Egyptian Informatics Journal 22 (2021) 105–117

Contents lists available at ScienceDirect

Egyptian Informatics Journal

journal homepage: www.sciencedirect.com

Review

Internet of things and ransomware: Evolution, mitigation and prevention

Mamoona Humayun [a], NZ Jhanjhi [b,*], Ahmed Alsayat [c], Vasaki Ponnusamy [d]

[a] Dept. of Information Systems, Faculty of Computer and Information Sciences, Jouf University, Al-Jouf, Saudi Arabia
[b] School of Computer Science and Engineering (SCE), Taylor's University, Malaysia
[c] Dept. of Computer Science, Faculty of Computer and Information Sciences, Jouf University, Al- Jouf, Saudi Arabia
[d] Faculty of Information and Communication Technology, Universiti Tunku Abdul Rahman Kampar, Malaysia

ARTICLE INFO

Article history:
Received 2 February 2020
Revised 18 April 2020
Accepted 12 May 2020
Available online 28 May 2020

Keywords:
Internet of Things (IoT)
Ransomware
Cloud
Attack
Cryptography
Malware
Bitcoins

ABSTRACT

Internet of things architecture is the integration of real-world objects and places with the internet. This booming in technology is bringing ease in our lifestyle and making formerly impossible things possible. Internet of things playing a vital role in bridging this gap easily and rapidly. IoT is changing our lifestyle and the way of working the technologies, by bringing them together at the one page in several application areas of daily life. However, IoT has to face several challenges in the form of cyber scams, one of the major challenges IoT has to face is the likelihood of Ransomware attack. Ransomware is a malicious kind of software that restricts access to vital information in some way and demand payment for getting access to this information. The ransomware attack is becoming widespread daily, and it is bringing disastrous consequences, including loss of sensitive data, loss of productivity, data destruction, and loss of reputation and business downtime. Which further leads to millions of dollar daily losses due to the downtime. This is inevitable for organizations to revise their annual cybersecurity goals and need to implement proper resilience and recovery plan to keep business running. However, before proceeding towards providing a practical solution, there is a need to synthesize the existing data and statistics about this crucial attack to make aware to the researchers and practitioners. To fill this gap, this paper provides a comprehensive survey on evolution, prevention and mitigation of Ransomware in IoT context. This paper differs from existing in various dimensions: firstly, it provides deeper insights about Ransomware evolution in IoT. Secondly; it discusses diverse aspects of Ransomware attacks on IoT which include, various types of Ransomware, Current research in Ransomware, Existing techniques to prevent and mitigate Ransomware attacks in IoT along with the ways to deal with an affected machine, the decision about paying the ransom or not, and future emerging trends of Ransomware propagation in IoT. Thirdly, a summary of current research is also provided to show various directions of research. In sum, this detailed survey is expected to be useful for researchers and practitioners who are involved in developing solutions for IoT security.

Contents

* Corresponding author.Jhanjhi
E-mail addresses: mahumayun@ju.edu.sa (M. Humayun), noorzaman.jhanjhi@taylors.edu.my (NZ Jhanjhi), asayat@ju.edu.sa (A. Alsayat), vasaki@utar.edu.my (V. Ponnusamy).

Peer review under responsibility of Faculty of Computers and Information, Cairo University.

https://doi.org/10.1016/j.eij.2020.05.003
1110-8665/

1. Introduction

Internet of things(IoT) refers to the interconnected network of devices, sensors, actuators, software, etc. that store and exchange information [1]. Some prevailing benefits of IoT include automation, communication, and flow of information using less time and effort [2]. In IoT infrastructure, physical devices possess the ability of organizing and management that make them smart devices and these smart devices are becoming a vital part of human life ranging from home to big industrial and institutional sectors [3]. IoT has brought a great innovation in our lives by introducing indirect communication between individual and smart devices which made it vulnerable to a range of cyber scams. One of the most frightening attacks faced by IoT is Ransomware attack [4–6].

Ransomware is a combination of two words "Ransom + Ware" ransom means payment and ware shows that it is a type of malware attack. In a Ransomware attack, the attacker attempts to encrypt victim's data by using a strong encryption algorithm and demand ransom (usually payment in the form of Bitcoins) for decryption key [7]. Consequences of Ransomware attack include temporary or in some cases, permanent loss of information, disruption of normal system operations and financial loss [8]. Ransomware is mainly classified into two types: namely crypto Ransomware and locker Ransomware [6,9]. In a crypto Ransomware attack, attacker encrypts some vital information from victims' computer and demands a ransom for decryption. This ransom is usually demanded in the form of Bitcoins or any other method that is not traceable. Crypto Ransomware attack does not encrypt the whole hard disk of victims' computer; rather, it searches for important file extensions that effect victims the most [10,11]. Crypto Ransomware attack uses both symmetric and asymmetric methods for data encryption. Some of the existing crypto Ransomware attacks are DirtyDecrypt, TelsaCrypt, Crypt Locker, PadCrypt and Cryptowall [12–16]. Locker Ransomware attack locks the victim's machine. In locker Ransomware attack. Victim's data file remains safe; however, access is restricted by locking the system computing resources. It usually locks computing devices or user interfaces and demand ransom for unlocking. Locker Ransomware has different types such as DMA Locker, Locky Ransomware, CTB-Locker, Winlock, and TorrentLocker [3,17–19].

First windows crypto Ransomware attack named "PC Cyborg attack" was launched in 1989. It used a symmetric key and an initialization vector combination to encrypt the victim's computer data files[21,22]. Despite its early beginning, Ransomware attack was not so prevalent in the late 1990's or the beginning of the 2000's due to lack of personal computers and limited use of internet[23]. Ransomware emerged as a strong cyber-attack from 2005 onward and there is a tremendous increase in Ransomware attack after 2012 due to the maturity of IoT. By the year 2013, the IoT has evolved in almost every field of life including the automation of homes and building [22,24]. According to Fig. 1, the damage cost from Ransomware attacks is increasing rapidly in the upcoming years. This shows the need to provide awareness to the researchers and practitioners about the severity of this attack, how it works? What are the possible remedies? In case, if an organization or individual becomes the target of Ransomware attack? And this is only possible by providing a detailed picture of Ransomware attacks in the form of a comprehensive survey especially in the context of IoT. To the best of our knowledge, there exists no survey that provides us with a complete picture of Ransomware attack, especially in the context of IoT. In this paper, we attempted to fill this gap by providing a complete state-of-the-art picture of Ransomware attacks in IoT. The outline of the remaining part is detailed below in Fig. 2.

2. Literature survey

In this section, we provide a detailed overview of the current state-of-the-art of Ransomware attacks in IoT. This section is composed of seven subsections, and each section provides the user with related knowledge to understand the Ransomware attack for IoT in detail. Section 2.1 describes IoT along with a lot of benefits associated with it. Section 2.2 describes the two main types of Ransomware in detail. Section 2.3 provides the evolution of Ransomware attacks year wise. Section 2.4 provides the detail about Ransomware attack along with the discussion of possible solutions used so far. Section 2.5 guides entrepreneurs about whether to pay the ransom or not. Section 2.6 provides some useful statistics about Ransomware attacks which include: Ransomware statistics in the past five years, the top 10 countries that are the key target of Ransomware attack, the ways that are used to propagate this attack and the sectors that are the key target of this attack. This literature survey end in section 2.7 that provides the key challenges of Ransomware attack along with prevention techniques

2.1. Overview

IoT is an innovative paradigm that has gained much importance in the last few years due to the integration of various technologies and communication solutions [25]. The basic idea behind IoT is the pervasiveness of a variety of things such as smart devices, sensors, actuators and Radio-Frequency Identification (RFID) tags, etc. which interact and communicate with each other to achieve a common goal [2]. The rapidly growing importance of IoT is due to its high impact on almost everyday life and behavior of users. Below we provide some definitions of IoT for better understanding of readers

According to [26] IoT is defined as a world in which physical objects are integrated with information networks, these physical objects involved in business processes as an active participant. [27] defines IoT as a self-organized system of autonomous devices that communicate with each other to improve business processes' efficiency. [28] defines IoT as the connectivity of objects to the internet using RFID, GPS, Sensors, laser scanner or any other information sensing device in order to realize identification, monitoring, tracking and management of objects. [29] defines IoT as the ability of interconnected sensing and actuating devices to share information across various platforms.

All the above definitions present the same idea of IoT as shown in Fig. 3, that IoT provides the interconnection between physical objects using the internet and it is a rapidly growing phenomenon

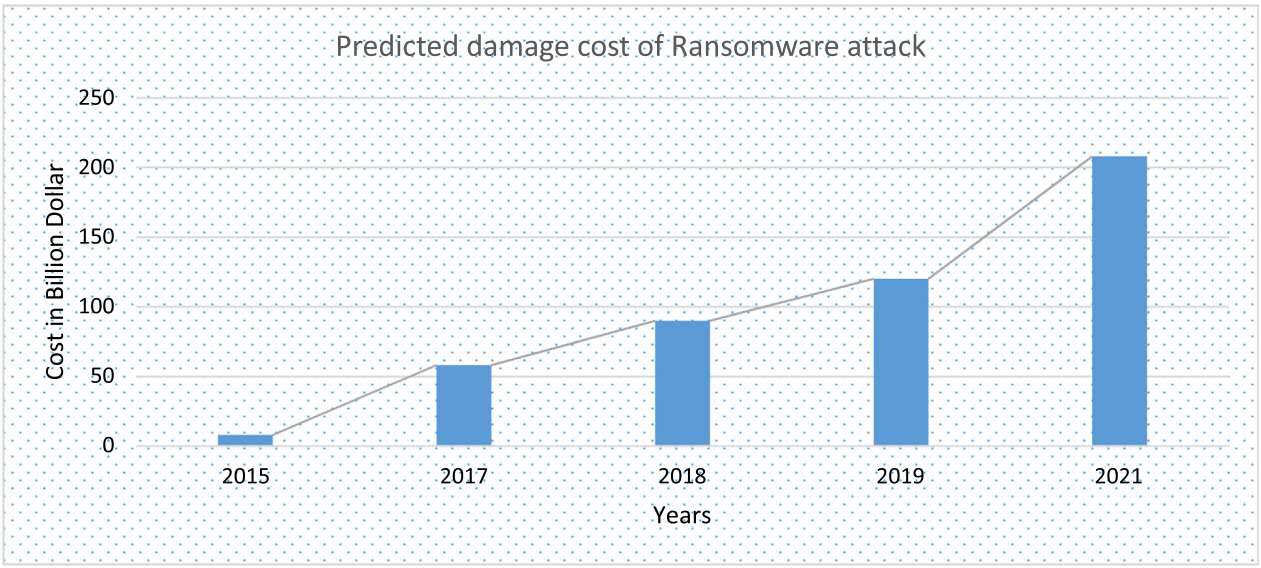

Fig. 1. Predicted damaged cost of Ransomware [20].

