ENHANCING SECURITY IN IoT PLATFORM USING SECURE AUTHENTICATION PROTOCOL

Ms. K. Devipriya[1]andDr. R. Hemalatha[2]
[1]Research Scholar,[2]Head & Associate Professor,
PG & Research Department of Computer Science
Tiruppur Kumaran College for Women,
Tamilnadu, India

ABSTRACT
In recent years IoT is becoming the trending technology which is playing a major role in business, health care, military applications. Wireless communications are highly vulnerable to security threats as anything connected to internet are prone to cyberattacks and place for hackers. Various challenges in IoT are causing security threats and not ensuring End-to-End encryption during transmission of information. Currently most IoT devices use default login credentials and not secured with better configurations and protocols which paves way for cyberattacks. Advanced security standards cannot be employed for all IoT devices. This paper proposed a secure authentication protocol for the IoT platform for ensuring security among IoT devices which keeps track of security threats. An evaluation of the proposed protocol is presented which proves that the protocol is able to address various security threats.
Keywords: Secure Authentication Protocol, IoT, Cyberattacks, End-to-End Encryption, Social Network Sites

1 INTRODUCTION

The development of wireless communication technology and devices has evolved into today's Internet of things, and is being easily found and utilized in our society. The IoT first appeared in terms of terms and concepts in 1999, and through continuous development, in 2018, more than 8 billion IoT devices were connected to the Internet. The development of the IoT is spreading in various forms in our society, and the convenience of daily life is increasing as people control and use devices without restrictions on time and space. However, in line with this development, there are also cases of exploiting it. Various security incidents such as hacking, leaking personal information, and exploiting DDoS attacks by exploiting the weaknesses of the network or device itself of the IoT.Actually, IoT devices currently in use significantly lower levels of process power and memory than existing PCs, mobiles, and tablets, and thus have limitations in applying existing security protocols(1,2). In fact, a large-scale DDoS attack using an IoT device occurred on Dyn, which serves Internet domains, and this attack caused many major Internet sites such as Netflix, Amazon, and Twitter, which are in high demand, to service for a long time. There was a case where I couldn't do it.

In the case of DDoS attack, it was a commonly used attack method, but it was mainly an attack method using a PC. However, through this case, it was confirmed that attacks using smart devices such as home IoT devices for home appliances used in everyday life, IP

cameras, and CCTV (Closed Circuit Television) are possible. In addition, a traditional HTTP fault attack was also found through an embedded device connected to Internet Explorer, which aimed to cause resource overload on cloud services. The attack used here was not from a traditional computer botnet, but from IP cameras around the world, and made up to 20,000 requests per second, and was made by about 900 CCTVs using the Linux embedded version and busybox toolkit. It is said to have lost. In the case of computers, software self-vulnerabilities or social engineering methods are used to infect malicious codes, but in the case of the attack method described above, the attack can be easily attacked because the Internet can be accessed through Telnet or SSH. There are also problems in terms of management. As the existing initial authentication value, the combination of ID and Password "ID: root. As the device size is limited according to the intended use, it is difficult to mount sufficient memory or power. This makes it difficult to install a security solution and to protect authentication and encryption keys because of easy physical access. Accordingly, it is expected that personal information leakage or DDoS attacks using IoT devices will continue to occur in the future.

The IoT continues to develop, and it is predicted that approximately 35 billion devices will be connected to the Internet by 2022. If vulnerability management is not performed, continuous confusion may occur [3~8].Therefore, in this paper, we propose an authentication and key exchange scheme for secure communication in an IoT environment, and an authentication scheme that can be applied to devices that are difficult to apply the existing security protocols due to limitations in memory and computing power.

The further sections are organized as follows. Section 1 described introduction about IoT and cyber security, section 2 review the various literatures to provide support to the problem statement. Sections 3 described the proposed methodology and section 4 discusses the results in detail. Section 5 concludes the paper along with used references.

