IJOICT
ISSN 2460-9056
http://socj.telkomuniversity.ac.id/ijoict/

Intl. Journal on ICT
Vol. 6, Issue. 1, June 2020. pp. 10-22
doi: 10.21108/IJOICT.2020.61.480

Increasing the Security of RFID-based Classroom Attendance System with Shamir Secret Share

Aji Gautama Putrada [1], Maman Abdurohman [1*]

[1]School of Computing, Telkom University
Bandung, Indonesia

[*] ajigps@telkomuniversity.ac.id

Abstract

This paper proposes an attendance system for increasing the security based on Shamir Secret Share algorithm. The use of RFID devices for classroom attendance is still vulnerable to certain attacks. Students usually make use of existing loopholes for prohibited things, such as forged attendance. Shamir Secret Share is a security method based on the Secure Multiparty Computation (SMC) concept. The SMC guarantees not only the confidentiality of external attacks but also of each member in the secure system. In the attendance scenario using Shamir Secret Share, a student and a lecturer must do tapping at the same time; otherwise, the secret that opens the lock for attendance at that class will not be opened. To realize this system, this paper uses two RFID modules, each of which is connected to one nodeMCU microcontroller. Both systems are connected to a database where the Shamir Shared Secret calculation is performed. Some experiment has been implemented for proving the concept. The result shows that some scenarios of fraud in RFID based attendance can be prevented.

Keywords: RFID Card, Secure Multiparty Computation, Classroom Attendance System, Shamir Secret Share

I. Introduction

All non-mobile phone devices that are connected to the Internet can be classified as the Internet of Things. The technology of the IoT field in the last decade has been growing and advancing. With the presence of IoT technology, many companies or offices use the technology to improve their used facilities [1][2], one of which is the use of RFID Cards. RFID is a technology that has existed for the last 50 years, and in various industries, more and more are considering RFID [2][3]. The security system provided by RFID can be used for a variety of things, such as user attendance, as well as door lock securities.

The case which will be discussed here is about the attendance system in classrooms. Classroom attendance is the main condition for students to get good academic results. In this case, the use of attendance with RFID is quite effective and efficient because it can uniquely identify a person based on the Card entered [4]. Each student has an RFID that has been given by the campus to tap attendance in class, using a unique code that stores the student's own identity by using a UID (Unique Identifier) code that distinguishes students from one another. However, the use of RFID is only limited to UID storage, so the RFID is said to be still not safe.

Received on 20 Mar 2020. Accepted on 18 May 2020

One of the scenarios of fraud is, students who did not attend class will secretly approach class and do tapping when a class has been dismissed, but there is still time left until the next class. So, in fact, the student did not come to class but was considered to be present by the system.

Therefore it is necessary to increase security and awareness of data storage in RFID users [5]. Efforts to increase security can be done by doubling security on RFID users [6]. What is meant by doubling the security of this system is to add code by implementing Secure Multiparty Computation (SMC), which performs simple correlations using card patterns. The card stores data that will be processed by the Shamir Secret Shared method. This increase in security is to prevent attendance fraud by students who can use more than one RFID card.

The concept of SMC is to guaranty not only the confidentiality of external attacks but also of each member, meaning that this system works highly effective when internal parties have low mutual trust, as in between lecturers and students. In an attendance system based on SMC, the key of two parties, in this case, the student and the lecturer, is needed to open the lock of the student's attendance in that classroom. In other words, there is no way a student can do RFID tapping without the presence of the lecturer.

Shamir Secret Share is one of many methods to implement SMC. The concept of this method is using algebra. The parties of the secrecy share a point in a function, and if not all points or parties are complete, the point of the secret will not be revealed. The consequence is that the more the parties in the SMC, the more complex the line is. For example, a two-party SMC will only need linear algebra, and a four-party SMC will need a polynomial line.

Based on the problem statement, which is a vulnerability in classroom attendance based on RFID Cards, this paper aims to increase the security of an RFID-based classroom attendance system with Shamir Secret Share.

Because the parties involved in this system are two, the student and the lecturer, linear algebra is used. Two RFID Card Readers will be involved in the system. This is necessary because the tapping needs to be executed simultaneously. Each reader will be controlled by one NodeMCU Microcontroller. This NodeMCU Microcontroller will be connected to a database. The Shamir Secret Share calculation will be done in the database. The attendance system will also reside in the database.

The systematic of this paper is as follows. The first chapter is about the introduction. Motivation, problem statement, and research aim are elaborated in this section. The second chapter is about related work. In this section, other researches and papers are explored to define the position of the current research. The third chapter is about the design of the system. This section will discuss the legacy system, possible attack scenarios, and the design of the secure system proposed. This section will also explain about the Shamir secret share used in the research. The fourth chapter is about evaluation. In this section, the defense of the system will be tested, and the results will be discussed. The fifth chapter is the conclusion. This section will mention and highlight findings in this research. Future work will also be provided.

