Enhancing The Physical Security System of The Company's Access Control Using RFID

*Dividing into two aspects: Human and equipment access control

Cheongjun Kim
Industrial Security
Chung-Ang University
Seoul, Republic of Korea
black6765@gmail.com

Jaehyun Shin
Computer Science & Engineering
Chung-Ang University
Seoul, Republic of Korea
skwent77@gmail.com

Myoungjin Oh
Computer Science & Engineering
Chung-Ang University
Seoul, Republic of Korea
omjin7g@gmail.com

Sangyeop Park
Computer Science & Engineering
Chung-Ang University
Seoul, Republic of Korea
peeringsy1@gmail.com

Seunghyeon Lee
Industrial Security
Chung-Ang University
Seoul, Republic of Korea
shlee9912@gmail.com

Uichan Kim
Computer Science & Engineering
Chung-Ang University
Seoul, Republic of Korea
kwchany066@gmail.com

Zhongyuan Hu
Polytechnic Institute
Purdue University
Indiana, US
hu692@purdue.edu

Minji Lee
PhD, Technology
Purdue University
West Lafayette, IN, USA
lee3450@purdue.edu

Anthony H. Smith
Computer and Information Technology
Purdue University
West Lafayette, IN, USA
ahsmith@purdue.edu

***Abstract*—The global pandemic caused the prevalence of 'homeworking,' and this made the blind spot of security. In this situation, the usage of primary equipment which contains confidential information needs to have better security system. To realize this system, applying the RFID technique to increase safety by function as a sensor to collect the information of IoT devices was chosen. Using RFID, a countermeasure to strengthen the company's physical security was devised for both humans and equipment. The protocol of hashing and removing for RFID's information to handle theft or loss in human access control was suggested. Besides, the access process will devise the equipment's control of entrance and exit security considering both safety and effectiveness. Since the research is based on some significant factors that the most companies have and the previous studies to enhance the security to cope with the vulnerabilities, the research results are expected to strengthen the security and effectiveness of access control.**

***Index Terms*—RFID, IoT, Security System, Database**

I. Introduction

Due to the spread of the unexpected virus, a society of 'non-Contact' has arisen and it caused changes. Among those changes, what society currently focuses on is a working environment. Even with the severity of the pandemic, the jobs inevitably need to continue to function, which is why working from home is so prevalent. However, even when working from home, access to the company is sometimes unavoidable, so the control of personnel and equipment is very likely to cause problems. By reason of the reduction in manual control, security accidents like equipment loss, damage, theft are very likely to happen. To prevent all kinds of bad consequences, the use of RFID to strengthen the security level of access control now seems to be feasible.

Radio-frequency identification(RFID) [1] is a technology that applies radio frequency to identify a tagged object passively. It can be popularized in gate security, car rental, amusement parks, health care, etc. The RFID tags and RFID readers can be used to control the access of people. RFID reader reads the UID(Unique Identification) [2] of the RFID tag by using radio-frequency; UID is transferred to the database and compare the information. The database gets the corresponding information if the UID is correct.

II. Importance of the research

First, the research strengthens the management of equipment and personnel in various companies. This makes the use of the equipment and people become clearer so that the management becomes more convenient. It also reduces the possibility of theft and loss. Even if theft and loss occur, liability can be found from the person who used the equipment. Secondly, the technology of security level based on RFID classifies the safety level according to the characteristics of different equipment. Using the classification of security level, it becomes more convenient to manage equipment. Finally, based on the function of collecting information through RFID, epidemiological investigation can be carried out. Through the

time information stored when people pass the system, tracing the movement becomes effective.

The direction of the project is divided into two areas: Access of human and equipment. The theft problem can be solved for access of humans, and an epidemiological survey can be applied. For access of equipment, the access of bringing in and out is emphasized to improve the security of equipment by applying security levels at the same time.

III. Literature Review

In this part, related studies and the background of the project is handled.

A. Component of RFID

Research was conducted based on the RFID, which collects information, and access control operates authentication with that information. To understand this process, focusing on key components of RFID is needed. The components of RFID is as follows:

- **Tag.** An RFID tag is a device which is called as transponder [3]. Microchips are contained in tags to store each object's UID. With IC chip storing UID and antenna, tags are attached to the equipment. By using the antenna, tags receive the electromagnetic wave signal from the RFID reader [4]. And then, the tag delivers the data it has to the reader. In other words, they act as the carriers of transferring the data to the reader.
- **Reader.** RFID reader reads data sent from tags via antennas at a typical frequency [5].
- **Antenna.** The antenna of RFID collects data and is used as a means for tag reading [5]. Both tag and reader have an antenna so that they can transmit the data.
- **Database.** The database is the logical placement for storing data of the server. By comparing the UID given by the reader with the data in the database, tags can be authorized and access.

