A Software Defined Network based Security Assessment

[1*]Dr B S N Murthy [2]Mr TVL Srinivas [3]Ch. S.S Prabha [4]A.S.Digvijay
[5]M. R Babu [6] T.L.N Pavan

[1,2,3,4,5,6]Department of CSE, BVC Engineering College, Odalarevu, India
bsnmurthy2012@gmail.com
[2]tvlsrinivas@gmail.com

Abstract: The integration of cloud computing with the Internet of Things, or "cloud IoT," has the ability to revolutionise numerous industries. While some companies are hesitant to implement such technologies because of security concerns, others choose to disregard such worries and instead integrate the Cloud IoT into their operations. Consequently, how to assess the security quality of cloud-resource providers and IoT devices is a crucial issue for promoting the use of Cloud IoT and lowering organisational security risks, considering the numerous options available. To solve this problem, we develop a system to evaluate the end-to-end security of a Cloud IoT service using Software Defined Networks (SDN). To streamline network management and free up analysts to focus on Cloud IoT data flow analysis, we suggest a three-layer architecture that combines SDN with Cloud IoT.

Keywords: Cloud IoT, Software Defined Network (SDN), Cloud

1. Introduction

An emerging paradigm in networking called the Internet of Things (IoT) has emerged lately to improve measurement, communication, and interaction with the actual physical environment [1]. On the other hand, cloud computing has gained a lot of popularity since it offers high-performance processing and almost infinite storage resources at a low cost [2, 3]. This is why Cloud IoT—a new paradigm in information technology that integrates the Internet of Things (IoT) with cloud computing—has gained a lot of traction as a means to improve various aspects of our daily lives, including smart grids, cities, healthcare, video surveillance, environmental monitoring, and many more. When it comes to mission-critical applications, Cloud IoT is actually an essential component of today's IT infrastructure. In view of the growing importance of information security in today's IT landscape [13] and the prevalence of cyberattacks (like the Ukraine Power Grid Attacks in December 2015, which knocked out electricity for nearly 1.4 million people for a few hours), the safety of the Internet of Things (IoT) in the cloud is clearly a pressing concern for academics and businesses alike.

Nevertheless, other Cloud IoT solutions have surfaced to fulfil client demand, thanks to the expansion of cloud computing and the Internet of Things in the past few years. Some examples of such solutions are the Azure IoT Suit3 and Google Brillo2. Customers have a non-trivial problem with evaluating the security level because Cloud IoT solutions are sophisticated. As a result of security concerns and a lack of knowledge about the hazards, some organisations may be reluctant to employ such technology. This could slow down the adoption of the Cloud IoT and the expansion of the related industry. However, not all companies will take the time to carefully consider the security implications of Cloud IoT before rushing to implement it. Users necessitate a method to assist in evaluating the security of Cloud IoT solutions.

The security of applications hosted in the cloud [14, 15] and the Internet of Things [16, 17, 18] have recently been the subject of security evaluation studies. Since they developed independently, the majority of current approaches examine security in isolation, exposing specific deficiencies in transparency and uniformity [19]. Considering more than simply the cloud or IoT is necessary when evaluating the safe data transfer, as Cloud IoT takes data from the real world via the IoT System, processes it using cloud services, and then allows actions to be

K. R. Madhavi et al. (eds.), *Proceedings of the International Conference on Computational Innovations and Emerging Trends (ICCIET 2024)*, Advances in Computer Science Research 112,
https://doi.org/10.2991/978-94-6463-471-6_145

triggered in the real world. Due to the present network architecture's reliance on closed networks, which restricts the introduction of new services and their interoperability with other devices and services, an autonomous system is needed to integrate all networks [19].

The combination of software-defined networking (SDN) with the internet of things (IoT) makes networks more agile and flexible to meet unpredictable demand, and it makes network management easier and less taxing by separating the two. With a software-defined network (SDN), data plane devices act as packet forwarders, and a logically centralised system known as a controller is responsible for administering the network [20]. When managing switches, the OpenFlow protocol is utilised. A protected OpenFlow channel is utilised for the controller's connection to the switch. The topic of SDN-based architecture has been extensively covered in the literature.

Given these issues, this article aims to provide a comprehensive approach to assessing cloud security when selecting an Internet of Things solution. Based on the data flow analysis, we develop a three-layer SDN-based framework with 23 indicators to evaluate the data-security-oriented security of the Cloud IoT solution. This is necessary because Cloud IoT will gather data from the real world and use this data to enable further applications. Next, researchers and practitioners are surveyed online to determine the importance of each indicator. The survey data is then combined using three methodologies: AdaRank, weighted-mean, and analytic hierarchical process (AHP). This crowd-wisdom weighting system is applied to each indicator. At last, we mapped security-related evidences into the framework and arrived at an overall security level. This will help consumers make informed decisions. We used the documentation for two popular Cloud IoT solutions, Google Brillo on Google Cloud and Microsoft Azure IoT Suite on Azure Cloud.

