Performance and Security Issues of Integrating Cloud Computing with IoT

Rubika Walia and Prachi Garg

Abstract Internet of things (IoT) empowers different gadgets to interface with one another by means of web. This guarantees the gadgets to be brilliant and send the data to an incorporated framework, which will at that point screen and take activities as per the undertaking given to it. IoT can be utilized in numerous areas such human services, transportation, amusement, power lattices, and keen structures. IoT is required to go about as a motivation for the future developments, and its utilization is relied upon to rise exponentially over the coming years. As indicated by security point of view, the IoT will be challenged with more extreme difficulties. Subsequently, the new security and protection issues will emerge.

Keywords Internet of things · Destination-oriented directed acyclic graph · Queue utilization · Service level agreement · Routing protocol for low power and lossy network

1 Introduction

Internet of things is a kind of setup of several physical entities or stuffs. This setup comprises software, microelectronics, and sensors to achieve superior facility through exchanging facts with makers, operatives, and several other associated devices. In direction to build mobile devices more capable, a combination of cloud work out expertise and mobile devices is used. Mobile cloud combination is helpful to increase computational supremacy and storing of mobile devices as in Fig. 1. In direction to realize the complete distribution, permitted transmission, on-demand use, and ideal distribution of several built-up assets and competences, the uses of the services of IoT and cloud work out in engineering are considered. Through the combination of IoT and cloud, we have the prospect to enlarge the use of the existing

R. Walia (✉)
MMEC, MMICT & BM, M. M. (Deemed to be University), Mullana, Ambala, Haryana, India

P. Garg
MMEC, M. M. (Deemed to be University), Mullana, Ambala, Haryana, India

N. Marriwala et al. (eds.), *Emergent Converging Technologies and Biomedical Systems*,
Lecture Notes in Electrical Engineering 841,
https://doi.org/10.1007/978-981-16-8774-7_1

Fig. 1 IoT and cloud computing integration

expertise which is available in cloud settings. This integration can provide cloud storage to IoT applications [1].

But integrating IoT with cloud arise new problems such as latency, bandwidth requirements, reliability, security, etc. All of these problems motivated to investigate, fog computing, as new distributing computing paradigms, to see the necessities of latency-sensitive IoT submissions. Most of the IoT devices are available with lowest level of security. Some of these devices do not get enough updates during its usage. These devices having obsolete hardware and software open to probable attack for their trusted customers [2]. The world is experiencing key changes or high-tech progresses with the arrival of PC "things," main on the web and then in cloud computing [3]. The fundamental problem here is safety which is not reflected in product plan because networking devices and other entities are comparatively fresh. Usually, IoT products are available with outdated operational system and software which cannot be easily patched. Another problem is usually buyers use smart devices with default passwords which are weak and often fail to modify adequately tough secret word as password. Encryption procedure shows a key role to deliver safe transmission above network [1].

1.1 Cryptography

From last few years, network security has grown considerable importance because it provides security mechanism for web-based applications. In order to mitigate modern attacks, protection is very necessary. Mitigation of attacks, confidentiality uncertainties is solitary the important traits of present attacks. Cryptography encodes information, and the individual having the key can decodes this. Cryptography makes sure that the data being communicated has not been transformed in transfer. A cryptographic procedure, or cryptogram, is a scientific task castoff for encryption and decryption process. Cryptography procedure along with a key (combination of numbers, alphabets or special symbols) is used to encode plaintext. The identical plaintext can be encoded to unique encrypted content with dissimilar keys. The security strength of encryption statistics depends on the power of set of rules of encryption procedure and secrecy of the key. In order to put on encryption procedures for IoT, it is required

to make additional work to more investigation to guarantee how these procedures can be effectively applied for IoT with restricted storage and small speed processor.

