Moving Target Defense and Trust management New Challenges for IoT and SIoT systems*

Souraya Hamida[1,2,*], Ammar Hamida[2] and Okba Kazar[3]

[1]University of Batna 2, Mostefa Ben Boulaid, Algeria
[2]Department of Computer Science, Mohamed Khider University of Biskra
[3]University of Kalba, Sharjah, United Arab Emirates

Abstract
A transition from traditional networks to a new era of IoT and social IoT has occurred as a result of the widespread use of mobile devices and wireless technology. Notwithstanding the advancements made, the safety of IoT and SIoT systems still has to be enhanced. For this need, we give a general overview of how trust management and moving target defense are used in IoT and SIoT to assure security.

Keywords
security, Internet of Things, Social Internet of Things, moving target defense, trust management.

1. Introduction

With the widespread use of wireless technologies and mobile devices, traditional networks are giving way to the Internet of Things (IoT). From industry to home services, the Internet of Things has a significant impact on many different areas [1] [2]

The Social Internet of Things (SIoT) is a groundbreaking new paradigm that was created by applying social networking concepts to the Internet of Things. The latter is a potent architectural substitute for Internet of Things solutions. Fig. 1. illustrates a mapping between IoT and SIoT architecture.

IoT and SIoT systems are being used more and more in the real world. However, they are less secure than modern non-IoT systems. In addition, to remove any obstacles to the general adoption of IoT and SIoT, security problems related to them must be addressed in light of their potential capabilities. A crucial component of security is managing trust and moving target defense [1] [3]. We must comprehend the existing technologies, framework for trust management, and moving target defense in IoT and SIoT systems to integrate security into these systems. In this paper, we provide an overview of the study of trust management and moving target defense for IoT and SIoT systems.

The remainder of this work is structured as follows: sections 2 and 3 present an overview of trust management and moving target defense in Iot and SIoT. Section 4 illustrates the difference between trust management and the moving target defense paradigm. Section 5 gives the conclusion and our future work.

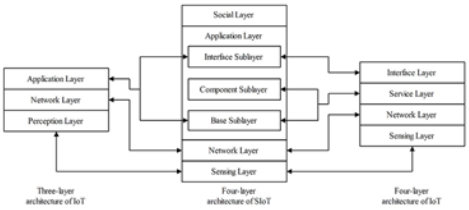

Figure 1: Mapping between IoT and SIoT architecture[1]

2. Trust management

One of the most important components of security is trust management. The purpose of trust management systems is to inform users about trust and assist them in making decisions. For trustworthy data fusion and mining, qualified services with contextual information, and improved user privacy and information security in the IoT, trust management is crucial.[1] [4] [5].

Trust management has been utilized in the Internet of Things to foster trustworthy information sharing among physical items and to construct social relationships autonomously.[6].

2.1. Trust management in IoT

2.1.1. Trust management technique

in IoT systems, trust management is essential to allay people's worries about data integrity and privacy. The

6th International Hybrid Conference On Informatics And Applied Mathematics, December 6-7, 2023 Guelma, Algeria
*Corresponding author.
souraya.hamida@univ-biskra.dz (S. Hamida); ammar.hamida@univ-biskra (A. Hamida); OKazar@sharjah.ac.ae (O. Kazar)

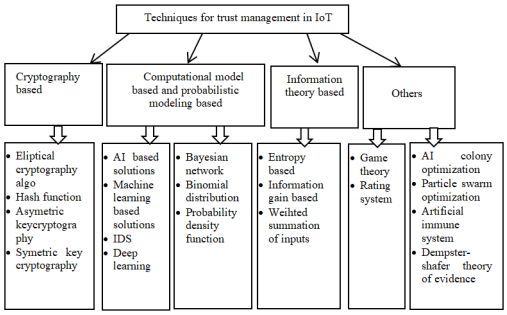

Figure 2: Classification of Trust management technique [2]

methodical process of eliminating and safeguarding a network from unreliable nodes, such as malicious nodes or attacking nodes, broken nodes or malfunctioning nodes, and selfish nodes, is known as trust management. Figure 2 is a summary of all trust management strategies found in the literature [7] [2].

2.1.2. Trust management Framework

The significant limitations that come with IoT-based wireless sensor networks make it difficult to suggest trust management for these kinds of networks [2].

Numerous works have presented a framework for IoT trust management. To increase a node's confidence, several of the themes took into account the security arrangements for each layer [8]. To provide a flexible secure framework that may enhance security based on trust evaluation in human-IoT interactions, other researchers employed a model-based security toolkit [9] . Authors [10] and [11] present a framework that enables developers to incorporate trust concerns in the network while accounting for the functional needs obtained from IoT scenarios. To distribute public keys at the edge of a fog network, the authors of [12] use trust tables at each node [13].