With these components, RFID can communicate by using the antenna of tag and reader [6]. Figure 1 shows how RFID operates.

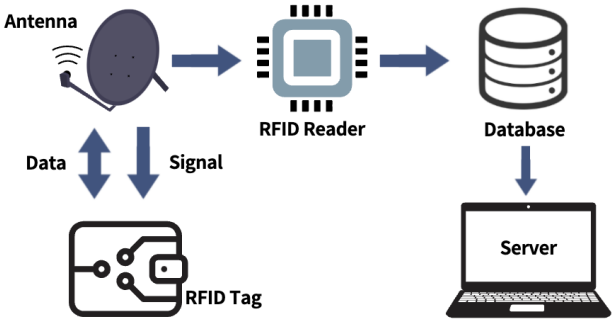

Fig. 1. RFID works in this way. Reader gets UID from tag by using antenna. And this UID is stored in the database so that server can access to that UID.

B. Radio-frequency of RFID

Each RFID tag has its own radio frequency, therefore tag can communicate with reader. The radio frequency of RFID is divided into three: Low frequency, high frequency, and ultra-high frequency [7]. Because each type of market requires different frequency, people need to apply adequate radio frequency to their business. Table I shows the types of radio frequency and their uses in the industry.

TABLE I
Types of Radio Frequency

Types of radio frequency	Radio frequency range	Features
Low frequency	125-135kHz	- Manufacturing business uses this range.
High frequency	13.56MHz	- Most usually used frequency. - Used for access control, management for equipment etc. [6] - Can be applied in various situations.
Ultra-high frequency	868-960MHz	- Can be applied in various situations [7].

Each type of radio frequency is used to the typical industries based on the frequency's features.

C. Relevant studies to improve the security of RFID systems

RFID system is useful in many areas, however, security systems need to avoid exposing data. In particular, the information transmitted by tags or stored in database should not be infringed. Therefore, hashing can be used in RFID systems same as cryptographic hash functions are used to protect the information in other systems. The followings are three typical characteristics of cryptographic hash function:

- **Pre-image resistance.** Characteristic that is difficult to find original input value from the hash value.
- **Second Pre-image resistance.** Characteristic that is difficult to find another input value that has the same hash value for the given input value.
- **Collision resistance.** Characteristic that is difficult to find different two input values with the same hash value.

These characteristics make it difficult to figure out the original plain text by output via hash functions. However, it is not impossible, so some hash algorithms are broken in security. Table II shows type and the state of security of representative algorithms.

TABLE II
Security for Typical Cryptographic Hash Algorithms

Algorithm	Year	Security
MD4	1990	Broken
MD5	1992	Broken
SHA-0	1993	Broken
SHA-1	1995	Broken
SHA-2	2001	Secure*
SHA-3	2015	Secure**

Table II consists of typical examples of cryptographic hash function. There are names for each algorithm, the year it was announced, and the security. The algorithm marked 'Broken' in the 'Security' column was exposed to critical attacks.

Security for the past hash algorithms such as MD4, MD5, SHA-0, and SHA-1 has become broken. In particular, the SHA-1 algorithm, which was actively used until the 2000s and 2010s, caused a big issue in 2017 when the attack on SHA-1 was successful [8]. SHA algorithm is the most commonly used algorithm of cryptographic hash functions, and the latest standard is SHA-3. SHA-3 is a more secure standard than SHA-2. Therefore, in this research, SHA-3 is used to hash the information in RFID systems. For additional security, "Salting" techniques are also applied to prepare for a variety of attack methods, brute force or rainbow table attack [9].

Meanwhile, there have been several studies based on "Security Level" as a way to enhance the security of RFID systems along with cryptographic hash functions [10], [11]. In this study, security level is applied to classify assets and improve the security. Security levels can be divided into several categories depending on the functionality of the asset. The application of the security level is possible through the modulo computation of each tag's UID. In this way, the access of corporate assets will be managed by classifying tags by security level in advance and combining them with corporate assets.

