Journal of Trends in Computer Science and Smart Technology (ISSN: 2582-4104)
www.irojournals.com/tcsst/

A Study on Two-Phase Monitoring Server for Ransomware Evaluation and Detection in IoT Environment

Amirthasaravanan Arivunambi[1], Arjun Paramarthalingam[2]

Department of CSE, University College of Engineering Villupuram, Tamillnadu, India

E-mail: [1]aasaravanan777@gmail.com, [2]arjun_ucev@ymail.com

Abstract

Current trending- Internet of things (IoT) is internetworking of an assortment of hardware devices to offer a collection of applications and services. In the present-day world, ransomware cyber-attack has become one of the major attacks in IoT systems. Ransomware is a hazardous malware that targets the user's computer inaccessible or inoperative, and then requesting the computer victim user to transfer a huge ransom to relapse the damage. At instance, the evolution rate outcomes illustrate that the level of attacks such as Locky and Cryptowall ransomware are conspicuously growing then other ransomware. Thus, these ransomware relations are the latent threat to IoT. To address the issue, this paper presents Two-phase ransomware prediction model based on the behavioral and communication study of Cryptowall ransomware for IoT networks.

This proposed Two-phase model equipped with, Phase-1: observes the inward TCP/IP flowing traffic through a monitoring server to avert the ransomware attack The procedure of the monitoring server is to monitor the IoT's TCP/IP. The process of Monitoring TCP/IP is to extract TCP/IP header and routines command and control (C&C) server IP blacklisting to discover the ransomware attacks.

In Phase-2: the proposed system will also analyze the application pattern for malicious behavior of the Web and URLs. Several societies have very affluent security tools in their milieu, but their events or logs are not monitored, which make affluent tools ineffective. The process of having efficient security based monitoring server is vital for detecting and controlling the ransomware attack.

Keywords: IoT-Internet of Things, Ransomware, Command and control server, Cryptowall, Two- phase monitoring server

DOI: https://doi.org/10.36548/jtcsst.2022.2.003
Received: 11.05.2022, received in revised form: 21.06.2022, accepted: 04.07.2022, published: 13.07.2022

1. Overview

The prevalent technology word IoT is a grid of networks where physical modules / systems are involved and interrelate with one another and customize the linked smart milieu which has a capability to influence social life. At this prevalent technology, devices have knack to accomplish, establish and create it as a smart devices and these devices are employed as a supporting part of social life such as modern homes, roads, offices, markets, industries and education sectors. IoT has unlocked a novel range of novelty by presenting an unintended communication of single user to user smart physical devices which correspondingly create IoT susceptible to a kind of attacks. The devices linked to the Inter-network displays the users count connected to the internet. But conferring to a review 68% of IoT modules are linked by network as susceptible.

1.1 Threat to IoT

There are several threats for IoT like, DoS Botnets, Man-in-the middle attack, Ransomware and Remote video recording. Security and law administration public agencies are in view of these type of attacks for IoT users. One of the utmost threatening attack is ransomware. Ransomware attack has stood budding from the past few ages but in 2019 it had turn out to be a key threat to IoT.

1.2 Ransomware Definition

Ransomware is a malevolent attack which later bug grips target's system or the system mechanism till a payment is acknowledged. [1] Ransomware attacks are recuperating continuously, the attackers making it tough to develop and plan active deterrence methods. [2] Ransomware can be injected to target system by mysterious data spam, download, phishing, advertisement and through communal engineering etc.

The first level of ransomware was identified way in 1989, which attacked a healthcare sector and in no period of time several ransomwares like Crytowall, Testlacrypt, locker ransom attack hit on healthcare sector, local government and IT industries.

2. Ransomware Classification

2.1 Crypto Ransomware

Cryptowall 3.0/4.0 encrypts or locks victim's important files and requests a payment for decrypting the affected files. Crypto ransomware never attack on complete hard disk

storage. [3] [4] It mostly hunts for file extensions like jpeg, .avi,.doc, .pdf, files comprising images, data/text - the ones that if gone astray can affect user the utmost. Crypto ransomware attack routines asymmetric and symmetric encryption methods [5].