The selection of trust attributes in certain studies is based on the quantity of successful and unsuccessful transactions or positive and negative behaviours. Others have just taken into account social interactions or QoS characteristics [2] [14].

2.2. Trust management in SIoT

A novel framework for the Social Internet of Things (SIoT) has surfaced in recent times. According to its owners' established norms, every object in this paradigm can autonomously form relationships with other objects in the network. Establishing trustworthy links between items and observing their dependability before depending on their knowledge is crucial. Last but not least, trust management has been applied to promote reliable information sharing among physical objects and foster social interactions on their own [15] [16] [17].

2.2.1. TRUST MANAGEMENT FRAMEWORK IN SIoT

the use of blockchain, machine learning, and deep learning in trust management frameworks are some of the most recent developments in this area [18] [19] [20][18] [19] [20]. Specifically, blockchain offers improved security, fault tolerance, immutability, and transparency [21].

Outlines a methodology for trust management in relation to node behaviour when Bad Mouthing Attack is introduced in [22] [22]. Overall trust is the product of expected and estimated trust, which is determined using a Bayes Model and Weighted Sum. The trust calculation makes use of past and anticipated behaviour to thwart malicious attacks [21].

3. Moving Target Defense

Moving Target Defense (MTD) is a cyberdefense paradigm. It can be used to address the security issues in Internet of Things networks. The fundamental idea behind MTD is to ward off attackers by constantly altering the attack surface (such as system and network configurations) to raise the complexity and cost of the attack and also refute any system intelligence that the attackers may have gathered [23] [24] [25].

3.1. MTD frameworks for IOT

In [26], authors presented an MTD framework appropriate for Internet of Things systems. The goal of the suggested framework is to support MTD strategy formulation and execution for Internet of Things systems. The authors developed two MTD techniques based on the framework: port-hopping, which targets UDP port numbers, and the Constrained Application Protocol (CoAP). Both strategies were implemented using actual Internet of Things hardware platforms. Kyi et al. presented a framework for IoT system security using an MTD approach as a place to start when combining diverse defense strategies at various IoT levels. The first component corresponds to a real IoT system. In addition, a virtual Internet of Things system relates to the second part of the framework. An assault detection system corresponds to the third component. There are not enough components in the framework to create MTD strategies for IoT systems [3].

3.2. MTD techniques for IoT

Three basic design questions must be defined by an MTD technique: WHAT, HOW, and WHEN to move. This last can be defined as follows [24]:

- WHAT to move determines the component(s) of the system to which the technique will be applied
- HOW to move deals with the procedures for (i) defining the moving parameter valid states and (ii) selecting a single valid state for the system. Three different types are used in MTD techniques: Shuffling (randomization), Diversification, and Redundancy-based.
- WHEN to move is about applying the state change, i.e., the decision process that triggers the MP value change. Three categories of decision processes (time, event-based, and hybrid) are distinguished in the literature.

An evolving, new technological idea called the MTD paradigm can safeguard an Internet of Things system despite obstacles [27]. Although network topology shuffling can effectively halt attack actions utilizing compromised IoT devices as stepping stones, none of the MTD-based techniques applied to IoT considered this [28] [29] [30].

Decoys are deployed so that the network shuffling-based MTD can deflect the attacker from real IoT devices and give a false impression of the network while also confusing the attacker with changing connections among IoT devices. This can effectively raise the cost and effort of the attack while lowering the likelihood that real IoT devices would be affected [25].

4. The difference between MTD and trust management

There is a difference between the use of MTD and trust management in IoT and SIoT systems. In this section, we will mention the most important one. Table 1 illustrates the difference between Mtd and trust management for IoT and SIoT systems. The most important difference is the Moving target defense is a defense mechanism that dynamically changes the attack surface, but Trust management is a security mechanism that dynamically creates reliable social networking. In addition, the Moving target defense applies to lower layers of the network but Trust management is applied to the social layer (application) in the object. Furthermore, several research papers use trust management for IoT and SIoT but no research work uses moving target defense for SIoT.

5. Conclusion

The rapid development of the internet and smartphone has led to the emergence of SIoT. This last is the integration of IoT and social networking. Despite the progress achieved, the IoT and SIoT still need to develop the safety aspect. For this need, we present in this paper an overview of the use of trust management and moving target defense to assure security in IoT and SIoT. In future work, we will try to use the moving target defense paradigm for SIoT security

References

[1] R. K. Chahal, N. Kumar, and S. Batra, "Trust management in social internet of things: A taxonomy, open issues, and challenges," *Computer Communications*, vol. 150, pp. 13–46, Jan. 2020, ISSN: 01403664. DOI: 10.1016/j.comcom.2019.10.034. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0140366419310953 (visited on 10/13/2023).

