A Prototypical Adoption Security Model for Major Vulnerabilities in Cloud Computing

S.G.M.U. Kumarasinghe[1*], M.S. Shafana[2] & M.J. Ahamed Sabani[3]

[1,2,3]*Department of Information and Communication Technology, Faculty of Technology, South Eastern University of Sri Lanka, Sri Lanka*

[1*]uddhika5004@gmail.com, [2]zainashareef@seu.ac.lk, [3]mjasabani@seu.ac.lk

Abstract- *Companies around the world are speedy in using the cloud to revolutionize their digital transformation initiatives. Cloud Computing enables companies to outsource the entire Information Technology process to stay focused on their core business to improve their productivity and creativity in providing clients with services. It allows companies to reduce the high cost of IT infrastructure without losing attention to customer needs. Although the cloud provides a lot of benefits that attract organizations, data security is one of few things which hold back companies from adopting cloud computing solutions. Cloud infrastructure could be complicated, and where complexity and security issues definitely exist. There exist unique cloud computing security issues in a cloud computing infrastructure. Data are stored in the cloud and accessed through the internet via a third-party provider. This means that there is limited visibility and control over the data, which is not a thing to be ignored. There are many other security threats to cloud computing vulnerabilities that cannot be ignored. This paper is going to describe some of the security threats on cloud computing vulnerabilities and will provide a prototypical model to adopt as a solution to overcome the major vulnerabilities. The goal is to convey the proper information to the users (organizations) who are thinking of deploying clouds for their organizations. This paper will help them to be conscious about opting for a proper cloud service provider and will help them in taking precautions to avoid the security issues.*

Keywords: Cloud computing, Threats, Security model, Vulnerabilities, CSP, cloud service provider

I. INTRODUCTION

The global market for public cloud services is steadily growing. According to Gartner, "The global market for public cloud services will expand by 17% in 2020 to $266.4 billion from $227.8 billion in 2019"(Worldwide Public Cloud Revenue to Grow 17% in 2020, 2019). Organizations are trying to migrate to existing cloud or developing new applications using cloud-based platforms. Analyzing cloud computing service provider is very crucial before deploying cloud computing infrastructure in organization. A company which adopts cloud computing or opt cloud service provider by ignoring all the risks associated with them is basically invites all the financial, technical and compliance risk to its organizations.

Cloud providers are a diverse, distributed and completely virtualized which makes cloud unique. Cloud has large pool of resources and has many specific characteristics if we compare it to traditional technologies. That's why traditional security precautions such as identification, authentication and authorization are not sufficient in case of cloud computing. Due to its method of service deployment, operations, and enabling technologies, cloud computing presents organizational risks different from traditional IT. The integration of security into the cloud services often makes it harder to solve the problem. Many companies concern moving the critical applications of the organization and its legacy database with sensitive information to the Cloud Service Provider. To reduce this concern, cloud service providers must ensure that its applications and sensitive data continue to be provided to customers with the same security and control as upstream systems. To achieve this, the cloud service providers must provide a customer with evidence that all service level contracts have been met and that auditors can ensure compliance. High data volume on the cloud is stored, and this data requires an internet connection. This means that anyone who uses cloud services may face cyber-attacks such as Distributed Denial of Service (DDoS) attacks, which are increasingly a common threat in cloud computing. Hackers send unprecedented traffic volumes to an application on the Web, thus further crashing the cloud servers. Companies should have steady regulations governing who can access the data. It can be challenging to track who really can access these

details with cloud computing easily access large-scale data(Khan and Al-Yasiri, 2016).

This study aimed to determine cloud computing vulnerabilities and threats that lead to those security issues. Vulnerabilities relate to system gaps that allow attacks to succeed, and threats are an assault that attempts to exploitations resources or information on system gaps. By dealing with these issues, we strive to strengthen the organizational preparedness of the cloud computing by providing a prototype for adoption. Since security is the most viable thing to cloud adoption, adding enough security is very important for cloud service providers.

