Data Science and Pattern Recognition ©2018 ISSN 2520-4165
Ubiquitous International Volume **2**, Number **2**, December **2018**

Characterizing Reliability Measure for Internet of Things by Markov Queue

Thi Thi Zin
University of Miyazaki, Miyazaki, Japan
thithi@cc.miyazaki-u.ac.jp

Pyke Tin
University of Miyazaki, Miyazaki, Japan
pyketin11@gmail.com

Hiromitsu Hama
Osaka City University, Osaka, Japan
hama@ado.osaka-cu.ac.jp

Abstract. *Today world is standing in the era of Internet of Things (IoT) where for almost every day we are connected in one way or another with one thing or another through the Internet creating the Internet of Things. Even we say that we are living in the world of Internet of Every Things. Having tremendous amount of potentials in application wise IoT becomes one of the most cutting edge technologies for our daily life living. Also, all most all of business, health care, academic institutions are harvesting the grains of the Internet of Things. So it is necessary to have reliable IoT devices to produce accurate information. In this paper, we proposed a method to characterize reliability measure of Internet of Things. The products of queuing theory such as the response times, queue lengths, delay times or waiting times and busy periods will be utilized for computing the reliability measures. In doing so, the Markov Chain properties will be employed to take the dependency of things into account in the IoT environments. Moreover, we will present some experimental results to confirm the proposed method.*
Keywords: Reliability Measure, Internet of Things, Markov Queue, Waiting Times, Access times and queue lengths

---

1. **Introduction.** We are now living in the era of Internet of Things. On the everyday news the buzzard word IoT is making front line topic. In very near future, all most all of things, human beings, animals, objects (things) are being and will be connected over the internet. In addition, the things in IoT are making actions and interactions among each other to transmit and receive information. In other words, IoT can be considered as a communication network in which devices or objects are connected by which information are received and transmitted. In such cases, reliability measures are important for making useful and reliable information. The Internet of Things is an ever growing connected network in which the connected things or devices are able to collect and send data to IoT platforms. For example, when you go to a hospital, once you pass the registration counter, the machine scan your registration card and make instructions to the unit where you may have medical treatment and the registration. How wonderful the IoT has made our life easy and lively. However, we have to remember that everything in IoT has a life expectancy as any other machines and they can make malfunctions due to interruption or

reach at the level expected life time which leads to the question of how much the things are reliable during their life time in IoT [1].

Recent surveys estimated that by the year 2020, 212 billion IoT devices will be connected and created the amount of data to reach at the level of 40 ZB [2-3]. This will make a challenging research for developing new technologies to cope with such amount of huge data and in some ways, it is an excellent opportunity for researchers to be able to show their innovative and creative ideas for real life problem solving to be benefit of human beings. Moreover, IoT based application areas are wide and huge, horizontal and vertical, various and gracious, social and global, community and security, e-health and e-wealth, and much more.

In addition, the Internet of Things can make our daily life smart in many ways; smart homes, smart cities, smart animal farming leading to smart every things. For those smarts, it is necessary to understand the fundamental concept of Internet of Things. Basically, the Internet of Things is made up of connected devices which send and receive data which are to be processed for decision making. Then the decisions and commands are sent to the application layers which are in the data centers or data followed by information queue linked between devices and application systems in IoT. The information queue has been widely used to control the huge amount of data created by the IoT. As the name suggests that the main function of information queue is to make scheduling messages for the IoT working smoothly [4].

