Designs A Multi-user Authentication Structure Optimized for Cloud Environments

Yoon-Su Jeong, Dong-Ryool Kim, Seung-Soo Shin

Abstract*: With the recent rapid development of IT technology based on the Internet, devices used in cloud environments are rapidly changing from regular PCs to cell phones or tablet PCs. Small devices, such as mobile phones or tablet PCs, are more easily used wirelessly than wired, so there is a problem with users' privacy information being exposed to maliciously from third parties. Performance evaluations show that small wireless devices using virtual multi-group factor in cloud environments have an average of 14.8 % more accuracy in the information they process to protect users' privacy. The processing efficiency with which users' privacy information using small wireless devices is sent and received to cloud-certified servers has increased by up to 19.6 %. In addition, processing time was 21.1% lower when users' privacy between small wireless devices and cloud-certified servers was handled in a virtual environment. In this paper, we propose user privacy protection techniques using virtual multi-group factor to prevent third parties from using the privacy of users with cloud services around small wireless devices in use in wireless environments. The proposed technique is used to replicate multi-group factor in a virtual environment for synchronization of servers and intermediate devices, and to shorten the time of authentication processing process that protects users' privacy. Proposed techniques use functions and random numbers for synchronizing servers and intermediate devices operating in virtual environments to safely prevent malicious attacks from third parties.

***Index Terms*: Cloud Service, Authentication, Multi-user, Signature.**

I. INTRODUCTION

Recently, cloud computing technology is receiving great attention to support users' Internet services with a focus on ultra-small wireless equipment [1]. However, since ultra-small wireless devices operating in a cloud environment require additional communication security requirements compared to conventional communications equipment, special security measures are needed.Most cloud services currently in operation support for both PCs and mobile devices, creating a variety of security issues. In order to ensure the seamless delivery of the services users want in a cloud environment, developers must create services tailored to mobile devices [2,3]. In the cloud computing environment, a variety of cryptographic algorithms and key generation techniques are used to protect the data sent/received between cloud servers and users. However, security policies and response technologies are needed because data stored in cloud computing systems can be encrypted and stored but still be leaked to third parties [4]. In this paper, we propose a technique to protect a user's privacy by using a hypothetical multi-group factor to prevent malicious use of the user's privacy in a small wireless device used by the user in a cloud environment. The purpose of the proposed technique is largely twofold. First, effectively prevent users' privacy from third parties while reducing the load on the devices that make up the cloud environment. Second, the proposed technique replicates the multi-group factor in the virtual environment, reducing the authentication processing time that protects users' privacy by synchronizing the server and intermediate devices. The proposed technique duplicates the user's key and simultaneously authenticates the user between the user and the server, the user and the intermediate gateway device in the virtual environment. To reduce authentication processing time, the proposed technique stores a user's replication key on an intermediate gateway device, so that if the server requests a user's authentication, it runs the authentication with the server in the background using the compound key instead of the key that the user owns. At this point, the proposed technique uses a Interleave() function to ensure synchronization between the user and the server, the intermediate gateway, and the server. Because Interleave() functions apply random numbers created by devices and certificate bureaus that act as intermediate gateways, they can protect users' privacy by preventing malicious attacks from third parties.The composition of this paper is as follows. Chapter 2 explores existing research to protect users' privacy in cloud environments. Chapter 3 proposes user privacy protection techniques using multiple group factors in the virtual environment, and Chapter 4 compares the safety and efficiency of the proposed techniques to existing techniques and finally concludes in Chapter 5.

II. RELATED WORKS

A. Cloud Services

Cloud services are one of the next promising areas along with big data. However, the introduction has been delayed due to concerns over security issues and privacy violations. Currently, no legal system exists or is currently in place to directly manage and regulate the world's cloud computing environment. This can be attributed to the fact that at the beginning of the cloud, countries' cloud computing

Revised Manuscript Received on May 22, 2019.

