Research Article

A Walkthrough into Cloud Security

C K Sripavithra [a], Dr. V B Kirubanand [b]

[a] Ph.D. Research Scholar, Dept. of Computer Science, Christ (Deemed to be University), Central Campus, Bangalore & Assistant Professor, Dept. of Computer Science, Maharani's Science College for Women (Autonomous), Mysore.
[b] Associate Professor, Dept. of Computer Science, Christ (Deemed to be University), Central Campus, Bangalore.

Abstract: With the recent advancements and migration of organizations to the cloud environment, there is also an increase in the vulnerabilities and threats in the cloud. A wide extent of attacks that are pertinent to a PC and the data in transmission likewise applies to cloud based organizations. And nowadays more are adopting a multi-cloud strategy and its security becomes a more and more complex task. A lot of security techniques and algorithms have been proposed on the security in the cloud. This paper describes the various techniques adopted in the security on the cloud. The walkthrough technique builds up a primary corpus of information upon which a more detailed analysis and meanings can be built later on. It also serves as a foundation for further security centered research. Also a two-phase encryption method has been proposed to provide maximum security.

Keywords: Vulnerabilities, attacks, multi-cloud, security, two-phase encryption

1. Introduction

Enterprises and organizations are expanding their horizons with the immense scope and benefits of cloud computing. At the same time, migrating to the cloud unfolds a variety of risks to an enterprise. It ranges from securing confidential information, trade secrets, personal information that could fall into some unacceptable hands.

Cybercriminals are progressively utilizing complex social designing strategies driving to disturb the business tasks and harming the monetary benefits of these companies. **(Liu, S., & Liu, Y., 2016)** They also present tremendous potential security dangers to people and social ventures. **(Taylor, 2016) (Escudero, C., et al., 2018)** New security weaknesses are found consistently.(NIST) With each new declaration, similar query emerge. How critical is this weakness? How predominant? How simple is it to exploit?

It is plausible to foresee the future with regards to cyber attacks, for example, distinguishing weakness patterns, envisioning security holes in the organization, optimizing resource allocation considerations and guaranteeing the key corporate resources in the most secure way. **(Gnanavelu, D., & Gunasekaran, G., 2014)** Security circumstance expectation has a huge impact and is the core of the cyber security protection. There are two general ways to deal with cyber attacks. First one, is to build up a proficient and viable strategy to recognize programming weaknesses and fix them prior to being misused. **(Abhineet Anand, et al., 2020)** And second is to build methodologies to foresee the conduct of attacks and execute protecting procedures. **(Tabrizchi, H., & Kuchaki Rafsanjani, M., 2020) (Iqbal Ahmed, 2019)**

2.Literature Review

As organizations have migrated its infrastructure and operations to the cloud, more are adopting a multi-cloud strategy. **(Gartner, 2016) (Flora Amato, et al., 2018)** That is because this kind of strategy embraces much more benefits. **(Splunk, 2020) (Chen-shin Chien & Jason Chien, 2010)**

The concept of cyber attacks awareness and a framework was first introduced by Tim Bass. **(Tim Bass, 2000)** And this established the basis for resulting research in Network Security Situational Awareness. **(Huiqiang Wang, 2006)**

Data protection by encryption is being used in great lengths. Cumbersome computations, cost-effectiveness and security enforcements in the cloud have led to new hybrid cryptosystems. **(NIST) (Sotto, LJ., et al., 2010)**

There are other dimensions on which security was researched. Considering the various sequential occasions of attacks for a particular duration of time delivers better performance over the occasion at a moment of time. **(Ye, N., Li, X., & Emran, S. M., 2000)** Since numerous digital attacks require a progression of related occasions to achieve, it is credible to improve prediction by fusing the requests of occasions. **(Yau, S. S., Buduru, A. B., & Nagaraja, V., 2015)**

It is important to understand one's network or infrastructure. The following series of questions arises when we analyse this dimension.

2.1. Research Questions

- How is user identity and account information stored?
- What type of encryption and level of encryption is in use?
- Have you identified the sensitive data?
- How have you secured your devices?
- How would you do patch management to something you don't even know you have?
- Is the funding adequate to obtain the required security technology?
- How to observe and analyze the type of client requests?
- Are there any unusual client requests?
- Have any requests been denied?
- Are there any denied requests in varied times?