II. RELATED WORK

RFID based attendance systems have long been the subject of research. One of them is research in 2016 [7]. This study explores the advanCardes of implementing an RFID-based attendance system. In addition to the attendance system, this study also discusses the RFID system in other fields such as logistics, animal husbandry, libraries, and also the use of active RFID. This research successfully proved that the attendance system using RFID would bring efficiency. This efficiency will lead to a return in investment and an increase in lecturer income.

Similar research in 2018 used several IoT devices to enhance the learning interactivity in the class [8]. RFID Card was one of the devices involved. This research bundled the RFID Card with nodeMCU to create a long-range Card system. The Card is used so that lecturers can report students. This research also applied QR Codes to ease the user's response system. Through the research, the authors can prove that the system increases student attendance in class.

Another research in 2019 studied the time improvement in using RFID Cards compared to conventional attendance system [9]. What is meant by the conventional attendance system is when the teacher calls the name of the students one by one and checks their names on the attendance form. To compare the time of each system, a stopwatch is used as a measurement tool. The results of this research prove that using RFID Cards, the time consumed to take attendance of a class is 20 to 40 seconds. Faster than a conventional method that takes approximately 40 to 200 seconds. The research states that fraud can occur when a student brings two or more cards, substituting their friends to take attendance in class.

Attacks and defenses on RFID Cards have also been a common research field. Many types of attacks can be launched upon an RFID Card system. Likewise, RFID Card defense systems also take many forms. A research in 2015 promotes Brute Force as an attack that has a high threat towards RFID Cards [10]. As a defense system, this research chooses hashing. Through the proposed system, the defense system will cause a brute force attack to have a cost of 2192. This is a way much higher cost than what it takes to brute force a conventional RFID system, which is 296. This also includes if the card went through eavesdropping.

Another paper discussing a different attack is research on Replay Attacks on RFID [11]. A replay attack is when an adversary steals information from a card and stores it in another card or a card emulator for fraud intention. The paper discusses a previous paper and points out the failure of that paper in handling Replay Attack, thus proposing a correct solution. In the previous paper, it said that the replay attack could be solved if two RFID Cards are involved; the method is called "Yoking Proof". But the amount of Cards involved is not the issue in Replay Attack as they can copy any amount of Card as they like. The previous paper then proposes "Grouping Proof", another method just like "Yoking Proof", but this time, adding timestamps, to distinguish the time difference in each operation. Again this is still not the issue, as timestamps can be forged. The paper proposes a better mechanism to defend against Replay Attack.

Besides brute force, eavesdropping, and replay attack, cloning is another famous attack against RFID Cards. Cloning is simply doubling or faking an RFID Card. There are no two RFIDs in the world with the same UIDs. But in cloning, the adversary creates a fake RFID Card with the same UID as the victim, using special kinds of RFID Cards, thus using it for fraud intention. The research discusses this attack and advices as a system to prevent cloning [12]. This paper proposes the idea of metaID. MetaID is a once in a lifetime ID. It is an ID stored in the memory of the RFID Card. Each time the card is used, the metaID changes, thus if cloned, the cloned version of the card will receive useless information. To also defend the card from eavesdropping, the system adds hashing, so communication of the metaID cannot be detected.

III. ARCHITECTURAL REQUIREMENTS

A. RFID Card

RFID is one of the "what you have" based authentication techniques. The RFID system consists of two parts, namely the RFID tag and the RFID reader. RFID tags are usually card-shaped, in this card there is a microchip that is able to store information, including a UID containing a unique number that is not owned by another RFID card in the world [13]. Communication between the tag and the reader occurs wirelessly, using radio frequency technology, hence the name RFID [13] [14]. During communication between the tag and the reader, a UID will be sent for authentication. In order to save power, communication between the tag and reader is done with a very low range; therefore, the way to authenticate is to touch the RFID tag with the

Reader. One of the RFID protocol technology users is advanCarde [14]. RFID systems have 2 important parts, namely:

1) RFID Reader. RFID Reader is the "keyhole" in the RFID authentication system. RFID Reader will be attached to a guarded or protected asset. RFID Reader is usually a peripheral for a computer [8]. RFID Reader consists of a microprocessor or microcontroller and an antenna [15]. Fig. 1 gives an overview of an RFID reader.
2) The antenna functions as a transmitter and receiver of radio frequency signals between RFID readers and RFID tags [15]. RFID tags have a compact form so that this antenna is not visible. In Fig. 1 can be seen that this tag is spiraling around the card. This antenna is hidden in the outer layers of the card and not visible. [16]. RFID card communication is passive, meaning that this card receives power from the emission of an RFID Reader signal to send data.

