International Journal of Engineering & Technology, 7 (2.12) (2018) 11-17

International Journal of Engineering & Technology

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

Research Paper



Attribute-based multiuser authentication scheme between IoT devices for 5G environment

Yoon-Su Jeong [1] *, Yong-Tae Kim [2], Gil-Cheol Park [2]

[1] Dept. of Information Communication Engineering, Mokwon University, 88, Doanbuk-ro, Seo-gu, Daejeon, 35349,Republic of Korea
[2] Dept. of Multimedia, Hannam University, 70 Hannam-ro, Daeduk-gu, Daejeon, 34430, Republic of Korea
**Corresponding author E-mail: bukmunro@mokwon.ac.kr*

Abstract

Background/Objectives: Due to the development of mobile communication technology, infrastructure construction from 4G to 5G service, which is currently being serviced, is actively under way. In particular, as the types and functions of mobile phones and IoT devices using 5G services are diversified, mutual authentication technology among multiple users is required.
Methods/Statistical analysis: In this paper, we propose a multi - user authentication scheme which can efficiently mutually authenticate different types of mobile phones and IoT devices that are provided with 5G service. The proposed method minimizes the authentication delay time because it identifies the authentication security parameter δ of multiple users requesting authentication to the server as a polynomial coefficient. As a result of the performance evaluation, the proposed method showed an average improvement of 9.3% in authentication processing time and 5.5% lower overhead than the existing method. In addition, the multiuser authentication latency was improved by 6.1% on average compared with the existing scheme.
Findings: The proposed scheme minimizes the user 's authentication delay time by constructing the users who simultaneously request the 5G service into a subnet and then applying the authentication security parameter δ constituting each subnet to n - bit and applying it to the polynomial coefficients. Especially, for multi - user authentication, the proposed scheme divides the authentication path into two paths (main path and secondary path) to guarantee user authentication and integrity. The proposed scheme is suitable for mobile phones and IoT devices that use low power because it generates keys without performing additional cryptographic algorithms like conventional techniques when performing multi - user authentication.
Improvements/Applications: In future research, we plan to apply the proposed method to the actual environment based on the results of this study.

Keywords: *Multi-User; 5G; Property Based; Authentication; Subnet; Security Parameter.*

1. Introduction

Recently, as the fourth industrial revolution has become more socially prominent, communication services are gradually changing from 4G to 5G in the mobile communication field1. 5G technology is expected to be used in all devices such as smart phones, automobiles and IT products from 2020, and delay, speed and streaming service will be more supported than 3G and LTE technologies [2], [3]. In particular, mobile communication service is one of the services that can generate and collect various kinds of socially required data and to develop modernized society in a more efficient way. Thus, it is possible to provide customized information for each personalized modern society member [4], [5], [6].
Researchers in the IOT field have already proposed solutions to improve the security of resource-constrained devices based on IP 5. Recently, many researchers are studying the datagram transmission layer security protocol considering IoT.
Sahid Raza et. al proposed a lightweight security solution for IoT7. The solution investigated IPSec, DTLS, and IEEE 802.15.4 security for secure communications at IoT, but still has a problem that can vary depending on the pre-shared key for authentication.
Sahid Raza et al. proposed a method to reduce the overhead of DTLS through header compression [8]. However, this technique shows that the header compression used for the purpose of increasing the efficiency of IoT is causing a lot of security problems.
Daniele Trabalza et al. Provide confidentiality and integrity for computer communication machines between other endpoints, such as sensor nodes, on the Internet of objects via CoAPS protocols such as Android devices [9]. However, the implementation of DTLS has a problem of sharing a standard dictionary key mechanism among the sensor nodes.
In this paper, we propose an authentication scheme that can perform user authentication when different types of mobile phones and IoT devices that are provided with 5G service connect to the server at the same time. The proposed method minimizes the processing time in the server by using the authentication security parameter δ and associating it with the probability value of the polynomial after decentralizing multiple users to process by property by block. The proposed scheme has the following three purposes and features to improve the efficiency of multiuser authentication. First, if there is a user's authentication request so that multiple users can easily access the server, the user's information is configured into a hierarchical subnet according to the attribute information of the user. Second, authentication efficiency is improved by extracting probabilistic property information based on different properties (size, usage, type, etc.) of users stored in the server. Third, the authentication delay time of the user is minimized by converting the vector repre-

Copyright © 2018 Yoon-Su Jeong et al. 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.

sented by the polynomial coefficients into a pair with the polynomial so as to quickly identify the authentication of the multiple users.
The proposed method minimizes the authentication delay time by processing the authentication execution according to the multi - user attribute to the forward and backward functions. Since the proposed scheme improves the efficiency of authentication processing of multiple users, it can minimize the burden on the server. Also, the proposed scheme is suitable for mobile phones and IoT devices that use low power because it generates keys without performing additional cryptographic algorithms like conventional techniques when performing multi-user authentication.
The composition of this paper is as follows. Section 2 discusses mobile communication services and existing research. In Section 3, we propose an attribute-based multi-user authentication scheme for 5G environment. In Section 4, we compare the proposed scheme with the existing scheme. Finally, Section 5 concludes the paper.