Yoon-Su Jeong, Department of Information and Communication Convergence Engineering, Mokwon University, Daejeon, Korea

Dong-Ryool Kim, School of Mechatronics Engineering, Tongmyong University, Busan, Korea

Seung-Soo Shin, Department of Information Security, Tongmyong University, Busan, Korea

policies were focused on activations, not privacy. At present, the issue of legal systems in each country is the management of personal information and the transfer of personal information to other countries. Given that most of the providers of cloud computing services are U.S. companies, the issue of each country's cloud legal system in the future depends on how to protect and prevent the outflow of personal information overseas. In Korea, a government-level law on personal information protection (the Cloud Computing Development and User Protection Act) has been enacted, but it has been delayed due to the lack of safety. It also puts more emphasis on the development of related industries than on the protection of personal information. As security issues related to cloud computing are becoming an issue, it is necessary to create an environment where users can use cloud services with confidence. To do this, a cloud policy that focuses on privacy and information protection needs to be established.Technologies that seek privacy protection in the cloud environment are defined by dividing them into personal information life cycle, OECD privacy principle, privacy measures, and cloud private-enabling technology (PET), as shown in Table 1. In particular, to protect cloud privacy from third parties, an analysis of information protection-related issues such as system complexity, multiple leasing environments, Internet connection services, and loss of control is needed. System complexity has a variety of components in a cloud computing environment, so there is a risk of loss, unauthorized use, and modification of personal information caused by an increase in user-to-user interaction in upgrading and improving functionality. In a multi-tenant environment, cloud services share various components and resources between service providers, consumers, and users. At this point, there is a risk of unauthorized information sharing. Internet-facing services are increasingly exposing users' personal information to risk due to high costs and the burden of organizing security measures.

Loss of control is exponentially increasing data as cloud services evolve. Continuous monitoring and updates are required.

Table 1. Cloud Privacy Enhancement Technology

Personal information life cycle	OECD Privacy Principles	Countermeasures for Privacy	Cloud PET Technology
Collecting and creating	- The principle of limiting collection - Principles of clarity of purpose	- Minimize data	Privacy Policy Language (P3P, EPAL, etc.)
Storage	- The principle of responsibility - principle of safety protection - Principles of information accuracy	-Provide confidentiality, integrity	Encryption (Adaptive PMS, homogeneous encryption, etc.)
Providing and Processing	- The principle of restriction on use - Principles of personal participation	- Data Access Control	Anonymous and pseudonymization (ID Management System)
Disposal	-Public principles -delete authority	-Confidentiality	media disposal technique

B.Previous Research

A lot of research into cloud computing is underway to date on storage grouping, security issues, process and memory security issues, and the IoT nodes for cloud systems.Cloud computing has the advantage of using large amounts of virtual storage over the Internet to build a large, expensive computing infrastructure, but it has the potential to create a lot of security problems with changes to local computing.Singh et al. presents the fundamentals of cloud computing, security issues associated with cloud environments, and various security issues related to focus cloud security [5].Singh et al. proposed a three-tier security architecture for security issues related to cloud computing [6]. Zhang et al. systematically analyzed security issues in the cloud environment using different algorithms and discussed more than 150 articles in addition to tackle [7]. varadharajan et al. for flexible security services, the provides some of the security services that the CSP performs [8].After the migration of IoT from a cloud system, Iera et al. proposed a specific solution to support IoT in the cloud [9]. This solution presents various advantages and disadvantages as well as traditional IoT cloud services. Saha et al. mentions cloud computing, self-control and IoT as well as how the Internet, wireless sensors and actuators are synchronized [10]. Celesti et al. has implemented devices that can improve IoT cloud services as an alternative to a lightweight, hyper visor-based approach [11]. Dar et al. proposed a virtualization framework using the SicthSense cloud platform to select metrics for obtaining availability and probabilities on demand [12].L. Echenauer et al. The technique uses the random key pre-distribution method to key-up to improve security over conventional techniques [13]. However, this technique has the problem of spending a lot of time looking for shared keys because it randomly distributes generated keys randomly.H. Chan et al. The technique proposed a technique for increasing efficiency by dividing nodes in a group into groups to derive shared keys [14]. However, this technique has the disadvantage of being heavily wasteful of memory, resulting in high communication costs.S. Zhu et al. The technique proposed a technique that reduces authentication processing

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

time by allowing the cluster head to authenticate instead before sharing a shared key that exists between two nodes [15]. However, this technique uses public keys to authenticate the two nodes, so it has the problem of having public keys pre-allocated across all cluster heads. In addition, when distributing session keys between two nodes, the hosts that make up the cluster are exposed to the session keys.A. Khalili et al. This technique improves convenience and efficiency so that the open and private keys of nodes can be applied to ID-based encryption technique [16]. However, this technique is very vulnerable to intermediate attacks because it acquires a private key as much as a critical factor from the surrounding node.