D. Background of the project

Reference [12] reveals the rapid development of attacks and changes in the environment prevailed with the spread of new virus, COVID-19. In this non-contact situation, there are changes in the working environment, such as teleworking [13], which stands for the situation people work in their private space. And these changes led to the result of an increase in the entrance and exit of company equipment and the loosening of the management of the come-and-go of people. Therefore, since RFID plays a vital role in preventing crimes [14], the importance of access control has become higher, and RFID can be applied to access control to enhance convenience and security. Many types of research and studies handled RFID to apply to access control and its effectiveness. Authors of [14] mentioned, through collecting personnel information, the system can track someone's trajectory and analyze the data given from RFID. Authentication of objects in complex areas also can be conducted by RFID [14]. However, when RFID tag and reader communicate using the antenna, the information leakage by eavesdropping on their communication channels or exposure of the data they transmit to the third party can happen [15]. With the importance of access control management on the rise, this research expects to construct the security system of companies and organizations by applying RFID to their access control system. Also, this research handles the implementation and effectiveness by dividing the primary elements which need to be controlled for access into two aspects: Humans and equipment.

IV. Environment Setting

A. Database

The system utilizes Google Cloud Firestore.

B. Technology infrastructure

The system's main operation is implemented with Python. There should be a JSON file containing the key to add Firebase to a server [16] and Figure 2 is an example of initializing Firebase. Libraries includes firebase-admin 5.0.1. Firebase-admin can be installed by using the command "pip install firebase-admin" [17].

```
cred = credentials.Certificate('./auth.json')
firebase_admin.initialize_app(cred)
db = firestore.client()
```

Fig. 2. The system initializes firebase in this way, and the private key should be used.

C. Equipment

Fig. 3. RFID tag can be in the shape of card and by tagging it to the reader, RFID reader can get the UID from tag.

There should be RFID readers and tags for getting UID values needed to test. Figure 3 is the picture of RFID reader and tag. MF(Mifare) RFID readers and MF 13.56Mhz RFID tags(ISO 14443A type) are used, and RFID readers are connected to the computer with the USB connector. When the RFID tags are sensed to the RFID readers, the UID value is entered by the keyboard emulator.

V. Principle

RFID system is implemented with hardware and software. The hardware consists of RFID tag, database, and RFID reader. There are two types of RFID tags to support personnel management and equipment management. For personnel management, only one type of RFID tag exists.

A. Code interface

1) Overall process: The application is executed before getting UID from RFID readers. As shown in Figure 4, since main.py runs, information such as UID, name, and password is entered through the console. If data needs to be protected, main.py uses hash function in hash.py to hash the data. In the case that needs to access or modify data in Firebase, main.py requests firebase.py to view and update information in the database. Figure 4 shows the overall process.

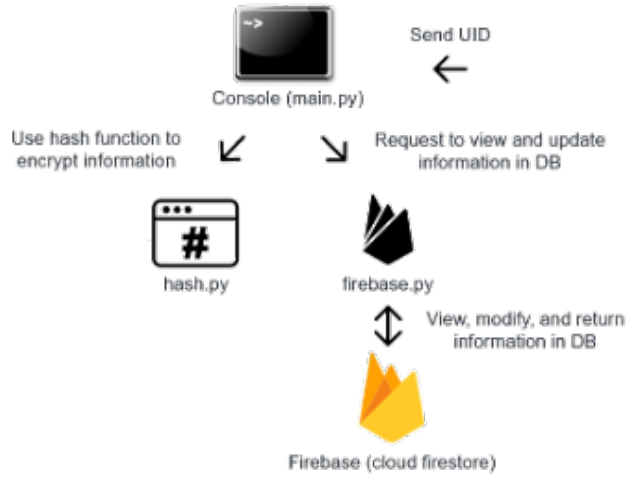

Fig. 4. The system works through this process when UID is entered.

2) Data hashing: When data is hashed, the SHA3-256 [18] is used. As shown in Code Snippet 1, sha3_256() is used for hashing.

```
hash(str, salt)
    data = str + salt
    return sha3_256(data)
```

Code Snippet 1. Pseudo-code of data hashing

And the most important thing is that there should be salt. A salt [19] is a random number or string that the system picks [9]. By adding salt to the existing data, information can be prevented from being read by rainbow table attack [9]. In most cases, each user uses a different salt stored in the database with the user's ID. And when system needs salt, the system retrieves salt value through the user's ID. However, in this application, the user's ID doesn't exist, and the UID used to access the information must be protected by hashing with salt. Therefore, it is designed to store multiple salt values in the database in advance, applying the salt values one by one when accessing the information, and find the correct salt value. This method has limitation that managers who can access the database can view all salt values. Still, if the salt value isn't exposed, it is meaningful that the information is stored differently, even if multiple users use the same password. The method is utilized in the process of hashing as shown in Figure 5.