2. Related works

2.1. Mobile communication service

5G service is one of the most popular mobile communication service technologies with the emergence of the fourth industrial revolution. 5G extends the network infrastructure to dynamic globalization using communication protocols compatible with existing Internet standards 10. In the early days of mobile communication service, M2M (Machine to Machine), transportation card, courier delivery tracking system, factory / facility management, ATM, navigation, bar code, (Smart Grid, Intelligent Vehicle Servicing, Healthcare, Smart Home, etc.) using devices such as computers and tablets.
In September 2012, KISA analyzed the evolution process of mobile communication. The mobile communication service started from the Internet connection and changed to connect the computer with the connected terminal (M-Interent). In recent years, the connection range has been expanded so that all peripheral devices can provide services by attaching communication functions.

Table 1: Generation-Specific Service and Performance Characteristics

Generation (G)	Service	Difference Point	Problem
1G	Analog voice call	Mobility	Inefficient bandwidth utilization, security vulnerability
2G	Digital voice calls and text messages	Security, Mobile Phone Popularization	Very limited data transfer - No internet or email
3G	Voice calls and text, data	Improve your Internet experience	Actual data performance insufficient, WAP-based Ethernet utilization failure
3.5G	Voice Call and Text Broadband Data	Broadband Internet, mobile applications	Limits according to existing mobile-specific structure and transmission protocol
4G	All IP-based services (Including voice and text)	- Broadband Internet speed improvement - Low transmission delay (lagtency)	Near 100% coverage and availability, ultra-dense networking environment, low power consumption technology
5G	Mass content service	Infrastructure-based technology that ensures high density, low power, reliability and availability of devices such as M2M communication or MCT	end-to-end communication,

source : GSMA Intelligence

Table 1 shows the service and performance characteristics of each generation from 1G to 5G 7-13. As shown in Table 1, 5G technology defines various methods to meet differentiated requirements (transmission speed, traffic capacity, power consumption, coverage, etc.) than existing technologies. However, the 5G technology provides more advanced features than the existing technology, but end-to-end communication or MTC troubleshooting has not yet been fully resolved.
MTC has not yet resolved the Massive MTC and Critical solution. MTC is divided into Massive MTC and Critical MTC. Massive MTCs can connect a huge number of very small devices such as sensors, but there is a problem that low power communication is required. Critical MTC is necessary for high reliability, such as traffic control and factory automation control. Critical MTC requires stable connectivity, high availability, and near-real-time transmission.
In the 5G service environment, unauthorized access by unauthorized users should be prevented as compared to 4G services. This is because each user's private key ciphertext access policy or attribute set is connected and used through the attribute-based encryption (ABE) method to apply to 5G technology than 4G.

2.2. Previous research

J. Hur et. al technique has proposed a property abolition planning system to compensate for the vulnerability of forward security11. However, this technique has the disadvantage of re-encrypting information when a single system with trusted authority or a user possessing data performs outsourcing.
Liu et. al method has proposed a Mona authentication method that securely shares data of multiple owners 12,13. The advantage of this technique is that the service is provided so that users accessing the system are subdivided. However, the user who has canceled the authentication has a disadvantage that it can be easily compromised by a third party.
The CP-ABE system of Bethencourt et. al was first proposed to formalize the concept of ciphertext-policy ABE (CP-ABE) 14. However, this method has a disadvantage in that the CP-ABE is not applied in a specific condition or environment because it proves the CP-ABE certification process based on a commonly used group model rather than a specific region group model.
Cheung et. al scheme proposed another CP-ABE scheme that extends the existing ABE scheme. This technique is characterized in that the security parameters are proved under the assumption of double linear Diff-Hellman decision to improve security than existing techniques 15.Chase et. al technique has proposed a multi-authority ABE (MA-ABE) scheme 16. This technique is characterized by issuing the attribute secret key to the user and distributing the secret key together with the global unique ID. In this paper, we propose a new scheme for the multi-authority ABE17,18.Emura et. al method is an extension of the CP-ABE scheme, and supports only (n, n) critical access policies for multi-valued attributes with a certain size of ciphertext 19. However, this technique has the disadvantage that the multiple attribute values must be fixed to a certain size.
Herranz et. al The technique is described by Emura et al. In order to solve the problem of Emura et. al method 19, another CP-ABE scheme with a certain size of cipher text has been proposed 20. However, this technique has the disadvantage of emphasizing the differentiation of policy decisions so that the threshold access value for a multi-valued attribute can be applied only for (t, n).

