International Journal of Latest Engineering Research and Applications (IJLERA) ISSN: 2455-7137

Volume –05, Issue – 10, October 2020, PP – 01-08

Internet of Things Base Smart Card Authentication Device for Smart Class Room Concept

Kadek Suar Wibawa[1], I Made Sunia Raharja[2]

[1]*(Information Technology Department, Faculty of Engineering Udayana University, Indonesia)*
[2]*(Information Technology Department, Faculty of Engineering Udayana University, Indonesia)*

Abstract: A smart classroom is a modern concept in the world of education. This concept has become a trend as a result of the direction of the industrial revolution 4.0. Internet of things technology as one of the foundations for the 4.0 industrial revolution provides convenience in service access, device interconnection, and system development. Centralized access to the smart class can facilitate service management and tracking of class users. NFC technology offers easy system user authentication. The user ID card device's design using the Mifare Classic NFC Tag with a storage capacity of 4Kbyte can provide a solution for modern smart class access. Mapping done on the Electronic Identity Card can store identity, security authentication, and user photos. Authentication was successfully performed with an average access time of 5.408 seconds using 8 test samples. The user's identity card still leaves 1,104 KB of space for other specific needs.

Keywords: Internet of Things,Electronic ID card authentication, Smart Class Room

I. INTRODUCTION

Technological developments have brought changes in various sectors, including academics [1] [2] [3]. The visible change's impact is the use of electronic devices to support the teaching and learning process. LCD Projector, Air Conditioner, and Smart LCD TV are generally found in modern classrooms [4] [5]. Access to electronic devices by multiple users results in higher user error rates resulting in shorter service life.

As one of the foundations for the 4.0 industrial revolution, the Internet of things technology encourages the level of connectivity and control of electronic devices. This technology can provide programmed electronic device connectivity services. With the support of the internet of things technology services, class support devices can be accessed centrally. This technology can improve flexibility, reduce costs, and optimize resources [6] [7].

Centralized device access requires a simple device authentication model. Able to provide fast access services and a good security system. It can be used as a single user identity for easy user tracking. A smart card is a suitable technology to support intelligent class concept services with centralized access to device services.

II. OVERVIEW

2.1. SCOPE OF RESEARCH

Smart card technology consists of an NFC tag and NFC Reader. This technology is widely circulating in the market and has been applied for various purposes, such as ticketing, public transportation purposes, or electronic payments. In this application, NIC technology is used for student identity cards as the basis for authentication for smart classroom development. An NFC card with ISO / IEC 1443A protocol standard has a storage capacity of 4K Kbyte. This type of NFC card consists of a manufacturing block, data block, value block, and trailer sector.

Internet of things technology is used to connect smart card authentication application devices, data acquisition, and database centers. Internet of things technology provides easy access to real-time database services.