1.2 Trust Models

Nowadays, documents are isolated in various data hubs, and faraway hosts contain the applications. This separate data and remote applications are fetched by the cloud to consumer's PC in simulated form. Cloud customers get computation and storing from cloud regardless of time and locality. But for the better commercialization of this cloud technology, there must have the reliance by the cloud users for the cloud providers that they complete their requested work as per the provision level contracts; thus, the data of the cloud users after processing the data will be secured as shown in Fig. 2. To achieve all these necessities, trust management can be an important portion of marketable traits of cloud tools. There are three kinds of provision transfer prototypes provided by the cloud infrastructure. They are such as "Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS)." Cloud service providers provide infrastructure, platform and software to consumers in a cost-effective and truthful manner. Firms like Google and Amazon grounded on the trust running system have implemented reputation and helped the customers to find the reliable source providers to perform e-business trades in a safe and assured way [4]. Now, the question arises how trust is computed. Trust can be measured in two ways:

(a) By checking the current abilities of the supplier whether it can offer worthy service to users.
(b) By checking previous credentials of the supplier. Previous credentials of cloud source define the past repute and facility archives of the assets. It comprises

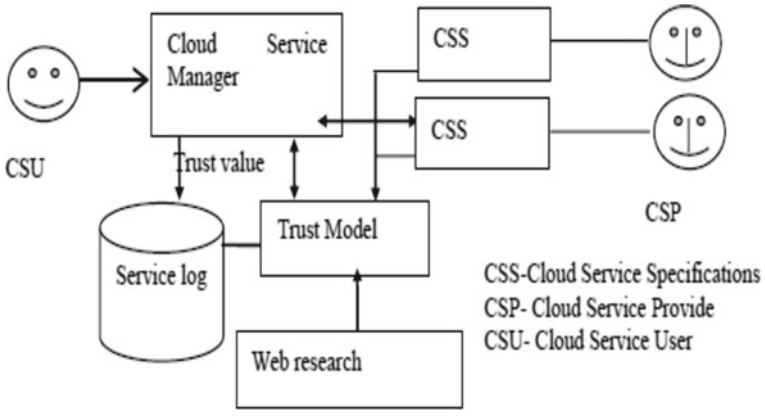

Fig. 2 Architecture of trust evaluation in cloud environment

consistency, obtain ability, turnaround time, and data truthfulness, safety level of the location, bandwidth and expectancy of the assets [4].

1.3 Load Balancing Based on Routing Protocol for Low Power and Lossy Networks (RPL)

One of the most well-known issues in WSNs is the manner by which to advance the information broadcast whereas augmenting the system lifespan. In this unique circumstance, the IPv6 Routing Protocol for low power and lossy networks (RPL) was suggested by the IETF. The IETF IPv6 Routing Protocol for low power and lossy networks (RPL) is extensively used to provide routing among sensor nodes as presented in Fig. 3. In most setups, a mainstay network of intermediate nodes is set up, which is likely to be fixed. RPL practices a hierarchical routing method for the static backbone network. Key characteristic of movement is an extremely self-motivated topology which marks in recurrent interruptions with neighboring nodes. As of these interruptions, data packets directed to a movable device can be directed to edges (parents) even then the mobile device is currently out of reach of these parents [5]. The practice of this protocol could become public and standard in IPv6 sensor networks in the future, even though some obstacles slow acceptance today [6].

Load Balancing

Load-balancing mechanism can benefit an IoT network between its sensor nodes in twofold methods: firstly, link to determine all possible routes available for routing can be enabled and secondly, the network can be distributed evenly to make finest practice of the system life span [6].