Cheng et al. scheme proposed a new CP-ABE scheme that reduces the computational cost for a certain size of ciphertext and access policy 21. Sreenivasa et. al technique proposed a new cryptosystem using the proposed method. (N, n) threshold access for multi-valued attributes 22.Zhang et. al technique has proposed a method for efficiently updating the ciphertext for a revocation event from the CP-ABE schema 23. In addition, The CP-ABE technique of Yu et. al is proposed to indirectly perform attribute-level abolition on the proxy placed in the server 24. Yang et. al scheme improved the CP-ABE technique by re-randomizing the key 25.

J. Hur et. al scheme proposed a CP-ABE scheme using a key tree encrypted with a binary key for attribute group key distribution. This technique is characterized by an immediate attribute-level discard mechanism 11.Unlike revocation at the attribute level, the termination at the user level loses all access to the system by the revoked user.

To solve these problems, Attrapadung et. al scheme proposed a CP-ABE scheme with direct user level abolition by combining broadcast encryption and ABE 26.

3. Multiple attribute based user authentication scheme

In recent mobile communication environment, interest in 5G technology, which is one step higher than 4G technology, is rising rapidly. 5G technology supports more latency, faster speed, and streaming service than 4G, so services are required to prevent unauthorized users from illegally accessing sensitive items. In this section, we propose an attribute-based authentication scheme that allows multiple users to communicate securely using 5G environment. In particular, the proposed method aims to minimize the processing time required to authenticate a user in a 5G environment after decentralizing the various attributes of users receiving services in the 5G environment so that they can be processed on a block basis.

3.1. Overview

Recently, with the development of mobile phone technology, communication technology for supporting mobile phone technology is rapidly evolving. Many services that are provided in 4G are user authentication based on company, but in 5G, personal authentication based on biometrics is performed. Particularly, as the technology of mobile phone and Internet of Things (IoT) is combined, the purpose of mobile communication is diversified and the processing technology related to user authentication is becoming more and more complicated. In addition, since user authentication is used in various environments according to the purpose of using mobile communication, requirements for not only safety for user authentication but also efficiency are increasing.

In this paper, we propose a secure and verifiable authentication scheme that reflects the characteristics of authentication in the 5G environment. The proposed method aims to minimize the user authentication time processed by the authentication server by extracting each authentication security parameter δ after decentralizing the various attributes of the user so that it can be processed in block units. In addition, the proposed method can maximize the efficiency of the equipment in the cluster to which the intermediate medium belongs by sharing the role of the server according to the attribute information of the data.

The proposed scheme improves the authentication access control of multiple users by stochastically assigning the attribute information according to the forward and backward functions of the access control of the intermediate medium which acts as a gateway among the devices constituting the 5G environment. As shown in Figure 1, the proposed method generates a 128-bit random value N to process the user's authentication access, firstly the intermediate medium performs access control, and secondarily to the server-side encryption / decryption keys. . In the last step, the authentication server and the certificate used by the user are encrypted using the generated random value N.

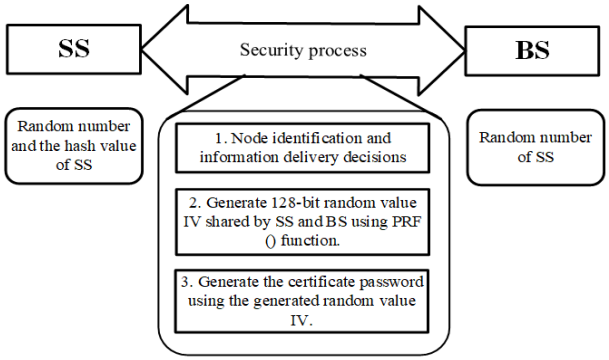
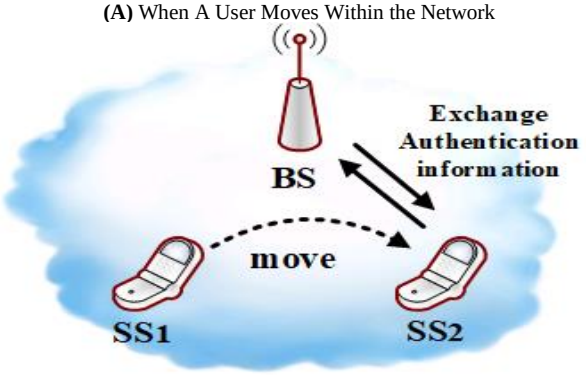


Fig. 1: Authentication Access Process of Proposed Scheme.