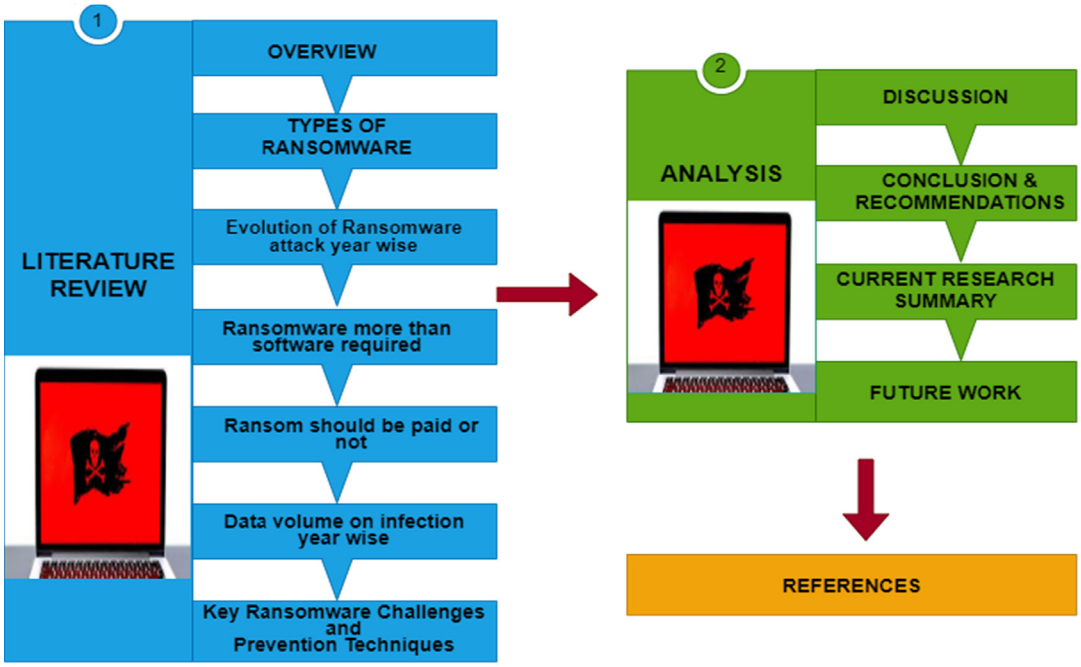

Fig. 2. Research Outline.

that is positively affecting every field of life. However, this rapid growth of IoT has to face different challenges, and from these, one such challenge is that of Ransomware attack [6,30]. As discussed above Ransomware is a type of malware attack that targets victim's computer information and encrypt or lock this information. The victim then needs to pay the demanded ransom in order to retrieve or access his data. With the growth of IoT, Ransomware attack is also growing rapidly. According to a report by Symantec, Ransomware attack increased 113% in 2014 and crypto Ransomware increased up to 4000% [31,32]. Another report presented by Kaspersky shows a 5-time increase in Ransomware attack between 2012 and 2015 [33]. This rapid growth of Ransom is not only limited to individuals, rather it is now targeting organizations as well [3].

2.2. Types of Ransomware

As we discussed above, there are two main types of Ransomware, Crypto Ransomware and locked Ransomware. Both these Ransomware usually start with an email attachment or a web link, when the victim opens the attachment or the received weblink the Ransom attack the victim computer by taking benefit of existing operating system flaws. Fig. 4 shows us the taxonomy of Ransomware attack.

In the case of crypto Ransomware, Once Ransomware becomes active, it encrypts some important user files. In this case, Ransomware do not attack the whole hard disk of the victim rather it chooses some important files based on file extensions. This attack usually uses 24-bit encryption scheme that is almost impos-

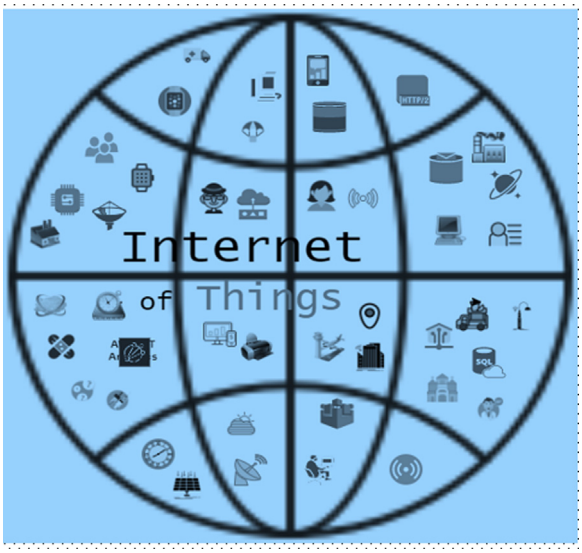

Fig. 3. Internet of Things.

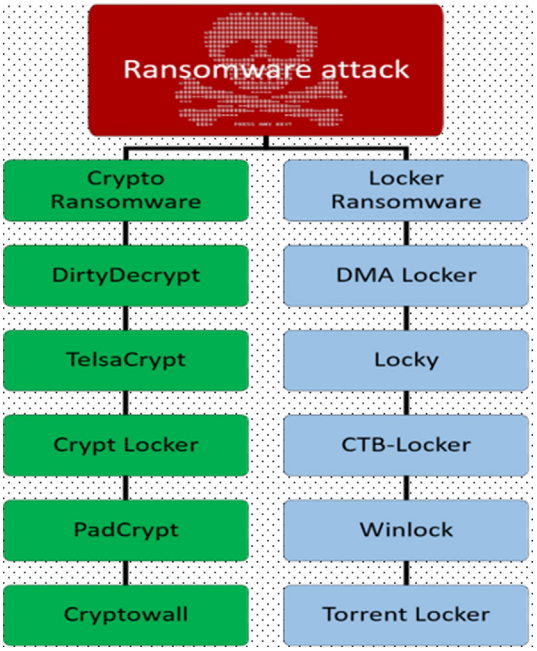

Fig. 4. Taxonomy of Ransomware attack.

sible to decrypt without unlocking key. Other than email attachment and web link, Ransomware attack spread through exploit kits.

In case of exploit kits victim does not need to open the attachment or to follow the web link rather victim is infected through a compromised missed website. After this, hacker demands payment from the victim, usually in the form of Bitcoins. The reason for choosing Bitcoins method for paying the ransom is that it is difficult to trace the attacker. If the victim pays the demanded money, the hacker sends the unlock key. In some cases, even after payment, hackers do not send the decryption key and data is lost forever. Some new forms of Ransomware attack take the benefit of operating system flaws and replicate themselves to spread through the network [34–37]. Fig. 5 describes the working of a crypto Ransomware attack

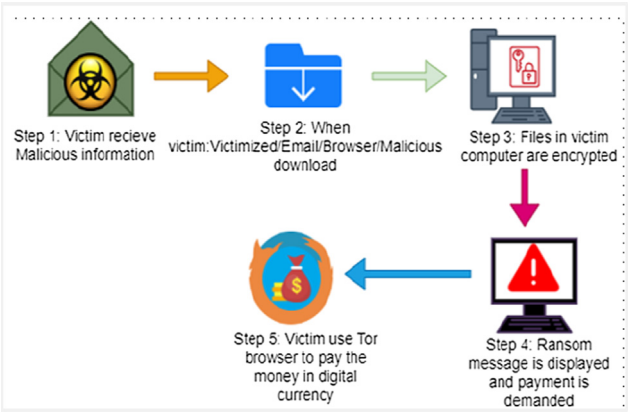

Fig. 5. How crypto Ransomware Work.

In case of Locker Ransomware attack, when the victim opens the attachment or weblink Ransomware becomes active and locks the victim's computer. The victim is now not able to use the computing device unless he pays the money. Once the demanded ransom is paid, the victim's device unlocks for use. However; in some cases, the attacker does not unlock the victim device even after getting demanded ransom [34,35]. Fig. 6 shows the working of Locker Ransomware attack

2.3. Evolution of Ransomware attack year wise

First Ransomware attack namely Aids Trojan (also named as PC Cyborg) was introduced in 1989 by a Harvard trained biologist Joseph L.Pop. However, at that time there was limited internet facility and the idea of IoT was not there, therefore; this AIDS Trojan was distributed through a floppy disk in an international conference on AIDS by world health organization. This Ransomware used a simple cryptography technique to encrypt the data which can be easily decrypted with little efforts [38,39]. Although Ransomware attack evolution goes back to 1989, it remained aloof until 2005 due to the limited use of the internet and limited digital currencies. In a report presented by international telecommunication union in the year 2005, the term IoT was suggested to connect the world's object in an intelligent way using technology [40]. Hence, we can say that Ransomware attack matured with the maturity of IoT. Below we discuss Ransomware attack and its impact from 2005 onward till 2019.

2005: A Malware attack named GPCoder was launched from year 2005–2008. An email was used as a source to spread this malware attack. In the case of opening this malicious email, GPCoder spread through victim computers and encrypt MS-Office and media files. Even at this time, due to the absence of smart gadgets, IoT was not so mature. Therefore, the Ransomware attack's extortion was relatively low and unsophisticated. This period is usually known as an era of "fake antivirus" where naive computer user was tricked to pay for the removal of a virus that does not exist [41,42].

2006: Ransom started to get hackers' attraction in 2006. Trojan. Cryzip appeared in March 2006. It copied victims' data files into password protected archived files which later on can be recovered easily. Trojan.Cryzip was just a hacker's attempt to try their hand. In the same year, Trojan.archiveus was launched, it was the first malware attack that demanded a ransom in the form of buying medication from specific online pharmacies [41,43].

