J Inf Process Syst, Vol.13, No.6, pp.1613~1627, December 2017
https://doi.org/10.3745/JIPS.03.0088

ISSN 1976-913X (Print)
ISSN 2092-805X (Electronic)

JOURNAL OF INFORMATION PROCESSING SYSTEMS JIPS

Internet of Things (IoT) Framework for Granting Trust among Objects

Vera Suryani*,**, Selo Sulistyo**, and Widyawan Widyawan**

Abstract

The concept of the Internet of Things (IoT) enables physical objects or things to be virtually accessible for both consuming and providing services. Undue access from irresponsible activities becomes an interesting issue to address. Maintenance of data integrity and privacy of objects is important from the perspective of security. Privacy can be achieved through various techniques: password authentication, cryptography, and the use of mathematical models to assess the level of security of other objects. Individual methods like these are less effective in increasing the security aspect. Comprehensive security schemes such as the use of frameworks are considered better, regardless of the framework model used, whether centralized, semi-centralized, or distributed ones. In this paper, we propose a new semi-centralized security framework that aims to improve privacy in IoT using the parameters of trust and reputation. A new algorithm to elect a reputation coordinator, i.e., ConTrust Manager is proposed in this framework. This framework allows each object to determine other objects that are considered trusted before the communication process is implemented. Evaluation of the proposed framework was done through simulation, which shows that the framework can be used as an alternative solution for improving security in the IoT.

Keywords

Framework, Internet of Things, Privacy, Security, Trust

1. Introduction

The Internet of Things, hereafter called IoT, is a paradigm that utilizes virtual connections from the Internet to link physical objects that can be controlled using those connections. Various definitions of IoT arise from a variety of sources, depending on the viewpoint of the business process being simulated. This study used the CASAGRAS definition of IoT:

> "*A global network infrastructure, linking physical and virtual objects through the exploitation of data capture and communication capabilities. This infrastructure includes existing and evolving Internet and network developments. It will offer specific object-identification, sensor and connection capability as the basis for the development of independent cooperative services and applications. These will be characterized by a high degree of autonomous data capture, event transfer, network connectivity and interoperability*" [1].

Manuscript received August 18, 2017; first revision September 20, 2017; accepted September 24, 2017.
Corresponding Author: Selo Sulistyo (selo@ugm.ac.id)
* School of Computing, Telkom University, Bandung, Indonesia (info@telkomuniversity.ac.id)
** Dept. of Electrical Engineering and Information Technology, Universitas Gadjah Mada, Bulaksumur Yogyakarta, Indonesia (selo@ugm.ac.id, teti@ugm.ac.id)

This definition by CASAGRAS can be illustrated as a vertical layering architecture, as shown in Fig. 1. There are three layers in the architecture of IoT: Perception, Network, and Application Layers. From a down-top perspective, the Perception Layer consists of objects that are composed of physical devices such as actuators, sensors, people, vehicles, etc. Devices are usually smart objects with the ability to interact with other objects in the IoT environment.

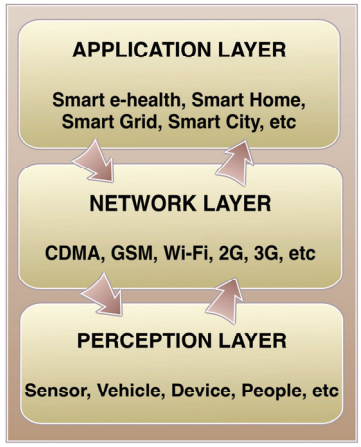

Fig. 1. IoT architecture.

This interaction only occurs when the object is provided with network connections. Connections may include short-distance connection-based network technologies such as Bluetooth, Wi-Fi, or other PAN network technologies. A network connection requiring long-distance connection-based network technologies may use GSM, 3G, or 4G. Once data are sent using these technologies, we can gain benefits from the controlled objects through various applications available on the Application Layer, such as smart homes, smart transportations, smart e-health, smart cities, etc.

However, behind the conveniences offered by IoT, some problems must be addressed, especially in the area of security. The objects in the IoT environment require a framework to reduce potential attacks that may occur. This security framework serves to enhance the security of objects in the IoT. Several researchers have developed security frameworks with each of their uniqueness, depending on their respective business processes.

Aside from IoT, several areas have also developed security frameworks to strengthen their security. The examples include Mobile Ad Hoc Network (MANET) [2,3], point-to-point network [4], Wireless Sensor Network [5–7], grid computing [8], and pervasive computing [9]. Security frameworks in these areas can be adapted for the IoT environment, with some adjustments to IoT characteristics.