III. OPTIMIZED USER PRIVACY PROTECTION WITH MULTI-GROUP FACTOR

In a cloud environment, users' information is handled through a variety of media, making it difficult to secure their privacy protection by third parties. In particular, the quality of service that can satisfy users is still not good enough, although various studies have been actively developing services that can protect users' privacy, as information on cloud services has been frequently abused through the web.To protect the privacy of users using cloud services through various media, the proposed technique of user privacy protection using a virtual multi-group factor is proposed after grouping user groups into a virtual environment.

A. Overview

In a cloud environment, thousands of users are grouped into different groups to provide services depending on the type of service. However, most cloud services currently in operation are vulnerable to illegal security attacks by third parties because they can be delivered without any special policy changes to users' access rights. To address these security challenges, the proposed technique classifies users who want to receive cloud services into a group of virtual users, and then presents information about the group as group index information to handle the hash with user information. The purpose of allocating indexes by virtualizing groups in the cloud is to cache user information and group index information to minimize server authentication to prevent third parties from exploiting users' privacy information. To maximize efficiency and reliability, the proposed technique creates n groups to hash out user privacy information so that it can be placed in a hierarchical distributed format when creating user groups, and then forward it to the intermediate devices in the virtual environment. The role of intermediate devices in the virtual environment has two main purposes. First, the intermediate device creates replication keys (k_1 and k_2) that enable users to safely receive cloud services, preventing third parties from using their privacy illegally. Second, it applies user-generated random key ur and random key gr generated by intermediate devices in the virtual environment to the hash function to efficiently authenticate users so that users and groups can receive cloud services efficiently.

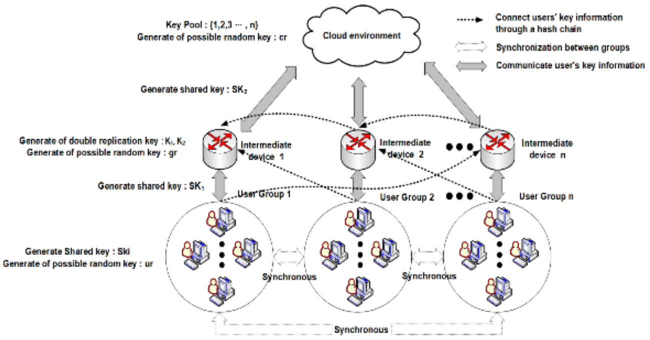
Key Pool : {1,2,3 ··· , n}
Generate of possible rnadom key : cr
Cloud environment
Connect users' key information through a hash chain
Synchronization between groups
Communicate user's key information
Generate shared key : SK₂
Generate of double replication key : K₁, K₂
Generate of possible random key : gr
Intermediate device 1
Intermediate device 2
Intermediate device n
Generate shared key : SK₁
User Group 1
User Group 2
User Group n
Generate Shared key : Ski
Generate of possible random key : ur
Synchronous
Synchronous
Synchronous

Figure 1. Overview Process of Proposed Model

Figure 1 shows the overall operation of the proposed technique. As Figure 1 shows, the proposed technique uses $H_U : \{0,1\} \rightarrow Z_N$ to describe the user's privacy information and then presents the group information as shown in $H_p : \{0,1\}^* \times Z_N \rightarrow Z_P$, which binds the intermediate devices in the virtual environment to interleaved with each other. In a virtual environment, an intermediate device is configured to represent a hierarchical structure by plotting the degree of connectivity, as shown in Equation (1).

$$CI_K = \begin{Bmatrix} ci_{00} & \cdots & ci_{oj} \\ \vdots & \ddots & \vdots \\ ci_{i0} & \cdots & ci_{ij} \end{Bmatrix}, K = 1,2,...n \quad (1)$$

Where i stands for the sequence of rows representing the user's privacy information and j refers to the hash chain values connected so that the virtual environment can be interleaved between intermediate devices.To efficiently manage users' privacy in a cloud environment, the proposed technique performs two functions: First, when communicating users' privacy information through different network equipment through smart devices, the proposed technique sub-segments the user's privacy information individually, forming a hierarchical structure, and consistently validating the user's privacy information through a double comparison value. Second, the proposed technique allows users to process their privacy verification by categorizing probabilistically similarities with existing information about users' privacy derived from smart devices in order to improve their management analysis and rapid verification of users' privacy.