In the proposed scheme, it is necessary to check whether the user can communicate with the server before the authentication process as shown in Fig. 2 (a)) It is divided into an attempt to enter the network range of the server from the external network. In Fig. 2, the user's location information LI is included in the message used in the initial authentication process of the user, and the server can grasp the user's current location information LI through this information. The location information LI of the user includes the user's recognition information, the current location information of the user, the information of the server to which the user belongs, and information on whether or not the user enters the network of the server to communicate with.

(A) When A User Moves Within the Network



(B) When A User Moves From Outside the Network to Inside

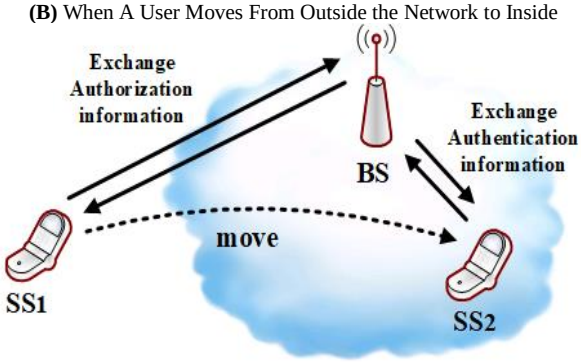


Fig. 2: Subscriber and Base Station Communication Method.

As shown in Fig. 2 (a), if the user exists within the network range of the server, the user sends the value of the user's location information LI along with the random number N to the server, It is used to generate a new random value that can be shared with each other. If the user does not exist within the network range of the server, the user first requests the server to enter the network by requesting the X.509 certificate.

In the proposed scheme, the user and the authentication server generate the random number value that they generated in advance, and the user registers with the authentication server using the location value of the user. In this case, the information transmitted and received between the user and the authentication server is encrypted

by using the 128-bit random value generated by the PRF () function to perform authentication by encrypting the certificate. Through this process, the proposed scheme is safe against attack such as reply attack and man-in-the-middle attack that can occur in radio section, and it can be lightweight compared with existing public key cryptosystem.
The proposed scheme is able to verify securely and accurately without applying user authentication delay time by applying the authentication security parameter δ processed in 5G environment to n - bit and applying it to the polynomial coefficients. In particular, the proposed scheme improves the efficiency of the user access control by converting the vector generated by the polynomial coefficients to polynomial and pair so as to improve the user authentication verification speed.

3.2. Notations

Table 2 summarizes the terms used in the proposed scheme.

Table 2: Notation

Parameter	Notation
δ	Security Parameter
GP	Global Parameter
AID	Authority Identifier
A	Authority
A'	Updated authority
SK	Security Key
PK	Public Key
AP	Access Policy
CT	Cypher Text
bd	Big data
UKey	Updated Key
AM	Authentication message
IV	Intermediate value

3.3. Generate subnet polynomial coefficients

In this section, in order to securely authenticate multiple users requiring service in the 5G environment, we divide the attributes of users so that various attributes of each user can be processed on a block-by-block basis. Then, polynomial coefficients that can extract each authentication security parameter δ FIG.
Users requesting 5G service are divided into several groups (here, subnet) according to service purpose. A user belonging to a group obtains a polynomial coefficient using a polynomial equation such as Equations (1) to (2). In the proposed scheme, $x_1,\cdots, x_n$ and finite number of tuples $(i_1,\cdots, i_n)\in N^n$ are used for multivariate polynomials for multi-user authentication.

$$Q(x_1,\cdots, x_n) = \sum_{i_1,\cdots,i_n} a_{i_1,\cdots,i_n} x_1^{i_1}\cdots x_n^{i_n} \quad (1)$$

Here, $a_i$is an i-order coefficient, and $a_0$denotes a constant term. If $Q(x_1,\cdots, x_n)$ is a nonzero polynomial, $a_n \neq 0$, that is, n=degP. degP is denoted by the degree of the polynomial $Q(x_1,\cdots, x_n)$.
Equation (1) can be expressed as Equation (2) using multiple indicator notation.

$$Q(x) = \sum_i a_i x^i \quad (2)$$

Here, Imeans the number of users constituting the group, and i (= $(i_1,\cdots, i_n)\in N^n$), x(= $(x_1,\cdots, x_n)$), $x^i(=x_1^{i_1}\cdots x_n^{i_n})$ are all vector components of the polynomial.
The polynomial coefficients of the group obtained from Eqs. (1) to (2) are constructed in pairs so that they can be associated with probability values in the proposed method. In particular, in the proposed technique, a user with a high similarity level of the authentication security parameter δ is found, and a probability value is set, and then the authentication security parameter δ is associated with the probability value.

3.4. Attribute-based multi-user authentication using polynomials

In this section, we propose a polynomial-based user authentication scheme to efficiently process multi-user authentication for service provision in 5G environment. The proposed scheme improves efficiency by securely authenticating multiple users without additional encryption algorithm required in 5G environment. In addition, the proposed method operates in three steps, such as an initialization process, an authentication link generation process, and a user authentication process, in order to perform authentication for each characteristic (type, function, characteristic, attribute, etc.) of a user.

