Hai V.T. "A Sofware Solution for Defending Against Man-in-the-Middle Attacks on Wlan". Department of Electronic Engineering and Information Sciences, RuhrUniversity Bochum, Germany, 2015.

[17] A. Mittal, A. K. Shrivastava and M. Manoria. "A review of DDoS attack and its countermeasures in TCP based networks", International Journal of Computer Science & Engineering Survey (IJCSES), Vol. 2, No. 4, 2011, pp. 177-187.

[18] TAN, Shuaishuai; LI, Xiaoping; DONG, Qingkuan. TrustR. "An integrated router security framework for protecting computer networks". IEEE Communications Letters, 2016, 20.2: 376-379, 2016.

[19] S. R. Borhade and S. A. Kahate. "Intrusion Detection System based on Hashing Technique". Global Journal of Engineering Science and Researches, Vol. 3, No. 6, 2016, pp. 31-34.

BIOGRAPHIES

MUSTAFA KARA (1989) Mustafa Kara received the BSc in Computer Engineering (CE), Beykent University/Turkey in 2013. He started working as software engineering about computer and system security at some private companies about 3 years. After that, he started working as Lecturer at Mustafa Kemal University/Turkey in 2016 and started his MSc İskenderun Technical University in 2016. He started his Ph.D at Hezarfen Aeronautics and Space Technologies Institute, National Defence University in 2018. His research interests are information, computer and system security, software engineering, industrial robots, electronic and mobile electronic signature and public key infrastructure, malware and spyware, personal and corporate information security and related fields.

MURAT FURAT (1977) received the B.Sc. in Electrical and Electronic Engineering (EEE), Gaziantep University/Turkey in 2002. He started to work as research assistant at Mustafa Kemal University/Turkey in 2002 and completed his M.Sc. at the same university in 2006. He completed his Ph.D at Çukurova University in 2014. He currently works as assistant professor doctor at Iskenderun Technical University. His research interests are process control, sliding-mode control, IoT, IIoT, metaheuristic algorithms and their applications to real systems.