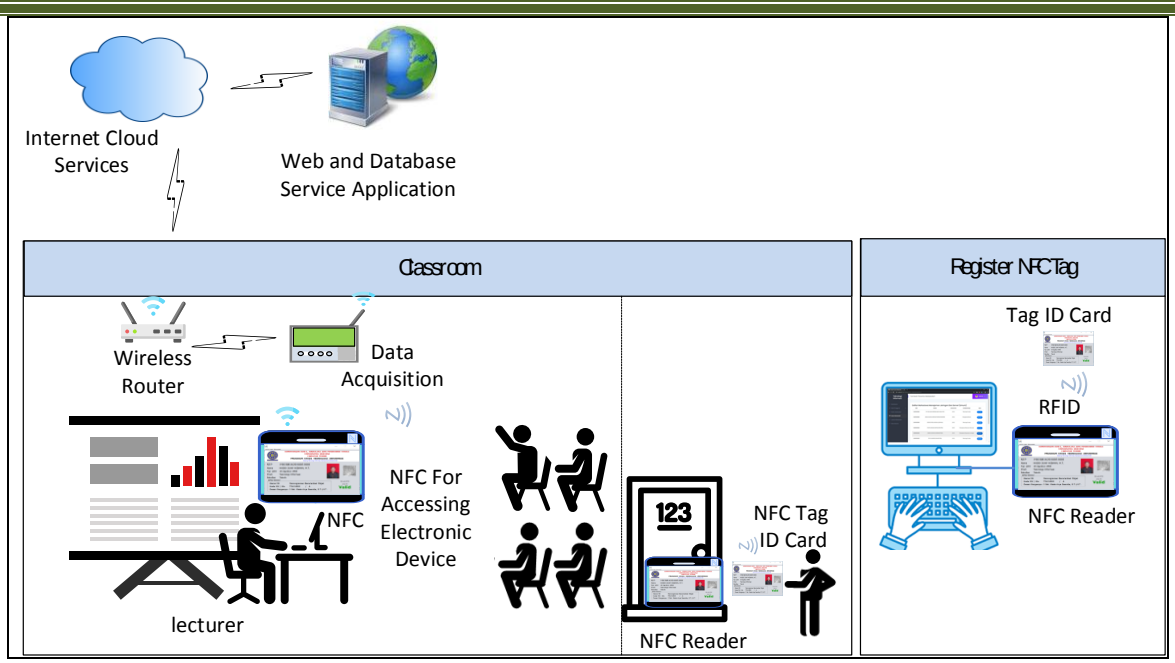

Fig 1. Authentication method for the smart class concept

2.2. SMART CARD

Smart card technology consists of an NFC tag and NFC Reader. This technology is widely circulating in the market and has been applied for various purposes, such as ticketing, public transportation purposes, or electronic payments. In this application, NIC technology is used for student identity cards as the basis for authentication for smart classroom development. An NFC card with ISO / IEC 1443A protocol standard has a storage capacity of 4K Kbyte. This type of NFC card consists of a manufacturing block, data block, value block, and trailer sector.

Sector	Block	Byte Number within a Block														Description
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
39	15	Key A						Access Bits				Key B						Sector Trailler 39
	14																	Data
	:																	:
	:																	:
	1																	:
	0																	Data
	:																	
	:																	
32	15	Key A						Access Bits				Key B						Sector Trailler 32
	14																	Data
	:																	:
	:																	:
	1																	:
	0																	Data
31	3	Key A						Access Bits				Key B						Sector Trailler 31
	2																	Data
	1																	Data
	0																	Data
	:																	
	:																	
0	3	Key A						Access Bits				Key B						Sector Trailler 31
	2																	Data
	1																	Data
	0	Manufacturer Data																Manufakturer Block

Fig 2. Memory structure Smart card ISO/IEC 14443 4K Byte

a. Block Manufacturer: block 0 in sector 0 contains a 16-byte hexadecimal value representing the manufacturer's data information. This block is rewritten or read-only protected.

b. Block Data: NFC tag with ISO / IEC 14443 standard protocol with a memory capacity of 4K Bytes with a total of 40 sectors. Each block consists of 16 bytes of data. Data in sector 0 can be filled in two blocks, namely, block one and block 2. Sector 1 to sector 31 can be filled in 3 data blocks. The last eight sectors can hold up to 15 data blocks. The total data storage capacity is up to 3440 Bytes.

c. Block Value: The block value allows for e-wallet use. In this block, read, write, increment, and decrement operators can be performed.

d. The sector trailer is the last block in each sector. The sector trailer consists of :

- secret keys A (required) and B (optional), which return a logic '0' during reading and operation.
- access conditions for each sector block, stored in 6 to 9 bytes.

If the key B is not required, the last 6 bytes of the sector snippet can be used as byte data.

III. SYSTEM DESIGN

3.1. AUTHENTICATIONMODEL

Authentication is an important part of the security system aspect. Authentication is a mechanism to prove that someone has rights or demands on something. Strong authentication techniques will sacrifice convenience and comfort in use. Proof of digital authentication can use auxiliary factors.

Auxiliary factors implemented in this system's design follow the general standards that are widely used in the use of electronic cards such as ATM cards. Two factors have been used to help correct that claim: What is owned? In this case, the electronic identity card (NFC tag) and What is known? The PIN is stored on the card. These two supporting factors for authentication are expected to provide services in terms of access time and access security that is carried out using electronic identity cards [8].

3.2. SYSTEM DIAGRAM BLOCS

The electronic identity card authentication device system application is designed using a system design architecture developed for the internet of things devices. This system design emphasizes scalability and application development for smart class concepts so that applications that have been developed can be reused or developed for other special needs.

The system design architecture consists of four layers: Device layer: the hardware used does not build the system. The Raspberry Pi model 3B + is a compact and compact embedded system device. They are supporting the internet of things technology services. Complete communication support and extensive software support. They are equipped with a user display for authentication devices using a color LCD with 720x480 pixels resolution with a touch layer as an input device. The NFC reader uses the ACR122U contactless model.