B. Definition of Notations

The notations used in this paper are shown in Table 2.

Table 2. Notations

Parameter	Notation
$H_U : \{0,1\} \rightarrow Z_N$	User's Privacy information
$H_p : \{0,1\}^* \times Z_N \rightarrow Z_P$	a user's privacy information group in a virtual environment
CI_K	The value of the Kth connection degree hashed between the intermediate devices of the virtual environment
SK_i	Shared key
q	The private key selected between [2, n -2]
Q	

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

ak_i	The public key computed via $q \times P$
sk_i	Auxiliary key
H()	Session key
ur , gr	Hash function
T	Random key
	Timestamp

C. Generating privacy information via multi-group factor

The proposed technique provides a service that is layered by classifying user privacy information, such as Table 3, so that users can store and manage their privacy information on a cloud server with small wireless equipment, and then providing attribute information according to conditions and behavior. In particular, the proposed technique uses attribute information such as Table 3 to prevent unlawful exploitation of users' privacy information from third parties [16].

Table 3. User Privacy Properties Information

Option		Property
Status	Data sharer	User name, group name etc.
	Purpose	Use purpose
	Obligation	Obligations
	Mandate	Delegator
	Location	Predefined tables, local coordinates
	Time	Time range, repetition time
	Sensor	Sensor channel name
	Status	situation which can be used in sensor
Action		Action, activity

In addition, third-party access control over users' privacy information is grouped and processed for distributed processing. The proposed technique is that the secondary server is responsible for double hash handling in the event of a third party's control of access to the user's privacy information. The reason for handling double hash on secondary servers in the proposed model is that third parties with property information have easy access to users' privacy information according to their authority.The proposed technique allows intermediate devices to generate duplicate keys in a virtual environment to authenticate users so that third parties may illegally exploit the privacy information of users used in cloud environments. The following key generation and initialization processes are required for users using cloud services to securely register their privacy information with the server:

- Step 1 : Generating user privacy information

This step creates the user's privacy information, $\vec{p}$ and expression (2). Here, n stands for the number of important information of the user.

$$\vec{p} = (a_1, a_2, \cdots, a_n) \tag{2}$$

- Step 2 : Delivering the user's privacy

The user's privacy information $\vec{p}$, generated in step 1, encrypts the user's recognizer information UI and random key ur with the shared key SK_i to deliver it to the intermediate device in the virtual environment. Where, the shared key SK_i refers to a pre-shared key through a secure path.

$$Transfer\,E_{SK_i}(\vec{p}, UI_i, ur) \tag{3}$$

- Step 3 : Creating a duplicate key

The intermediate devices in the virtual environment use the pre-shared shared keys $E_{SK_i}(\vec{p}, UI_i, ur)$ that are passed from the user and generate random key gr that is compatible with the user's recognizer information UI_i as shown in Equation (4).

$$Generate\ gr \in Z_q^* \tag{4}$$

The intermediate device in the virtual environment creates a double-replication key SK_i by using a process such as expression (5) through expression (6) to act as the intermediate user-server for privacy information.

$$ak_i = (q^{x+at_1}, q^{t_1}, q^{t_2}) \tag{5}$$

$$sk_i = H\ (UI_i \| \vec{p} \| ak_i) \| T \| SEN \tag{6}$$

Where, other than the sk_i share key(ur , gr) means the session key of the cache function used to improve the performance of the intermediate device while preventing maliciously stealing the user's privacy to a third party. T means the timestamp where the session key sk_i can be used.