II. LITERATURE REVIEW

Recently, the Cloud computing has emerged as a new paradigm which is enabling organizations to migrate all of their infrastructure from physical to virtual (cloud). Cloud Service Providers (CSP) around the globe are attracting organizations to adopt cloud and use their services. These providers attract them by mentioning bunch of advantages (High storage, high performance computing scalability etc.) moving towards cloud (Ramamurthy et al., 2020). They actually provide these benefits but there are a lot of security threats on cloud computing vulnerabilities which are ignored. Users does not give much importance to those issues and in the end, they find problems after moving towards cloud. Cloud security threats are multifaceted, and hackers continue to exploit those security vulnerabilities in clouds (Girma, Garuba and Li, 2015). Security defects must be detected to provide better quality of service for cloud users, so that an effective defense mechanism must be established (Chandra, Challa and Pasupuleti, 2016). Cloud service providers must check the cloud at regular intervals to prevent external threats from occurring. Furthermore, cloud providers must ensure that all Service Level Agreements (SLAs) are met, and human errors are reduced to make it possible for them to work smoothly (Ibrahim, Varrette and Bouvry, 2018). Keep in mind that cloud service providers are using a shared security responsibility model. Responsibilities for some security aspects are taken by the CSP. The CSP and the consumer share other security aspects. And certain security aspects remain a consumer's sole responsibility. The knowledge and performance of all consumer responsibilities depends on effective cloud security. Consumers' lack of understanding or lack of fulfillment of their responsibilities is a major cause of cloud-based cybersecurity threats. Our studies indicate the importance of data confidentiality in this field and introduction to *cloud computing security threats(Gupta and* Kumar, 2019). Most of the researchers work on the use of encryption techniques in the field of cloud computing, data security and organizational cloud deployment issues. This paper produces a simple and basic security analysis of security threats on cloud computing vulnerabilities and possible solution to those threats. Researchers seldom ignore vulnerabilities regarding cloud computing security. Therefore, this research identified the major and up to date vulnerabilities and also analyzed possible solution to cloud computing deployment threats. These vulnerabilities are major concern in cloud computing security. This study emphasizes strengthening the organizational preparedness of the cloud computing adoption framework. Since security is the most viable thing to cloud adoption, adding enough security is very important for cloud service providers.

III. METHODOLOGY

The methodology that is used to collect the knowledge on finding the facts about Security threats on cloud computing vulnerabilities, is to use the academic journals and the research papers that are interrelated with the topic of this study. By reading several kinds of research papers and academic papers related with this topic on Security threats on cloud computing vulnerabilities, it was able to get a rich knowledge on the respective field. The sources for this study are from various kind of multiple databases, university repositories, digital libraries, and web sites.

The technological information such as details about cloud platforms and related software information are collected from various kind of technology related and technical business official websites. By studying those resources that are published with those websites were gathered to analyze the common approach related with them to conduct the major research on Security threats on cloud computing vulnerabilities.

Those materials that collected to gain the knowledge, and ideas can be categorized as several types such as the related articles from blogs, e-commerce websites, and the research paper related to this study. Most of the information is based with the original works of those authors. Therefore, their originality and the trustworthiness

along with the content included with those papers are within the satisfied levels. Because of that it was able to do this study by consisting more valuable and correct information from that updated set of data. It was chosen the most appropriate research papers from the various type of research papers and the articles that are related with the cloud computing, that are more similar with this topic.

Within the research papers that gathered upon the vulnerabilities and attacks towards the computer systems, it was chosen the set of articles where they are only about the vulnerabilities that are interrelated with the cloud computing platforms.

Further, after the collection that it was gained by reading various kind of research papers, it was able to analyze them in a proper way to get the summarized ideas and the knowledge that are written over them. Furthermore, it was examined the frequently asked questions related with the topic of this study to identify the recent and current issues with them. By having all that information related with this topic, it was able to conduct the research in a better way.

As a deliverable of this study, it provides a prototypical model to overcome these vulnerabilities. This model has been prepared by having a thorough analysis of the collected information from already available various research and technology based sources. This model has three (03) types of actor levels: service provider, administrator, and user to achieve indented protections with specific responsibilities for each. As a lack of this research, it is unable to test this prototype to evaluate the effectiveness of the outcome due to the inability to access all these related resources at a needed actor level to perform their responsibilities. Therefore, this time we provide this as a prototypical model that can be provided as an evaluated model in the future.

IV. DISCUSSION

In this research we have identified almost seven risks and their solutions. In future we will try to describe maximize the number of threats and their solutions. We may focus on precautions which organizations can take to avoid or solve these types of threats.