As we can see in the architecture the IoT is composed of the IoT access network and the Internet protocol (IP) information queue link to IoT application networks. In the IoT access network, the devices generate information. The information is transmitted to an information queue. Then, the information queue makes decisions by data analysis and gives commands to actuators in the application network [5-9]. Therefore, IoT services are provided by monitoring data in the physical domain of the access network protocoled with an information queuing system for decision makings to application networks. Since IoT is a queuing system controlled, it involves information or messages coming and going out from the system and the way or patterns that are arriving and how they have been executed. The output of a queuing system is very much dependent on the inputs into the system. In the current system the inputs are highly correlated with how the IoT devices functioning well. If the IoT devices failed to produce proper or correct functions, the information produced by the queuing system will lead wrong decisions making process and service unreliability and service inefficiency. This kind of situation will effect to the whole network so that the continuously generated information become unreliable. Then, the information queue turns out distortional results through the data analysis. Furthermore, injecting additional data with wrong information can happen in the queue and the wrong decision will decrease the user experience for services. Therefore, we must be careful with the input data to have reliable and reputable sources [10]. In this concerns, the theory of queue system can investigate the message delays, traffic congestion and busy times. By studying those patterns, we can find the reliability measures for the Internet of Things.

In this paper, we shall propose a Markov Chain based queuing model to characterize the reliability measures of Internet of Things. In order to do so, we organize the rest of the paper composed of some related works in section 2, the overview of proposed system in section 3 and some illustrative experimental results in section 4 followed by conclusions in the final section.

2. **Some Related Work.** In order to advance the Internet of Things technology, many researchers have done some aspects of IoT devices reliability and system reliability measures [11-12]. Generally these advances are applicable to almost all types of smart environments such a smart homes, smart cities, health care systems, and deep learning processes [13]. However, in the task of designing IoT the greatest challenging is building a standard of reliability measure. For example, a simple device such as a temperature sensor to the Internet can be complex and expensive, especially if the device does not have its own processor. In addition, different types of IoT devices have various actions and interactions. Thus we need to collect and aggregate the data from a disparate set of IoT devices by a means of bridging devices with a range of processing capabilities and interfaces together in a consistent and reliable way [14]. The information queues offer an elegant means for simplifying the networking of "things" and messages through IoT gateways. As a consequence, the individual devices do not need to bear the complexity or cost of a high speed Internet interface in order to be connected. An IoT gateway is an intelligent component based on an IoT platform [15,16]. As state-of-the-art IoT gateways are designed to connect to mobile and wireless networks, they emphasize the provision of flexible connections among smart devices and a user's cloud to enable intelligent big data analysis and data-driven decision making.

The internet of things devices are mostly relied on the wireless communication which can affect data transmission among each other. It is also noted that wireless communication has a higher channel error than wired communication. These channel error can cause the transmitted information damage. Since the damaged data are not reliable and will not function properly, we should not include these information during the performing data analysis process. To detect the malfunctioning data or unusual data, an intrusion detection system can be exploited [17-18]. Generally the regular data in IoT are periodic. Event-driven data is different from normal data. Although the similarity between the event-driven data and the normal data is low, the event-driven data should not be blocked in the information queue system, but the existing methods do not process the event-driven data. The problem of IoT service performance modeling reference to the quality of service measure can be considered as response time, throughput and network utilization. In this context many authors have studied in the literature [19-21]. Among them some authors proposed and validated web application performance tool for the performance by obtaining the response time distribution of IoT cloud system modeled on a classic M/M/m network queues in which the both interarrival time of the information and processing times have has negative exponential probability density functions. Then the response time distribution is utilized to derive the optimal level of services which can perform the maximum number of workloads. The response time takes into account both the waiting time in the queue and the service time. However, the existing ways of data processing is not enough for providing reliable IoT services [11-12]. Therefore, in this paper, we propose a Markov dependent queuing system for information queue which can adaptively finds the suspicious data using the waiting times and expected queue length. It includes the valid data (i.e., the normal data and the event-driven data) and excludes the malfunctioning data in data analysis at the management level. In this context, the concept of reliability based on queue theory and Markov Chain has not been utilized conjunction with IoT devices and related Networks. The reliability theory is well developed in the field of Operation Research [22-23] and queue theory and Markov Chains are the most power tools in studying Stochastic Processes and their applications [24-25].