- Step 4: HASH Information HI_i Generation

This step creates the user's group index information DII_i. The intermediate device generates hash information HI_i such as expression (7) using the user's group block B_i and user's privacy information $\vec{p}_i$, then generates group index information such as expression (8), DII_i.

$$HI_i = H\ (B_i, \vec{p}_i,), 1 \le i \le n \tag{7}$$

$$DII_i = H\ (B_i) \in L\ , 1 \le i \le n \tag{8}$$

Where L is the hash length value used to extract user privacy information with group index information DII_i.

- Step 5 : Register the duplicate key sk_i and the group index information DII_i with the server

This step encrypts the duplicate key sk_i used by the intermediate device to protect the user's privacy and the group index information DII_i as in expression (9), using the shared key gr .

$$Transfer\,E_{gr}(sk_i\ , DII_i) \tag{9}$$

D. User Privacy Protection Course

To protect users' privacy,

the proposed technique stores the user's privacy information in the server database through an intermediate device existing in the virtual environment, analyzes the user's privacy information, and performs the following five levels of feedback.

- Step 1: Collecting virtual multi-group user privacy information

Users classified into multiple virtual groups to receive cloud services generate their privacy information $\vec{p}_i$ $(=a_1, a_2, \cdots, a_n)$ according to the number of multiple media. where a_n refers to the privacy information of users who wish to receive cloud services according to the number of multiple media.

- Step 2: Delivering user privacy information

Users' privacy generated through multiple media is delivered to the cloud server via smartphones or the Web.

- Step 3: Check user privacy information

Privacy information for users classified as virtual multi-group is stored on cloud servers through a wired and wireless environment. The user's privacy information stored on the server periodically checks the status of the user's privacy information according to service property information.

- Step 4: Determining whether or not to provide services according to the user's privacy authority

The privacy information of the user stored on the server is analyzed according to the service authority. When the user's privacy information is analyzed according to the service, the server provides customized services for the user.

- Step 5: User Privacy Real-Time Management

The server periodically checks users for service changes by storing the results of an analysis of users' privacy and service authority and usage in the database. At this point, if a user occurs that requires a service with a high privilege rating, the server can provide the service in real time through a 1:1 interview with the user.

III. EVALUATION

A. *Environment Setting*

Table 4 sets up an experimental environment consisting of IoT devices and sensors, gateways, and servers that provide services to perform the performance evaluation of the proposed model.

Table 4. Parameter Setup

Parameter	Setting
Number of IoT Devices	ln= {1, 2, 5, 10, 20}
Number of Data generated through IoT devices	dn={50, 100, 250, 500, 1000}
Number of Property	pn= {1, 2, 3, 4, 5}
Threshold	th = {1, 3, 5}
Transmission Distance of IoT Device	1m ~ 5m
Data generation interval of IoT devices	0.01 ms
Initial self-data set time	60 s ~ 120 s
Compressed data size(Bytes) through IoT devices	ds={20, 30, 50, 60, 180}
Average Compress time(ms)	40
Average Decompression time(ms)	35

B. *Security Analysis*

The proposed technique ensures the safety of the mid-term information by creating a gateway user by acting as a gateway in a replication environment such as $ak_i = (q^{x+at_1}$, q^{t_1}, $q^{t_2})$, and $sk_i = H\ (UI_i \| \vec{p} \| ak_i) \| T \| SEN$. One of the biggest features is that the proposed technique can prevent illegal access by intermediate devices or third parties without access. In particular, the proposed technique ensures safety in multi-level service access certification attacks by using the ak_i and sk_i that many IoT devices use to perform authentication on servers that provide cloud services.Because the proposed technique uses the ak_i and sk_i to double-use session keys, it not only makes it easy to manage a large number of user groups that can be sent and received by encrypting a user's privacy, but also ensures availability for user privacy.To prevent Blackhole/Sinkhole attacks, the proposed technique uses timestamp T and serial number SEN to prevent attacks such as packet passing between communications using Flood based protocols when generating session keys sk_i . In addition, the proposed technique is safe from Blackhole/Sinkhole attacks because the intermediate device periodically updates and checks the random key gr in addition to time stamp T and serial number SEN . The proposed technique uses hash information HI_i and group index information GII_i , and random values (ur , gr) to ensure secure communication between users and intermediate devices to prevent Hello Flow attacks. In addition, the proposed technique is updated periodically with the time stamp T , serial number SEN , and random value (ur , gr) delivered with session key sk_i to provide integrity and up-to-date.The proposed technique uses random numbers (ur , gr) and hash information HI_i and group index information GII_i generated by users and intermediate devices to prevent wormhole attacks that tunnel directly with users in recording and tracking user privacy information.

