J Supercomput (2017) 73:3065–3084
DOI 10.1007/s11227-016-1825-5

CloudRPS: a cloud analysis based enhanced ransomware prevention system

Jeong Kyu Lee[1] · **Seo Yeon Moon**[1] · **Jong Hyuk Park**[1]

Published online: 25 July 2016

Abstract Recently, indiscriminate ransomware attacks targeting a wide range of victims for monetary gains have become a worldwide social issue. In the early years, ransomware has used e-mails as attack method. The most common spreading method was through spam mail or harmful websites. In addition, social networking sites or smartphone messages are used. Ransomware can encrypt the user's files and issues a warning message to the user and requests payment through bitcoin, which is a virtual currency that is hard to trace. It is possible to analyze ransomware but this has its limitations as new ransomware is being continuously created and disseminated. In this paper, we propose an enhanced ransomware prevention system based on abnormal behavior analysis and detection in cloud analysis system—CloudRPS. This proposed system can defend against ransomware through more in-depth prevention. It can monitors the network, file, and server in real time. Furthermore, it installs a cloud system to collect and analyze various information from the device and log information to defend against attacks. Finally, the goal of the system is to minimize the possibility of the early intrusion. And it can detect the attack quickly more to prevent at the user's system in case of the ransomware compromises.

Keywords Ransomware · Abnormal behavior · Prevention system · Intrusion detection · Cloud

✉ Jong Hyuk Park
jhpark1@seoultech.ac.kr

Jeong Kyu Lee
jungkyu21@seoultech.ac.kr

Seo Yeon Moon
moon.sy0621@seoultech.ac.kr

[1] Department of Computer Science and Engineering, Seoul National University of Science and Technology, Seoul, Korea

1 Introduction

With increased usage of the computer and the growth of the internet, cybercrime has also increased [1]. Many security-related systems to prevent cybercrime have been proposed, still cyberattacks keep evolving [2]. The attack and defense between cybercrime and information security technology have become more complicated [3]. The most talked topic in these days is ransomware attacks. In the past, these attacks used symmetric keys, and therefore, restoration was possible through extraction of the key value based on malicious code analysis [4]. But recently public key encryption system using public key and private key makes it impossible to restore unless one has the private key. This private key is stored on the C&C server, and sometimes a fee for restoration is required [5].

The file formats used for spreading ransomware are DOC and PDF extension and icon, files that disguise themselves as screensaver extensions (.SCR), macro included in text files, and crypt extension (.js). Recently, the range has expanded to include whitelist, live chat, high quality design, and ransomware as a service (RaaS), becoming more intelligent and various forms [6]. The major examples include targeted attacks on specific classes or institutions, and attacks on large community sites. They all aim at monetary gain [7]. Ransomware is spread in a similar way to existing malicious codes such as bot, trojan, or worm [8]. The traditional attacks used one form of attacks where the symptom appeared instantly and the target was anonymous. But ransomware attacks avoid detection and only encrypt information that the attacker wants.

There is continuous research and development by various security-related institutions and companies to provide solutions for ransomware but the reality is that they are not able to provide fundamental solutions [9]. In addition, because restoration is difficult if there is no previous data backup, priority needs to be focused on minimizing the damage.

In general, ransomware attacks targeted personal information and files but recently they are targeting more and more social infrastructure, corporate information, or specific classes such as graphic designers or academic associations. Since only the attacker holds the decryption key and the attacks become more sophisticated, early detection of intrusion doesn't necessarily mean defense [10,11]. Therefore, the ransomware attacks pose a large threat and a new countermeasure is needed [12].

Because new variants of ransomware are difficult to detect or define as malicious behavior, it is difficult to detect using existing solutions [13]. Therefore, to detect and prevent malicious and abnormal behaviors, further researches on prevention and detection need to be undertaken. In particular, cloud based system that comprehensively manages malicious and abnormal behavior with that threats information. In this paper, the network, file, and server are monitored in real time to defend against constant and sophisticated ransomware attacks. By installing a cloud system, the intrusions of ransomware are monitored through the collection of logs, ransomware samples and threat information. In this paper, CloudRPS that protects user data is proposed. This minimizes the intrusion possibility of ransomware. Also when recognizes the attack, the damage can be reduced with fast respond.

This paper is organized as follows; In chapter 2, we describe the ransomware attack cases, and analysis of the ransomware prevention method. In addition, we describe security threats, security requirements, and the existing researches. Chapter 3 discusses our proposed system and shows a service scenario, performance analysis. In chapter 4, we conclude our research.

2 Related works

This chapter describes the core elements of ransomware attack methods and cases. It also analyzes the prevention method against ransomware. In addition, existing researches of different security threats and requirements are discussed in this chapter.

2.1 Ransomware attack methods and attack cases

In this section, we discuss the attack methods and cases of ransomware, and analyze the types and its characteristics.

Ransomware is spread through attached files in emails with unclear origins, or web ActiveX installation and execution of infected files. The attached files can be zip, exe, cab, or pdf. If commonly used files in the PC such as office extension, hwp, doc, pdf, txt, jpg, mp3, etc. are executed, the infected file with ransomware is downloaded from the server and executed [14,15].

There are two major methods for ransomware attacks. First, there is the malicious code, infection by a drive-by-download method. If users visit an infected website, the malicious code will be spread. The reason ransomware can be spread through just accessing a website, unlike other viruses, is because it uses code insertion method. Ransomware forced terminates windows security center and saves important files in the following file pattern through the RSA-2048 encryption algorithm.

(File name).(Encryption object file<u>*extension*</u>*). Encrypted*

In an infected environment, the windows operating system can be used without problems. When saving an encrypted file to a location except for specific directory, then it is encrypted and it cannot be opened. Then a warning message is issued through the web browser or notepad and the user is led to make a payment through bitcoin, a virtual currency that is hard to trace [16].