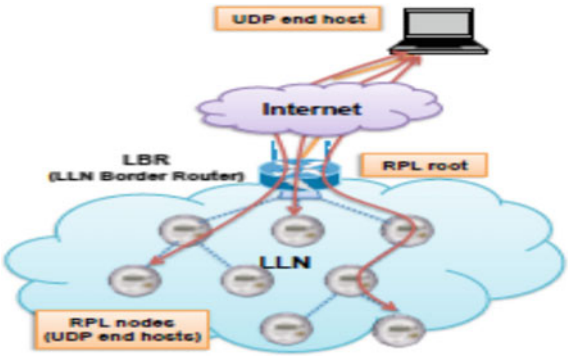

Fig. 3 Illustration of an IOT multi-hop LLN scenario

2 Related Work

2.1 Security and Privacy of IoT

Nie et al. [5] reviewed the base functions of two algorithm (DES and Blowfish)), examined the safety of procedures, and assessed encryption function speed grounded on altered memory bulks. Patil et al. [7] applied and investigated price tag and enactment of widely used cryptography algorithms (DES, 3DES, AES, RSA and Blowfish). It is concluded that based on the entropy Blowfish scores highest among all these procedures and is top appropriate against guessing attack. Poonia et al. [8] enhanced and evaluated the Blowfish procedure on the base of dissimilar constraints. Suresh et al. [9] analyzed several safety mechanisms for IoT and the importance of encryption in IoT. After several comparisons, "Blowfish" as a capable encryption procedure is designated. Bruschi et al. [10] proposed an intercommunication layer which allows isolating the physical assets but managing the migration of facility instances according to the operator's location. Mota et al. [11] compared commonly used cryptography procedure such as symmetric algorithms (DES, Blowfish, AES) and asymmetric algorithms (ECC, RSA). It is concluded that Blowfish is finest in footings of finishing time, memory used, throughput, power intake, safety, and is fit for IOT. Stergiou et al. [12] presented a review of IoT and cloud computing with an emphasis on the safety concerns of both skills. The author joints the two above-mentioned skills to inspect the shared topographies and reported the profits of their combination. Nandy et al. [13] reported on IoT safety mainly on validation mechanisms. The author emphasized massive attacks and real methodologies on the IoT verification mechanism and argued current safety authentication procedures and assessment systems of IoT validation. Kamgueu et al. [14] reviewed latest workings on RPL and highlights key offerings to its enhancement, particularly those associated to topology optimization, safety, and movement. Donno et al. [15] presented the current and well-structured investigation of the safety problems of integrating cloud computing with IoT. A clear picture of various security issues and their potential impact was presented. It is concluded that securing IoT devices is not enough, as many cyber-storms come from clouds also. Malge and Singh [16] state that IoT has four main modules comprising recognizing, data handling, applications and facilities, diverse access and supplementary modules, e.g., safety and confidentiality. The author offered safety view from the viewpoint of layers that covers IoT. Adamou et al. [17] focused on safety and confidentiality thoughts by examining selected probable challenges and threats that must to be fixed. The author examined the IoT design and present uses to complete this and talk over safety as well as confidentiality worries and problems. Kutzias et al. [2] derived general integration design as a supporting tool for the suggestion of the different integration contests. Vijayalakshmi et al. [18] discussed about the motive, investigation carried out in this field, diverse skills, and the future progress of edge computing background. Kaur et al. [19] focused on cloud providers to offer a pay-as-you-use prototypical where clients pay for the particular

assets used. Similarly, cloud accommodating by worth of a facility adds value to IoT startups by providing cost-cutting of scale to lessen their total cost configuration.

2.2 Trust Models

Li et al. [20] examined some trust prototypes castoff in big and scattered location and then presented a new cloud trust prototype to resolve safety problems in cross-clouds setting in which cloud client can select dissimilar suppliers' facilities and assets in dissimilar fields. Manue et al. [21] presented a unique trust prototype established on previous credentials and existing aptitudes of a cloud source supplier. Trust assessment is done using four constraints such as obtain capability, consistency, turnaround competence, and data reliability. Kaur et al. [22] discussed several constraints and reliance prototypical structure for particular web service and a number of constraints used by them for computing reliance. Xu et al. [23] provided a categorized trust demonstrating technique to consumer to expand safety situational consciousness in the cloud computing situations. Kaur et al. [19] focused on cloud providers to offer a pay-as-you-use model where clients pay for the particular resources used. Also, cloud hosting as a facility adds value to IoT startups by providing cost-cutting of scale to lessen their total cost configuration.