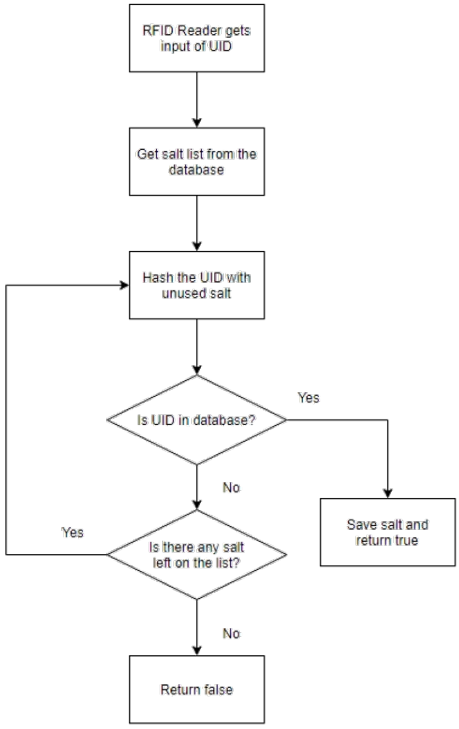

Fig. 5. Flowchart shows the overall process of hashing.

3) Access, register information: For security purposes, when inputting private information, such as UID and password, the input values should not be visible on the screen. Thus, the function is devised, which proactively prevents information leakage by outputting entered values in a '*' shape instead of the original values. There are two functions to register the information, and they are implemented separately according to material & user management. There are several ways to access the data stored in the database. The system can find documents with specific name or with username and password. Also, the system can find particular fields in a specific document, and get a list of all the salt values stored in the database. The list of salts is used as a source for finding the correct salt value in the process of verifying that the UID is already stored.

VI. Access Control of Human

A. Implementation

1) How it works: RFID personnel tracking software, with RFID reader and tag, stores personnel's entry_time and exit_time inside the 'User' table. Database in the Figure 6 means the database of security team in company. Figure 6 shows the flow of information. RFID reader and tag store personnel's information, and this database can be used to manage the status of employee. When the user walks in the company gateway with an RFID card tag, the entry_time field is updated. When a user leaves the company, exit_time

is updated. Employers can use the information to organize employees' attendance management.

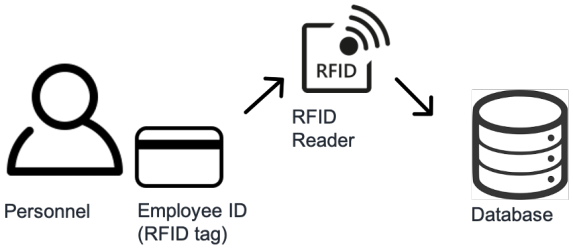

Fig. 6. Personnel tags RFID tag into the RFID reader. Then the reader sends tag ID to the database to check if the ID exists in the database.

2) Flowchart for corporate employee's attendance management: Human access control using RFID tags has two purposes, first to prevent outsiders from coming inside a company, and second for corporate attendance management. Figure 7 shows the overall process of corporate access control in the security system.

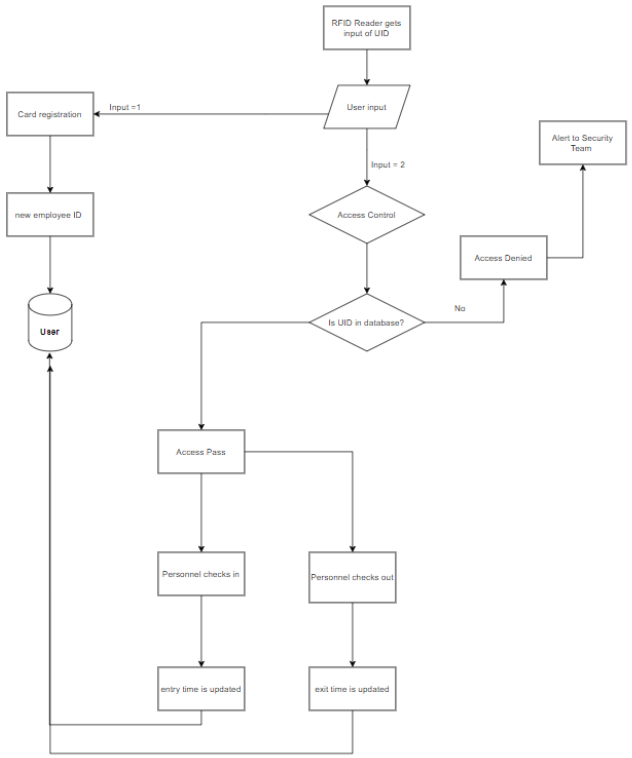

Fig. 7. Flowchart shows overall process of human access control.