2 LITERATURE REVIEW

IoT-related research is being actively conducted recently. In general, the introduction of IoT, technology trends, system improvement, and smart cities are mainstream. Prior research related to IoT can be largely classified into industrial aspects, security aspects, and logistics aspects. First of all, research on IoT in the industrial field is focused on improving the efficiency of operating systems and management. Joo Jong-hyuk (2019) analyzed and suggested a plan to overcome limitations and problems when introducing the IoT infrastructure into a supply chain management system and factors for sustainable SCM implementation. In the study of Yoon-Soo Jeong (2019), a model that can efficiently collect and transmit patient information using the Internet of Things was proposed to reduce the operating cost of medical institutions by integrating IoT services in a cloud environment and improve service quality. Yangbeom and Dongwoon (2014) modeled a livestock house management system using IoT technology to manage livestock houses efficiently. In addition, by collecting livestock information through the cloud and identifying the appropriate transaction timing, a plan was suggested to increase the operating profit rate of users and the efficiency of the livestock house operation.

Next, IoT research in the field of security mainly focuses on research on security systems and security safety. Kim Dong-won and Han(2018) are It looked at the security

threats and the direction of security technologies to cope with them, and suggested ways to create a smart medical security ecosystem through the establishment of smart medical security experts and information sharing centers. Seungyong Kim and 4 others (2019) are workers in high-risk occupational groups for safety, an IoT/ICT convergence technology system, such as technology that detects dangerous conditions such as floating, was designed and implemented and analyzed. Through this, it was possible to increase the life-saving rate, and the important functional elements in the operation of the smart safety management system were identified. Yong-hee (2017) analyzed security vulnerabilities and threats in the IoT environment and presented security requirements through security modeling to derive security requirements to cope with them and analyzing examples of possible attacks.

Lastly, the research in the field of logistics focuses on improving the efficiency of logistics and improving logistics services as the target of IoT application. Shin Seung-mok and Jang Myung-hee (2016) analyzed the case of operating an RFID-based warehouse management system among the companies operating the warehouse to derive problems. In order to solve the problem of the RFID-based logistics warehouse system, we proposed an improvement plan that can improve the efficiency by applying the Internet of Things.Hyukjun Choi and Hyunhyun Jung (2017) review smart logistics trends therefore, based on this, we will determine Analyzed. As a result of the analysis, the cargo monitoring system was found to be the most important factor, and it was suggested that efficient port operation is possible if the monitoring system is improved. As a result of reviewing the previous research, IoT-related research mainly focuses on research to achieve efficiency in common in each field. In particular, in the field of logistics, it presents the effects of applying IoT to improve logistics efficiency and services. Logistics is an industrial field that has a high dependence on ICT, and container terminals, among others, have an influence to the extent that ICT influences competitiveness. Despite its importance, research on the application of IoT technology to container terminals is still incomplete.

3. PROPOSED METHODOLOGY

In this paper, we propose a secure authentication protocol using user code, random data, and real time values from the viewpoint of devices, users and authentication centers. The procedure of this paper is divided into three steps. The first is the process of registering the user and the IoT device. In order to use the device, the ID/PW-based registration process is performed for user registration at the authentication center. In this process, the serial number and random value of the product, and then the authentication process It goes through the polynomial transmission process that will be used in The second is a procedure for acquiring access rights to the authentication center. After performing the authentication process of the user, the authentication center, and the device, if it is determined that it is a suitable user, access is allowed. Third, in the real-time access and control process of the device, the user connects to the device, is certified as an appropriate user, and receives authority to directly control it. In the case of the proposed protocol, a group key method between devices, authentication centers, and users was applied for secure and secure communication. In addition, it is designed to improve the reliability of the authentication process as the number of other IoT device devices including devices increases. Therefore, a

strong authentication system was established by reflecting the current era of using many IoT devices.

Table1.ProposedNotation

Notation	Meaning
Ek	Encryptausingkeyk
Dk	Encryptciphertextusingkeyk
R	RandomNumber
f(k)	Polynomialforsecretsharing
SN	SerialNumber
lj(x)	Formulaforsecretcombinations

3.1 Internal Connection Protocol

In this paper, we propose a method to distribute keys after forming a certain group, and to view images by restoring the keys when more than a certain number of them agree when an access request is received internally. In the process of exchanging keys, the group key is used, and the security of the key is also guaranteed by periodically updating the group key and its size.