2.3 Load Balancing

Kim et al. [24] proposed QU-RPL (an effective queue utilization which is based on RPL) that significantly improved the performance of e2e packet distribution as compared to the regular RPL. It is planned to choose the parental node for each node by considering their hop distances to an LBR as well as the queue consumption of its nearby nodes. Zhou et al. [25] proposed a context-aware unburdening decision procedure targeting to deliver code offloading choices at runtime on picking wireless intermediate and which probable cloud resources as the offloading place established on the device situation. Zhu et al. [6] proposed a routing protocol with an energy equalization to make the most of the living time of the constrained nodes. Also based on the cache utilization, a multi-path advancing path is suggested. Qasem et al. [26] proposed a protracted objective function that set of scales the count of kid's nodes of the parent nodes to escape the congestion problem and guarantee node life span expansion in RPL. The usual OFs are castoff to figure a destination-oriented directed acyclic graph (DODAG) where the traffic jam nodes may suffer from unbalanced traffic burden. Tarak Nandy et al. [13] reported on IoT safety mainly on validation mechanisms. The author emphasized massive attacks and useful methodologies on the IoT verification mechanism and argued current safety authentication procedures and assessment systems of IoT validation. Kaur et al. [19] focused on cloud providers to offer a pay-as-you-use model where clients pay for the particular resources used.

Also, cloud hosting as a facility adds value to IoT startups by providing cost-cutting of scale to lessen their total cost configuration.

2.4 Cloud Computing

Gonzalez et al. [27] reported that cloudlet idea is a subclass of edge computing useful to mobile systems, and the fog idea is a subclass of edge computing practical to Internet of things (IoT). The author delivered a detailed investigation of associated issues, classifying the focal study areas associated to edge computing concerning the state of the art and the prospect of edge computing. Singh et al. [28] depict a comprehensive systematic works investigation of resource administration in the area of cloud in broad and cloud resource planning. Wazir et al. [29] present the various models projected for SLA in cloud computing, to beat on the challenges exists in SLA. Challenges associated with performance, client level fulfillment, safety, profit, and SLA Defilement and additionally discuss SLA design in cloud computing, existing models projected for SLA in several cloud service models like SaaS, PaaS, and IaaS or the benefits and restrictions of present models with the assistance of tables. Padmaja et al. [30] to increment the proficiency of the work load of cloud computing application, programming is the tasks performed to urge most extreme profit. Author mentioned concerning reasons to adopt programming, programming phases, programming sorts, and a few of the programming algorithms utilized in differing kinds of clouds (Table 1).

Table 1 Findings and research gaps

Author	Year	Approach/technique	Findings	Research gaps
Wenjuan Li and Lingdi Ping	2009	Trust model in cross-clouds environment to solve security issues	Experimental results showed the suggested model can competently and securely build trust association in cross-clouds setting	In reality entities behaviors are more complex and there are many other potential security risks
Paul Manue	2014	Trust model built on previous credentials and current abilities of a cloud resource supplier	Showed in what way a facility level arrangement is organized joining excellence of facility necessities of consumer and abilities of cloud store supplier	However, there are some more attributes such as Honesty, Return on Investments and Utilization of Resources to measure trust

(continued)

Table 1 (continued)

Author	Year	Approach/technique	Findings	Research gaps
Rizwana Shaikh and M. Sasi Kumar	2015	Trust model to measure the security strength	Competence of the model is also confirmed by estimating trust worth for present cloud services	
Usvir Kaur and Dheerendra Singh	2015	Trust model for web services	Majority of trust models focused on reviews provided by consumers and providers	
Hyung-Sin Kim	2015	Queue utilization-based RPL (QU-RPL)	Improved the performance of end-to-end packet delivery as compared to the standard RPL significantly	
Bowen Zhou	2015	Context-aware offloading decision algorithm	Proficiency of mobile policies has been upgraded in latest years	Performance of the decision making algorithm can be improved by considering more context parameters, e.g., context of public cloud to provide an optimal solution for code offloading decision making process
Gokulnath and Rhymendthari araj	2016	Analyzed available solutions for cloud trust	Any safety negotiation toward lessening the cost is highly unbearable	As cloud is dynamic and hence needs sophisticated approaches to solve the problem of cloud trust dynamism
Nelson Mimura Gonzalez	2016	Analysis of edge computing concerning the state of the art and the coming of edge work out	Fog computing is quickly moving toward mobile networks and mobile technologies	
Manju Suresh and Neema M	2016	An efficient cryptographic algorithm "Blowfish."	Enhancements in footings of encryption time by 16.9% and output by 18.7%	Implementation of modified Blowfish algorithm in an IoT environment

(continued)

Table 1 (continued)