B. Legacy RFID-Based Classroom Attendance System

The Telkom University Classroom Attendance System is used as a case study in this research. In this case, The Student ID Card given to each student is actually an RFID card. This Student ID Card can be used for class attendance. In each class, one RFID Reader has been installed and is connected to the campus information system. During class, students can do the tapping. This tapping will go into the campus information system and be considered as attendance at the class. Tapping is considered valid only if the lecturer concerned has already done the tapping. If outside of lecture time tapping is done, tapping will not be considered valid.

C. Attack Schemes

As discussed in Chapter 1 and Chapter 2, there are many scenarios that can be launched against an RFID system and specifically in an RFID-based Classroom Attendance System. The First scheme is attendance forgery. There have been two scenarios. The first scenario is done by tapping attendance in an opportunity window between the end of class and the next class. The second scenario is done by substituting a friend, bringing the friend's RFID Card, and tapping on the friend's behalf without the lecturer paying attention. The second scheme is brute force. The adversary uses a fake card, with fake UID but does not know the correct UID, hence trying a UID one by one. The third scheme is the Replay attack. The adversary saves the data inside a card emulator and uses it for fraud intent. The last is cloning; the card is copied into another card, thus creating a replicate card, used for fraud.

D. Secure Multiparty-Computation

In a conventional RFID-based attendance system, the RFID Reader will be located near the classroom door [9]. The reason is to follow the flow of students entering the classroom. In an SMC system, the tap of the student's RFID Card will need to be simultaneous with the tap of the lecturer's RFID Card. Hence, another Reader is required. To ease the flow mentioned before, the Reader for the lecturer's RFID Card needs to be near by the lecturer's desk. Fig. 2 shows the planning of the classroom and the Two RFID placements.

In Fig. 2 it can be seen that there are two RFID Readers; One near the Door and one above the Lecturer Desk. Students will tap their cards on the reader near the door, and lecturers will tap their RFID Cards on the reader on the desk.

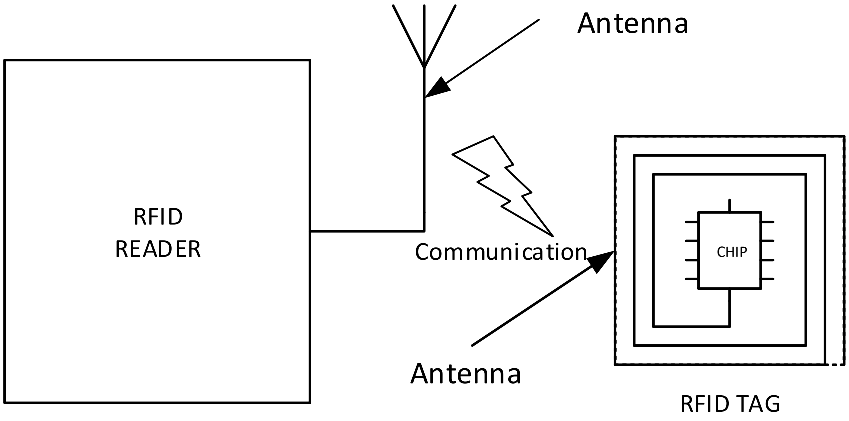

Fig. 1. RFID Reader and Tag wireless communication

E. System Block Diagram

To implement the system, two RFID Readers are required. Each RFID reader needs to be connected to a common database, so each RFID Reader will be connected to a NodeMCU. A NodeMCU is a microcontroller with Wi-Fi capabilities. A database is deployed in a server. The server communicates with the NodeMCU, creating the Shamir Secret Share system. Fig. 3 shows a comprehensive view of the system.