C. *Performance Analysis*

Figure 2 shows the accuracy of information that small wireless devices that use virtual multi-group factors in cloud environments process to protect users' privacy. As Figure 2 shows, information accuracy of proposed techniques is 14.8 percent or more on average compared to wireless devices used in traditional cloud environments. These results are the result of the user's collection and analysis of privacy information in real time in a virtual environment using a virtual multi-group factor. In addition, the results of the user's privacy information collected through the small wireless equipment were obtained because the authentication server determined the user's privacy information according to the various virtual multi-group factor.

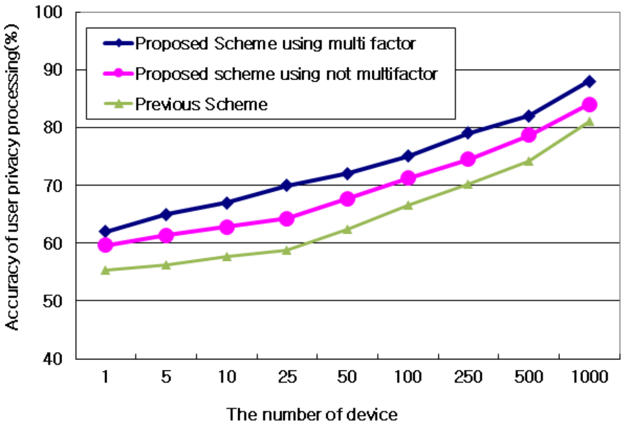

Figure 2. Accuracy of small wireless devices using virtual multiple group factors in a cloud environment

Figure 3 shows the effectiveness of the process by which users' privacy information using small wireless devices is sent and received by a cloud-certified server. As Figure 3 shows, the processing efficiency of sending and receiving users' privacy information to and from a cloud-certified server using multiple group factors in a virtual environment resulted in up to 19.6% improvement over traditional techniques. These results are due to the fact that users' privacy stored on small wireless devices has been pre-certified by using multiple factors in a virtual environment, thereby reducing the time required for cloud-certified servers to process user privacy information.

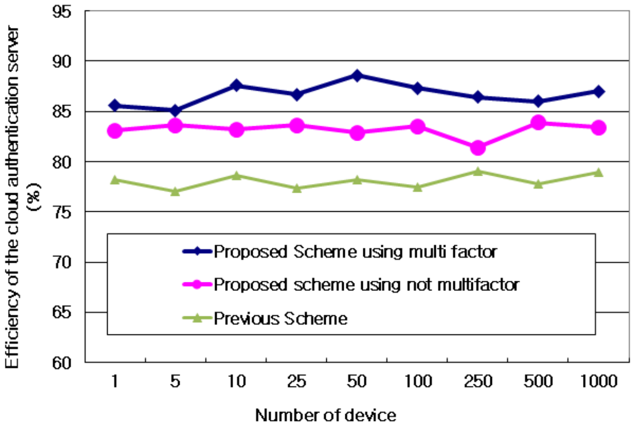

Figure 3. Efficiency of user privacy handled by the cloud authentication server

Figure 4 shows comparison of throughput times when users' privacy between small wireless devices and cloud-certified servers was handled in a virtual environment. The experiment showed that the processing time was 21.1% lower than the use of a multi-group factor in a hypothetical environment. These results are due to the authentication server's handling of users' privacy first in a virtual environment and then the authentication server handles the detailed authentication factor.