3.4.1. Initialization process

In the initialization process, it is assumed that N users who are provided services in the 5G environment are defined as $\widehat{U}\subseteq$Uamong N user U_i, which can accurately authenticate the user.

$$U= \{u_1, u_2, ..., u_N\}\ , i\in [1, N] \quad (3)$$

$$U_i= \{\widehat{U}\subseteq U \mid i\in [1, N]\} \quad (4)$$

Here, the user U_i(i∈[1, N]) constructs a dataset D_i by sampling the authentication security parameters δ in N pieces.
Then, the user and the server respectively generate the private key (p, q) and the public key (N=pq, e) selected by the user. Where p and q are arbitrary large prime numbers satisfying p = $2q'$+1 and q = $2p'$+1.

$$\text{Select p, q} \quad (5)$$

When Eq. (5) is generated, Eq. (6) is generated using an integer satisfying 0<M<N and arbitrarily selected k.

$$M^{k\Phi(N)+1}= M^{k(p-1)(q-1)+1} \equiv M \bmod N \quad (6)$$

Here, Φ(N) means a function that is a positive integer smaller than N or mutually adjacent to N.
In the proposed scheme, when p and q are prime, Eq. (7) satisfies Φ(pq)= 2pq.

$$ed= k\Phi(N) + 1 \quad (7)$$

Where e and d are the multiplicative inverses of mod Φ(N). According to modular arithmetic rules, e and d are mutually Φ(N).
The user has (p, q) and (N, e) a private key and a public key, respectively. In this case, the user uses a secure hash function such as $H : \{0,1\} \rightarrow Z_N$, and the server uses a secure hash function such as $H : \{0,1\}^* \times Z_N \rightarrow Z_N$.
To access the 5G environment in the proposed scheme, different attribute information P_i should be specified for each user. In order to designate different attribute information P_i for each user, the value of the vector component of the polynomial equation is obtained from the equations (8) to (9).

$$P_i= (p_1, p_2, ..., p_n)\ , i\in[1, N] \quad (8)$$

$$\bar{v} = \{D_iP_j\in Z \mid D_i\sim DP_j\},\ 1\leq i\leq N,\ 1\leq j\leq N \quad (9)$$

Where p_i denotes the vector component value of the polynomial among the elements of the set Z(i∈Z). $\bar{v}$ is a set of vector component values of all polynomials related to p_i. DP_j(j∈[1, N]) denotes the probability of the authentication information included in the dataset.

3.4.2. Authentication association information generation process

In this section, the process of generating a key for user authentication when a user attempts to receive a service in the 5G environment is shown in three steps as follows.
Step 1: In order to generate a key for authenticating a user who wishes to receive services in the 5G environment, the proposed scheme constructs users into groups and then transforms the authentication security parameter δ constituting each group into n -bit blocks to generate a polynomial to be applied to the coefficient.
Step 2: The server receives the user's security parameter δ and applies it to the key generation function as in (10).

$$\text{Keygen}[\delta] \rightarrow \sigma \quad (10)$$

Where, σ denotes linkage information between users generated through the key generation function.
Step 3: The server checks the user to see if the authentication security parameter δ has been successfully converted into an n-bit block. If the check result is a normal result, the server executes the symmetric encryption algorithm by applying the authentication linkage information σ between users to each n-bit block, and if an abnormal result is obtained, the server regenerates the authentication linkage information σ between users.
Step 4: The server generates a power of attorney m_i as shown in Eq. (11) using the user authentication association information σ and the user's location information LI.

$$m_i = (-1)^{d_2} \cdot e^{d_1} \cdot \text{h}(\frac{\sigma + LI}{2}, \text{T}) \bmod \text{N} \quad (11)$$

Step 5: The server passes the mandate m_i to the user and uses it while the user is in the group.

3.4.3. User authentication signature process

In the user authentication process, multiple users can be authenticated by multiple users based on the mandate m_i received from the server without additional authentication.
Step 1: The user receives r′stored in the server in advance and calculates R(=r^2 mod N) after selecting random integer r∈Z_n.
Step 2: The user uses the mandate m_i to generate the global key, signing key ρσ, instead of the additional authentication operation, as Eq. (12).

$$\rho\sigma = (m_i, \text{T}, \text{r}', \text{r}, \sigma, \text{LI}) \quad (12)$$

Step 3: When the user makes an authentication request to the server using the global key, that is, the signature key ρσ, the server sends the information of the previously registered user (mandate m_i,, user authentication linkage information σ, user's location information LI, random number r′, etc.) to perform authentication without additional authentication.
·Step 4: The server applies the mandate m_i to the hash function of two paths (main path and auxiliary path) for user authentication and integrity. In this case, the information applied to the proposed scheme checks authentication and integrity while sequentially decreasing the number n of multiple users (n> 0).

