Journal of Soft Computing Exploration
Homepage: https://shmpublisher.com/index.php/joscex
p-ISSN: 2746-7686
e-ISSN: 2746-0991

.

Application of the TAM model for assesing the acceptance of IoT technology in a residential security application

Rajib Ghaniy[1], Binanda Wicaksana[2], Fahmi Arnes[3], Laras Melati[4], Helena Septiana[5]
[1,2,3,4,5]Faculty of Informatics and Computer Science, Universitas Binaniaga Indonesia, Bogor, Indonesia

Article Info

Article history:

Received Dec 9, 2025
Revised Dec 22, 2025
Accepted Dec 29, 2025

Keywords:

IoT security
TAM
User acceptance
PLS SEM
Hypothesis

ABSTRACT

Housing is an area vulnerable to crime, especially if it is not supported by an adequate security system. Many housing complexes still rely on conventional security systems that only involve officers without technological support. Therefore, the application of technology, especially the Internet of Things (IoT), is needed to improve housing security systems. The success of a system is largely determined by the level of user acceptance, which can be measured using the Technology Acceptance Model (TAM). This study aims to measure user acceptance of an IoT-based housing security system using the TAM model. Data were obtained from 100 respondents and analyzed using the PLS-SEM method to test the research hypotheses. The results showed that four hypotheses had a significant relationship, namely the relationship between Subjective Norm (SN) and Perceived Usefulness (POU), Perceived Ease of Use (PEU) and POU, PEU and Attitude Toward Use (ATU), and POU and Behavioral Intention (BEI). Meanwhile, the other four hypotheses did not show a significant relationship.

Corresponding Author:

Fahmi Arnes,
Department of Information System,
Universitas Binaniaga Indonesia
Jl Pajajaran, No. 100 Bogor, Indonesia
Email: fahmi.arnes@unbin.ac.id
https://doi.org/10.52465/joscex.v6i4.629

1. INTRODUCTION

According to Law of the Republic of Indonesia Number 1 of 2011, housing is a collection of houses equipped with infrastructure, facilities, and public utilities that support the residential environment [1]. Security systems are an important facility in residential areas. In general, the security system of a housing complex relies on guard posts and security officers to monitor and control access. To maintain security, each housing complex usually implements its own standard operating procedures, which may vary from complex to complex, but all aim to maintain a safe residential environment [2].

Home security systems are one of the many areas where Internet of Things (IoT)-based digital technology is gaining ground. Physical devices such as smart locks, motion sensors, and cameras can be connected to the internet and controlled through a phone app. This technology makes it easier to monitor home conditions in real time, improving home security [3].

As of July 2024, theft remains the most common criminal offense, according to the National Crime Information Center (PUSIKNAS) [4]. The individual characteristics of the perpetrator and the surrounding environmental conditions both contribute to criminal behavior [5]. The high number of crimes indicates that the layout and accessibility of residential areas greatly influence their level of vulnerability. Places that lack adequate security systems and are located near main roads tend to be more attractive to criminals. Therefore, to carry out effective crime prevention, physical environmental planning such as spatial planning and architecture must be combined with better social supervision in the community [6].

Due to the popularity of the internet, the concept of the "internet of things" was first popularized by Kevin Ashton, who described a concept where physical objects could connect to the internet through sensors such as RFID and communicate with each other without human assistance [7].

Despite its many advantages, implementing Internet of Things (IoT)-based security applications still faces various challenges. Users continue to question the benefits of new technology compared to conventional security systems, particularly regarding its ability to prevent crime activity [8]. Furthermore, users are also concerned about privacy and data security, as the potential for data leaks can erode user trust [9].

In the context of Human Computer Interaction (HCI), user acceptance of an application is influenced by perceived usefulness and ease of use. Applications that are perceived as difficult to use can lead to user frustration, even if the features offered are actually useful [10]. Therefore, user experience is a crucial factor in the successful implementation of IoT-based digital security systems [11]. Developing a system requires precise analysis, and therefore, an appropriate development model is needed, appropriate to the type of system being developed. This refers to the System Development Life Cycle [12]. System development needs to be tested to determine the effectiveness of the developed system [13].