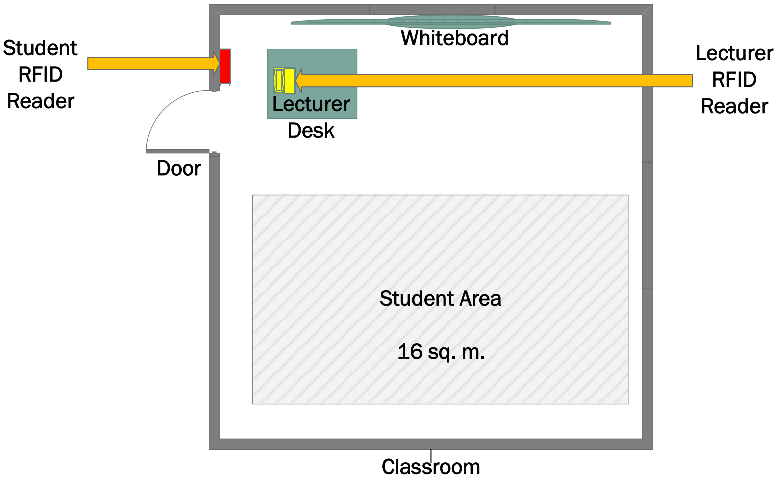

Fig. 2. Placement of Student RFID Reader and Lecturer RFID Reader in Classroom

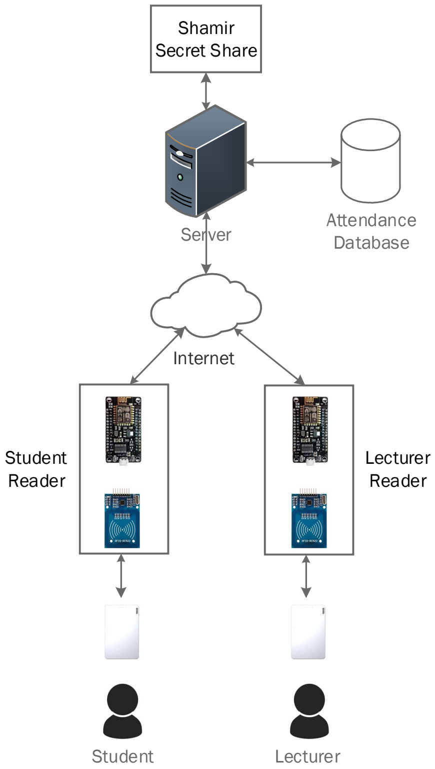

Fig. 3. System Block Diagram

F. *Shamir Secret Share*

Shamir Secret provides a very important basic secret sharing scheme concept. In understanding this sharing scheme, it is divided into sections in the secret scheme, which are separated into n sections to share with the participants. When using it by doing a merge that has been agreed to access the secret. The process of reconstructing this secret is very important for the prevention of attacks against the system. In 1979, Shamir and Blakley each proposed a method of sharing this secret with the Lagrange interpolation formula and the nature of vector spaces. The proposition is given a value of N + 1 points (xi, f (xi)) in a polynomial [17]. One can identify the polynomial f(x) degree n by calculating formula (1).

$$f(x) = \sum_{i=1}^{n}(y_i \prod_{1\le k\neq i\le n} \frac{x_k}{x_i - x_k}) \tag{1}$$

where x is the input variable, y is the output variable, k is the degree of each equation, and i is the degree of the equation.

Equation (1) is a Lagrange formula that has been modified to optimize the computation of the Shamir Secret Share. The resultant of the secret will be the free coefficient of the final formula.

The way to share the secret is to divide it into n pieces. In Shamir Secret Share, these n pieces form a line. For example, if three pieces of points of a parabola curve are known, the function of the curve can be calculated via Lagrange Formula in equation (1). Without one piece of information, the function cannot be formed. The number of pieces of information needed to open the secret is known as k.

As defined by Shamir, k pieces of points are needed to form a polynomial of degree k-1. Because in this case, the secret is shared between the lecturer and the student, the k value is 2, meaning that the degree of the polynomial is 1, in other words, a linear curve.

By limiting the case to s = k = 2, and the use of a linear curve, as an alternative to equation (1), the slope-intercept mechanism can also be used to find the curve. By deriving the slope-intercept equations, the equation to find the secret is as in equation (2).

$$c = y_1 - \frac{y_2 - y_1}{x_2 - x_1} x_1 \tag{2}$$

where c is the intercept or the free coefficient of a linear curve or the secret itself, (x1, y1) is the first point, and (x2, y2) is the second point. It should also be noted that y2 and x2 in the equation above can be substituted by y1 and x1; the result will not differ.

Technically this secret division will become a share by using two users. So, in this case, the calculation of interpolation theory is used to form a linear equation, namely y = a0 + a1x. So we need two points, the points are (x1, y1) and (x2, y2). The steps taken are as follows:

Interpolate two points on a straight line y = a0 + a1x, namely (x1, y1) and (x2, y2). Where (x1, y1) is determined as the lecturer point and (x2, y2) is determined as the student point

The two points are translated into the following linear equations:

a) y1 = a0 + a1x1
b) y2 = a0 + a1x2

Fig. 4 illustrates an example of the Shamir Secret Share in the RFID-based Classroom Attendance. In the example shown in Fig. 4, the secret piece saved in the lecturer's RFID Card is (6,5), and the secret piece saved in the student's RFID Card is (10,7). By illustration, when the two tap their cards together, the two points will show up and form a line. The line's intersection with the Y-axis will be the secret to unlock the student's attendance of that class at that time.