First, the RFID reader reads a tag's UID. Second, the system checks if the UID exists in the database. If UID exists, entry_time is updated into the user table. Otherwise, the manager of the system checks if the user has permission to register to the system. If there's no permission for the user, then manager of the system denies the entrance of the user. Otherwise, the manager of the system allows user to write personal information. Then, the system saves personal information into the database. If UID exists in the database and if the user tags the card to exit, the system updates entry_time into the user table.

3) Test for entry_time and exit_time: Figure 8 shows a snippet of python console, which is the user interface. Employee's entry_time and exit_time from Figure 8 are exactly the same as 'User' table fields in Figure 9. When RFID tag is sensed by a reader, the time information is synchronized in the database.

```
Input = 5
**********
Entry_time : 2021-08-07 14:42:49.408450+00:00
Exit_time : 2021-08-07 16:11:10.063118+00:00
1 : Card registration
2 : Access control mode
3 : Report lost and stolen
4 : Card release
5 : Check the entry and exit time
0 : Exit
```

Fig. 8. The snippet of python console shows the functions of the user management.

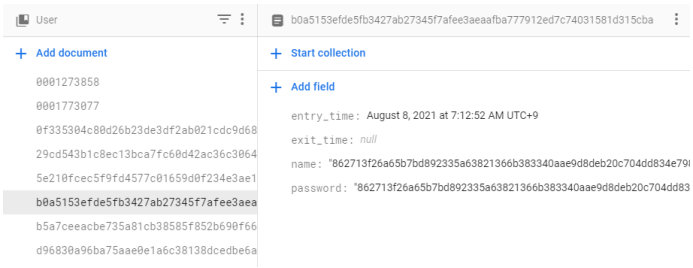

Fig. 9. User documents have four fields which are entry_time, exit_time, name, and password. Document's name means hashed UID. Name and password are hashed in the database.

4) Database schema for user: Table III shows the database schema of user.

TABLE III
DB SCHEMA

UID	Entry_time	Exit_time	Name	Password
UID-1	Entry_time-1	Exit_time-1	Name-1	Pw-1
UID-2	Entry_time-2	Exit_time-2	Name-2	Pw-2
...	...	...	...	...
UID-n	Entry_time-n	Exit_time-n	Name-n	Pw-n

UID means personnel's unique ID. Entry_time is recorded into the database when personnel enter a facility. Exit_time is recorded into the database when personnel exit a facility. Password is given by personnel who registers to the system.

VII. Entrance and Exit Control of Equipment

A. Implementation

1) How it works: Each RFID tag has a UID value, and the security level of RFID tags is classified according to the Table IV. The security level above are designed solely to

reduce the amount of computation in the database, and levels don't mean the degree of security.

TABLE IV
SECURITY LEVEL OF MATERIALS

Level	Type of material
1	Radio communication available equipment
2	Recording available equipment
3	Storage device
4	Confidential document

Security level divides equipment for efficiency of management. These levels can be revised by security manager based on each company's environment.

$$UID\ value\ mod\ 4\ +\ 1 \tag{1}$$

(1) is for the security level of the RFID tag. For example, since 0001234567 mod 4 = 3, the security level of the RFID tag whose UID is 0001234567 is 4. The reason for this security level division is to reduce the amount of computation. Since there are four security levels, these levels allow the equipment's data to be stored separately in four different tables. When security level is calculated to access or modify the information, the computation range can be reduced by a quarter to a particular table. When the system gets UID value, the system calculates the security level of UID and checks if UID is already stored in the database, which has the same security level. In the database, there is due_date information, so the system can check if the due_date is over, and send the messages to the manager of equipment.

2) Flowchart for equipment management: Entrance and exit control of equipment using RFID tags has the purpose to manage company's equipment efficiently.