In this research, a web based and mobile based residential security system was developed. In the process, researchers used a prototype development model due to its flexibility, allowing developers to make allows developers to make changes or improvements to the system at any time. The system is integrated with internet of Things technology and then its usability is measured using the Technology Acceptance Model (TAM) measurement. These three things improve previous studies where the application of IoT was not integrated with web-based and mobile systems, and usability measurements used the Technology Acceptance Model (TAM).

To understand the acceptance of technology by users, the security system must be measured based on user perception. This study uses the Technology Acceptance Model (TAM), developed by Davis (1989). This model serves as a framework to predict the level of acceptance and use of technology by users through two main constructs: Perceived Usefulness (POU) and Perceived Ease of Use (PEU). Davis (1989) in attie say stated that According to recent research, POU and PEU are the main factors in predicting user attitudes and intentions towards Internet of Things-based technology [13], [14].

According to the description, this research will focus on evaluating an IoT-based residential security application by utilizing the TAM model to analyze user perceptions. The hypotheses to be tested in this study are as follows:

1) Subjective Norm (SN) has a positive effect on Perceived Usefulness (POU) of Mobile-Based Security Applications (H1)
2) Subjective Norm (SN) has a positive effect on Perceived Ease of Use (PEU) of Mobile-Based Security Applications (H2)
3) Perceived Ease of Use (PEU) has a positive effect on Perceived Usefulness (PU) of Mobile-Based Security Applications (H3)
4) Perceived Ease of Use (PEU) has a positive effect on Attitude Toward Using (ATU) Mobile-Based Security Applications (H4)
5) Perceived Usefulness (POU) has a positive effect on Attitude Toward Using (ATU) Mobile-Based Security Applications (H5)
6) Perceived Usefulness (POU) has a positive effect on Behavioral Intention (BEI) to Use Mobile-Based Security Applications (H6)
7) Attitude Toward Using (ATU) Mobile-Based Security Applications has a positive effect on Behavioral Intention (BEI) (H7)
8) Behavioral Intention (BEI) has a positive effect on Actual Use (ACU) of Mobile-Based Security Systems (H8)

The findings of this study are expected to contribute to application developers, residential managers, and academic literature related to digital technology acceptance.

2. METHOD

Research Design

This study employs a quantitative approach using a survey method. This approach was chosen because it is appropriate for examining the relationships among variables in the Technology Acceptance Model (TAM) through data collected from respondents in a structured manner [15].

Population and Sample

The population of this study consists of potential users of IoT-based residential security applications in urban housing environments. The sampling technique used is purposive sampling, with the following criteria:

a. Owning an Android or iOS smartphone
b. Having used or having experience with security applications or IoT devices.

The total sample consists of 100 respondents, which is the recommended number for analysis using Partial Least Square–Structural Equation Modeling (PLS-SEM) with latent constructs [15], [16].

Research Variables

The variables used refer to the TAM model [17], [18], namely:

a. *Perceived of Usefulness (POU)*
b. *Perceived Ease of Use (PEU)*
c. *Attitude Toward Using (ATU)*
d. *Subjective Norm (SN)*
e. *Behavioral Intention (BEI)*
f. *Actual Use (ACU)*

Research Instrument

Data were collected using a Likert scale questionnaire ranging from 1 to 5 (1 = strongly disagree, 5 = strongly agree). The following are the instruments adopted from TAM assessment items [19], [20]:

a. *Perceived of Usefulness (POU)*

To determine the extent to which the application provides real benefits in improving residential security.

Table 1. POU instrument items

No	Question/Statement	1	2	3	4	5
1.	This application helps me improve home security.					
2.	This application makes me feel more at ease regarding neighborhood security conditions.					
3.	This application allows me to monitor security more effectively.					
4.	Using this application increases efficiency in maintaining residential security.					

b. *Perceived Ease of Use (PEU)*

To determine the extent to which the application is easy to learn and operate.

Table 2. PEU instrument items

No	Question/Statement	1	2	3	4	5
1.	This security application is easy to learn.					
2.	I can use this application without assistance from others.					
3.	The features in this application are easy to understand.					
4.	Navigation within this application is clear and easy to use.					

c. *Attitude Toward Using (ATU)*

To determine users' attitudes or positive feelings toward using the application.

Table 3. ATU instrument items

No	Question/Statement	1	2	3	4	5
1.	I feel satisfied using this security application.					

.