2007: Locker Ransomware attack appeared in 2007, and it targeted Russia. The victim computer was locked and a pornographic image was displayed on the victim device to demand payment for

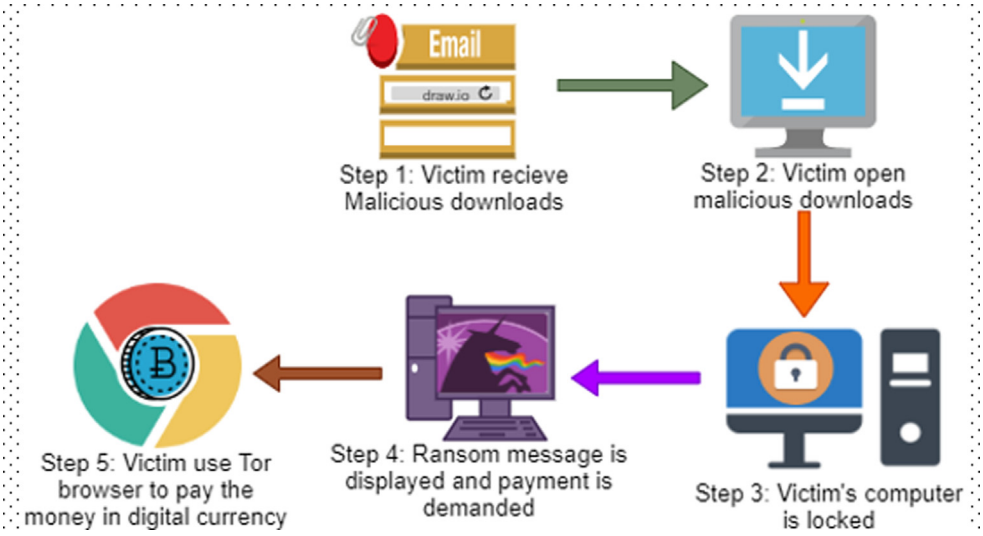

Fig. 6. How locker Ransomware Work.

unlocking either through text message or by calling a premium rate phone number [22,44].

2008: A new variation of Trojan GPCoder called GPCode.AK appeared in the year 2006. It used a 1024-bit RSA key for encrypting victim's data files and demanded 100$ to 200$ payment in digital gold currency using the Liberty Reserve method [45]. Liberty Reserve was a centralized digital currency service through which the user was able to transfer money just by using sender name, date of birth or email address without any significant effort [46,47].

2010: Winlock appeared in the year 2010, it is a kind of locker Ransomware attack [48]. Winlock disable I/O interface of the computer and victim consider it as locked. Winlock attack displays a blurred image on the victim's device and demands 10-dollar premium-rate SMS to get the unlock code. In the same year, a group of ten people was arrested in Moscow who were involved in the Winlock attack, and they earned over 16 million dollars from this SMS scheme [49].

2011–2012: Before 2011, direct users' extortion was limited due to the limited digital currencies and limited IoT infrastructure. Reveton Ransomware attack was launched in 2011–12, it was a variant of locker Ransomware. It was a malware-driven attack in which the user computer gets locked just by visiting a malicious website once. In Reveton, the message displayed on the victim's screen deceive the victim as it seems from the message contents that it is given by an authoritative body in response to some serious cyber rule violations. Victims were asked to pay the demanded ransom using coercion payment method otherwise victim was warned for strict criminal charges [50,51].

2013: In July 2013, dirty decrypt ransom was launched, it belongs to one of the family of crypto Ransomware. It targets and encrypt eight different kind of victim's files and ask for payment [52]. This ransom was usually launched via exploit kits or while using websites having adult contents. It spread by taking advantage of malicious JavaScript files that are uploaded on porn websites. This attack mainly targeted various versions of Windows operating system including Windows 2000, NT, XP, Vista, and Windows 2007. Once dirty decrypt gets activated, it creates malicious files in various Windows directories [53].

2014: In 2014, torrent locker and Cryptowall emerged as a family of crypto Ransomware attacks. Both these attacks were spread through spam emails or malicious link, as the user opens the spam email, the TorrentLocker or Cryptowall file was automatically downloaded and executed [54]. Another way of these attacks was through a malicious link that automatically redirects the victim towards the download of TorrentLocker or Cryptowall file [55]. One of the serious drawbacks of these attacks is that both these attacks steal the email contacts from infected machine and spread [56]. Both these attacks use a hollow process technique to execute malicious code. The hollow process is a malicious code injection technique in which the legal process residing in memory is replaced with malicious code. Once these attacks become active, the user computer get locks and ransom message appear on the screen [57]. In December 2014, CTB-locker that is considered as one of the latest forms of TorrentLocker came on the screen. IoT was quite mature by the end of 2014, CTB-Locker also spread through spam email or malicious link. The name CTB-Locker comes from its core advantage: Curve-Tor- Bitcoins. Curves come from the elliptic curve-based cryptography technique which this Ransomware attack use to encrypt victim's files. Core comes from the malicious server placed in TOR that was very difficult to takedown and Bitcoins was the currency in which victim have to pay the ransom for getting decryption key [58].

2015: The widespread and maturity of IoT brought a lot of positive changes and ease in human life especially with the widespread use of smart devices. However, this tremendous growth of technology also benefited the criminals in finding new ways of attacks. A lot of Ransomware attacks emerged in 2015 that targeted many individuals and organizations and criminals earned more than 4.5 million dollars through Ransomware attacks [59]. Cryptowall 3.0 appeared in early 2015, and since that time criminals are making it harder to detect. Cryptowall 3.0 is a virus that is cheap and easy to use plus it spreads very fast. This virus not only encrypts your file, rather it hides inside the operating system and tries to add itself to the startup folder. In the worst cases, it deletes some important files, and it became harder to restore these files [60]. In Feb 2015, TelsaCrypt appeared as a family of crypto Ransomware attacks. Amongst other types of files, TelsaCrypt also targets the gaming files of the victim. TelsaCrypt encrypts victims' files and asks for 500$ for decryption that gets double in case of nonpayment [61]. Another version of Cryptowall Ransomware, namely Cryptowall 4.0 also appeared in 2015. Cryptowall 4.0 not only encrypts victims' files, but it also changes the name of files so that victim couldn't check it in the backup [62]. Another Ran-

somware attack Linux. Encoder also appeared in late 2015, this Ransomware target Linux servers and Linux based websites. It spread by exploiting a flaw in Magento that is an open-source application for E-commerce. Files locked by Linux.Encoder displays the file extensions. encrypted. Once the victim file gets infected, payment is demanded in the form of Bitcoins. However; this Ransomware attack does not double the payment like Cryptowall 3.0 [63].

2016: 2016 is known as the year of Ransomware attacks because most notorious and damaging cybercrimes hit both individuals as well as small and medium-sized enterprises. Among the most dangerous Ransomware that appeared in 2016 were Locky and mamba. One of the most publicized attacks by mamba in the year 2016 was the public transport system of San Francisco, it also targeted the corporate network of KSA in 2017 [64,65]. Mamba Ransomware does not target some files rather it targets the whole hard disk of the victim computer. It uses diskcryptor tool to encrypt full hard disk and its partitions and can be only decrypted by a hacker after paying demanded ransom [66]. Locky Ransomware attack also appeared in early 2016 and it remained successful by leveraging large attack surfaces, stealth, and expensive money extortion ways. Locky Ransomware embeds macro in word documents and spam emails [67]. SimpleLocker appeared in early 2016 and android that emerged as the most prevailing operating system for smartphones and tablets at that time was the key target of this Ransomware attack. It was the first Ransomware that targeted the android platform and encrypted files to make them inaccessible by the victim [68]. Another Ransomware attack Cerber appeared in March 2016, it is one of the active kinds of Ransomware that target victim computer even when it is not connected with internet, so victim can't protect its machine by unplugging. In the Cerber attack, the victim receives an email with the MS-word document attachment. Once the user downloads attachment, Cerber encrypts the file and change their extension as.Cerber [69].

Petya Ransomware discovered in May 2016, it targets a Windows-based system and infects the boot record to encrypt hard disk files and stop the computer from booting. It spread through various large films including advertisements. When Petya Ransomware targets a victim computer, it demands 300$ ransom in the form of Bitcoins [71]. Another Ransom CryptXXX also appeared in mid-2016, it is from the same cyber mafia that was behind Reveton. CryptXXX also target windows operating system and encrypt files. When a victim is infected by CryptXXX, a ransom amount of about 2.4Bitcoins is demanded to get the decryption key [72]. RAA Ransomware was also reported in 2016, it is classified Ransomware as a service and was written in the java scripting language. RAA is usually distributed by email or in a password protected attachment that is difficult to detect through antivirus. RAA usually target businesses instead of ordinary users [73]. Another Ransomware attack Satana also appeared in 2016, it goes to the boot record and prevents the system from booting [66]. Satana Ransomware hides under a different name in a temporary folder and will prompt the user, again and again, to download the malicious file unless user clicks yes. After Satana installs and run its malicious code, it waits until the computer restart and informs the user that the machine is infected [74]. Stampado Ransomware also appeared in 2016, and this Ransomware includes self-propagating functionality due to which it effects the overall network. It can encrypt the files over 1200 extensions and demand ransom amount within 96 h. If the victim does not pay the ransom amount in a given time, the files are deleted [69,75]. Fig. 7 shows the evolution of Ransomware attack from 2005 to 2016 along with the description of attack strategy.

2017–2019: In June 2017, one of the virulent Ransomware attacks NotPetya appeared and became the second global security issue in the world. This attack is the modified version of Petya Ransomware attack that appeared in 2016. NotPetya is different from Petya in the sense that it encrypts the whole system instead of targeting a few files only. It reboots the infected system and changes its master boot record and make it useless. The user of the system is not able to aces any file as the master boot record is necessary to locate any file in the system [71,76]. WannaCry also known as WannaCrypt Ransomware appeared in May 2017 as a massive incident. The difference between WannaCrypt and previous Ransomware attack was a massive scale of incidents. WannaCrypt targeted more than 200,000 computers across more than 150 countries of the world [77]. Some other Ransomware attacks of the year 2017–2018 include Jaff, Spora, Cryptomix, Jigsaw, bad rabbit, breaking bad, SamSam and Crysis, etc. [78–81].