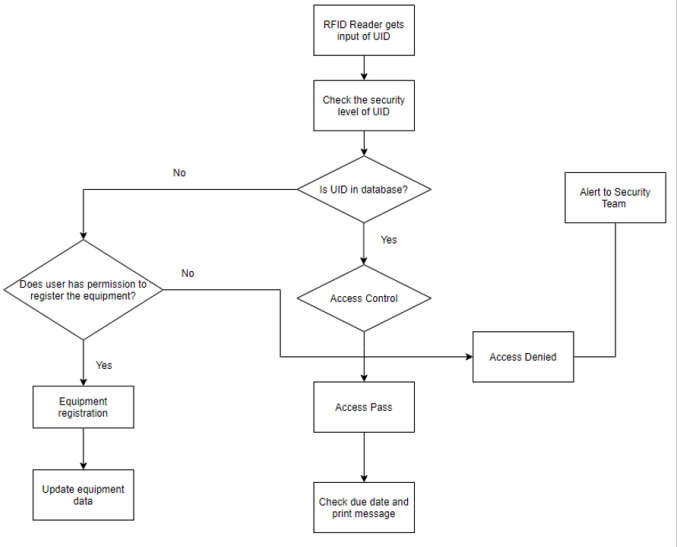

Fig. 10. Flowchart shows the overall process of equipment management.

As shown in Figure 10, the system is designed to provide registration, return and access control of the equipment. First, if RFID reader gets UID value from tag, the system checks the security level of UID and find the information in certain database. If UID is already stored in the database, system checks due_date and prints message to the manager. Otherwise, the system verifies the right to register the equipment and proceeds with equipment registration. User's name is required in equipment registration. If user doesn't have the permission, the access is denied.

3) Test for registration and access control: Figure 11 shows the test of the equipment's registration. Personnel enters his name "Steve" in this registration process. As shown in Figure 12, the information of equipment and due_date are stored in the database. Also, since UID used as a test is 0001234567, which is included in the security level 4, so the data is stored in the collection "Material_4." Figure 13 shows the test for access control, entered UID denoted as "**********" is 0000000000, so the system prints warning message.

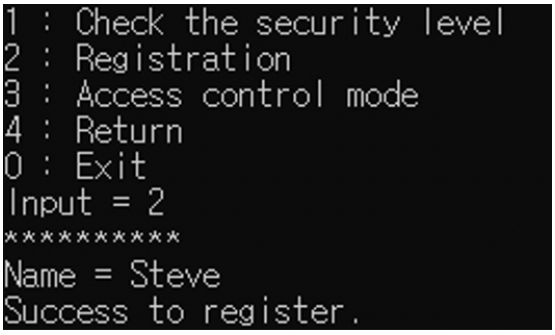

Fig. 11. When UID is entered, registration of equipment is proceeded.

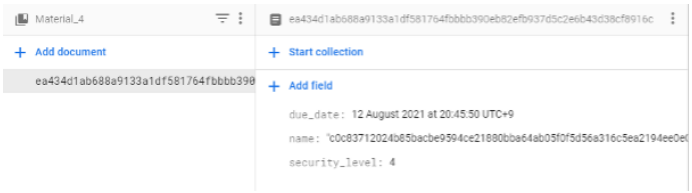

Fig. 12. After the registration, the information of equipment is stored in the database.

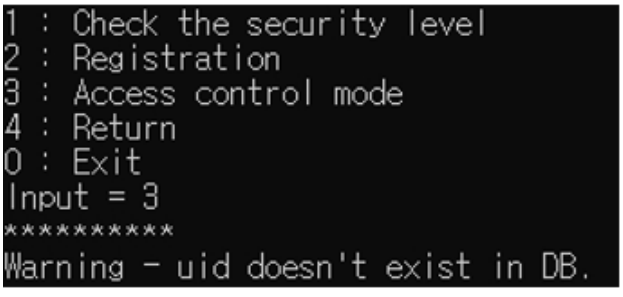

Fig. 13. During access control, external equipment is not accessible.

4) Database schema for material: Table V shows the database schema of material.

TABLE V
DB SCHEMA

UID	Name	Security_level	Due_date
UID-1	Name-1	Security_level-1	Due_date-1
UID-2	Name-2	Security_level-2	Due_date-2
...	...	...	...
UID-n	Name-n	Security_level-n	Due_date-n

UID refers to equipment's unique identification. Username and due_date are stored when equipment registration is in progress. Security_level is calculated with modulo operation.