The real process is to reconstruct the equation of the two points. This is done by executing equation (2), producing C, which is the secret to unlock the attendance.

To implement the system, two RFID Readers are required. Each RFID reader needs to be connected to a common database, so each RFID Reader will be connected to a NodeMCU. A NodeMCU is a microcontroller with Wi-Fi capabilities. A database is deployed in a server. The server communicates with the NodeMCU, creating the Shamir Secret Share system. Fig. 4 shows a comprehensive view of the system.

As shown in Fig. 4, the absence of a single point will give infinite possibilities of intercepts to the only point in the graph with the Y-axis.

Shamir Secret Share also addresses the issue of scalability. A classroom does not only consist of one lecturer and one student. Also, one student can have many lecturers, meaning that there are many relationships between students and lecturers. To illustrate that Shamir's Secret Sharing can be scaled and can adapt to scale-up systems, an example is given. An example can be seen in Fig. 5.

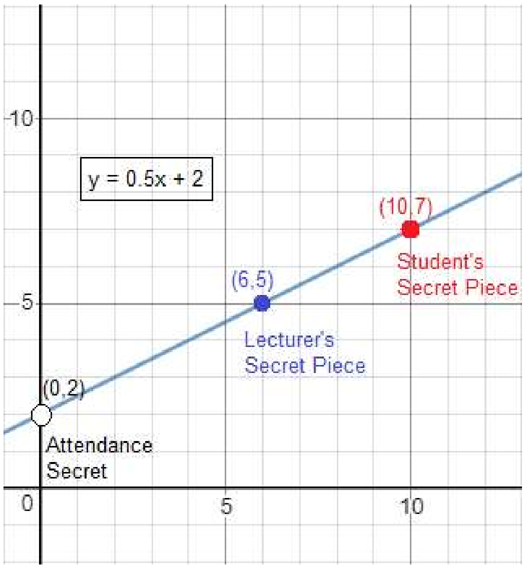

Fig. 4. Illustration of Shamir's Secret Share on RFID-based Classroom Attendance System

The RFID-based Classroom Attendance System with Shamir Secret will apply polynomials of degree 1, aka linear curves. One can argue that the number of polynomials must follow the number of students in the class. So that all students plus lecturers must do tapping so that attendance is recognized. But this is not applied, because if there is at least one student not present, then the whole class cannot do the tapping. In addition, the complexity increases because there must be adjustments to polynomials for different class sizes. The solution for a class with many students is to make one point in the graph that is unique to one lecturer or one student, which means that the relationship between each pair of lecturer-student points in the graph will lead to secrets.

The system can be designed to be user friendly. For example, lecturers feel bothered because they have to tap repeatedly every student doing the tapping. This will not happen because lecturers can place and leave their card on the lecturer tapping machine while the students take turns tapping.

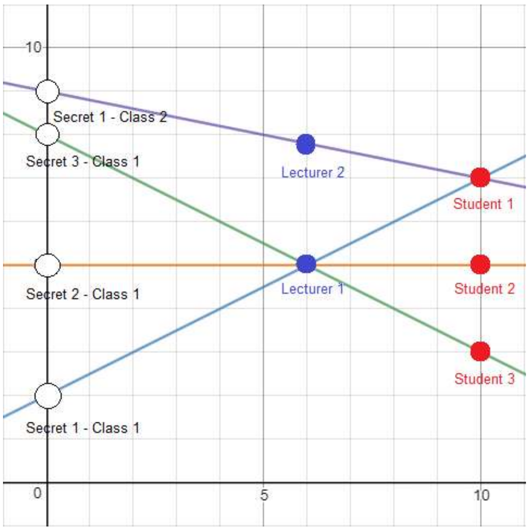

Fig. 5. A scalability showcase that is an illustration of a multiclass - multistudent secret sharing system

IV. RESULTS AND ANALYSIS

A. Analysis over Attendance Forgery Attack

There are two scenarios of attendance forgery attack concerned in this paper. To explain each forgery attack, Fig. 5 has been made. There it can be seen that a window is present between the end of the class and the next class where an adversary can forge an attendance.

A hypothetical system can be imagined where the problem in the sequence diagram in Fig. 5 can be overcome by a second lecturer tap. The second tap of the lecturer will end the attendance session. After the second tap, students cannot tap again. But this does not address the second attendance forgery scheme. The second forgery scheme is when a student carries two RFID cards; a student card and a friend's card, and taps both of them without the teacher realizing it [9]. That will be called Substitute Attendance Forgery. Fig. 6 explains the scheme. It can be seen here that forged tapping can still occur in permitted sessions.