Author	Year	Approach/technique	Findings	Research gaps
Licai Zhu	2017	Routing protocol with energy equalization	Surviving time of restricted nodes has improved	To make the most of the persistence time of the nodes around the sink, they can be further optimized
Xu W	2018	Hierarchical trust modeling method	Proposed method reduces the complexity of trust computing and assists cloud computing participants to make good trust decisions	
Christos Stergiou	2018	Surveyed various security issues related with the integration of IoT and cloud computing	Benefits of integration of IoT and cloud have discovered	
Ado Adamou	2019	Security and privacy considerations	All records in a CoT system cannot have the similar level of sensitivity. Particular statistics as medicinal or economic data are more delicate than others, and then prerequisite additional care and more care should be reserved for it	The IoT entity secretes large quantity of statistics. So to accomplish the objective of competently handling the huge volume of produced data; the present cloud design needs to be secure. This enhancement is essential to be more effectual and useful for the IoT-based real-time facilities in footings of energy ingesting, safety, confidentiality, and end-to-end delays
Sunil Kumar Malge	2019	Highlights the research status in this field from encryption mechanism, communication safety, protecting sensor data, and encryption procedure		Expansion of the IoT will bring additional thoughtful safety glitches, which are constantly the attention and the key undertaking of the investigation

(continued)

Table 1 (continued)

Author	Year	Approach/technique	Findings	Research gaps
Michele De Donno	2019	Provides an up-to-date and well-structured review of the safety matters of cloud computing in the IoT era	Massive common of attacks presently directed to IoT devices are fueled by trivial faults, such as absence of validation procedures	Formal approaches and rigorous semantics have also not been considered in this work despite their importance for cloud and distributed concurrent systems in general

3 Findings and Research Gaps

4 Conclusion and Future Scope

Hybrid encryption for security of IOT devices can be used for safety in multi-clouds, at user level (to improve the safety of IoT devices) and at sever side (to secure the data before sending to cloud. Attaining good performance at server is conditional and depends on an optimal division of the application mechanism among the IoT devices and cloud platforms that depends on runtime conditions. Implementation of framework consisting of hybrid encryption before uploading the customer records to cloud in vision to safely distribute data among several clouds by trust evaluation is our immediate future work.

References

1. Bonomi F, Milito R, Zhu J, Addepalli S (2012) Fog computing and its role in the internet of things. In: MCC'12, August 17, 2012, ACM 978-1-4503-1519-7/12/08
2. Kutzias D, Falkner J, Kett H (2019) On the complexity of cloud and IoT integration: architectures, challenges and solution approaches. In: Proceedings of the 4th international conference on internet of things, big data and security, pp 376–384
3. Fotouhi H, Moreira D, Alves M, Yomsi PM (2017) mRPL+: a mobility management framework in RPL/6LoWPAN. Comput Commun 104(2017):34–54
4. Dillon T, Wu C, Chang E (2010) Cloud computing: issues and challenges. In: 24th IEEE international conference on advanced information networking and applications
5. Nie T, Zhang T (2009) A study of DES and blowfish encryption algorithm. In: IEEE Reg. 10 Annu. Int. Conf. Proceedings/TENCON, pp 1–4. https://doi.org/10.1109/TENCON.2009.5396115
6. Zhu L, Wang R, Yang H (2017) Multi-path data distribution mechanism based on RPL for energyconsumption and time delay. Information 8(4):1–19. https://doi.org/10.3390/info8040124
7. Patil P, Narayankar P, Narayan DG, Meena SM (2016) A comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA and Blowfish. Procedia Comput Sci 78:617–624. https://doi.org/10.1016/j.procs.2016.02.108