VIII. Challenges

A. Finding the appropriate salt value for hashing

The first devised method for finding appropriate salt value for hashing was adding salt field to the user and the material table. The problem was that to find the salt value, the system needs a UID. However, to find a UID, the system needs salt since the UID should be hashed with salt value. To handle the dilemma, the salt table is added to the system. Figure 14 shows the salt table in the database.

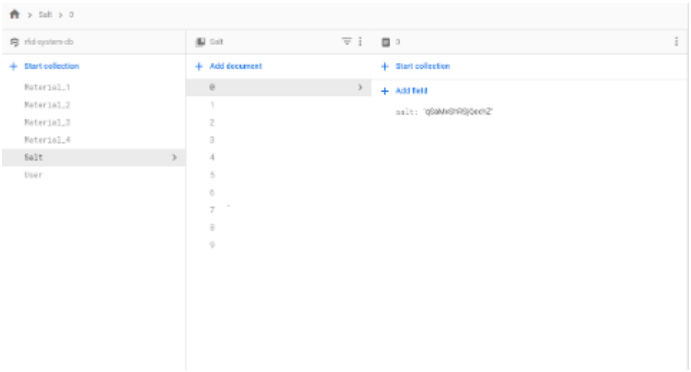

Fig. 14. The manager of the system can add new salt values into the salt table. One of the salt values is randomly chosen from the salt table.

However, a limitation exists for the method. To check if personnel or equipment is registered in the database, the system should continue combining all salt values one by one with UID until the hashed result of the combined value matches with the UID in the database. This process is inefficient since the size of the salt table affects the time complexity for checking if personnel or equipment is registered in the database. The best case is when appropriate salt value is found at once. The time complexity for the optimal case is then O(1) in Big O notation [20]. The worst case is when all salt values is used for finding UID in the database. The time complexity for the worst case is then O(n) in Big O notation.

B. Software requirements

Code execution environment should be confined to window operating system. Msvcrt [21] module is from python3 built for windows library file. Msvcrt provides access to some useful capabilities on Windows platforms. The code was implemented for windows platform command line interface, so the target users of this software should be organizations using window system.

IX. Conclusion

RFID access control system suggested in this research can be placed at the gate where the company's critical assets are located. People or equipment will be identified when they pass through the gate. This process has been simplified by tagging RFID cards on the reader. The gate will only open if the authentication of tag is valid.

A. Effectiveness for human access control

1) Budget perspective: Automated gate systems with RFID will save a lot of money by significantly reducing the number of people who control access.

2) Security perspective: It would be possible to have security against social engineering attacks that exploit "Human Error." Also, all access logs are automatically recorded, making it easier to trace back crimes.

3) Efficiency perspective: The system can be maintained around the clock, identification can be done within seconds.

B. Effectiveness for equipment access control

1) Security perspective: Companies can identify which equipment was brought by whom. This advantage protects the confidential information or documents stored in the company's equipment from security accidents such as theft or loss.

2) Efficiency perspective: Classifying tags with security levels improves efficiency. The process to identify the tags is simplified, and this leads to the efficient operation of RFID. This makes management of the equipment effective.

C. Expected effect for companies and society

This research was conducted to enhance the physical security system based on the access control using RFID. In this study, the access control system is executed effectively with a developed algorithm, even though there are limitations that the research couldn't find out the solution to find a salt value efficiently and does not support cross-platform. Introducing this program to the companies' access control system can get advanced safety and convenience with less effort. Besides, with the time data recorded when people has passed through the access control system, collecting the personal information for the epidemiological survey becomes easier. This is a strong point in society these days.

Consequently, the limitation has to be revised in further research and this system could bring more advantages for the environment changing continuously.

Acknowledgement

We thank Purdue University - Indiana's Land Grant University and Chung-Ang University for taking us to do project 11 in IITP-Summer-Program-2021. We would like to thank our supervisor Minji Lee for making feedbacks on our paper. We also would like to acknowledge our advisor, Professor Anthony Smith for gratefully giving feedbacks for deciding the directions of our project.

REFERENCES

[1] "Radio Frequency Identification (RFID)." FDA.gov. https://www.fda.gov/radiation-emitting-products/electromagnetic-compatibility-emc/radio-frequency-identification-rfid (accessed Jul. 30, 2021).

[2] M. Roberti, "Do tags and readers all have unique ID numbers?" RFID-journal.com. https://www.rfidjournal.com/question/do-tags-and-readers-all-have-unique-id-numbers (accessed Aug. 6, 2021).