3. **Characteristics of Internet of Things Reliability Measure.** In order to characterize the reliability measure for Internet of Things, we propose a stochastic model in

which the fundamental concepts of queueing theory with the independent and identical distributed arrival process and exponential service time distribution are utilized. In particular the proposed system is described in FIGURE 1. And it contains three components: (i) input process (ii) processing messages and number of processors to produce decisions and commands, and (iii) the application layers process those decisions and commands to measure the reliability of the Internet of Things. While processing the messages, several random disturbances and interruptions may occur causing message damages, delays and getting no responses. From the queueing theory point of views we can compute the useful quantities such as time of delayed responses and their corresponding waiting time distributions and the number of messages left in the queue waiting to be processed. These computed quantities are used to characterize the reliability measures for internet of things. In order to realize the proposed system, we consider the IoT network as a multiple queueing system having multiple waiting lines consisting multiple servers or processors making first in first out queue discipline. Let the number of input channels or servers be N for i = 1, 2,..., N. The messages or information transmitted by the IoT devices will be flowed into those input channels and form a queue to be processed. In particular to make calculation simple we assume that the flow of information are distributed according to the mixture of gamma distribution described in equation (1).

In this context, the concept of reliability based on queue theory and Markov Chain has not been utilized conjunction with IoT devices and related Networks. The reliability theory is well developed in the field of Operation Research [22-23] and queue theory and Markov Chains are the most power tools in studying Stochastic Processes and their applications [24-25].

$$g(x, \alpha, \beta, \lambda) = \frac{\lambda x^{\lambda\alpha-1} exp(-\frac{x}{\beta}\lambda)}{\beta^{\lambda\alpha}\Gamma(\alpha)} \quad (1)$$

where $x,\ \alpha, \beta, \lambda > 0$

with mean $E(x) = \frac{\beta\Gamma(\frac{\lambda\alpha+1}{\lambda})}{\Gamma(\alpha)}$.

Where α, $\beta > 0$ and x is a positive real number. The parameter α is called the shape parameter and is called the rate parameter (or inverse scale parameter).

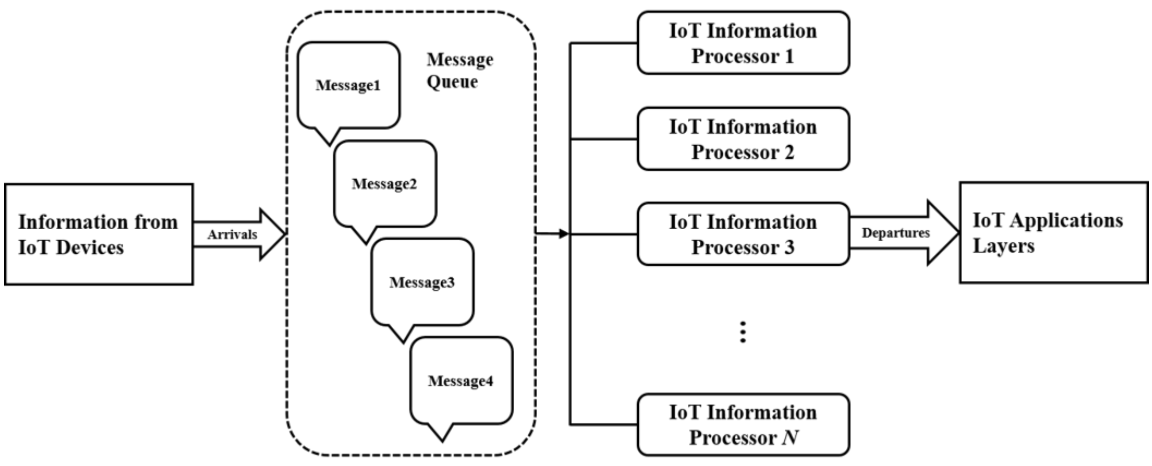

FIGURE 1. Architecture of IoT Message Queue

Each processing unit in message queue has the same service rate and is equal to μ, this is $\mu = \mu_i, i = 1, 2, ..., N$. Connecting servers in the message queue are fed with gamma arrival and service distributions. So α/β is the feeding distribution for the customers leaving the entering server.