Further, research on security framework development can be found in [10]. Conzon et al. [10] have developed a security framework in IoT with emphasis on the use of Extensible Messaging and Presence Protocol (XMPP). They developed a middleware called VIRTUS. This middleware uses authentication scheme through Transport Layer Security (TLS) protocol and encryption scheme via Simple Authentication and Security Layer (SASL). However, VIRTUS needs improvements in the areas of reasoning section and filtering features, object discovery, and semantic addressing.

Other researchers [11] have improved existing IoT security framework called iCore using Security Toolkit named SecKit, which aims to protect user data. However, this framework needs improvements

regarding trust section and risk models. Meanwhile, [12] also tried to build a security framework to protect user privacy using cooperative distributed systems (CDS). The strategy, used here was to separate into two phases: limiting non-authorized process or operation, and neutralizing non-authorized commands. Privacy protection level (PPL) was used afterward. PPL is a probabilistic model aimed to find the effectiveness of the previously-used strategy.

The lack of security solution with light computation formula becomes a challenge for the IoT environment. This solution is an important aspect to be considered since objects in IoT have limited memory and storage capacity for the computational purpose. Centralized security scheme certainly cannot be used here because of its computational cost; otherwise, the solution falls to the semi-distributed scheme. In this paper, we propose a new security framework with semi-distributed characteristic to enhance security in general and privacy in particular. The proposed framework is the development of ConTrust model [13], which was studied earlier.

The contributions are explained as follows: first, a novel security framework is proposed in this paper, including all the processes described in the framework. Secondly, the new algorithm for selecting the coordinator within the IoT network is also described in the proposed security framework. Finally, the proposed framework expects to contribute to an improvement in security, particularly privacy. The other expected contribution is providing flexibility to an object to opt for trusted objects before the communication process, in terms of providing and consuming services.

The paper is organized as follows: Section 2 describes the related works, Section 3 describes the proposed security framework, Section 4 describes the simulation, result, and discussion of performance evaluation, and Section 5 explains the conclusion and future works.

2. Related Works

The study of security in IoT has been carried out by many earlier researchers, ranging from the centralized scheme [11,14–17] to the decentralized scheme [12,18]. The scheme of centralization and decentralization is a classification of security models based on the authentication process. The centralization scheme relies on trusted third parties, such as a certificate authority (CA), to handle authentication processes. The use of third parties is just one method to save the energy that must be spent by each object. In contrast to the process performed by the centralization scheme, in the decentralization scheme, each object is responsible for authenticating process. The absence of trusted third party in this scheme results in the computational cost of the authentication process being charged to the object itself. Although more energy is spent, the decentralization scheme provides the advantage of ease and speed of authentication without involving third parties.

In the decentralization scheme, the object authentication process can be accomplished in various ways, through the use of certain key distributions to mathematical models. Mathematical models use certain parameters, one of which is the trust parameter, to help the process of quantization. Researchers [19] use the trust value with a certain threshold, where the trust value is derived from the total calculation of direct interactive trust, friend recommendation trust, and historical trust. The proposed method is thought to improve the privacy aspect of the object concerned and is relatively more energy-efficient.

Different approaches were made by [20], wherein trusts were not derived from mathematical models

but by defining area-wise trusts. These area-wise trusts were evaluated, using device identification and monitoring device behaviors, connection processes to devices, connection protocols and still considering the assessment conducted by the conventional trust framework. This research is still being developed at this time to improve the approach proposed by those researchers.

The approach is not limited to the one described previously; in fact, we can use different approaches to solve the object's security problem in IoT, for example, by utilizing the current authentication and encryption algorithms or even combining mathematical models with authentication algorithms as done in [13]. Computational cost should always be considered in any approach that is used to increase the value of trust. An approach to the convoluted process will cause minimal energy efficiency. The use of two-layer security can result in higher computational cost. The security framework, proposed in this paper, was compared to the processes that were associated to seek the impact of processes in the framework against computational cost.

3. Proposed Security Framework: ConTrust Model

ConTrust is a trust model for objects in IoT, consisting of current and past assessments [13]. The ConTrust model uses a mathematical approach to calculate the trust value of an object regarding other objects by using the current trust and reputation values held by others. Details of the mathematical approach will not be discussed here, while the further processes that must be performed by the object and coordinator are the focus of this study. In other words, this paper only discusses the processes inside the framework used in ConTrust. The assumptions used in this framework, as seen in Fig. 2, are:

1. Objects are things in IoT, and they can be in the form of a sensor, person, vehicle, camera, etc.; each of these objects may have static or dynamic characteristics.
2. The topology used here is social IoT (SIoT), where a user owns each object, and a user may have more than one object.

