Analysis of Ransomware Technology on Cloud Storage Systems

Advait Deochakke, Amit Kumar Tyagi [0000-0003-2657-8700]

School of Computer Science and Engineering, Vellore Institute of Technology, Chennai 600127, Tamilnadu, India

advaitdeochakke@gmail.com, amitkrtyagi025@gmail.com

Abstract. Over the years cloud computing and cloud storage solutions have grown into over a 50-billion-dollar industry, and that signifies over 50 percent of all corporate data being stored in the cloud as of 2021. In accordance, attacks over these files have grown exponentially, with average damages exceeding multiple millions of dollars per attack. Cloud storages are more susceptible to these attacks, due to the physical factor of accessing local storage being removed, and a simple connection to the internet. Despite the great convenience and arguably fulfilling core necessities during the pandemic, the Cloud storage model is vulnerable and an incredibly juicy target. These ransomware attacks are proving to be huge security risks around the world as such. Combine these with various other problems such as area of jurisdiction of law enforcement agencies and blockchain-based payments making tracing these payments a nigh-impossible task, and the threat is apparent at even the first glance. In this paper, (i) we analyse the insidious nature of ransomware and their power and threat levels, (ii) various papers and industry data to give a comprehensive analysis of the level of security that currently exists, (iii) discuss large security breaches in recent history, and (iv) consider up and coming solutions for cloud storage security. After going through these, we shall draw a final (v) conclusion, on the state of cybersecurity and cloud storage based on presented data.

Keywords: Cloud Storage, Ransomware, Network Security, Decentralized Cloud Storage, Dynamic Data

1 Introduction

Ransomware is a type of malware attack on a computer system, which aims to coerce or threaten the victim to pay money in return for giving them access back to their encrypted and locked system. Ransomware encrypts the software and poses a real threat toward files which are not backed up, in the form of deletion of these files, making the victim lose access to the data, and voiding a vast amount of work and effort [1]. Another threat that ransomware poses is stealing of data. Once the attacker has discovered the various valuable files on the system and encrypts them, it will often lead to the attacker also making a copy of these valuable and sensitive files, which could in turn lead to the victim being blackmailed, the files being publicly released, or worse [1, 2].

In recent years, the threat of ransomware has risen as technologies like cryptocurrency come into the focus of development. The difficulty of tracing transactions and

tracking down perpetrators of the attack to real world persons has been increased by Bitcoin wallets, and compounded with the real-world problem of prosecuting someone who is not in the same country as the victim, makes it much easier to get away after committing such crimes [3, 4].

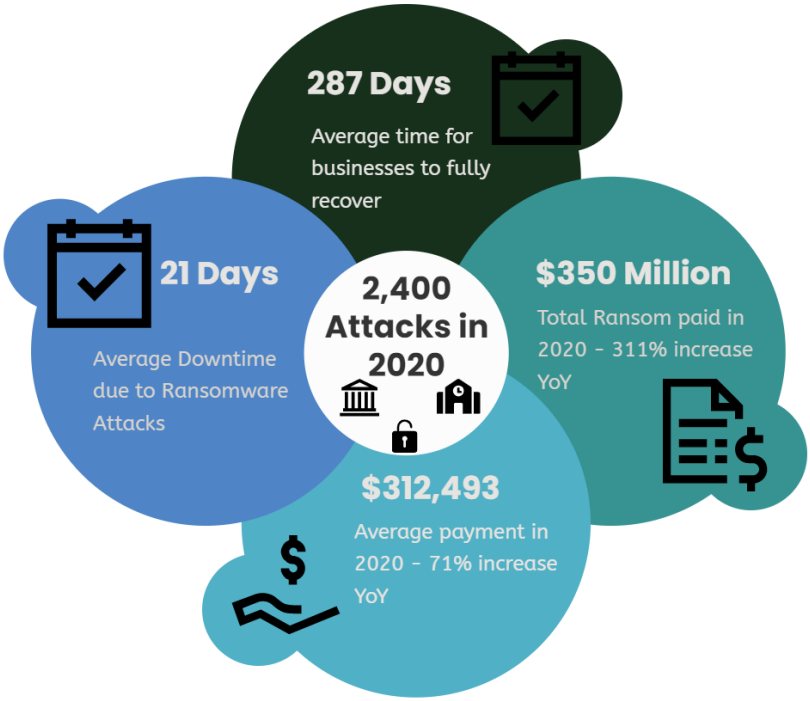

Fig. 1. Damage from Ransomware Attacks in the US [36]