2. Literature Survey

Software as a service (SaaS) and the way IT equipment is designed and purchased could be significantly altered by cloud computing, which is the practical application of the idea of computing as a utility. Developers of state-of-the-art Internet services are no longer constrained by the resources needed to construct and maintain their infrastructure. They will not be concerned about squandering funds by over-providing a service whose demand turns out to be lower than anticipated or by under-providing a service whose popularity surges beyond their wildest dreams. As soon as their programmes can scale, firms with massive batch-oriented operations can start seeing returns because using one server for a thousand is the same as using a thousand servers for an hour. Through ubiquitous networks enabled by things, the Internet of Things ushers in a new era of user interaction with the online world. The networked pool of programmable computing resources in the cloud is excellent for a wide variety of circumstances due to its flexibility, scalability, and adaptability. The CloudThings architecture, a well-liked approach to merging the Internet of Things and Cloud Computing, is the main focus of this article. Our focus here is on the most up-to-date methods for merging Cloud Computing with the Internet of Things. To examine the requirements for IoT applications, we examine a smart house scenario that is enabled by the Internet of Things. In addition, we suggest the Cloud Things architecture, a cloud-based Internet of Things (IoT) platform that supports Cloud Things Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) to facilitate better IoT application creation, administration, and management. Finally, we will showcase our progress on the CloudThings architecture. Building a WSN framework for Internet of Things-based environmental monitoring over extended periods of time.

The Internet of Things (IoT) uses the Internet Protocol to digitally represent many different types of physical objects, including cars, teacups, buildings, and even forest trees. Its appeal stems from the fact that we can easily monitor the location and status of any "thing" that matters to us. Wireless sensor networks are ideal for gathering environmental data over an extended period of time in order to represent the Internet of Things (IoT). Several long-term Internet of Things (IoT) applications in environmental monitoring are covered in this study, including the functional design and implementation of a complete WSN platform. Affordable, highly-sensitized, quickly-deployed, long-lasting, low-maintenance, and service-quality application requirements informed the specification and design of the platform and its components. We consider the platform's reusability

for a range of related monitoring applications from the specifications through all design stages with an eye on minimising effort for future reuse.
With the advent of Software Defined Networks (SDN) in recent years, network operators have gained greater flexibility in managing and programming their networks. One such framework is a secured SND for the Internet of Things (K. S. Sahoo, B. Sahoo, and A. Panda). This more recent innovation circumvents the shortcomings of earlier networks. Devices on the data plane just transmit packets and leave all decision-making to the controller because the two planes are disconnected. Still, SDN security is an issue, no matter how helpful it is. Sensors and actuators are now integral parts of almost every industry because to wireless sensor network (WSN) technology, which has given birth to a new academic discipline called the Internet of Things (IoT). The Internet of Things makes SDN architecture implementation more challenging. Here we'll go over some of the issues with SDN security and then present a solution for the Internet of Things (IoT) in an SDN-based network. New paradigms in communication and information science, such as the Internet of Things and cloud computing, have just come to the fore. The lack of security designs is a major reason why many studies indicate that the integration of the Internet of Things and cloud computing is still in its early phases. That rules out the possibility of enhancing the Cloud IoT with the features of numerous preexisting applications. We propose secure means of data transmission in the Cloud IoT from this vantage point. In order to safeguard Map Reduce operations on the cloud computing platform, this work creates an elliptic curve cryptography for the Internet of things and uses group signatures with threshold secret sharing approaches. The cloud service controller, security gateway, and service controller server are all components of the suggested design. In addition to protecting the cloud computing infrastructure from external assaults, the architecture created in this work enables encrypted data transmission and mutual authentication of IoT items.

3. Proposed Method

Cloud Security and IoT Security Model:
There are two primary parts to the model. The first is a conceptual model that includes features like cost, flexibility, efficiency, and security. The second part is a FIS architecture that uses five primary criteria and eleven inputs to determine how satisfied a user is with a particular cloud service. This security index consists of four layers: perceptual, transport, application, and cloud computing. To find the best indications that represent the level of IoT security, the Fuzzy-AHP approach is employed to rank their importance.
Integration of Cloud and IoT:
The break-down of cloud computing and IoT integration into three distinct types, an outline of present goals for this integration, challenges that have yet to be addressed, and open concerns about the state of the field.
The UPECSI method provides an all-inclusive answer to the problem of user-driven privacy enforcement for IoT cloud services.
Integration of SDN and IoT:
Discussed the pros and cons of integrating SDN with the IoT in terms of security and scalability. “Al Jararweh e. To manage the enormous volumes of data produced by IoT devices, you need provide a software-defined networking (SDN) Internet of things (IoT) framework based on the SDN idea.

The Convolutional Neural Network (CNN) is a popular Deep Learning architecture for picture recognition and classification problems. The various layers that make it up include fully connected, pooling, and convolutional ones. After the pooling layer downsamples the image to reduce computation, the convolutional layer uses filters to extract features from the input image, and the fully connected layer makes the final prediction. In order to find the most effective filters, the network employs gradient descent and backpropagation.

1. The neurobiological underpinning for neuronal function is provided by orientation-selective and spatially sensitive nerve cells in the visual cortex.
2. Their foundation is a multi-layer neural network.
3. They determine relevant traits by inference.
4. The fact that they are feed-forward networks means that they can 4) extract topological characteristics from datasets.
5. They are able to detect patterns in photos straight from pixels with minimal preprocessing.
6. Their extraordinary power lies in their capacity to detect patterns characterised by remarkable variety. Consider the NSL dataset.

7. CNNs are trained using a variation of the back propagation technique.
8. Convolutional neural networks (CNNs) are based on visual cortical neuronal cells, which enable them to track particular features.

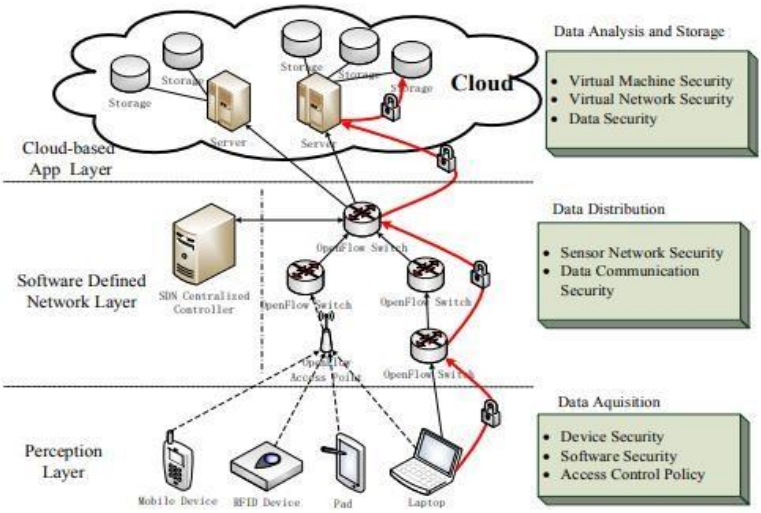

Fig 1. Work Flow

4. Results

Straightforwardly, we can employ the presented indicators to evaluate the security level for the CloudIoT. However, different indicators in different layers have different contributions for the overall security. Therefore, to get the weight for different indicators, in this section, an online interview with researchers and practitioners is carried out to assign the weight for these indicators based on their experiences.

Until now we already get the different weights for different indicators representing their importance for the overall security. Therefore, given a CloudIoT solution, we can map its security-related mechanism into the framework to figure out whether they offer the necessary security guarantee. Since we offer its definition for each indicator, we can use the related key words to search over the solution's description documents to find the related security mechanisms. Then for each found mechanism, we can further evaluate its relevance to the indicator. To assess this relevance, similarly, we invite 5 security experts chosen from the survey participants, then show them the related evidence and ask them to remark the relevance in "Low", "Medium" and "High", which represents the degree that the solution can solve the security concern. Finally we can get the ranking based on the input from these experts and then calculate the overall security score by multiplying the indicators' weights and the covered degree.

The overall performance of the proposed method is shown in table 1.

Table 1: Comparison of Results

	Ranking Results		
INDICATOR	Azure IoT	Google Brillio	Proposed Method
Secure Booting	11	12	9
Device Hardware Physical Security	14	12	10
Firewall and IPS 22 20 21	13	13	9
Antivirus and Antimalware	15	14	8
Software Updates and Patches	14	12	7
Authentication	13	13	12
Access Control	14	12	7
Security Audit	15	12	9
Network Socket	16	10	11
Web Interface Security	11	12	13
Port Security	14	11	14
Data Transfer Protocol	13	10	12
Transport Encryption	15	11	9
VM Image Repository Security	14	12	8
VM Boundaries	11	12	12
DNS Server Security	14	12	13
Virtual Switch Security	13	13	9
Malicious Network Attack	15	14	8
Data Locality	14	12	7
Data Integrity	11	12	12
Data Confidentiality	14	13	7
Post-termination Data Management	13	14	9
Overall	**13.5**	**12.18**	**9.8**

