Journal of Reliable Intelligent Environments (2019) 5:67–89
https://doi.org/10.1007/s40860-019-00080-3

REVIEW

Systematic literature review and metadata analysis of ransomware attacks and detection mechanisms

Abdullahi Mohammed Maigida[1] · Shafi'i Muhammad Abdulhamid[1] · Morufu Olalere[1] · John K. Alhassan[1] · Haruna Chiroma[2] · Emmanuel Gbenga Dada[3]

Received: 2 January 2019 / Accepted: 20 April 2019 / Published online: 3 May 2019

Abstract
Ransomware is advanced and upgraded malicious software which comes in the forms of Crypto or Locker, with the intention to attack and take control of basic infrastructures and computer systems. The vast majority of these threats are aimed at directly or indirectly making money from the victims by asking for a ransom in exchange for decryption keys. This systematic literature analysed the anatomy of ransomware, including its trends and mode of attacks to find the possible solutions by querying various academic literature. In contrast to previous reviews, sources of ransomware dataset are revealed in this review paper to ease the challenges of researchers in getting access to ransomware datasets. In addition, a taxonomy of ransomware current trends is presented in the paper. We discussed the articles in detail, the evolution and trend in ransomware researches. Most of the techniques deployed could not completely prevent ransomware attacks because of its obfuscation techniques, but rather recommend proper and regular backup of important files. This review can serve as a benchmark for researchers in proposing a novel ransomware detection methodology and starting point for novice researchers.

Keywords Ransomware · Crypto ransomware · Locker ransomware · Cyber-attack · Malware · Ransomware detection

1 Introduction

Ransomware is a type of malware that restricts access to the infected computer system. This is a form of technological blackmail that exploits software and hardware vulnerabilities, sometimes, via drive-by attacks on maliciously crafted web pages. It comes in the form of Cryptolocker, CryptoWall, CryptoDefense or Manamecrypt [62]. They employed strong encryption to scramble nearly every files they targeted, mostly in document storage formats such as office, PDF, CSV, making them impossible to recover without the unique, private key used to encrypt them. The cracker then puts up a display note on the computer screen explaining the processes to follow to recover the decrypted files after payment which will mark the end of the cryptovirology [23, 37, 43].

On the side of ransomware producers, one of the most important issues is to prolong the lifetime of the malware in the wild, as much as possible. It is achievable if the ransomware is able to abscond from the antivirus scanner engines well. Consequently, the camouflage of the malware code is a significant factor to make it successful in the wild. Malware's main weakness is its source code. If the source code is revealed through decompiling or disassembling, anything about the malware is laid bare. The ransomware attacks have a serious negative impact on information technology infrastructure. The impacts of these attacks include system

✉ Shafi'i Muhammad Abdulhamid
shafii.abdulhamid@futminna.edu.ng

Abdullahi Mohammed Maigida
mohammandin@gmail.com

Morufu Olalere
lerejide@futminna.edu.ng

John K. Alhassan
jkalhassan@futminna.edu.ng

Haruna Chiroma
freedonchi@yahoo.com

Emmanuel Gbenga Dada
gbengadada@unimaid.edu.ng

[1] Department of Cyber Security, Federal University of Technology, Minna, Nigeria

[2] Department of Computer Science, Federal College of Education (Technical), Gombe, Nigeria

[3] Department of Computer Engineering, University of Maiduguri, Maiduguri, Nigeria

shutdown of most organization, data or information loss as a result of file encryption, financial cost to the companies for incident response and other security-related issues and loss of life due to unexpected shutdown of some important medical equipment [7, 21, 22].

The negative impact of the ransomware prompted researchers to deploy efforts in a bit to find a lasting solution to these attacks being perpetrated by the ransomware [24, 27, 53]. In turn, the proposed solutions are expected to drastically reduce its negative impact, prevent the attack or if possible eliminate it from existence. As a result of finding solution to ransomware, analysis on ransomware activities including its attack model, encryption types, Bitcoin usage, mode of operation, prevention and protection mechanism flooded the literature. However, lasting solution to ransomware is yet to become a reality despite that the massive efforts have been deployed by researchers [12, 15, 36].

There are previous systematic reviews on ransomware in the literature. However, the major issue with those previous reviews is that they mainly concentrated on ransomware in healthcare sectors and some other specific areas, whereas it is well known that ransomware has no domain boundary.

In this paper, we propose to conduct a comprehensive systematic review of all analysis carried out on ransomware activities which include its attack model, encryption types, Bitcoin usage, mode of operation, prevention and protection of users, facilities, infrastructure and environment as shown in Fig. 1.

The purpose for this review work is to have a clear view on the mode of attack, structure, composition, makeup and the behaviour of various ransomwares, to understand the factors that made ransomwares to grow in both complexity and multiplicity, and to see what the experts researchers are saying and doing to curtail the excesses of ransomware. The major contributions of the paper are as follows:

- We create taxonomy of ransomware attack techniques.
- We analysed the parameters used for the evaluation of ransomware attack, defence and detection mechanisms.
- We summarized and tabulate all available research datasets for future analysis of ransomware anatomy.
- We present a systematic literature review of ransomware attacks and detection mechanisms.

The remaining parts of the paper are organized as follows: Sect. 2 presents a detailed analysis of previous related surveys. Section 3 details the research methodology, whereas Sect. 4 presents the taxonomy of ransomware attacks. In Sect. 5, the analysis of datasets used for ransomware evaluation was done. Further discussion was done in Sect. 6 before concluding the paper in Sect. 7.

Table 1 shows a list of abbreviations and their meanings used in the paper.

2 Previous related surveys

This section presents previous related surveys in the area of ransomware research as shown in Table 2 and Fig. 2. Gupta and Tripathi [23] created awareness among the unskilled computer users on the dangers of ransomware activities to organizations. The authors listed the potential threat posed by the malware which includes system shutdown due to infection, data or information loss, financial cost and sometimes loss of life. It proposed several mitigating techniques and controls among its safeguard knowledge which should include email security, intrusion prevention, download insight, browser protection, exploit protection and adoption of best practice. However, Hernandez-Castro et al. [25] in his submission analysed the economic analysis of Cryptolocker, CryptoWall, TeslaCrypt and other major strands on their price discrimination and strategy considering the value and volume of data available at their disposal. This encourages the criminal to demand more but with proper and constant data backup, it will dissuade the attacker from their illicit act. Mercaldo et al. [39, 40] dwelled on the analysis of android environment because of its ease of attack by ransomware and other malwares and proposed a method of model checking that will automatically dissect malware samples through the adoption of manual scrutiny of their

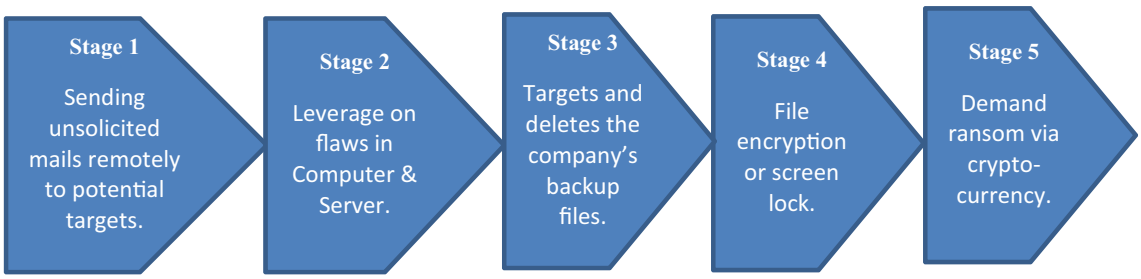

Fig. 1 Stages of ransomware attacks

Table 1 Abbreviations and meanings

Abbreviations	Meaning
ACM	Association for computing machinery
AES	Advance encryption standard
APK	Android package kit
AV	Antivirus
BBT	Bayesian believe network
BIOS	Basic input/output system
C&C	Command and control
C-I-A	Confidentiality, integrity and availability
CMP	Configuration monitoring and processing
CPU	Central processing unit
CRA	Cyber routine activities
CSV	Comma separated values
DNS	Domain name system
DRF	Diagnostic risk factor
EMV	Eurocard, master and visa
FCM	Frequency centric model
FPR	False-positive rate
FSRM	File server resource manager
FSRM	File server resource manager
GDP	Global domestic product
HEK	Hybrid encryption key
HIPS	Host intrusion prevention system
HSR	High survivable ransomware
HTML	Hypertext markup language
HTTP	Hypertext transfer protocol
I/O	Input/output
ICS	Industrial control system
IDS	Intrusion detection system
IEEE	Institute of electrical electronic engineering
IoT	Internet of things
LSR	Low survivable ransomware
MAC	Macintosh
MFT	Master file table
MSC	Malice score calculation
OS	Operating system
PRPB	Policy recursive-folder, process and monitoring
PUP	Potentially unwanted program
RADDAR	Real-time automation to discover, detect and alert of ransomware
RDP	Remote desktop control
ROI	Region of interest
RSA	Rivest–Shamir–Adleman
SDN	Software define network
TPR	True-positive rate
VLAN	Virtual local area network
VM	Virtual machine
VSS	Volume shadow copy services
vssadmin	Volume shadow services administrator

behaviour by applying some set of logic rules to identify some set of ransomware samples.

Upadhyaya and Jain [57] discussed the anatomy and nature of the ransomware family that usually blocks the task manager, commands prompt and other executable files and renders the potential system unusable. The paper streamlines its focus on CTB Locker, analyses its mode of attack and how it creates its Bitcoin wallet per victim and mode of payment using the Tor gateway. Some physicist proposed the design of quantum cryptography systems that would be devoid of loopholes which look like a mirage, while others recommend prior protection of digital asset before attack and regular backup as the best solution. Furthermore, Gagneja [21] presents various ways that ransomware exploits system security vulnerabilities to spread infections through some running outdated application on victims computer. It subsequently removes the backup files and directories to prevent system restored and finally encrypt the system files. It suggested regular training of personnel on system security issues, update of patches, installation of firewall, email scanning and the use of licensed operating system for prevention against ransomware attack. Bhardwaj et al. [9] throw light on how cyber criminals utilized traffic redirection, infected email attachment, Botnets, social engineering and rendering of ransomware services in cloud computing to hold ransom on user systems. It described the digital age activities around three critical aspects which include: the use of digital data and files, the computer systems and unsecure internet. Ransomware leveraged on the vulnerabilities available on the systems to attack vital information and records to extort threat to home and organization.