Figure 1 shows some statistics with respect to damages via Ransomware Attacks in previous decade. The first documented ransomware was recorded in 1989, and called the AIDS trojan. Since then, use of such attacks has grown exponentially, hitting over 304 million attacks in 2020, rising to over 62% over 2019. Some high-profile examples are Locky, CryptoLocker, FBI MoneyPak, and WannaCry, which caused damages totaling over $4 Billion according to some estimates [2, 5]. Note that Ransomware doesn't just affect individuals, but can even grind the operations of large corporations to halt, prominent example being an attack on Ultimate Kronos Group's cloud storage, one of the largest human resources companies in the world, which caused damage to millions of workers and companies' dependent on their Private Cloud service.[6] Another example is DDS Safe, where hackers caused irreversible damage to over 400 doctor's offices and their patient data. LinuxEncoder1 is another large-scale ransomware which was the first to target Linux based servers across the globe [5]. Documentation of ransomware is often difficult, due to the largely non-representative nature of the data collected. Reporting various attacks, analyzing ransomware, finding solutions are all relatively relevant for users with high awareness of cybersecurity and a desire to contribute.

As such, most data are collected from customers who have the knowledge and wherewithal to report such attacks to authorities and analysis labs such as BitDefender Labs. Similarly, corporate and government data is typically understated due to fear of backlash from backers, citizens, and users [2].

As resources and possessions stored in the cloud gain value, they become more lucrative targets to attack. As a result, attackers will utilize greater force and effort to take hold of these assets. In an era where organizations are quickly transitioning to cloud-based services, ransomware protection is of the utmost importance. Critical infrastructure such as pipelines, hospitals, government databases are constantly under threat. Many researchers have given solutions to combat such cloud-based cybercrime, and we shall discuss those along with newer and more novel solutions.

2 Nature of Cybercrime and Ransomware

Cybersecurity is an important factor in our times. As such, all analysis and data regarding cybersecurity, whether it be from experience, studies, or derived data, is shared on a wide scale, covering various large international organizations and through governments. As such, every day we get a clearer view into aspects of cybersecurity threats such as ransomware, from various sources such as Symantec, Deloitte, BitDefender Labs, etc., [5, 7]. Cloud computing is an emerging technology, and all models of its service, (a) Software as a Service (SaaS), (b) Platform as a Service (PaaS), and (c) Infrastructure as a Service (IaaS), are vulnerable to attacks. Such cloud service vulnerabilities typically include threats to the user's data, exploits in the API for accessing the cloud, threats from insiders which could bypass a great deal of protection, faults in the cryptography algorithms used, and misconfiguration of service deployment models by organizations [7]. Once a target is selected, the attackers use various methods to install the ransomware onto the system, and valuable data and system functionality is locked.

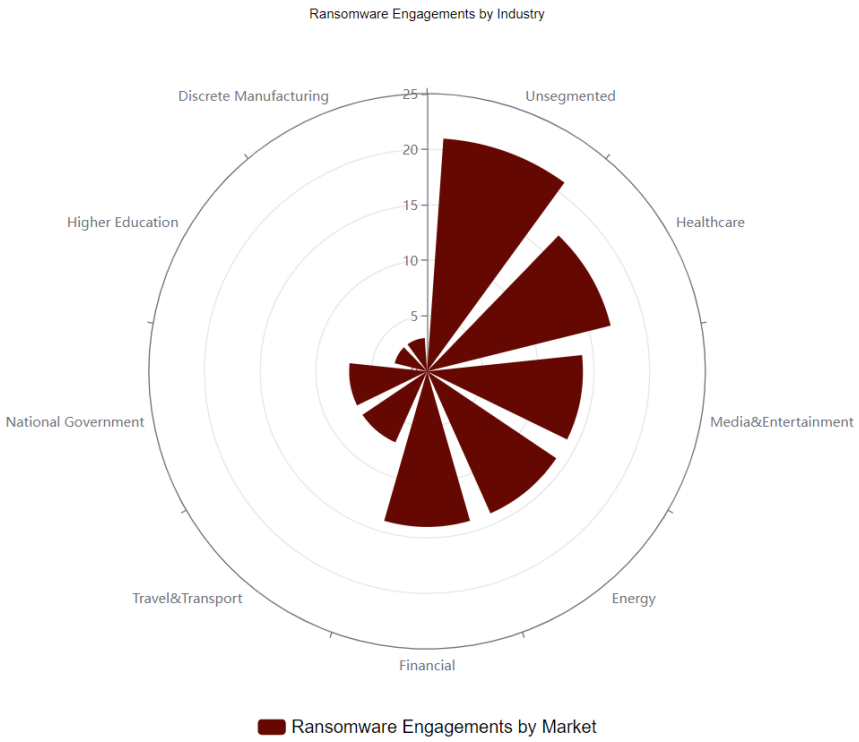

Fig. 2. Ransomware Engagements by Industry [10]