The formulas for determining the operating characteristics for the multiple server queuing model are based on the same assumptions as the single-server model-Poisson arrival rate, exponential service times, infinite waiting space and queue length, and FIFO queue discipline are derived as follows. In this terminology, let the number of population (here in IoT the number of packets of messages) in the system (message queue) be n, then we can define n, then we can define λ_n and μ_n as the arrival and service rates depend on the number in the system. The probability that there are no customers in the system (all servers are idle) is

$$P_0 = \frac{1}{[\sum_{n=0}^{S-1} \frac{1}{n!}(\frac{\lambda}{\mu})n] + \frac{1}{S!}(\frac{\lambda}{\mu})^S\{\frac{S\mu}{S\mu-\lambda}\}} \tag{2}$$

The probability of n customers in the queuing system is

$$P_n = \begin{cases} \frac{1}{S!S^{n-s}(\frac{\lambda}{\mu})^n P_0}, & n > S \\ \frac{1}{n!}(\frac{\lambda}{\mu})^n P_0, & n \leq S \end{cases} \tag{3}$$

The probability that a new message arriving in the system must wait for process (i.e., the probability that all the processors are busy) is

$$P_w = \frac{1}{S!}(\frac{\lambda}{\mu})^S\{\frac{S\mu}{S\mu-\lambda}\}P_0 \tag{4}$$

Similarly, the average number of messages waiting for processing is given by

$$L = \frac{\lambda\mu(\frac{\lambda}{\mu})^S}{(S-1)!\{S\mu-\lambda\}^2}P_0 + (\frac{\lambda}{\mu}) \tag{5}$$

The expression in (4) is also known as Erlang's delay formula. By using this formula, we can compute the waiting time distribution as follows.

$$P(W > t) = \frac{1}{S!}(\frac{\lambda}{\mu})^S\{\frac{S\mu}{S\mu-\lambda}\}P_0 e^{-\{\frac{S\mu}{S\mu-\lambda}\}t} \tag{6}$$

This probability can be considered as IoT device failure if the t is big enough. Therefore, we define the reliability function $R(t) = 1 - Pr(W > t)$. By using equation (6), we finally obtain the reliability function for each server in IoT message queue becomes as described in equation (7).

$$R(t) = 1 - \frac{1}{S!}(\frac{\lambda}{\mu})^S\{\frac{S\mu}{S\mu-\lambda}\}P_0 e^{-\{\frac{S\mu}{S\mu-\lambda}\}t} \tag{7}$$

That can be interpreted as the probability of a sever functioning until time t. Thus the probability of the whole IoT massage queue to have reliable informing processing can be determined by using a threshold value say α such that $P = 1$ -$[1 - R(t)]^N \geq \alpha$, otherwise the IoT system is not reliable.

4. **Some Simulated Experimental Results.** In this section, we shall illustrate the proposed method of reliability measure in IoT environments. We have understood that the main theme of an information reliability is to determine whether we can use the information which can answer to our research or real world problems. Sometimes, to perform the assessments of IoT, only a certain potion of the information may be necessary and relevant to our research problems.

We may need to assess only a few elements of a database or we may need to as-sess many variables in various modules of a data collection system. The way we deal with the assessment is to be determined how much we expect for the importance, reliability and reputability of the data to be included in our outputs. The relationship between the correlation of the things in IoT and the number quality services available are also discussed by using numerical methods. Although most of existing reliability computing algorithms are subjects of iterations demanding the rate of convergence, the proposed methods need only one time computation. So it is not necessary to worry about the convergence problems. The proposed method has taken care of convergence concepts implicitly. This merits to reducing the computation time for calculating IoT service and device reliability measures. The reliability distribution patterns are calculated using queuing theory concept proposed in section 3. In this aspect, it is shown that how much one can vary the values of the traffic intensity and the maximum correlation one can use is presented. In which, the probability of time duration where the IoT devices can perform without failure has been taken into account.