A. Abusive use of computational resources

In the previous era, hackers were using multiple computers or a botnet to generate a high level of computer power to perform cyber-attacks on computer systems. This has been a complicated process which may take months. Now a powerful computer infrastructure can be easily built in the cloud computing service provider by a simple registration process. The software and hardware components are available in this infrastructure. Due to prevailing computing power of cloud computing, hackers can attack very quickly in short time(Chou, 2013). Brute force attacks and DoS attacks are included in abusive use of computational resources.

B. Brute force attack

A brute force attack is a breaking-password technique. It is basically the easiest way to access a website, a server or anything that is protected by a password. It repeatedly tries different combinations of usernames and passwords until they are included(Brute Force Attacks: Password Protection, no date; Idhom, Wahanani and Fauzi, 2020) The attack's success depends on strong computing ability as thousands of possible passwords must be sent to a target user's account until the correct one to access is found. Cloud computing offers a perfect platform for hackers to start such an attack(Hickey, 2011).

C. Denial of service attack

An attack by DoS is an attempt to prevent authorized users from using their services. In this type of attack, many requests flood the server that provides the service and therefore no authorized user can access the service. When trying to access the site, we sometimes see that we can no longer access the site and observe a mistake because the server is overloaded by requests for access to the site. This occurs if the number of requests that a server can process is higher than its capacity(Patil et al., 2018).

D. Misconfiguration

Cloud security misconfigurations are one of the leading causes of cloud data breaches(Bisson, 2021) Cloud security adaptation strategies of many organizations are not sufficient to protect their cloud infrastructure. The cloud infrastructure is designed to be simple to use and to facilitate data sharing, making it difficult for organizations to make certain that only authorized parties have access to their data. Cloud-based companies also have not completed visibility and infrastructure controls which means that they need security controls from their cloud service provider (CSP) to configure and secure their cloud

deployments(Top Cloud Security Issues, Threats and Concerns, no date). As many organizations have no familiarity with a cloud infrastructure and often have multi-cloud deployments (all with a vendor-based security system)(Ramamurthy et al., 2020), it is easy to leave cloud-based resources of an organization exposed to attackers when it comes to configuration or security monitoring.

One of the most frequent problems is not to diffuse well-known security configuration in baseline settings. This means that the learning from the past can be taken for future instances of an app or part of a cloud infrastructure.

E. Insecure Cryptography

Cryptography algorithm produces random numbers, which are used to generate actual random numbers by uncertain sources of information to gain a larger entropy pool. If only a small entropy pool is provided by the random number generators, the numbers can be brutally forced. The primary source of randomized in client computers is the movement of the user's mouse and key presses, but the servers run without human input(Lukan, 2014). Consequently, virtual machines must rely on the sources available, so that numbers that do not provide much entropy in cryptographic algorithms can easily be guessed.

F. Insecure APIs

The primary tools that allow interactions with cloud storage systems are application user interfaces (APIs). Two different groups of employees normally use APIs such as own staff of organization means the users who would use the API to access cloud data, and staff of cloud service provider.

Unfortunately, several APIs are still vulnerable to security and cloud storage providers usually have unwarranted data access levels(Johnson, 2014). For example, it appeared a few months ago that some popular social network and online platforms stored user passwords in plaintext, which would enable their employees to read them(Chapman, 2019; JOHNNY LIEU, 2019). As dependence upon APIs increases, attackers possess easy methods to use unreliable APIs for malicious purposes.

Developers often develop APIs without properly controlled authentication. As a consequence, these APIs seem to be entirely open to Web and can be used by anyone to access company data and systems. Most of the developers believe that the attackers would not see backend API calls and do not implement adequate authorization control measures. If not, backend data compromise is insignificant.

G. Data Sovereignty

A huge proportion of geographically spread data centers are provided to most cloud providers. This enables the ease of access and performance of Cloud-based resource base to be improved and facilitates CSP's ability to maintain service level contracts in the face of disruptive activities such as natural disasters, power interruption, etc. Organizations that store their data in the cloud mostly do not know in which their information is fully stored in a CSP data center range. This creates important concerns for thirty seven percent (37%) of organizations with respect to data sovereignty, residence and control. Using a cloud platform with data centers outside the authorized area can lead to a regulatory non-compliance for an organization through data protection regulations(Top Cloud Security Issues, Threats and Concerns, no date). Moreover, there are different jurisdictions with different laws on availability to law enforcement data and national defense which can affect customers' security and privacy.