2.	Using this application is beneficial.					
3.	I believe this application provides a positive experience.					
4.	I have a positive attitude toward using this security application.					

d. *Subjective Norm (SN)*

To determine the extent to which social influence (friends, family, neighborhood, local housing administrators) affects users' decisions to use the application.

Table 4. SN instrument items

No	Question/Statement	1	2	3	4	5
1.	People who are important to me recommend the use of this security application.					
2.	I feel encouraged to use this application because people around me also use it.					
3.	Support from neighborhood administrators (housing managers) influences my decision to use this application.					
4.	Opinions from friends/family make me more confident in using this security application.					

e. *Behavioral Intention (BEI)*

To determine the user's intention to continue using or recommending the application.

Table 5. BEI Instrument Items

No	Question/Statement	1	2	3	4	5
1.	I intend to continue using this security application in the future.					
2.	I will recommend this application to others.					
3.	I will use other features of this application if available.					
4.	I plan to use this application regularly.					

f. *Actual Use (ACU)*

To determine the user's actual behavior in using the application.

Table 6. ACU instrument items

No	Question/Statement	1	2	3	4	5
1.	I regularly use this security application.					
2.	I use this application whenever I monitor security conditions.					
3.	I frequently utilize the features available in this application.					
4.	This application has become part of my routine in maintaining home security.					

3. RESULTS AND DISCUSSIONS

This chapter explains the result and discussions of the research that has been conducted

A. Results

Before the system was developed and the IoT components were designed, a system analysis was carried out. The researcher analyzed what kind of system was needed and how the system would be used. The results of the system analysis included the system scenarios and a use case diagram [21].

This system is used by actors, and each actor has their own role in the system. The following is a list of actors and their roles in the system.

Table 7. System actor

Actor Name	Role
Super Admin	Actors who play a role in validating RT accounts
Neighborhood Leader (Ketua RT)	Is an actor who acts as a system administrator
Security officer	Is an actor whose job is to validate the presence/arrival of guests.
Resident	The actor who acts as the primary business actor, registering guests who will visit.
Guest	The actor who receives the QR code from the resident.

The system is initiated and started by the super admin actor, The Super Admin logs into the system using registered credentials. The primary responsibility of the Super Admin is to register RT Head accounts by entering required information such as National ID Number, full name, phone number, home address, term of office, and the official appointment letter issued by the authorized authority. Upon completing system operations, the Super Admin may log out.

The following is a system scenario run by the Neighbourhood Leader. The Neighbourhood Leader accesses the system using a registered username and password. The Neighbourhood Leader is responsible for managing resident data, including the Head of Family’s National ID Number, name, home address, phone number, number of occupants, list of occupants, and resident status (local resident or newcomer).

The system notifies the Neighbourhood Leader when residents submit information regarding planned guest visits or their temporary absence from home. The Neighbourhood Leader validates guest visit requests, particularly when the guest intends to stay for more than 24 hours. Additionally, the Neighbourhood Leader can view the list of residents, security officers, and guest visit records within a specified period. The Neighbourhood Leader may log out after completing required tasks.

Furthermore, The Security Officer logs into the system using registered credentials. The officer performs verification by scanning the QrCode presented by guests who have been registered by residents. The system also provides notifications of planned guest visits immediately after residents submit the data. The Security Officer is able to view the list of planned guest visits for the current day. The officer may log out after completing system-related duties.

Residents access the system using registered accounts. They can submit planned guest visit information, including guest name, the resident being visited, number of guests, type of vehicle, and duration of the visit. The system automatically generates a QrCode based on the submitted data, which residents can share with guests through messaging applications such as WhatsApp. The QrCode is temporary and remains valid according to the visit duration.

Residents may also provide information regarding travel plans or indicate unavailability for receiving guests. This allows security personnel to inform unexpected visitors about the resident’s absence or unavailability. Residents can view records of guest visits within a given time range and may log out after completing their actions.

Guests receive a QrCode from the resident who has registered a planned visit. Upon arrival, guests present the QrCode to the Security Officer for verification.