[3] D. P. Chech et al., "The RFID technology and its applications: A review," *International Journal of Electronics, Communication & Instrumentation Engineering Research and Development*, vol. 2, pp. 109-120, Sep. 2012.

[4] X. Wang and Y. Wang, "An office intelligent access control system based on RFID," *2018 Chinese Control And Decision Conference (CCDC)*, 2018, pp. 623-626, doi: 10.1109/CCDC.2018.8407206.

[5] K. Ahsan, H. Shah and P. Kingston, "RFID Applications: An introductory and exploratory study," *International Journal of Computer Science Issues*, Vol. 7, No. 3, Jan. 2010, doi: http://ijcsi.org/articles/RFID-Applications-An-Introductory-and-Exploratory-Study.php.

[6] M. S. Son and B. L. Cho, "Technology of RFID Tag,"(in Korean), *Polymer Science and Technology*, vol. 17, no. 1, Feb. 2006.

[7] J. N. Kim *et al.*, "An analysis of RFID case studies,"(in Korean), *ETRI*, vol. 21, no. 2, pp. 161-169, Apr. 2006.

[8] M. Stevens, E. Bursztein, P. Karpman, A. Albertini and Y. Markov, "The First Collision for Full SHA-1," in *Annual International. Cryptology Conference*, Jul. 2017, pp. 570-596, doi: 10.1007/978-3-319-63688-7_19.

[9] U. Rathod, M. Sonkar and B. R. Chandavarkar, "An Experimental Evaluation on the Dependency between One-Way Hash Functions and Salt," in *2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, 2020, pp. 1-7, doi: 10.1109/ICCCNT49239.2020.9225503.

[10] S. H. Oh, J. Kwak, "RFID Tag's Security Level Based RFID Authentication Protocol," in *The Journal of Korea Information and Communications Society*, vol. 30, no. 6C, pp. 593-600, 2005.

[11] J. Y. Kim, J. J. Jung, G. S. Jo, and K. H. Lee, "A Study on Security Level-based Authentication for Supporting Multiple Objects in RFID Systems," in *The Journal of Society for e-Business Studies*, vol. 13, no. 1, pp. 21-32, 2008.

[12] T. Himdi, M. Ishaque and J. Ahmed, "Cybersecurity Challenges during Pandemic in Smart Cities," *2021 8th International Conference on Computing for Sustainable Global Development (INDIACom)*, 2021, pp. 445-449, doi: 10.1109/INDIACom51348.2021.00079.

[13] E. Babulak, "Teleworking and Next Generation Cyberpace," *2009 International Conference on Computational Intelligence, Modelling and Simulation*, 2009, pp. 142-146, doi: 10.1109/CSSim.2009.33.

[14] A. Mai, Z. Wei and M. Gao, "An Access Control and Positioning Security Management System Based on RFID," *2015 7th International Conference on Intelligent Human-Machine Systems and Cybernetics*, 2015, pp. 537-540, doi: 10.1109/IHMSC.2015.227.

[15] A. Razaq, W. T. Luk and L. M. Cheng, "Privacy and Security Problems in RFID," 2007 International Workshop on Anti-Counterfeiting, Security and Identification (ASID), 2007, pp. 402-405, doi: 10.1109/IWASID.2007.373665.

[16] Google, Mountain View, CA, USA, *Add the Firebase Admin SDK to your server*. (2021). Accessed: Jul. 25, 2021. [Online]. Available: https://firebase.google.com/docs/admin/setup

[17] *pip*. (v21.3.dev0). [Online]. Available: https://pip.pypa. io/en/latest/installation/

[18] L. Wagner. "How SHA-256 Works Step-By-Step." Qvault.io. https://qvault.io/cryptography/how-sha-2-works-step-by-step-sha-256/ (accessed Aug. 16, 2021).

[19] "LinkedIn Password Leak: Salt Their Hide," June 2012. [Online]. Available: https://queue.acm.org/detail.cfm?id=2254400&ref=fullrss

[20] P. E. Black. "big-O notation." NIST.gov., https://www.nist.gov/dads/HTML/bigOnotation.html (accessed Aug. 11, 2021).

[21] Python Software Foundation, *Useful Routines from the MS VCC++ Runtime*, Python Software Foundation, Aug. 16, 2021. Accessed on: Aug. 17, 2021. [Online]. Available: https://docs.python.org/3/library/msvcrt.html