The malvertising is the second method ransomware uses. Malvertising is a synthesized word that combines the word ‘malicious’ and ‘advertising’. The method uses a normal network to spread malicious code and infection [17]. For example, the attacker produces an advertising website that is similar to a normal domain. This fake website redirects the user to a vulnerable page after which one moves onto the normal website. The company offering the normal services usually provides a URL with a specific parameter that can dynamically receive ads so that users can be exposed to many advertisements. The provided URL is used on many websites. The malvertising adware has an encoded URL with a specific parameter that proactively receives advertisements. The pop-ups or free applications are used as disguises to install then from

P2P, crack, pornography, or free game websites [18]. There are two cases of infection by malicious code. They are shown in pop-ups on the web browser when surfing the web. If it is a web browser vulnerable to security or if flash player, acrobat reader, silverlight, or java have been installed, then infection may occur. The user is redirected to a vulnerable website and then the afore-mentioned web application plug-ins are used to infect them by malicious code. The method using malvertising can target a large number of people, and can often change the domain, making it difficult to trace the origin or block it [19].

Cryptowall3.0 uses the specific extension file for encryption via RSA-2048 algorithm and leaves four files in the relevant file. The files that correspond to HELP_DECRYPT.HTML, HELP_DECRYPT.PNG, HELP_DECRYPT.TXT, and HELP_DECRYPT explains what the RSA-2048 algorithm is, how to restore the system and how to normalize files. In exchange, it asks for monetary compensation. The recently discovered cryptowall4.0 is a ransomware that changes the file name and extension to a random combination of letters and numbers [20,21].

Crypt0L0cker changes the file's extension to encrypted and generates two files within the encrypted file (DECRYPT_INSTRUCTIONS.* / HOW_TO_RESTORE _FILES.*). It is operated once the back-up version for the system protection feature is deleted [22].

CTB-Locker changes the file's extension into a seven digit word upon infection and generates two files in the encrypted file. It then explains what needs to be done to normalize and asks the user money in return. But even after making the payment, it is impossible to verify whether it can be restored [23].

TeslaCrypt changes the file's extension from ecc → ezz → exx then generates the file (HELP_RESTORE_FILES.*) within the encrypted file. The files of 200MB or more do not get damaged. Restoration tools have recently been developed but it has been updated to delete the key file from the PC, making it impossible to restore even with a decryption tool. The files of the Temp folder are not encrypted [24].

The NK_, VO_ steals a user account through malicious code, then remotely accesses the terminal from the PC or server, registers the infected ransomware file on the work scheduler to operate it. Within the encrypted folders where the words NK_, VO_ are added to the front of the file, is generated a file (NK_IN YOUR FILES.*/VO_IN Documents.*). Unlike the general ransomware, there is no specific name and it has evolved from existing PC attacks to server DB attacks. It has changed from the existing server basis to an email basis program. Unlike existing ransomware, it is executed upon OS being started. So when the device is booted, it is on constant operation mode. This requires the infected files (1.bat, sysdll.exe) registered on the Windows work scheduler to be deleted [25].

Locky generates the file (_Locky_recover_instructions.*,_HELP_instructions.*) within the encrypted file that has the extension changed to locky. This is a ransomware that infects usually through attached files. The home screen is changed to the generated file content and its file name is changed into one that is encrypted, such as the cryptowall4.0. The difference from other ransomware is that even on disconnected networks, the share data is encrypted [5,26].

2.2 Analysis of the ransomware prevention method

This section presents major cases of the ransomware attacks, their correlations with prevention methods and the analysis, detection and prevention methods of each scenario.

- **PC Update:** As for Java, if a new update is not implemented or the program is not used, it is safer to uninstall it from the PC. Update Adobe Reader and Adobe Flash Player to the latest version, as well as the Windows and the protection software to strengthen security.
- **PC & Server Data Back up:** If data backup is deferred to the user, then backup is not implemented correctly. Backup by the administrator setting is safer.
- **Web page files & sites security Check:** Check the safety status of the website on www.virustotal.com and another website before browsing it.
- **Share Folder Management:** When a shared folder is operated, it should be changed to a hidden setting so that only authorized users can access it.
- **System Security Settings:** If the system protection window is opened, one can verify whether the driver backup is set up. If there is not a point of restoration, then after selecting the relevant drive, select the configuration menu to set the restoration point in time. If it is not an OS driver, even by just activating the restoration menu of the former version file, a stable management is possible. The restoration point in time must be generated for a safer management of the data.
- **Read-only folder settings:** By changing the data into a read-only folder, the folder can be protected from being infected if ransomware intrudes. If it is locked and a revision is needed, the folder can be unlocked and used but Crypt0L0cker is an exception.

The Table 1 shows which prevention methods can be used for each case of ransomware attack type.

Among the prevention methods, PC update and read-only folder settings can be used across the board. But PC & server data backup, web page file & sites safety check, share folder management, and read-only folder settings differ in their effectiveness

Table 1 Analysis of ransomware prevention methods

Step						
Type	PC update	PC & Server sata backup	Web page file and sites safety check	Share folder management	System security settings	Read-only folder settings
CryptoWall3.0	●	●	●	●	◑	●
Crypt0L0cker	●	○	●	●	●	●
CTB-Locker	●	●	●	●	●	●
TeslaCrypt	●	●	●	◑	●	◑
NK_, VO_	●	●	●	○	○	●
Locky	●	●	○	○	●	●

(● possibility, ◑ partially possibility, ○ nothing)

for each type of ransomware attack. Unless a backup copy of the system protection features in Crypt0L0cker is deleted before operation and then physically separated before the backup, prevention is difficult. The TeslaCrypt does not damage files of 200MB or more but since it deletes the key file of the PC, even with a decryption tool, restoration is difficult once infected.

2.3 Security threats and requirements

In this section, we discuss security threats posed by ransomware and draw the security requirements.

2.3.1 Security threats

- **Server-based threats:** Malicious code can be distributed through service. Malicious code distribution using servers include methods of automatically downloading malicious code. This can be achieved by inserting a script into a webpage and when the user opens it, the malicious code is automatically downloaded. Another method is by linking a website to another one controlled by the attacker and inducing a download. Malicious code infection using servers have severe problems in security due to the users not being aware of it and giving consent subconsciously.
- **Network-based threats:** Security threats in the network primarily occur in the local wireless network and wired network. In particular, ransomware can be transmitted through a web browser or web page. It is not easy to detect malware and its abnormal behavior when attackers exploit security vulnerabilities in unspecified destinations or use a normal web page to disguise the ransomware. In addition, the threat is more serious because the user is not aware of the presence or absence of transmission data. If the security in the network is weak or the attack is disguised inside a normal Web page, the detection of the malware and its abnormal behavior becomes even harder. Also, since the user is not aware of the data transmission, the security threat is even greater.
- **File-based threats:** The ransomware attacks are likely to be spread through a USB that has an infected file or through files attached to email. Especially due to the prolific use of file insertion form in normal documents, it is difficult to detect with existing security detection and analysis methods. The infected files are disguised to look like normal files so the user is not aware of the infection, which leads to security issues.