4. Evaluation

The evaluation of the proposed technique is divided into security evaluation and performance evaluation. Performance evaluation compares authentication processing time, overhead, and attribute delay time between multiple users with existing techniques.

4.1. Environment setting

In this section, we use OMNet ++ as the simulation tool to validate the proposed method and the existing method. Table 3 shows the experimental environment for the simulation to show the objective evaluation.

Table 3: Parameter Setting

Parameter	Setting
Channel capacity	11Mbps
Backoff slot time	10 ms
Minimum contention window size(voice/data)	8/32
Maximum contention window size(data)	1024
Backoff Stage limit(data)	5
Retransmission limit(data)	7
PLCP&preamble	192
MAC header	24.7
AIFS/DIFs(data)	50 ms
Minislot duration	0.3ms
Time slot duration	1.5ms
Transmission time(data)	1.18ms
Gurad time	20 ms
Average on/off time	352/650ms
Minislot contention provbability(data)	0.2
Transmission queue length	10,000 packets
Superframe time(delay bound)	100m

4.2. Security evaluation

4.2.1. Reuse attack

In the proposed authentication scheme, to prevent the reuse attacks that may occur in the 5G environment, various attributes of each user are decentralized so as to be processed in a block unit, and a polynomial coefficient is generated so that each authentication security parameter δ can be extracted.
Since the polynomial coefficients are applied to multivariate polynomials of $x_1, \cdots, x_n$ and finite number of tuples $(i_1, \cdots, i_n) \in N^n$, safety is assured even if they are eavesdropped on third parties.
In addition, the proposed authentication scheme is safe for a reuse attack because it constructs a pair of polynomial coefficients to associate with a probability value, finds a user with high similarity of the authentication security parameter δ, and processes the probability values.

4.2.2. Spoofing attack

The proposed authentication scheme is secure against spoofing attacks because the third party does not know the authentication security parameter δ applied to the polynomial coefficients by converting the authentication security parameter δ into n -bit blocks. Also, even if the third party obtains the authentication security parameter δ, it does not know the information such as d_1, d_2, σ, and LI required for the creation of the mandate m_i, so it can prevent the third party from attacking the mandate $m_i$have.

4.2.3. Preventing information disclosure

In the proposed scheme, each time the user accesses the authentication server, the global key generated by the user and the server, that is, the signature key ρσ is changed each time. Therefore, when the third party carries out the authentication request to the server, m_i,, user authentication linkage information σ, user location information LI, random number r′, etc.), the third party can not illegally use the user information.

4.2.4. Attack based on multi-level service access authentication

In the proposed scheme, since the user receives the r′stored in the server in advance and selects the random number r∈Z_n selected by the user and calculates R(=r^2 mod N), the unauthorized third party It can not be illegally accessed. In the proposed scheme, for authentication and integrity of the user, authentication is performed through a hash function of two paths (main path and auxiliary path) of mandate m_i. In this case, the information applied to the proposed scheme is secure against attacks due to multi-level service access authentication because it sequentially checks the authentication and

integrity while decreasing the number n of the multi-users sequentially (n> 0).

4.2.5. Privacy attack

In the proposed scheme, the user information can be safely protected by using the mandatory m_i, the user authentication association information σ, the user 's location information LI, and the random number r′, which are needed when generating the global key, ie, the signature key ρσ. When a third party tries to collect information of several users, the server can secure the authentication and integrity of the user by using the global key or signature key ρσ, thereby protecting the user's privacy.

4.3. Performance evaulation

4.3.1. Authentication processing time

Figure 3 shows the processing time that occurs when multiple users making up a subnet request authentication to the server. As shown in Figure 3, the proposed method shows an average 9.3% improvement in the authentication processing time of users processed by the server according to the user's authentication information (type, function, feature and attribute) and subnet configuration. This result shows that when the proposed method accesses the server for multi-user authentication, the proposed method distributes the various attributes of the user so that they can be processed in units of blocks, extracts the authentication security parameter δ of each user, As shown in Fig 3. In addition, the proposed scheme shows that multiple users can authenticate multiple users based on the mandate m_i received from the server without additional authentication.

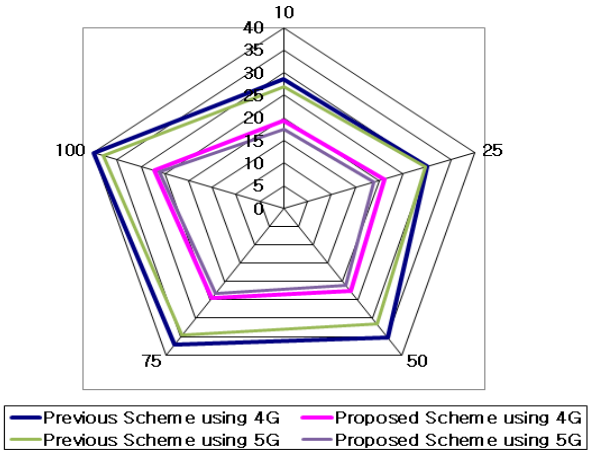


Fig. 3: Authentication Processing Time.