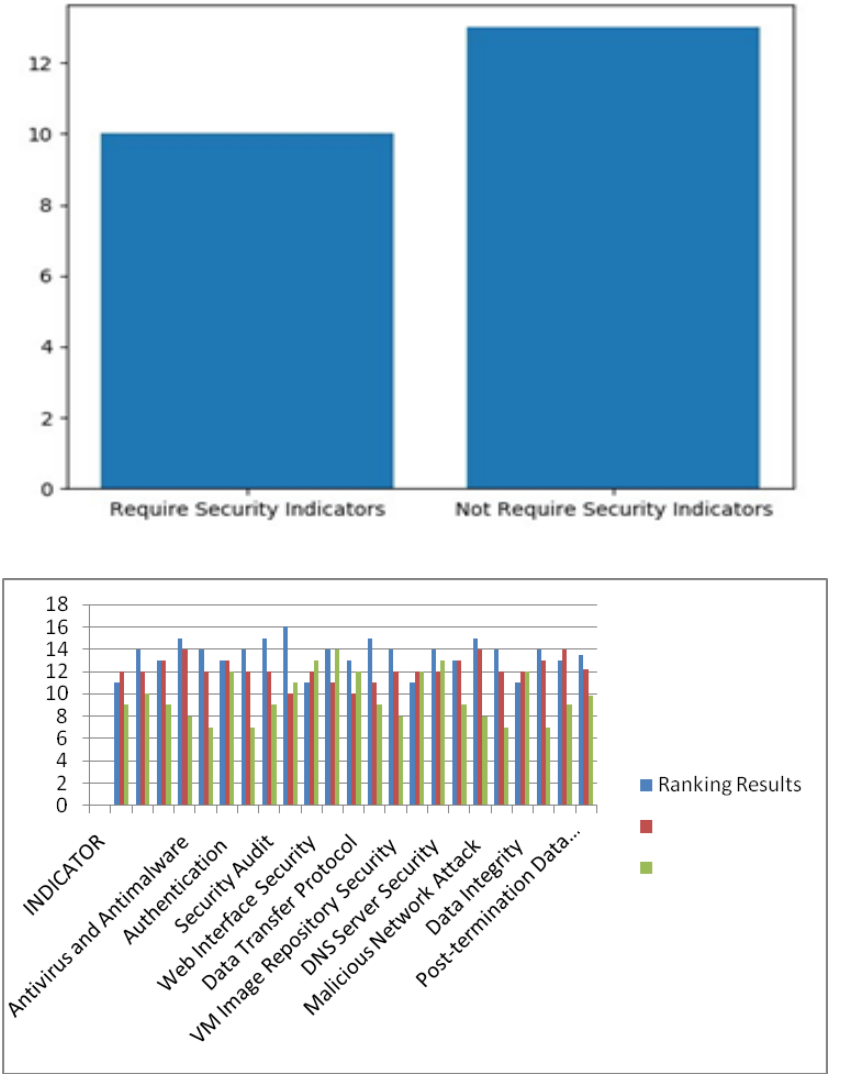

Figure 2. The count is shown on the y-axis, while the feature kind is shown on the x-axis as require or not require. The following graph shows that out of 23 security elements, 10 are desired or needed by experts, whereas 13 are not. An indication is a term used to describe each security feature.

5. Conclusion And Future Enhancement

The integration of IoT with cloud computing is the primary factor propelling the development of Cloud IoT. Since security has become a major issue for its adoption, customers should find it both beneficial and vital to evaluate the solution's level of security. Based on a study of the data flow via the Cloud IoT, we provide a three-layer indication framework with 23 indications that is based on software-defined networking (SDN). We developed a web-based survey and polled experts in the subject to ascertain the relevance of these indicators. After then, the weights were determined using an aggregate rating that was the result of three separate methods. By analysing two existing Cloud IoT solutions, we can see how these solutions ensure customer security by identifying the evidences for the linked security mechanisms based on the weights of several indicators. This allows us to give the client a full picture of how to evaluate the security of different solutions and identify the providers' vulnerabilities.