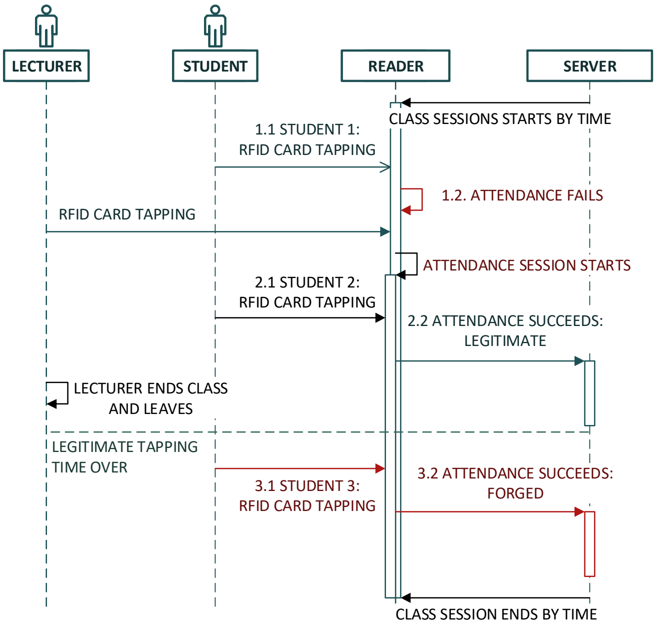

Fig. 5. Legacy RFID-based Attendance System and Fragilities

Fig. 7 shows how Shamir Secret Share will defend against the first forgery scheme. It can be seen that the adversary cannot tap the forged attendance because the lecturer's RFID Card is released from the reader.

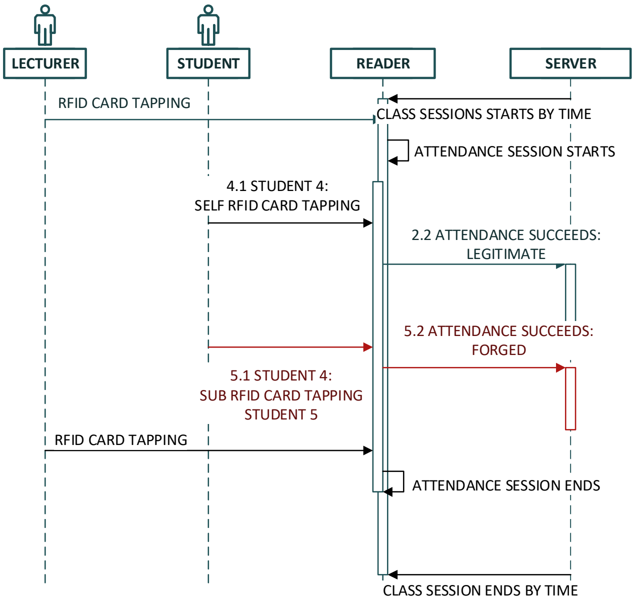

Fig. 6. RFID Card Substitution Tapping Attendance Forgery Scheme

Fig. 7 also shows how Shamir Secret Share will defend against the second forgery scheme. It can be seen that only one pair of secret pieces will work at one time. Hence tapping two cards at the same time will not work. Here an assumption must be made where the reader used has anti-interference. Anti-interference prevents two or more cards from being tapped at once. So if a student wants to tap two cards at a time, the student must have to wait for a while until there is a sign where the student can do a second card tapping.

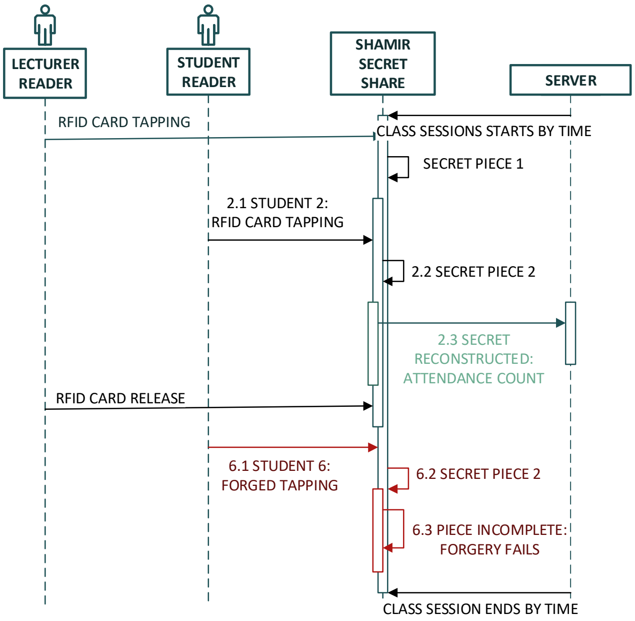

Fig. 7. Shamir Secret Share solution to Attendance Forgery

B. Analysis over Brute Force Attack

In order so that the attendance forgery scheme in the previous part can succeed, the lecturer should be present, or at least the lecturer's card should take place in the second card reader. This can only happen if the card is stolen or in a second scenario, a rewritable UID card or clone card is used. If the real card is not present to be copied, one can only brute force the lecturer's secret piece into the system.