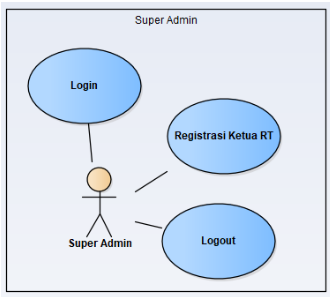

Figure 1. Usecase diagram super admin

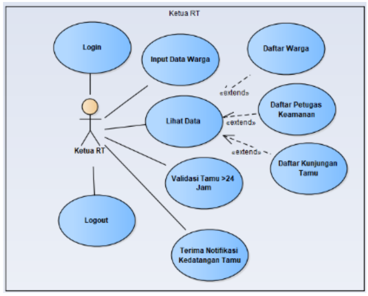

Figure 2. Usecase diagram RT head

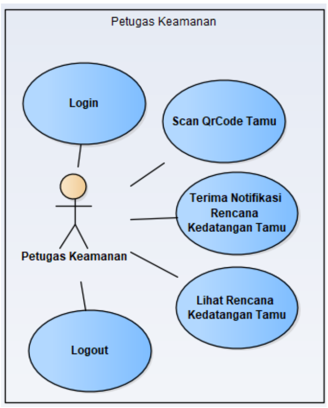

Figure 3. Usecase diagram security officer

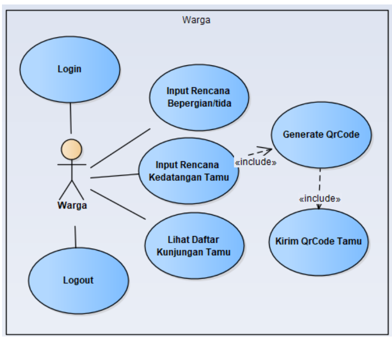

Figure 4. Usecase diagram resident

.

System Design

Figure 5. Guest registration form

Figure 5 describe that This form is used by residents to register guests who plan to visit their homes. Residents input detailed information based on the required fields.

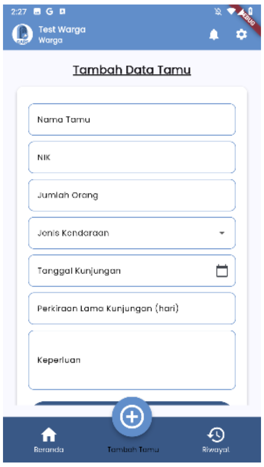

Figure 6. Guest data form fields

Figure 6 describe that This form is filled out by residents to register the guests who will be visiting.

Figure 7. QR code form

Figure 7 describe that This is the QR code generated from the guest data entered. Residents will share this QR code with the guests who plan to visit.

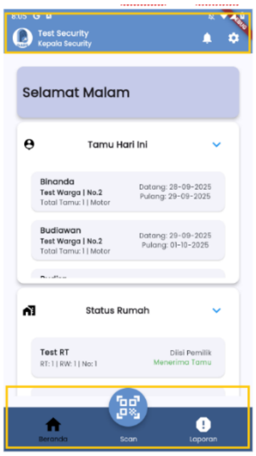

Figure 8. Security officer form

Figure 8 describe that This form contains the main feature: QR code scanning. Security officers will scan the QR code shown by the guest.

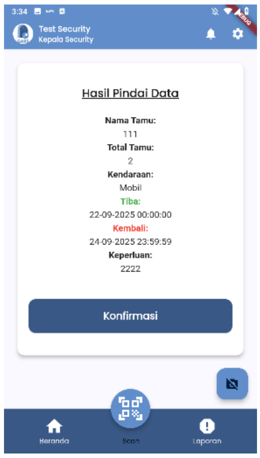

Figure 9. QR Code scan result form

After the guest's QR code is scanned by the security officer, the detailed contents of the QR code will appear, including the name, date and time of visit, and the vehicle used.

IoT Architect

In the developed prototype, supporting tools are required to represent a real-world scenario. The tools used in this prototype are described as presented in Table 8.

Table 8. Tools and sensors used in the prototype

No	Tool/Sensor	Description
1	ESP32 Dev Kit	**ESP32 Dev Kit** is a development board designed to simplify the use of the ESP32 microcontroller (System on a Chip/SoC) developed by Espressif Systems. This board typically includes all the essential components (such as a voltage regulator, USB-to-UART chip, and pin headers) so you can directly program and test the ESP32 chip without needing to build a complex supporting circuit [22].
2	Breadboard	**Breadboard** is a board used for assembling and testing electronic circuits temporarily without requiring any soldering [23].
3	Ultrasonic Sensor HC-SR04	**HC-SR04** is a widely used, low-cost ultrasonic distance sensor. It works based on sonar principles by using ultrasonic waves (sound waves above 20 kHz) to determine the distance of an object [24].

.

4	Direct Current Motor	**DC Motor** (Direct Current Motor) is an electric machine that converts direct current (DC) electrical energy into mechanical energy in the form of rotational motion [25].
5	L298N Motor Driver	**L298N Motor Driver** is an electronic module based on the L298N Dual H-Bridge Integrated Circuit (IC) [26], [27].
6	Limit Switch	**Limit Switch** is a type of mechanical sensor used to detect the presence, position, or movement boundary of an object or machine [28].
7	Jumper Wires	**Jumper Wires** are short conductive cables used to connect two points in an electronic circuit [29].
8	QR Code Scanner	**QR Code Scanner** is a hardware or software tool designed to read and decode information stored in a QR Code (Quick Response Code) [30].

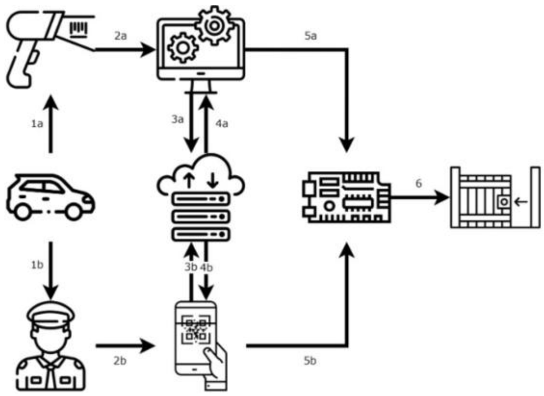

Figure 10. Workflow proses sistem

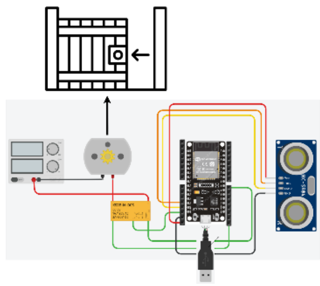
Figure 11. IoT prototype architect

B. Discussion

The prototype system was tested in front of the respondents. After observing how the system works and its performance results, the respondents were asked to provide an evaluation using a prepared questionnaire. The questionnaire refers to the research instrument. A total of 100 respondents successfully completed the questionnaire for this study. The majority of respondents were between 25–40 years old (60%), with diverse occupational backgrounds such as private employees, entrepreneurs, and university students. Nearly all respondents (92%) had previously used basic IoT-based applications, such as online CCTV or smart locks, making them relevant to the context of this research.

The following are the results of the questionnaire analysis processed using SEM-PLS.

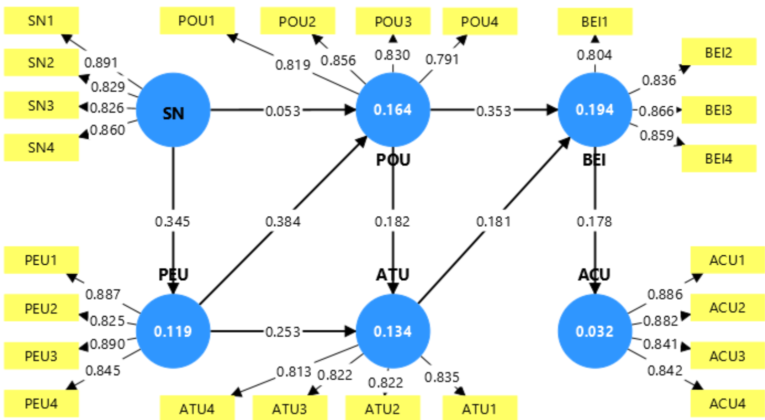

Figure 12. Outer loading model values

Figure 11 shows that the outer loading values obtained in the model are greater than 0.70; therefore, an indicator is considered valid [15], [31], Since all outer loading values are above 0.70, they are declared valid.

Table 10. Fit model

	Estimated Model
RSMR	0,074

NFI	0,773

In measuring the FIT model in PLS-SEM, the model fit used as a reference is by looking at the SRMR (Standardized Root Mean Square Residual) and NFI (Normed FIT Index) values.

Table 10 shows the results of the FIT test. In this study, the fit test used was the SRMR (Standardized Root Mean Square Residual) to determine the global FIT value and the NFI (Normed FIT Index). Based on the values in the table, the model fit evaluation shows that the SRMR value of 0.074 meets the model feasibility criteria (<0.08) [15]. The NFI value of 0.773 indicates an acceptable level of model fit in the PLS-SEM approach, thus the resulting model demonstrates an acceptable level of fit [15].

Table 11. Construct validity and reliability

	Cronbach Alpha	**rho_a**	**rho_c**	**AVE**
ATU	0,841	0,845	0,893	0,677
POU	0,844	0,856	0,894	0,679
BEI	0,863	0,866	0,907	0,708
SN	0,874	0,822	0,913	0,725
PEU	0,855	0,888	0,921	0,743
ACU	0,892	0,973	0,921	0,744

Based on the values of Cronbach's Alpha, Composite Reliability, and AVE shown, it can be concluded that all variables in the TAM model (ATU, POU, BEI, SN, PEU, ACU) have high reliability and excellent convergent validity [32]. This refers to the criteria Cronbach's Alpha and rho_c > 0.70 and AVE > 0.50 [15].

The hypothesis testing results using a significance threshold of $p < 0.05$ are explained in Table 12.

Table 12. Interpretation of hypothesis results

Relationship	**p-value**	**Decision**
H1: SN → POU	0,602	Not Significant
H2: SN → PEU	0,000	Significant
H3: PEU → POU	0,000	Significant
H4: PEU → ATU	0,023	Significant
H5: POU → ATU	0.108	Not Significant
H6: POU → BEI	0,000	Significant
H7: ATU → BEI	0,073	Not Significant (marginal, approaching significance)
H8: BEI → ACU	0,134	Not Significant

4. CONCLUSION

Based on the results and discussion presented, the conclusions of the tested hypotheses are as follows:

1. H1: Subjective Norm (SN) toward Perceived Usefulness (POU)
   With a p-value of 0.602, the result is not significant. This means that social influence is not strong enough to shape the perception that the application is useful. Users do not perceive the application's benefits based on social encouragement.
2. H2: Subjective Norm (SN) toward Perceived Ease of Use (PEU)
   With a p-value of 0.000, the result is significant, indicating that subjective norms have a strong positive influence on PEU. When the environment encourages application use, users perceive the application as easier to learn and use.
3. H3: Perceived Ease of Use (PEU) toward Perceived Usefulness (PU)
   With a p-value of 0.000, the result is significant, consistent with TAM theory. The easier the application is to use, the higher the perceived usefulness.
4. H4: Perceived Ease of Use (PEU) toward Attitude Toward Using (ATU)

With a p-value of 0.023, the result is significant. Ease of use contributes to forming a positive attitude toward the application.

5. H5: Perceived Usefulness (POU) toward Attitude Toward Using (ATU)
   With a p-value of 0.108, the result is not significant. Users do not yet perceive usefulness as the main factor in shaping a positive attitude.
6. H6: Perceived Usefulness (POU) toward Behavioral Intention (BEI)
   With a p-value of 0.000, the result is significant. Although usefulness does not shape attitude, it still drives users' intention to use the application.
7. H7: Attitude Toward Using (ATU) toward Behavioral Intention (BEI)
   With a p-value of 0.073, the result is not significant, though close to significant (borderline). A positive attitude is not yet strong enough to influence intention to use.
8. H8: Behavioral Intention (BEI) toward Actual Use (ACU)
   With a p-value of 0.134, the result is not significant. Intention has not yet influenced actual usage, possibly because the application is still in the trial phase or users are not familiar enough with it.

The measurement results for this hypothesis indicate that the perceived acceptance of a residential security system using Internet of Things technology indicates that Perceived Ease of Use (PEU) is a key variable in the acceptance of the security application. Subjective Norm (SN) was shown to have a significant effect on perceived ease of use, but not a direct effect on perceived usability. Furthermore, ease of use significantly influenced both perceived usefulness and user attitudes toward the application, in line with the Technology Acceptance Model (TAM) theory.

REFERENCES

[1] "Undang-undang Republik Indonesia Nomor 1 Tahun 2011 Tentang Perumahan dan Kawasan Permukiman," *Pemerintah Republik indonesia*, 2011. .