3.2 Registration Process

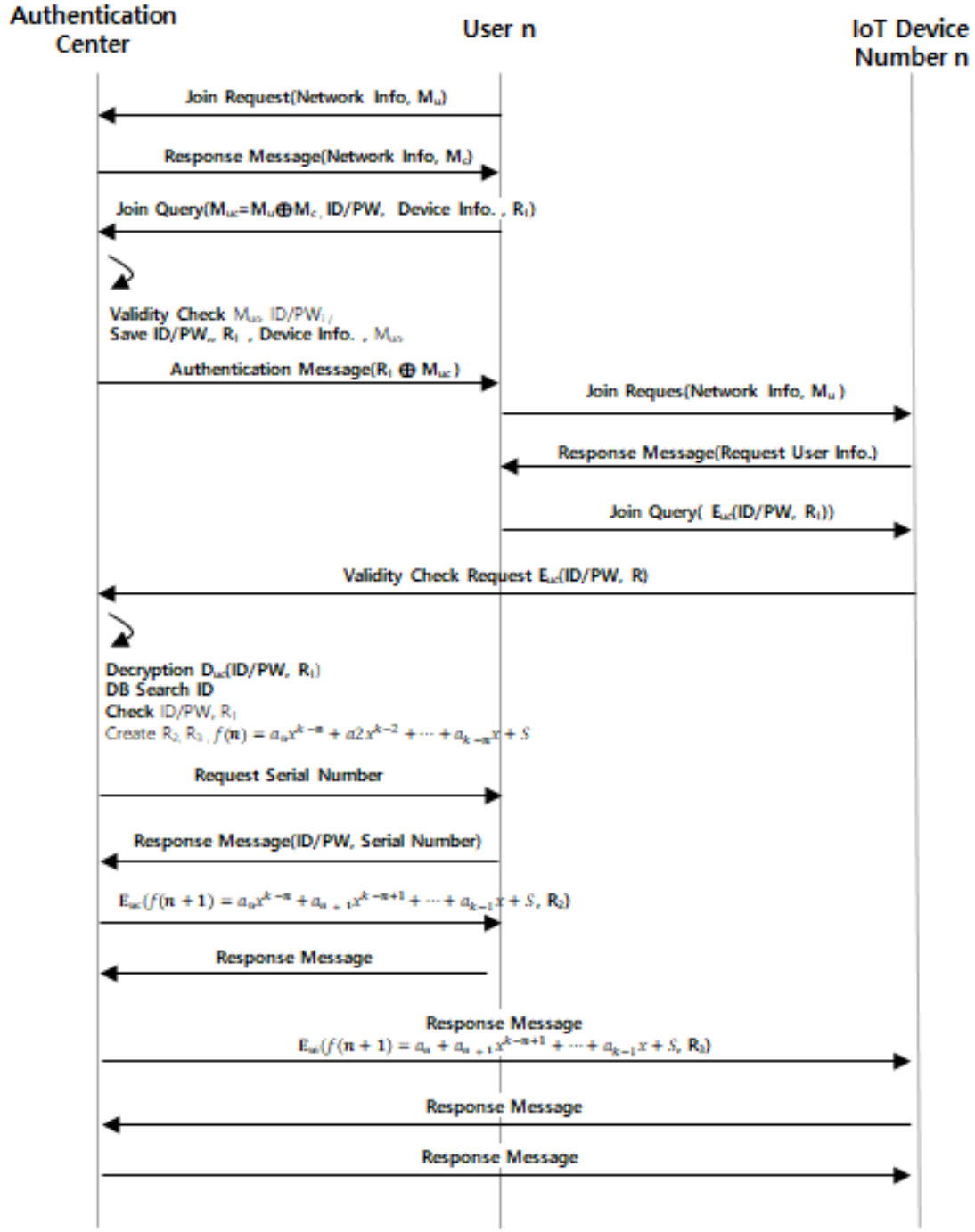

Fig1.Registrationprocess

(1) User transmits Join Request to authentication centre for registration procedure.

(2) The authentication centre sends a response message to the user and proceeds with the ID/PW-based membership registration process, generates a random value and transmits it together.

(3) The authentication centre closes by storing the user's subscription information in the database.

(4) Users can use the network to register the desired device. Requests to connect to the device through the network.

(5) The device requests user information, and the user transmits the ID/PW generated in the authentication centre registration procedure and a random value in response to the request.
(6) Sends a request to check the validity of the user to the authentication centre corresponding to the device.
(7) The certification centre determines the suitability of the user and performs subsequent authentication. For this, a polynomial is transmitted, and a polynomial key distribution method is described.
(8) Complete the user and device registration process.

3.3 Device Access Overview

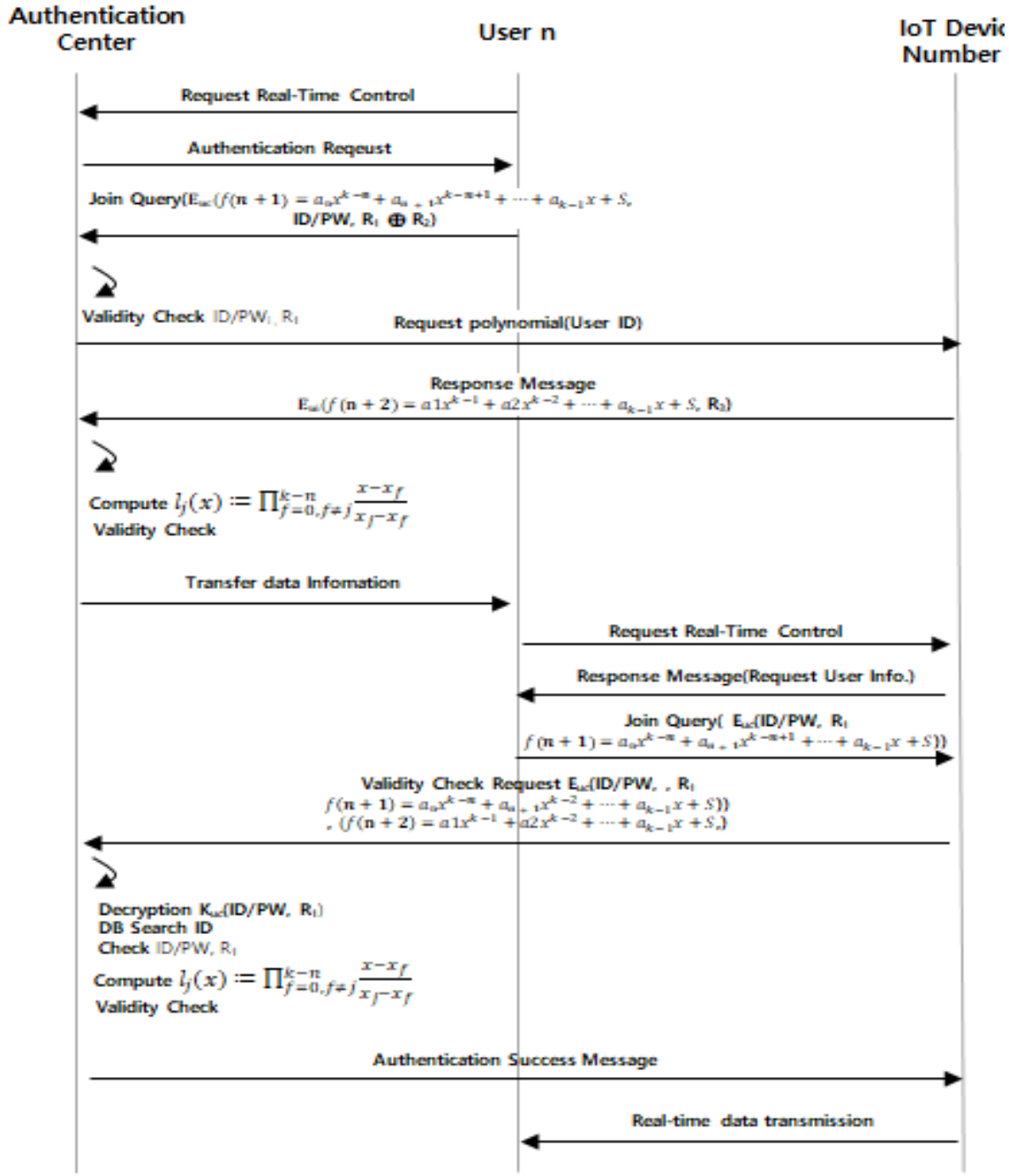

Fig 2.AuthenticationProcess

Step (1) The user transmits an access request message.

Step (2) In this paper, authorization is obtained through agreement of more than n devices according to the group match of the authentication centre. Each device determines the suitability of the user's request and, if deemed appropriate, transmits the polynomial information owned by the device to the operation server.
Step (3) If more than a certain number of polynomial key values are collected, access is allowed after verification.

3.4 Polynomial Key Distribution and Transmission Method

The key distribution method uses a k-1 order polynomial. In this paper, examples are given based on the simplest structure, user, authentication centre, and device, and the stronger the authentication system is, the more groups are formed.
(1) The control centre selects a polynomial f(k) of the k-1 order with s as a constant term.
(2) The control centre sets the value of j and transmits f(j). In this paper, n users, n+x authentication centre, IoT devices is assigned a value of n+(x+keysize), in this case, encryption is performed using the group key created through the Pre-distribution and local Collaboration-based Group Rekeying[11] group key generation method.
(3) When transmitting a key from the authentication centre, it is encrypted with a group key and transmitted.
(4) The authentication centre is Lagrange if more than k distribution keys are collected.The original key is restored using a polynomial [12].

3.5 Key Exchange to Ensure Safety

In order to prevent the situation by the attacker stealing the ciphertext transmitted from the authentication centre, this paper is designed based on mutual authentication so that the attacker's man-in-the-middle attack and reuse attack are impossible by generating and using a random value in the encryption process.
(1) In each initial transmission process, a random value R is generated, encrypted, and then transmitted.
(2) Each node obtains the R value after decryption, uses it for key use through XOR operation, and then performs the authentication process hits.
(3) Key generation and authentication procedures for random numbers between nodes use a polynomial-based function of the previous protocol.

3.6 Real-time Access Control

(1) For device control, the user requests access to the IP camera and transmits the ID/PW and polynomial key values encrypted with the group key.
(2) The device requests the polynomial key value for the received login information to the control centre and the surrounding devices according to the degree of security requirements.
(3) When the suitability of the polynomial key value is confirmed, access is permitted.
(4) When the user ends the session, the polynomial key value is discarded. The polynomial key value is updated according to a certain period.

4. EXPERIMENTAL RESULTS AND DISCUSSIONS

4.1 Security Evaluation

In this section, it is used on the network for security evaluation. Evaluate the safety of attacks against well-known vulnerabilities the excellence was verified through comparison with existing studies.

4.1.1 Mutual Authentication

In this paper, we proceed with the ID/PW subscription procedure using encryption method to join the authentication centre. In this process, random number values are exchanged, which are later used to update key and authentication values. In addition, in the case of the authentication centre, the polynomial f(k) is transmitted to the user and the IoT device respectively for the subsequent authentication process, and after initial authentication, mutual authentication is possible by having a verification procedure with this polynomial value. In the case of subsequent authentication process, the polynomial f(k) is used in the direct authentication process of the user and the IoT device, respectively, as the authentication centre controls the authentication process, thereby enabling secure authentication.

4.1.2 Reuse Attack

Device-device and person by unauthorized users this is an attack that steals and reuses a message generated in the process of communication between a device, etc... Even if the message is stolen, it is possible to authenticate the previous transmission value through continuous exchange of random numbers. Also, since this paper assumes that the timestamp is transmitted during the authentication process, it is possible to verify the information sent at the previous time.

4.1.3 Message Forgery Attack

This is an attack in which an unauthorized user steals a message generated in the process of communicating between a device-device and a person-device, and transmits a message that forgery or alters the message for the purpose desired by the attacker. Encryption during data transmission It creates and transmits the cipher text through the key, so it is safe against message forgery attacks unless an attacker steals the key.

4.1.4 Sniffing

As one of the attack methods to peek at messages transmitted on the network, messages generated in the communication process are encrypted using a secret key, and even if an attempt is made to peek through messages through sniffing by continuously updating the key, encryption It is safe against the attack because it can only see the message.

4.1.5 Spoofing

It is an attack method that disguises the identification information of users and devices on the network as an authorized user and deceives the other party. The authentication procedure is already performed in the pre-communication process, and even if a spoofing attack occurs, the secret between each node shared in the initial authentication procedure Since the value is unknown, it is safe against the attack.

