iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 2017 **Issue:** **Month of publication:** March 31, 2017

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

A Frame Work for Cloud Computing and Internet of Things Its Applications Parameters Comparison

S. Sivakumar [1,] V. Anuratha[2], S. Gunasekaran [3]

[1]*Ph.D Research Scholar, Sree Saraswathi Thiyagaraja College, Pollachi, TN,India-642 107*

[2]*Head, PG Department of Computer Science, Sree Saraswathi Thiyagaraja College, Pollachi,TN,India-642 107*

[3]*Prof and Head, Department of CSE, Coimbatore Institute of Engineering and Technology, TN, India-641109*

Abstract: ***Cloud computing is a type of computing that relies on sharing computing resources rather than having local server or personal devices to handle applications. IoT is also upcoming emerged field which limited with computational and storage capacity. Cloud computing technology is ubiquitous whereas IoT is pervasive in nature. By combining Cloud Computing and Internet of Things together have lot of scope for research.*** *This paper presents* ***communicating between cloud and internet of things with security aspects methods and Cloud with Internet of Things different application various parameter similarities discussed. Finally define future directions for cloud with internet of things platform and followed by a conclusion.***

Keywords: ***Internet of Things, IoT, Cloud Computing, Smart things, Cloud Communication, Cloud, Applications***

I. INTRODUCTION

Most of the papers proposed the model for cloud and IoT separately. This paper proposed integrations of cloud with internet of thins frame work. Cloud computing services can be private, public or hybrid. Private cloud services are delivered from a business data centre to internal users. This model offers versatility and convenience, while preserving management control and security. Internal customers may or may not be billed for services through IT chargeback. In the public cloud model, a third-party provider delivers the cloud service over the internet. Public cloud services are sold on-demand, typically by the minute or the hour. Customers only pay for the CPU cycles, storage or bandwidth they consume. Communication between cloud and internet of things secure way to be proposed. A growing number of physical objects are being connected to the Internet at an unprecedented rate realizing the idea of the Internet of Things (IoT). These applications include transportation, healthcare, industrial automation, and emergency response to natural and man-made disasters where human decision making is difficult. The IoT enables physical objects to see, hear, think and perform jobs by having them ―talk together, to share information and to coordinate decisions. The IoT transforms these objects from being traditional to smart by exploiting its underlying technologies such as ubiquitous and pervasive computing, embedded devices, communication technologies, sensor networks, Internet protocols and applications.

II. COMMUNICATION AMOUNG CLOUD AND INTERNET OF THINGS

Interactions between internet of things and the cloud computing there is a bi-directional flow of information. Data might flow from internet of things to the cloud, perhaps for storage or analytics. The cloud may also be the mediator and/or through

Which data (including actuating commands) are sent to internet of things. Much data will be sensitive, whether alone or in aggregate. It is therefore important that communication is secure,

and user-access to cloud services is properly controlled.

There are two motivations for securing communication: secrecy is preventing eavesdropping and data leakage and integrity is protecting data from corruption/interference. Note that here we do not consider communication within subsystems, but rather are concerned with the interaction of internet of things with cloud services. Communications Technology is secure communication is required to prevent unauthorized access to data (or metadata) that might be sensitive. Transport Layer Security (TLS) [1] uses cryptography to establish a secure channel to protect transmissions (including metadata such as protocol state, thus limiting side-channels) from both eavesdropping and interference. TLS employs a certificate-based model, relying on PKI and certificate authorities for authentication. TLS is a common feature of cloud-provider offerings, and can be used to secure the confidentiality and integrity of communications between internet of things and the cloud provider. With a general view to making secure communication more commonplace, there is recent work on enabling TLS over protocol stacks other than TCP/IP to better suit the requirements of internet of things, in terms of complexity and resource requirements. Examples include DTLS (Datagram Transport