2.2 Locker Ransomware

Locker ransomware deadlock the target's devices. Consequently, the target user cannot use the system but the important files are gone unscathed. Mostly, locker ransomware is intended to chunk access to computer user sources. [6] It characteristically locks workstation devices, edges and then requests for a ransom payment to refurbish choked or damaged sources. [7] Later locker attack allows user only restricted access. This means accesses to the system devices be restricted like, keyboard access being restricted to cash card numeric keyboard, authorizing the user merely to form digits for payment.

2.3 Ransomware Growth Rate

[8] The ransomware attacks figure for the earlier year and ballpark the evolution rate of the developing ransomware relations to appraise the utmost aggressive ransomware attacks for IoT.

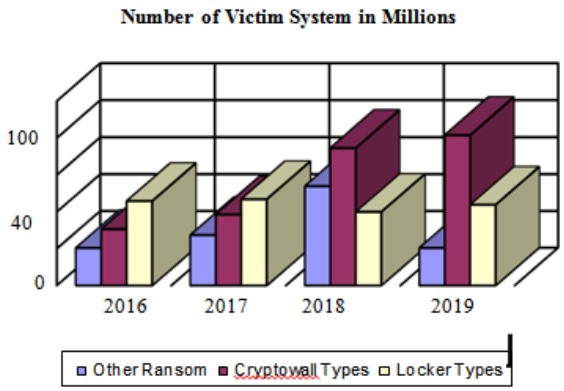

Figure1. Ransomware Growth Rate [8]

Growth rate grades illustrates that the sum of attacks for locky ransomware and cryptowall are remarkably growing and consequently, these ransomware relations are the latent hazard to IoT.

3. Related Work

IoT and its applications proliferate to mainstream of life's infrastructure scope from health, food production and smart cities management. While competence and frequency of

IoT are rising, security problems remain an indispensable concern in different environment. Malware finding and mitigation on IoT systems are the main exploration challenges and prospects recognized, and is a progressing research nowadays [9]. Many researchers have proposed prediction models based on malware's possessions (e.g., application types), and tracing of malicious nodes with its energy utilization [10]. Ransomware is fairly a novel malware that tries to encrypt a conciliation device data by a tough encryption procedure. [11] The victim user will then have to give the ransom in order to get the decryption key or password. Consequences comprise permanent or temporary loss of interruption of standard operations, responsive information, and direct/indirect economic losses.

In [12], authors use a compound statistical come up to make assessment based on power usage. Yet, computational cost for IoT nodes is too much. The authors also engaged frequencies waveform in their advance; consequently, vary in the CPU's description would have an extensive influence on the results even and if the waveform's visual form be invariant.

[12] [13] As per the report of Cybersecurity Ventures, it has calculated that cybercrime will cost the humankind $6 trillion yearly by 2021, up from $3 trillion in 2015. This symbolize the supreme transfer of financial wealth in record, risks the reason for modernization and investment, and will be new cost- effective than the worldwide trade of all key unlawful drugs pooled.[14] The damage cost protrusion is based on past cybercrime figures together with recent year by year growth, a vivid increase in unfriendly nation state supported and planned crime gang hacking actions, and a cyber-attack plane which will be in rising order of magnitude larger in 2021 than it is at present.

In [14] [15] another paper, the author proposed a model that blocks the IP which is formerly affected. That is, if an IP 10.0.0.1 affected a system in the IoT environment, then that 10.0.0.1 IP is consider as blacklisted, thereafter if a message packet receives from 10.0.0.1 IP, it will be blocked and considered as malicious.

4. Proposed System

The most recent technique is to hack a system and infect them by a ransomware. This is due to lack of prevention strategies in network oriented background. A process for having security based monitoring server is important for detecting and controlling the ransomware attack. In-order to triumph over the issue, a novel ransomware evaluation detection system has been proposed. This proposed system has a unique Two -phase Monitoring Server. This

server will be a gateway of any connection in the IoT environment and deduct the ransomware in two phases.

In Phase-1, monitoring server model will observe the arriving TCP/IP traffic to thwart the ransomware attack and that monitoring server include procedures for monitoring and overcrowding malicious users.

In phase-2, to optimize the detection of ransom this phase also monitors the behavior of the URLs and web pages. Hence Two-phase level of monitoring will provide effective security in IoT environment.

5. System Architecture and Evaluation

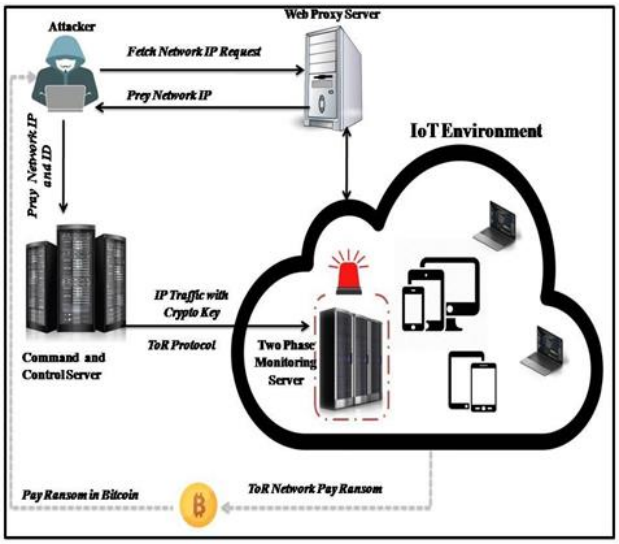

Figure 2. Proposed System Architecture

6. Attitude of Proposed Model

The present hackers use proxy servers to fetch the IP address of the devices connected in the network and process them with Identifiers (ID) to the Command and Control Server (C&C). This (C&C) server uses ToR (Onion Router) network to enter the IoT environment to Attack victim user. Hence the victim user gets infected by ransomware and the data in the system gets encrypted. Generally, ransomware uses MD5, RSA or SHA type of encryption, which are very strong and highly tough to decrypt. Thus, hackers demand victim user for ransom in bitcoin payment to decrypt the system files. To facilitate the above issue, the proposed model is enhanced with a Two-phase monitoring server, which inhabit inside the IoT connected surroundings and all the system /devices are authenticated with user ID and a

password by monitoring server. Server must give acquiescence for the users to enter into the IoT environment which act as first level endorsement, whenever a new user is tried to enter the IoT environment then, and all the incoming packet flowing to the IoT setup will pass through Phase -1 monitoring server and further evaluated by Phase-2.