Table 1. Technical Specification

No	Unit	Specification
1	Main board	➢ Raspberry Pi 3B - Memory flash: 8GB, RAM 1GB ➢ Peripheral Board - USB - HDMI - Port data Communication ➢ Processor Quad Core 1.2GHz ➢ Voltage in DC 5 Volt
2	LCD Touch screen	➢ 720x480 pixel
3	Smart Card Reader	➢ ACR 122U

The internet network layer uses wireless and serial bus communication mods that connect the authentication device with other devices on the internal network. NFC reader device supports Universal serial bus (USB) communication.

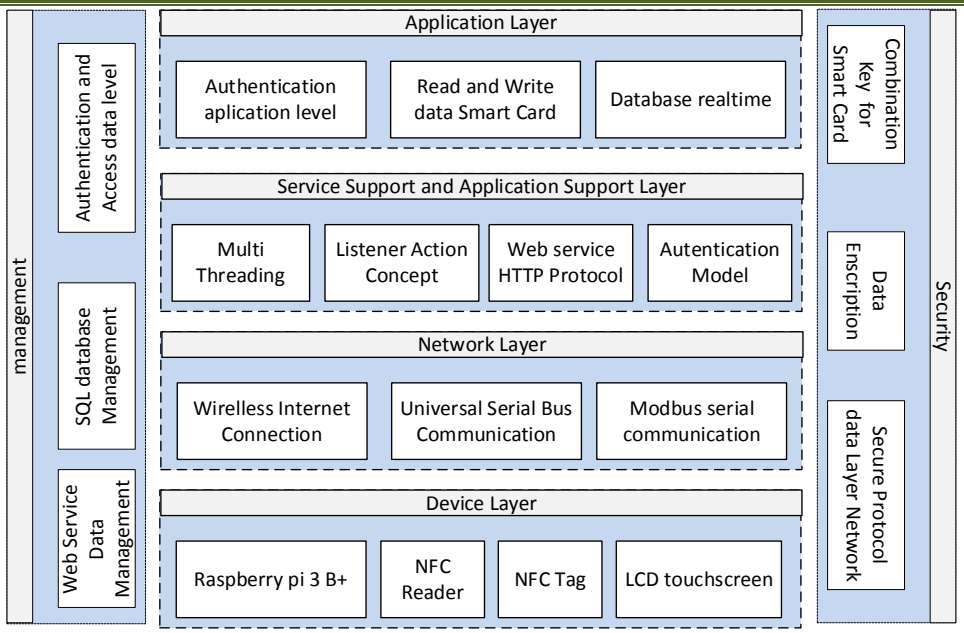

Fig 3. Architecture Design System

The service support and application support layers serve as application support services using a listener model to reduce device consumption. And in the application layer as an interface between the device and the end-user.

3.3. SOFTWARE DESIGN

Application software was developed using the Java programming language that supports the multi-threading technique and event listeners' concept. The application software runs on the Linux-based Raspbian pi operating system. Application development using the Java Netbeans IDE. The remote application technology makes it easy to develop and develop applications. Completing the application design can be developed more widely, and it is easier to update the application version.

Users in the application consist of two entities, users and administrative services and end-users. Service administration performs write action on NFC Tag, whereas end-user uses NFC Tag for class access and write action on PIN. Electronic student ID card issued by the administration. Each registered card is updated and synchronized in the database. So that electronic student identity cards can be used and recognized on any special reader devices installed.

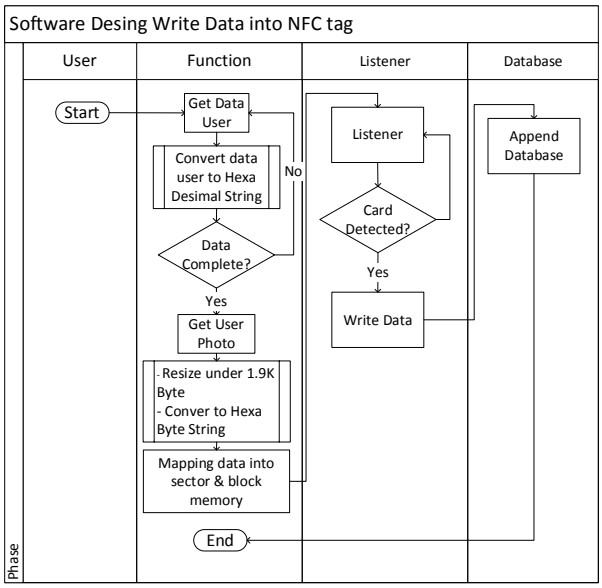

Fig 4. User admission Software Design

Users can change the default PIN on the student card using the built-in NFC reader application. The authentication model compares three data: the user inputted pins, the student card, and the database.