[2] R. Prabowo dan M. R. Lubis, "Tinjauan Hukum Pidana terhadap Kebijakan Keamanan di Perumahan Berdasarkan Peraturan Perumahan (Studi tentang Tanggung Jawab Pengelola dan Hak Warga)," *J. Begawan Huk.*, vol. 3, no. 2, 2025, doi: https://doi.org/10.62951/jbh.v3i2.133.

[3] G. Vardakis *et al.*, "Review of of Smart-Home Security Using Using the," *electronics*, vol. 13, no. 3343, 2024, doi: https://doi.org/10.3390/ electronics13163343.

[4] A. D. Ayuningtias, "Pencurian Jadi Kejahatan Paling Masif di Indonesia," *Goodstas*, 2024. https://goodstats.id/article/pencurian-jadi-aktivitas-kejahatan-paling-masif-di-indonesia-JbbSi.

[5] K. Rinaldi, D. Prayoga, dan H. Mianita, "Enviromental Criminology : Penerapan Defensible Space Sebagai Alternatif Pencegahan Kejahatan," *J. Mahupiki*, vol. 3, no. 1, 2022, doi: https://doi.org/10.51370/jhpk.v3i1.66.

[6] Z. Hidayanti dan M. Noviana, "Korelasi Akses Perumahan dan Kriminalitas di Perumahan Kota Samarinda," *J. Kreat.*, 2013, doi: https://doi.org/10.46964/jkdpia.v1i1.113.

[7] C. World, "The Internet of Things : An Overview," no. October, 2015.

[8] L. Y. Rock, F. P. Tajudeen, dan Y. W. Chung, "Usage and impact of the internet-of-things-based smart home technology: a quality-of-life perspective," *Springer Nat. Link*, vol. 23, hal. 345–364, 2022, doi: https://doi.org/10.1007/s10209-022-00937-0.

[9] J. M. Haney dan S. M. Furman, "NISTIR 8330 Research Report : User Perceptions of Smart Home Privacy and Security," *Comput. Secur. Resour. Cent.*, 2020, doi: https://doi.org/10.6028/NIST.IR.8330.

[10] C. Z. Id, Y. Qian, dan J. Kaner, "A study on smart home use intention of elderly consumers based on technology acceptance models," *PLoS One*, hal. 1–26, 2024, doi: 10.1371/journal.pone.0300574.

[11] I. P. Dewi dan R. Fikri, "Optimalisasi Keamanan Rumah dengan Implementasi Sistem Notifikasi Gerbang Cerdas Berbasis Internet of Things (IoT)," *J. Comput. Syst. Informatics*, vol. 4, no. 4, hal. 816–829, 2023, doi: 10.47065/josyc.v4i4.4004.

[12] O. E. Olorunshola dan F. N. Ogwueleka, "Review of System Development Life Cycle (SDLC) Models for Effective Application Delivery," *Springer Nat. Link*, hal. 281–289, 2021, doi: https://doi.org/10.1007/978-981-16-0739-4_28.

[13] M. Tool, "Using Extended Technology Acceptance Model to Assess the Adopt Intention of a Proposed IoT-Based Health," *Sensors*, vol. 16, no. 6092, 2022, doi: https://doi.org/10.3390/s22166092.

[14] E. Attié dan L. Meyer-Waarden, "The acceptance and usage of smart connected objects according to adoption stages: an enhanced technology acceptance model integrating the diffusion of innovation, uses and gratification and privacy calculus theories," *Technol. Forecast. Soc. Change*, vol. 176, 2022, doi: https://doi.org/10.1016/j.techfore.2022.121485.

[15] J. F. Hair, G. T. M. Hult, dan C. M. Ringle, *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*. 2022.

[16] M. Ali, T. Ramayah, dan J. Cheah, "PLS-SEM STATISTICAL PROGRAMS : A REVIEW," *J. Appl. Struct. Equ. Model.*, vol. 5, no. 1, 2021, doi: 10.47263/JASEM.5(1)06.

[17] E. S. Park dan M. S. Park, "applied sciences Factors of the Technology Acceptance Model for Construction IT," *Appl. Sci.*, 2020.