A crucial process that needs to be carried out in the ConTrust framework is the election of the ConTrust Manager. The ConTrust framework uses a semi-centralized approach and employs a coordinator known as ConTrust Manager, tasked to maintain the reputation values of the whole objects. Two entities are involved in the election of the ConTrust Manager, i.e., the Service Invoker and the Service Provider. A ConTrust Manager is elected through the methods shown in Fig. 3. At the beginning of the ConTrust Manager election, where the ConTrust Manager position is vacant, given default values are deployed for α, β, and γ parameters. Further, if the ConTrust Manager has been elected, it is entitled to determine the values of α, β, and γ used to select the next ConTrust Manager. Next, the ConTrust Manager must broadcast the values of α, β, and γ to all objects. This step is beneficial for calculating C_M value of objects that will carry out the election of the next ConTrust Manager after the current manager is no longer on duty.

Thus, the formula for calculating the value of ConTrust Manager is:

$$C_M = \alpha.T + \beta.M + \gamma.K \tag{1}$$

where C_M is the value of ConTrust Manager election; T is the most trustable object parameter; M is the object memory capacity; K is the number of objects that are connected; α is the weight component for the trust parameter or T; β is the weight component for the memory capacity parameter or M; γ is the weight component for the number of object parameter or K; α, β, γ are variables for weighting the T, M, and K parameters used in electing the ConTrust Manager, where $\alpha+\beta+\gamma=1$.

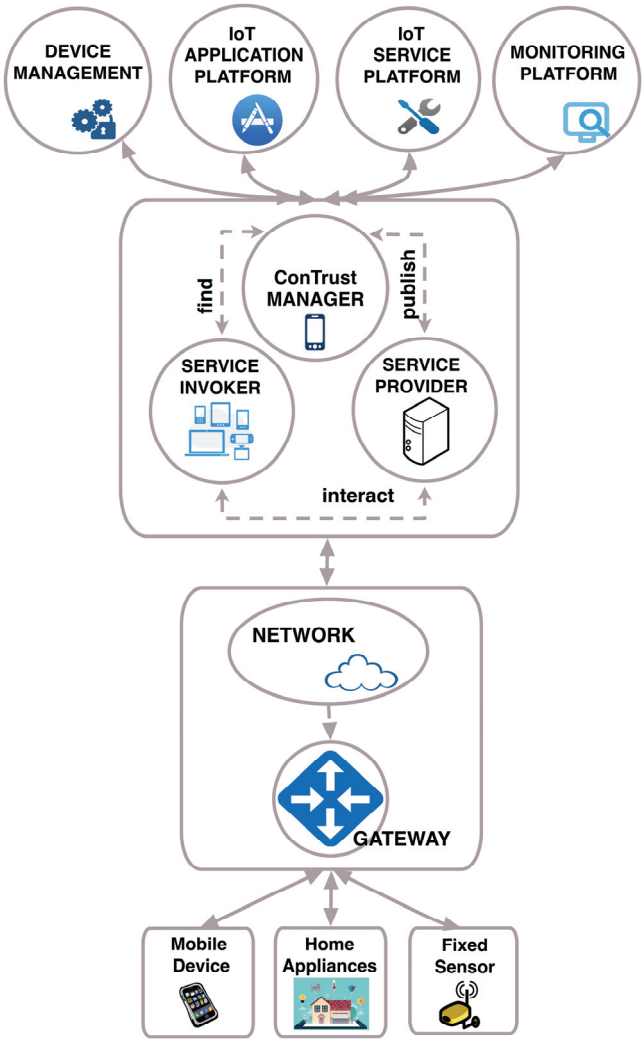

Fig. 2. ConTrust security framework.

The T parameter has a value ranging from zero to one or [0, 1]. Meanwhile, M and K parameters can be quite varied. Since M parameter contains memory capacity, it might range from a few MB to hundreds of GB. Similarly, the value of K parameter can also range from a few to hundreds of connected objects. Therefore, M and K parameters result in highly randomized C_M value, and therefore, normalization is on demand by clustering M and K values to generate C_M value within the range of [0, 1]. The normalization values are shown in Table 1.

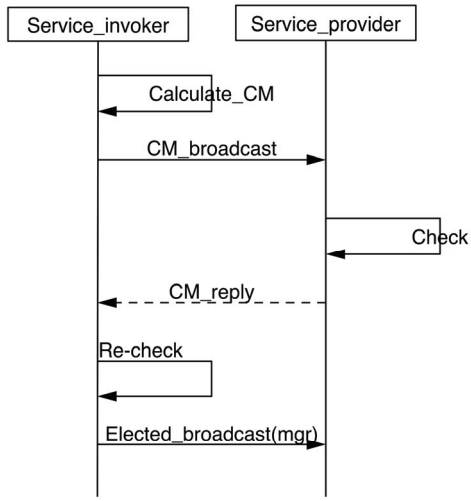

Fig. 3. ConTrust election process.