Layer Security [2], [3]) for datagram oriented protocols such as UDP, and LLCPS [4] that applies TLS over the Near Field Communications LLCP (Logical Link Control Protocol). Depending on the deployment, architecture and interfaces to cloud services, these technologies could facilitate new forms of secure 'thing'-cloud interactions. Apart from TLS there are, of course, other mechanisms of securing 'thing'-cloud communication. Data can be encrypted by applications, which protect data not only in transit, but also beyond. Sharing secrets naturally entails management and engineering considerations [5]. Aside from any vulnerabilities inherent in the approach, the protection offered by any secure communication mechanism
is only as good as its implementation. For example, the recent Heartbleed vulnerability in the widely-used Open SSL library is estimated to have left 24–55% of TLS/SSL protected endpoints open to attack [6]. Extra care and consideration must be given to the newer schemes and implementations currently being developed to support IoT, especially those that may not have been widely scrutinized or deployed.

Access controls for IoT-Cloud is important that (external) access to cloud resources is regulated. Access controls [5] operate to govern the actions that may be taken on objects, be they accessing particular data (a file, record, data stream), issuing a query, performing some computation, and so forth. Controls are typically principal focused, in the sense that control policy governing a particular action is defined to regulate those undertaking the action, enforced when they attempt to take that action. There are two aspects to access control: authentication and authorization. Authentication refers to verifying who a principal is, i.e. are they who they say they are? Authorization rules follow authentication; once a principal is identified, what are their rights and privileges; what actions are they authorized to undertake? In a general cloud context, the provider will offer access controls to ensure that only the correct tenants/users (the principals) access the appropriate data and services. Cloud providers often have login/credential-based services for authenticating tenants/users. Authorization policy will be enforced as a principal attempts to take an action, based on their level of privilege, which might allow them to access storage and files held by the provider, initiate computation services etc.

The precise controls will depend on the specific service offering, but often include access control lists, role-based access controls, capabilities etc. See [5] for an overview of a number of security engineering techniques in an IoT context, a challenge for any access control regime is accounting for the fact that the interactions between internet of things may involve encounters with internet of things never before seen, or owned and operated by others. Towards this, Trusted Platform Modules [7] offer promise by providing strong guarantees, for example, with respect to device identity [8] and configuration [9], which access control mechanisms can leverage. Currently, cloud policy is focused: authorization rules are to ensure that a tenant accesses only its own resources, i.e. their files, VMs, databases, etc. However, for the IoT-Cloud, the lines are blurred. The data and resources of a tenant may be relevant to a number of different principals, and/or may control and coordinate a number of internet of things. Policy must be able to be consistently defined and applied across both of these dimensions. Access controls may be contextual, e.g. people may in general only access data concerning themselves. In exceptional circumstances, such as medical emergencies [10], wider access may be desirable, as specified by "break-glass policies".

Mechanisms are required to enable flexible access control policies to be defined by different parties, while also being able to identify and resolve potential policy conflicts. Such concerns are non-trivial, and will likely require some external constraints, such as ownership or economic incentives (e.g. those paying for the service) to help make access control policy more manageable.

Note that access controls govern the tenant/user provider interactions at the interface between them. These mechanisms typically do not, by themselves, offer users control beyond that point, e.g. how their data is managed internally by the provider(s). Controlling and coordinating internet of things: The cloud will play a role in mediating and coordinating internet of things, where actuating commands, the initiation/cessation of data flows, and so forth will be initiated from the cloud. It is clear that 'things' will need to maintain some form of access control, to prevent potentially anyone from taking over. This is illustrated, for example, by an access control vulnerability discovered in a consumer lighting system, allowing an attacker to issue lighting commands (causing blackout) by masquerading as a user-device [11].