[18] W. R. Malatji, R. Van Eck, dan T. Zuva, “Understanding the usage , Modifications , Limitations and Criticisms of Technology Acceptance Model,” *Adv. Sci. Technol. Eng. Syst. J.*, vol. 5, no. 6, hal. 113–117, 2020, doi: https://dx.doi.org/10.25046/aj050612.

[19] K. A. Manan, “Developing Questionnaires for the Technology Acceptance Model (TAM): A Study on the Teachers ’ Acceptance of Using Online Education,” *J. Komun. Malaysian J. Commun.*, vol. 40, no. 3, hal. 529–553, 2024.

[20] V. A. C. Assessment, M. Biases, dan F. D. Davis, “A critical assessment of potential measurement biases in the technology acceptance model : three experiments,” *Int. J. Hum. Comput. Stud.*, vol. 45, no. 1, hal. 19–45, 1996, doi: 10.1006/ijhc.1996.0040.

[21] M. Ražinskas, B. Miliūnas, M. Jurgelaitis, dan L. Čeponienė, “Transforming Sketches of UML Use Case Diagrams to Models,” *IEEE Access*, 2024, doi: 10.1109/ACCESS.2024.3514455.

[22] E. W. Pratana dan A. Kiswantono, “ELECTRICAL ANALYSIS USING ESP-32 MODULE IN,” *J. Electr. Eng. Comput. Sci.*, vol. 7, no. 2, hal. 1273–1284, 2022, doi: https://doi.org/10.54732/jeecs.v7i2.21.

[23] K. A. Peppler, R. M. Sedas, dan N. Thompson, “Paper Circuits vs . Breadboards : Materializing Learners ’ Powerful Ideas Around Circuitry and Layout Design,” *J. Sci. Educ. Technol.*, vol. 32, no. 4, hal. 469–492, 2023, doi: 10.1007/s10956-023-10029-0.

[24] A. Agung, N. Gunawan, dan M. Sumadiyasa, “Water Level Detection System Based on Ultrasonic Sensors HC-SR04 and ESP8266-12 Modules with Telegram and Buzzer Communication Media,” *Instrum. Mes. Métrologie*, vol. 18, no. 3, hal. 305–309, 2019.

[25] A. Sikora, A. Zielonka, M. Woźniak, P. Orság, T. Mlčák, dan L. Hrabovský, “Fuzzy control system to improve the efficiency of the brushless direct current motor by correcting the control angle,” *Int. J. Electr. Power Energy Syst.*, vol. 169, 2025, doi: https://doi.org/10.1016/j.ijepes.2025.110762.

[26] P. Peerzada, W. H. Larik, dan A. A. Mahar, “DC Motor Speed Control Through Arduino and L298N Motor Driver Using PID Controller,” *Int. J. Electr. Eng. Emerg. Technol.*, vol. 04, no. 02, hal. 21–24, 2021.

[27] H. Technology, “L298N Dual H-Bridge Motor Driver.” www.handsontec.com.

[28] P. Megantoro, A. Latif, B. A. Pramudita, dan P. Vigneshwaran, “Automatic limit switch calibrator for control valve at steam turbine of a geothermal power plant,” *Bull. Electr. Eng. Informatics*, vol. 10, no. 3, hal. 1245–1251, 2021, doi: 10.11591/eei.v10i3.3031.

[29] M. Hemings, “What is a Jumper Wire?,” *SparkFun Education*, 2018. https://blog.sparkfuneducation.com/what-is-jumper-wire.

[30] A. S. Rafsanjani, N. B. Kamaruddin, H. M. Rusli, dan M. Dabbagh, “QsecR : Secure QR code Scanner According to a Novel Malicious URL Detection Framework,” *IEEE Access*, vol. PP, hal. 1, 2023, doi: 10.1109/ACCESS.2023.3291811.

[31] M. R. Rabbani, A. Lut, M. A. Ashraf, dan N. Nawaz, “Role of arti fi cial intelligence in moderating the innovative fi nancial process of the banking sector : a research based on structural equation modeling,” *Front. Environ. Sci.*, no. January, hal. 1–16, 2023, doi: 10.3389/fenvs.2022.978691.

[32] J. S. Simons *et al.*, “Response Rates, Reliability, and Convergent Validity in Experience Sampling Data,” *Assessment.*, vol. 32, no. 8, hal. 1195–1210, 2025, doi: 0.1177/10731911241300002.

.