[2] H. Tyagi, R. Kumar, and S. K. Pandey, "A detailed study on trust management techniques for security and privacy in IoT: Challenges, trends, and research directions," *High-Confidence Computing*, vol. 3, no. 2, p. 100 127, Jun. 2023, ISSN: 26672952. DOI: 10.1016/j.hcc.2023.100127. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S2667295223000259 (visited on 10/13/2023).

[3] A. A. Mercado-Velazquez, P. J. Escamilla-Ambrosio, and F. Ortiz-Rodriguez, "A moving target defense strategy for internet of things cybersecurity," *IEEE Access*, vol. 9, pp. 118 406–118 418, 2021, ISSN: 2169-3536. DOI: 10.1109/ACCESS.2021.3107403. [Online]. Available: https://ieeexplore.ieee.org/document/9521488/ (visited on 10/13/2023).

[4] Y. Ruan, P. Zhang, L. Alfantoukh, and A. Durresi, "Measurement theory-based trust management framework for online social communities," *ACM Transactions on Internet Technology*, vol. 17, no. 2, pp. 1–24, May 31, 2017, ISSN: 1533-5399, 1557-6051. DOI: 10.1145/3015771. [Online]. Available: https://dl.acm.org/doi/10.1145/3015771 (visited on 10/13/2023).

[5] Z. Yan, P. Zhang, and A. V. Vasilakos, "A survey on trust management for internet of things," *Journal of Network and Computer Applications*, vol. 42, pp. 120–134, Jun. 2014, ISSN: 10848045. DOI: 10.1016/j.jnca.2014.01.014. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S1084804514000575 (visited on 10/13/2023).

Table 1
Difference between MTD and trust management.

Moving target defense	Trust management
Moving target defense is a defense mechanism that dynamically changes the attack surface	Trust management is a security mechanism that dynamically creates reliable social networking
Apply to lower layers of the network.	Apply at the social layer (application) in the object
Use it against network attacks by fooling adversaries in real-time.	Use it against social attacks by calculating the reliability of the services provided by the objects.
Increase the uncertainty, complexity and diversity of the network system.	Increase reliable relationships between objects in the social network

[6] H. Bangui, B. Buhnova, D. Kusnirakova, and D. Halasz, "Trust management in social internet of things across domains," *Internet of Things*, vol. 23, p. 100 833, Oct. 2023, ISSN: 25426605. DOI: 10.1016/j.iot.2023.100833. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S2542660523001567 (visited on 10/13/2023).

[7] R. Kumar and R. Sharma, "Leveraging blockchain for ensuring trust in IoT: A survey," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 10, pp. 8599–8622, Nov. 2022, ISSN: 13191578. DOI: 10.1016/j.jksuci.2021.09.004. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S131915782100255X (visited on 10/13/2023).

[8] D. Chen, G. Chang, L. Jin, X. Ren, J. Li, and F. Li, "A novel secure architecture for the internet of things," in *2011 Fifth International Conference on Genetic and Evolutionary Computing*, Kitakyushu, Japan: IEEE, Aug. 2011, pp. 311–314, ISBN: 978-1-4577-0817-6. DOI: 10.1109/ICGEC.2011.77. [Online]. Available: http://ieeexplore.ieee.org/document/6042788/ (visited on 10/14/2023).

[9] I. Kounelis, G. Baldini, R. Neisse, G. Steri, M. Tallacchini, and A. Guimaraes Pereira, "Building trust in the human?internet of things relationship," *IEEE Technology and Society Magazine*, vol. 33, no. 4, pp. 73–80, 2014, ISSN: 0278-0097. DOI: 10.1109/MTS.2014.2364020. [Online]. Available: https://ieeexplore.ieee.org/document/6969184 (visited on 10/14/2023).

[10] S.-C. Arseni, M. Mitoi, and A. Vulpe, "Pass-IoT: A platform for studying security, privacy and trust in IoT," in *2016 International Conference on Communications (COMM)*, Bucharest, Romania: IEEE, Jun. 2016, pp. 261–266, ISBN: 978-1-4673-8197-0. DOI: 10.1109/ICComm.2016.7528258. [Online]. Available: http://ieeexplore.ieee.org/document/7528258/ (visited on 10/14/2023).