The role of the cloud as a mediator of internet of things, brings several considerations. First is that the access controls are not necessarily symmetric, in that the process by which a internet of thing may access the cloud is not necessarily the same as how the cloud can initiate access to the internet of things. Because there will be far more internet of things than cloud services, there will likely also be a far greater range of access control implementations, credential services, etc., employed by internet of things. The cloud provider must be able to account for these. As such, standardization is clearly an important issue, and the role of gateway components will assist in limiting the diversity. Secondly, any cloud-based mediation and coordination will be driven by policy components, many of which reside within the cloud. To realize the wider IoT vision, policy enforcement mechanisms must be

sufficiently flexible to be defined across the range of devices, while accounting for the differences in access control models. That is, the cloud-deployed policy enforcement components must be able to dynamically switch between them to enable context-aware coordination when/ where appropriate, e.g. to adapt security levels based on a perceived risk [12].

III. APPLICATIONS

In this section describe a wide set of applications that are made possible or significantly improved

Table 1 SIMILARITY Among Different Applications And Its Parameters

Applications / Parameters	Smart System: loT for University[13]	Agriculture and Forestry[14]	Smart Classroom[15]	Smart Building with cloud computing[16]	Medical and Smart Health Care[17]
Architecture Model	Two tire	Three tire	Three tire	Three tire	Multi- tier
Protocol /Parameter	Zigbee, Z-wave, Wi-Fi, Bluetooth LE	B/S,C/S PDA,IR, RFID	Fidgeting Noise Sound level	Communication Standards Internet Protocol	RFID,IPv6, TCP/IP
Bandwidth/ Service Model	N/A	SaaS PaaS	N/A	SaaS PaaS IassS	N/A
Front-end Technology	Mobile App	GPS	Real-time feedback, Real Laboratory world, Sound interaction integrity	Mobile, System, User Teriminals	Smart Phone
Database technology	Big data	Knowledge Management databa	Data Center	Big data	Cloud storage Cloud SQL Big Query
Energy/ Reliability/ Efficiency	Energy lead to Saving	High Reliability, High Efficiency	N/A	Computational power, Enhance Reliability	Efficient storing, Processing, Retrieving valuable data.
Internet Connectivity	GPRS, 3G,WiFi, RJ 45, LAN,RFID, RF,Internet	TD/GPRS	HTTP/XML	N/A	3G,4G,ADSL DSLAM RoutersWiFi
IoT Device Sensor	Wireless, Zigbee, Gateway	Barcodes, IR Sensor, RFID, Wireless Transmission network.	PIR Sensor, Microphone Existence camera, Sound Sensor	Arduino Raspberry Pi	RTX-4100, AEKG, Arduino Raspberry Pi Blood oxygen sensor, Pulse oximatry, Smart phoneSensor
Algorithm/ Software	N/A	PDA Cycle Software core Calculation, Core Calculation R&D Platform, ES,DSS 3S	Signal Analysis & Classification	JS Service Under Arch Linux, JavaScript	Restful Services for iOS, Android, Java Script/ Machine Learning Algorithm
Security	Network Security, SMS alerts, e-mail	Safety Traceability System	N/A	N/A	N/A

IV. CONCLUSION

This paper proposed cloud computing and internet of things communication aspects scenario, which accommodates secure connection methods and privacy preservation during data sharing. Comparison of different IOT applications and its parameters help to future to develop efficient implementations. The future work to implement real time complete frame work developments for approaching Cloud with Internet of Things architecture which is provided assessing power consumption and communication improvement and open issues like performance, security, reliability, privacy, integrations of IoT with cloud, storage to analyze among cloudThings.

REFERENCES

[1] T. Dierks and C. Allen, "The TLS Protocol Version 1.0," IETF, Tech.Rep.1999.

[2] D. McGrew and E. Rescorla, "Datagram Transport Layer Security(DTLS) Extension to Establish Keys for the Secure Real-time Transport Protocol (SRTP)," IETF, 2010.

[3] S. L. Keoh, S. Kumar, and H. Tschofenig, "Securing the Internet of Things: A Standardization Perspective," Internet of Things Journal, vol. 1, no. 3, pp. 265–275, 2014.

[4] P. Urien, "LLCPS: A new security framework based on TLS for NFC P2P applications in the Internet of Things," in Consumer Communications and Networking Conference (CCNC), 2013 IEEE. IEEE, 2013, pp. 845–846.