7. Two-Phase Monitoring Server

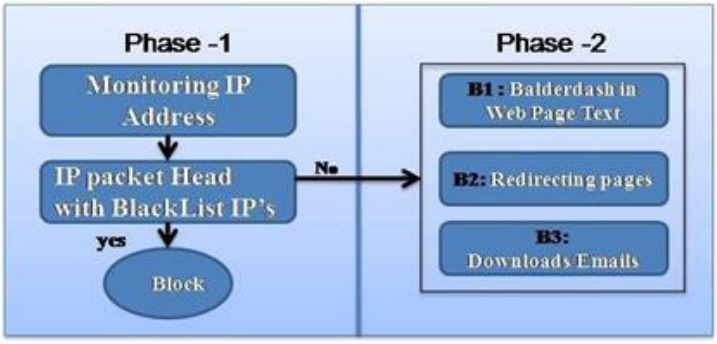

Figure 3. Block Diagram of Two-Phase Monitoring Sever

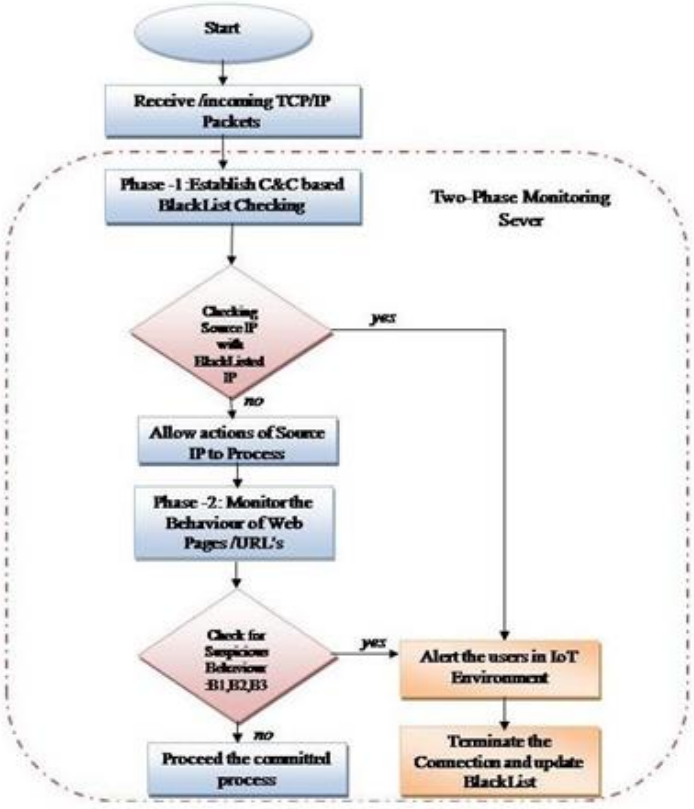

Figure 4. Work Flow Diagram of Two-Phase Monitoring Server

The proposed model has Two -phases of monitoring process. Phase -1and Phase 2. These two phases are the gateway and are implanted with IoT environment as mentioned

earlier. The vital reason for implanting the monitoring server is to have centric monitoring and control of nodes in IoT environment. Moreover, this two-phase monitoring process will boost the security and provide effectual control and alert to the IoT nodes.

Phase 1: Observes the arriving TCP/IP traffic through a monitoring server to thwart the ransomware attack. It then abstracts TCP/IP header and customs C&C server IP blacklist to perceive the ransomware assaults. It extracts the TCP/IP header and customs C&C server blacklisted IP to discover the ransomware assaults. For example, if an IP 10.1.1.1 affected a system, then that 10.1.1.1 IP is considered as blacklisted, thereafter if a message packet receives from 10.1.1.1 IP, it will be blocked and considered as malicious and the connection is terminated.

Phase 2: In this phase the URL's and the Web pages used by the user are monitored. The behaviour of the URL is analyzed and if there exist any suspicious activity from any URL then, alerted raised to user by a warning message. In this Phase, critical three important behaviours are monitored and they are depicted as B1, B2 and B3.

- Behaviour B1: Balderdash in Web Page/Text
- Behaviour B2: Redirecting pages
- Behaviour B3: Downloads/E-mails

Balderdash in Web Page/Text(B1): This type of web pages or text propose unwanted materials which appear to the user. This type of text or hyperlink will lead to diffusion of Ransomware on clicking.

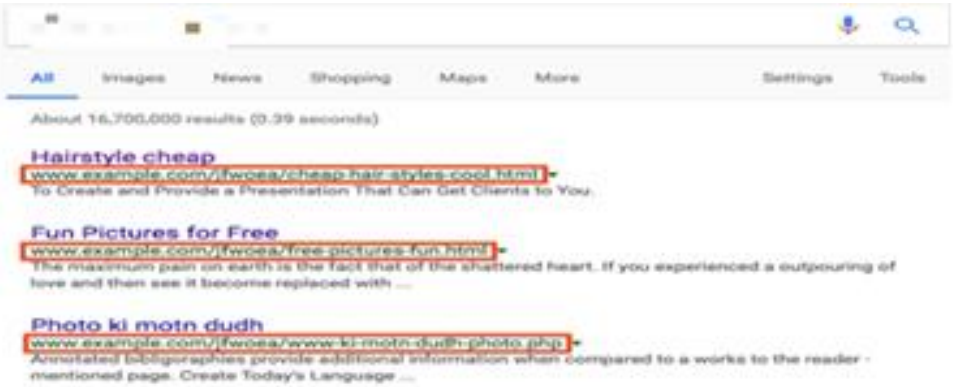

Figure 5. Example of Balderdash in Web Page/Text

For example, if user is searching on particular keyword, but there display unwanted and balderdash contents. if user clicks the links knowingly or unknowingly, then user may be the prey of the ransomware.

Redirecting pages (B2): This behavior is to divert the user or confuse the user by providing multiple processing options, on click event of such options will lead to adware or redirect to some other web pages.