Saiyed [47] talked about a new malware called crypto ransomware and analysed how it works and the way its encrypt data at rest using public key structures; it recommended the right combination of understanding the fundamentals of CryptoLocker security measure coupled with prescriptive guidance for basic prevention, detection, mitigation, and recovery controls that are beyond the normal IDS/IPS mechanism. While Richardson and North [46] bring to bear the history and evolution of the first ransomware virus called the AIDS Trojan in 1989 (also known as PC Cyborg) to the present CryptoLocker family, it also touched on the ranking of the country that is most affected (USA–Turkey) and discussed the discrepancy for or against the payment of ransom which largely depends on the importance of the files and the level of backup. Similarly, Formby et al. [20] directed their research on the emerging trend in high profile attacks on hospitals by ransomware. It indicated that the perceived absence of threat on the industrial control system (ICS) over a long period of time and lack of regular update of their network systems contributed to the exposure of confidential information to the hackers. It is on this basis that a novel system of defence against ransomware that targets programmable logic

Table 2 Related surveys on ransomware attack

S/N	References	No. of references covered	Survey focus	Taxonomy (Classification)
1	Gupta and Tripathi [23]	7	Attack and its prevention	No
2	Hernandez-Castro et al. [25]	29	Economic analysis	Yes
3	Mercaldo-Nardone et al. [39, 40]	32	Inside out	Yes
4	Upadhyaya and Jain [57]	10	Legality, ransomware, underground web and bitcoin wallet	Yes
5	Gagneja [21]	14	Building defense system-specific to healthcare institutes	Yes
6	Bhardwaj et al. [9]	13	A rising threat of new age digital extortion	Yes
7	Saiyed [47]	4	CryptoLocker	Yes
8	Richardson and North [46]	71	Evolution, mitigation and prevention	Yes
9	Formby et al. [20]	17	Ransomware for industrial control systems	No
10	Deloitte [17]	41	Holding your data hostage (Deloitte)	Yes
11	Securities and Commission [50]	7	Ransomware alert	No
12	Wyke and Ajjan [59]	1	The current state of ransomware	Yes
13	Kruse et al. [34]	38	Systematic review of modern threats and trends	No
14	Savage et al. [48]	14	The evolution of ransomware (Symantec)	Yes
15	Demuro [18]	416	Ransomware negotiation in the healthcare industry	No
16	Laszka et al. [35]	36	On the economics of ransomware	No
17	Smith [54]	40	Ransomware incident response for law enforcement	Yes
18	Yaqoob et al. [60]	90	The rise of ransomware and emerging security challenges in the Internet of Things (IoT)	Yes
19	Brewer [10]	4	Detection, prevention and cure of ransomware	No
20	Sgandurra et al. [51]	45	Automated dynamic analysis of ransomware	Yes

controllers in hospitals was designed coupled with strong policies that will mitigate against future attack.

Deloitte [17] reviewed the history of ransomware and categorized them into two, namely: locker which lock the systems after infection and Crypto which encrypt system files and they both demand ransom to unlock and decryption code. It described common infection vectors and ransomware types and proposed strategies for detection, remediation, and recovery. Furthermore, Securities and Commission [50] examined ransomware attack known as WannaCry or Wanna Decryptor whose findings show how it compromised the enterprise servers through Microsoft Remote Desktop Protocol (RDP)3 and the exploitation of some critical Windows Server Message Block to carry out its nefarious activities. Sometimes it deployed phishing and pharming techniques on emails and malicious websites. Protection against the WannaCry ransomware would require the review of the alert published by the United States Department of Homeland Security's Computer Emergency Readiness. Also, it requires evaluation of applicable Microsoft patches for Windows XP, Windows 8, and Windows Server 2003 operating systems for effective protection. Wyke and Ajjan [59] focus on the insight into the current state of ransomware and present a detailed analysis of the four most prevalent variants—CryptoWall, TorrentLocker, CTB Locker and TeslaCrypt which have their roots traced back to the early days of FakeAV and Locker. It described various aspects of their operation, their infection mechanisms and the geographic distribution of each variant across the globe, as well as exploring Sophos HIPS Technology proactively blocks against crypto ransomware attack.

Kruse et al. [34] conducted a systematic review with three separate searches: CINAHL and PubMed (MEDLINE) and the Nursing and Allied Health Source via ProQuest

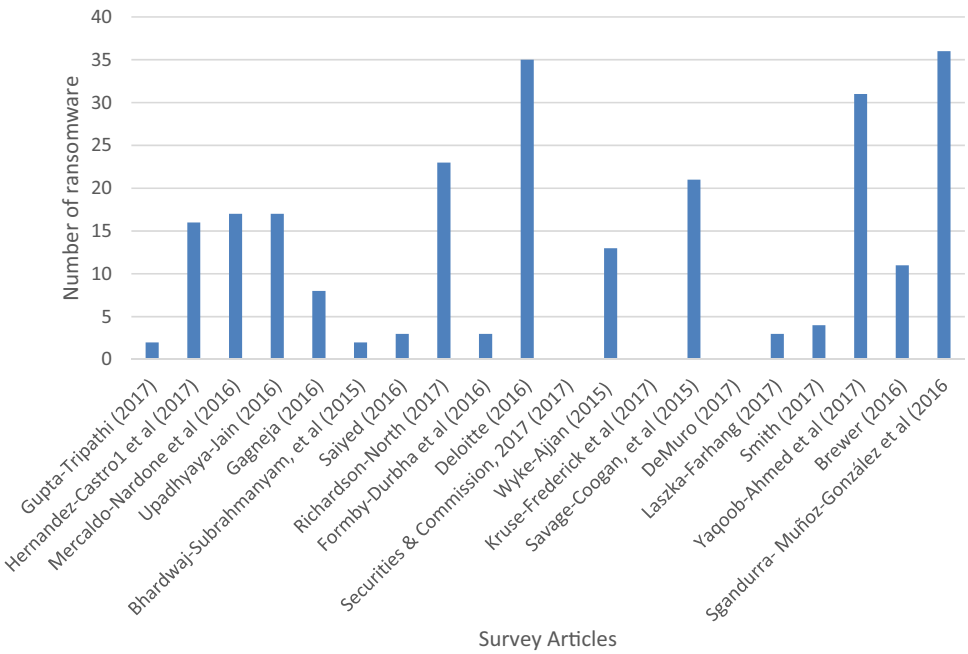

Fig. 2 Number of ransomware covered per survey articles

databases. The result shows that healthcare industry lags behind in dealing with the fundamental information security and cyber threat issues. It is noted that technological advancements and federal policy initiatives have dramatically expanded the healthcare industry's exposure to cyber. It recommended to clearly define cyber security duties, clear procedure for the upgrade of software and handling of data breaches and the use of VLANs and DE authentication and cloud computing as a mitigating factor to be taken to minimize the risk of cyber attack to the healthcare sector. Furthermore, Savage et al. [48] analysed ransomware from the technological and psychological point of view; it shows the progressive nature of ransomware from less persuasive forms through direct revenue generation using misleading applications to a more aggressive level using PC performance tools. The cybercriminals behind Ransomware target more affluent or populous countries in the hope of finding rich pickings; as a result, 11 of the top 12 countries impacted by ransomware are members of the G20 organization, representing industrialized and developing economies that make up roughly 85% of the world's global domestic product (GDP) [38]. It suggested that updating of system, application and regular training of employee on the new trends and behaviour of ransomware will help in reducing the impact of ransomware attack on organizations. Demuro [18] looked at the importance and power of law in the negotiation context, adopting clear legal principles tailored to negotiations in specific contexts will help willing and unwilling negotiators reach their desired outcome, it suggested some alternative methods such as taxing ransom payments, imposing stricter cyber testing requirements, and requiring inspections by experts in the cyber security field can be helpful legal tools to curb the ransomware problem. Laszka et al. [35] developed the first game-theoretic model of the ransomware ecosystem which captures a multi-stage scenario involving hospitals and universities facing a sophisticated ransomware attack. The model focused on key aspects of the adversarial interaction between organizations and ransomware attackers and derived under what condition a victim organization will pay the requested ransom after looking at the effort the organization put into mitigation techniques, policies, security features and level of backup will help in preventing the danger of ransomware attack. Finally, Coccaro [14] analysed the ransomware threat on law enforcement agencies because of the belief that their reputation will scare off any potential attacker against their infrastructures and unit. The research revealed several important findings in 2016, such as the number of ransomware attack, most targeted organization, available securities breaches and law enforcement agencies among the targeted organization due to lack of incident response capability. Understanding of organization structure, drafting of incident response plan, creation of a Dual-Purpose on digital forensic unit to response to lunching of internal security program agenda, combination of expert in information technology and other similar units for internal security among others will protect, prevent and mitigate against any form of cyber security breaches.

Imran et al. [28] present ransomware attacks and security concerns in internet of Things (IoT) despite its associated advantages to human activities. The research exposes the likely vulnerabilities and threat associated with the IoT devices and recommends several measures to thwart against

such threat. The proposed measures include: data integrity, lightweight security mechanisms, improve software security, upgradability and patchability features, physical protection of trillions of devices, privacy, and trust among others. Brewer [10] analysed ransomware attacks on business organizations and recommend the understanding of five distinct phases of ransomware attacks which include: exploitation and infection, delivery and execution, backup spoliation, file encryption and user notification to know the indicator of compromise (IOC) to guide in building a defence or mitigating its effect. Meanwhile, Sgandurra et al. [51] presented a framework tagged EldeRan, an accurate dynamic learning machine design to compliment antivirus. It consists of feature selection and classification phases that help in analysing and classifying both new and old variant of ransomware attacks and quick in arriving at result.

The previous survey articles revealed several recommendations that could help in tackling the spread of ransomware. Nevertheless, the articles also contain some shortcomings which could be as a result of priorities. The following are the summary of gaps found in most of the survey articles.

- Some paper focuses on the victims that are willing or unwilling to pay the ransom. However, it did not consider those who found themselves in state of dilemma who may prefer an incremental payment format as against incremental release of encrypted files. This is to avoid double jeopardy of losing out the important documents and money if they are unable to decrypt the files for use.
- Some overview papers carry out experiments which utilize manual inspection of few samples of ransomware for the preventive experiment, which cannot be used as a preventive technique.
- Other analysis of ransomware could detect and deactivate ransomware attack but could not guarantee the restoration of the infected files.
- Few other analyses can only work against a signature-based ransomware or those whose signatures have been added into the intrusion detection systems or the detection network device indicator.
- Some suggested that the use of cloud-based sandbox for malware detection could prove dangerous to the entire network systems if the sandbox is compromised by the malware; the infections could spread easily to other location of the network.
- While others have the limitation of focussing geographically on the American healthcare system.

3 Research methodology

The research methodology section presents the research steps followed to review the existing works in the area of ransomware attacks and detection systems. We also explain the selection of the existing studies which was done through a set inclusion and exclusion criteria.

Table 3 Search database sources

S/N	Sources	URL	No of articles
1	IEEE explore	URL: http://ieeexplore.ieee.org/	35
2	Google scholar	URL: https://scholar.google.com/	62
3	ACM digital library	URL: http://dl.acm.org/	43
4	EBSCOHOST	URL: http://ebsco.com/	55
5	Science direct	URL: http://www.sciencedirect.com/	63
6	Scopus	URL: https://www.scopus.com/	62
7	Springer	URL: http://www.springer.com/	44
8	Taylor and Francis	URL: http://taylorandfrancis.com/	21
9	Web of Science	URL: https://apps.webofknowledge.com/	19
10	Wiley online library	URL: http://onlinelibrary.wiley.com/	15
	Total		419

3.1 Search/data sources

Several databases were queried to gather appropriate literature related to ransomware attack, defence and mitigation techniques. The articles were properly scrutinized using identification of primary studies with other different techniques. The research procedure adopted in this article spanned through relevant papers from a variety of academic databases including ACM Digital Library, IEEE Explore, EBSCOHOST, Google Scholar, Science Direct, Scopus, Springer, Taylor & Francis, Web of Science and Wiley Online Library as shown in Table 3.

3.2 Search keywords

Kitchenham et al. [32] 's literature search strategy was adopted in this review. The primary search terms were carefully selected to ascertain the most appropriate search terms. Using the review set goals, the following terms were applied to search the relevant literature in some reputable academic archives: 'Ransomware', 'Malware', 'Malware + ransom',

Table 4 Inclusion/exclusion criteria

S/N	Inclusion criteria	Exclusion criteria
1.	The study focuses on ransomware attack, defense or detection mechanism	The study did not focus on ransomware activities
2.	The subject matter was peer reviewed and published in reputable journals or conference papers	The subject matter was not peer reviewed or published in any scholarly journals or conference papers
3.	The study is written in English language text	The study is not written in English language
4.	The articles are either published survey or research papers	The articles are neither a survey nor research papers but a news flash nor magazine publications

'Ransomware + defense', 'Wannacry, Cyber-attack', 'Cyber threats + Malware'.

3.3 Explicit inclusion and exclusion criteria

In order to have direct focus on the subject matter and to avoid biases of any kind in the review of articles, we adopted various principles in the selection of the articles which are enumerated in the Table 4.

3.4 Data collection and synthesis of results

The articles reviewed are in consonant with the reality of the day, acknowledging the growing threat of ransomware attacks in modern digital world. The devastating effect of the malware on information and information systems of most reputable companies and organizations has led to huge losses. Dealing with the threats has become a mirage of nightmare to the information security experts. The two strong drivers that led to the growth of this malwares include the ever-changing technological landscape where new information technology systems are fast implemented as compared to the security components which are meant to protect them, and lack of policy initiative, proper understanding and training of the end users on the use and application of information technology facilities.

3.5 Study selections

The procedure followed in the review of the articles starts with the definition of common terms related to cybersecurity or information security issues using search keywords in Sect. 3.2. It helps to eliminate unaligned articles with the subject matter of the proposed research work. The focus was based on research and survey articles whose subject matters related to ransomware and were writing in English Language text. The selections and the elimination criteria process are shown in Fig. 3. The entire review process went smoothly as articles were screened out based on: unrelated titles from 419 to 321; based on abstract, 321–98 and the final evaluation based on the contents and directions of the full text from 98 to 41 (Fig. 4).

Figure 5 shows the database sources of all the articles considered for the systematic review.

4 Proposed taxonomy of ransomware attacks

This is the taxonomy of ransomware attacks based on the techniques proposed in the literature presented in Fig. 6.

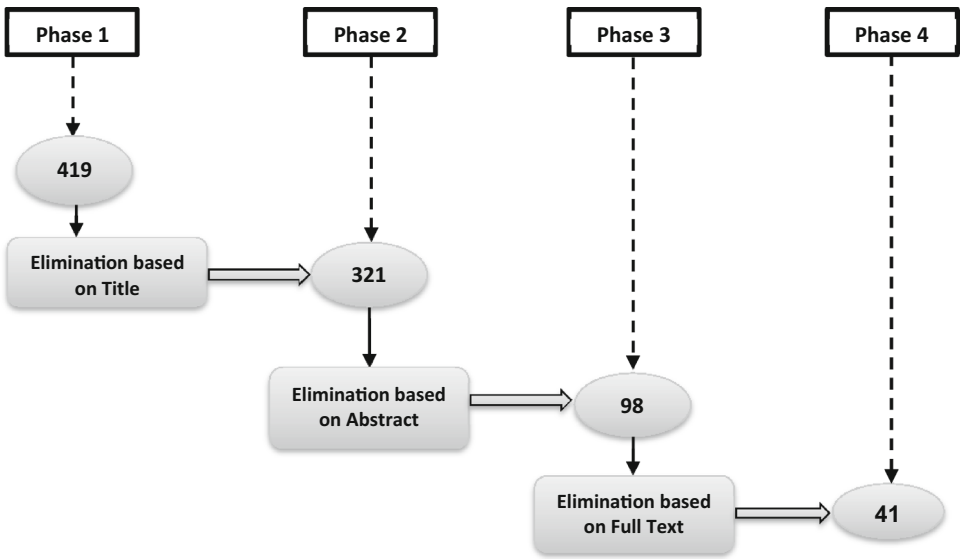

Fig. 3 Literature search process

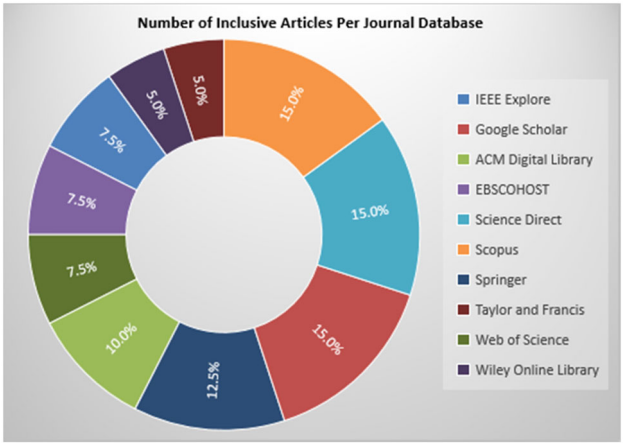

Fig. 4 Number of articles per journal database

4.1 Synthesis of crypto-based techniques

Al-rimy and Maarof [5] and Al-rimy et al. [6] put forward a well-organized outline for structuring operative framework and incorporating an adaptive anomaly detection that can handle the dynamicity style of building crypto ransomware early detection models that shield users and organization of becoming a victim of such attack. While Cabaj et al. [11] talked about a new detection method called "Software-Defined Networking" (SDN) which analysed the HTTP messages' classifications and their respective content sizes to detect threats The approach exploits feature of ransomware interaction which was based on observation from network communication of two crypto ransomware families (Cryptowall and Locky). Meanwhile, Song et al. [55] highlighted in his submission an efficient approach that can prevent the attacks of modified ransomware on Android platform. The proposed technique specifies and intensively monitors processes and specific file directories using statistical methods based on processor usage, memory usage, and I/O rates so that the process with abnormal behaviours can be detected, stop and confirm for deletion. The method is reliable and fast and does not require signatures of ransomwares to be stored in the database before it could be detected.

Yang et al. [61] described the rudimentary Android components that made it vulnerable to attack; the components include: activities, services, content providers and broadcast receivers which are all activated by an asynchronous message termed intent. An automated performance protection system with high ideal security tools which has the ability to detect active and passive malicious activities was incorporated into the system, unfortunately technical details were not comprehensively spelt out. Moore [42] worked and used Honeypot as a trap at the boundary of a setup network system to monitor the activities of several malwares including Ransomware. Honeypot is like other computer system deployed by network administrator as additional system to collect information about any potential attack; it contains a lot of attractive resources that will lure any potential malware attack to the scene; the resources and the environment are closely monitored against any changes to call for an action. Wecksten et al. [58] focussed on the four most common Crypto ransomwares (*Crypto-Wall*, *Testa Crypt, CTB Locker and Locky)* whose infections rely on tools available on the targeted system to stop a simple recovery after attack has been noticed. The article recommended renaming of the system tool "vssadmin.exe" that controls shadow copies and system restore points created before the infection took place, and will allow infected files and folders to be recovered after the system has been restored and scanned with antivirus. The paper suggested some proactive steps such as antivirus update, a well-configured firewall, updated operating system and software, and a proper backup scheme.

ShieldFS was proposed as an add-on driver that makes the windows instinctive filesystem resistant to ransomware attacks. For every action, ShieldFS vigorously toggles a protection layer that acts as copy-on-write mechanisms, which monitor the system activities at runtime against any form of violation and triggered an action which will roll back the malicious activities and transparently recover all the original files [16]. Patyal et al. [44] study the functionality of various ransomware attacks and lifecycle and proposed a four multi-layered defense architecture which comprises policies, recursive folder, process monitoring and backup and recovery. The mechanism does not rely on attack signatures and was able to combat ransomware by protecting the system against ransomware infiltration, file encryption, system processes activities, and data backings, and Ray et al. [45] describe how to use an ILP system ALEPH to interactively assist human experts in learning rules to better understand the conduct of cyberattacks. The algorithm was developed alongside a network log that obtained a sandbox computer which was deliberately infected with the CryptoWall-4 malware and showed how ALEPH can be used to interactively learn simple rules comparable to those hand-crafted by a human expert. Table 5 presents summary of major research findings on crypto-based ransomware attacks and defense.

Kolodenker et al. [33] paper described how to deploy and implement a prototype defense mechanism called PAYBREAK. This is a proactive defense system that relies on hybrid encryption mechanism to unlock any system with symmetric session keys using key escrow mechanism that stores session keys in a key vault. The system relies on low overhead dynamic hooking methods and asymmetric encryption to realize the key escrow mechanism which allows victims to restore encrypted files by ransomware.

Aziz [8] carried out full analysis of ransomware types, and how it progressed from the malware and Trojan codes and also explained the common encryption scheme (AES &

Table 5 Synthesis of crypto-based techniques

S/N	References	Techniques	Problem addressed	Comparison methods	Results/findings	Limitations
1	Al-rimy et al. [6]	Enhance Frequency Centric Model (EFCM) & TF-IDF Data-Centric Detection	Building an effective crypto ransomware model for early detection of ransomware	Monitoring C&C communications, utilizes the dynamic approach to detect the threatening text embedded in the payload of crypto ransomware and data-centric crypto ransomware detection solutions	EFCM techniques have features that is suitable for the behavioural detection of ransomware as compared to the static data-centric feature	The detection scheme cannot cope with the dynamism of crypto ransomware attack
2	Cabaj et al. [11]	Novel Software-Defined Networking (SDN) Based Detection System	Using SDN technology approach to analyse HTTP messages, sequence and contents size to detect threat	Heldroid system, early warning detection system for ransomware, EldeRan, SDN context using Openflow compliant switches and NOX controller	SDN model achieved better detection results accuracy as compared to heldroid because of its static taint analysis	The system can only perform network measurements for Crypto-Wall and Locky family only
3	Song et al. [55]	Using statistical methods based on configuration, monitoring, and processing (CMP)	Preventing a modified ransomware attack on android platform	Running test based on V3 mobile one vaccine system against avast antivirus	The CMP techniques performed better than the vaccine systems, because it can detect modified and new pattern ransomware	The method is not robust enough to work on other platform except android operating system
4	Yang et al. [61]	Using android package kit (APK) file for automated malware detection	To analyse why android components are prone to attack and to develop automated model approach for malware detection	FlowDroid, TaintDroid, SCanDroid and DroidMiner	The automated system can detect both active and passive malware attack as against android immune detection system tools which is static	The proposed technique was only used for analyses and could not be practically implemented
5	Moore [42]	Using HoneyPot through file screening service & eventsentry	To investigate the method of using honeypot to detect ransomware activities	AppLocker, machine learning based system, monitoring the Master File Table (MFT), HitmanPro, file server resource manager (FSRM) and EventSentry product	Honeypot together with other IDS help to improve monitoring, detection and screening of network logs against attack	The system could be bypass and other vulnerability exploited by the dynamism of modern ransomware
6	Wecksten-Frick, et al. [58]	Using ZELTZERS analysis and renaming system tool (vssadmin.exe file) to recover from malware infections	Using a renaming system tool method to allow system recover from 4 most common crypto ransomware attack	Cloud based solutions for detection, best practices and preventive maintenance	The Windows native function which allow for the renaming of the system tool (vssadmin) to handle shadow copies helps the user's to recover encrypted files	The novel method is more of reactive and not proactive to ransomware attack

Table 5 continued

S/N	References	Techniques	Problem addressed	Comparison methods	Results/findings	Limitations
7	Continella et al. [16]	Designing ShieldFS Software on OS to detect and transparently recover from malware attack	To develop a self-healing hard-on driver that could make a window filesystem immune to ransomware attack	UNVEIL, CryptoDrop, HelDroid and graph isomorphism techniques	The add-on driver on the window makes it immune to ransomware attack and allows the native filesystem to rollback suspicious event	The model cannot detect Ransomware whose encryption process fall below the set out threshold
8	Patyal et al. [44]	Using policies, recursive folder, process monitoring, backup and recovery layers (PRPB) architecture to protect against ransomware	Using four multi-layered approach of policies, recursive folder, monitor and backup and recover from ransomware attack	Disable processes running from LocalAppData/AppData folders, Disable macros, Stay up-to-date and use security suite that provides process monitoring, filter executables in email, make use of BIOS clock to extend our time for payment, Regular backups, user education, Block end users from executing the malware and limit user access to mapped devices	The defense architecture which uses PRPB against malware executionworks better than the existing McAfee anvirusand network security systems proposed by other authors	The listed layered approaches are not dynamic enough to cope with the activities of some Ransomwa.
9	Ray et al. [45]	Using ILP system ALEPH learning algorithm to understand ransomware Behaviours Through the Analyses of DNS and HTTP log Data	To develop and use ILP learning algorithm to assist human to understand the behaviour of cryptoWall-4 ransomware	Not disclosed	The technique interactively assist human experts in learning new rules to better understand the behaviour of ransomware as compared to the signature-based technique	The ILP mechanism is designed to learn the behaviour of only cryptowall Ransomware
10	Kolodenker et al. [33]	Using a session hybrid encryption key (HEK) escrow mechanism for file recovery	To develop an automated proactive defense mechanism (PAYBREAK) that can secure system file from encryption by Ransomware	Microsoft Cryptographic API, measurements of I/O characteristics of ransomware samples and states that these characteristics are sufficient for a monitoring mechanism to distinguish ransomware from benign applications, ShieldFS,	The protection mechanism leverages on low overhead dynamic hooking techniques using the key escrow from the key-vault to restore the encrypted files back to normal rather than relying on ad hoc mitigation techniques	Paybreak is a signature-based mechanism that may not be able to identify ransomware with strong obfuscation techniques

Table 5 continued

S/N	References	Techniques	Problem addressed	Comparison methods	Results/findings	Limitations
11	Aziz [8]	Using Python Programme on Ubuntu to Analyse the Efficiency of Ransomware Encryption Algorithm (AES & RSA) Attacks	To use python programming language to show the efficiency of AES & RSA common encryption algorithms used by most ransomware	A cloud analysis based enhanced ransomware prevention system, static and dynamic Heuristic detection, The File-Based Intrusion techniques, IP Trace Back Algorithm	The method analysed the ransomware encryption codes to better revealed the anatomy of ransomware attacks, so as to guide on building effective preventive measures against ransomware attack	The algorithm can only detect ransomware which uses AES 256 bit's key encryption scheme and does not encrypt file extensions
12	Kiraz et al. [31]	Using EXPMONITOR for analysis & detection against public key cryptographic attack	To detect and analyse ransomware public key cryptosystem type of attack on computer CPU	Unveil, CryptoDrop, ShieldFS, PayBreak and automated identification of cryptographic primitives in binary programs	The defense mechanism has an accurate detection rate against ransomware that uses AES encryption scheme	ExpMonitor cannot detect ransomware running symmetric key cryptography on the system
13	Sgandurra et al. [51]	Using EldeRan, a Machine Learning Classifier to Dynamically Detect Ransomware Attack.	The approach was able to cope with ransomware sophisticated packing techniques.	EldeRan result accuracy was compared with support vector machine (SVM) and Naive Bayes	EldeRan achieves an area under the ROC curve of 0.995 and can detect new variant ransomwares	It uses a sandbox environment with unlicensed window Xp for its analysis
14	Shaukat and Ribeiro [52]	A layered defense system against cryptographic ransomware attacks using machine learning	Using various supervised machine learning algorithm to detect cryptographic ransomware attack	Four different machine learning algorithm was compared with the static-based of 60 Security Engines linked to VirusTotal	Gradient tree boosting algorithm perform better than the other four learning algorithm in terms of accuracy and false-positive results	
15	Ferrante et al. [19]	A hybrid system of static and dynamic approach using frequency of Opcodes, CPU, memory, network usage and system log statistic to detect ransomware on android platform	To build a hybrid system that can effectively detect ransomware attack	The system was compared with HelDroid static mechanism	The performance of static, dynamic and hybrid system were evaluated one at a time and the results shows that the hybrid system perform best in terms of detection accuracy with low false-positive rate	The system is only designed for Android operating system platform

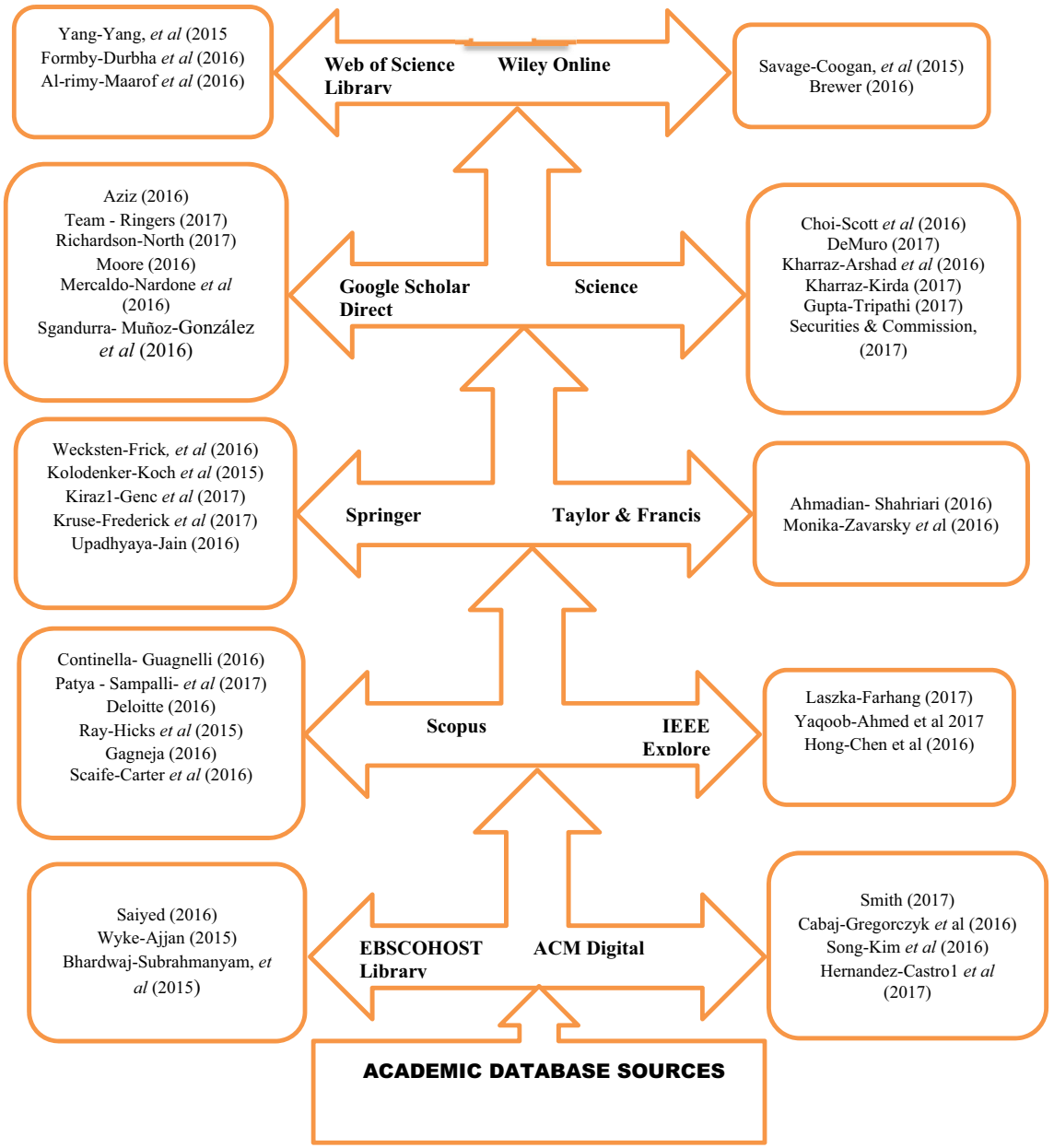

Fig. 5 Database sources of ransomware articles

RSA) used to infect systems. The article explained an alternative approach for data encryption using python programming language to display the effectiveness of those algorithms in real attacks by implementing this section on Ubuntu virtual machine to recognize the system vulnerability, which can be very useful to prevent the ransomware. As per the practical approach, this paper runs a crypto-type ransomware which is designed by Sen and it is entirely written in C sharp programming. It also utilized combined algorithms of AES and RSA in making the encryption more sophisticated and harder to decrypt until ransom is paid. It compares the various encryption algorithms to see which is more complicated to decrypt and suggests certain steps to be taken such as regular backup, patching software and other outstanding techniques to stop ransomware attack. Kiraz et al. [31] introduced a new enhanced detection and analysing approach called ExpMonitor, which observed encryption algorithm running on CPU. It has the capability to detect large integer arithmetic operation which constituted the backbone of public key encryption on victim's computer, unlike the existing detection mechanisms which target specific cryptographic functions. One of

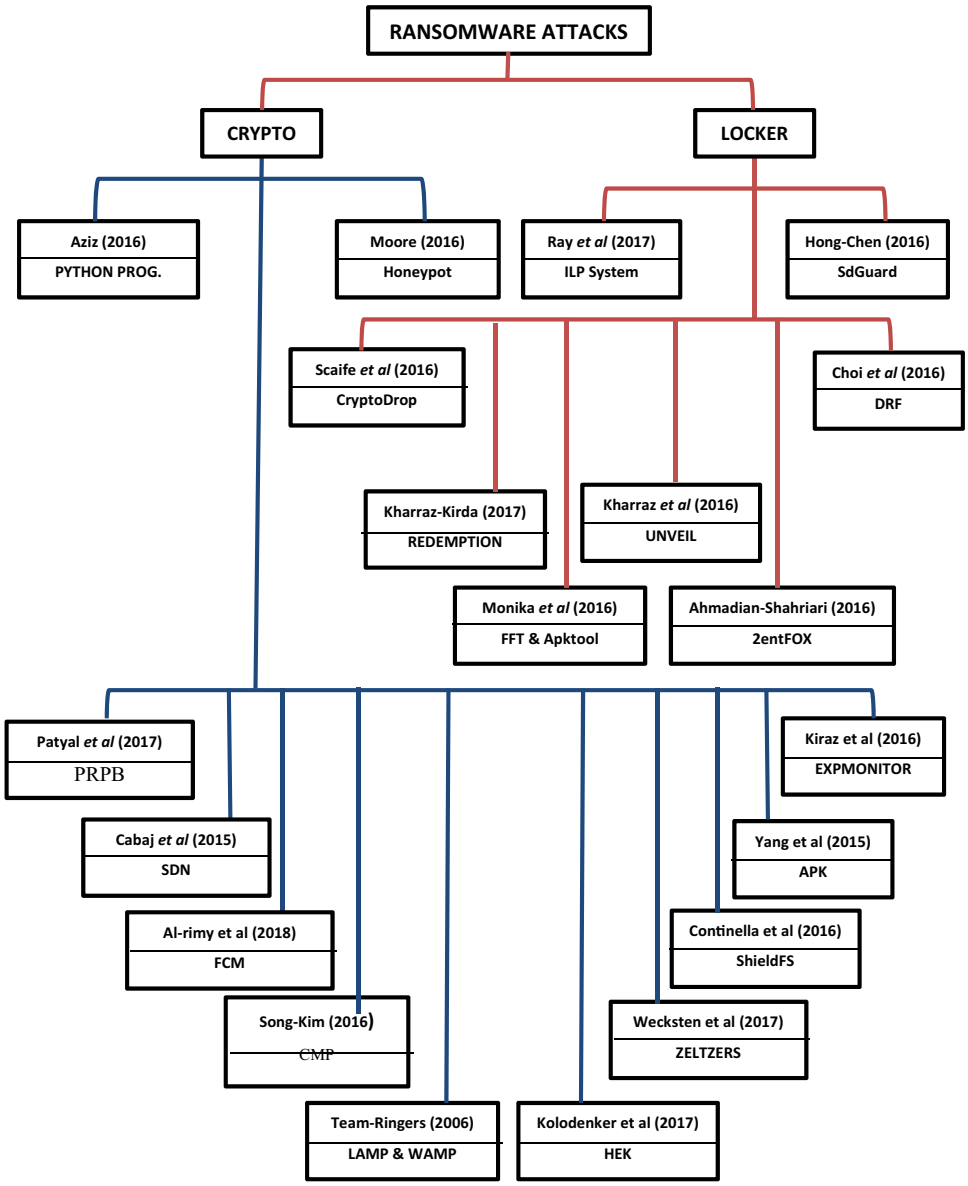

Fig. 6 Taxonomy of ransomware attacks

its shortcomings has been described as the inability to detect and prevent new attacks.

Sgandurra et al. [51] presented a framework-tagged EldeRan, an accurate dynamic learning machine design to detect ransomware attacks. It consists of feature selection and classification phases which help to select the most discriminating features in analysing and classifying both new and old variant of ransomware family and quick in arriving at result. Meanwhile, Shaukat and Ribeiro [52] present a hybrid of layered defense mechanism monitoring capabilities for the protection and detection of cryptographic ransomware in real time. The designed system combined static, dynamic and trap layers analysis to generate a novel compact set of features as input into the system, and deployed different machine learning engines to classify the executables as ransomware or benign software. It employs four supervised machine learning engine of logistic regression, support vector machines (Gaussian kernel), artificial neural networks, random forests and gradient tree boosting for the offline training exercise on ransomware and benign application datasets for the unearthing zero-day intrusion detection. The performance of each machine learned algorithm was evaluated and showed that Gradient Tree Boosting is the most effective against cryptographic ransomware because it obtained the highest false-positive and zero false-negative results.

Furthermore, Ferrante et al. [19] proposed a hybrid detection system by combining static and dynamic approach on Android platform for the detection of ransomware. In imple-

menting the two mechanisms, the static approach uses the frequency of the opcode, while the dynamic relies on runtime observation of CPU usage, memory usage, network usage and system call statistics. The execution traces containing this information were collected after effecting the applications one at a time on the android emulator in a controlled environment at two second interval. Log files for CPU, memory, and network are later unified using timestamps recorded at execution time. The research work intends to complement the coverage of static detection with the one of dynamic detection with the introduction of pre-processing, learning, and classification schemes. The performances of the static, dynamic and hybrid system stand-alone methods using precision, recall, F-measure, and receiver operating characteristics (ROC) curve were compared and evaluated, and the results show that the hybrid method performs best, being able to detect ransomware with 100% precision and having a false-positive rate of less than 4%.

4.2 Synthesis of Locker-based techniques

Team and Ringers [56] setup a LAMP and WAMP server in an artificial environment to study and analysed the behaviour and characteristics of ransomwares. The approach could not yield the required result because older versions of ransomwares whose activities were already curtailed were deployed for the experiment; the experimental environment did not allow effective and efficient results to be obtained, while Scaife et al. [49] designed a CryptoDrop, an early warning detection system that signals a user of any suspicious file activity. It analysed some set of behaviour indicators that appear to be interfering with a huge amount of the user's data. The analysis includes the ability of the system to inspect, capture, and alert user of ransomware attack with low false-positive results. Similarly, [4] introduced a novel framework called 2entFOX, which has the ability to detect high survivable ransomware (HSR) unlike other detection tools which worked on some extractive features; its architecture is supported with another detection system with the help of Bayesian belief network which was used to extract features and their statistical possibilities. The feature set can be decreased or increased based on the security countermeasures, but Monika Zavarsky and Lindskog [41] research paper focuses on analysing the activities of ransomware on Android and Windows environment from inception till March 2016. The article revealed that ransomware behaved in similar patterns using variant payload and it also discloses how a ransomware interacts with the file system, registry activities, and network operations when a machine is under a ransomware attack. It suggested the deployment of appropriate defense mechanism and continuous monitoring of the activities of file system and registry in Windows environment, while a closer attention should be paid to permission request by android applications.

Hong and Chen [26] focus on protecting external storage device on smart phones by introducing an application called Sdguard. This is a permission-based Linux-based mechanism which has the ability to detect crypto ransomware malwares that can attack external storage device or sometimes lock system screen. Installing Sdguard requires the smartphones to be rooted and the use of FUSE filesystem on the external storage device, sdcard daemon of android (i.e. FUSE daemon) to be swapped with a modified sdcard daemon which after system reboot, the modified daemon is loaded, and each component of Sdguard begins to run against any crypto ransomware attack. Choi et al.'s [13] article uses a theoretical approach to unravel why ransomware has become a viral phenomenon. It collated data from recent reported cases of attack by ransomware from police departments in US to build a victim profile for analysis. The research shows that online lifestyle and digital-capable guardianship (cybersecurity), lack of awareness of their vocational online activities, download attachments or digital faxes as well as click hyperlinks in emails sent to them without adequate scrutiny are one of the noticeable factors that contribute to the ransomware victimization. The article finally recommended the establishment of pro-social views of promoting adequate vocational activities and utilizing efficient computer security will help in reducing the effect of ransomware attack. Summary of major research findings on Locker-ransomware attacks and defense is shown in Table 6.

A novel defense approach that focussed on Redemption was proposed. This method is saddled with the responsibility of making the operating system immune to ransomware attacks. Though, the approach may require some modification of the transparent buffer for all storage I/O requests to make it more sensitive in detecting abnormal activities and automatically terminate the process by restoring the original data. The entire Redemption system approach does not require additional application support or any other prerequisite to protect users against ransomware and can guarantee zero data loss against current ransomware families without detracting from the user experience or inducing false alarm [30].

Kharraz et al. [29] research paper applied a novel dynamic analysis system called UNVEIL. It was designed to use the out-put of filesystem monitor to specifically detect crypto and locker ransomwares on a generated artificial environment. UNVEIL filesystem monitor has the ability to directly access data buffer used in I/O request, full visibility into all file system alterations, timestamp operation type, file system path and pointer to the data buffer. All these activities make the system to outperform all existing AV scanners and the modern industrial sandboxing technology in detecting sophisticated and new ransomware attacks. The assessment

Table 6 Synthesis of Locker-based techniques

S/N	References	Techniques	Problem addressed	Comparison methods	Results/findings	Limitations
1	Team and Ringers [56]	LAMP & WAMP Servers System Using Win7 & Ubuntu as Os Environment	Using LAMP & WAMP server to analyse different types of ransomware	None	The experiment carried out on virtual environment revealed the behaviour of ransomware, its mode of attack and recommend the appropriate mitigating techniques against it	The experiment did not utilized current ransomware family for analysis
2	Scaife et al. [49]	Using CryptoDrop to Detect Malware Through Indicator Scoreboard, Union Indicator and Shanon Entropy	To develop a cryptoDrop system that can alert the user of any suspicious file activity on the system	Signature matching, commonly found in most modern antivirus and IDS deployments, analyses programs based on known malware characteristics and flags those that match previously observed intrusions	The designed system which has a low false-positive rate against cryptographic ransomware, alert the user of any suspicious file activities in real-time and performed better than other technique which inspect programs for ransomware activities	The method could not distinguish between ransomware and benign activities
3	Ahmadian and Shahriari [4]	Using 2entFOX to detect high survivable ransomwares (HSR) through bayesian network-based analysis	To use a 2entfox approach to detect high survivable ransomware attack	None	The system has speed, generality and simplicity in its detection engine, which aid in the detection of HSR, and does not allow the malware to bypass the VSS monitoring mechanism	The design framework cannot cope with the low survivable ransomware
4	Monika Zavarsky and Lindskog [41]	using file fingerprinting technique (FFT) and Apktool to extract and detect malware attack	To analysed how ransomware activities have evolved on window and android environment right from inception to the year 2016	Not disclosed	The technique shows improvement in encryption techniques using process monitoring of abnormal filesystem and registry activities on windows, while greater emphasis placed on permissions request of Android applications	No any former technique for prevention and protection against ransomware

Table 6 continued

S/N	References	Techniques	Problem addressed	Comparison methods	Results/findings	Limitations
5	Hong and Chen [26]	Designing SdGuard, android app mechanism to detect and prevent ransomware	To develop and install Sdguard app to protect and detect ransomware responsible for the encryption of file on external devices	Not disclosed	The application allows the setting of some specific access rules to regulate the fine-grain permission control based mechanism of the android OS for monitoring of stack activities and I/O log analyser for ransomware detection	The Sdguard mechanism cannot differentiate between genuine activities and ransomware on the system files
6	Choi et al. [13]	Using a Diagnostic Risk Factor (DRF)Through Cyber Routine Activities (CRA) to Analyse ransomware attack	Using a Cyber Routine Theoretical approach in explaining why ransomware victimization has become a viral phenomenon	None	This practical analysis shows that lack of proper guidance in the preventive measures is the salient factors that contributed to the victimization of users	The article did not recommend a strong proactive preventive measures to be taken to avoid Ransomware attack
7	Kharraz et al. [29]	Designing UNVEIL using 56 VMs running windows XP SP3 on a ganeti cluster based on Ubuntu 14.04 LTS to detect ransomwar	Using dynamic analysis system to automatically create artificial desktop environment to detect ransomware interactions with the user data	Design of obfuscation-resilient detection systems, higher-level semantic characterizations of their runtime behaviour, honeywords, used	This dynamic analysis setup revealed that any Locker ransomware attack must tempered with desktop user's file for its illicit acts to be fully implemented	The system designed cannot detect crypto ransomware attack
8	Kharraz and Kirda [30]	Integrating redemption as a defense system support services to the operating system	Introducing a redemption defense system on operating system I/O storage ports to detect ransomware attack	Unveil, CryptoDrop, ShieldFS, PayBreak	The defense mechanism is an end-point interaction solution that regulates privileges to the user files by assigning a malice score to differentiate benign and ransomware activities compared SSIM index method	The mechanism can only detect crypto and not Locker ransomware

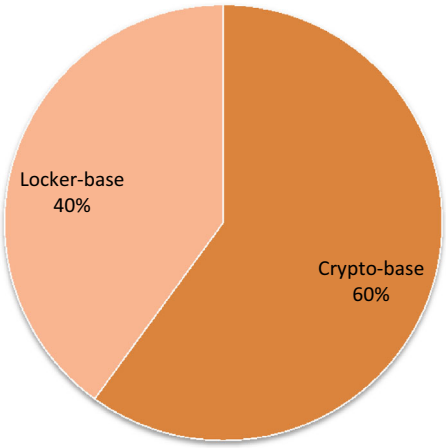

Fig. 7 Crypto-based and Locker-based ransomware techniques

of UNVEIL shows that the approach was able to correctly detect 13,637 ransomware samples from multiple families in a real-world data feed with zero false positives (Fig. 7).

4.3 Synthesis of parameter

In this section, we present the metrics used in assessing the effectiveness of the methods proposed in the literature.

1. Central Processing Unit (CPU) utilization which is expected to rise during file encryption was actually used for the analysis. The performance distance square was initially at 25 minimally, while the maximum distance was 893. For the purpose of arriving at accurate result, the limit distance was taken to 1050 to determine the true-positive rate and the false-positive rate. TPR and FPR were calculated as the ratio of flagged traces of ransomware or flagged traces of benign activities sampled as against the total number of samples in the dataset. The new set out threshold for the CPU was able to obtain 100% detection accuracy according to Cabaj et al. [11], Kiraz et al. [31] and Song et al. [55].
2. Signature-based approach using information on ransomware activities which was stored in the META-INF directory that is used to ensure the integrity of APK packages. The permission management mechanism in android OS makes use of the information stored in APK file to detect malicious applications [4, 16, 26, 33, 41, 42, 49, 58, 61].
3. Content and behavioural-based using ROI which is part of the computing environment where file encryption takes place. It applied an extracting algorithm which dynamically samples the trace files into smaller part called sliding window and continuously monitors the file and the frequency of interaction with the environment against the set out threshold for malware detection [5, 29, 30].
4. DeepFreeze Software (reboot-to-restore); this is a software that is designed to keep computer configurations intact. So if it noticed any changes to the original configuration or suspect malicious activities on the stored files; the system immediately reboots and restores back to default or desired configurations [56].

Figure 8 depicts the evaluation metrics used in the literature for assessing the effectiveness and efficacy of the ransomware detection methods. The signature-based parameter has the longest bar. This signifies that the signature-based parameter received the highest number of attention in the literature compared to other evaluation parameter. On the other hand, the DeepFreeze Software has the shortest bar compared to the bars of the other evaluation parameters, signifying that it has the lowest patronage from researchers. Evidence indicated that most literature relied on the signature-based parameter for the evaluation of ransomware detection method.

In evaluating the performance analysis of the experiment, most researchers adopt various parameters in arriving at their decisions. Some of the metrics used include: Region of Convergence (ROC) against file encryption, CPU utilizations, true-positive rate (TPR), false-positive rate (FPR), accuracy, precision and recall as tabulated in the Table 7.

5 Ransomware attacks to operating system

These research papers reviewed aid in the understanding of ransomware, its evolution, method of attacks and different mitigating techniques adopted. Most of research papers focused on windows and android operating system because it is the breeding ground for ransomware activities.

In defending against ransomware attack on windows; Wecksten et al. [58] proposed a solution which makes use of the windows native functions, shadow copies and tweaks it by running the suggested script to constitute a safety net for systems attacked by Crypto ransomware, while Continella et al. [16] equipped the window operating systems with practical self-healing capabilities called ShieldFS. The add-on driver that has a protective layer which monitors low-level file activities makes the windows native filesystem immune to ransomware attacks. Kharraz and Kirda [30] introduced another defense mechanism called Redemption which makes the windows more resilient to ransomware attack, by just little modifications of the operating system by maintaining the transparent buffer, and monitor input/output request patterns of all applications on a per-process basis to identify ransomware behaviour.

Kolodenker et al. [33] developed a prototype mechanism called PayBreak which relies on hybrid encryption that can decrypt an encrypted file that uses symmetric session key. Kharraz et al. [29] developed a dynamic system called

Table 7 Parameters for performance evaluation in the reviewed literatures

S/N	References	Parameters for performance evaluation											
		ROC	CPU ultilizations	True-positive rate	False-positive rate	Memory usage	I/O rate	DeepFreeze application	MD 5 Checksum value	Malice score	Accuracy	Precision	Recall
1	Al-rimy et al. [6]	√									√		
2	Cabaj et al. [11]		√	√	√								
3	Song et al. [55]		√			√	√						
4	Continella et al. [16]			√	√						√		
5	Kolodenker et al. [33]											√	
6	Kiraz et al. [31]		√										
7	Team and Ringers [56]							√					
8	Scaife et al. [49]			√	√				√				
9	Ahmadian and Shahriari [4]			√	√							√	√
10	Monika Zavarsky and Lindskog [41]								√				
11	Kharraz et al. [29]			√	√						√	√	√
12	Kharraz and Kirda [30]			√	√					√			
13	Sgandurra et al. [51]	√		√	√								
14	Shaukat and Ribeiro [52]			√	√								
15	Ferrante et al. [19]	√	√	√	√	√						√	√

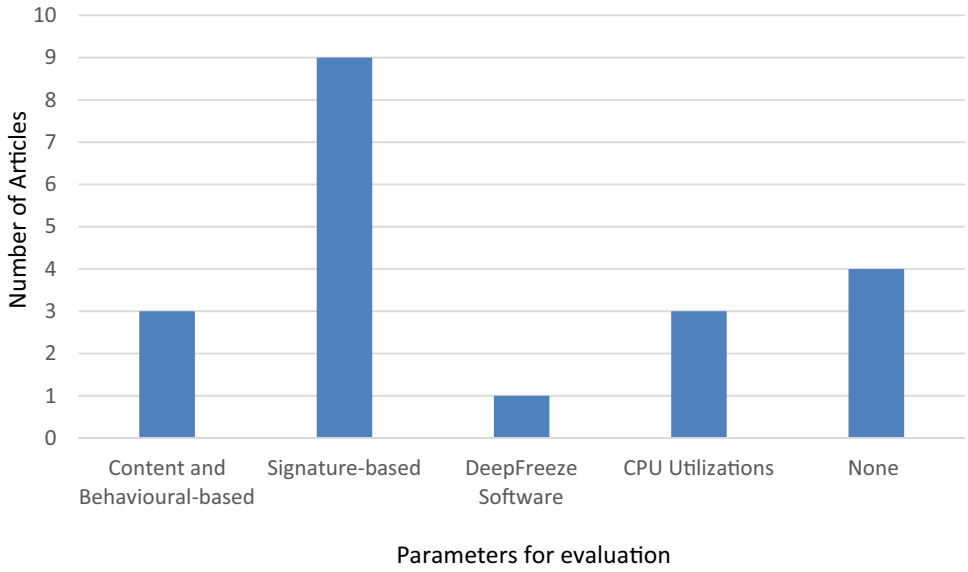

Fig. 8 Parameters used for the evaluation of ransomware

UNVEIL which automatically generates an artificial desktop environment to track changes to the file systems as a result of ransomware interactions with the user data. Alrimy and Maarof [5] framework against crypto ransomware attack consists of three modules: pre-processing module, features engineering module, and detection module to cope with the dynamicity nature of Crypto ransomware attacks, while Kiraz et al. [31] proposed a detection mechanism called ExpMonitor which monitors any public key encryption scheme running on the central processing unit. ExpMonitor only deals with detection and analyses rather than prevention.

In analysing cryptographic ransomware on windows, Cabaj et al. [11] present a novel software-defined networking (SDN) that provides rapid reaction in analysing HTTP messages' sequences and their respective content sizes which can detect threats from two Crypto ransomware families (Crypto and Locky ransomware). The drawback of this approach is its inability to detect other cryptographic ransomware families, but Team and Ringers [56] set up an experiment using LAMP and WAMP server to study and analysed how different type of ransomware is deployed to infect the system; the analysis shows a clear understanding on how attack is organized which serves as a guide for the cyber security expert on how to develop a mitigating technique to defend against ransomware attack. Scaife et al. [49], in his work, present CryptoDrop technique which is an early warning detection system that monitors the real-time change of user data and other behavioural indicator once the set out threshold is reached, the process is stopped and user is alerts on the impending ransomware attack. Moore, [42] set up a Honeypots which are bogus computer resources deployed by network administrators to act as decoy computers to detect any illicit activities. The approach adopted two options: The File Screening service of the Microsoft File Server Resource Manager feature and EventSentry to manipulate the Windows Security logs. Attack was staged on the system which triggered an alarm that informs the user of ongoing attack. This limitation is that, if the honeypot is free from attack, it is not an indication that other areas are not being targeted.

In analysing ransomware activities with the aid of some detective algorithm, Ahmadian and Shahriari [4] proposed a detection framework called 2entFOX1 based on Bayesian architecture with some notable extractive features of ransomware; this framework is meant to target high survivable ransomwares (HSR) in window environment. The major shortcoming is its inability to detect low survivable ransomware, because the writer does not consider the threat to be significant. Patyal et al. [44] propose four multi-layered defense architectural techniques that are made up of policies, recursive folder, process monitoring, and backup and recovery to combat ransomware infiltration in the front line and prevent file encryption. While Ray et al. [45] proposed a practical machine learning tools using the ILP system ALEPH to interactively assist human experts in learning rules to better understand the behaviour of ransomware and other cyberattacks. The major limitation of the proposed mechanism is its inability to detect an attack. Aziz [8] demonstrated practical approach to analyse programming languages used to build cryptographic ransomware, using python programming language to show the efficiency of those algorithms in real attacks by executing it on Ubuntu virtual machine. The experiment revealed the anatomy of ransomware, how it distributes it files and established connection with the attackers' server in order to infect the system and send back the decrypted information. The drawback was that the algorithm could not encrypt file extensions.

In the study of Android operating system against ransomware attack, Song et al. [55] proposed an intensive

monitoring technique which is based on three modules: Configuration, Monitoring, and Processing. The technique is added to the open source of Android source file on some specific file directories using statistical methods based on processor usage, memory usage, and I/O rates so that the process with abnormal behaviours can be isolated or detected, stopped and possible deletion. Yang et al. [61] dwelled more on analysing the basic Android component and manifest that makes it vulnerable to ransomware attack. It revealed the permissibility of android operating to several applications exposed it to attack; it then proposed an automatic immune detection system that can detect a new pattern ransomware and also distinguish between a benign activity, but could not explain further on the way to implement the automatic tools. Hong and Chen [26] proposed a permission control application software called Sdguard, which is customised to replace the default sdcard daemon, when properly installed, it can implement fine-grain permission control which is based on Linux DAC mechanism, that can detect crypto ransomware that usually encrypts content of file stored in external storage device and also lock user screen.

In developing a hybridized techniques against ransomware attacks on windows and android environment; Monika Zavarsky and Lindskog [41] setup an experiment that comprehensively analyses samples of ransomware that attacks window and android operating system. It revealed that, for Windows, ransomware can be detected through checking of MD5 checksum values for each analysed sample and monitoring of abnormal file system and registry activities. While in Android environment, closer attention be paid to permissions requested by the Android applications. Furthermore, Choi et al. [13] present comprehensive report from police department, whose authenticity is based on social media network sites, which revealed that online lifestyle and other salient factors contributed to the ransomware victimization. It recommended the creation of awareness campaign program on the use of social medial among the populace to guide against ransomware attack.

6 Synthesis of ransomware datasets

The major challenges faced in the analysis of ransomware activities are accessibility to essential datasets. Most of the research papers could not make available the sources of their dataset while some complained about lack of recent dataset to test their proposed model. However, recent dataset is very critical in evaluating newly proposed intrusion detection system because of the advancement of technology which renders old datasets irrelevant; detailed discussion can be found in Abubakar et al. [1]. In this review exercise, we have summarized some of the ransomware datasets used in Table 8. This can help researchers interested in proposing alternative algorithm for detecting the behaviour of ransomware attacks to easily have access to ransomware datasets for evaluating the efficacy of a proposed algorithm for detecting ransomware.

7 Unresolved problems and future research directions

Ransomware technology is fast evolving and many unresolved research problems are yet to be attended to. The research and survey articles analysed above show that there are currently few researches on ransomware prediction models, as most researches are based on either prevention or detection. This is because most ransomware preventive and detective techniques depend on data or information extracted during the execution of the attacks which rendered them ineffective due to the nature of this new attack. In addition, pre-encryption data acquisition from within the malicious codes of the ransomware is also done at runtime data. These types of pre-encryption are also not effective for ransomware attacks. One of the most effective cyber security strategies against ransomware going forward is to provide smarter prediction techniques capable of predicting new ransomware. This should be in conjunction with a layered security model. Therefore, ransomware attack prediction models are more effective in these scenarios. Furthermore, as a future research, we recommend proactive computational intelligent prediction models. Intelligent techniques proposed by Abdulhamid et al. [2] and Abdullahi and Ngadi [3] can be used to predict a ransomware attack even before it was triggered.

Ransomware attacks are very dynamic in nature. Therefore, to handle the dynamicity of crypto ransomware attack approaches, early detection systems with ensemble classification principles with incremental learning to yield active and efficient crypto ransomware detection and prevention systems are needed. For effective ransomware attack detection, more unique and specific features of the ransomware need to be engineered. This is important in training the current detection systems to achieve high degree of accuracy and precision. This is also closely related to another relatively unresolved problem of the availability of ransomware research datasets. Lack of readily researchable ransomware datasets is also hindering the speedy developments of detection and prevention solutions. In this paper, we made an effort to compile some sources of available datasets for research purpose. The list is non-conclusive but we still need more comprehensive list with robust extracted features.

Current ransomware payment methods utilize the cryptocurrency online transaction platforms like the Bitcoin. These platforms allow for anonymous transaction which made it very difficult to trace the movement of the ransom paid. To track and identify the identity of the attackers, new methods of cyber profiling need to be developed and crypt-

Table 8 Ransomware dataset sources

S/N	References	Datasets	URL addresses	Number of instances
1	Choi et al. [13]	Locky and cryptowall family	malwr.com maccdc.org	787
2	Scaife et al. [49]	TeslaCrypt and CTB-Locker families		492
3	Continella et al. [16]	Malware family	http://shieldfs.necst.it VirusTotal IntelligenceAPI	383
4	Monika Zavarsky and Lindskog [41]	16 ransomware family	Virus total	25
5	Kolodenker et al. [33]	Real-world ransomware	https://www.virustotal.com 5Malc0de, http://malc0de.com/rss 6VXVault, http://vxvault.siri-urz.net/URL https://cuckoosandbox.org/	107
6	Aziz [8]	tear_hidden ransomware (MSIL/Zyzerlo)	Locally created by the author	1
7	Kharraz et al. [29]	Real-world malware samples	VirusTotal,Anubis and malwr.com	3156
8	Kharraz and Kirda [30]	504 ransomware samples from 12 families with 65 benign executables	Minotauranalysis.com http://www.malwareblacklist.com	569
9	Sgandurra et al. [51]	582 ransomware from 11 families with 942 benign application	http://virusshare.com/ http://www.cuckoosandbox.org/	1524
10	Shaukat and Ribeiro [52]	574 ransomware samples from 12 Cryptographic families and 442 Benign Software	http://virusshare.com/	1016
11	Ferrante et al. [19]	672 ransomware application and 2386 Benign Application	https://play.google.com/store http://ransom.mobi https://github.com/liato/android-market-api-py https://www.virustotal.com	3058

analytic transaction tracing schemes must be improved. This way, ransomware attacks will be made unattractive to cybercriminals. These new improved cryptanalysis schemes will also increase the chances of ransom recovery and data recovery after a ransomware attack.

An effective ransomware prediction, detection and prevention schemes are the ones that have predictive abilities to make clever threat inferences of anonymous processes. This is possible when all executing processes are treated as unknowns and the threat level is constantly updated using how the executing process is working. This type of detection technique should utilizes a method of dynamic and robust behaviour forecasting analysis together with intelligent machine learning to deliver predictive capabilities of zero-day ransomware detection.

8 Conclusions

In this paper, we present a systematic review on ransomware attack and defense mechanism. The reviewed articles explained some basic features and symptoms of ransomware. It is an open fact that ransomware or any other kind of malware extortion models have come to stay with a stable growth both in complexity, adversity and multiplicity, offering a lot of ready-to-go solutions to the unskilled activist with resources and time to enable them to improve their efficiency. The players are moving from a chaotic environment to a more stable one just to have a grip and control of their activities.

The reviewed articles dwelled much on the environment, both windows and android platform which happen to be the breeding ground for ransomware activities because of its prevalent vulnerabilities. The success stories of ransomware attack have provided an encouragement to other activist to join in perpetrating their illicit acts. Most of the papers proposed several defensive techniques ranging from PayBreak, Redemption, UNVEIL, CryptoDrop and others in defending against the attack, but the challenge is its inability to cope with the obfuscation techniques. The research papers show some tremendous improvement on the security upgrade of the OS; it incorporated self-defense mechanism that allows the system handpicked any sign of CryptoLocker ransomware activities. Finally, the reviewed papers show that the most

reliable defense mechanism against ransomware attack is the regular file backup. Further research work could be directed towards improving the security features of the operating systems with more emphasis in developing an algorithm that could distinguish malicious attacks from benign system activities.

References

1. Abubakar AI, Chiroma H, Muaz SA, Ila LB (2015) A review of the advances in cyber security benchmark datasets for evaluating data-driven based intrusion detection systems. Proc Comput Sci 62:221–227
2. Abdulhamid SM, Latiff MSA, Madni SHH, Oluwafemi O (2015) A survey of league championship algorithm: prospects and challenges. arXiv preprint arXiv:1603.09728
3. Abdullahi M, Ngadi MA (2016) Symbiotic organism search optimization based task scheduling in cloud computing environment. Future Gener Comput Syst 56:640–650
4. Ahmadian MM, Shahriari HR (2016) 2entFOX: a framework for high survivable ransomwares detection. In: 13th International ISC conference on information security and cryptology, ISCISC 2016, pp 79–84. https://doi.org/10.1109/ISCISC.2016.7736455
5. Al-rimy BAS, Maarof MA (2018) A 0-day aware crypto-ransomware early behavioral detection framework. Recent Trends Inf Commun Technol. https://doi.org/10.1007/978-3-319-59427-9
6. Al-rimy BAS, Maarof MA, Shaid SZM (2018) Ransomware threat success factors, taxonomy, and countermeasures: a survey and research directions. Comput Secur 74(2018):144–166
7. Andronio N, Zanero S, Maggi F (2015) Heldroid: dissecting and detecting mobile ransomware. In: International workshop on recent advances in intrusion detection. Springer, Cham, pp 382–404
8. Aziz SM (2016) Ransomware in high-risk environments IT-792, independent research project December 2016 Advisor
9. Bhardwaj A, Avasthi V, Sastry H, Subrahmanyam GVB (2016) Ransomware digital extortion: a rising new age threat. Indian J Sci Technol 9(14):1–5. https://doi.org/10.17485/ijst/2016/v9i14/82936
10. Brewer R (2016) Ransomware attacks: detection, prevention and cure. Netw Secur 2016(9):5–9. https://doi.org/10.1016/S1353-4858(16)30086-1
11. Cabaj K, Gregorczyk M, Mazurczyk W (2015) Software-defined networking-based crypto ransomware detection using HTTP traffic characteristics. https://arxiv.org/ftp/arxiv/papers/1611/1611.08294.pdf. Accessed 27 Apr 2019
12. Chen J, Wang C, Zhao Z, Chen K, Du R, Ahn GJ (2018) Uncovering the face of android ransomware: characterization and real-time detection. IEEE Trans Inf Forensics Secur 13(5):1286–1300
13. Choi K-S, Scott TM, Leclair DP, Ks C, Tm S, Dp L (2016) Ransomware against police: diagnosis of risk factors via application of cyber-routine activities theory virtual commons citation ransomware against police: diagnosis of risk factors via application of cyber-routine activities theory. Int J Forensic Sci Pathol 4(7):253–258. https://doi.org/10.19070/2332-287X-1600061
14. Coccaro R (2017) Evaluation of weaknesses in US cybersecurity and recommendations for improvement (Doctoral dissertation, Utica College)
15. Cohen A, Nissim N (2018) Trusted detection of ransomware in a private cloud using machine learning methods leveraging meta-features from volatile memory. Expert Syst Appl 102:158–178
16. Continella A, Guagnelli A, Zingaro G, Pasquale GD, Barenghi A, Zanero S, Maggi F (2016) ShieldFS: a self-healing, ransomware-aware filesystem. https://doi.org/10.1145/2991079.2991110
17. Deloitte (2016) Ransomware holding your data. Deloitte Threat Intelligence and Analytics. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-aers-ransomware.pdf
18. Demuro PR (2017) Keeping internet pirates at bay: ransomware negotiation in the healthcare industry keeping internet pirates at bay: ransomware negotiation in the healthcare industry. Nova Law Rev 41(3):5
19. Ferrante A, Malek M, Martinelli F, Mercaldo F, Milosevic J (2017) Extinguishing ransomware—a hybrid approach to android ransomware detection. Springer, Cham
20. Formby D, Durbha S, Beyah R (2017) Out of control: ransomware for industrial control systems. In: RSA conference, 1–8. http://www.cap.gatech.edu/plcransomware.pdf. Accessed 27 Apr 2019
21. Gagneja KK (2017) Knowing the ransomware and building defense against it-specific to healthcare institutes. In: Proceedings of the 2017 3rd conference on mobile and secure services, MOBISECSERV 2017. https://doi.org/10.1109/MOBISECSERV.2017.7886569
22. Gómez-Hernández JA, Álvarez-González L, García-Teodoro P (2018) R-locker: thwarting ransomware action through a honeyfile-based approach. Comput Secur 73:389–398
23. Gupta G, Tripathi K (2017) Study on ransomware attack and its prevention. Int Educ Res J 3(5):260–262
24. Hampton N, Baig Z, Zeadally S (2018) Ransomware behavioural analysis on windows platforms. J Inf Secur Appl 40:44–51
25. Hernandez-Castro J, Cartwright E, Stepanova A (2017) Economic analysis of ransomware. Soc Sci Res Netw 2017(1):1–14. https://doi.org/10.2139/ssrn.2937641
26. Hong S, Chen J (2016) Poster: sdguard—an android application implementing privacy protection and ransomware detection, 26362. In: Proceedings of the 15th annual international conference on mobile systems, applications, and services. MobiSys '17, Niagara Falls, New York, USA, June 19–23, p 149. https://doi.org/10.1145/3081333.3089293
27. Idris I, Abdulhamid SM (2014) An improved AIS based e-mail classification technique for spam detection. arXiv preprint arXiv:1402.1242
28. Imran M, Guizani M, Yaqoob I, Ahmed E, Al-garadi MA, Imran M (2017) The rise of ransomware and emerging security challenges in the internet of things. Comput Netw. https://doi.org/10.1016/j.comnet.2017.09.003
29. Kharraz A, Arshad S, Mulliner C, Robertson W, Kirda E (2016) UNVEIL: a large-scale, automated approach to detecting ransomware. In: 25th USENIX security symposium (USENIX security 16), pp. 757–772
30. Kharraz A, Kirda E (2017) Redemption: real-time protection against ransomware at end-hosts. In: Dacier M, Bailey M, Polychronakis M, Antonakakis M (eds) Research in attacks, intrusions, and defenses. RAID 2017. Lecture notes in computer science, vol 10453. Springer, Cham, pp 98–119
31. Kiraz MS, Genç ZA, Öztürk E (2017) Detecting large integer arithmetic for defense against crypto ransomware. Cryptology, Report 2017/558. http://eprint.iacr.org/2017/558. Accessed 21 Dec 2018
32. Kitchenham B, Brereton OP, Budgen D, Turner M, Bailey J, Linkman S (2009) Systematic literature reviews in software engineering—a systematic literature review. Inform Softw Technol 51(1):7–15
33. Kolodenker E, Koch W, Stringhini G, Egele M (2017) PayBreak: defense against cryptographic ransomware. AsiaCCS 15:599–611. https://doi.org/10.1145/3052973.3053035
34. Kruse CS, Frederick B, Jacobson T, Monticone DK (2017) Cybersecurity in healthcare: a systematic review of modern threats and

trends. Technol Health Care 25(1):1–10. https://doi.org/10.3233/THC-161263
35. Laszka A, Farhang S, Grossklags J (2017) On the economics of ransomware. http://arxiv.org/abs/1707.06247
36. Latiff MSA, Madni SHH, Abdullahi M (2018) Fault tolerance aware scheduling technique for cloud computing environment using dynamic clustering algorithm. Neural Comput Appl 29(1):279–293
37. Lee K, Yim K, Seo JT (2018) Ransomware prevention technique using key backup. Concurrency and Computation Practice and Experience 30(3):e4337
38. Lee J, Lee K (2018) Spillover effect of ransomware: economic analysis of web vulnerability market. Res Brief Inform Commun Technol Evol 3(20):1–11
39. Mercaldo F, Nardone V, Santone A (2016) Ransomware inside out. In: Proceedings—2016 11th international conference on availability, reliability and security, ARES 2016, 628–637. https://doi.org/10.1109/ARES.2016.35
40. Mercaldo F, Nardone V, Santone A, Visaggio CA (2016) Ransomware steals your phone. Formal methods rescue it. In: International conference on formal techniques for distributed objects, components, and systems. Springer, Cham, pp 212–221
41. Monika Zavarsky P, Lindskog D (2016) Experimental analysis of ransomware on windows and android platforms: evolution and characterization. Proc Comput Sci 94:465–472. https://doi.org/10.1016/j.procs.2016.08.072
42. Moore C (2016) Detecting ransomware with honeypot techniques. In: Proceedings—2016 cybersecurity and cyberforensics conference, CCC 2016, pp 77–81. https://doi.org/10.1109/CCC.2016.14
43. Nieuwenhuizen D (2017) A behavioural-based approach to ransomware detection. Whitepaper. MWR Labs Whitepaper
44. Patyal M, Sampalli S, Ye Q, Rahman M (2017). Multi-layered defense architecture against ransomware. Int J Bus Cyber Secur 1(2): 52–64. http://ezproxy.umuc.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=121205538&site=eds-live&scope=site
45. Ray O, Hicks S, Moyle S (2017) Using ILP to analyse ransomware attacks. CEUR Workshop Proceedings 1865:54–59
46. Richardson R, North M (2017) Ransomware: evolution, mitigation and prevention. Int Manag Rev 13(1):10–22. https://doi.org/10.1108/17506200710779521
47. Saiyed BC (2016) CryptoLocker. Inform Syst Secur Assoc J 2016(4):14–18
48. Savage K, Coogan P, Lau H (2015) The evolution of ransomware. Secur Response 15:57. https://doi.org/10.5437/08953608X5403011
49. Scaife N, Carter H, Traynor P, Butler KRB (2016) CryptoLock (and Drop It): Stopping ransomware attacks on user data. In: Proceedings—international conference on distributed computing systems, 2016–Augus, pp 303–312. https://doi.org/10.1109/ICDCS.2016.46
50. SEC E (2017) Cybersecurity: ransomware alert. Natl Exam Progr Risk Alert 5(4):15–16
51. Sgandurra D, Muñoz-González L, Mohsen R, Lupu EC (2016) Automated dynamic analysis of ransomware: benefits, limitations and use for detection. Przeglad Elektrotechniczny 15:1–13. https://doi.org/10.15199/48.2015.11.48
52. Shaukat SK, Ribeiro VJ (2018) IEEE copyright notice: RansomWall: a layered defense system against cryptographic ransomware attacks using machine learning. This paper is a preprint (IEEE "accepted" status)
53. Silva JAH, Hernández-Alvarez M (2017) Large scale ransomware detection by cognitive security. In: Ecuador technical chapters meeting (ETCM), 2017 IEEE. IEEE, pp 1–4
54. Smith J (2017) Ransomware incident response for law enforcement (Doctoral dissertation, Utica College)
55. Song S, Kim B, Lee S (2016) The effective ransomware prevention technique using process monitoring on android platform. Mobile Inform Syst 2016:15–20. https://doi.org/10.1155/2016/2946735
56. Team T, Ringers D (2017) The cost of ransomware attacks. InforSec J 22(6):25–26
57. Upadhyaya R, Jain A (2017) Cyber ethics and cyber crime: a deep dwelved study into legality, ransomware, underground web and bitcoin wallet. In: Proceeding—IEEE international conference on computing, communication and automation, ICCCA 2016, pp 143–148. https://doi.org/10.1109/CCAA.2016.7813706
58. Wecksten M, Frick J, Sjostrom A, Jarpe E (2017) A novel method for recovery from Crypto Ransomware infections. In: 2016 2nd ieee international conference on computer and communications, ICCC 2016—Proceedings, pp 1354–1358. https://doi.org/10.1109/CompComm.2016.7924925
59. Wyke J, Ajjan A (2015) The current state of ransomware 1(December):61
60. Yaqoob I, Ahmed E, Ur Rehman MH, Ahmed AIA, Al-garadi MA, Imran M, Guizani M (2017) The rise of ransomware and emerging security challenges in the Internet of Things. Comput Netw 129:444–458
61. Yang T, Yang Y, Qian K, Lo DCT, Qian Y, Tao L (2015) Automated detection and analysis for android ransomware. In: Proceedings—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 conference on embedded software and systems. H, (1), 1338–1343. https://doi.org/10.1109/HPCC-CSS-ICESS.2015.39
62. Zimba A, Wang Z, Chen H (2018) Multi-stage crypto ransomware attacks: a new emerging cyber threat to critical infrastructure and industrial control systems. ICT Express 4(1):14–18