2.3.2 Security requirements

- **Server-based detection and response:** Ransomware attacks continue to be an issue not only for PCs but also for mobile devices. If administrator authority is gained, then personal information is leaked through the malicious code. If vulnerabilities exist within the OS of the mobile web, malicious code can exploit them to download and install ransomware. As such, the constant monitoring has to be

used to prevent the installation of malicious code or abnormal activities. Thus, detection and response to such cases are required.

- **Network-based detection and response:** Attacker can use attack which host or external other system based on network. The network is simply used as an attack route for ransomware. Because there are weakness that is lack of infection status recognition caused by difficulty in the user transmitting data. As such, to prevent abnormal activities and malicious codes that are disguised or altered, traffic monitoring and network monitoring is required for detection and response.
- **File-based detection and response:** Ransomware attacks may also be distributed through email attachments and previously infected files on USB drives. Problems of security occur because users do not detect the malicious code because it is masqueraded as normal files. Therefore, the installation of unauthorized OS images or files must be averted and administration management of the files must be conducted. Moreover, through the real-time data backup, data must be segregated and managed. Constant monitoring is also required for file verification of files infected by malicious code or those that are disguised or altered.
- **Real-time updates:** There is a need for real-time updates on various threat information such as existing ransomware information, categorize information, and signature values to detect new and variant malicious and abnormal behaviors apart from known ransomware. It needs to maintain malicious code information up-to-date on the database to maintain high detection rates.
- **Accuracy:** The most important problem of detection systems is the many error results caused by detection methods. For detection systems, it is a severe problem and it is not an acceptable result. Inaccurate detection affects response mechanisms, causing unnecessary traffic or system errors through detection system execution to end her normal behavior of the user. Therefore, accuracy and detection are important requirement.
- **Reliability:** The inherent function of the detection system should not affect other systems while detecting server and network files. By maintaining detection system information independently, data management needs to be done. Also, in this security threats, when malicious behavior and abnormal behavior are detected, system files, processes, registry, and network should not be arbitrarily changed. Lastly, there cannot be system internal data edit or deletion by unauthorized users.
- **Availability:** For the normal operation of detection systems, there needs to be accuracy and reliability as well as availability. There cannot be delays in the user conducting necessary functions through the system. Also there needs to be verification on availability due to the possibility of examination and tracking within the system. Also through independence and virtualization of detection systems there needs to be availability on system attacks or disabilities.

2.4 The existing researches

Amin Kharraz et al. researched about ransomware attack possibility detection, ransomware attack prevention and file system operation monitoring. By classifying

ransomware, groups through samples were proposed and results were derived through experiment and analysis. Also on continuous response on ransomware attacks, security threat of ransomware with function was derived and proposed a general method of detecting ransomware of zero-day attacks [27].

Tianda Yang et al. analyzed malicious code and ransomware characteristics in mobile environment and proposed automated analysis method. The study wrote about dynamic analysis and malicious attack methods in android through path and data flow, domain axis, and android permissions and discussed the proposed automatic analysis method divided into API call order, resource, and APK structure. The study analyzed APK files through dynamic and static analysis in mobile environment and through blacklist method, malicious domain information was collected. Also by monitoring transfer data, data flow was tracked [28].

Mohammad Mehdi Ahmadian et al. discussed a new approach method for ransomware detection and damage prevention. It includes GA-detector technology and newly suggests the monitoring framework of Connection-Monitor & Connection-Breaker (CM&CB). It classifies non-encrypted ransomware (NCR), encrypted ransomware (CGR), personal encryption ransomware (PrCR), public encryption ransomware (PuCR), and hybrid encryption ransomware (HCR). It is classified by main characteristics based on samples and in the key exchange stage, high survivable ransomware (HSR) is detected. Through high survivable ransomware detection, a new method to prevent user data encryption is suggested. Through experiment evaluation ransomware variant detection was analyzed [29].

Alexandre Gazet investigated the basics of security threats over case. Through comparative analysis of various ransomware virii, technical review was discussed based on reverse engineering without getting towards analysis methodology. Also through business model analysis, several results were derived [30].

Francesco Mercaldo et al. detected ransomware according to threat and implemented characteristic guidelines of ransomware in malicious code to suggest methodology according to official method that can identify characteristics. The technique was suggested based on official method without paying the fee for the encryption key in the infected android platform environment. It is a method where based on sample, data sets are composed and identified, and there is need for future research to expand solutions in race environments [31].

Siegfried Rasthofe et al. explained 20,000 new malicious codes infected in Korea based on android and the analysis technique. The study identified, compared, and analyzed malicious codes distributed through emails, attached files, SMS spam, etc. Also they wrote about a vulnerability that influences all android versions through tapjacking attacks done through Android/Bad Accents malicious code [32].

3 CloudRPS

In this chapter, we discuss our proposed CloudRPS including CloudRPS architecture, service scenario, case studies, and performance analysis in details.

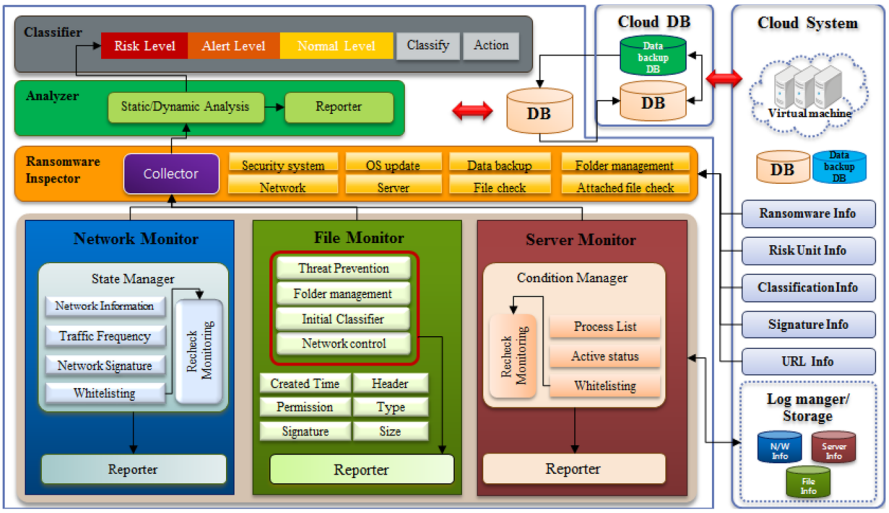

Fig. 1 Architecture of CloudRPS

3.1 Architecture

The proposed CloudRPS collects information from the cloud system and analyzes it to prevent ransomware attacks. The proposed system consists of six components: classifier, analyzer, ransomware, inspector, network monitor, file monitor, and server monitor. The following Fig. 1 presents the structure of the proposed system.

The classifier categorizes the data transmitted from the network monitor, files monitor, server monitor, and analyzer modules according to threat level and relays the information to the DB (Databases). To classify is to categorize the threat of ransomware by severity. The action feature relays the blocking order for the detected ransomware to the cloud system. The risk level and alert level are elements of the classifier that signify the threat level of the malicious code. The normal level refers to a safe level. The risk level refers to the discovered malicious code, and the alert level is an element that categorizes the warning level within the user system.

The analyzer consists of static analysis, dynamic analysis functions and reporter. There are analyses through the file's signature and through the hash value under static analysis. The under dynamic analysis methods are sandbox, activity-based detection technology. This module conducts a secondary analysis for files, traffic and ransomware. When the analysis is complete, information is provided to the Classifier.

The ransomware Inspector reviews the user system's status and manages the system state and information. The ransomware prevention factors include Security system, OS update, data backup, network, server, file check, and attached file check. The information of the relevant elements is synchronized in real time through the Cloud system to provide confidence.

The network Monitor analyzes the traffic inside the user system and reports on it. A state manager has the elements of network information, traffic frequency, network signature, and whitelisting, and analyzes the traffic and ransomware. Through the network information, the network composition, web page and browser can be verified. The network monitor module can extract as a file the traffic suspected of being malicious. Moreover, the traffic frequency refers to the set maximum traffic for network composition equipment. The network signature stores the malicious network traffic and ransomware's signature. Whitelisting has the information on the authorized traffic and ransomware. To detect disguised the traffic and ransomware using whitelisting, recheck monitoring is conducted to detect and respond to malicious codes and abnormal activities.

The file Monitor is the module that monitors files. It consists of threat prevention, folder management, and initial classifier, network control, and reporter features. Threat prevention helps the PC updating the patch for the security of programs used on the PC. The folder management automatically hides the shared folder and only allows authorized users to access it. The initial classifier monitors the user's file operation and categorizes dubious processes as the first step. The network control controls the application's network connections. The reporter relays the analysis results of the file or information on its behavior. The file is also monitored for its size, form, signature, revisions or generation time.

The server monitor consists of Condition Manager and Reporter components. Condition Manager checks the server's status through process list, active status, and whitelisting. Through each server's process list, the activities that are carried out in a specific server can be viewed. Through Active status, servers' activities can be monitored, and through whitelisting, malicious codes of the data that access the server or abnormal activities can be detected.

The cloud DB has the role of synchronizing DB and data backup within cloud system and through independent management when there is stability or cloud system attacks, availability is secured and it provides data when conducting system inspection tracking.

The cloud system offers real-time synchronization using ransomware, threats and categorization information. The information is managed through the DB and when infected by ransomware, to ward off the possibility of not being able to decrypt after infection. The user's data is backed up in real time through the DB. *The log manager* and *the storage* receive the log on files or traffic detected for the threats of malicious codes. These are received from network monitor, file monitor, and server monitor and then analyzed. Through the analysis the audit trail is concluded to find the end-point where the malicious software is currently installed. In addition, from the network monitor, file monitor, and server monitor, it saves information on the network, file and server. If there is suspicion of a malicious code or abnormal activity later on, the saved information is transmitted to a different module to help with the analysis. Also, approach is done through hypervisor rather than approaching system resources for devices through system internal virtualization and makes it difficult to approach from the exterior by operating within each virtualized domain. Through this function, malicious and abnormal behaviors are analyzed and functions are provided for sample code collection.

Table 2 Definition of acronyms

Term	Explanation
CS	Cloud system
DB	Databases
RI	Ransomware inspector
AN	Analyzer
CL	Classifier
Backup DB	Data backup DB
SM	Server monitor
NM	Network monitor
FM	File monitor

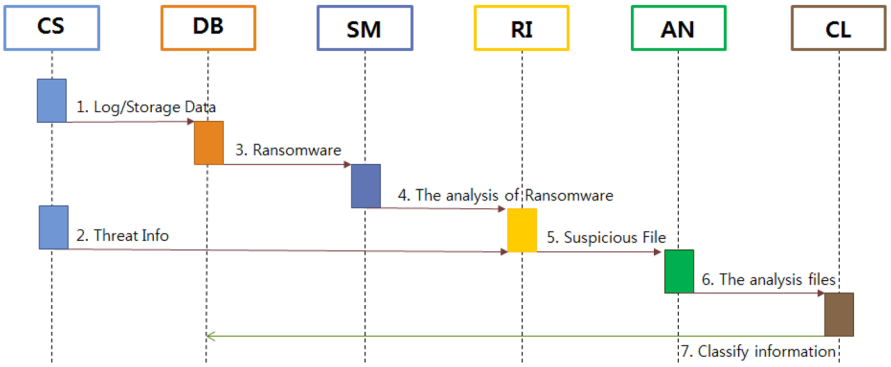

Fig. 2 Detection scenario of server side

3.2 Service scenarios

This section discusses the service scenario for the proposed the CloudRPS. The acronyms used here are as in Table 2.

Figure 2 shows detection scenario for the ransomware security threats and requirements as mentioned in Sect. 2.3.

The Fig. 2 shows detection scenario for the ransomware attack's server-based security threats and requirements as mentioned in Sect. 2.3. The DB collects data from an external cloud system then transmits it to the server monitor. SM detects ransomware malicious and abnormal behavior through monitoring. Behavior detected through SM is tested through RI and suspicious files are delivered to the AN. AN, through initial analysis of this information, verifies whether there is a ransomware infection. The ransomware that is ruled as malicious is sent to the CL. The CL categorizes the ransomware by threat level and this information is sent to the DB.

The ransomware attacks happen through infection of websites or attached files to email. Usually, the attacks can be prevented only when the network reinforces security. The Fig. 3 shows detection scenario for the network-based security threats and requirements as mentioned in Sect. 2.3. In Fig. 2, the threat information travels

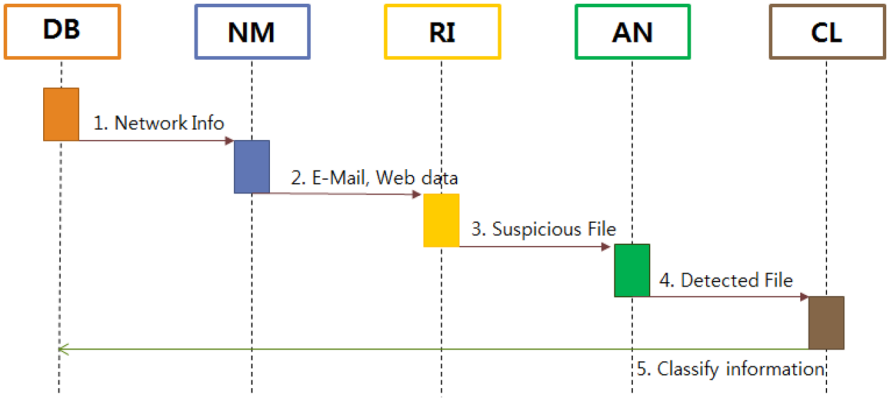

Fig. 3 Detection scenario of network side

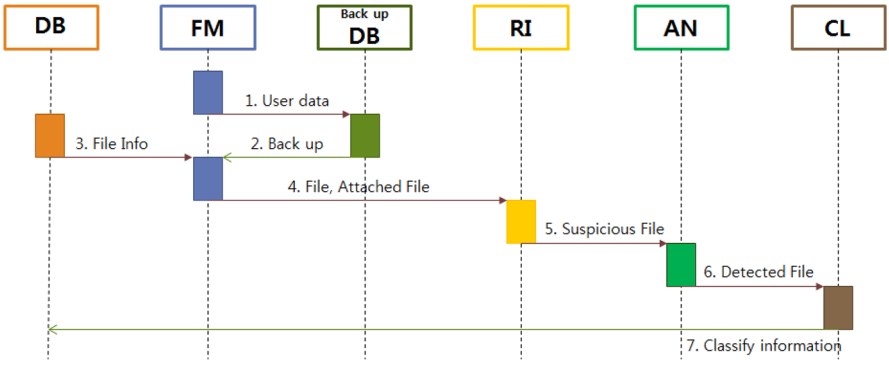

Fig. 4 Detection scenario of file side

from the cloud system to the log, while storage information goes to the DB and threat information goes to NM. From the DB, the threat information such as ransomware transmitted via emails or websites, risk and classification is collected and forwarded to NM. The NM analyzes the traffic and when abnormality is detected the file is extracted from the network stream. The AN uses various analysis methods to rule whether there is a malicious code infection of the files. If a file is determined to be ransomware, this information is sent to the CL and CL categorizes the detected threat according to its severity. This is then sent to DB for synchronization.

The Fig. 4 shows a scenario where server-based threats and requirements in the ransomware attack as mentioned in Sect. 2.3 is shown. In Fig. 2, information traveled from the cloud system to the log, and storage information traveled to the DB, while threat information was provided to the NM. File detection and response is done through FM. FM stores user data through backup DB and when the backup is complete it is provided with file information for monitoring through DB. FM delivers execution file, but that is file, etc. to RI and after primary inspection, delivers to RI. The AN primarily categorizes the existing file to the user through the initial classifier. For files where abnormal activity has been detected, this information is forwarded to the AN for

analysis on whether it is malicious. If a file is deemed malicious, then it is forwarded to CL and CL identifies the threat level and sends it to DB so that this information can be synchronized with the file.

3.3 Case studies

This section shows a ransomware attack case that is defended using the CloudRPS. Case1 prevents infection by monitoring the conversion of large quantity files in a windows environment then alerting the user. Case2 shows prevention of infection through a prior test of the execution and attached file to be downloaded from email or a website.

Case 1: The detection of malicious activity through monitoring of conversion of large quantity files in the windows environment

The Fig. 5 shows a scenario where the CloudRPS is used to defend against an early stage intrusion, when conversion of a large size file is detected through the monitoring of the network or file. In an operating system, if a large amount of data is converted, the CloudRPS starts to conduct an analysis in advance. At this point, the existing data is backed up through the cloud system is the data backup DB. To verify whether there is a malicious code the pre-processing step and threat components are extracted. The information is received from the data base that has the existing ransomware's information, threat information and classification information, and it is then categorized into the risk level, alert level, or normal level. For accurate detection, other application programs are terminated. Based on the level identified, the data is classified to defend against ransomware. The detected ransomware is stored in the database after analysis. On Ransomware information stored in the database, real-time update is done. When it is not detected through prevention defense, infection status is confirmed and when it is not infected, continuous monitoring is done. On the other hand, if it is infected, decrypted file with the corresponding extension is moved to a certain folder and restoration is conducted. If restoration is not done, through data backup DB of CloudDB, data is restored and when the restoration is done successfully, continuous monitoring is conducted.

Case 2: The detection of malicious activity through tests on the execution files

When an email arrives, monitoring of the network and the file takes place as well as mirroring onto the CloudRPS. The mirrored data is analyzed by the CloudRPS. Before the user reads the email, it is sent to the File monitor. If an attached file is downloaded or a linked web page is visited for downloading a file, the user will end up downloading a malicious code. Whenever an email moves, the log is sent to the CloudRPS and analysis is constantly conducted. The file to be executed is tested prior and if the file monitor detects malicious software then the CloudRPS informs the user of infection and shows the trace of malicious codes through the log information. For accurate detection, other application programs are terminated. The CloudRPS, by tracing the infection path, deletes the malicious activity or abnormal activity from all terminals that are along the infection path, thus removing the threat of additional infection. When malicious or abnormal behaviors are not removed, restoration is connected. If

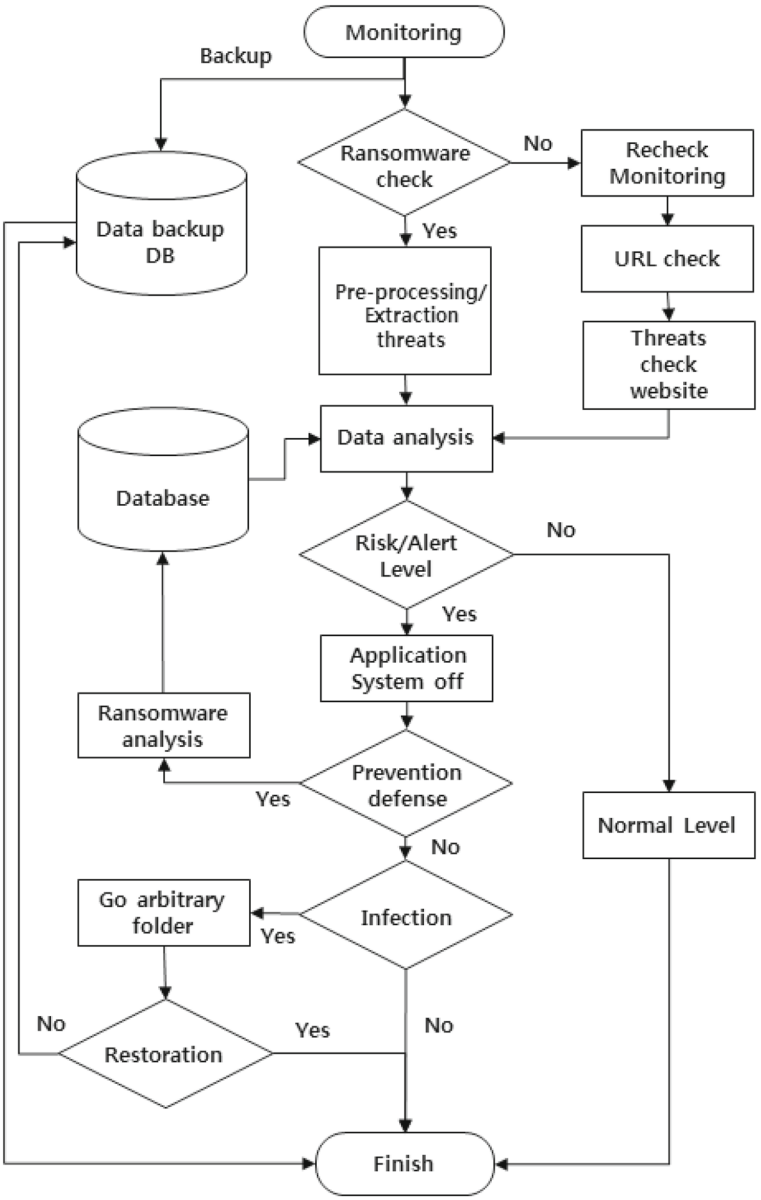

Fig. 5 Detection of malicious activity through monitoring of conversion of large quantity files in the windows environment

restoration is not completed, through data backup DB of CloudDB, data is restored and when the restoration is done successfully, continuous monitoring is conducted. Figure 6 shows a scenario where the file monitor is used to defend against CloudRPS during a detection of malicious activity through tests.

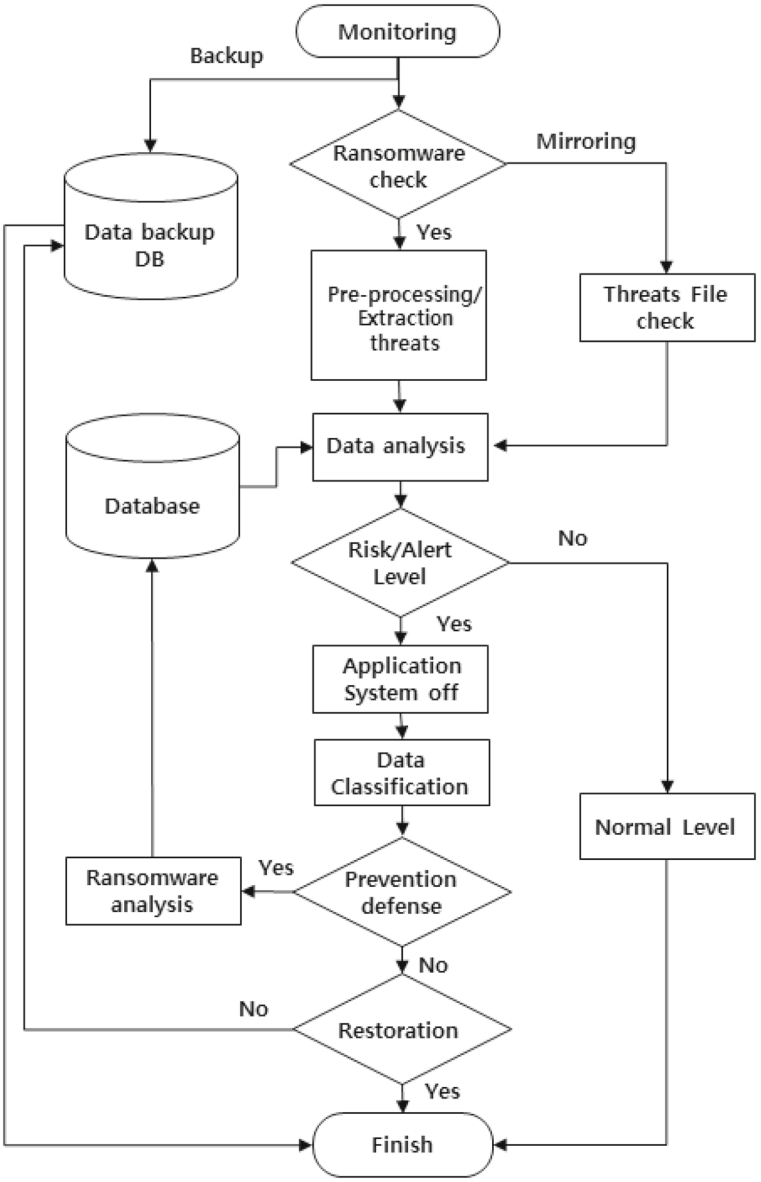

Fig. 6 Detection of malicious activity through tests on the execution and attached files

3.4 Performance analysis of CloudRPS

This section conducts an analysis on the proposed system based on key components in security considerations (Table 3).