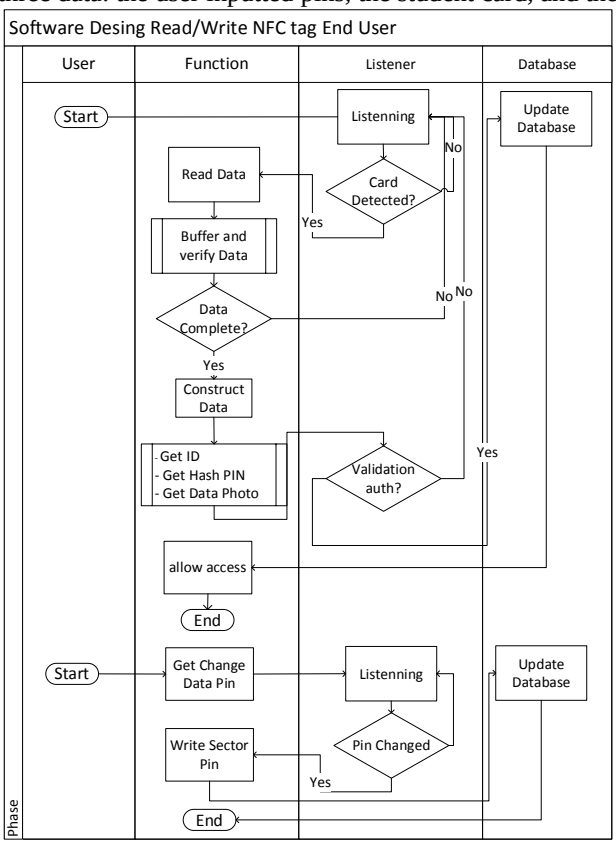

Fig 5. End User Chart

IV. RESULT AND TESTING

The results of software implementation show the success rate of system design. The use of remote technology in developing and developing systems makes it easy to develop and update software applications.

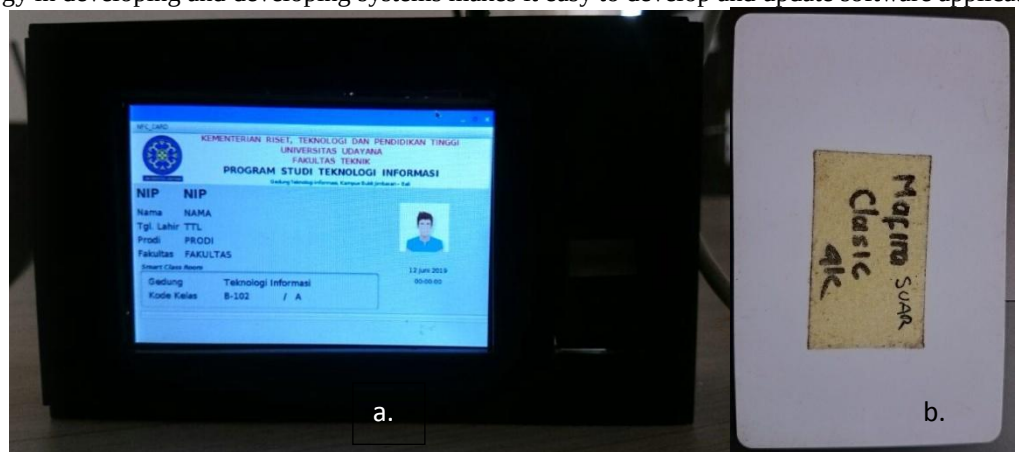

Fig 6. a) Authentication devise for the electronic identity card. b). NFC tag mafire classic 4K

The interface of the application software is made by prioritizing aesthetics, and the information conveyed. The preview contains important information stored on the electronic ID card. Admission fills in user identity data, including a photograph in accordance with the size set on the written form.