Table 1. Normalization of parameter values in C_M

Parameter	Raw data	Normalization value
M	$M \leq 128$ MB	[0 0.5]
	$M \geq 128$ MB	[0.5 1]
K	$K \leq 25$	[0 0.5]
	$K \geq 25$	[0.5 1]

The proposed security framework lies between the application and the network layers, as depicted in Fig. 2. It is located below the application layer because it has additional functions of the object before accessing the application layer. There are three main logical functions in the framework, namely, Service Invoker, Service Provider, and ConTrust Manager. Service Invoker can retrieve information from Service Provider, as well as other information and direct interaction with ConTrust Manager. Information taken there can be an initial trust or reputation value, and other information shared by the Service Provider. Meanwhile, the Service Provider is in charge of providing the required information during the election process, the calculation of trust valued by the object, and interacts directly with ConTrust Manager. Finally, the ConTrust Manager is assigned as the coordinator to be contacted during the authentication process, an initiator for group communication, and generator for the authentication key group. Since it is a collection of logical functions, the Service Invoker, Service Provider, and ConTrust Manager can reside in the same object, although it is also possible for them to reside in different objects.

Once the C_M value of object is calculated, the next step is to broadcast a message or MSG to other objects. A MSG contains the following values:

1. C_M value from other objects
2. Value of elected C_M
3. ID of selected objects
4. Time to live (TTL) of the message

Each object is entitled to receive a broadcast MSG. Subsequently, each object will calculate the value of its C_M value and compare it with the C_M value of other received broadcast messages. When an object's C_M value is higher than the others, the object will broadcast a message indicating that it has been elected as the ConTrust Manager. This object will remain the elected ConTrust Manager as long as there are no other objects with a broadcast message with higher C_M values. TTL value will also be reduced one-by-one each time a message passes an object. This broadcast mechanism was adopted from the Distance Vector routing protocol [21], where updates are sent to all connected neighbors or objects. Respectively, objects check incoming messages and compare C_M values to find one with the highest value. Fig. 3 depicts all phases involved in the election, and a short explanation of the steps carried out during the election process can be seen in Table 2.

Table 2. ConTrust election process

Phase	Objective
Calculate_ C_M	Object calculates its own C_M value
C_M _broadcast	Objects broadcast messages containing C_M value
C_M reply	Reply message which contains other objects' C_M value
Re-check	Comparing other objects' C_M values with its own
Elected_broadcast(mgr)	Broadcast message containing the elected ConTrust Manager

Further, the ConTrust framework process can be seen in Fig. 4. The process contains as follows.

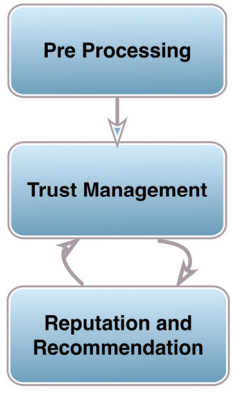

Fig. 4. Process of ConTrust framework.

3.1 Pre-processing

At this stage, pre-processing aims to identify which active objects are in the network. The identification will produce some matrixes: connectivity, initial trust value, and initial reputation value of objects. The connectivity matrix is given the value of zero or one, where zero signifies no connection, and one signifies a connection between objects. Meanwhile, the initial trust and reputation matrixes can be given any values, according to their default trust and reputation values. Since we use the SIoT [22] for describing the topology of 9 objects directly connected to each other in a community, the initial connectivity matrix of these objects will resemble, as described in Eq. (2).

$$C_M = \begin{bmatrix} a_{11} & \dots & a_{in} \\ \dots & \dots & \dots \\ a_{j1} & \dots & a_{jn} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \quad (2)$$

where a is the object, and a_{jn} are other objects connected to this object in one community or network.

Details on the pre-processing stage can be seen in Fig. 5. At this stage, all objects in the community have to authenticate each other by using the Diffie-Hellman method to ensure that each of these objects is trustable. Only a trustable object can perform the next process, i.e., the ConTrust Manager election. Details of the processes carried out at this stage can be found in Table 3.