More innovative and new security techniques are the needs to address the recent enormous security threats. **(Yau, S. S., Buduru, A. B., & Nagaraja, V., 2015) (David Linthicum, 2021)** A holistic approach to defend the system in various dimensions is necessary. **(Gupta, P.K., Tyagi, V., & Singh, S. K., 2017)** Data Analytics usage in a variety of domains. **(Sharma, Shree Krishna, & Xianbin Wang, 2017)** Cloud is best suitable for real time data analysis.

Predictive computing requires inference of invisible patterns and identifying associations among the stored parameters. This analyses client requests of the cloud by maintaining service requests and logs with additional parameters. This helps to classify the client service requests as threat or not. By this suspicious patterns of recurrent requests can be deduced.

A typical technique is to use a mobile agent to acquire, share and utilize data for various analyses. **(Wang, J., Zhang, L., Duan, L. et al., 2017)** And a new algorithm that ranks the vulnerabilities or notifies alerts over time is also framed for further possible analytics. **(Rieke, R., Stoynova, Z., 2010)**

A lot of research is on the trend to isolate the workspace of customers for security reasons. **(Karinerhysolate, 2020)** In this isolation technology to secure workspace of confidential and sensitive data**. (Azure, 2020) (Shi, B., et al., 2018)**

3.Two-Phase Hybrid Encryption Method

In the cloud, security and privacy are in danger consistently. Cryptography is the most ideal approach to safeguard information. Privacy can be accomplished through established encryption techniques: Symmetric or Asymmetric encryption algorithms. Information encryption, alongside hashing, can be a potential answer to shield from fraudsters.

User authentication process corresponds to the privacy of data in the cloud. Absence of solid authentication validation can prompt unapproved admittance to clients account. This paper proposes a new two-phase hybrid encryption method. Two distinct techniques are combined to give the most extreme security to the information. The strategies are encryption and password hashing.

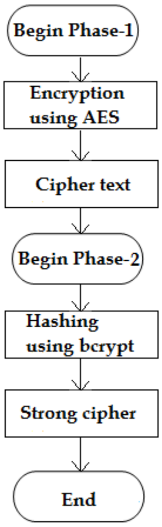
3.1. Phase-I

- How AES algorithm is used to provide security on the confidential information.
- AES is asymmetric encryption algorithm.
- Here the sender uses public key of the receiver to encrypt the message.
- The encrypted message called 'Cipher text' is used in the next phase.

3.2. Phase-II

- Bcrypt offers a truly powerful solution. It is based on the Blowfish block cipher cryptomatic algorithm.
- Bcrypt is a key derivation function, which can be considered as a slow hash function. It gradually changes the input 'Cipher text' to a fixed-size, deterministic, and incalculable output.

Figure.1 Two-phase hybrid encryption method.



This is an idea of how encryption with another simple technique can reduce global cloud theft and risk of data leak to a great extent.

4.Conclusion and future scope

Cloud computing is very prominent with its advancements and challenges. The frequent myriad of cyber security breaches shows the abundant resources of adversaries. Recent advances in many fields owe to the predictive analytics of real time data. In this paper, the various strategies and techniques of managing security in the cloud has been discussed. And a new hybrid method for utmost security is suggested. There is an impressive degree for groundbreaking plans to be discovered to ensure security in the cloud environment. This would then make cloud computing safer taking the advanced IT world on to the next higher level.

References (APA)

[1]. Abhineet Anand, Naresh Kumar Trivedi, & Ajay Kumar. (2020) Data security issues and their solutions in cloud computing, Journal of Critical Reviews, 7(14).

[2]. Azure. (2020) Azure for Secure Worldwide Public Sector Cloud Adoption, https://azure.microsoft.com/mediahandler/files/resourcefiles/azure-for-secure-worldwide-public-sector-cloud-adoption/Azure%20for%20WW%20Public%20Sector.pdf

[3]. Chen-shin Chien & Jason Chien. (2010) Insight to cloud computing and growing impacts, ICICA 2010, Part I, CCIS 105, 250–257, Springer-Verlag Berlin Heidelberg.

[4]. David Linthicum. (2021) The new normal needs new cloud security, https://www.infoworld.com/article/3605011/the-new-normal-needs-new-cloud-security.html Accessed January 2021.