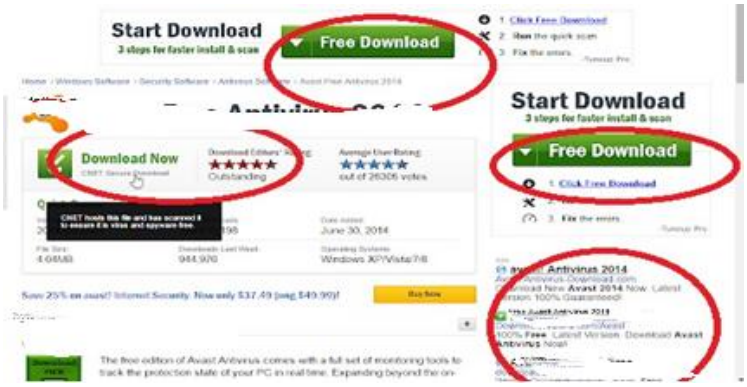

Figure 6. Example of Redirecting pages

In the above figure there are multiple download buttons for single software download. If the user clicks the misleading button, then it may redirect to another web pages or unwanted Download which may inject ransomware codes. Downloads/Suspicious E-mails (B3): This behavior is where, user gets suspicious e-mail with attachments and driven by the malicious links in the mail, the user may redirect or download malware contents which will replicate in the system slowly and affect it. Generally suspicious E-mails are filtered user account as Spam emails, but if user is not aware of the such emails and accessing the links or downloading the attachment may lead to ransomware infection.

Figure 7. Example of Suspicious Emails/ Downloads[16]

8. Two-Phase Scenario

Phase -1

TCP/IP Monitoring:

$$\left.\begin{array}{l} IP\_Blacklist = IP\_source \rightarrow Block \\ IP\_Blacklist = IP\_source \rightarrow Allow \end{array}\right\} \quad (1)$$

Phase-2

Behavioral Monitoring:

$$B1 \wedge B2 \wedge B3 \rightarrow Alert \quad (2)$$

The proposed Two-phase Monitoring Server system which is used to perceive and control the malicious user even if the IP is new. If the arriving message is from new IP, this proposed system analyze the behavior of the web pages & URL's and weigh up that incoming message format with the ransomware virus message format and alert the user. This particular property of the model will certainly enrich the security level at and provide safe in IoT environment.

9. Conclusion

This proposed system has delivers a considerable level of security in IoT environment. The major security threats for IoT environment are malwares, DDoS attack and ransomware attacks. But, ultimately the ransom is more threatening than others in view of the fact that such attack demand ransom. Moreover, such attacks are very tough to trace and rollback or finding the attacker. The proposed system has addressed this issue by providing security at ingress level through Two- phase monitoring server. All the nodes of IoT environment are connected to the centric Two- phase monitoring server and provides authentication from the server, since it will help in follow-up of all node to ensure primary security endowment. Then the Two -phase monitoring server will monitor all the IoT nodes and TCP/IP traffics that connects the IoT environment for any blacklisted IP's. Moreover, server also monitor and alert the user for any suspicious activity in URL's which are accessed by the user by its suspicious behavior. This proposed approach can be extended for detection other ransomware that are not based on network traffic and to detect ransomwares which leak user data in near future.

References

[1] Ahmadian, Mohammad M, & Hamid Reza Shahriari, "A framework for high survivable ransomwares detection." Information Security and Cryptology, 13th IEEE Conference International Iranian Society of Cryptology Conference, (2016).

[2] Bertino E, Choo KKR, Georgakopolous D, Nepal S, "Internet of things (IoT): smart and secure service delivery", ACM Trans Internet Technol, 16(4), pp.22:1–22:7,(2016).

[3] Broadanalysis Threat Intelligence and Malware Research,"Neutrino EK from 104.238.185.187 sends DMA Locker4.0". Available:www:broadanalysis:com/2016/ 05/22/neutrino-from-104-238-185-187-sends-dma- locker-4-0/, (2016).

[4] Daniel Gonzalez,"Detection and prevention of crypto-ransomware, ubiquitous computing", Electronics and Mobile Communication Conference (UEMCON), Tech. Rep. CERIAS Tech Report 17,(2017).

[5] Dell Secure Works Counter Threat Unit Threat Intelligence, "CryptoWall ransomware threat analysis".Available: www:secureworks:com/research/ cryptowall-ransomware,(2014).

[6] Emsisoft Lab, "CryptoDefense: The story of insecure ransomware keys and self-serving bloggers". Available: blog:emsisoft:com/ 2014/04/04/cryptodefense-the-story-of-insecure ransomware keys- and-self-serving-bloggers/,(2016).

[7] Kharraz, Amin, Sajjad Arshad, Collin Mulliner, William K. Robertson, and Engin Kirda. "UNVEIL: a large-scale, automated approach to detecting ransomware" In USENIX Security Symposium, pp. 757-772. (2016).