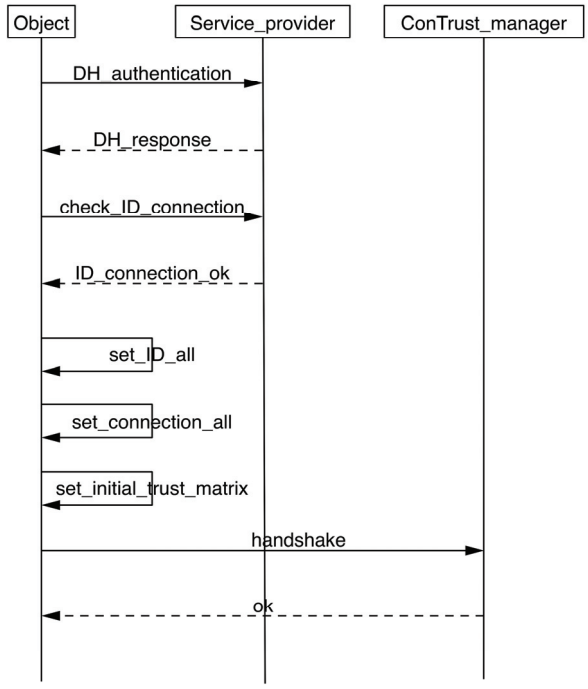

Fig. 5. Pre-processing processes.

Table 3. Pre-processing stages

Phase	Objective
DH_authentication	Authentication process using the Diffie-Hellman method carried out by trustor
DH_response	Response of the Diffie-Hellman authentication process from trustee
check_ID_connection	Checking of connection matrix contents
ID_connection_ok	Returns value of connection matrix content: true if connection exists between trustor and trustee
set_ID_all	Setting ID matrix for all objects connected to trustor
set_connection_all	Setting connection matrix for all objects connected to trustor
set_initial_trust_matrix	Setting content of trust matrix value in cold start condition
handshake	Initialization process to connect with the ConTrust Manager
ok	Response from the ConTrust Manager that object has been identified

3.2 Trust Management

Trust management is an assessment, conducted by the object, using the formula in [13]. Trust assessment essentially tries to find the trust level of each object, using current trust and reputation values. Each object can calculate the trust value of other objects by first taking the reputation value held by ConTrust Manager. Subsequently, the object can calculate the trust value from the trustee to determine whether to continue or terminate the communication process.

The outcome of this process is the trust value of an object within the range of [0, 1]. Details of trust assessment stage can be seen in Fig. 6 and Table 4, respectively.

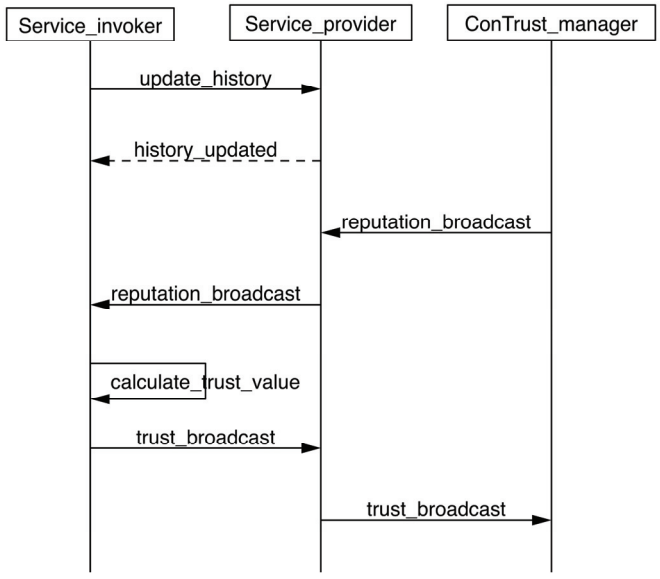

Fig. 6. Trust assessment process.

Table 4. Trust assessment stages

Phase	Objective
Update_history	Checking latest trust value of connected objects
History_updated	Update latest trust value
Reputation_broadcast	Provide reputation value of trustee
Calculate_trust_value	Calculate total trust value of trustee
Trust_broadcast	Broadcast total trust value of trustee

3.3 Recommendation and Reputation

The trust value, generated from the previous trust assessment, is used to consider whether the object is trustable. The recommendation is not only limited to two category values but can also be categorized similarly to the fuzzy system as very trustable, trustable, not trustable, and very not trustable level. The purpose of this categorization is to help the object to decide whether or not to communicate with another previously-assessed object. Details of recommendation stage can be seen in Fig. 7 and Table 5.

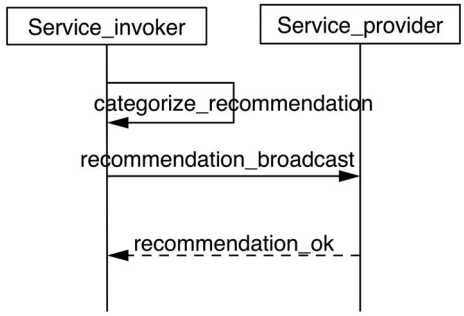

Fig. 7. Recommendation process.

Table 5. Recommendation stages

Phase	Objective
Categorize_recommendation	Create categories for recommendation purpose
Recommendation_broadcast	Broadcast categories of recommendation result
Recommendation_ok	Response message indicates other objects have received recommendation message

Reputation value is used to calculate the total trust value of an object that represents history function. Details of reputation value calculation can be found in [13]. Process and stages involved in reputation can be found in Fig. 8 and Table 6.

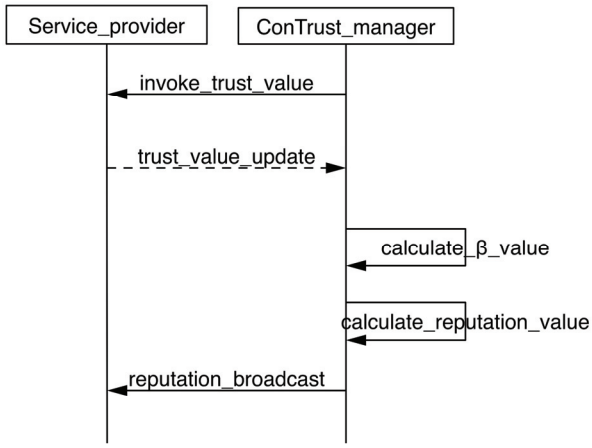

Fig. 8. Reputation process.

Table 6. Reputation stages

Phase	Objective
Invoke_trust_value	Invoke value of current and previous trust from trustee
Trust_value_update	Update trust value to other objects
Calculate_β_value	Calculate β value of trustee
Calculate_reputation_value	Calculate reputation value of trustee
Reputation_broadcast	Broadcast reputation value of trustee

The ConTrust Manager stores reputation values, aiming to reduce objects' computational loads that affect the use of their resources. The approach of the proposed framework is considered a semi-centralized one.

4. Performance Analysis

We conducted several simulations to evaluate the proposed framework. The simulations were performed with the use of the MATLAB tool version 7:13. The evaluation goal is to look at the feasibility of the proposed framework. The scenarios used in the simulations:

i. Varying α, β, and γ values to investigate the correlation of α, β, and γ parameters and C_M value.
ii. Varying the values of T, M, and K parameters to investigate the correlation of these parameters and C_M values.
iii. Comparing the proposed framework with other security frameworks to recognize the effectiveness of the proposed framework regarding the computational operation process and computational complexity.

Fig. 9 analyzes the simulation results with α, β, and γ variations to find out the correlation between α, β, and γ values and C_M value. The simulation showed that α, β, and γ variables were important aspects to differentiate which of T, M or K parameters has more emphasis. The ConTrust Manager must identify which of α, β, and γ variables has the main emphasis.

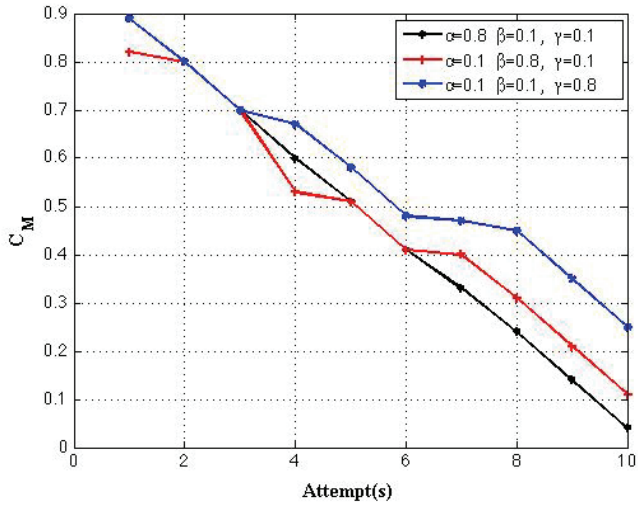

Fig. 9. Variation of different α, β, and γ values.

Meanwhile, Fig. 10 depicts the simulation results with the variation of T, M, and K parameters. This simulation was intended to discover the effect of these three parameters to the value of C_M. Further, these parameters resulted in the decrease of C_M value along with the decrease of the values of trust, memory capacity, and the number of connected objects.

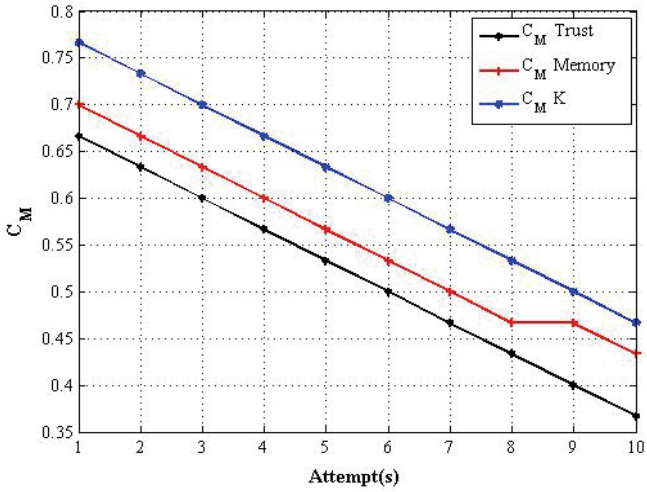

Fig. 10. Variation of different *T, M,* and *K* values.

Moreover, as depicted in Tables 7 and 8, it appears that the ConTrust framework is simpler than two PPTE schemes. Simplification is essential to reduce the computational complexity of the object. Nevertheless, the ConTrust framework is still quite secure to implement in spite of its lower computational cost, thanks to the Diffie-Hellman authorization mechanism.

Table 7. Computational operation of ConTrust framework and two PPTE scheme

Entity	Procedure	Two PPTE scheme	ConTrust
Authorization Process	System setup	√	√
	Encryption transform	√	–
Evaluation Process	Trust pre-evaluation	√	–
	Evidence recovery	√	√
Evidence Provider	Evidence provision	√	√
Requesting Node	System setup	√	–
	Trust evaluation	√	√

Table 8. Computational complexity of ConTrust framework and two PPTE scheme

Entity	Computational operation		ConTrust
	Scheme 1	Scheme 2	
Authorization Process	*O(J)*	*O(J)*	$O(J^n)$, $n>1$
Evaluation Process	*O(N - J)*	*O(N + J)*	*O(1)*
Evidence Provider	*O(1)*	*O(1)*	*O(1)*
Requesting Node	*O(J)*	*O(J)*	*O(J)*

5. Conclusions

Security requirements in IoT can be fulfilled, with the development of the security framework. This paper proposes a new security framework to enhance privacy and security in the IoT environment,

using a semi-centralized approach. It is semi-centralized because a coordinator, called the ConTrust Manager, was used to maintain the reputation values of all objects. The ConTrust Manager election algorithm, proposed in this framework, is a new algorithm.

The future development of this research can be done by checking the implementation feasibilities of the proposed algorithm, using the more appropriate techniques. The importance of this work is to find out the algorithm's robustness for implementation. Further, an additional security feature, instead of the Diffie-Hellman method, which is more resistant to trust-based attacks, is another work to be resolved in the future. Some mitigating efforts to overcome the trust-based attacks were also planned to be in future works. It is not only trust-based attacks but also other attacks, such as Denial of Service (DoS) and DDoS, are expected to be addressed in this framework. Two-phase security protection is the next work to be inspected, especially the usage of the key group authentication and statistical approach to providing a more robust framework.

Acknowledgement

This research was funded by Penyiapan Publikasi Internasional (PPI), Universitas Gadjah Mada in 2017. This research was also partially supported by the Ministry of Research, Technology, and Higher Education, Indonesia, under the PUPT grant (No. 751/UN1-P.III/LT/DIT-LIT/2016) for 2016–2019. We would also like to thank the Laboratory of Sistem Elektronis for permitting us to use the laboratory facilities.

References

[1] CASAGRAS Partnership, "CASAGRAS final report: RFID and the inclusive model for the internet of things," *EU Project No. 216803*, 2009.

[2] S. Umamaheswari and G. Radhamani, "Enhanced ANTSEC framework with cluster based cooperative caching in mobile ad hoc networks," *Journal of Communications and Networks*, vol. 17, no. 1, pp. 40-46, 2015.

[3] E. E. Zakaria, H. S. Hamza, and I. A. Saroit, "An integrated security framework for access control and address auto-configuration for MANETs," in *Proceedings of 8th IFIP Wireless and Mobile Networking Conference (WMNC)*, Munich, Germany, 2015, pp. 253-260.

[4] A. B. Waluyo, D. Taniar, W. Rahayu, and B. Srinivasan, "Trustworthy data delivery in mobile P2P network," *Journal of Computer and System Sciences*, vol. 86, pp. 33-48, 2017.

[5] B. Zhang, Z. Huang, and Y. Xiang, "A novel multiple-level trust management framework for wireless sensor networks," *Computer Networks*, vol. 72, pp. 45-61, 2014.

[6] C. Zhu, H. Wang, X. Liu, L. Shu, L. T. Yang, and V. C. M. Leung, "A novel sensory data processing framework to integrate sensor networks with mobile cloud," *IEEE Systems Journal*, vol. 10, no. 3, pp. 1125-1136, 2016.