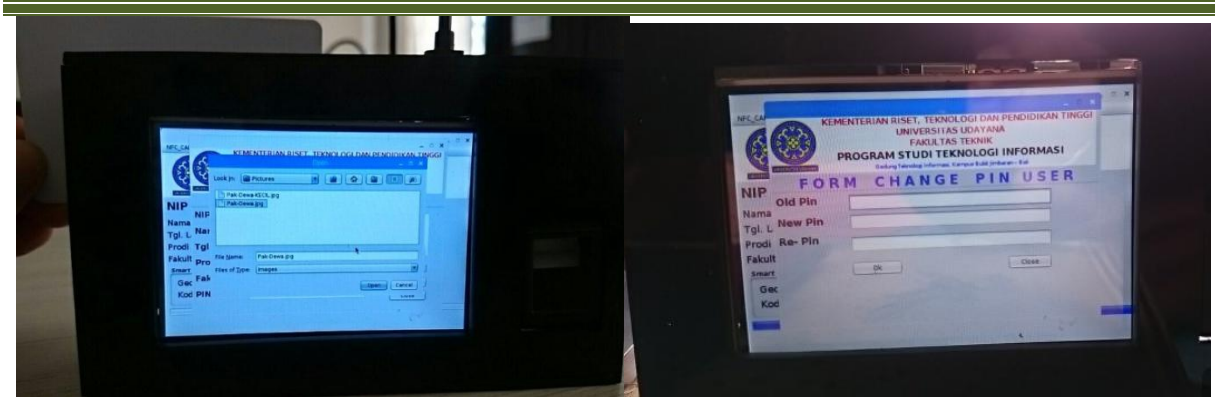

Fig 7.The writing process on NFC Tag.

After the NFC Tag writing process is complete, the user can change the default PIN provided by the admission via the change PIN menu. The user's new PIN data will be automatically stored on the user's identity card, synchronized in the user database. The following is a mapping table for user identities on the NFC tag of an electronic identity card.

Table 2. NFC TagMapping Memory

No	Identity	No .Sector	No. Blok	Max Data lenght	Max. Bit Data
1	Photo data lenght	0	2	16 byte	128 bit
2	ID	1	0 s/d 2	48 byte	384 bit
3	Name	2	0 s/d 2	48 byte	384 bit
4	Birthdate	3	0 s/d 2	48 byte	384 bit
5	Study program	4	0 s/d 2	48 byte	384 bit
6	Faculty	5	0 s/d 2	48 byte	384 bit
7	Hash PIN	6 – 7	0 s/d 2	96 byte	768 bit
8	Free Space	8 - 31	0 s/d 2	1104 byte	8832 bit
9	Photo	32 - 39	0 s/d 15	1920 byte	15360 bit

Smart class access is performed using a user authentication model. Authentication is done by comparing the PIN stored on the user's identity card with the pin's input known to the user and comparing it with the database stored in the user's data. Users can authenticate by bringing the electronic identity card closer to the NFC reader that runs the application program. Card validation is carried out and reads the card. The system asks the user to enter a PIN known to the user. If the hash of the PIN entered by the user does not match the results of the PIN stored on the electronic identity card and the database server, the user's access is denied.

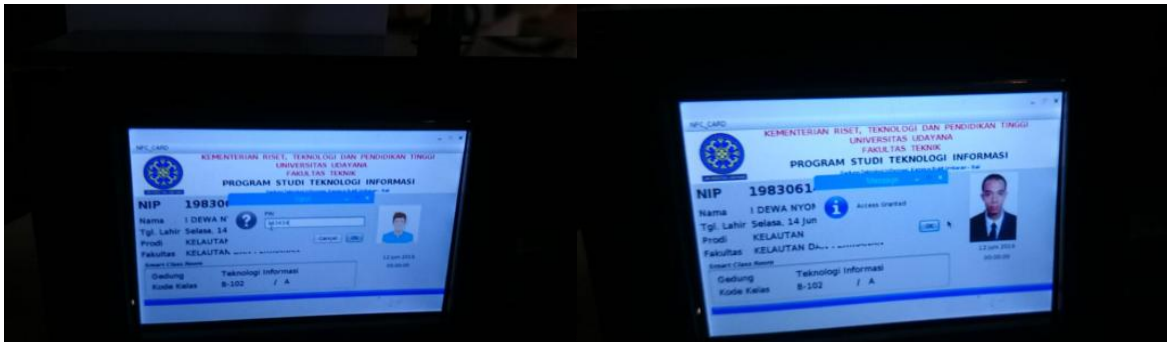

Fig 7. Electronic Identity Card Authentication Process.