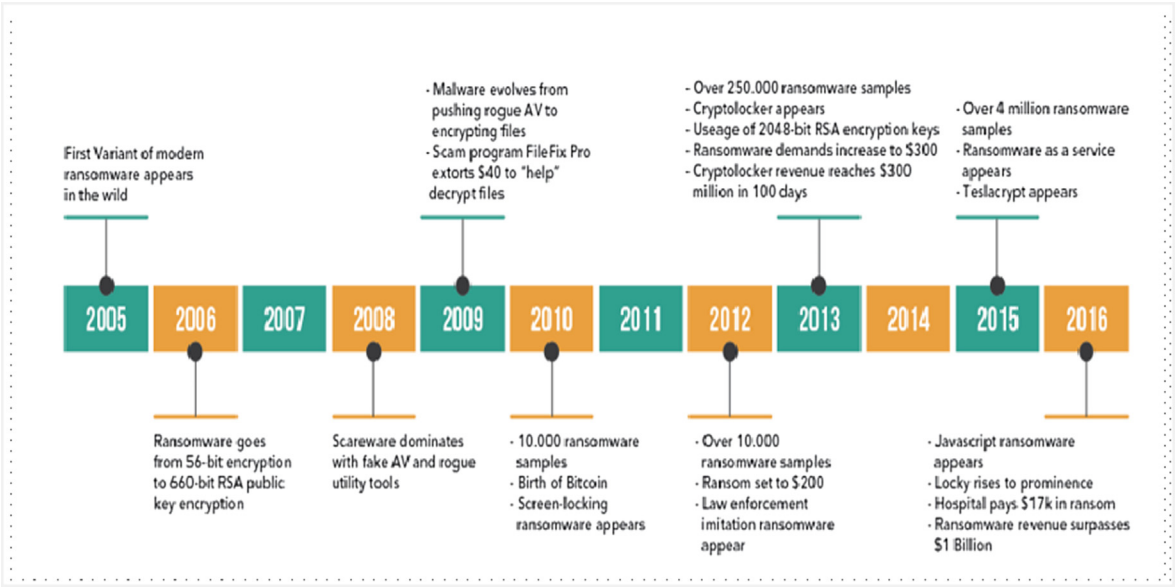

Fig. 7. Evolution of Ransomware [70].

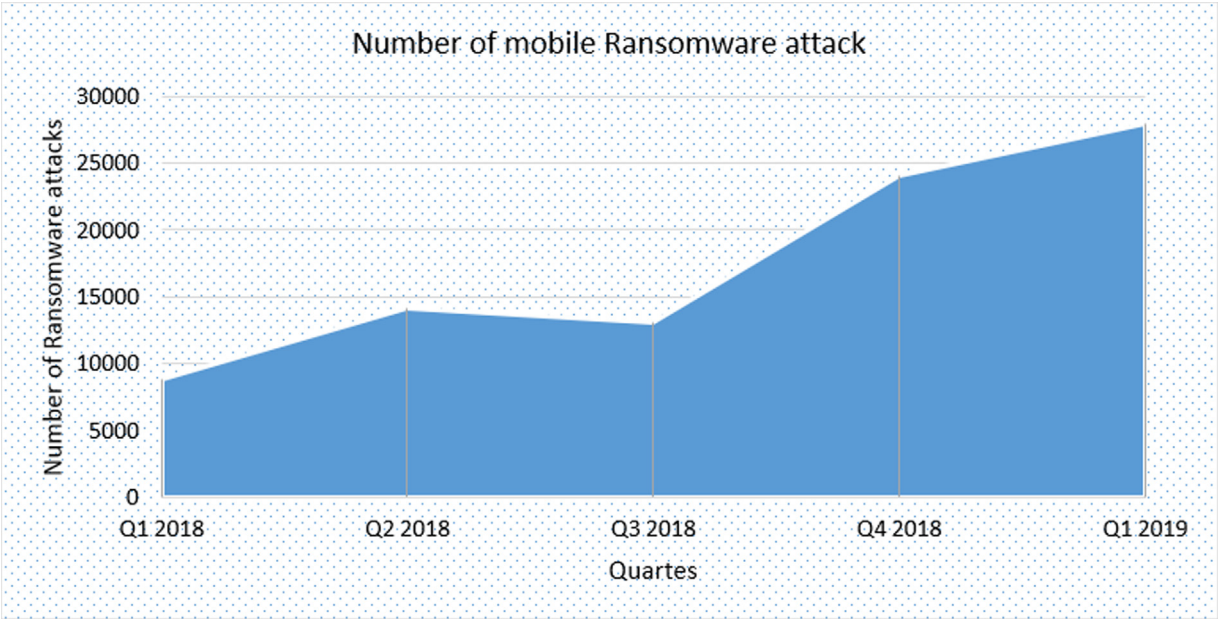

Fig. 8. Number of mobile Ransomware attack [82].

The year 2019 has also faced a lot of challenges regarding Ransomware attacks. In early 2019, one of the well-known manufacturers of hearing aids in Denmark became the victim of a Ransomware attack and its damaged cost was about 100 million dollars. In the same year, another US-based global shipping company named as Pitney Bowes also faced Ransomware attack and almost. This year experienced a wave of a Ransomware attack in the USA, where 90% of the Fortune 500 companies were affected by Ransomware attack.

Recently, a new type of Ransomware CCryptor has been captured by the 360 Security Centre. This virus is propagated through fishing emails and Ransomware attack was released to the victim machine using CVE-2017–11882 vulnerability. This Ransomware attack can encrypt files in 362 different formats using RSA + AES256 encryption technique. It encrypts the user files and waits for 10 days for the Ransomware, if the amount is not paid within 10 days, all the files will be deleted.

Fig. 8 shows us the number of mobile Ransomware attacks from the first quarter of 2018 to the first quarter of 2019, this figure is taken from the findings of Kaspersky Lab which is one of the well-known multinational cybersecurity and antivirus provider organization in the world with origin in Moscow. According to Fig. 8, the number of Ransomware attacks is increasing with time especially after the rapidly growing use of smart IoT devices particularly mobiles. This shows the need to protect individuals and organizations from a Ransomware attack and to provide the researchers and practitioners with state-of-the-art knowledge about the Ransomware attack.

2.4. Ransomware more than software required

The discussion done so far shows that Ransomware is one of the key cyber threats faced by individuals and organizations these days and it has become a huge business now. Security researchers have tried to provide various solutions to protect individuals and enterprises from Ransomware attacks. However, with the advancement of IoT, individual life, as well as business, is becoming fully dependent on the internet and interconnectivity between human and computing devices. Hackers are also coming in the market with new faces and technologies and their way of attack is every time different and unpredictable. In such a situation, it is the responsibility of every single individual and organizational worker to take extra care of their individual and organizational assets to not become the victims of Ransomware. There exist various software and preventive measures to protect the computational environment, but individuals and entrepreneurs must update security software from time to time. There exist the latest patches by Microsoft to protect the operating systems. Next, once you are satisfied that your system is infection-free, better to take a timely backup of your system. Once the backup gets completed, it is better to unplug your hard drive for safe storage. Just software is not sufficient to protect from Ransomware, below we discuss some measures that can be used to protect the computing devices from Ransomware attacks [76,83–86].

2.5. Ransom should be paid or not

One critical situation faced by victims after a Ransomware attack is to decide about whether to pay the ransom or not? The fact that Ransomware attack source is not identifiable and the payment method is very simple through Bitcoins, this strengthens the attacker space. In some cases, hackers even double the amount of ransom if it is not paid within a given amount of time. Further, the ransom amount is also increasing with the widespread growth of Ransomware attacks. The usual amount or Ransom demanded from the organizational sector is on average about 10,000$ and from the individual, it ranges on average from $300 to $700. However, sound statistics in this regard are not possible to collect because some organizations and individuals are not reporting the issues they faced. There is always a debate about to pay or not to pay? The encryption technology used in some Ransomware attack is so difficult to decrypt that sometimes it becomes necessary to pay or sometimes due to the sensitivity of the information it seems more efficient to pay as soon as possible. There is always a fear in victims' minds that if he pays the money, whether he will be able to get back the data and, in the future, he will not be the target of some such attacks? On the other hand, if every victim pays the money to get back the data, this business will promote more and more, and more people will get affected. Below we provide some discussion about whether to pay or not to pay the ransom or what

Table 1
Common Ransomware attack statistics in the past five years.

Ransomware Attack	Year	Paid Ransom	Platform
CryptoLocker	2014	>$ 3million	Windows
Cryptowall	2015	$18 Million	Windows
Linux.Encoder	2015	.....	Linux
TelsaCrypt	2015	>$80,000	Windows
Cerber	2016	>$ 500,000	Windows
Jigsaw	2016	>$ 2000	Windows
Locky	2016	>$1 million	Windows
Petya	2016	>$30,000	Windows
Bad Rabbit	2017	.....	Windows
Not Petya	2017	>$10,000	Windows
WannaCry	2017	>$140,000	Windows
SamSam	2018	>$850,000	Windows

Table 2
Top 10 Countries impacted by Ransomware.

Rank	Country	Percentage
1	USA	29%
2	Japan	9%
3	Italy	8%
4	India	4%
5	Germany	4%
6	Netherlands	3%
7	UK	3%
8	Australia	3%
9	Russia	3%
10	Brazil	3%

should be done to avoid ransom in the light of existing literature [83,84,87–89]

The above discussion shows that the ransom amount should not be paid to discourage hackers. However, it is compulsory for the organizations and individual to use proper measures to save their data.

2.6. Data volume on infection year wise

Even though many individuals and organizations do not pay, still the business of Ransom is growing day by day especially with the advancement of IoT. This section will present some statistical figures to show the: countries who were mainly targeted by a Ransomware attack, the ways of a Ransomware attack, the ratio of attacks with respect to time and advancement in IoT.