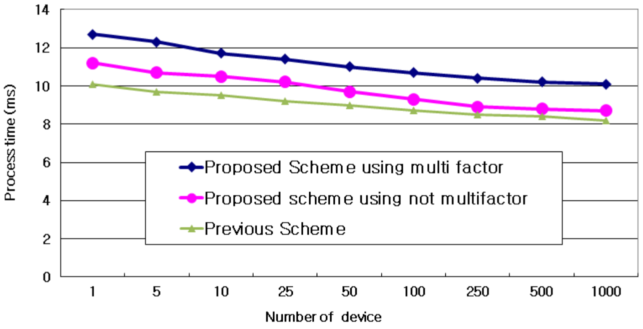

Figure 4. User's privacy processing time between small wireless device and cloud authentication server

Figure 5 shows a comparison of the virtual environment with the overhead of authentication servers with the use of multiple devices in a virtual environment. As shown in Figure 5, when users' privacy transactions were handled using a multi-group factor in a virtual environment, they were shown to be 22.8 percent higher on average than those handled by the authentication server. These results are in addition to processing user privacy information by the authentication server. However, the proposed technique is suitable for servers that support low-capacity cloud services rather than high-capacity cloud services, as these results result in an ever-increasing number of small wireless devices that handle users' privacy in a virtual environment. In particular, because the proposed technique links users' privacy information in a virtual environment rather than being handled separately by the authentication server, the overhead of the authentication server was lower than that of the existing technique.

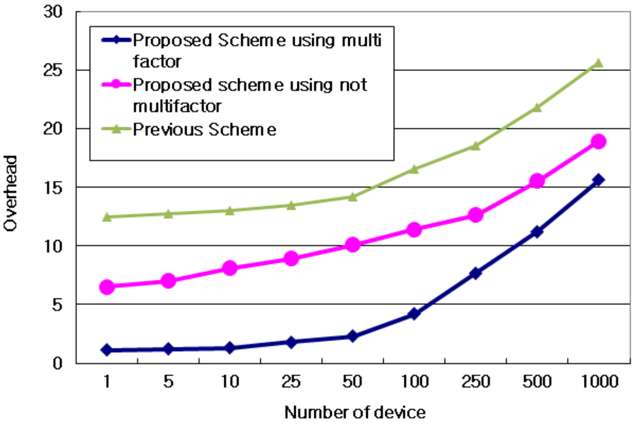

Figure 5. Overhead incurred by the authentication server in a virtual environment

IV. CONCLUSION

Cloud services are one of

the fastest growing areas in recent years. This paper proposed a multi-group factor-based user privacy protection technique for stable protection of users' privacy from third parties in a socially emerging cloud service. The proposed technique is aimed at efficiently preventing users' privacy from third parties while reducing the load on the devices that make up the cloud environment, as well as reducing the authentication processing time of user privacy through the synchronization of servers and intermediate devices by replicating multi-group factors in the virtual environment. Because the proposed technique duplicates the user's key and simultaneously authenticates the user between the user and the server, between the user and the intermediate gateway device, it stores the user's replication key on the intermediate gateway device, enabling authentication with the server using the compound key instead of the user's proprietary key. Performance evaluations show that small wireless devices using virtual multi-group factor in cloud environments have an average of 14.8 percent more accuracy in the information they process to protect users' privacy. The processing efficiency with which users' privacy information using small wireless devices is sent and received to cloud-certified servers has increased by up to 19.6 percent. In addition, processing time was 21.1% lower when users' privacy between small wireless devices and cloud-certified servers was handled in a virtual environment. When small wireless devices are handled using multiple factors in a virtual environment, the overhead generated by virtual environments and authentication servers was 22.8 percent higher. Based on the results of this study, future studies plan to perform a performance assessment of a system by applying it to a system that supports actual cloud services.