Research by Microsoft's Digital Crime Unit [9] shows that such attacks focus their target primarily on the healthcare sector, followed closely by the media & entertainment, and energy sectors. Findings from the Institute for Security and Technology's Ransomware Taskforce [4, 10] support these findings, as do reports from the Becker Hospital Review. The reason for the lopsided targeting statistics is due to the nature of these systems. Patient data is incredibly valuable to hospitals, and Internet of Things (IoTs) technologies are widespread in modern hospitals which mean hackers can critically affect patient health by locking the systems connected. Similarly, for energy sectors, where power grids are on threat. For attacks on the media and entertainment industry, they tend to focus on live streams of large broadcasters and encrypting source code for various applications such as video games [9, 11]. Figure 2 discusses industry the need of engagement on Ransomware in the previous decade.

2.1 Technical Vectors of Attack

Vectors for ransomware attacks include e-mail spam and phishing attacks, a popular method including JavaScript trojan downloader, Nemucod. Exploit Kits are another aspect involved in these attacks. Exploit Kits are a sort of repository for managing various exploits for any given system, which vastly broadens the attack surface by attacking

multiple possible vulnerabilities instead of just one. Another vulnerability commonly exploited is Microsoft's Remote Desktop Protocol, which allows anyone with credentials to log onto another machine with RDP enabled and use it as their own, as long as it is connected to the internet, often used in scam phishing-based attacks [3, 4]. Unpatched vulnerabilities can also lead to such ransomware deployments, some of which are part of zero-day exploits. Zero-day exploits involve utilizing bugs in the code which remained unknown, generally involving hacking into the developer's files to get hold of software before release. More advanced tactics utilize man-in-the-middle attacks to exploit the synchronization token system of cloud services, so that the attacker can intercept the token and replace it with a new one which provides access to the attacker. The compromised user may never know about it, as the attacker can also place the synchronization token right back in [7].

2.2 Socially Engineered Vectors

Phishing is a type of attack which uses social-engineering concepts and sends a target authoritative-looking emails or messages, typically including company logos and email ids similar to official ones, which can be easily mistaken if one does not look closely. Such phishing attempts may frequently involve Whaling or CEO fraud. Spear phishing involves specifically targeting the organization to gain access by compromising one of the many organization member accounts [12]. Stolen passwords are also a real threat, as many unaware users will use the same password or its iterations across multiple or all of their accounts. This could lead to the compromise of one system leading to another completely unrelated organization and their systems falling under threat, due to an employee of one organization using the same password for their account in another system and application [13].

2.3 Ransomware-as-a-Service

Sometimes the creator of the ransomware may not be the party who actually uses it, but will act as a seller for the ransomware, leading to the coining of the term Ransomware-as-a-Service (RaaS). [14] Similar to SaaS solutions, the developers of the Expoilt-Kits and other malware tools will lease their products to interested parties, letting any inexperienced, run-off-the-mill crook deploy and initiate ransomware attacks. Reports by Group-IB state that over two-thirds of all ransomware attacks in 2020 used RaaS solutions. [15] Two of the key players in this business are REvil and DarkSide, who were responsible for the JBS attacks and Colonial Pipeline attacks respectively, which we have previously mentioned [11]. In ransomware attacks on cloud systems, the responsibility is shared between the customer and the service provider, even though it might appear as if the user has less responsibility due to the assumed and contract-bound trust being handed to the service provider. Both must remain vigilant against such threats. In today's web of interconnected web services, a single breach can sometimes bring down entire networks [7].

3 Current Countermeasures

While ransomware is threatening, there are various countermeasures to mitigate its effects and ensure some degree of safety. We discuss various such widely used countermeasures below.

3.1 Repositories and Data Sharing

One of the best methods of making sure that countermeasures we use are solid and up to date, is using and sharing information repositories for this task. Maintaining such repositories and being aware of them helps organizations cover their bases, as the repositories will store countermeasures and solutions for multitudes of software vulnerabilities. Notable repositories include the MITRE Common Vulnerabilities and Exposures initiative from 1990, the National Institute of Standards and Technology's National Vulnerability Database. Typically, it may not be ideal for many users to actively keep track of such and such many vulnerability and threat management systems have been devised, such as Microsoft's Defender for Endpoint [7, 16].