[5] R. J. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, 2nd ed. Wiley Publishing, 2008.

[6] Z. Durumeric, J. Kasten, D. Adrian, J. A. Halderman, M. Bailey,F. Li, N. Weaver, J. Amann, J. Beekman, M. Payer, and V. Paxson,"The Matter of Heartbleed," in Proc. Internet Measurement Conference (IMC). ACM, 2014, pp. 475–488.

[7] T. Morris, "Trusted Platform Module," in Encyclopedia of Cryptography and Security. Springer, 2011, pp. 1332–1335.

[8] C. Lesjak, T. Ruprechter, J. Haid, H. Bock, and E. Brenner, "A Secure Hardware Module and System Concept for Local and Remote Industrial Embedded System Identification," in Emerging Technology and Factory Automation (ETFA). IEEE, 2014, pp. 1–

[9] M. Hutter and R. Toegl, "A Trusted Platform Module for Near Field Communication," in International Conference on Systems and Networks Communications (ICSNC). IEEE, 2010, pp. 136–141.

[10] J. Singh and J. Bacon, "On Middleware for Emerging Health Services," Journal of Internet Services and Applications, vol. 5, no. 6, pp. 1–34,2014

[11] N. Dhanjani, "Hacking Lightbulbs: Security Evaluation of the Philips hue Personal Wireless Lighting System," 2013, accessed:21st July 2015.

[12] R. M. Savola and H. Abie, "Metrics-driven Security Objective Decomposition for an e-Health Application with Adaptive Security Management," International Workshop on Adaptive Security. ACM, 2013.

[13] Dr. Kamlesh Sharma and Dr. T. Suryakanthi Smart System: loT for University2015 International Conference on Green Computing and Internet of Things (ICGCloT978-1-4673-7910-6/15/$31.00 ©20 15 IEEE

[14] Bo, Yifan, and Haiyan Wang. "The application of cloud computing and the internet of things in agriculture and forestry." Service Sciences (IJCSS), 2011 International Joint Conference on. IEEE, 2011

[15] Gligorić, Nenad, Ana Uzelac, and Srdjan Krco. "Smart classroom: real-time feedback on lecture quality." Pervasive Computing and Communications Workshops (PERCOM Workshops), 2012 IEEE International Conference on. IEEE, 2012.

[16] Tragos, Elias Z., et al. "An IoT based intelligent building management system for ambient assisted living." 2015 IEEE