According to the Federal Bureau of Investigation (FBI's) internet crime center (ICT) report 2017, ICT received 4,063,933 internet crime reports since its inception and the ratio of complaints has tremendously increased in the last few years. According to ICT statistics from 2013 to 2017, the number of crimes reported was 14, 20,555 and the total loss was about $5.52 billion.

As we discussed above, the advancement of IoT has benefited a lot to the community but the increase in Ransomware attack has also been seen in the past few years. Table 1 shows the top few Ransomware attacks in the past 5 years [90–92].

Table 1 shows that Windows is a key target of a Ransomware attack. Therefore, it is necessary for the Windows users' to keep their operating system up-to-date and install the latest critical patches launched by Microsoft to protect their device from being a victim of a Ransomware attack. Table 2 shows us the list of countries who were mainly targeted by Ransomware attack according to internet security threat report

According to Table 2 and Fig. 9, the USA is the key target of Ransomware attack with a 29% record from the pool, while Japan is the second key target of a Ransomware attack. India and Germany are almost at the same pace with 4% ration while Netherlands, UK, Australia, Russia, and Brazil are 4th in the pool with a 3% ratio of a Ransomware attack.

The key sources of spreading Ransomware attacks are emails, malicious links, social media, USB sticks, and business applications. From these sources, the most common and easy to use way of targeting is via email link and email. Other than email, the second source of a Ransomware attack is web sites other than social media and email, and then comes the social media and USB stick. Table 3 Ranks the list of top 5 sources used for Ransomware propagation [9,35,93].

According to Fig. 10, Email and email links play a key role in spreading Ransomware attacks. The title of these emails is usually written in such a way that users consider it from an authentic source, but it is not. Further, email attachment is also a way of spreading Ransomware attacks. These attachments are executable files that when users click automatically it start downloading and

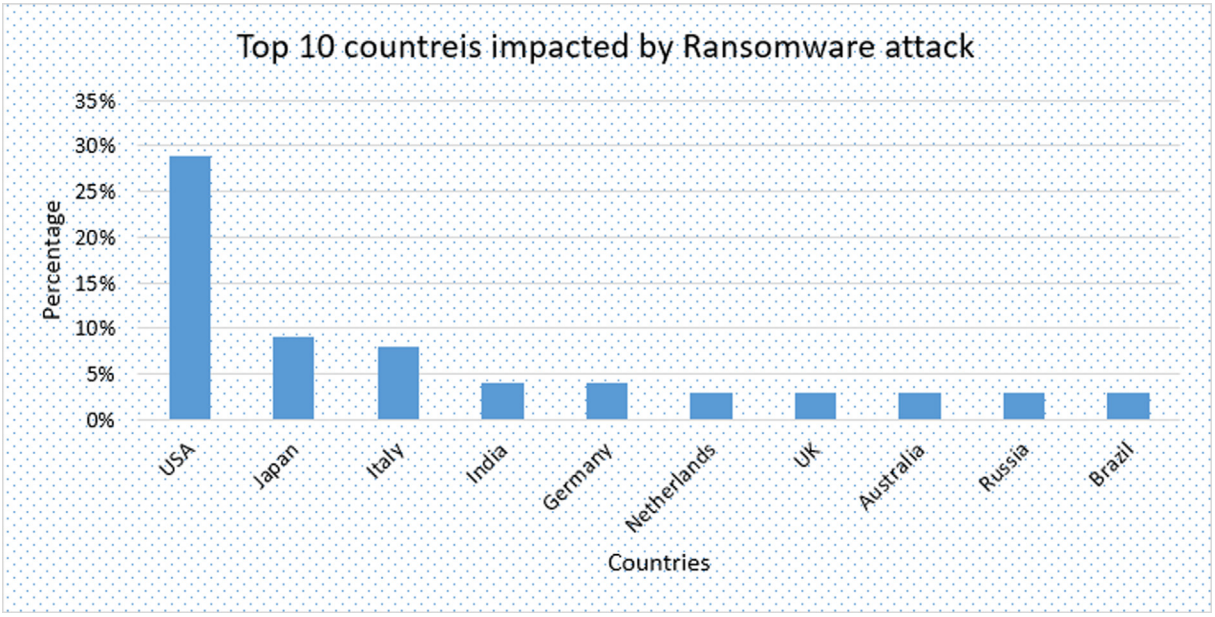

Fig. 9. Countries that are the key target of a ransomware attack.

Table 3
Key sources of Ransomware propagation.

Rank	Source	Percentage
1	Email link	31%
2	Email attachment	28%
3	Website other than social media and email	24%
4	Social Media	4%
5	USB stick	3%

Table 4
Key targets of a Ransomware attack.

Rank	Target
1	Healthcare Sector
2	Government Institutions
3	Education
4	Law firms
5	Mobile and MAC users

spreading itself. Some websites are also designed to get the attention of the user by providing various deals and incentives to the user, but these are used as a source of spreading Ransomware attacks. Social media is also being used as a source of Ransomware propagation these days. Last but not least is the use of a USB stick without scanning it.

Although Ransomware attack is one of the key cybersecurity threats of the current era. However, some applications are a key target of hackers due to their sensitivity to data. Table 4 shows the key targets of a Ransomware attack.

According to Table 4, healthcare organizations are the key targets of Ransomware attack due to the vitality and confidentiality of patient data. Then comes the governmental institutions as criminal knows the importance of data for the government and they expect to get back the ransom. The third main target of Ransomware attack is higher educational institutions due to weak IT hierarchy, then come the law firms and mobile users who become the target of Ransomware attack.

2.7. Key Ransomware challenges and prevention techniques

Cybersecurity and law enforcement vendors are paying special attention to Ransomware threats. Newly emerged ways of attacks are reported, and awareness is provided to people from time to time, it has made the criminals to change their minds and way of attack. Criminals are trying to find ways of hiding their attack tricks and the method of payments that are difficult to trace. In such a situation, individuals and organizations need to be more vigilant. Table 5 discusses some notable challenges that may arise during prevention from Ransomware attacks and their possible solutions [7,94–96].

Other than above prevented measures, vigilance is very important as it is a well saying that "precautions are better than cure". Individuals, as well as organizations, need to implement best practices to protect themselves from paying the ransom. Some of the best practices proposed by FBI include limited privileged, timely backup, disable macro and java scripts, software restriction policies and employee training regarding Ransomware awareness. Further reading related to the ransomware in different domains can be referred to [97–106] this covers ransomware in smart homes, E-health applications, Android smartphones, criminal networks, etc.

3. Discussion

The recent world's growth and advancement are in accordance with technological development. This advancement accompanied the risk and open threats for the technologies besides of the individuals and organizations. The ransomware is one of the most influencing sources among it, which has the power to shake the organizations, individuals as well as technological growth. The recent studies show a high rise in ransomware affected globally, with impacting the advanced countries mainly to the USA as depicted in Fig. 11. The studies prevail that the security breaches increased by 67 percent over the last 5 years. the frequency of ransomware attacks to the industries and individuals will increase to every 11 s by 2021 which is predicted increase in ransomware attack by 5 times compared to the current attack rate. Furthermore, Cybercrime damages are anticipated to cost $6 trillion annually by 2021.

This research prevails in-depth the information related to the ransomware in different aspects to help, understand and for the future directions of the research community. This research covers,

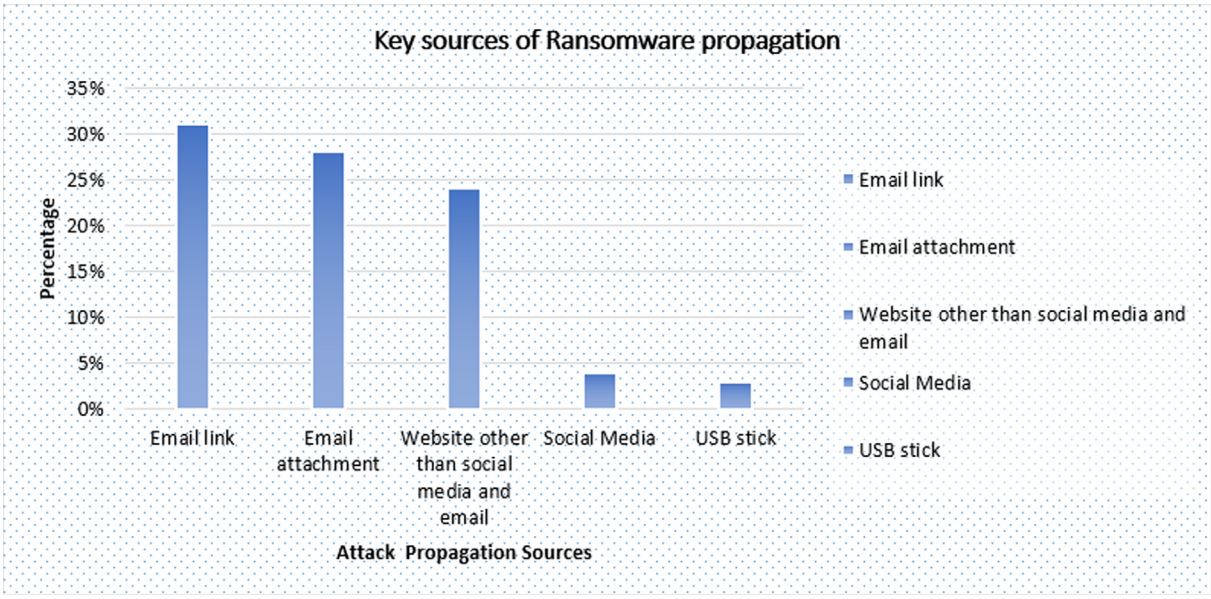

Fig. 10. Key sources of Ransomware propagation.

Table 5
Ransomware challenges and prevention techniques.