H. Reused IP Addresses

An IP address is provided for every node of the network and therefore a limited amount of an IP address exists. Several cases have been observed recently with regard to the reused IP-address issue. If a specific user leaves the network, a new user is assigned the associated IP-address (former). This sometimes affects the security of the new user because it takes a time to clear the IP address in DNS and in DNS caches(Akinola and Odumosu, 2015). Because of this, sometimes even though the old IP address is given to a new user, it is not insignificant that some other user still has the opportunity to access the data, given that the address remains in the DNS cache and data from a certain user can be available to some other damaged user.

I. Loss of Control over End-User Actions

If companies don't know how their staff use cloud computing services, they can lose control and eventually become vulnerable to violations and threats to security of the insider. Insiders need not to break through private virtual networks (V PNs), proxy servers, or other security defenses to obtain

access to an enterprise's cloud-related internal data. You can access sensitive data directly without too much trouble in the cloud computing. The loss of intellectual property and confidential data can lead to obvious consequences for the company. In order to deal with the loss of supervision over end-user actions, it is important to check, monitor, escalate, analyze incidents, remedy, investigate and respond to incidents. All these measures must be part of the data protection program of the company(Calam et al., 2019).

The following proposed prototypical model (Figure 1) suggests some effective adoptable techniques or solution to overcome these discussed major security threats by cause of vulnerabilities in cloud computing. In deeper by this prototype model, in order to overcome the Brute force attacker, service providers must ensure that system passwords are encrypted at the highest possible encryption rates, such as with 256-bit encoding. The more bits the encryption system contains, the more difficult is