4.3.2. Overhead

Figure 4 shows the server overhead change when using the global key or signature key ρσ to authenticate multiple users with different attributes in the 5G environment. As shown in Figure 4, the proposed scheme achieves a 5.5% lower overhead change than the existing scheme as the number of multiple users increases. In particular, the proposed scheme does not use an additional algorithm for user authentication processing, and the change in overhead is not higher than that of the existing scheme because the global key or signature key ρσ is generated to hierarchically represent the authentication processing configuration according to user attributes.

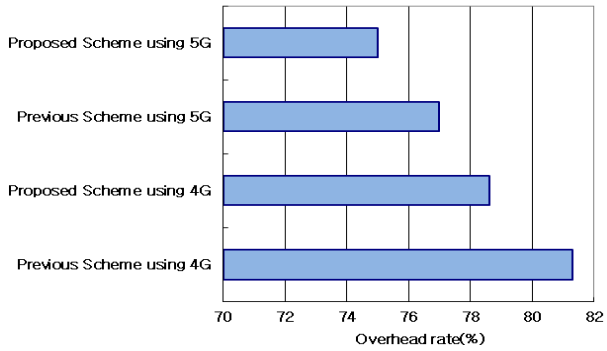


Fig. 4: Overhead of Server.

4.3.3. Multi-user authentication latency

Figure 5 shows the authentication latency that occurs when multiple users are authenticated in a 5G environment. As shown in Figure 5, according to the attribute-based multi-user authentication policy, the vector is extracted using the polynomial coefficients of the user identification information, so that the authentication delay time between multi-users is improved by 6.1% This result is the result of applying the security parameter δ to the polynomial coefficients for multi - user authentication after the user information stored in the server is configured in subnet for the multi - user authentication. Also, it is a result that the key used to process the authentication information in real time between attribute-based multi-user for 5G environment is generated by using multi-hash chain.

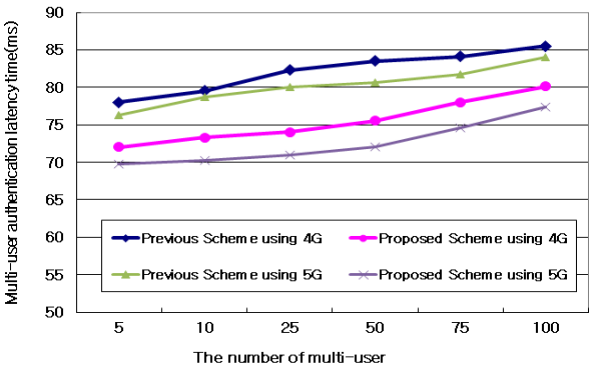


Fig. 5: Multi-User Authentication Latency Time.

5. Conclusion

Along with the development of the Internet, 5G technology is increasingly attracting attention in place of 3G and LTE technologies. In this paper, we propose a method to perform authentication based on attributes of users using different types of mobile phones and IoT devices. The proposed method minimizes the processing time in the server by using the authentication security parameter δ and associating it with the probability value of the polynomial. In order to improve the efficiency of multi - user authentication, user authentication And the efficiency of the authentication is improved. In addition, the proposed scheme minimizes the authentication delay time of the user by converting the vector represented by the polynomial coefficients into a pair with the polynomial so as to quickly identify the authentication of multiple users. As a result of the performance evaluation, the proposed method improves the average authentication processing time of the users processed by the server by 9.3% on average according to the user 's authentication information (type, function, feature and attribute) and subnet configuration. As the number of multiple users increases, the overhead is 5.5% lower than the proposed method. Finally, according to the property - based multi - user authentication policy, the proposed method of extracting the vector using the polynomial coefficients of the user identification information is improved by 6.1% on average compared with the existing method. In future research, we plan

to apply the proposed method to the actual environment based on the results of this study.

Acknowledgment

This paper has been supported by 2018 Hannam University Research Fund.
This work was supported by the Security Engineering Research Center granted by the Ministry of Trade, Industry and Energy.

References

[1] Roman R,Najera P, Lopez J, Securing the Internet of Things, Computer, 2011, 44(9), pp.51-58.
[2] Raza S, Shafagh H, Hewage K, Hummen R, Voigt T, Lithe: Lightweight Secure CoAP for the Internet of Things, IEEE Sensors Journal, 2013, 13(10), pp. 3711-3720.
[3] Roman R, Zhou J, Lopez J, On the Features and Challenges of Security and Privacy in Distributed Internet of Things, Computer Networks, 2013, 57, pp. 2266-2279.
[4] WurmG M, Zhu Y, Millard M, Fung S, Gura N, Eberle H, Shantz S C, Sizzle : A standards – Based End to End Security Architecture for the Embeded Internet, Pervasive mobile computing, 2005, 1, pp. 425-446.
[5] Heer T, Garcia-Morchon O, Hummen R, Keoh S L, Kumar S S, and Wehrle K, Security challenges in the ip based interent of things, Wireless Personal Communications, 2011, 61(3), pp. 527-524.
[6] Weber R H, Internet of Things: New Security and Privacy Challenges, Computer Law & Security Review, 2010, 26(1), pp. 23-30.
[7] Raza S, Lightweight security solutions for the Internet of Things, Malardalen University Sweden, 2013.
[8] Lippi M, Mamei M, Mariani S, Zambonelli F, An Argumentation-based Perspective over the Social IoT, IEEE Internet of Things Journal, 2017, PP(99), pp. 1-1.
[9] Tiburski R T, Amaral L A, de Matos E, de Azevedo D F G, Hessel F, Evaluating the use of TLS and DTLS protocols in IoT middleware systems applied to E-health, 2017 14th IEEE Annual Consumer Communications & Networking Conference , 2017, pp. 480-485
[10] Roman R, Najera P, Lopez J, Securing the Internet of Things, Computer , 2011, 44(9), pp.51-58.
[11] Hur J, Noh D K, Attribute-based access control with efficient revocation in data outsourcing systems, IEEE Transactions on Parallel and Distributed Systems, 2011, 22(7), pp. 1214–1221.
[12] Liu X, Zhang Y, Wang B, Yang J, Mona: Secure multiowner data sharing for dynamic groups in the cloud, IEEE Transactions on Parallel and Distributed Systems, 2013, 24(6), pp. 1182–1191.
[13] Zhu Z, Jiang Z, Jiang R, The attack on Mona: Secure multiowner data sharing for dynamic groups in the cloud, 2013 International Conference on Information Science and Cloud Computing Companion (ISCC-C), 2013, pp. 185–189.
[14] Wang H, Dong X, Cao Z, Multi-value-Independent Ciphertext-Policy Attribute Based Encryption with Fast Keyword Search, IEEE Transactions on Services Computing, 2017, PP(99), pp. 1-1.
[15] Cheung L, Newport C, Provably secure ciphertext policy ABE, Proceedings of the 14th ACM conference on Computer and communications security, 2007, pp. 456-465.
[16] Chase M, A multi-authority attribute-based encryption access control for social network, 2017 3rd IEEE International Conference on Control Science and Systems Engineering (ICCSSE), 2017, pp. 671-674.
[17] Lin H, Cao Z, Liang X, Shao J, Secure threshold multi authority attribute based encryption without a central authority, Information Sciences, 2010, 180(13), pp. 2618-2632.
[18] Rouselakis Y, Waters B, Effcient statically-secure large-universe multi-authority attribute-based encryption, International Conference on Financial Cryptography and Data Security, 2015, 8975, pp. 315-332.
[19] Emura K, Miyaji A, Nomura A, Omote K, Soshi M, A ciphertext-policy attribute-based encryption scheme with constant ciphertext length,International Conference on Information Security Practice and Experience, 2009, 5451, pp. 13-23.
[20] Herranz J, Laguillaumie F, Ràfols C, Constant size ciphertexts in threshold attribute-based encryption, International Workshop on Public Key Cryptography, 2010, 6056, pp. 19-34.
[21] Chen C, Zhang Z, Feng D, Efficient ciphertext policy attributebased encryption with constant-size ciphertext and constant computation-cost, International Conference on Provable Security, 2011, 6980, pp. 84-101.
[22] Rao Y S, Dutta R, Recipient anonymous ciphertext-policy attribute based encryption, International Conference on Information Systems Security, 2013, 8303, pp. 329-344.
[23] Zhang Y, Chen X, Li J, Li H, Li F, Attribute-based data sharing with exible and direct revocation in cloud computing, KSII Transactions on Internet and Information Systems, 2014, 8(11), pp. 4028-4049.
[24] Yang K, Jia X, Ren K, Attribute-based ne-grained access control with efficient revocation in cloud storage systems,Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security, 2013, pp. 523-528.
[25] Yu S, Wang C, Ren K, Lou W, Attribute based data sharing with attribute revocation, Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, 2010, pp. 261-270.
[26] Attrapadung N, Imai H, Conjunctive broadcast and attribute-based encryption, International Conference on Pairing-Based Cryptography, 2009, 5671, pp. 248-265.