[11] C. Fernandez-Gago, F. Moyano, and J. Lopez, "Modelling trust dynamics in the internet of things," *Information Sciences*, vol. 396, pp. 72–82, Aug. 2017, ISSN: 00200255. DOI: 10.1016/j.ins.2017.02.039. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0020025517305364 (visited on 10/14/2023).

[12] M. S. Haghighi, M. Ebrahimi, S. Garg, and A. Jolfaei, "Intelligent trust-based public-key management for IoT by linking edge devices in a fog architecture," *IEEE Internet of Things Journal*, vol. 8, no. 16, pp. 12 716–12 723, Aug. 15, 2021, ISSN: 2327-4662, 2372-2541. DOI: 10.1109/JIOT.2020.3027536. [Online]. Available: https://ieeexplore.ieee.org/document/9209045/ (visited on 10/14/2023).

[13] M. Ebrahimi, M. H. Tadayon, M. S. Haghighi, and A. Jolfaei, "A quantitative comparative study of data-oriented trust management schemes in internet of things," *ACM Transactions on Management Information Systems*, vol. 13, no. 3, pp. 1–30, Sep. 30, 2022, ISSN: 2158-656X, 2158-6578. DOI: 10.1145/3476248. [Online]. Available: https://dl.acm.org/doi/10.1145/3476248 (visited on 10/13/2023).

[14] W. Alnumay, U. Ghosh, and P. Chatterjee, "A trust-based predictive model for mobile ad hoc network in internet of things," *Sensors*, vol. 19, no. 6, p. 1467, Mar. 26, 2019, ISSN: 1424-8220. DOI: 10.3390/s19061467. [Online]. Available: https://www.mdpi.com/1424-8220/19/6/1467 (visited on 10/14/2023).

[15] S. Sagar, A. Mahmood, Q. Z. Sheng, and S. A. Siddiqui, "SCaRT-SIoT: Towards a scalable and robust trust platform for social internet of things: Demo abstract," in *Proceedings of the 18th Conference on Embedded Networked Sensor Systems*, Vir-

tual Event Japan: ACM, Nov. 16, 2020, pp. 635–636, ISBN: 978-1-4503-7590-0. DOI: 10.1145/3384419.3430434. [Online]. Available: https://dl.acm.org/doi/10.1145/3384419.3430434 (visited on 10/13/2023).

[16] R. M.S., S. Pattar, R. Buyya, V. K.R., S. Iyengar, and L. Patnaik, "Social internet of things (SIoT): Foundations, thrust areas, systematic review and future directions," *Computer Communications*, vol. 139, pp. 32–57, May 2019, ISSN: 01403664. DOI: 10.1016/j.comcom.2019.03.009. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0140366418307655 (visited on 10/14/2023).

[17] J. An, X. Gui, W. Zhang, J. Jiang, and J. Yang, "Research on social relations cognitive model of mobile nodes in internet of things," *Journal of Network and Computer Applications*, vol. 36, no. 2, pp. 799–810, Mar. 2013, ISSN: 10848045. DOI: 10.1016/j.jnca.2012.12.004. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S1084804512002512 (visited on 10/14/2023).

[18] P. Kochovski, S. Gec, V. Stankovski, M. Bajec, and P. D. Drobintsev, "Trust management in a blockchain based fog computing platform with trustless smart oracles," *Future Generation Computer Systems*, vol. 101, pp. 747–759, Dec. 2019, ISSN: 0167739X. DOI: 10.1016/j.future.2019.07.030. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0167739X19301281 (visited on 10/14/2023).

[19] H. Taneja and S. Kaur, "Fake feedback detection to enhance trust in cloud using supervised machine learning techniques," in *Proceedings of Data Analytics and Management*, D. Gupta, Z. Polkowski, A. Khanna, S. Bhattacharyya, and O. Castillo, Eds., vol. 91, Series Title: Lecture Notes on Data Engineering and Communications Technologies, Singapore: Springer Singapore, 2022, pp. 789–796, ISBN: 9789811662843 9789811662850. DOI: 10.1007/978-981-16-6285-0_61. [Online]. Available: https://link.springer.com/10.1007/978-981-16-6285-0_61 (visited on 10/14/2023).

[20] S. Wang, Y. Hu, and G. Qi, "Blockchain and deep learning based trust management for internet of vehicles," *Simulation Modelling Practice and Theory*, vol. 120, p. 102 627, Nov. 2022, ISSN: 1569190X. DOI: 10.1016/j.simpat.2022.102627. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S1569190X22001034 (visited on 10/14/2023).

[21] S. Alam, S. Zardari, S. Noor, S. Ahmed, and H. Mouratidis, "Trust management in social internet of things (SIoT): A survey," *IEEE Access*, vol. 10, pp. 108 924–108 954, 2022, ISSN: 2169-3536. DOI: 10.1109/ACCESS.2022.3213699. [Online]. Available: https://ieeexplore.ieee.org/document/9917502/ (visited on 10/13/2023).

[22] A. Meena Kowshalya and M. Valarmathi, "Trust management for reliable decision making among social objects in the social internet of things," *IET Networks*, vol. 6, no. 4, pp. 75–80, Jul. 2017, ISSN: 2047-4954, 2047-4962. DOI: 10.1049/iet-net.2017.0021. [Online]. Available: https://onlinelibrary.wiley.com/doi/10.1049/iet-net.2017.0021 (visited on 10/14/2023).

[23] S. Wang, H. Shi, Q. Hu, B. Lin, and X. Cheng, "Moving target defense for internet of things based on the zero-determinant theory," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 661–668, Jan. 2020, ISSN: 2327-4662, 2372-2541. DOI: 10.1109/JIOT.2019.2943151. [Online]. Available: https://ieeexplore.ieee.org/document/8847365/ (visited on 10/13/2023).

[24] R. E. Navas, F. Cuppens, N. Boulahia Cuppens, L. Toutain, and G. Z. Papadopoulos, "MTD, where art thou? a systematic review of moving target defense techniques for IoT," *IEEE Internet of Things Journal*, vol. 8, no. 10, pp. 7818–7832, May 15, 2021, ISSN: 2327-4662, 2372-2541. DOI: 10.1109/JIOT.2020.3040358. [Online]. Available: https://ieeexplore.ieee.org/document/9270287/ (visited on 10/13/2023).

[25] M. Ge, J.-H. Cho, D. Kim, G. Dixit, and I.-R. Chen, "Proactive defense for internet-of-things: Moving target defense with cyberdeception," *ACM Transactions on Internet Technology*, vol. 22, no. 1, pp. 1–31, Feb. 28, 2022, ISSN: 1533-5399, 1557-6051. DOI: 10.1145/3467021. [Online]. Available: https://dl.acm.org/doi/10.1145/3467021 (visited on 10/13/2023).

[26] R. E. Navas, H. Sandaker, F. Cuppens, N. Cuppens, L. Toutain, and G. Z. Papadopoulos, "IANVS: A moving target defense framework for a resilient internet of things," in *2020 IEEE Symposium on Computers and Communications (ISCC)*, Rennes, France: IEEE, Jul. 2020, pp. 1–6, ISBN: 978-1-72818-086-1. DOI: 10.1109/ISCC50000.2020.9219728. [Online]. Available: https://ieeexplore.ieee.org/document/9219728/ (visited on 10/14/2023).

[27] J.-H. Cho, D. P. Sharma, H. Alavizadeh, *et al.*, "Toward proactive, adaptive defense: A survey on moving target defense," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 709–745, 2020, ISSN: 1553-877X, 2373-745X. DOI: 10.1109/COMST.2019.2963791. [Online]. Available: https://ieeexplore.ieee.org/document/8949517/ (visited on 10/13/2023).

[28] K. Zeitz, M. Cantrell, R. Marchany, and J. Tront, "Changing the game: A micro moving target IPv6 defense for the internet of things," *IEEE Wireless Communications Letters*, vol. 7, no. 4, pp. 578–581, Aug. 2018, ISSN: 2162-2337, 2162-2345. DOI: 10.1109/LWC.2018.2797916. [Online]. Available: https://ieeexplore.ieee.org/document/8269320/ (visited on 10/14/2023).

[29] A. Almohaimeed, S. Gampa, and G. Singh, "Privacy-preserving IoT devices," in *2019 IEEE Long Island Systems, Applications and Technology Conference (LISAT)*, Farmingdale, NY, USA: IEEE, May 2019, pp. 1–5, ISBN: 978-1-72812-100-0. DOI: 10.1109/LISAT.2019.8817349. [Online]. Available: https://ieeexplore.ieee.org/document/8817349/ (visited on 10/14/2023).

[30] M. Kahla, M. Azab, and A. Mansour, "Secure, resilient, and self-configuring fog architecture for untrustworthy IoT environments," in *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, New York, NY, USA: IEEE, Aug. 2018, pp. 49–54, ISBN: 978-1-5386-4388-4. DOI: 10.1109/TrustCom/BigDataSE.2018.00018. [Online]. Available: https://ieeexplore.ieee.org/document/8455886/ (visited on 10/14/2023).