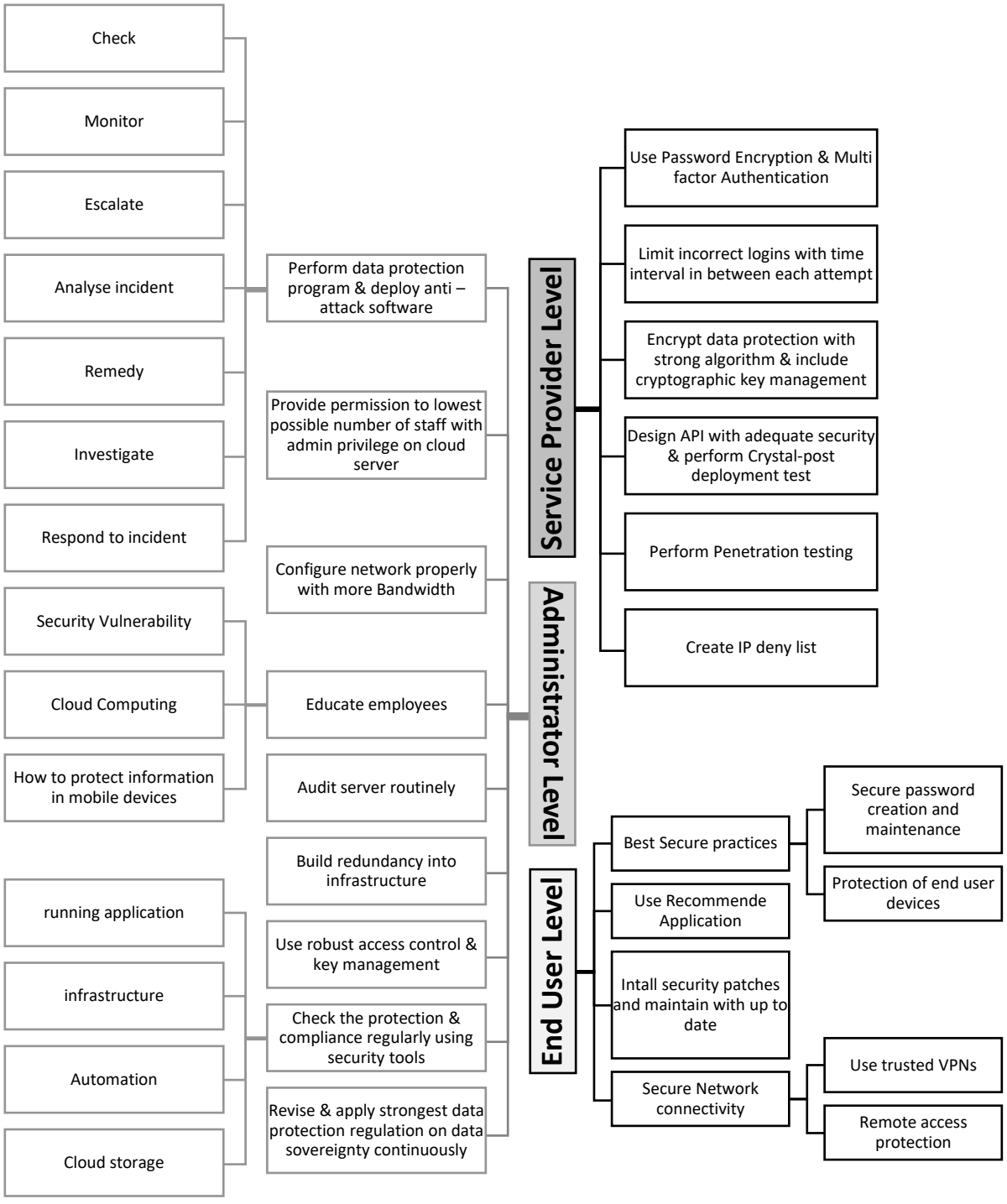

Figure 1: A prototypical model for Security guideline at different levels of cloud interactors

the password to break. also using two factor authentications can minimize brute force service attack. Further we can limit the number of attempts to enter password also reduces the risk of Brute force attacks. If a hacker can continue to try passwords even after a temporary lockout, it can go back to try again. If the account is locked and the user requires IT contact for unlock, this activity will be deterred. If Attacker's efforts for breaking passwords can also be reduced by setting times in between each single login attempt. If a login fails, the timer can stop log in for a short time. Some hackers may stop breaking the passwords if they have to wait. Also, using an IP denylist for the purpose of blocking known hackers (attackers) can also reduce brute force attack(Brute Force Attacks: Password Protection, no date).

In case of Denial-of-Service attack, by buying more bandwidth will help the system to avoid DoS attack. Further security can be achieved over DoS attack by building redundancy into infrastructure, configuring the network properly, and deploying anti-DoS software modules.

The misconfigured base causes problems from the beginning of deployment. Agile development methods(Kalem, Donko and Boskovic, 2013), such as DevSecOps(Zaydi and Bouchaib, 2019), utilize scale developed to assist developers in secure code development and code deployment. But companies do not go far enough sometimes. Protection and compliance should be checked regularly for all running applications and infrastructure and automation can also be helpful(Lemos, no date). Specific tools can also be used to check security configurations for cloud storage. The security tools in the cloud help you to check the security settings in a schedule and identify vulnerabilities before it is too late(ZELLEKE, 2021). During developments and speeding up application deployment, automation should not be restricted to testing code. Critical post-deployment testing should be made as regular cloud services safety testing.

Companies and organizations must take a data-centric approach to preserve their sensitive information from emerging attacks to virtualization, cloud services and mobility in dynamic and complex surroundings. Companies are supposed to deploy data security solutions that consistently protect sensitive data, including cryptographic key management and encryption data protection. An extensive cloud security and encryption platform should also provide robust access controls and key management capabilities that enable companies to use encryption to achieve strategic goals in a useful, cost-effective and exhaustive fashion.

As a mitigation for in secure APIs, developers must be encouraged by cloud service providers to design APIs that provide strong authentication, encryption, intrusion detection and access control. Providers need to secure the APIs. Cloud providers need to perform penetration tests to replicate an external attack to target one's API endpoints and get a safe code review. It is best to make sure secure life cycle of software development through which that reliable applications and APIs are constantly developed. Cloud service providers should consider utilizing data-in-transit SSL/TLS cryptography. Implement multi-factor authentication using schemas such as unique passwords, digital identities, etc.

In order to overcome this issue, the strongest of regulations should be applied uniformly by companies. If an organization has a global presence, it is a continuous challenge to comply with the legislation on data sovereignty of each region. The strongest of these legislations and consistently implement it in every region, irrespective of what other regions require, is one way to reduce complexity. That can be helped by the cloud. Evaluate which cloud services offer these options usually, larger providers and those focusing on certain vertical industries will do their best. Initial and thorough backup discovery and classification must be performed by the cloud service provider. Based on the results, any noncompliance will be identified, and the backups will either be complied with, relocated, or destroyed. It should ensure the establishment of ongoing assessment processes to ensure compliance. Laws and legislation on data sovereignty are continually changing and increasingly compulsory. The tsunami of data continues. And cloud adoption is growing fast(Ashwin Krishnan, 2020).