In order to brute force the lecturer's secret piece, the complexity cost will be 232 that is the number of possible UIDs if the field is 32 bits long. This is still a higher cost compared to the legacy system where brute force is not required.

C. Analysis over Other Attacks

Despite being safe from attendance forgery and relatively safe from brute force attacks, the system is still vulnerable to other attacks. The attacks discussed here are eavesdropping, cloning, and replay attack. Through eavesdropping, the adversary can receive transmission between the communication between card and reader, thus retrieving the UID for the cloned card. Through cloning, the adversary can steal the card for a moment or use phishing readers to create a clone card for fraud intentions. Through a replay attack, the adversary can create a card emulator by tapping the emulator to the lecturer's card; the adversary emulates the same card to forge attendance.

Cloning is also a threat for the legacy system. Despite the threat of cloning by Shamir Secret Share, cloning lecturer's card will be more challenging than cloning a student's card for forgery. The effort also increases because two cards need to be cloned for a complete cloning attack. Other solutions to these attacks are such as metaID and mutual hashing or synchronized secrets. These methods can be implemented in future work.

Table I summarizes the security comparison of the legacy system and the new system against all the attacks that have been discussed, namely Forgery, Brute Force, Eavesdropping, Cloning, and Replay Attack.

TABLE I
SECURITY COMPARISON

No.	System	Security Attack				
		Forgery	Brute Force	Eaves-Dropping	Cloning	Replay
1	Legacy System	X	X	X	X	X
2	RFID-based Classroom Attendance System with Shamir Secret Share	O	△	△	△	△

O = secure, △ = partially secure, X = vulnerable

D. Performance Analysis

Performance Analysis of the addition of security in the form of Shamir Secret Share is done by comparing the time complexity and the communication round of the new system with the legacy system. The new system or RFID-based Class Attendance System with Shamir Secret Share consists of two main processes; linear curve reconstruction and linear search of shared key results. The linear curve reconstruction algorithm is an equation that is not limited by the size of the variable, meaning that whatever the value is sought, the time spent will be the same. This means that linear curve reconstruction has a constant time complexity; the big O notation is O(1). Furthermore, the linear search of the shared key result has linear time complexity; the big O notation is O(n). So the big O notation (worst case) of the overall time complexity of the RFID-based Class Attendance System with Shamir Secret Share is O(n). Whereas the legacy system only uses linear search to find ID tags from a lecturer or student cards, the time complexity is linear, and the big O notation is O(n). Then the time complexity of the two systems is the same.

The second performance analysis is done by calculating the communication round of the two systems. Legacy systems require three communication rounds, the first to activate class time, the second to activate lecturer time, the third to activate student time. The same number of communication rounds needed by the new system. The first round is for class time. Class time activates the possibility of a shared secret. The second round is for the first secret piece, and the third round is for the second secret piece. The conclusion is that both systems have the same number of communication rounds. A summary of the RFID Based Attendance System with Shamir Secret Share performance analysis can be seen in Table II. The second performance

TABLE II
PERFORMANCE ANALYSIS

No.	System	Computational Cost		
		Operation	Time Complexity	Communication Round
1	Legacy System	LS	O(n)	3
2	RFID-based Classroom Attendance System with Shamir Secret Share	LCR + LS	O(n)	3

LCR = Linear Curve Reconstruction, LS = Linear Search

V. CONCLUSION

An RFID-based Classroom Attendance System using Shamir Secret Share has been implemented. The system consists of two RFID Readers with Wi-Fi Connection capabilities and a Server containing a Database and the Shamir Secret Share computation. The implementation exercises one of the Shamir Secret Share properties, which is flexible, as it is proven to no be burdened by the complexity of the multiclass – multistudent nature of a university. The implementation is tested over several attack scenarios and is proved to tackle the main problem addressed in this paper, which is Attendance Forgery. Two forgery scenarios have been proven not applicable in this secure system. The linear curve reconstruction of the second-degree polynomial type Shamir Secret Share is computationally lightweight, meaning that the addition of the security will not be a difference in time complexity compared to the legacy system. For the proposed system, in order so that attendance forgery can succeed, the brute force needs to take place. In this case, the implementation also proves to complicate the brute force attack, although, through eavesdropping attacks, the cost of brute force can decrease. Despite this situation, the complication is still at a high level compared to the legacy system. For future work, a finite field algorithm can be implemented to harden the system against the eavesdropping attack. Moreover, the system can be enhanced to defend against other attacks. The implementation of a metaID can be used against cloning attack threats. The implementation of hashing and random number generation can be used against replay attacks.

