Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control
Journal homepage: http://kinetik.umm.ac.id
ISSN: 2503-2267
Vol. 5, No. 1, February 2020, Pp. 37-44

Context-aware smart door lock with activity recognition using hierarchical hidden markov model

Aji Gautama Putrada*[1], Nur Ghaniaviyanto Ramadhan[2], Maman Abdurohman[3]
Telkom University, Bandung[1,2,3]

Article Info
Keywords:
Context-Aware, Smart Door Lock, Activity Recognition, Hierarchical Hidden Markov Model, Wireless Sensor Network

Article history:
Received 06 August 2019
Revised 17 November 2019
Accepted 06 December 2019
Published 06 February 2020

Cite:
Putrada, A., Ramadhan, N., & Abdurohman, M. (2020). Context-Aware Smart Door Lock with Activity Recognition using Hierarchical Hidden Markov Model. Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control, 5(1). doi:https://doi.org/10.22219/kinetik.v5i1.904

*Corresponding author.
Aji Gautama Putrada
E-mail address:
ajigps@telkomuniversity.ac.id

Abstract
Context-Aware Security demands a security system such as a Smart Door Lock to be flexible in determining security levels. The context can be in various forms; a person's activity in the house is one of them and is proposed in this research. Several learning methods, such as Naïve Bayes, have been used previously to provide context-aware security systems, using related attributes. However conventional learning methods cannot be implemented directly to a Context-Aware system if the attribute of the learning process is low level. In the proposed system, attributes are in forms of movement data obtained from a PIR Sensor Network. Movement data is considered low level because it is not related directly to the desired context, which is activity. To solve the problem, the research proposes a hierarchical learning method, namely Hierarchical Hidden Markov Model (HHMM). HHMM will first transform the movement data into activity data through the first hierarchy, hence obtaining high level attributes through Activity Recognition. The second hierarchy will determine the security level through the activity pattern. To prove the success rate of the proposed method a comparison is made between HHMM, Naïve Bayes, and HMM. Through experiments created in a limited area with real sensed activity, the results show that HHMM provides a higher F1-Measure than Naïve Bayes and HMM in determining the desired context in the proposed system. Besides that, the accuracies obtained respectively are 88% compared to 75% and 82%.

1. Introduction

Context-Aware Security can be said as flexible security [1]. Actually, users desire heavy security for unauthorized people and light security for authorized people. Here the security system is demanded to be more dynamic. To obtain the dynamic security, several contexts are usually trained through various machine learning methods. One of them is Naïve Bayes [2]. The problem with these kinds of machine learning methods is that the method only gives good results when working with high level attributes [3]. Usually to reach such high level attributes some data needs to undergo various processes such as feature extraction and normalization.

What if a system is working with low level attributes or attributes that are not directly related to a certain context. In an earlier system, the system proposes IP Camera, only providing camera footage for context switching [4]. In the proposed system, the system works with movement data obtained from a PIR Sensor Network [5]. If machine learning method such as Naïve Bayes is implemented to such data, the result would probably be garbage in garbage out [6]. To solve this problem a hierarchical learning approach is proposed. The learning approach first transforms low level attributes into high level attributes and then provides context-aware or dynamic security by learning from the high level attributes. Hence, it forms a hierarchy. The first hierarchy will transform movement data into activity data. Such transformation is usually called Activity Recognition [7]. Activity Recognition is a research term frequently implemented in the case of home automation also anomaly behavior in elderly living [8]. But it is seldom in context-aware security. Hence, the novelty of the proposed method.

This research proposes Hierarchical Hidden Markov Model (HHMM) as the method for Activity Recognition. HHMM is an extension of Hidden Markov Model (HMM) [9]. In HMM a single Hidden Layer is used to deduce input as output. The hierarchy in HHMM can add inference from the previous deduction.

To detect the movement of the user inside the house, a Passive Infrared (PIR) sensor network is deployed [10]. PIR is a sensor to detect human movement. Three PIR sensors will be used to detect movement across the house. It will be distributed inside the house in the living room, dining room, and kitchen. NodeMCU will be used to build the wireless sensor network. NodeMCU is a microcontroller with Wi-Fi capabilities.

To carry out three different levels of security, this research will implement a smart lock [11]. Multilevel Security will be carried out in forms of a combination of password, Wi-Fi connection, and device buttons implemented on the smart lock [12].

To prove the hypothesis that Hierarchical Learning will be suited for context-aware security, a comparison will be made between HHMM, Naïve Bayes, and HMM. Naïve Bayes and HMM will represent the non-hierarchical learning method. The highest learning performance between the three methods will be the conclusion of the research.