This study highlights a solution for this issue is that the organizations need to educate their employees about handling security vulnerabilities, for example spoofing and malicious software. Educate them about cloud computing and about how to protect their confidential information on mobile devices or laptops outside the organization. Tell them about the effects of malicious activities. There ought to be Audit

servers routinely within the cloud infrastructure to recognize and timely fix data-security vulnerabilities. Focus on authorized images that are routinely scanned for security vulnerability. Then deploy new image servers to continuously scan for proper setup and vulnerabilities. If the server is vulnerable, do not fix it, replace this with a hardened image, which is approved. Ensure that a lowest possible number of people are limited to privileged central servers and access security systems but that those staff have appropriate training to safely handle their administrator privileges on a cloud server(Cloud Computing Security Vulnerabilities and What to Do About Them, 2020).

V. CONCLUSION

In order to move successfully towards the cloud, a company must be aware of the cloud threats. Instead, we should understand safety threats in our cloud service providers and communicate with our CSP to determine the way in which they deal and from there continue to address security threats. The use of cloud computing has changed the way businesses and hackers act. It brought a wide range of opportunities and a whole new set of risks to cloud security. Companies must continually address the risks and challenges of cloud security while adopting appropriate security tools to simplify operational operations. None of the mentioned security threats are new, but they are more important than ever because staff members are forced to work in this pandemic from home. Encryption is therefore essential to protect against regular audits that have access to your cloud storage and choose a high-quality cloud service provider. In the end, organizations will also protect their data, staff, and customers on a long-term basis by using this opportunity to better their cloud security. The goal of this study is to convey the proper information through a prototypical model to the users (organizations) who are thinking of deploying clouds for their organizations. This paper will help them to be conscious about opting for a proper cloud service provider and will help them in taking precautions to avoid these security issues.

REFERENCES

Akinola, K. E. and Odumosu, A. A. (2015) "Threat Handling and Security Issue in Cloud Computing," *International Journal of Scientific and Engineering Research*, 6(11), pp. 1371–1385.

Ashwin Krishnan (2020) *Steps to ensure data sovereignty in cloud computing*. Available at: https://searchcloudsecurity.techtarget.com/tip/3-steps-to-ensure-data-sovereignty-in-cloud-computing (Accessed: May 11, 2021).

Bisson, D. (2021) *Misconfigurations: A Hidden but Preventable Threat to Cloud Data*. Available at: https://securityintelligence.com/articles/misconfigurations-hidden-threat-to-cloud-data/ (Accessed: May 11, 2021).

Brute Force Attacks: Password Protection (no date) *Kaspersky*. Available at: https://www.kaspersky.com/resource-center/definitions/brute-force-attack (Accessed: May 11, 2021).

Calam, M. *et al.* (2019) "Perspectives on transforming cybersecurity," *McKinsey Global Institute*, (March). Available at: https://www.mckinsey.com/~/media/McKinsey/McKinsey Solutions/Cyber Solutions/Perspectives on transforming cybersecurity/Transforming cybersecurity_March2019.ashx.

Chandra, J. V., Challa, N. and Pasupuleti, S. K. (2016) "Advanced persistent threat defense system using self-destructive mechanism for cloud security," *Proceedings of 2nd IEEE International Conference on Engineering and Technology, ICETECH 2016*, (March), pp. 7–11. doi: 10.1109/ICETECH.2016.7569181.

Chapman, G. (2019) *Facebook admits storing passwords in plain text*. Available at: https://phys.org/news/2019-03-facebook-passwords-plain-text.html (Accessed: May 13, 2021).

Chou, T.-S. (2013) "SECURITY THREATS ON CLOUD COMPUTING VULNERABILITIES," *International Journal of Computer Science & Information Technology (IJCSIT)*, 5(3), pp. 79–88. doi: 10.5121/ijcsit.2013.5306.

Cloud Computing Security Vulnerabilities and What to Do About Them (2020) *Towards Data Science*. Available at: https://towardsdatascience.com/7-cloud-computing-security-vulnerabilities-and-what-to-do-about-them-e061bbe0faee (Accessed: May 11, 2021).