Bibliography

1. J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," Future Generation Computer Systems, vol. 29, no. 7, pp. 1645–1660, 2013. [Online]. Available: http://dx.doi.org/10.1016/j.future.2013.01.010
2. M. Armbrust, A. Fox, R. Griffith, A. Joseph, and RH, "Above the clouds: A Berkeley view of cloud computing," University of Califomia, Berkeley, Tech. Rep. UCB, pp. 07–013, 2009.
3. R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility," Future Generation Computer Systems, vol. 25, no. June 2009, p. 17, 2009.
4. A. Botta, W. De Donato, V. Persico, and A. Pescape, "Integration of ´ Cloud computing and
5. Internet of Things: A survey," Future Generation Computer Systems, vol. 56, pp. 684–700, 2016.
6. M. D´ıaz, C. Mart´ın, and B. Rubio, "State-of-the-art, challenges, and open issues in the integration of Internet of things and cloud computing," Journal of Network and Computer Applications, pp. 1–19, 2015.
7. J. Zhou, T. Leppanen, E. Harjula, M. Ylianttila, T. Ojala, C. Yu, and H. Jin, "CloudThings: A common architecture for integrating the Internet of Things with Cloud Computing," Proceedings of the 2013 IEEE 17th International Conference on Computer Supported Cooperative Work in Design, CSCWD 2013, pp. 651–657, 2013.
8. M. Yun and B. Yuxin, "Research on the architecture and key technology of Internet of Things (IoT) applied on smart grid," in 2010 International Conference on Advances in Energy Engineering, ICAEE 2010, 2010, pp. 69–72.
9. I. PodnarZarko, A. Antonic, and K. Pripuzic, "Publish/subscribe middleware for energyefficient mobile crowdsensing," Proceedings of the 2013 ACM conference on Pervasive and ubiquitous computing adjunct publication - UbiComp '13 Adjunct, pp. 1099–1110, 2013.
10. A. Forkan, I. Khalil, and Z. Tari, "CoCaMAAL: A cloud-oriented context-aware middleware in ambient assisted living," Future Generation Computer Systems, vol. 35, pp. 114–127, 2014. [Online]. Available: http://dx.doi.org/10.1016/j.future.2013.07.009
11. G. Fortino, D. Parisi, V. Pirrone, and G. Di Fatta, "BodyCloud: A SaaS approach for community Body Sensor Networks," Future Generation Computer Systems, vol. 35, pp. 62–79, 2014. [Online]. Available: http://dx.doi.org/10.1016/j.future.2013.12.015
12. A. Prati, R. Vezzani, M. Fornaciari, and R. Cucchiara, "Intelligent Video Surveillance as a Service," Intelligent Multimedia Surveillance: Current Trends and Research, vol. 9783642415, no. November 2013, pp. 1–16, 2013.
13. M. T. Lazarescu, "Design of a WSN platform for long-term environmental monitoring for
14. IoT applications," IEEE Journal on Emerging and Selected Topics in Circuits and Systems, vol. 3, no. 1, pp. 45–54, 2013.
15. R. Anderson and T. Moore, "The economics of information security," Science, vol. 314, no. 5799, pp. 610–613, 2006.
16. A. Abuhussein, H. Bedi, and S. Shiva, "Evaluating Security and Privacy in Cloud
17. Computing Services: A Stakeholder's Perspective," Internet Technology And Secured Transactions, pp. 388–395, 2012.
18. M. Sookhak, A. Gani, H. Talebian, A. Akhunzada, S. U. Khan, R. Buyya, and A. Y. Zomaya, "Remote Data Auditing in Cloud Computing Environments: A Survey, Taxonomy, and Open Issues," ACM Computing Surveys, vol. 47, no. 4, pp. 65:1–65:34, 2015.
19. S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in
20. Internet of Things: The road ahead," Computer Networks, vol. 76, pp. 146–164, 2015. [Online]. Available: http://dx.doi.org/10.1016/j.comnet.2014.11.008

21. H. Yu, J. He, T. Zhang, P. Xiao, and Y. Zhang, “Enabling end-toend secure communication between wireless sensor networks and the Internet,” World Wide Web, vol. 16, no. 4, pp. 515–540, 2013.
22. B. Zhang, Z. Zou, and M. Liu, “Evaluation on security system of internet of things based on Fuzzy-AHP method,” in E-Business and E-Government (ICEE),, 2011, pp. 2230–2234. [Online]. Available: http://dx.doi.org/10.1109/ICEBEG.2011.5881939
23. S. Kim and W. Na, “Safe data transmission architecture based on cloud for internet of things,” Wireless Personal Communications, vol. 86, no. 1, pp. 287–300, 2016.
24. K. S. Sahoo, B. Sahoo, and A. Panda, “A secured sdn framework for iot,” in Man and Machine Interfacing (MAMI), 2015 International Conference on. IEEE, 2015, pp. 1–4.