The first chapter of this paper is the explanation of the motivation of the researchers and the method applied. The second chapter will discuss about related researches. The third chapter provides scientific method elaboration and the proposed system design. The fourth chapter will consist of experiment documentation and analysis reports. The fifth and final chapter will be the research's conclusion and potential future work.

2. Research Method

A research was conducted in 2016 in the area of context-aware smart homes [13]. The scope of research was not limited to only smart lock but all appliances in homes. The research used fuzzy logic for the context-awareness, using multiple sensors such as PIR Sensor, Light Intensity Sensor, etc. The system controls door locks, AC, TV, lights, and others. Elaborate detail about the fuzzy design and detail of the experiment dimension were not provided in this paper.

In 2017 another research was conducted on context-aware smart homes [14]. This research provided an example scenario for the context such that the system will remind the user to lock the door based on the user's activity in the house. For user localization, the research uses multiple sensors, namely PIR sensor, door sensor, and microphones. For activity recognition the research uses a method called Markov Logic Networks. The research names pattern of activities as situation recognition. The research also provides an adequate performance measurement on the proposed method showing accepted level of accuracy.

In 2018, another research was conducted for context-aware accessibility for IoT environment in campus area [15]. This research states static accessibility method as the main problem of the research and intends to propose a dynamic accessibility method that appears seamless and robust, connoting that one's accessibility to a resource can change based on context. The additional context that influences the fluidity of the accessibility is environmental context. Though proposing interesting ideas, the research does not provide an adequate machine learning method that supports such dynamics.

Basically, a smart door lock is a conventional lock that is enhanced by the emerging capabilities of Internet of Things, meaning that a door lock can be opened by unlimited resource connected to the Internet, for example, Wi-Fi frequency, Bluetooth, RFID, and others. In 2017 there was a research that enhanced the capability of a smart door lock by implementing Block Chain [16]. Block Chain is a popular security method to secure online transaction benefiting from *cryptocurrency* or Bitcoin. Adapting the same technology, the main concept is the not any different, a chain of ledger is distributed between the rightful users of a smart door lock, anyone to access the home is to enter the ledger with the correct mechanism.

In the same year, another innovation was made related to smart door lock [17]. In this research, visible light is used as an additional authentication for the user to enter the house. The proposed system still maintained wireless connection, in this case, Bluetooth as the main authentication, but whilst communicating Bluetooth, there is also visible light transaction between the "key" and the "key hole". To add the accuracy of the authentication, the system adds a method called triple sampling. An accuracy performance test is provided in the research and returns sufficient results.

In 2019 a design was presented through a research on a smart door lock with face recognition [18]. The paper stated that the problem identification is that users frequently have problems opening the door lock because their hands are occupied, thus being the objective of using face recognition. It was a problem statement provided by user survey. The smart lock device uses a typical solenoid lock for the actuator. However, it adds another two relays for the lock controller. Adding two relays for the controller can provide levels in security. It also provides additional servo motor mechanics to open the door handle.

A well-known method for Activity Recognition is HMM. There are other methods, such as Cross-Validated Likelihood (CVL). A research was conducted to compare the two methods [19]. In this research, an amount of sensors with various types were distributed in two separate homes. The types of sensors were acoustic sensor, PIR Sensor, pressure matts and thermoelectric sensors. The experiment results of the research show that CVL has a better performance than HMM in predicting user activities.

Hierarchical HMM or HHMM has been used as method for Human Activity Recognition (HAR) in a research in 2019 [20]. This research used two homes for observation of the HAR experiment. The aim is to compare the effectiveness of the system in two different environments. Two types of sensors are used, namely motion sensor and door sensor. The research also introduces a term called "interrupted activity" where an activity can overlap with another activity.

2.1 System Design

Several types of sensors are needed to complement the home security system based on IoT with user Activity Recognition. From the design, the sensors needed are PIR, NodeMCU, and Buzzer. PIR sensor for detection of human

movements. Buzzers are used to provide alerts. Then NodeMCU is the main hardware for connecting PIR and Buzzer sensors. The smartphone here serves to receive notifications from NodeMCU containing information from the PIR sensor for movements that have been through the marshalling process, which will be sent directly to the smartphone in the form of notifications. Figure 1 is a block diagram of the PIR Sensor Network.

Figure 1 illustrates that one node of PIR Sensor Network consists of one PIR Sensor and one NodeMCU. The network is connected to the Internet via Wi-Fi. The data collected form the PIR Sensor is stored in Firebase, an open source cloud database. From data collection, the security level is determined and is sent to the Smart Door Lock system.

The PIR sensor does not capture movement, the security level becomes high and the door will be locked. Moreover, if the PIR sensor captures movement, the security level will be low and the door will not be locked. Other security levels are determined by activity. As seen in Table 1, the level of security in this system is divided into high security, medium security, and low security.

Table 1. Security-Level vs Activities

Security Level	Activities	Security Access
Low	Resting Watching TV	Button on the door
Medium	Eating Eating while watching TV	Smartphone Wi-Fi connection
High	Cooking Washing dishes	Password on smartphone

As seen in Figure 2, the PIR Sensor is placed in each room to get the accuracy of capturing human movements around the room. In the Living Room, a single PIR Sensor is placed in the middle. In the Family Room another PIR Sensor is placed in the middle. In the Dining Room one PIR Sensor is placed and in the Kitchen one PIR Sensor is placed.

The workflow of the system begins with the initialization of the PIR Sensor. Next the NodeMCU will check whether the PIR Sensor is on or not. Then if there is no movement of the PIR Sensor, it will be detected. If there is activity, the movement to the next state will be calculated. After the activity is derived, it will send a message to the smart lock system.

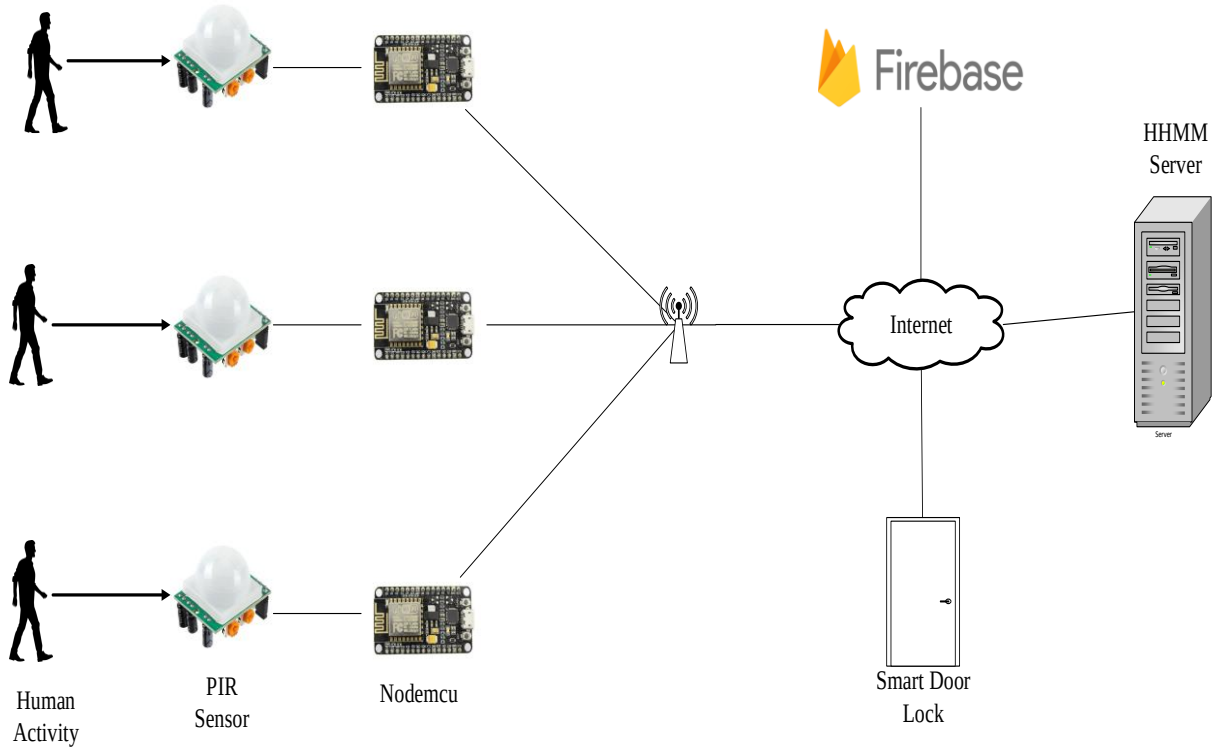

Figure 1. PIR Sensor Network

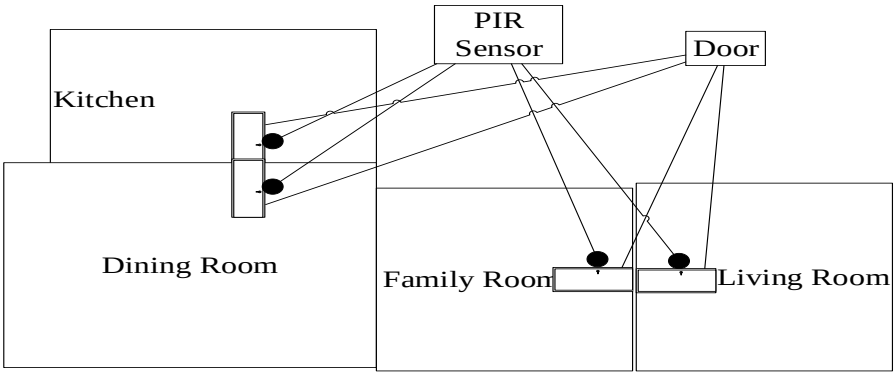

Figure 2. Sensor Placement

The output of the system determines the security level of the door lock. A smart lock device is built for this purpose. This smart lock device has the capacity to open and close a lock electrically and remotely with Wi-Fi capabilities by user smartphone.

The main controller is the NodeMCU. A button and a relay is attached directly to the NodeMCU. The NodeMCU has embedded Wi-Fi capabilities so it can connect directly to the Internet. The button is one of the three levels of security. The two other security levels are accessed via smartphone, hence, using the Internet connection. The Internet connection is also connected to the context-aware decision making system. The NodeMCU can control the state of the Solenoid Lock by sending digital pulse via the Relay. Control of the Lock is only determined by the allowed security level determined by the context-aware system.

2.2 Activity Recognition

2.2.1 Hierarchical Hidden Markov Model

HHMM is an extension of HMM that consists of two levels of hidden variables while the observation process is in the first level and user's hidden interests in the second level [21]. HMM is a method usually used for reinforcement learning in the area of temporal pattern recognition. HMM can be applied in areas such as speech recognition, handwriting recognition, and also can be applied in supply chain prediction [22]. The following is a detailed description of Figure 3 [21]. T is the hidden state of the first level, N is a number of states in the first level, R is the state of observation, M is a number of observation symbols (items), P is a two-level hidden state, K is a state number on two levels. Transitions between nodes are calculated as probabilities.

The definition of HMM based on [23] is a statistical model where a system modeled is assumed to be a markov process with conditions that cannot be directly observed. The fundamental difference from the markov chain with the HMM is that the markov chain is useful for calculating the probability of the sequence of events that can be observed, while the HMM is a development model that functions on problems that want to be known but cannot be observed. Problems that can be solved using HMM include evaluation, conclusions, and learning.

Figure 4 is the initial state of HHMM which is used with initial probability values, probabilities between zones to paths, and probabilities between lines. In this state, there are three zones and paths or activities have five activities.

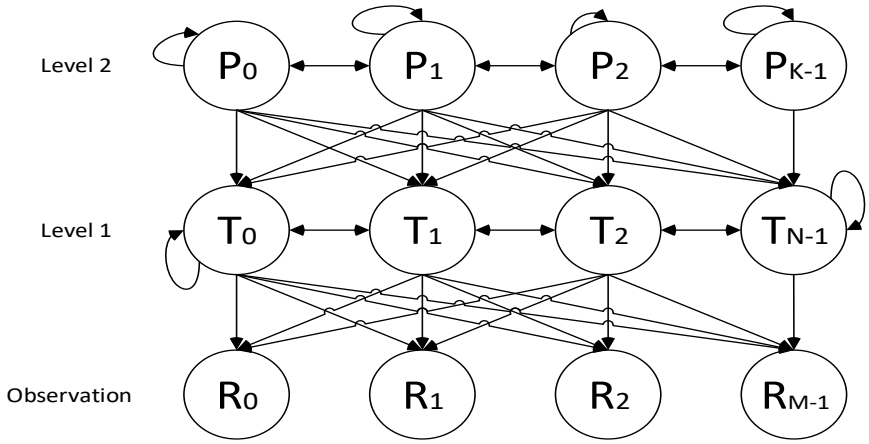

Figure 3. Hierarchical Hidden Markov Model

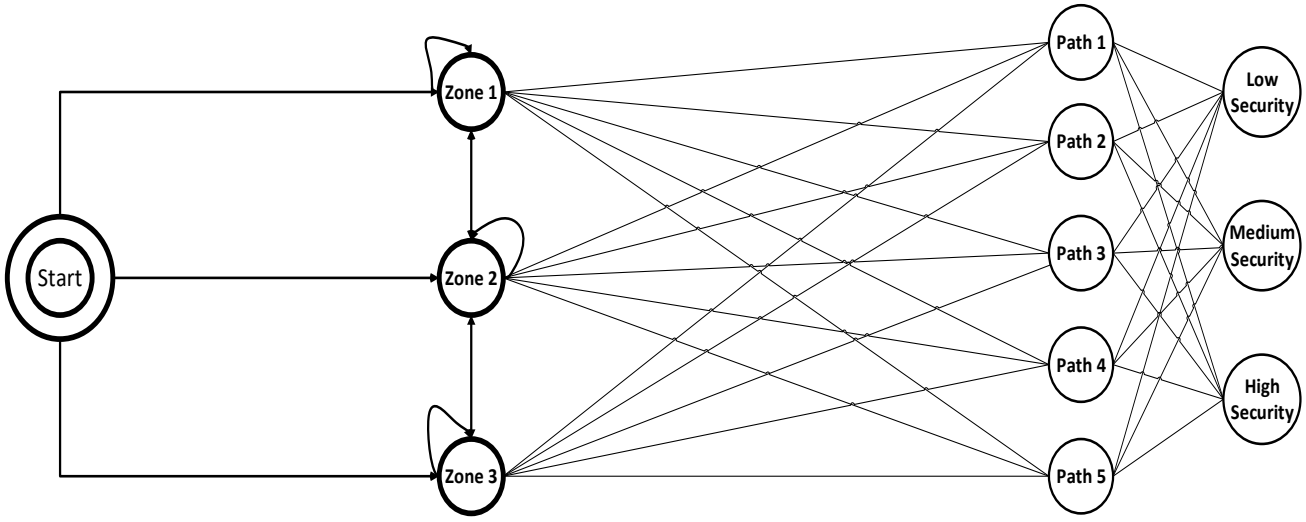

Figure 4. The HHMM Model

The initial probability taken from the value of each initial zone begins. Probability between zones to paths is taken from the value of the transfer of activities carried out during testing. Probability between lines is taken from the value of the transfer of activities carried out during testing. Zone probabilities to the path are taken from activities carried out in zone 1 through path 1, path 2, path 3, path 4, path 5 and etc.

2.2.2 Viterbi Algorithm

Viterbi algorithm is an algorithm to find the possibility of hidden status circuits (commonly called viterbi path) that are generated in a series of event observations, especially in the HHMM scope [24]. To find the best status series, q = (q(1), q(2)....q(r')), for the observational series O = (o(1), o(2).....o(r')), need to be defined as the following Equation 1. [24].

$$\delta t(i) = \max P[q(1), q(2) \ldots . q(t-1), q(t) = i, o1 \; q(1), q(2) \ldots q(t-1) \; o(2) \ldots . o(t) \mid \lambda] \quad (1)$$

δt(i) is the best circuit, that is, with the greatest probability, at time t where the calculation for the first observation t and ends at status i. For the value of q(1) is the best status in the first status while o(1) is the first series in the observation state. After the results are obtained, the max value will be taken as the optimal value. Complete steps to find the best path can be formulated as follow Equation 2 [24].

$$\delta 1(i) = \Pi i bi(o1), 1 \leq i \leq N \quad Ar(1) = 0. \quad (2)$$

In the initialization stage, the process of initialization will be carried out. Here's the detailed explanation, Π_i is the initial probability of each state, $b_i(o_1)$ is the probability output from the first element of state observation. 1 ≤ i ≥ N is the equation with i is the state to -i and N is the number of states, Ar' (1) is the transition probability value for the first time.

Next stage is recursive stage. It is a repetition process is carried out on the process itself with equation δt(i) = max [δt-1(i)aij]bj(ot) for 1 ≤ i ≤ N, where t-1(i) is a time series reduced by 1 with the state i, aij is the probability of displacement from state i to j while bj is a density probability state. The next stage is termination stage that maintain P* = max [δ_T(i)] for 1 ≤ i ≤ N. In the termination stage, the decision stage is carried out with P*, namely by taking the maximum value from each sequence of observations and generating the best path. Finally, is the step for determining the status path.

3. Results and Discussion

The results obtainesd in the system are in the form of an activity pattern that will be used to lock the door automatically. This system is tested using 3 nodes along with 3 PIR sensors which are spread to several points. Data obtained from the PIR sensor will be processed using the Viterbi algorithm in the HHMM so that it will produce the optimal path and the path will be used to lock the door.

1822 amount of movement data collection from all PIR sensors were stored through a span of 21 days. The data was collected particularly from 03.15 p.m. to 06.00 p.m. on each day. This data was divided into training data and testing data, 50% each.

The methodology is to determine activity from movement data in the first hierarchy of the HHMM. This is done with the testing data. The learning process is documented in a Zone to Zone Matrix. In the next hierarchy, patterns of activity are predicted to determine the level of security needed in the Context-Aware Smart Door Lock. The learning process of the pattern is documented in an Activity to Activity Matrix. Finally, with the testing data, the performance of the Context-Aware Smart Door Lock in determining the right security level is tested.

3.1 Activity Recognition Implementation

Table 2 is a matrix of each zone with a total of 3 zones, which have the chance of different displacements in each zone. Zone 1 is the kitchen, zone 2 is the dining room, and zone 3 is the living room.

Table 2. Zone to Zone Matrix

	Kitchen	Dining R.	Living R.
Kitchen	0.89	0.03	0.08
Dining R.	0.02	0.90	0.08
Living R.	0.10	0.10	0.80

Table 2 explains user movement probability through each zone in the house. Through this probability matrix, activity is recognized.

Table 3 is a matrix of the results of movement between activities or also called paths. The value generated from each transfer varies. Activity 1 is a cooking activity, activity 2 is eating activity, activity 3 is an activity of resting or watching television, activity 4 is an activity of washing dishes, activity 5 is an activity of eating while watching television.

Table 3 explains the probability of the exchange of user activity from one activity to the next. Through this probability matrix, prediction pattern is created thus determining the security level of the Smart Door Lock.

Table 3. Activity to Activity Matrix

	Cooking	Eating	Watching	Washing	Eat-Watch
Cooking	0.58	0.02	0.07	0.28	0.05
Eating	0.00	0.98	0.02	0.00	0.00
Watching	0.02	0.02	0.87	0.07	0.02
Washing	0.11	0.02	0.06	0.81	0.00
Eat-Watch	0.00	0.10	0.24	0.10	0.56

3.2 Context-Aware Smart Door Lock Performance

Testing data were used to measure the performance of the Context-Aware Smart Door Lock in determining the correct level of security. Four parameters are used for measuring the system performance as compassed in previous paper. They are recall, accuracy, precision and F-Measure. These parameters are calculated based on False Positive, True Positive, True Negative and False Negative value [25].

Table 4 presents the performance results of predictions produced by HHMM, which are the results of the door lock experiment. Low level is the security level of the door lock that uses the button. Medium level is the security level of the door lock that uses Wi-Fi. High level is the security level of the door lock that uses the password.

Table 4. Smart Door Lock Security Level Performance

	Accuracy	Recall	Precision	F1-Score
Low Level	84%	62%	73%	67%
Medium Level	88%	64%	78%	70%
High Level	91%	75%	90%	82%

There are two states: locked door and unlocked door. Locked door is considerd Positive. Unlocked door is considerd Negative. Also, there are two state types: Predicted and Actual. True Positive is the number of data where Predicted Locked door is also Actual Locked door. False Positive is the number of data where Predicted Locked door is actually Actual Unlocked door. False Negative is the number of data where Predicted Unlocked door is actually Actual Locked door. Finally, True Negative is the number of data where Predicted Unlocked door is also Actual Unlocked door.

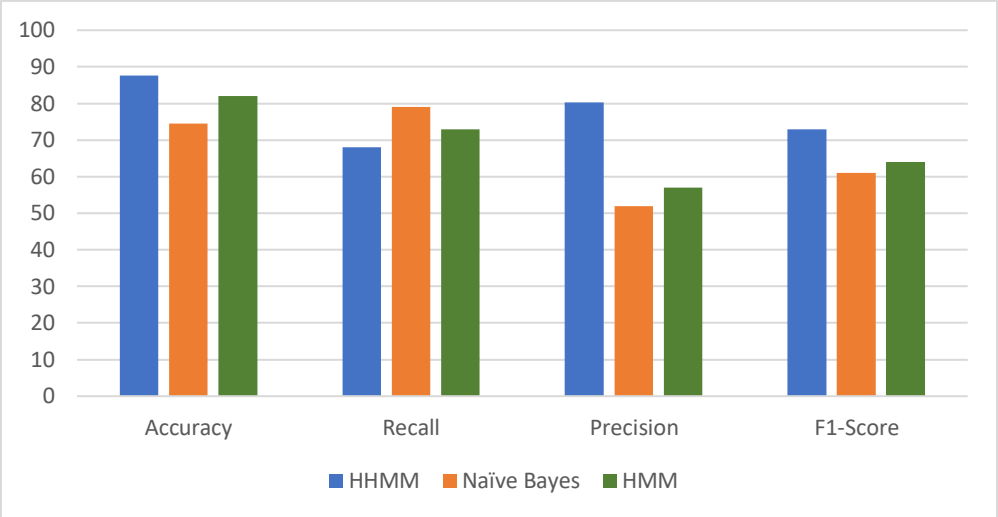

Figure 5. Comparison of HHMM, HMM and Naive Bayes Performance

Based on Table 4 the highest accuracy is High Level, which is 91%. The reason is the amount of data that is used to determine High Level Security is the largest. The time of data collection can be the reason. High Level Security is defined when the user is cooking. This is decided because, by observing Figure 2, it can be seen that activity in the kitchen is not in eye sight if standing in the area of the front door, hence higher security is required. High level uses a password through a Wi-Fi connected Smart Phone. This can also be an indication that Cooking, being a kitchen activity, is well separated from other activities. So, it is unlikely if that activity is mixed up with another activity.

For other performances, The F1-Score for Low Level, Medium Level, and High Level security respectively are 67%, 70%, and 82%. Increasing the amount of PIR Sensors, PIR Sensor placements that are more representative to activity, or sensor diversity can improve the results. Although for proof, further testing is required.

Next a comparison is made to measure the HHMM performance against some non-hierarchical learning methods. Here the comparison methods used are Naïve Bayes and HMM. The Naïve Bayes and HMM learning are done by training a collection of motion sensor data labeled with the desired context. Motion data is considered low level data because it does not directly relate to the desired context. After applying data to the methods, performance measurements are carried out. Figure 5 shows a comparison between the performance of Naïve Bayes, HMM and HHMM.

Recall is also called the True Positive Rate. Recall determines the success rate of a decision maker in detecting correct data from all correct data. In Figure 5, Naïve Bayes and HMM has higher Recall values than HHMM. But on the other hand it must be noted that HHMM precision is very low. Whereas Precision is Positive Predictive Value, meaning Naïve Bayes and HMM are less able to distinguish wrong data from correct data. When the HHMM Recall is lower and the Precision is higher, F1-Measure is used to determine which method provides better overall performance. F1-Measure is a harmonic average of Recall and Precision. As it can be seen in the chart, the F1-Measure of HHMM is higher than the others, so it can be concluded that HHMM has better overall performance than non-hierarchical methods such as HHMM and Naïve Bayes.

4. Conclusion

A system based on an Activity Recognition through a PIR Sensor Network and HHMM has been implemented. The HHMM uses user movement training data collection obtained from the PIR sensing for Activity Recognition. A zone to zone and activity to activity matrix is presented in the research as a model that shows the creation of the Activity Recognition. Testing data were used to measure the performance of the Context-Aware Smart Door Lock in determining the correct security level. The results show that High Level security provides the highest accuracy, which is 91%. The F1-Score for each level from Low to High respectively are 67%, 70%, and 82%. The novelty of this system is that it is hierarchical based, meaning that to reach a certain desired context the system goes through a number of learning levels. Here the first level is the movement data pattern and the second level is the activity pattern. The context is defined after the activity pattern has been predicted. To measure the success rate of this proposed system, it is compared with non-hierarchical learning methods, which are Naïve Bayes and HMM. It is proven that HHMM has better performance than other methods, providing an F1-Measure of 73% compared to Naïve Bayes' 61% and HMM's 64%. Though this system is a proof-of-concept that context-aware security can be generated through activity recognition, the supervised learning nature of the HHMM method causes this system to be un-adaptive; the context-aware results in the experimental environment of this research will not work in another home's environment. Hence, for future work, the

challenge is to create a context-aware locking system that is provided by unsupervised learning. Also, this system can be integrated into other smart home projects involving Activity Recognition. More sensors, like door sensors and pressure matts, can be used to add the accuracy in predicting activity.

References

[1] Covington, Michael J., et al. "A context-aware security architecture for emerging applications." 18th Annual Computer Security Applications Conference, 2002. Proceedings.. IEEE, 2002. https://doi.org/10.1109/CSAC.2002.1176296

[2] Hayashi, Eiji, et al. "CASA: context-aware scalable authentication." Proceedings of the Ninth Symposium on Usable Privacy and Security. ACM, 2013. https://doi.org/10.1145/2501604.2501607

[3] Li, Qiang, Qi Han, and Limin Sun. "Context-aware handoff on smartphones." 2013 IEEE 10th International Conference on Mobile Ad-Hoc and Sensor Systems. IEEE, 2013. https://doi.org/10.1109/MASS.2013.32

[4] Ashibani, Yosef, Dylan Kauling, and Qusay H. Mahmoud. "A context-aware authentication framework for smart homes." 2017 IEEE 30th Canadian Conference on Electrical and Computer Engineering (CCECE). IEEE, 2017. https://doi.org/10.1109/CCECE.2017.7946657

[5] Arora, Anish, et al. "Exscal: Elements of an extreme scale wireless sensor network." 11th IEEE International Conference on Embedded and Real-Time Computing Systems and Applications (RTCSA'05). IEEE, 2005. https://doi.org/10.1109/RTCSA.2005.47

[6] J. Saxe, "Garbage In , Garbage Out : How Purportedly Great Ml Models Can Be Screwed Up By Bad Data," 2017.

[7] Hidehiko Takara. "TK-3-4 IEC TC76 Standardization Trend on Safety of Optical Communication Systems (TK-3. International Standardization and Business Strategy, Meeting Committee Planning)." Proceedings of IEICE General Conference 2015.2 (2015).

[8] D. Tang, Y. Yoshihara, T. Obo, T. Takeda, J. Botzheim, and N. Kubota, "Evolution strategy for anomaly detection in daily life monitoring of elderly people," *2016 55th Annu. Conf. Soc. Instrum. Control Eng. Japan, SICE 2016*, Pp. 1376–1381, 2016. https://doi.org/10.1109/SICE.2016.7749272

[9] T. V Duong, H. H. Bui, D. Q. Phung, and S. Venkatesh, "Activity Recognition And Abnormality Detection With The Switching Hidden Semi-Markov Model Computer Vision And Pattern Recognition, 2005. Cvpr 2005," *IEEE Comput. Soc. Conf.*, Vol. 1, No. Cvpr, Pp. 20–25, 2005. https://doi.org/10.1109/CVPR.2005.61

[10] Z. Zhang, X. Gao, J. Biswas, and K. W. Jian, "Moving targets detection and localization in passive infrared sensor networks," *FUSION 2007 - 2007 10th Int. Conf. Inf. Fusion*, 2007. https://doi.org/10.1109/ICIF.2007.4408178

[11] A. Kassem, S. El Murr, G. Jamous, E. Saad, and M. Geagea, "A smart lock system using Wi-Fi security," *2016 3rd Int. Conf. Adv. Comput. Tools Eng. Appl. ACTEA 2016*, Pp. 222–225, 2016. https://doi.org/10.1109/ACTEA.2016.7560143

[12] N. Hashim, N. F. A. M. Azmi, F. Idris, and N. Rahim, "Smartphone activated door lock using wifi," Vol. 11, No. 5, Pp. 3309–3312, 2016.

[13] Patel, Arpit, and Tushar A. Champaneria. "Fuzzy logic based algorithm for Context Awareness in IoT for Smart home environment." 2016 IEEE Region 10 Conference (TENCON). IEEE, 2016. https://doi.org/10.1109/TENCON.2016.7848168

[14] P. Chahuara, F. Portet, and M. Vacher, "Context-aware decision making under uncertainty for voice-based control of smart home," *Expert Syst. Appl.*, Vol. 75, Pp. 63–79, 2017. https://doi.org/10.1016/j.eswa.2017.01.014

[15] A. Alkhresheh, K. Elgazzar, and H. S. Hassanein, "Context-aware Automatic Access Policy Specification for IoT Environments," *2018 14th Int. Wirel. Commun. Mob. Comput. Conf. IWCMC 2018*, Pp. 793–799, 2018. https://doi.org/10.1109/IWCMC.2018.8450323

[16] D. Han, H. Kim, and J. Jang, "Blockchain based smart door lock system," *Int. Conf. Inf. Commun. Technol. Converg. ICT Converg. Technol. Lead. Fourth Ind. Revolution, ICTC 2017*, Vol. 2017-Decem, Pp. 1165–1167, 2017. https://doi.org/10.1109/ICTC.2017.8190886

[17] S.-J. Song and H. Nam, "Visible Light Identification System for Smart Door Lock Application with Small Area Outdoor Interface," *Curr. Opt. Photonics*, Vol. 1, No. 2, Pp. 90–94, 2017. https://doi.org/10.3807/COPP.2017.1.2.090

[18] A. Ibro and A. R. Wong, "Face Recognition Door Lock," No. April, 2019.

[19] Alemdar, Hande. Human Activity Recognition With Wireless Sensor Networks Using Machine Learning. Diss. Bogaziçi University, 2015.

[20] Asghari, Parviz, Elnaz Soelimani, and Ehsan Nazerfard. "Online Human Activity Recognition Employing Hierarchical Hidden Markov Models." arXiv preprint arXiv:1903.04820 (2019).

[21] M. H. Aghdam, "Context-aware recommender systems using hierarchical hidden Markov model," *Physica A*, 2018. https://doi.org/10.1016/j.physa.2018.11.037

[22] M. Sharma and M. Singh, "Predictive Analysis of RFID Supply Chain Path Using Long Short Term Memory (LSTM): Recurrent Neural Networks," No. July, Pp. 66–77, 2018. https://doi.org/10.5815/ijwmt.2018.04.05

[23] Prasetyo, Muhammad Eko Budi. "The basic theory of the hidden markov model." Institut of Technology Bandung (2010).

[24] Irfani, Angela, Ratih Amelia, and Dyah Saptanti. "Viterbi Algorithm in Hidden Markov Models Method in Speech Recognition Technology." Computational Science and Engineering Laboratory. Department of Informatics Engineering, Institut of Technology Bandung (2006).

[25] R. Ghafoor *et al.*, "A performance comparison of machine learning classification approaches for robust activity of daily living recognition," *Artif. Intell. Rev.*, Vol. 52, No. 1, Pp. 357–379, 2019. https://doi.org/10.1007/s10462-018-9623-5