In TABLE 1., for small value of number of IoT things the results of reliability distribution are presented for large correlation value and small size of demands. In TABLE 2, the results of reliability distribution for minimum allowable correlation and the maximum size of inputs are shown. These results are also shown in graph forms in FIGURE 2. and FIGURE 3. Again, through the varying the parameters thresholds, inputs and the number of devices it is observed that the threshold value is range from 0.7 to 0.9 for large value of N, the total number of IoT things within the datasets.

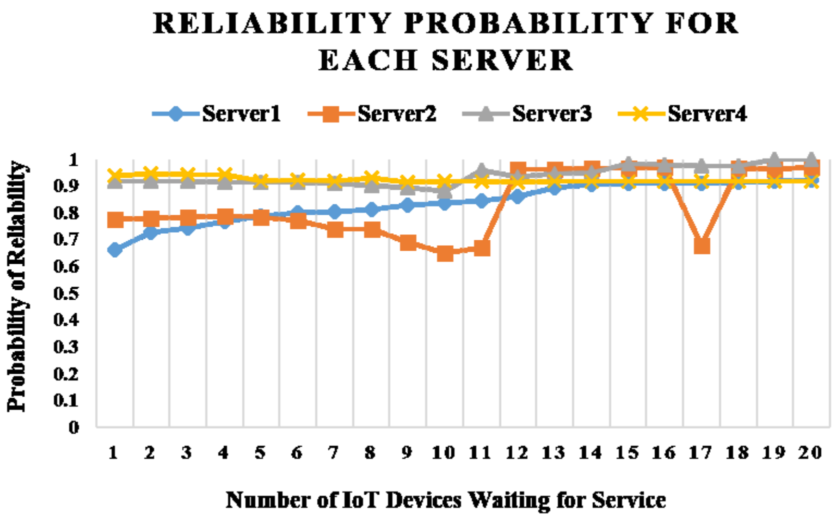

FIGURE 2. Distribution of Reliability and Expected Waiting Time for Service N=20

5. **Conclusions.** In this paper, we had presented a new look into the reliability measuring system for the Internet of Things environments. We observed that the approach based

TABLE 1. Distribution of Reliability and Expected Waiting Time for Service N=20

N	Probability of Reliability	Expected Waiting Time
1	0.938	0.6579
2	0.946	0.679
3	0.9394	0.7034
4	0.941	0.6885
5	0.918	0.8219
6	0.919	0.8012
7	0.9164	0.7942
8	0.9282	0.7955
9	0.914	0.8571
10	0.915	0.8564
11	0.9176	0.8504
12	0.9142	0.8422
13	0.918	0.8289
14	0.918	0.8217
15	0.9172	0.8383
16	0.9176	0.8304
17	0.91712	0.8333
18	0.91712	0.8333
19	0.91712	0.8333
20	0.91712	0.8333

TABLE 2. Reliability Counts for Variable Thresholds

N/α	0.7	0.8	0.9	0.95
1	3	2	2	0
2	4	2	2	1
3	4	2	2	0
4	4	2	2	0
5	4	2	2	0
6	4	2	2	0
7	4	3	2	0
8	3	3	2	0
9	3	3	1	0
10	3	3	2	0
11	4	4	3	1
12	4	4	4	2
13	4	4	4	2
14	4	4	4	2
15	4	4	4	2
16	3	3	3	1
17	3	3	3	1
18	4	4	4	2
19	4	4	4	2
20	4	4	4	2