The research [27] can detect and respond to various ransomware attacks based on server, network, and file using monitoring of filesystem operation as a counter-

Table 3 Comparison among the existing researches and our proposed CloudRPS

Researches							
Characteristics	Amin et al. [27]	Tianda et al. [28]	Mohammad et al. [29]	Alexandre et al. [30]	Francesco et al. [31]	Siegfried et al. [32]	CloudRPS
Server-based detection and response	△	△	△	△	△	△	◎
Network-based detection and response	○	◎	○	△	○	○	◎
File-based detection and response	○	◎	○	○	○	△	◎
Real-time updates	△	○	△	△	△	△	◎
Accuracy	○	○	◎	△	○	○	◎
Reliability	○	◎	○	△	○	△	○
Availability	○	○	△	△	△	△	◎

(◎: good, ○: middle, △: weak)

measure. In the proposed method, it is difficult to conduct response and detection on distribution and attacks through URL such as network, server and new variants in the research [28] analyzed ransomware characteristics to suggest an automated analysis method. It conducts file analysis through dynamic and static analysis and monitoring through collecting domain information through blacklist method but it is only possible to detect when there are analyzed samples. Other researches [29,31,32] categorized various ransomware types. However, ransomware that does not encrypt user data cannot be seen as different from general malicious code. Furthermore, in the research [29], response and detection in categorizing characteristics based on extracted samples to prevent ransomware attacks in the process of exchanging keys is difficult if there is no sample or information about ransomware. There are difficulties in detecting and responding to ransomware attacks distributed in various forms in some researches [28–32]. On the other hand, our proposed CloudRPS uses server, network, and file based detection and response; it is possible to respond to various attack methods. For ransomware distributed through web browsers and pages such as network and server, network monitor on masked data and whitelisted data and abnormal behavior detection through server monitor is possible. Real-time updates represent the degree of updates of the analysis data for malicious or abnormal behavior detection. If there is no real-time update of things such as new and very and ransomware information, thread information, signature values, and URL information, response and detection can become difficult and become security vulnerabilities. The existing researches [27–32] do not provide real-time updates, while the proposed system provides real-time updates through cloud system which is convenient for response and action. Accuracy is the degree of occurrence of errors through detection. To provide accuracy, various detection and response methods based on numerous data is required. The proposed system provides ransomware related information and thread information, and necessary information for detection and response in real time through cloud system. Also because it detects and responds based on server, network, and file through attack technique and prevention technique analysis on ransomware distribution which means accuracy is superior to the existing researches. Reliability represents independent management of analysis information within various security threats while executing inherent functions of detection systems without influencing other systems. The research [27] group through samples to detect zero-day attacks of ransomware, it does not affect other systems but when there are network, server attacks detection and response is difficult and analysis data is not independently managed. The researches [28,31,32] discussed malicious code analysis on mobile environment. The research [28] analyzes APK files through dynamic and static analysis and maintains reliability by conducting blacklist method and monitoring. The researches [29,31,32] prevents user data encryption based on categorized ransomware but it only researched about detection system analysis and not mentioned about reliability. However the proposed system through independent information management through CloudDB, even if attacks are made on the system, data is managed synchronized and can be protected. When malicious or abnormal behaviors are detected, to provide highly accurate detection, other application programs are terminated and then detection and response is conducted. Availability of detection system represents the ability to perform detection function without delay or disability using detection system function. Compared to the existing

all researches, our proposed system has high availability while conducting detection and response. Because the researches do not have consideration about attacks on system, there is poor availability in detection and response function fusion. However, the proposed system considers independent management of cloud system virtualization and CloudDB independence management to acquire availability. Also through CloudDB system inspection and tracking is possible. Therefore, the proposed system has strong availability.

4 Conclusion

There are too many direct or indirect damages by cyber threats - leakage of the private information, leakage of the corporate confidential information, monetary loss, etc. Among the cyber threats, ransomwares attacks target not only anonymous people but also specific organizations or social classes. When the attacks have been successfully done, the attacks encrypt the information so that the attacker can gain monetary benefits. Because the decryption key is known only to the attackers, it is very difficult to respond for the attacks.

In this paper, we discussed various methods of the attacks by showing cases of the ransomware attacks and presented the need for an in-depth detection system. In addition, we proposed a CloudRPS that monitors the network, the file and the server. The CloudRPS is installed in a cloud system that can analyze the network information, the file information, the server information, the ransomware, and the logs to defend against the attacks. This system conducted monitoring of the network, file, and server in the real time and through the data backup DB, it backs up user's data in real time to defend against the ransomwares. Therefore, a more advanced detection and minimization of the damage can be achieved. In addition, accuracy and reliability was increased through cloud system, and availability was increased through CloudDB. As a result, attack damage caused by the ransomware can be reduced and it can be used as detection and response plans for various malicious codes.

We expect that our research will have a positive effect on not only the IT industry but also the development of many industries converged with IT in the near future research. Finally, it is needed for a follow-up study in which an advanced algorithm can decrypt mutant ransomware as well as normal ransomware.

Acknowledgements This work was partly supported by Institute for Information & communications Technology Promotion(IITP) Grant funded by the Korea government(MSIP) (No.R-20160222-002755, Cloud based Security Intelligence Technology Development for the Customized Security Service Provisioning) and This research was supported by the MSIP(Ministry of Science, ICT and Future Planning), Korea, under the ITRC(Information Technology Research Center) support program (IITP-2016-H8501-16-1014) supervised by the IITP(Institute for Information & communications Technology Promotion).

References

1. Jang-Jaccard J, Nepal S (2014) A survey of emerging threats in cybersecurity. J Comput Syst Sci 80(5):973–993
2. Furnell S, Emm D, Papadaki M (2015) The challenge of measuring cyber-dependent crimes. Comput Fraud Secur 2015(10):5–12

3. Jingle IDJ, Rajsingh EB (2014) ColShield: an effective and collaborative protection shield for the detection and prevention of collaborative flooding of DDoS attacks in wireless mesh networks. Hum. Centric Comput. Inf. Sci. 4(1) 1–19
4. Feng L, Liao X, Han Q, Li H (2013) Dynamical analysis and control strategies on malware propagation model. Appl Math Model 37(16–17):8225–8236
5. Symantec (2014) Internet security threat report. http://www.symantec.com/security_response/publications/threatreport.jsp
6. Andronio N, Zanero S, Maggi F (2015) HELDROID: dissecting and detecting mobile ransomware, RAID 2015, LNCS 9404, pp 382–404
7. Everett C (2016) Ransomware: to pay or not to pay? Comput Fraud Secur 2016(4):8–12
8. Elsevier Network security (2016) Ransomware expands, attacks hospitals and local authorities, and moves to new platforms. 2016(3):1–2. Editied by Steve Mansfield-Devine, Publishing Director: Bethan Keall. http://www.sciencedirect.com/science/article/pii/S1353485816300228
9. Nath HV, Mehtre BM (2014) Static Malware analysis using machine learning methods. Second International Conference SNDS 2014 Proceedings, Communications in Computer and Information Science, vol 420, pp 440–450
10. Cisco (2015) Ransomware on steroids: Crytowall 2.0. http://www.blogs.cisco.com/security/talos/crptowall-2
11. Threatpost (2013) Researchers uncover affiliate network for ransomware, by Tom Spring. https://www.threatpost.com/researchers-uncover-affiliate-network-for-ransomware/118452/
12. Journal Network Security (2015) Ransomware defeated but new forms emerge. 2015(11). Editied by Steve Mansfield-Devine, Sarah Gordon, Publishing Director: Deborah Logan. http://www.dl.acm.org/citation.cfm?id=2850884
13. Narudin FA, Feizollah A, Anuar NB, Gani A (2014) Evaluation of machine learning classifiers for mobile malware detection. Soft Comput Methodol Appl 20(1):343–357
14. Gazet A (2010) Comparative analysis of various ransomware virii. J Comput Virol 6(1):77–90
15. Microsoft. File system minifilter drivers. https://www.msdn.microsoft.com/enus/library/windows/hardware/ff540402%28v=vs.85%29.aspx,2014
16. Spagnuolo M, Maggi F, Zanero S (2014) BitIodine: extracting intelligence from the bitcoin network. Financial cryptography and data security (FC 2014), LNCS, vol 8437, pp 452–463
17. Xing X, Meng W, Lee B, Weinsberg U, Sheth A, Perdisci R, Lee W (2015) Understanding malvertising through Ad-injecting browser extensions. WWW '15 Proceedings of the 24th International Conference on World Wide Web, pp 1286–1295
18. Sood AK, Enbody RJ (2011) Malvertising—exploiting web advertising. Comput Fraud Secur 2011(4):11–16
19. Symantec (2013) Massive malvertising campaign leads to browser-locking ransomware. http://www.symantec.com/connect/blogs/massive-malvertising-campaign-leads-browser-locking-ransomware
20. Malware don't need Coffee (2015) Guess who's back again? Cryptowall3.0. http://www.malware.dontneedcoffee.com/2015/01/guess-whos-back-again-cryptowall-30.html
21. Cabaj K, Gawkowski P, Grochowski K, Osojca D (2015) Network activity analysis of CryptoWall ransomware. PRZEGLAD ELEKTROTECHNICZNY 2015(15):201–204
22. Dell secureworks (2014) Cryptolocker ransomware. http://www.secureworks.com/cyber-threatintelligence/threats/cryptolocker-ransomware/
23. Mansfield-Devine S (2014) Tor under attack. Comput Fraud Secur 2014(8):15–18
24. Cisco (2015) Threat spotlight: TeslaCrypt—decrypt it yourself. http://www.blogs.cisco.com/security/talos/teslacryptj
25. RanCERT (2015) https://www.rancert.com/bbs/bbs.phpmode=view&id=18&bbs_id=case&page=2&part=&keyword=
26. EnigmaSoftware (2016) locky File extension' ransomware. http://www.enigmasoftware.com/lockyfileextensionransomwareremoval/
27. Kharraz A, Robertson W, Balzarotti D, Bilge L, Kirda E (2015) Cutting the Gordian knot: a look under the hood of ransomware attacks. Detection of Intrusions and Malware, and Vulnerability Assessment(DIMVA): 12th International Conference, pp 3–24
28. Yang T, Yang Y, Qian K, Lo DCT, Qian Y, Tao L (2015) Automated Detection and Analysis for Android Ransomware. In: HPCC-CSS-ICESS '15 Proceedings of the 2015 IEEE 17th International Conference on High Performance Computing and Communications, 2015 IEEE 7th International Symposium on

Cyberspace Safety and Security, and 2015 IEEE 12th International Conf on Embedded Software and Systems. IEEE Computer Society Washington, DC, USA, pp 1338–1343
29. Ahmadian MM, Shahriari HR, Ghaffarian SM (2015) Connection-monitor & connection-breaker: a novel approach for prevention and detection of high survivable Ransomware. In: 12th International ISC Conference on Information Security and Cryptology (ISCISC 2015), pp 79–84
30. Gazet A (2010) Comparative analysis of various ransomware virii. J Comput Virol 6(1):77–90
31. Mercaldo F, Nardone V, Santone A, Visaggio CA (2016) Ransomware steals your phone. Formal methods rescue it. In: Lecture Notes in Computer Science, vol 9688. pp 212–221
32. Rasthofer S, Asrar I, Huber S, Bodden E (2015) How current android malware seeks to evade automated code analysis. 9th IFIP WG 11.2 International Conference, WISTP 2015, Heraklion, Crete, Greece, August 24–25, 2015. Proceedings, Information Security Theory and Practice, vol 9311, pp 187–202