ACKNOWLEDGMENT

This work was supported by the BB21+ Project in 2019

REFERENCES

1. J. G. Choi and B. N. Noh, “Security Technology Research in Cloud Computing Environment”, *Journal of Security Engineering*, vol. 8, no. 3, Jun. 2011, pp. 371-384.
2. Y. S. Jeong, “An Efficiency Management Scheme using Big Data of Healthcare Patients using Puzzy AHP”, *Journal of Digital Convergence*, vol. 13, no. 4, Apr. 2015, pp. 227-233.
3. Y. S. Jeong, “An Efficient IoT Healthcare Service Management Model of Location Tracking Sensor”, *Journal of Digital Convergence*, vol. 14, no. 3, Mar. 2016, pp. 261-267.
4. Y. S. Jeong, “Measuring and Analyzing WiMAX Security adopt to Wireless Environment of U-Healthcare”, *Journal of Digital Convergence*, vol. 11, no. 3, Mar. 2016, pp. 279-284.
5. A. Singh and K. Chatterjee, “Cloud security issues and challenges: A survey”, *Journal of Network and Computer Applications*. Vol. 79, Feb. 2017, pp. 88-115.
6. S. Singh, Y. S. Jeong and J. H. Park, “A survey on cloud computing security: Issues, threats, and solutions”, *Journal of Network and Computer Applications*, vol. 75, Nov. 2016, pp. 200-222.
7. J. Zhang, H. Huang and X. Wang, “Resource provision algorithms in cloud computing: A survey”, *Journal of Network and Computer Applications*, vol. 64, Apr. 2016, pp. 23-42.
8. V. Varadharajan, U. Tupakula, “Security as a service model for cloud environment”, *IEEE Transactions on Network and Service Management*, vol. 11, no. 1, Mar. 2014, pp. 60-75.
9. A. Iera, G. Morabito and L. Atzori, “The internet of things moves into the cloud”, *Proceedings of the 2016 IEEE International Conference on Cloud Engineering Workshop (IC2EW)*, Apr. 2016, pp. 191-191.
10. Saha HN. Mandal A. Sinha A. Recent trends in the internet of things. *Proceedings of the 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC)*, Jan. 2017, pp. 1-4.
11. A. Celesti, D. Mulfari, M. Fazio, M. Villari and A. Puliafito, “Exploring container virtualization in iot clouds”, *Proceedings of the 2016 IEEE International Conference on Smart Computing (SMARTCOMP)*. May 2016, pp. 1–6.
12. K. S. Dar, A. Taherkordi and F. Eliassen, “Enhancing dependability of cloud-based iot services through virtualization”, *Proceedings of the 2016 IEEE First International Conference on Internet-of-Things Design and Implementation (IoTDI)*. Apr. 2016, pp. 106–116.
13. L. Echenauer and V. D. Gligor, “A Key-Management scheme for Distributed sensor networks”, *Proceedings of the 9th ACM conference on Computer and communications security*. Nov. 2002, pp. 41-47.
14. H. Chan, A. Perrig and D. Song, “Random key predistribution schemes for Sensor networks”, *Proceedings of the 2003 IEEE Symposium on Security and Privacy*. May 2003, pp. 197-213.
15. S. Zhu, S. Setia and S. Jajodia, *A distributed group key managemet protocol for ad hoc networks*”, Unpublished manuscript, George Mason University, 2002.
16. A. Khalili, J. Katz and W. A. Arbaugh, “Toward Secure key Distribution in Truly Ad-Hoc Networks”, *Proceedings of the 2003 Symposium on Applications and the Internet Workshops(SAINT'03 Workshops)*, Jan. 2003, pp. 342-346.

AUTHORS PROFILE

Yoon-Su Jeong is received the B.S. degree in the department of computer science, Cheongju National University in February 1998. He received the M.S. degree and Ph.D in the department of computer science, Chungbuk National University in February 2000 and 2008. He is currently working professor in the department of Information and Communication Convergence Engineering, Mokwon University. His research interests also include cryptography, network security, information security, healthcare service, bioinformatic, cloud service, wire/wireless communication security, Privacy, Big data.

Dong-ryool Kim was born in Busan, Korea in 1967. He received a bachelor's degree in mathematics at Ulsan University. He received his master's degree in mathematics at Ulsan University in February 2001 and his doctorate at College of Education Kyung-nam University in 2005. He has been working in the Department of Engineering at the University of Tongmyong since 2005. His interest in research is also. Includes cryptographic technology, network security, information security and mathematics education.

Seung-Soo Shin is received the B.S. degree in the department of mathematic, Chungbuk National University in February 1988. He received the M.S. degree and Ph.D in the department of mathematic, Chungbuk National University in February 1993 and 2001. And He received the Ph.D in the department of computer engineering, Chungbuk National University in February 2004. He is currently working professor in the department of Information Security, Tongmyong University. His research interests also include cryptography, network security, information security.