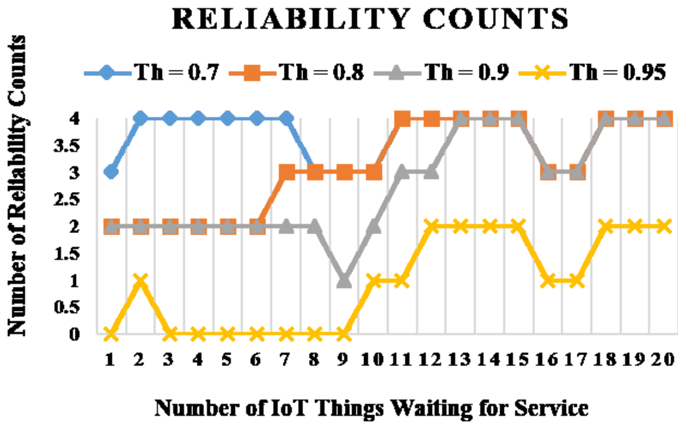

FIGURE 3. Reliability Counts for Variable Threshold

on the Markov queuing theory seems to be efficient and promising. Although we have employed the synthetic data for illustration, we will use real world datasets in future.

6. **Acknowledgment.** This work was supported in part by SCOPE: Strategic Information and Communications R&D Promotion Program (Grant No. 172310006).

REFERENCES

[1] R. Lu, X. Li, X. Liang, X. Shen, and X. Lin, "GRS: The green, reliability, and security of emerging machine to machine communications," *IEEE Communications Magazine*, vol. 49(4), pp. 28–35, 2011.
[2] J. Gantz and D. Reinsel, "The digital universe in 2020: Big data, bigger digital shadows, and biggest growth in the far east," *IDC iView: IDC Analyze the Future*, vol. 2007, pp. 1–16, 2012.
[3] M. Diaz, C. Martín and B. Rubio, "State-of-the-art, challenges, and open issues in the integration of Internet of Things and cloud computing," *Journal of Network and Computer Applications*, vol. 67, pp. 99–117, 2016.
[4] R. Buyya and A. V. Dastjerdi, "Internet of Things: Principles and Paradigms," *Elsevier*, 2013.
[5] S. Kim and W. Na, "Safe data transmission architecture based on cloud for Internet of Things," *Wireless Personal Communications*, vol. 86(1), pp. 287–300, 2016.
[6] Y. Kang, "New approach to the platform for the application development on the Internet of Things environment," *Journal of Platform Technology*, vol. 3(1), pp. 21–27, 2016.
[7] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future generation computer systems*, vol. 29(7), pp. 1645–1660, 2013.
[8] S. Mahamure, P. N. Railkar, and P. N. Mahalle, "Communication protocol and queuing theory-based modelling for the Internet of Things," *Journal of ICT Standardization*, vol. 3(2), pp. 157–176, 2015.
[9] D. Y. Kim, Y. S. Jeong, and S. Kim, "Data-filtering system to avoid total data distortion in IoT networking," *Symmetry*, vol. 9(1), article 16, J2017.
[10] K. Chelli, "Security issues in wireless sensor networks: attacks and countermeasures," *World Congress on Engineering*, vol. 1, pp. 1–3, 2015.
[11] L. Wei, M. Yong, T. Y. Wei, L. Dong, and H. Bin "Iot system reliability testing and evaluate technology," *Software*, 4, pp. 001, 2012.
[12] L. Li, Z. Jin, G. Li, L. Zheng, and Q. Wei, "Modeling and analyzing the reliability and cost of service composition in the IoT: A probabilistic approach," *IEEE International Conference on Web Services*, pp. 584–591, 2012.
[13] B. Kang and H. Choo, "A deep-learning-based emergency alert system," *ICT Express*, vol. 2(2), pp. 67–70, 2016.
[14] B. Kang, N. Kwon, and H. Choo, "Developing route optimization-based PMIPv6 testbed for reliable packet transmission," *IEEE Access*, 4, pp. 1039–1049, 2016.

[15] G. Yang, L. Xie, M. Mäntysalo, X. Zhou, Z. Pang, L. D. Xu, S. Kao-Walter, Q. Chen, and L. Zheng, " A health-IoT platform based on the integration of intelligent packaging, unobtrusive bio-sensor, and intelligent medicine box," *IEEE transactions on industrial informatics*, vol. 10(4), pp. 2180–2191, 2014.
[16] R. Lea and M. Blackstock, " CityHub: A cloud based IoT platform for smart cities," *IEEE International Conference on Cloud Computing Technology and Science*, pp. 799–804, 2014.
[17] J. Sen, " A survey on wireless sensor network security," *International Journal of Communication Networks and Information Security*, vol. 1(2), pp. 59–82, 2009.
[18] P. Albers, O. Camp, J.M. Percher, B. Jouga, L. Me', and R. Puttini, " Security in ad hoc networks: a general intrusion detection architecture enhancing trust based approaches," *Wireless Information Systems*, pp. 1–12, 2002.
[19] L. Guo, T. Yan, S. Zhao, and C. Jiang "Dynamic performance optimization for cloud computing using m/m/m queueing system," *Journal of Applied Mathematics*, vol 2014, article ID 756592, pp. 1–8, 2014.
[20] P. N. Railkar and P. N. Mahalle, "A queuing theory-based modelling for performance analysis towards future Internet," *Annual IEEE India Conference*, pp. 1–7, 2014.
[21] J. Vilaplana, F. Solsona, I. Teixidó, J. Mateo, F. Abella, and J. Rius, "A queuing theory model for cloud computing," *The Journal of Supercomputing* , vol. 69(1), pp. 492–507, 2014.
[22] G. Levitin and L. Xing, "Reliability and Performance of Multi-State Systems with Propagated Failures Having Selective Effect," vol. 95(6), pp. 655–661, 2010.
[23] M. S. Noughabi, M. Kayid, and M. A. Aabdulrahman, "Dynamic multivariate quantile residual life in reliability theory," *Mathematical Problems in Engineering*, vol. 2018, pp. 1–10, 2018.
[24] Z. A. Lomnicki, "Mathematical theory of reliability", *Journal of Operational Research Society*, vol. 17(2), pp. 213–215, 1996.
[25] A. A. Fattah and A. H. N. Ahmed, "A unified approach for generalizing some families of probability distributions, with applications to reliability theory," *Pakistan Journal of Statistics and Operation Research*, vol. 14(2), pp. 253–273, 2018.

Thi Thi Zin received the B.Sc. degree (with honor) in Mathematics in 1995 from Yangon University, Myanmar and the M.I.Sc degree in Computational Mathematics in 1999 from University of Computer Studies, Yangon, Myanmar. She received her Master and Ph.D. degrees in Information Engineering from Osaka City University, Osaka, Japan, in 2004 and 2007, respectively. From 2007 to 2009, she was a Postdoctoral Research Fellow of Japan Society for the Promotion of Science (JSPS). She is currently a Professor of Graduate School of Engineering, University of Miyazaki, Miyazaki, Japan. Her research interests include human behavior understanding, ITS, and image recognition. She is a member of IEEE.

Pyke Tin received the B.Sc. degree (with honor) in Mathematics in 1965 from University of Mandalay, Myanmar, the M.Sc. degree in Computational Mathematics in 1970 from University of Rangoon, Myanmar and the Ph.D. degree in stochastic processes and their applications in 1976 from Monash University, Australia. He was the Rector of the University of Computer Studies, Yangon and Professor of Computational Mathematics. He is now a visiting professor of International Relation Center, University of Miyazaki, Miyazaki, Japan. His research interests include image search engines, queueing systems and computer vision, stochastic processes and their applications to image processing.

Hiromitsu Hama received the B.E., M.E. and Ph.D. degrees in electrical engineering from Osaka City University, Osaka, Japan, in 1968, 1970 and 1983, respectively. He is currently an emeritus Professor at Osaka City University, and continues his R&D activity at the incubator of Osaka City University. His research interests are in the areas of next generation search engine, surveillance systems, ITS (Intelligent Transport Systems), smile and laughter science, image processing, computer vision, reconstruction of 3D world. He is a member of IEEE.