[7] J. Wu, K. Ota, M. Dong, and C. Li, "A hierarchical security framework for defending against sophisticated attacks on wireless sensor networks in smart cities," *IEEE Access*, vol. 4, pp. 416-424, 2016.

[8] A. Sheikhi, M. Rayati, S. Bahrami, A. M. Ranjbar, and S. Sattari, "A cloud computing framework on demand side management game in smart energy hubs," *International Journal of Electrical Power & Energy Systems*, vol. 64, pp. 1007-1016, 2015.

[9] U. S. Premarathne, I. Khalil, and M. Atiquzzaman, "Location-dependent disclosure risk based decision support framework for persistent authentication in pervasive computing applications," *Computer Networks*, vol. 88, pp. 161-177, 2015.

[10] D. Conzon, T. Bolognesi, P. Brizzi, A. Lotito, R. Tomasi, and M. A. Spirito, "The VIRTUS middleware: an XMPP based architecture for secure IoT communications," in *Proceedings of 21st International Conference on Computer Communications and Networks (ICCCN)*, Munich, Germany, 2012, pp. 1-6.

[11] R. Neisse, G. Steri, I. N. Fovino, and G. Baldini, "SecKit: a model-based security toolkit for the internet of things," *Computers & Security*, vol. 54, pp. 60-76, 2015.

[12] A. Samani, H. H. Ghenniwa, and A. Wahaishi, "Privacy in internet of things : a model and protection framework," in *Procedia Computer Science*, vol. 52, pp. 606-613, 2015.

[13] V. Suryani, S. Sulistyo, and W. Widyawan, "ConTrust : a trust model to enhance the privacy in internet of things," *International Journal of Intelligent Engineering & Systems*, vol. 10, no. 3, pp. 30-37, 2017.

[14] K. Kang, Z. B. Pang, and C. Wang, "Security and privacy mechanism for health internet of things," *The Journal of China Universities of Posts and Telecommunications*, vol. 20(Suppl 2), pp. 64-68, 2013.

[15] X. Xu, N. Bessis, and J. Cao, "An autonomic agent trust model for IoT systems," in *Procedia Computer Science*, vol. 21, pp. 107-113, 2013.

[16] M. Henze, L. Hermerschmidt, D. Kerpen, R. Haubling, B. Rumpe, and K. Wehrle, "A comprehensive approach to privacy in the cloud-based internet of things," *Future Generation Computer Systems*, vol. 56, pp. 701-718, 2016.

[17] J. Su, D. Cao, B. Zhao, X. Wang, and I. You, "ePASS: an expressive attribute-based signature scheme with privacy and an unforgeability guarantee for the internet of things," *Future Generation Computer Systems*, vol. 33, pp. 11-18, 2014.

[18] M. S. Farash, M. Turkanovic, S. Kumari, and M. Holbl, "An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the internet of things environment," *Ad Hoc Networks*, vol. 36(Part 1), pp. 152-176, 2016.

[19] Z. Chen and L. Tian, "Privacy-preserving model of IoT based trust evaluation," *IEICE Transactions on Information and Systems*, vol. E100-D, no. 2, pp. 371-374, 2017.

[20] H. Sato, A. Kanai, S. Tanimoto, and T. Kobayashi, "Establishing trust in the emerging era of IoT," in *Proceedings of IEEE Symposium on Service-Oriented System Engineering (SOSE)*, Oxford, UK, 2016, pp. 398-406.

[21] A. S. Tanenbaum, *Computer Network*. Boston, MA: Pearson Education Inc., 2003.

[22] L. Atzori, A. Iera, and G. Morabito, "SIoT: giving a social structure to the internet of things," *IEEE Communications Letters*, vol. 15, no. 11, pp. 1193-1195, 2011.

Vera Suryani

She received a master's degree in Information Technology from Institut Teknologi Bandung, Indonesia, in 2009. She joined as a lecturer the School of Computing and Informatics, Telkom University, in 2003. Her research interests include wireless sensor networks, distributed systems, and the Internet of Things. Currently, she is a PhD candidate at the Department of Electrical Engineering and Information Technology, Universitas Gadjah Mada, Indonesia.

Selo Sulistyo https://orcid.org/0000-0002-0427-6421

He is an associate professor of Information and Communication Technology at the Department of Electrical Engineering and Information Technology. He is also the head of the Sistem Elektronis laboratory at Universitas Gadjah Mada. His research interests include software modeling, mobile application development, and security for the Internet of Things and connected objects.

Widyawan Widyawan

He is an assistant professor of Information and Communication Technology at the Department of Electrical Engineering and Information Technology, Universitas Gadjah Mada. He is also the director of the Center of System and Information Resource at Universitas Gadjah Mada. His research interests include pervasive computing, computer security, ubiquitous computing, and wireless systems.