[8] WendyZamora,"how-to-beat-ransomware-prevent-dont-react", Available: https:// blog. malware how-to-beat-ransomware -prevent-dont-reactytes.com /101/2016/03/ how-to-beat ransomware- prevent-dont-react/, posted on: july2018, (2018).

[9] Arjun, P., Stepheniaj, S., Naveen Kumar, N., Naveen Kumar, K.: "A Study on IoT based Smart Street Light Systems, IEEE International Conference on System, Computation, Automation and Networking(ICSCAN), pp. 1-7,(2019).

[10] Yang H, Tang R," Power consumption based android malware detection", J. Electr Comput Eng ,pp1–7,(2016).

[11] Huang .D. Y., D McCoy, M. M. Aliapoulios, V. G. Li, L. Invernizzi, E. Bursztein, K. McRoberts, J. Levin, K. Levchenko, and A. C. Snoeren, "Tracking ransomware end-to-end," in 39th IEEE S&P, pp.1– 14,(2018).

[12] Herjavec Group,"The 2020 Official Annual Cybercrime Report"Available: https://www.herjavecgroup.com /the- 2019-official- annual-cybercrime report/ https://cybersecurity ventures .com /hackerpocalypse-cybercrime-report- 2016/Oct. 16, (2017).

[13] Shaerpour K, Dehghantanha A, Mahmod R "Trends in android malware detection", J Digit Forensics Secur Law, 8(3), pp.21–40,(2014).

[14] Jarvis. K., "CryptoLocker Ransomware". Available: www:secureworks:com /research /crypto locker-ransomware, (2013).

[15] Buczak AL, Guven E "A survey of data mining and machine learning methods for cyber security intrusion detection",IEEE Commun Surv Tutor 18(2),pp.1153–1176,(2016).

[16] Imperva, “phishing-attack-scam”. Available: https://www.imperva.com/learn/ application-security/ phishing-attack-scam/, Source taken on :11th jan.2021,(2021).

[17] Ganenja, Kandaval, “knowing the ransomware and building defense against it - specific to healthcare institutes”, International Conference on Mobile and Secure Services, pp. 286–302, (2016).

[18] Faruki P, Bharmal A, Laxmi V, Ganmoor V, Gaur MS, Conti M, Rajarajan M " Android security: a survey of issues, malware penetration, and defenses", IEEE Commun Surv Tutor ,17(2),pp.998–1022,(2015).

[19] B. Stone-Gross, “The lifecycle of peer to peer (gameover) zeus”. Available: www:secureworks:com / research/the lifecycle of peer to peer gameover zeus,(2012).

[20] Francesco Mercaldo, Isco Alarci , “TOR traffic analysis and identification”, AEIT IEEE International Conference, 2485, pp. 26, (2017).

[21] Gerald, sileshi Yalew, “Hail to the thief: protecting data from mobile ransomware with ransomsafedroid”, IEEE Conference on Network Computing and Applications, pp. 657–666, (2017).

[22] Krebs, Brian., "FBI: North Korea to blame for Sony hack." Retrieved from Krebs On Security: Available: http://krebsonsecurity. com/2014/12/fbi- north-korea-to-blamefor-sony-hack,(2014).

[23] Liao.K, Z. Zhao, A. Doup´e, and G.-J. Ahn, “Behind closed doors: measurement and analysis of cryptolocker ransoms in bitcoin,” in APWG eCrime Research, pp. 1–13,(2016).

[24] Sgandurra, Daniele, Luis Muñoz-González, Rabih Mohsen, and Emil C. Lupu. "Automated dynamic analysis of ransomware: benefits, limitations and use for detection." arXiv preprint arXiv:1609.03020,(2016).

[25] Sicari S, Rizzardi A, Grieco LA, Coen-Porisini A "Security, privacy and trust in internet of things: the road ahead", Comput Netw, 76pp.146–164,(2015).

[26] Spagnuolo. M, F. Maggi, and S. Zanero, “BitIodine: extracting intelligence from the bitcoin network,” in Springer Financial Cryptography and Data Security, LNCS, 8437, pp. 457–468,(2014).

[27] Steve Morgan" Cybercrime Damages $6 Trillion By 2021" the Hood of Ransomware Attacks,” in 12th Springer DIMVA, pp. 3–24, (2015).