3.2 Behavior based detection

System-based detection entails regular integrity checks for various files, detecting whether there have been suspicious API calls, or detecting keylogging and window captures, and finally monitoring resource usage of OS and I/O systems. Traffic analysis can unveil whether there exist significant fluctuations from the normal and expected rates [16]. File-based detection generally involves checking for signs of malicious activity in specific formats for files, typically involving disguised executables and other known ransomware file extensions and signatures. File activity monitoring such as files being accessed over the network beyond a certain expected threshold are commonly used, but can often result in false negatives [17].

Honeypot strategies involve setting up a VM or sacrificial storage to temporarily store new files in, and checking their immediate behavior. If files start getting encrypted, it serves as an early warning system. Throttling the throughput of these honeypots can further increase the time that is available to system administrators to cut off the honeypot and prevent cloud-wide infection.[18]

3.3 Reverse Engineering

Reverse engineering involves discovering the key to the ransomware encryption and using it to recover infected files. The most important use case for this method is when prevention techniques used by antivirus software fail, resulting in system damage. Reverse engineering may be able to recover lost data without causing complete destruction or having to pay the ransom. The key disadvantage here being that the necessary prerequisite for this method, the existence of a decryption key of the targeted system, might not always be fulfilled [5, 19].

3.4 Risk Disclosure and Awareness

Getting affected by ransomware, for corporations, often means that there is a threat of bringing harm to shareholder and customer interests. With this statement in mind, it makes sense when a non-negligible number of incidents are either reported to be much less severe than in actuality, or go unreported and privately resolved. Awareness of cybersecurity entails reducing risks of employees leaking valuable and sensitive company data, whether they have malicious intentions in mind, or unintentionally let it happen. Underestimating dangers posed by cybersecurity threats and simply ignoring risk control instructions are some reasons due to which such breaches might occur. Peer behavior, previous experience, and regularly prompting employees to take action to ensure security are all key components to this [20, 21].

3.5 Decentralization and All-Or-Nothing Transforms

Decentralization inherently limits the ceiling of risk and threats that ransomware poses. The utilization of multiple independent and comparatively reduced risk of compromise, as there is no longer a single point of failure. All files are added only when the majority clears the file for addition to the main server, and verifying data integrity is easy due to multiple copies of data existing across the users. AONT facilitates both availability and security of data against malicious actors [22, 23]. Despite so many powerful countermeasures, ransomware still remains an extremely huge threat. We shall now look at various large breaches and ransomware related incidents in recent history.

4 Impact of Ransomware in Recent History

As long as data holds value, hackers will desire to utilize it as a means for profit or even furthering their agenda in niche cases.

4.1 Healthcare incidents

A study by Comparitech shows over $20 billion in losses due to ransomware attacks on clinics, hospitals, and healthcare organizations. J&J's chief information security officer, Marene Allison, further states that Johnson & Johnson Group receives over 15.5 billion cybersecurity incidents on a daily basis. [24]. The WannaCry ransomware in 2017 also had a tremendous impact on hospitals, crippling tens of thousands of computers from the National Health Service hospitals in Great Britain [25].

4.2 Colonial Pipeline

Having to pay over $4.4 million in bitcoin as ransom, the need to mitigate disruption of nationwide critical infrastructure is very visible. Amidst the 2021 April oil shortages, this feeling felt much more impactful than it would usually, in times of prosperity and abundance [26]. Even though the FBI were able to recover over $2.3 million of the

Bitcoin, catching the perpetrators from the DarkSide gang remained difficult, due to the very nature of such attacks [9, 27].

4.3 CD Projet Red

Polish hit game developer, CD Projket Red, were hit in February of 2021, where the HelloKitty group got hold over the source code for their recently released billion-dollar game, Cyberpunk 2077, amongst others, and demanded high ransom, with CD Projekt Red denying to pay the fees, as they had backups in place [28]. This demonstrates good corporate practices, as not paying ransom discourages hackers from performing more malicious activities.

4.4 Ultimate Kronos Group

One of the most recent cases we will analyse in this paper, when hackers gained control of their Kronos Private Cloud service, leading to payroll systems of over dozens of private and government entities. Over 8,000 workers have experienced problems with their paychecks, upt o as recent as mid-January 2022 [6]. This is closely timed to the reporting of the Log4J vulnerability in Java running machines, on which Kronos' servers were based. However, there is no confirmation of this from Kronos Group. [29]

4.5 REvil Group

Most likely one of the highest profiles RaaS groups, the Russian based operation has recently been declared as dismantled by the Russian Federal Service. Multiple ransomware attacks have been attributed to them, including the attack on JBS, the world's largest meat packer, the attack on Kaseya Group, a large software infrastructure management company based in America, and also the stealing various plans for Apple's up and coming products from one of their suppliers, Quanta Computer [26]. Its impact remains immeasurable, as a group member claimed to earn over $100 million in ransoms per month, and due to the similarities of its code and ransom structure with another highly prominent group, DarkSide. The similarities could imply that REvil is an offshoot of DarkSide, or a partner. Another important aspect is the peculiar code to check that the victim of the cyberattack is not situated in Russia, or more accurately the Commonwealth of Independent States which formed after the fall of the Soviet Union, perhaps leading to concerns about state-run hacker organizations.

5 Emerging Solutions

Few of existing solutions for tracing the cyber-attacks can be included here as:

5.1 Secure Network Protocols for Dynamic Data

B.Sengupta's paper leverages Secure Network coding techniques in the construction of a protocol, DSCS I, enabling a guarantee for dynamic provable data possession. DSCS, we work well on a standard data model, while a second protocol introduced in the same paper, DSCS II, finds a use in being very efficient for real-world append-only data, but is not efficient for arbitrary modifications for generic data [30]. The protocol facilitates authenticity of data, as the storage server must keep the proof of data possession tags untampered, lest the challenge of testing integrity by customer fails. The protocol further necessitates the freshness of data, as the provider must keep the storage up to date if the authentication challenge is to be passed [30].

5.2 Analysis of Network Traffic on Multiple Classifiers

A paper by Ahmad O. has illustrated clearly how ransomware will affect all kinds of network traffic data, with the Locky ransomware as the test case [31]. The paper found over five times increase in TCP resets when a malicious software was introduced to the testbed, an increase of over 80 times in HTTP-POSTs. A sudden and incredibly high increase in the error frequencies for DNS names was also found, due to the large amount of pseudo-random domain names generated by the DGA algorithm in Locky. By analysis of network-based ransomware, the model was able to achieve over 97% accuracy in detecting the software, and signifies a leap in preventing network-based ransomware once samples are analyzed [31].

5.3 Dynamic Distributed Storage

Dynamic distribution provides a high degree of confidentiality, security, and resilience of data in the cloud. It utilizes fast and local encryption prior to the data leaving the local network, along with a permanently stored key with a filtered interface to prevent as much of the attack surface as possible. Storing the data over multiple cloud servers provides a high degree of redundancy, and can be scaled as high as desired. This helps in the event that the cloud provider faces a compromise in their servers, so that in the event where even some of the servers on which data is stored are affected, the data stored in the rest is still salvageable and as such can be restored and redistributed [8, 32].

5.4 Machine Learning and Artificial Intelligence

Symantec, a leading player in cybersecurity, has introduced its machine learning heuristic technology, Sapient. It applies natural language processing to help train computers in finding the hidden patterns in all the tens of thousands of cybersecurity incidents which could be happening on a daily basis for large organizations. Machine learning takes a step past recognizing threats and fixing them, to predicting such threats and acting on the data to minimize losses [10]. Symantec's Sapient blocked a full 100% of ransomware samples seen with cloud support. The WannaCry outbreak was also

prevented at zero-day on systems with Symantec's Endpoint Protection enabled, showcasing the power of such techniques.

5.5 Decentralization

Albeit mainstream, it is still an emerging technology. Decentralization involves shifting the control over infrastructure from a single entity, and a single point of failure, to a trustless, distributed environment, with very few points of weakness. It further helps facilitate optimization of resources, and opens up a shared ledger to guarantee the validity of data movements. As no one "owns" the data, it becomes a collectively owned and maintained system, however it comes with the drawback of performance decreasing for all members as more and more members join the decentralized system, but that is the cost of security which must be paid [20, 33].

5.6 Key Backup

Key encryption uses a public-private key pair to encrypt the data, and the private key is stored locally. The "public" key can either be in the form of (1) Using a public key for encryption, making it easy to manage target data, or (2) Using group or individual keys for targets. Using a hook, we can latch onto the key backup which gets stored on the target's systems, and extract the key to prevent extensive harm to the victim [7]. As opposed to other solutions showcased in this paper, K. Lee's paper on key backup highlights a general case which does not require prior knowledge of the ransomware or its habits, utilizing the locally stored key in addition with a public key, which can be obtained after paying one set of ransom at a reasonable price [16]. Further, researchers are suggested to refer several possibilities with cyber security including issues, challenges and recommended countermeasures with modern techniques/ technologies in [37-45].

6 Conclusion

The number of criminals and cybersecurity threats in the world is far lesser in number than the number of experts constantly working towards improving security and reliability. However, due to exploits being much too easy to find than they are to fix, these few continue to be a large global threat, which the entire world is slowly coming to realize and act against.

The constant improvements in all fields related to security all over the world are slowly but surely leading to a privacy-guaranteed, and security-guaranteed environment, but the journey remains ever so dangerous. Without realizing and acknowledging the threats we face, we will not be able to act appropriately against them, and I hope that this paper facilitates to not only highlight the problem, but also help drive the development of improvements in all fields continuously.

7 References

1. Ransomware: What It Is & What To Do About It, Internet Crime Complain Center, [Accessed Jan2022]https://www.ic3.gov/Content/ PDF/Ransomware_Fact_Sheet.pdf
2. C. Simoiu, C. Gates, J. Bonneau, S. Goel, “A study of ransomware, USENIX Symposium on Usable Privacy and Security (SOUPS) 2019”. August 11–13, 2019, Santa Clara, CA, USA
3. Deloitte Threat Intelligence and Analysis Report: Ransomware, August 2016, [Accessed January 2022]
4. Symantec ISTR: Ransomware Special Edition, 2017, [Accessed January 2022] https://docs.broadcom.com/doc/istr-ransomware-2017- en
5. "WannaCry" ransomware attack losses could reach $4 billion, May 2017, [Accessed Jan 2022] https://www.cbsnews.com/news/wannacry ransomware-attacks-wannacry-virus-losses/
6. Kronos Community report on the cyberattack, December 2021, [Accessed Jan 2022] https://community.kronos.com/s/feed/0D54M00004wJKHiSAO? language=en_US
7. Does a Ransomware Attack Constitute a Data Breach? Increasingly, It May, Jan 2021, [Accessed Jan 2022].
8. Ramesh, D., Mishra, R. & Edla, D.R. Secure Data Storage in Cloud: An e-Stream Cipher-Based Secure and Dynamic Updation Policy. Arab J Sci Eng 42, 873–883 (2017). https://doi.org/10.1007/s13369- 016-2357-2
9. Kemba Walden, Assistant General Counsel, Microsoft Digital Crime Unit, at HEARING ON "STOPPING DIGITAL THIEVES: THE GROWING THREAT OF RANSOMWARE": US House of Energy and Commerce [Accessed Jan 2021] https://energycommerce.house.gov/committee-activity/hearings/hearing-on-stopping-digital-thieves-the-growing-threat-of-ransomware
10. IBM X-Force Threat Report : Executive Summary, 2021, [Accessed Jan 2022] https://www.ibm.com/downloads/cas/AWJ3PE1M
11. The 2021 Evil Internet Minute, RiskIQ, [Accessed Jan 2022] https:// www.riskiq.com/resources/infographic/evil-internet-minute-2021/
12. Junger, M., Wang, V. & Schlömer, M. Fraud against businesses both online and offline: crime scripts, business characteristics, efforts, and benefits. Crime Sci 9, 13 (2020). https://doi.org/10.1186/s40163-020- 00119-4
13. Ling Li, Wu He, Li Xu, Ivan Ash, Mohd Anwar, Xiaohong Yuan, “Investigating the impact of cybersecurity policy awareness on employees’ cybersecurity behavior,” International Journal of Information Management, Volume 45, 2019, Pages 13-24, ISSN 0268-4012, https://doi.org/10.1016/j.ijinfomgt.2018.10.017.
14. Manky D. Cybercrime as a service: a very modern business. J Comput Fraud Sec. 2013;2013(6):9-13.
15. Ransomware Uncovered 2020/2021, [Accessed Jan 2022], https://explore.group-ib.com/ransomware-reports/ransomware_uncove red_2020
16. Lee, K, Yim, K, Seo, JT. Ransomware prevention technique using key backup. Concurrency Computat: Pract Exper. 2018; 30:e4337. https://doi.org/10.1002/cpe.4337
17. Securing your AWS Cloud environment from ransomware, April 2021, [Accessed Jan 2022] https://d1.awsstatic.com/WWPS/pdf/AWSPS_ransomware_ebook_Ap r-2020.pdf
18. Takahashi, T, Panta, B, Kadobayashi, Y, Nakao, K. Web of cybersecurity: Linking, locating, and discovering structured cybersecurity information. Int J Commun Syst. 2018; 31:e3470. https://doi.org/10.1002/dac.3470

19. Linux Ransomware Debut Fails on Predictable Encryption Key, Nove 2015, Bitdefender Labs, [Accessed Jan 2022] http://labs.bitdefender.com/2015/11/linux-ransomware-debut-fails-on predictable-encryption-key/
20. E. Bacis, S. De Capitani di Vimercati, S. Foresti, S. Paraboschi, M. Rosa and P. Samarati, "Securing Resources in Decentralized Cloud Storage," in IEEE Transactions on Information Forensics and Security, vol. 15, pp. 286-298, 2020, doi: 10.1109/TIFS.2019.2916673.
21. He Li, Won Gyun No, Tawei Wang, SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors, International Journal of Accounting Information Systems, Volume 30, 2018, Pages 40-55, ISSN 1467-0895, https://doi.org/10.1016/j.accinf.2018.06.003.
22. J. Castiglione and D. Pavlovic, "Dynamic Distributed Secure Storage Against Ransomware," in IEEE Transactions on Computational Social Systems, vol. 7, no. 6, pp. 1469-1475, Dec. 2020, doi: 10.1109/TCSS.2019.2924650.
23. Giuseppe Ateniese, Özgür Dagdelen, Ivan Damgård, Daniele Venturi, Entangled cloud storage, Future Generation Computer Systems, Volume 62, 2016, Pages 104-118, ISSN 0167-739X, https://doi.org/10.1016/j.future.2016.01.008.
24. Ransomware attacks on US healthcare organizations cost $20.8bn in 2020, [Accessed Jan 2022] https://www.comparitech.com/blog/information-security/ransomware attacks-hospitals-data/
25. Cloud presents biggest vulnerability to ransomware, September 2021, [Accessed Jan 2022] https://www.securitymagazine.com/articles/96148-cloud-presents biggest-vulnerability-to-ransomware
26. Report on Ransomware Trends, May 2021, HC3, [Accessed Jan 2022] https://www.hhs.gov/sites/default/files/ransomware-trends 2021.pdf
27. US recovers millions in cryptocurrency paid to Colonial Pipeline ransomware hackers, June 2021, [Accessed Jan 2022] https://edition.cnn.com/2021/06/07/politics/colonial-pipeline-ransomware-recovered/index.html
28. Tweet title: Important Update, CDPROJEKTRED, [Accessed Jan 2022] https://twitter.com/CDPROJEKTRED/status/1359048125403590660
29. Apache Log4j Vulnerability Guidance: CISA, [Accessed Jan 2022] https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance
30. B. Sengupta, A. Dixit and S. Ruj, "Secure Cloud Storage with Data Dynamics Using Secure Network Coding Techniques," in IEEE Transactions on Cloud Computing, doi: 10.1109/TCC.2020.3000342.
31. A. O. Almashhadani, M. Kaiiali, S. Sezer and P. O'Kane, "A Multi Classifier Network-Based Crypto Ransomware Detection System: ACase Study of Locky Ransomware," in IEEE Access, vol. 7, pp. 47053-47067, 2019, doi: 10.1109/ACCESS.2019.2907485.
32. F. Lu, W. Li, H. Jin, L. Gan and A. Y. Zomaya, "Shadow-Chain: A Decentralized Storage System for Log Data," in IEEE Network, vol. 34, no. 4, pp. 68-74, July/August 2020, doi: 10.1109/MNET.011.1900385.
33. What is Decentralization in Blockchain?, [Accessed Jan 2022] https://aws.amazon.com/blockchain/decentralization-in-blockchain/
34. Share of corporate data stored in the cloud in organizations worldwide from 2015 to 2021, [Accessed Jan 2022] https://www.statista.com/statistics/1062879/worldwide-cloud-storage of-corporate-data/
35. Annual number of ransomware attacks worldwide from 2016 to 2020, [Accessed Jan 2022, https://www.statista.com/statistics/494947/ransomware-attacks-per year-worldwide/
36. Institute for Security and Technology, Ransomware Task Force Report: April 2021, [Accessed January 2022] https://securityandtechnology.org/wp-content/uploads/2021/04/IST-Ransomware-Task-Force-Report.pdf