8. Poonia V, Yadav NS (2015) Analysis of modified Blowfish algorithm in different cases with various parameters. In: ICACCS 2015 - Proceeding 2nd international conference on advanced computing and communication systems, pp 5–9. https://doi.org/10.1109/ICACCS.2015.7324114
9. Suresh M, Neema M (2016) Hardware implementation of blish algorithm for the secure data transmission in internet of things. Procedia Technol 25(Raerest):248–255. https://doi.org/10.1016/j.protcy.2016.08.104.
10. Bruschi R et al (2017) Open stack extension for fog-powered personal services deployment. In: Proceeding of 29th international teletraffic congress ITC 2017, vol 2, pp 19–23. https://doi.org/10.23919/ITC.2017.8065705.
11. Mota AV, Azam S, Shanmugam B, Yeo KC, Kannoorpatti K (2018) Comparative analysis of different techniques of encryption for secured data transmission. In: IEEE International conference on power, control, signals and instrumentation engineering ICPCSI 2017, pp 231–237. https://doi.org/10.1109/ICPCSI.2017.8392158.
12. Stergiou C, Psannis KE, Kim BG, Gupta B (2018) Secure integration of IoT and cloud computing. Futur Gener Comput Syst 78(December 2017), 964–975. https://doi.org/10.1016/j.future.2016.11.031
13. Nandy T et al (2019) Review on security of internet of things authentication mechanism. IEEE Access 7(October):151054–151089
14. Kamgueu PO, Nataf E, Ndie TD (2018) Survey on RPL enhancements: a focus on topology, security and mobility. Comput Commun 120(July 2017):10–21
15. De Donno M, Giaretta A, Dragoni N, Bucchiarone A, Mazzara M (2019) Cyber-storms come fromclouds: security of cloud computing in the IoT era. Futur Internet 11(6), 1–30. https://doi.org/10.3390/fi11060127.
16. Malge S, Singh P (2019) Internet of things IoT: security perspective. Int J Trend Sci Res Dev 3(4):1041–1043. https://doi.org/10.31142/ijtsrd24010
17. Ari AAA et al (2019) Enabling privacy and security in cloud of things: architecture, applications, security and privacy challenges. Appl Comput Inf xxxx. https://doi.org/10.1016/j.aci.2019.11.005
18. Vijayalakshmi V, Vimal S (2019) A new edge computing based cloud system for IoT applications. Int J Recent Technol Eng (IJRTE) 8(2)
19. Kaur C (2020) The cloud computing and internet of things (IoT). Int J Sci Res Sci Eng Technol 7(1) (www.ijsrset.com)
20. Li W, Ping L (2009) Trust model to enhance security and interoperability of cloud environment. Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics) 5931:69–79. https://doi.org/10.1007/978-3-642-10665-1_7
21. Manuel P (2015) A trust model of cloud computing based on quality of service. Ann Oper Res 233(1):281–292. https://doi.org/10.1007/s10479-013-1380-x
22. Kaur U, Singh D (2015) Trust: models and architecture in cloud computing. Int J Comput Sci Inf Secur 13(12):150–155
23. Xu W (2018) Study on trust model for multi-users in cloud computing. Int J Netw Secur 20(4), 674–682
24. Kim HS, Paek J, Bahk S (2015) QU-RPL: queue utilization based RPL for load balancing in largescale industrial applications. In: 2015 12th Annu. IEEE Int. Conf. Sensing, Commun. Networking, SECON2015, pp 265–273. https://doi.org/10.1109/SAHCN.2015.7338325
25. Zhou B, Dastjerdi AV, Calheiros RN, Srirama SN, Buyya R (2015) A context sensitive off loading scheme for mobile cloud computing service. In: Proc.—2015 IEEE 8th Int. Conf. Cloud Comput. CLOUD2015, pp 869–876. https://doi.org/10.1109/CLOUD.2015.119
26. Qasem M et al (2018) Load balancing objective function in RPL draft-qasem-roll-rpl-load-balancing-01. Stand Track October:1–10
27. Gonzalez NM, et al. (2016) Fog computing: data analytics and cloud distributed processing on the network edges. In: Proc.—Int. Conf. Chil. Comput. Sci. Soc. SCCC. https://doi.org/10.1109/SCCC.2016.7836028

28. Singh S, Chana I (2015) Q-aware: quality of service based cloud resource provisioning. Computers and electrical engineering. Elsevier Ltd, Amsterdam
29. Wazir U, Khan F, Shah S (2016) Service level agreement in cloud computing: a survey. Int J Comput Sci Inf Secur (IJCSIS) 14(6)
30. Padmaja K, Seshadri R, Anusha P (2016) Different scheduling algorithms in types of clouds. Int J Comput Sci Trends Technol (IJCST) 4(5)