Challenges	Prevention techniques
Mere resetting the IoT devices may not work in all cases because already compromised devices sometime leave no option except paying the ransom	To overcome this challenge, researchers should develop some strategies for the early detection of Ransomware. IoT devices vendor should also provide a list of data files extensions that are safe to run within the IoT network.
IoT networks are heterogeneous therefore implementing a single security policy is difficult	To fully protect IoT devices from a Ransomware attack, Ransomware mitigation ability should be incorporated in IoT devices during the entire lifecycle of application execution
Some attacker targets the connected backup system	Backup is a good way of recovering the data instead of paying Ransom, but the backup should be current. Some attacker targets the connected backup system as well, so to address this challenge it is better to take the services of some reliable cloud service provider for the backup. Another solution to the backup challenge is keeping multiple backup of data and keep it secure
Criminals use malicious email and link for advertisement, novel user sometime get fascinated from these advertisements and open the link	To overcome this issue, organizations should provide training to their employee regarding trusted websites. Further, security should be embedded in IoT to prompt the user
One of the Ransomware challenge is propagation of Ransomware attack throughout the network	Organizations should restrict user rights to protect the security of data, the malicious node needs to be detected on time so that network may not get effected. Infected machine should be switched off immediately after infection detection
Misuse of privileges	Limited privileges

mainly the different types of ransomware from 2005 to onwards, data and volume infected and predictions of further infection in upcoming recent years, research challenges and prevention techniques. This research further dominates the main reasons of being targeted by the ransomware attacks including 1)user behaviors, most of the user are not aware for the safe use of the internet, studies suggested that the 70 percent of the employee in the USA don't understand the cybersecurity issues 2) malicious email is the major sources of ransomware targets CSO online estimated that the emails are responsible for spreading the malicious by 92 percent, 3) high rate of easily infected IoT devices as of NETSCOUNT report for 2018 reveals that any IoT device requires 5 min to be attacked after it goes only, 4) connected backups for the systems, 5) use of malicious websites other than the social networks is another increasing source 6) misuse of the privileges, 7) mobile ransomware increased by 33 percent by 2018 based on the Symantec report [107]. In addition, to the stated finding of this research Table 6 shows the current research with the research title and its type of research. In [108] authors have elaborated the current research on ransomware and different tools used by researchers for the ransomware.

4. Conclusion and Recommendations

This booming in technology is bringing ease in our lifestyle and making formerly impossible things possible. Internet of things playing a vital role in bridging this gap easily and rapidly. IoT is changing our lifestyle and the way of working the technologies, by bringing them together at the one page in several application areas of daily life. However, it is critical to manage them securely and maintain emerging applications safe and secure. These are prone to several security threats, and specifically to the ransomware, where once data or access can be restricted by unauthorized users/hackers, and it is hard to gain it back safely.

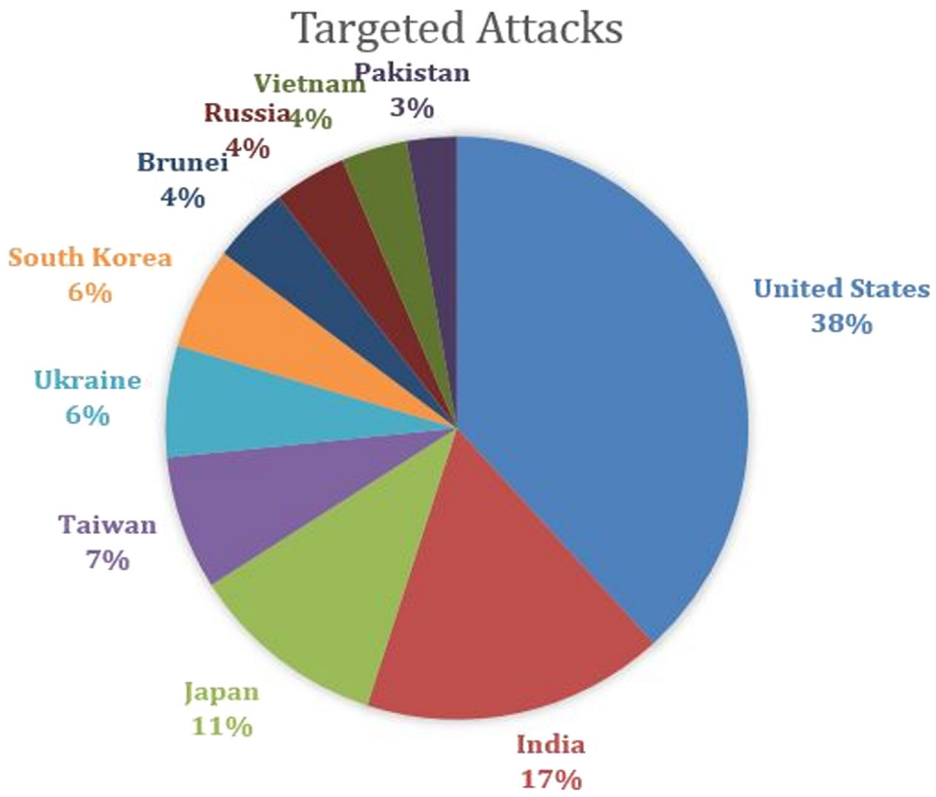

Fig. 11. Ransomware Targeted Attacks [106,107].

Table 6
Current Research Summary.

Ref	Year	Research Titles	Research Type		
			Review Paper	Proposal Paper	Testing Paper
[3]	2017	IoT based ransomware growth rate evaluation and detection using command and control blacklisting		✓	
[10]	2018	Software-defined networking-based crypto ransomware detection using HTTP traffic characteristics)			✓
[21]	2016	Experimental analysis of ransomware on windows and android platforms: Evolution and characterization	✓		
[45]	2017	Evolution target and safety measures	✓		
[48]	2016	Automated dynamic analysis of ransomware: Benefits, limitations and use for detection			✓
[84]	2016	Detecting ransomware with honeypot techniques		✓	✓
[93]	2018	Tracking ransomware end-to-end	✓		
[109]	2018	On the Economic Significance of Ransomware Campaigns: A Bitcoin Transactions Perspective	✓		
[110]	2017	Economic Analysis of Ransomware	✓		
[111]	2017	Analysis and Detection of Ransomware Through Its Delivery Methods			✓
[112]	2018	Leveraging Machine Learning Techniques for Windows Ransomware Network Traffic Detection	✓		✓
[113]	2018	Ransomware Behavioral Analysis on Windows Platforms	✓		✓
[114]	2017	Ransomware Detection based on V-detector Negative Selection Algorithm			✓
[115]	2018	Ransomware Detection Method based on Context-aware Entropy Analysis			✓
[116]	2018	Zero-Day Aware Decision Fusion-Based Model for Crypto-Ransomware Early Detection.	✓		
[117]	2018	RAPPER: Ransomware Prevention via Performance Counters.			✓
[118]	2018	R-Locker: Thwarting Ransomware Action through a Honeyfile-based Approach			✓
[119]	2016	Automated Approach to Detecting Ransomware			✓
[120]	2017	Automatic Ransomware Detection and Analysis Based on Dynamic API Calls Flow Graph			✓
[121]	2017	Crypto Ransomware Analysis and Detection Using Process Monitor	✓		✓
[122]	2017	Deep Learning LSTM based Ransomware Detection			✓
[123]	2017	PayBreak: Defense against Cryptographic Ransomware			✓
[124]	2018	Detecting Ransomware using Support Vector Machines			✓
[125]	2018	Improving Backup System Evaluations in Information Security Risk Assessments to Combat Ransomware	✓		
[126]	2017	Evaluating shallow and deep networks for ransomware detection and classification			✓
[127]	2017	. Extracting the Representative API Call Patterns of Malware Families Using Recurrent Neural Network			✓
[128]	2018	Evolution of Ransomware	✓	✓	
[129]	2018	A novel Self-Organizing Network solution towards Crypto-ransomware Mitigation		✓	
[130]	2017	A 0-day aware Crypto-ransomware early Behavioral Detection Framework		✓	
[131]	2019	Classification of Ransomware Families with Machine Learning based on N-gram of Opcodes			✓
[132]	2018	Talos: No more Ransomware Victims with Formal Methods			✓
[133]	2018	Trusted Detection of Ransomware in a Private Cloud using Machine Learning Methods leveraging Meta-features from Volatile Memory			✓
[134]	2019	DRTHIS: Deep Ransomware Threat Hunting and Intelligence System at the Fog Layer			✓
[135]	2018	Automatically Traceback RDP-Based Targeted Ransomware Attacks			✓
[136]	2018	Ransomware threat Success Factors, Taxonomy, and Countermeasures: A Survey and Research Directions	✓		
[137]	2018	Intrusion and Ransomware Detection System			✓
[138]	2018	White list-based Ransomware Real-time Detection and Prevention for User Device Protection			✓
[139]	2018	Ransomware Detection Considering User's Document Editing			✓
[140]	2017	A State of the Art Survey-impact of Cyber Attacks on SME's	✓		
[141]	2018	Security, privacy & efficiency of sustainable cloud computing for big data & IoT			✓
[142]	2020	Proposing Secure RPL based Internet of Things Routing Protocol: A Review	✓		
[143]	2019	IoT transaction processing through cooperative concurrency control on fog–cloud computing environment			✓
[144]	2020	Lightweight Authenticated-Encryption Scheme for Internet of Things Based on Publish-Subscribe Communication			✓
[145] framework	2018 ✓	Security, privacy and trust of different layers in Internet-of-Things (IoTs)			
[146]	2019	Proposing a Rank and Wormhole Attack Detection Framework using Machine Learning		✓	
[147]	2017 ✓	Security in Internet of Things: issues, challenges, taxonomy, and architecture			
[148]	2020	A Three-Level Ransomware Detection and Prevention Mechanism			✓
[149]	2018 ✓	An overview of Internet of Things (IoT): Architectural aspects,challenges and protocols			
[150]	2019	Cyber Security Issues and Challenges for Smart Cities: A survey	✓		
[151]	2018	Advanced Media-based Smart Big Data on Intelligent Cloud Systems			✓

In recent years ransomware attacks are increasing with a high ratio in each domain of life and targeting individuals, organizations, and industries. The literature shows a higher curve towards ransomware attacks which is expected to be 5 times higher by 2020 and it will exceed more than 6 trillion dollars as ransom against ransomware attacks. In addition, this research further reveals that every 11 s a ransomware attack will occur around the globe. Further, this research focused on the existing IoT linked ransomware attack, mitigation approaches, and suggested prevention methods against ransomware. Prevention becomes easier than getting a remedy after the ransomware attack. User behavior and user training is the key to protect the industries, organizations, and individuals from being infected. Some of the best practices proposed by the FBI include limited privileged, timely backup, disable macro and java scripts, software restriction policies and employee training regarding Ransomware awareness.