37. G. Vishnuram, K. Tripathi and A. Kumar Tyagi, "Ethical Hacking: Importance, Controversies and Scope in the Future," 2022 International Conference on Computer Communication and Informatics (ICCCI), 2022, pp. 01-06, doi: 10.1109/ICCCI54379.2022.9740860.
38. A. Deshmukh, N. Sreenath, A. K. Tyagi and U. V. Eswara Abhichandan, "Blockchain Enabled Cyber Security: A Comprehensive Survey," 2022 International Conference on Computer Communication and Informatics (ICCCI), 2022, pp. 1-6, doi: 10.1109/ICCCI54379.2022.9740843
39. Meghna Manoj Nair, Amit Kumar Tyagi, Richa Goyal, Medical Cyber Physical Systems and Its Issues, Procedia Computer Science, Volume 165, 2019, Pages 647-655, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2020.01.059.
40. Amit Kumar Tyagi, G. Aghila, "A Wide Scale Survey on Botnet", International Journal of Computer Applications (ISSN: 0975-8887), Volume 34, No.9, pp. 9-22, November 2011.
41. Amit Kumar Tyagi. Article: Cyber Physical Systems (CPSs) – Opportunities and Challenges for Improving Cyber Security. International Journal of Computer Applications 137(14):19-27, March 2016. Published by Foundation of Computer Science (FCS), NY, USA.
42. G. Rekha, S. Malik, A.K. Tyagi, M.M. Nair "Intrusion Detection in Cyber Security: Role of Machine Learning and Data Mining in Cyber Security", Advances in Science, Technology and Engineering Systems Journal, vol. 5, no. 3, pp. 72-81 (2020).
43. S. Mishra and A. K. Tyagi, "Intrusion Detection in Internet of Things (IoTs) Based Applications using Blockchain Technology," 2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2019, pp. 123-128, doi: 10.1109/I-SMAC47947.2019.9032557.
44. Amit Kumar Tyagi, N. Sreenath, Cyber Physical Systems: Analyses, challenges and possible solutions, Internet of Things and Cyber-Physical Systems, Volume 1, 2021, Pages 22-33, ISSN 2667-3452,https://doi.org/10.1016/j.iotcps.2021.12.002.
45. Shabnam Kumari, Amit Kumar Tyagi, Aswathy S U, "The Future of Edge Computing with Blockchain Technology: Possibility of Threats, Opportunities and Challenges", in the Book "Recent Trends in Blockchain for Information Systems Security and Privacy", CRC Press, 2021.

Biographies

Advait Deochakke is currently a student enrolled in Vellore Institute of Technology, Chennai, pursuing a bachellors' degree in Computer Science and Engineering. His main interests include cybersecurity, distributed computing, and a newfound curiosity for marketing. He hopes to pursue a Masters in IT after graduation.

Amit Kumar Tyagi is Assistant Professor (Senior Grade), and Senior Researcher at Vellore Institute of Technology (VIT), Chennai Campus, Chennai, Tamilandu, India. He received his Ph.D. Degree (Full-Time) in 2018 from Pondicherry Central University, India. He joined the Lord Krishna College of Engineering, Ghaziabad (LKCE) for the periods of 2009-2010, and 2012-2013. He was an Assistant Professor and Head- Research, Lingaya's Vidyapeeth (formerly known as Lingaya's University), Faridabad, Haryana, India in 2018-2019. His supervision experience includes more than 10 Masters' dissertations and one PhD thesis. He has

contributed to several projects such as “AARIN” and “P3- Block” to address some of the open issues related to the privacy breaches in Vehicular Applications (such as Parking) and Medical Cyber Physical Systems (MCPS). He has published over 50 papers in refereed high impact journals, conferences and books, and some of his articles awarded best paper awards. Also, he has filed more than 20 patents (Nationally and Internationally) in the area of Deep Learning, Internet of Things, Cyber Physical Systems and Computer Vision. He has edited more than 15 books for IET, Elsevier, Springer, CRC Press, etc. Also, he has authored 3 Books on Internet of Things, Intelligent Transportation Systems, Vehicular Ad-hoc Network with BPB Publication, Springer and IET publisher. He is a Winner of Faculty Research Award for the Year of 2019, and 2020 (consecutive years) given by Vellore Institute of Technology, Chennai, India. Recently, he has been awarded best paper award for paper titled “A Novel Feature Extractor Based on the Modified Approach of Histogram of oriented Gradient”, ICCSA 2020, Italy (Europe). His current research focuses on Next Generation Machine Based Communications, Blockchain Technology, Smart and Secure Computing and Privacy. He is a regular member of the ACM, IEEE, MIRLabs, Ramanujan Mathematical Society, Cryptology Research Society, and Universal Scientific Education and Research Network, CSI and ISTE.