Table 2. SecurityAnalysis

	Wu's	Porambage	Li Method	Min and	**Proposed**
MutualAuthentication	X	O	O	O	**O**
ReplayAttack	X	O	X	O	**O**
DataIntegrity	O	X	X	O	**O**

ManintheMiddleAttack	X	O	X	O	**O**
Sniffing&Spoofing	O	O	O	O	**O**

4.2 Safety Comparative Analysis

Table 2 summarizes the safety of network attacks for comparison with the security protocols proposed in the existing IoT environment. As a result of the analysis, first, the Wu protocol has vulnerabilities in mutual authentication and reuse attacks and man-in-the-middle attacks between IoT devices, and the Li protocol has vulnerabilities in reuse attacks, data integrity, and man-in-the-middle attacks. In addition, the (Kerberos) Proamb and Minand Lee's protocol had a risk in terms of data integrity and was exposed to the risk of session keys used in secure communication. In the case of this proposed protocol, it was confirmed that security for well-known vulnerabilities is secure through 4.1 security evaluation. Shows a big difference. This is the number of devices is expected to be suitable in the IoT environment that is growing in the exponential rate.

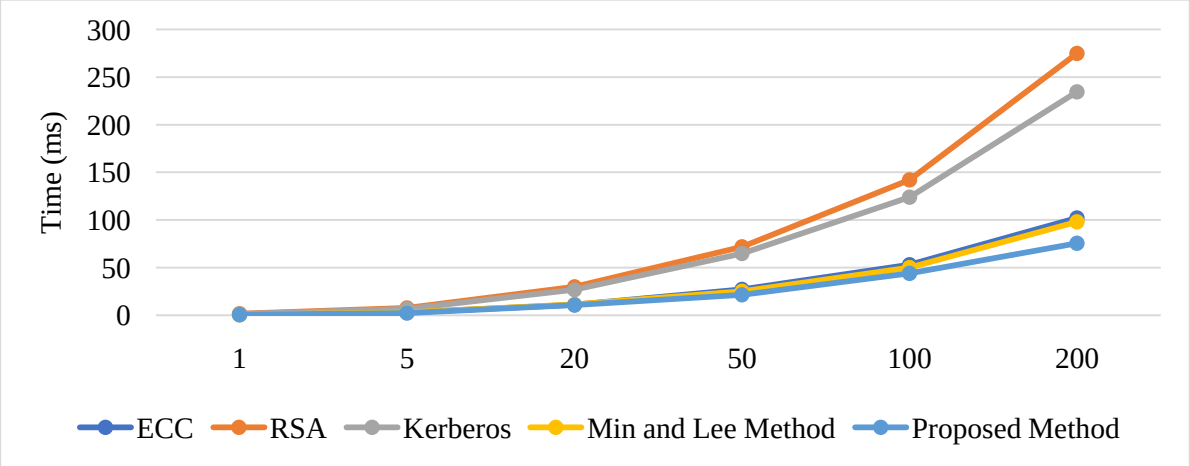

Fig 3.Re-AuthenticationPerformance

Table3.PerformanceAnalysis

Number of Device	ECC	RSA	Kerberos	Min and Lee Method	**Proposed Method**
1	0.62321	1.54231	1.41233	0.56013	**0.52145**
5	2.99140	7.57351	6.86393	2.80066	**2.17323**
20	11.21770	29.74191	26.86250	11.20260	**10.74253**
50	27.18130	71.79453	64.96720	25.00660	**21.49862**
100	53.10370	142.20100	124.12900	50.01320	**43.95426**
200	102.33100	274.91060	234.72900	98.02640	**75.73222**

Table4.Re-AuthenticationPerformanceAnalysis

NumberofDevice	ECC	RSA	Kerberos	Min and Lee Method	**Proposed Method**
1	0.62321	1.54231	2.01233	0.0232	**0.0214**
5	2.99764	7.6113	9.93085	0.10672	**0.10061**
20	11.7562	29.67404	39.0794	0.42363	**0.164681**
50	28.7112	72.56569	96.8937	1.05676	**0.71829**
100	56.7744	142.0468	189.360	2.05784	**0.12915**
200	107.690	271.826	375.098	4.01824	**4.00016**

5. CONCLUSION

With the advancement of technology, most of them can easily access smart devices in their daily lives. The advancement of internet technology and hardware technology provides many conveniences to people, but unfortunately, numerous security threat cases are occurring at the same time. Malware and hacking methods used in the existing PC environment are expanded to IoT devices have been tried frequently and caused numerous damages, but the performance of IoT devices. Due to limitations in memory and power, it is difficult to apply the security protocol of the existing PC environment. Thus, seen the paper is a security protocol considering the characteristics of the IoT call was designed and the security and performance suitability were confirmed through performance evaluation. Therefore, if the proposed protocol is applied, it is expected that it will be possible to provide an efficient security system in the future Internet environment.

Acknowledgements

The authorwould like to thank the authors of the work ECC, RSA,Kerberos and Minlee Method for results comparison.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

REFERENCES

1 Kolias, Constantinos, et al. DDoS in the IoT: Mirai and other botnets. Computer, 2017, 50.7: 80-84. DOI: https://doi.org/10.1109/mc.2017.201

2 Yang, Yuchen, et al. A survey on security and privacy issues in internet-of-things. IEEE Internet of Things Journal, 2017, 4.5: 1250-1258. DOI: https://doi.org/10.1109/jiot.2017.2694844

3 Frustaci, Mario, et al. Evaluating critical security issues of the IoT world: Present and future challenges. IEEE Internet of Things Journal, 2017, 5.4: 2483-2495. DOI: https://doi.org/10.1109/jiot.2017.2767291

4 Khan, Minhaj Ahmad; SALAH, Khaled. IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems, 2018, 82:395-411. DOI: https://doi.org/10.1016/j.future.2017.11.022

5 Bkamble, Ashvini; BHUTAD, Sonali. Survey on Internet of Things (IoT) security issues & solutions. In: 2018 2nd International Conference on Inventive Systems and Control (ICISC). IEEE, 2018. pp. 307-312. DOI: https://doi.org/10.1109/icisc.2018.8399084
6 Samie, Farzad; BAUER, Lars; HENKEL, Jörg. IoT technologies for embedded computing: A survey. In: Proceedings of the Eleventh IEEE/ACM/IFIP International Conference on Hardware/Software Codesign and System Synthesis. ACM, 2016. p. 8.DOI: https://doi.org/10.1145/2968456.2974004
7 Saha, Himadri Nath; MANDAL, Abhilasha; SINHA, Abhirup. Recent trends in the Internet of Things. In: 2017 IEEE 7th annual computing and communication workshop and conference (CCWC). IEEE, 2017. pp. 1-4.
8 Sohoel, Halldis; JAATUN, Martin Gilje; BOYD, Colin. OWASP Top 10-Do Startups Care. In: 2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security). IEEE, 2018. pp. 1-8. DOI: https://doi.org/10.1109/cybersecpods.2018.8560666
9 Joo Jong-hyuk (2019), A Study on Supply Chain Management Strategy in the IoT Environment, Cheongju University Industrial Science Research Institute, 1-5.
10 Hyuk-Jun Choi and Hyun-Jung Jung (2017), Smart Logistics Trend and Pyeongtaek Port IoT Application Plan, e-Business Research, Vol. 18, No. 6,145-158.
11 Choi Hyung-lim (2015), IOT Technology and Logistics Innovation, Korean Intelligent Information Systems Society Spring Conference Papers, 1-16.
12 Information and Communication Technology Promotion Center (2014), IoT R&D Promotion Plan Offshore Korea (2015), Special Plan Smart Logis 2015-IoT and Logistics BDI (2014), Internet of Things (IoT) Era and Busan's Response, BDI Policy Focus No. 257, 1-12.
13 IDC(2019), Worldwide Internet of Things Spending Guide.
14 KMI(2018), KMI trend analysis, VOL 98.
15 KT Economic Management Research Institute (2014), Opportunities and Strategic Directions in the IOT Era
16 Saaty Kearns (1985), Analytical planning: The Organization of Systems, Pergamon Press, Oxford.
17 Saaty, T.L (1996), The Analytic Network Process, RWS Publications, Pittsburgh.
18 Min, S. Y., & Lee, J. S. (2019). Authentication and Group Key Management Techniques for Secure Communication in IoT. Journal of the Korea Academia-Industrial cooperation Society, 20(12), 76-82.