To conclude, this research paper provides deeper insights into various aspects of Ransomware including the taxonomy of Ransomware, the evolution of Ransomware, mitigation techniques from Ransomware, ransom payment guidelines and data volume and infection year wise. The paper discusses various challenges that still exist in literature. It also provides the list of current studies to provide work directions to researchers for overcoming existing and upcoming challenges.

5. Future works

Ransomware is the key concern of emerging technological development. However, this development requires a safe and secure path to continue its boom further. This increase in a ransomware attack is an open research issue and a challenge for further growth. In the future, we will further investigate more efficient ransomware mitigation approaches.

References

[1] Azmoodeh A et al. Detecting crypto-ransomware in IoT networks based on energy consumption footprint. J Ambient Intell Hum Comput 2017:1–12.
[2] Lee I, Lee K. The Internet of Things (IoT): Applications, investments, and challenges for enterprises. Bus Horiz 2015;58(4):431–40.
[3] Zahra A, Shah MA. IoT based ransomware growth rate evaluation and detection using command and control blacklisting. IEEE; 2017.
[4] Koopman, M., Preventing Ransomware on the Internet of Things. 2017.
[5] Sharma, P., S. Zawar, and S.B. Patil. Ransomware Analysis: Internet of Things (Iot) Security Issues, Challenges and Open Problems Inthe Context of Worldwide Scenario of Security of Systems and Malware Attacks. in International conference on recent Innovation in Engineering and Management. 2016.
[6] Yaqoob I et al. !!
[65] Alelyani S, Kumar H. Overview of Cyberattack on Saudi Organizations. J Info Security Cybercrimes Resear (JISCR) 2018:1(1).
[66] Mehnaz, S., A. Mudgerikar, and E. Bertino. RWGuard: A Real-Time Detection System Against Cryptographic Ransomware. in International Symposium on Research in Attacks, Intrusions, and Defenses. 2018. Springer.
[67] Homayoun S et al. Know abnormal, find evil: Frequent pattern mining for ransomware threat hunting and intelligence. IEEE Trans Emerging Top Comput 2017.
[68] Mercaldo F, Nardone V, Santone A. Ransomware inside out. IEEE; 2016.
[69] Ganorkar SS, Kandasamy K. Understanding and defending crypto-ransomware. ARPN J Eng Appl Sci 2017;12(12):3920–5.
[70] Matthias Gruber, Evolution of Ransomware, Detecon Switzerland, Accessed on December 2019.
[71] Fayi, S.Y.A., What Petya/NotPetya ransomware is and what its remidiations are, in Information Technology-New Generations. 2018, Springer. p. 93-100.
[72] Paquet-Clouston, M., B. Haslhofer, and B. Dupont, Ransomware payments in the bitcoin ecosystem. arXiv preprint arXiv:1804.04080, 2018.
[73] Aziz SM. Ransomware in High-Risk Environments. Information Technology Capstone Research Project Reports. 2016;1.
[74] Hull G, John H, Arief B. Ransomware deployment methods and analysis: views from a predictive model and human responses. Crime Science 2019;8(1):2.
[75] Kawaguchi Y, Yamada A, Ozawa S, AI,. Web-Contents Analyzer for Monitoring Underground Marketplace. Springer; 2017.
[76] Scaife N, Traynor P, Butler K. Making sense of the ransomware mess (and planning a sensible path forward). IEEE Potentials 2017;36(6):28–31.
[77] Furnell S, Emm D. The ABC of ransomware protection. Computer Fraud & Security 2017;2017(10):5–11.
[78] Bajpai, P., A.K. Sood, and R. Enbody. A key-management-based taxonomy for ransomware. in 2018 APWG Symposium on Electronic Crime Research (eCrime). 2018. IEEE.
[79] Ahn, G.-J., et al., Ransomware and cryptocurrency: partners in crime, in Cybercrime Through an Interdisciplinary Lens. 2016, Routledge. p. 119-140.
[80] Lemmou, Y. and E.M. Souidi. An overview on Spora ransomware. in International Symposium on Security in Computing and Communication. 2017. Springer.
[81] Kiru, M.U. and A.B. Jantan, The Age of Ransomware: Understanding Ransomware and Its Countermeasures, in Artificial Intelligence and Security Challenges in Emerging Networks. 2019, IGI Global. p. 1-37.
[82] Victor Chebyshev, F.S., Denis Parinov, Boris Larin, Oleg Kupreev, Evgeny Lopatin, IT threat evolution Q1 2019 Statistics. https://bit.ly/2Pv1UcZ.
[83] Luo X, Liao Q. Awareness education as the key to ransomware prevention. Information Systems Security 2007;16(4):195–202.
[84] Moore, C. Detecting ransomware with honeypot techniques. in 2016 Cybersecurity and Cyberforensics Conference (CCC). 2016. IEEE.
[85] Kharraz, A. and E. Kirda. Redemption: Real-time protection against ransomware at end-hosts. in International Symposium on Research in Attacks, Intrusions, and Defenses. 2017. Springer.
[86] Gagneja KK. Knowing the ransomware and building defense against it-specific to healthcare institutes. IEEE; 2017.
[87] Everett C. Ransomware: to pay or not to pay? Computer Fraud & Security 2016;2016(4):8–12.
[88] Mercaldo, F., et al. Ransomware steals your phone. formal methods rescue it. in International Conference on Formal Techniques for Distributed Objects, Components, and Systems. 2016. Springer.
[89] Yang, T., et al. Automated detection and analysis for android ransomware. in 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. 2015. IEEE.
[90] Zimba A, Chishimba M. Understanding the Evolution of Ransomware: Paradigm Shifts in Attack Structures. Int J Comput Network Info Security 2019;11(1):26.
[91] Kao, D.-Y. and S.-C. Hsiao. The dynamic analysis of WannaCry ransomware. in 2018 20th International Conference on Advanced Communication Technology (ICACT). 2018. IEEE.
[92] Sultan, H., et al., A SURVEY ON RANSOMWARE: EVOLUTION, GROWTH, AND IMPACT. International Journal of Advanced Research in Computer Science, 2018. 9(2).
[93] Huang, D.Y., et al. Tracking ransomware end-to-end. in 2018 IEEE Symposium on Security and Privacy (SP). 2018. IEEE.
[94] Popoola SI et al. Ransomware: Current Trend, Challenges, and Research Directions. 2017.
[95] Gharib A, Ghorbani A. Dna-droid: A real-time android ransomware detection framework. Springer; 2017.
[96] Kim, M.-S., et al., Security challenges in recent Internet threats and enhanced security service model for future IT environments, 2016. 17(5): p. 947-955.
[97] Z.A. Almusaylim and N. Zaman, "A review on smart home present state and challenges: linked to context-awareness internet of things (IoT) Wireless Networks", 25 (6), 3193-3204.
[98] M. Almulhim, and N. Zaman, "Proposing secure and lightweight authentication scheme for IoT based E-health applications", 2018 20th International Conference on Advanced Communication Technology (ICACT), 481-487.
[99] S. Jawad Hussain, Usman Ahmed, H. Waqas, S. Mir, NZ. Jhanjhi, and M. Humayun, "IMIAD: Intelligent Malware Identification for Android Platform," IEEE 2019 International Conference on Computer and Information Sciences (ICCIS), Al Jouf, Saudi Arabia, 2019.
[100] S.H. Kok, A. Abdullah, NZ. Jhanjhi and M. Supramaniam, "A Review of Intrusion Detection System using Machine Learning Approach", International Journal of Engineering Research and Technology 12 (1), 8-15.
[101] Kok SH, Azween Abdullah NZ, Jhanjhi and Mahadevan Supramaniam,. Ransomware, Threat and Detection Techniques: A Review, IJCSNS International Journal of Computer Science and Network. Security 2019;19 (2):136–46.
[102] Humayun M, Niazi M, Jhanjhi N, et al. Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study. Arab J Sci Eng 2020. doi: https://doi.org/10.1007/s13369-019-04319-2.
[103] M. Lim, A. Abdullah, N. Jhanjhi, M. Khurram Khan and M. Supramaniam, "Link Prediction in Time-Evolving Criminal Network With Deep Reinforcement Learning Technique," in IEEE Access, vol. 7, pp. 184797-184807, 2019. doi: 10.1109/ACCESS.2019.2958873.
[104] M. Lim, A. Abdullah, N. Jhanjhi and M. Khurram Khan, "Situation-Aware Deep Reinforcement Learning Link Prediction Model for Evolving Criminal Networks," in IEEE Access, vol. 8, pp. 16550-16559, 2020.doi: 10.1109/ACCESS.2019.2961805.
[105] Zaman Noor, Ahmed Mnueer. Towards the Evaluation of Authentication Protocols for Mobile Command and Control Unit in Healthcare. J Medic Imaging Health Info 2017;7(3):739–42.
[106] I. Afzal Chesti, M Humayun, N. Us Samar, and NZ. Jhanjhi, Evolution, Mitigation and Prevention of Ransomware, in IEEE 2020 International Conference on Computer and Information Sciences (ICCIS), Al Jouf, Saudi Arabia, 2020.
[107] Casey Crane, 80-eye-opening-cyber-security-statistics-for-2019, Hashedhout by the SSL store at: https://www.thesslstore.com/blog/80-eye-opening-cyber-security-statistics-for-2019/ Accessed on January 2020.
[108] Herrera Juan A, Silva,, et al. A Survey on Situational Awareness of Ransomware Attacks—Detection and Prevention Parameters, in. Remote Sens. 2019;11(10):1168. doi: https://doi.org/10.3390/rs11101168.
[109] Conti, M.; Gangwal, A.; Ruj, S. On the Economic Significance of Ransomware Campaigns: A Bitcoin Transactions Perspective. Comput. Secur. 2018. [CrossRef]
[110] Hernandez-Castro, J.; Cartwright, E.; Stepanova, A. Economic Analysis of Ransomware. arXiv 2017, arXiv:1703.06660.
[111] Gangwar, K.; Mohanty, S.; Mohapatra, A. Analysis and Detection of Ransomware Through Its Delivery Methods. In Proceedings of the International Conference on Recent Developments in Science, Engineering and Technology, Gurgaon, India, 13–14 October 2017; Springer: Berlin/Heidelberg, Germany, 2017; pp. 353–362.
[112] Alhawi OM, Baldwin J, Dehghantanha A. Leveraging Machine Learning Techniques for Windows Ransomware Network Traffic Detection. In: Cyber Threat Intelligence. Heidelberg, Germany: Springer:; 2018. p. 93–106.
[113] Hampton, N.; Baig, Z.; Zeadally, S. Ransomware Behavioural Analysis on Windows Platforms. J. Inf. Secur. Appl. 2018, 40, 44–51. [CrossRef]
[114] Lu, T.; Zhang, L.; Wang, S.; Gong, Q. Ransomware Detection based on V-detector Negative Selection Algorithm. In Proceedings of the 2017 International Conference on Security, Pattern Analysis, and Cybernetics (SPAC), Shenzhen, China, 15–17 December 2017; pp. 531–536.
[115] Jung S, Won Y. Ransomware Detection Method based on Context-aware Entropy Analysis. In Soft Computing. Heidelberg, Germany: Springer:; 2018. p. 1–10.
[116] Al-rimy, B.A.S.; Maarof, M.A.; Prasetyo, Y.A.; Shaid, S.Z.M.; Ariffin, A.F.M. Zero-Day Aware Decision Fusion-Based Model for Crypto-Ransomware Early Detection. Int. J. Integr. Eng. 2018, 10, 82–88 [CrossRef].
[117] Alam, M.; Bhattacharya, S.; Mukhopadhyay, D.; Chattopadhyay, A. RAPPER: Ransomware Prevention via Performance Counters. arXiv 2018, arXiv:180203909.