ACKNOWLEDGEMENT

The author would like to thank Telkom University for allowing making the problem in the RFID-based classroom attendance system a case study in this research.

REFERENCES

[1] S. Singh, A. Kaushik, and S. S. Chitkara, "Ubiquitously controlled personalized smartlock," *Proc. Int. Conf. IoT Soc. Mobile, Anal. Cloud, I-SMAC 2017*, pp. 686–691, 2017.

[2] Y. M. Hwang, M. G. Kim, and J. J. Rho, "Understanding Internet of Things (IoT) diffusion: Focusing on value configuration of RFID and sensors in business cases (2008–2012)," *Inf. Dev.*, vol. 32, no. 4, pp. 969–985, 2016.

[3] S. L. Ting, A. H. C. Tsang, and Y. K. Tse, "A framework for the implementation of RFID systems," *Int. J. Eng. Bus. Manag.*, vol. 5, no. 1, pp. 1–16, 2013.

[4] T. S. Lim, S. C. Sim, and M. M. Mansor, "RFID based attendance system," *2009 IEEE Symp. Ind. Electron. Appl. ISIEA 2009 - Proc.*, vol. 2, no. Isiea, pp. 778–782, 2009.

[5] M. Burmester, J. Munilla, and A. Ortiz, "Comments on 'Unreconciled collisions uncover cloning attacks in anonymous RFID systems,'" *IEEE Trans. Inf. Forensics Secur.*, vol. 13, no. 11, pp. 2929–2931, 2018.

[6] F. Kerschbaum and N. Oertel, “Privacy-preserving pattern matching for anomaly detection in RFID anti-counterfeiting,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 6370 LNCS, pp. 124–137, 2010.

[7] M. Meghdadi and A. A. Azar, “The Possibility of Using RFID System to Automate and Integrate the Attendance of Professors and Students in the Classroom,” *Intell. Control Autom.*, vol. 07, no. 04, pp. 93–109, 2016.

[8] P. Tan, H. Wu, P. Li, and H. Xu, “Teaching Management System with Applications of RFID and IoT Technology,” *Educ. Sci.*, vol. 8, no. 1, p. 26, 2018.

[9] P. Sihombing, J. Timanta Tarigan, A. Khair, and H. Rumapea, “The Student Attendance Controlling by Using RFID (Radio Frequency Identification) to Increase the Time Optimization and Accurate of Data,” *J. Phys. Conf. Ser.*, vol. 1235, p. 012039, 2019.

[10] J. S. Cho, Y. S. Jeong, and S. O. Park, “Consideration on the brute-force attack cost and retrieval cost: A hash-based radio-frequency identification (RFID) tag mutual authentication protocol,” *Comput. Math. with Appl.*, vol. 69, no. 1, pp. 58–65, 2015.

[11] S. Piramuthu, “On Existence Proofs for Multiple RFID Tags,” no. June, pp. 317–320, 2006.

[12] T. Dimitriou, “A lightweight RFID protocol to protect against traceability and cloning attacks,” *Proc. - First Int. Conf. Secur. Priv. Emerg. Areas Commun. Networks, Secur. 2005*, vol. 2005, pp. 59–66, 2005.

[13] S. Nath, P. Banerjee, R. N. Biswas, S. K. Mitra, and M. K. Naskar, “Arduino based door unlocking system with real time control,” *Proc. 2016 2nd Int. Conf. Contemp. Comput. Informatics, IC3I 2016*, pp. 358–362, 2016.

[14] Z. Zhi-yuan, R. He, and T. Jie, “A method for optimizing the position of passive UHF RFID tags BT - RFID-Technology and Applications (RFID-TA), 2010 IEEE International Conference on,” no. June, pp. 92–95, 2010.

[15] M. Andriansyah and M. Subali, “e-KTP as the Basis of Home Security System using Arduino Uno,” *CAIPT*, pp. 1–5, 2017.

[16] K. V. Seshagiri Rao, Pavel V. Nikitin, and Sander F. Lam, “Antenna design for UHF RFID Tags: A review and a practical application,” *IEEE Trans. Antennas Propag.*, vol. 53, no. 12, p. 3870, 2005.

[17] A. Shamir, “How to share a secret,” *Commun. ACM*, vol. 22, no. 11, pp. 612–613, 1979.