[5]. Escudero, C., Sicard, F., & Zamai, E. (2018). Process-aware model based IDSs for industrial control systems cybersecurity: approaches, limits and further research. [Paper presentation]. 23rd IEEE International Conference on Emerging Technologies and Factory Automation (Italy), Turin.

[6]. Flora Amato, Francesco Moscato, Vincenzo Moscato, & Francesco Colace. (2018) Improving security in cloud by formal modeling of IaaS resources, Future Generation Computer Systems, 87, 754-764, https://doi.org/10.1016/j.future.2017.08.016. (http://www.sciencedirect.com/science/article/pii/S0167739X17305964)

[7]. Gartner. (2016). Press Releases. https://www.gartner.com/en/newsroom/press-releases, 2016. Accessed January 2021.

[8]. Gnanavelu, D., & Gunasekaran, G. (2014) Survey on security issues and solutions in cloud computing, International Journal of Computer Trends and Technology (IJCTT), 8(3).

[9]. Gupta, P.K., Tyagi, V., & Singh, S. K. (2017) Cloud-Based Information Security, Predictive Computing and Information Security. Springer, Singapore. https://doi.org/10.1007/978-981-10-5107-4_6

[10]. Huiqiang Wang. (2006). Survey of network situation awareness system, Computer Science, 33, 5-10.

Iqbal Ahmed. (2019) A brief review: security issues in cloud computing and their solutions, Telkomnika, 17(6), 2812-2817. https://doi.org/10.12928/TELKOMNIKA.v17i6.12490

[11]. Karinerhysolate. (2020) What Attackers Think About Your Cybersecurity Isolation Strategy, https://www.hysolate.com/blog/cybersecurity-isolation-strategy/ Accessed January 2021

[12]. Liu, S., & Liu, Y. (2016). Network security risk assessment method based on HMM and attack graph model [Paper presentation]. 17th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel Distributed Computing (China), Shanghai.

National Vulnerability Database https://nvd.nist.gov/. Accessed January 2021

[13]. NIST National Institute of Standards and Technology. (2009) The NIST Definition of cloud computing, Information Technology Laboratory.

[14]. Rieke, R., Stoynova, Z. (2010) Predictive Security Analysis for Event-Driven Processes. In: Kotenko I., Skormin V. (eds) Computer Network Security. Lecture Notes in Computer Science, 6258. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-14706-7_25

[16]. Sharma, Shree Krishna, & Xianbin Wang. (2017) Live data analytics with collaborative edge and cloud processing in wireless IoT networks, IEEE Access 5, 4621-4635.

[17]. Shi, B., Cui, L., Li, B., Liu, X., Hao, Z., & Shen, H. (2018) Shadow monitor: an effective in-VM monitoring framework with hardware-enforced isolation. In: International Symposium on Research in Attacks, Intrusions, and Defenses. Springer, Berlin, 670–690.

[18]. Sotto, LJ., Treacy, BC., & McLellan, ML. (2010) Privacy and data security risks in cloud computing. Electronic Commerce & Law Report, 15, 186.

[19]. Splunk. (2020) A Brief Guide to Securing Your Multicloud. https://www.splunk.com/ Accessed January 2021.

[20]. Tabrizchi, H., & Kuchaki Rafsanjani, M. (2020) A survey on security challenges in cloud computing: issues, threats, and solutions. J Supercomput 76, 9493–9532. https://doi.org/10.1007/s11227-020-03213-1

[21]. Taylor, H. (2016). Biggest cybersecurity threats in 2016. CNBC. http://www.cnbc.com/2015/12/28/biggest-cybersecurity-threats-in-2016.html. Accessed January 2021.

[22]. Tim Bass. (2000) Intrusion detection system and multi-sensor data fusion, Communications of the ACM, 43(4), 99-105.

[23]. Wang, J., Zhang, L., Duan, L. et al. (2017) A new paradigm of cloud-based predictive maintenance for intelligent manufacturing, J Intell Manuf 28, 1125–1137. https://doi.org/10.1007/s10845-015-1066-0

[24]. Yau, S. S., Buduru, A. B., & Nagaraja, V. (2015) Protecting critical cloud infrastructures with predictive capability, 8th IEEE International Conference on Cloud Computing (USA), New York, 1119-1124, https://doi.org/10.1109/CLOUD.2015.165.

[25]. Ye, N., Li, X., & Emran, S. M. (2000) Decision trees for signature recognition and state classification, IEEE SMC Information Assurance and Security Workshop.