[118] Gómez-Hernández, J.; Álvarez-González, L.; García-Teodoro, P. R-Locker: Thwarting Ransomware Action through a Honeyfile-based Approach. Comput. Secur. 2018, 73, 389–398 [CrossRef].
[119] Kharraz, A.; Arshad, S.; Mulliner, C.; Robertson, W.K.; Kirda, E. UNVEIL: A Large-Scale, Automated Approach to Detecting Ransomware. In Proceedings of the USENIX Security Symposium, Austin, TX, USA, 10–12 August 2016; pp. 757–772.
[120] Chen, Z.G.; Kang, H.S.; Yin, S.N.; Kim, S.R. Automatic Ransomware Detection and Analysis Based on Dynamic API Calls Flow Graph. In Proceedings of the International Conference on Research in Adaptive and Convergent Systems, Krakow, Poland, 20–23 September 2017; pp. 196–201.
[121] Kardile, A.B. Crypto Ransomware Analysis and Detection Using Process Monitor. Ph.D. Thesis, UT-Arlington, Arlington, TX, USA, 2017.
[122] Maniath, S.; Ashok, A.; Poornachandran, P.; Sujadevi, V.; Sankar, A.P.; Jan, S. Deep Learning LSTM based Ransomware Detection. In Proceedings of the 2017 Recent Developments in Control, Automation & Power Engineering (RDCAPE), Noida, India, 26–27 October 2017; pp. 442–446.
[123] Kolodenker, E.; Koch, W.; Stringhini, G.; Egele, M. PayBreak: Defense against Cryptographic Ransomware. In Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security, Abu Dhabi, UAE, 2–6 April 2017; pp. 599–611.
[124] Takeuchi, Y.; Sakai, K.; Fukumoto, S. Detecting Ransomware using Support Vector Machines. In Proceedings of the 47th International Conference on Parallel Processing Companion, Eugene, OR, USA, 13–16 August 2018; p. 1.
[125] Thomas J, Galligher G. Improving Backup System Evaluations in Information Security Risk Assessments to Combat Ransomware. In Computer and Information Science; CCSE 2018;Volume 11, ISSN:1913–8989.
[126] Vinayakumar, R.; Soman, K.; Velan, K.S.; Ganorkar, S. Evaluating shallow and deep networks for ransomware detection and classification. In Proceedings of the 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Udupi, India, 13–16 September 2017; pp. 259–265.
[127] Kwon I, Im EG. Extracting the Representative API Call Patterns of Malware Families Using Recurrent Neural Network. Proceedings of the International Conference on Research in Adaptive and Convergent Systems, Krakow, Poland September 2017;20–23:202–7.
[128] O'Kane, P.; Sezer, S.; Carlin, D. Evolution of Ransomware. IET Netw. 2018, 7, 321–327 [CrossRef].
[129] Sotelo, M.; Maestre, J.; García, L. A novel Self-Organizing Network solution towards Crypto-ransomware Mitigation. In Proceedings of the 13th International Conference on Availability, Reliability and Security, Hamburg, Germany, 27–30 August 2018; pp. 40–48.
[130] Al-rimy, B.A.S.; Maarof, M.A.; Shaid, S.Z.M. A 0-day aware Crypto-ransomware early Behavioral Detection Framework. In Proceedings of the International Conference of Reliable Information and Communication Technology, Johor Bahru, Malaysia, 23–24 April 2017; Springer: Berlin/Heidelberg, Germany, 2017; pp. 758–766.
[131] Zhang, H.; Xiao, X.; Mercaldo, F.; Ni, S.; Martinelli, F.; Sangaiah, A.K. Classification of Ransomware Families with Machine Learning based on N-gram of Opcodes. Future Gener. Comput. Syst. 2019, 90, 211–221. [CrossRef]
[132] Cimitile, A.; Mercaldo, F.; Nardone, V.; Santone, A.; Visaggio, C.A. Talos: No more Ransomware Victims with Formal Methods. Int. J. Inf. Secur. 2018, 17, 719–738 [CrossRef].
[133] Cohen, A.; Nissim, N. Trusted Detection of Ransomware in a Private Cloud using Machine Learning Methods leveraging Meta-features from Volatile Memory. Expert Syst. Appl. 2018, 102, 158–178 [CrossRef].
[134] Homayoun, S.; Dehghantanha, A.; Ahmadzadeh, M.; Hashemi, S.; Khayami, R.; Choo, K.K.R.; Newton, D.E. DRTHIS: Deep Ransomware Threat Hunting and Intelligence System at the Fog Layer. Future Gener. Comput. Syst. 2019, 90, 94–104 [CrossRef].
[135] Wang, Z.; Liu, C.; Qiu, J.; Tian, Z.; Cui, X.; Su, S. Automatically Traceback RDP-Based Targeted Ransomware Attacks. Wirel. Commun. Mob. Comput. 2018, 2018 [CrossRef].
[136] Al-rimy, B.A.S.; Maarof, M.A.; Shaid, S.Z.M. Ransomware threat Success Factors, Taxonomy, and Countermeasures: A Survey and Research Directions. Comput. Secur. 2018, 74, 144–166 [CrossRef].
[137] El-Kosairy, A.; Azer, M.A. Intrusion and Ransomware Detection System. In Proceedings of the 2018 1st International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, 4–6 April 2018; pp. 1–7.
[138] Kim, D.Y.; Choi, G.Y.; Lee, J.H. White list-based Ransomware Real-time Detection and Prevention for User Device Protection. In Proceedings of the 2018 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 12–14 January 2018; pp. 1–5.
[139] Honda, T.; Mukaiyama, K.; Shirai, T.; Ohki, T.; Nishigaki, M. Ransomware Detection Considering User's Document Editing. In Proceedings of the 2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA), Pedagogical University of Cracow, Cracow, Poland, 16–18 May 2018; pp. 907–914 [CrossRef].
[140] Saleem, J.; Adebisi, B.; Ande, R.; Hammoudeh, M. A State of the Art Survey-impact of Cyber Attacks on SME's. In Proceedings of the International Conference on Future Networks and Distributed Systems (ICFNDS), Cambridge, UK, 19–20 July 2017; Art. No. 52, ISBN 978-1-4503-4844-7.
[141] Stergiou C, Psannis KE, Gupta BB, Ishibashi Y. Security, Privacy & Efficiency of Sustainable Cloud Computing for. Big Data & IoT, Sustainable Computing, Informatics and Systems. 2018.
[142] Zahrah A. Almusaylima, Abdulaziz Alhumam, N.Z Jhanjhi, Proposing Secure RPL based Internet of Things Routing Protocol: A Review, in Adhoc Networks, Vol 101, April 2020. https://doi.org/10.1016/j.adhoc.2020.102096.
[143] Al-Qerem A, Alauthman M, Almomani A, Gupta BB. IoT transaction processing through cooperative concurrency control on fog–cloud computing environment. Soft Comput 2020;24(8):5695–711.
[144] Diro A, Reda H, Chilamkurti N, Mahmood A, Zaman N, Nam Y. Lightweight Authenticated-Encryption Scheme for Internet of Things Based on Publish-Subscribe Communication. IEEE Access 2020;8:60539–51.
[145] Tewari, A., & Gupta, B. B. (2018). Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework. Future generation computer systems.
[146] Fatima-tuz-Zahra, N. Jhanjhi, S. N. Brohi and N. A. Malik, "Proposing a Rank and Wormhole Attack Detection Framework using Machine Learning," 2019 13th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS), Karachi, Pakistan, 2019, pp. 1-9.
[147] Adat V, Gupta BB. Security in Internet of Things: issues, challenges, taxonomy, and architecture. Telecommunication Systems 2018;67(3):423–41.
[148] Ren Amos Loh Yee. Chong Tze Liang, Im Jun Hyug, Sarfraz Nawaz Brohi, NZ Jhanjhi, A Three-Level Ransomware Detection and Prevention Mechanism, EW. EAI 2020. doi: https://doi.org/10.4108/eai.13-7-2018.162691.
[149] Gupta, B. B., & Quamara, M. (2018). An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols. Concurrency and Computation: Practice and Experience, e4946.
[150] B. Hamid, N. Jhanjhi, M. Humayun, A. Khan and A. Alsayat, "Cyber Security Issues and Challenges for Smart Cities: A survey," 2019 13th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS), Karachi, Pakistan, 2019, pp. 1-7.
[151] Psannis KE, Stergiou C, Gupta BB. Advanced media-based smart big data on intelligent cloud systems. IEEE Trans Sustainable Comput 2018;4(1):77–87.