Girma, A., Garuba, M. and Li, J. (2015) "Analysis of Security Vulnerabilities of Cloud Computing Environment Service Models and Its Main Characteristics," *Proceedings - 12th International Conference on Information Technology: New Generations, ITNG 2015*, pp. 206–211. doi: 10.1109/ITNG.2015.39.

Gupta, H. and Kumar, D. (2019) "Security threats in cloud computing," *2019 International Conference on Intelligent Computing and Control Systems, ICCS 2019*, (Iciccs), pp. 1158–1162. doi: 10.1109/ICCS45141.2019.9065542.

Hickey, A. R. (2011) *Amazon Cloud Can Be Used To Crack Wi-Fi Passwords With "Brute Force," CRN*. Available at:

https://www.crn.com/news/cloud/229000447/amazon-cloud-can-be-used-to-crack-wi-fi-passwords-with-brute-force.htm (Accessed: May 11, 2021).

Ibrahim, A. A. Z. A., Varrette, S. and Bouvry, P. (2018) "On Verifying and Assuring the Cloud SLA by Evaluating the Performance of SaaS Web Services Across Multi-cloud Providers," *Proceedings - 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops, DSN-W 2018*, pp. 69–70. doi: 10.1109/DSN-W.2018.00034.

Idhom, M., Wahanani, H. E. and Fauzi, A. (2020) "Network security system on multiple servers against brute force attacks," *Proceeding - 6th Information Technology International Seminar, ITIS 2020*, pp. 258–262. doi: 10.1109/ITIS50118.2020.9321108.

JOHNNY LIEU (2019) *Google stored some users' passwords in plain text for years*. Available at: https://mashable.com/article/google-plaintext-password-enterprise/ (Accessed: May 13, 2021).

Johnson, M. C. (2014) "Cloud Insecurity and True Accountability," *Guardtime*, p. 15. Available at: https://guardtime.com/files/Cloud_Insecurity_and_True_Accountability_1403.pdf.

Kalem, S., Donko, D. and Boskovic, D. (2013) "Agile methods for cloud computing," *2013 36th International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO 2013 - Proceedings*, pp. 1079–1083.

Khan, N. and Al-Yasiri, A. (2016) "Identifying Cloud Security Threats to Strengthen Cloud Computing Adoption Framework," *Procedia Computer Science*, 94, pp. 485–490. doi: 10.1016/j.procs.2016.08.075.

Lemos, R. (no date) *Cloud misconfigurations and security: How to avoid your next fail*, *TechBeacon*. Available at: https://techbeacon.com/security/cloud-misconfigurations-security-5-ways-avoid-your-next-fail (Accessed: May 11, 2021).

Lukan, D. (2014) *The top cloud computing threats and vulnerabilities in an enterprise environment*, *CLOUD TECH*. Available at: https://cloudcomputing-news.net/news/2014/nov/21/top-cloud-computing-threats-and-vulnerabilities-enterprise-environment/ (Accessed: May 11, 2021).

Patil, A. *et al.* (2018) "A multilevel system to mitigate DDOS, brute force and SQL injection attack for cloud security," *IEEE International Conference on Information, Communication, Instrumentation and Control, ICICIC 2017*, 2018-Janua, pp. 1–7. doi: 10.1109/ICOMICON.2017.8279028.

Ramamurthy, A. *et al.* (2020) "Selection of cloud service providers for hosting web applications in a multi-cloud environment," *Proceedings - 2020 IEEE 13th International Conference on Services Computing, SCC 2020*, pp. 202–209. doi: 10.1109/SCC49832.2020.00034.

Top Cloud Security Issues, Threats and Concerns (no date) *Check Point Software*. Available at: https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/top-cloud-security-issues-threats-and-concerns/ (Accessed: May 11, 2021).

Worldwide Public Cloud Revenue to Grow 17% in 2020 (2019) *Gartner*. Available at: https://www.gartner.com/en/newsroom/press-releases/2019-11-13-gartner-forecasts-worldwide-public-cloud-revenue-to-grow-17-percent-in-2020 (Accessed: May 11, 2021).

Zaydi, M. and Bouchaib, N. (2019) "DevSecOps PRACTICES FOR AN AGILE AND SECURE IT," 22(December), pp. 527–540.

ZELLEKE, L. (2021) *Best Cloud Security Tools for 2021*. Available at: https://www.comparitech.com/net-admin/cloud-security-tools/ (Accessed: May 11, 2021).