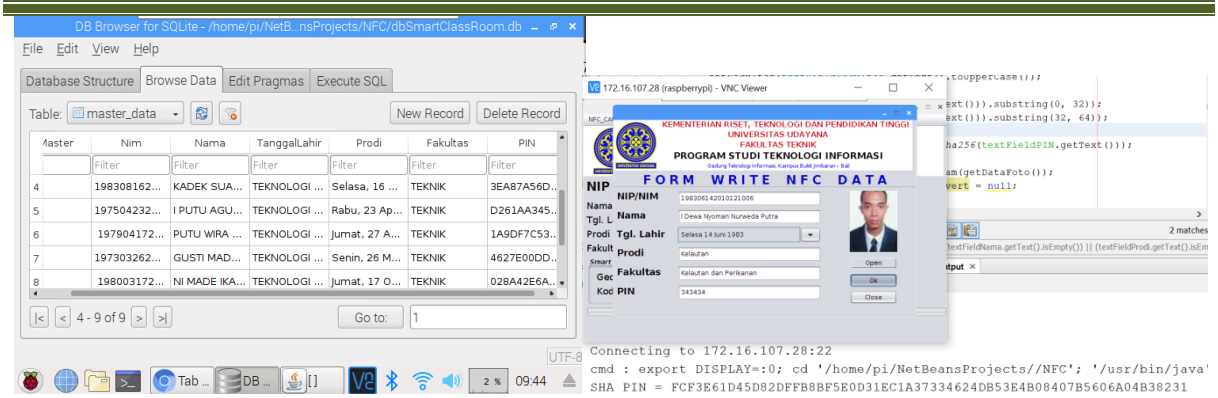

Fig 8. Database processing and user PIN authentication.

Table 3. Electronic ID card reading speed

No	ID	Read Time
1	19750227200031000	5477 mS
2	198308162018031000	5366 mS
3	197504232003121000	5421 mS
4	197904172008121000	5343 mS
5	197303262000031002	5471 mS
6	198003172009122000	5400 mS
7	197510242003121000	5374 mS
8	198306142010121006	5414 mS

From the tests carried out, the system has been able to synchronize the database between the database server and the NFC Reader device and validate the Sha PIN. The following is an example of the hash value of the entered PIN. It takes an average of 5,408 seconds to authenticate participants using an electronic identity card.

V. CONCLUSION

The results of tests that have been carried out using 8 test samples using the NFC card mafire classic 4Kbyte. The system design has met the requirements of the required authentication model with an average access speed of 5.408 seconds. The system still has an empty storage capacity of 1,104 K Bytes from the results of the electronic user identity card memory mapping.

Acknowledgements

Future research development can be continued by adding supporting factors in user biometric data stored on electronic ID cards.

REFERENCES

[1]. Maryam Bagheri ; Siavosh H. Movahed , in *2016 12th International Conference on Signal-Image Technology & Internet-Based Systems, (2016).* The Effect of the Internet of Things (IoT) on Education Business Model, pp. 435-441

[2]. R. Huang, Y. Hu, J. Yang, G. Xiao, The concept and characters of smart classroom(in Chinese). Open Education Research **18**(2), 22–27 (2012)

[3]. Finch G. (2018). Classroom design then and now. Diakses pada 10 Februari 2019 <https://www.viewsonic.com/library/education/classroom-design-trends-layout>

[4]. Li, S.C. Kong, G. Chen, Development and validation of the smart classroom inventory. Smart Learning Environments **2**(1) (2015). Diakses pada 10 Februari 2019 <https://doi.org/10.1186/s40561-015-0012-0>

[5]. J. MacLeod, H.H. Yang, S. Zhu, Y. Li, Understanding students' preferences toward the smart classroom learning environment: Development and validation of an instrument. Computers and Education **122**(March), 80–91 (2018).). Diakses pada 10 Februari 2019 <https://doi.org/10.1016/j.compedu.2018.03.015>

[6]. P.R. Temkar, M. Gupte, S. Kalgaonkar, Internet of things for smart classrooms. International Research Journal of Engineering and Technology **3**(7), 203–207 (2016)

[7]. S. Song, X. Zhong, H. Li, J. Du, F. Nie, in *2014 International Conference on Intelligent Environments, (2012)*. Smart classroom: From conceptualization to construction (2014), pp. 330–332

[8]. B U D I R A H A R D J O 2018, Keamanan Informasi . Diakses pada 28 Juli 2019 <http://budi.rahardjo.id/files/keamanan.pdf>