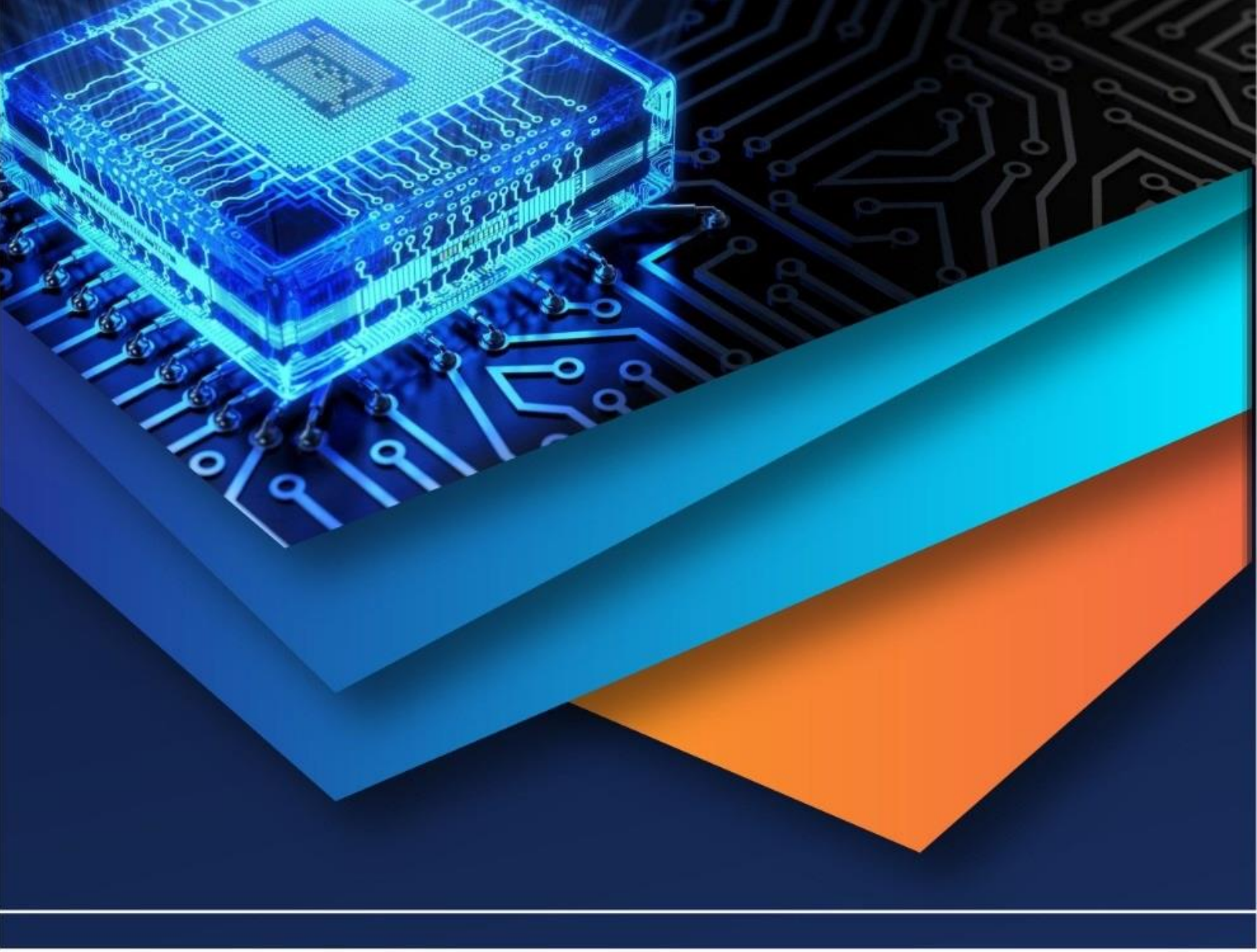
[17] International Conference on Communication Workshop (ICCW). IEEE, 2015.

AUTHOR DETAILS

Author1: S.Sivakumar, is a Research Scholar in the Department of Computer Science, Sree Saraswathi Thiyagaraja College, Affiliated to Bharathiar University, Coimbatore. Pursuing research in the field of Cloud Computing and Internet of Things, He completed his B.Sc and M.Sc Degree in 2001 and 2003 under Bharathiyar University, India. He received his M.Phil degree from Bharathidasan University, Tiruchirapalli, in 2005. He has more than 12 Years of Teaching Experience and currently working as an Assistant professor of Computer Science, Pollachi College of Arts and Science, Pollachi,TN,India.

Author2: Dr.V.Anuratha did her UG graduation in Computer Science at PSG CAS, Coimbatore. She did her MCA at Madras University, M.Phil at Manonmaniam Sundaranar University, Tirunelveli, Ph.D in the area of Wireless Area Networks through Mother Teresa University, Kodaikanal. Her area of interest is Wireless Networks, Cloud Computing and MANET. She have guided more than 20 M.Phil Research scholars and currently guiding 6 Ph.D Scholars in the area of Computer Science. She has published more than 10 research papers in reputed journals.

Author3: Dr.S.Gunasekaran, completed his B.E and M.E degree in 2001 and 2005 under Bharathiyar University and Anna university respectively. He received his Ph.D degree from Anna University Coimbatore, in 2011. He published around 25 papers in referred International Journals. He has 11 years of teaching experience and currently working as a prof and head Department of CSE, Coimbatore Institute of Engineering and Technology. His area of interest accumulated in Mobile Computing, Data Mining, NLP, Cloud Computing and IoT.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY