International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 6 | ISSN : 2456-3307

Security and Authentication for Devices to Achieve Qos in IOT & Cloud

Dr. R. Jemima Priyadarsini[1], S. Vivin Jose[2]
[1]Associate Professor, Department of Computer Science, Bishop Heber College, Trichy, Tiruchirappalli, Tamil Nadu, India
[2]Research Scholar Department of Computer Science, Bishop Heber College, Trichy, Tiruchirappalli, Tamil Nadu, India

ABSTRACT

The IoT (Internet of Things) is a network which connects things to the Internet for the intend of interchanging information through the information sensing devices with acceptable protocols. On the other hand, Cloud computing has virtually unlimited capabilities in terms of storage and processing power, is a much more mature technology, and has most of the IoT issues at least partially solved. Sensing Devices utilize in households and smart city is now interconnected with the Internet. These interconnections provide a full series of data that can be serene, aggregate, and then collective in sheltered and privacy-aware style. Some essential fields such as Wireless Sensor Network and Intelligent Transport System (ITS), base nodes collect information and transmit it to the destination nodes. Destination sends commands by the relay devices to the base nodes. Therefore, the integration of cloud and Internet of Things to providing the best service to users and have the highest level of customer satisfaction should always provide quality of service can be guaranteed. The purpose of this paper is to evaluate the integrity requirements of cloud services and Internet of Things so that quality of service in these services must be guaranteed. Thus maintaining the security of both base nodes and destination nodes in this kind of communication is a pressing problem. Instead of proposing yet another security scheme, this can be made easy if devices are identified before communication with secure routing.

Keywords: IoT (Internet of Things), Sensor nodes, Routing algorithm, Security.

I. INTRODUCTION

With the progress in wireless communication, Pervasive computing and mobile computing, resulted in a new model known as the internet of things (IoT). IoT is attracting a lot of researchers and industrial innovation. The definition for the IoT could be as the ubiquitous and global networks, which offer various applications for controlling and monitoring the physical world activities of the information collection, data cleaning, processing and analysis of data generated by IoT sensors. It can be seen as a network of wide-range devices that introduces not only the various security issues available in sensor devices, mobile communication, and the internet, but also some abnormal and accentuated issues like user and network privacy, sensor life cycle, secure routing and quality of service among these devices [1].

In IoT, people and objects are interconnected with the internet. In recent years, widespread consideration has been given to Internet of Things, because it opens marvelous prospects for a large number of innovative applications. This new paradigm promises to advance the quality of our lives. It has massive impact on supply chain management, location tracking, agriculture, real time financial analysis, energy efficiency, remote monitoring and maintenance, business process management and so on. It also has received much attraction from researchers

and industrialists all around the world. Developments in the IoT scenario allow us to save loads of dollars in business improvements and mark our lives enhanced. Though, many researches are going on in this field, it still has many potential issues and challenges [2]. This document deal one of the famous issues that are safety in IoT. Safety leftovers one of the highest issue that base the growth and application of IoT.

With the appearance of the Internet of belongings (IoT), it is essential to describe repair model, which can classify IoT application and decide the Quality of repair (QoS) factor necessary to satisfy the requirements of those military. On the other hand, as Wireless Sensor Networks (WSN) constitutes a main component of the IoT, they become a key factor concerning QoS provision [3]. In this viewpoint, we center our psychoanalysis on the likely WSNs addition approach in the IoT while as long as QoS and which best practice to adopt. It concerning QoS supplies, we also define repair model for the IoT and depiction their viability from side to side a classification of IoT application.

As an emerging area in terms of technology, application areas and research, IoT has wide research scope in all of the areas like architecture, implementation, protocols, standardizations and QoS management and implementations. Near are a small explore, assessment and implementations of IoT training, QoS system and IoT obedience / area by a variety of researchers and attention collection [4]. Day by day more and more 'things' are becoming integral part of human life by the way each of objects adapt the capabilities of sensing, interactive capability, communicative, computing and with decision making capabilities using the blend of local and globally available data, resources and computing power making everything to become part of IoT with heterogeneity in the real and literal sense. Since of the wide diversity of scope, rising number of devices in IoT, the ubiquitous presence, varied nature of IoT system and wide diversity of request areas address the quality of service in IoT is very critical. Fineness of repair (QoS) in IoT is one of the dangerous factors which need study and stabilization for QoS completion, running and optimizations. The assessment is done to grant a thought of disparate QoS proposal, implementations and architectures for an array of nature of tune limit of IoT.

Cloud systems in IoT are fundamental to manage the devices connected through the Internet in a given administrative domain [5]. This special issue includes high quality and novel contributions from researchers coming from both the academic and industrial communities who work on the integration of distributed sensor networks, cloud computing, and IoT environments. In particular, it advances the state of the art in IoT Cloud considering the following main aspects: i) integration of IoT devices with the Cloud, ii) configuration of IoT devices over the Cloud, iii) communication of IoT devices over the Cloud, and iv) security of IoT devices over the Cloud.

II. RELATED WORKS

In [6] Diego Mendez, Ionic Papapanagiotou, Beijing Yang et al present The Internet of Things (IoT) is future for ever-present connectivity among dissimilar entities or "things". As its reason is to give effectual and ordered solution, safety of the devices and system is a challenging issue. The number of devices connected all along with the ad-hoc nature of the system further exacerbates the location. Then, safekeeping and seclusion has emerged as a noteworthy brave for the IoT. In this thesis, we aim to supply a careful study linked to the isolation and sanctuary challenge of the IoT. This essay addresses these challenges from the perspective of technology and architecture worn. This work focus also in IoT inherent vulnerabilities as well as the safety

challenge of a variety of layer base on the safety values of data privacy, integrity and availability.

In [7] Carla Mouradian, Diala Naboulsi, Sami Yangui, Roch H. Glitho, Monique J. Morrow, and Paul A. Polakos et al present blur compute with its three key facet (i.e., IaaS, PaaS, and SaaS) and its intrinsic reward (e.g., elasticity and scalability) still faces several challenges. This item presents a comprehensive survey on fog compute. It critically reviews the condition of the art in the light of a concise set of assessment criterion. We cover both the architectures and the algorithms that make fog systems. Challenges and research directions are also introduced. In addition, the lessons learned are reviewed and the prospects are discussed in terms of the key role fog is likely to play in emerging technologies such as Tactile Internet.

In [8] Hourieh KHODKARI, Saied Ghazi MAGHREBI et al presents IoT and cloud computing working in integration makes a new paradigm, which we have termed here as Cloud IoT. The two worlds of Cloud and IoT have seen an independent evolution. However, several mutual advantages deriving from their integration have been identified in literature and are foreseen in the future. On the one hand, IoT can benefit from the virtually unlimited capabilities and resources of Cloud to compensate its technological constraints. Specifically, the Cloud can offer an effective solution to implement IoT service management and composition as well as applications that exploit the things or the data produced by them. On the other hand, the Cloud can benefit from IoT by extending its scope to deal with real world things in a more distributed and dynamic manner, and for delivering new services in a large number of real life scenarios.

In [9] Gonçalo Marques, Nuno Garcia, Nuno Pombo et al presents The vision for the Internet of Things (IoT) states that various “things”, which include not only communication devices but also every other physical object on the planet, are going to be connected and will be controlled across the Internet. The thought of the IoT has paying attention considerably notice from a lot of investigators in new being. The nonstop scientific improvement creates likely to build smart devices with huge potentials for sensing and between, allowing several enhancements based on the IoT paradigm. This episode present a appraisal on investigate on IoT and analysis quite a few IoT projects focused on IoT architectures, elements, Quality of Service (QoS) and currently open issues. The main objective of this chapter is to allow the reader to have an overview on the most important concepts and fundamental knowledge in IoT.

In [10] M.Mullaiarasu, Dr S.Veni et al presents The interconnection via the Internet of computing devices embedded in everyday object enable them to send and receive data. In the paper, we tend to report on the Packet Delivery Ratio and Throughput of the subsequent communication protocols MQTT, CoAP and DDS in the traffic protocol nodes. MQTT protocol is employed for aggregation devices knowledge and acts it to servers. CoAP could be a specialized internet transfer protocol to be used in forced nodes and network.

III. EXISTING METHODS

3.1 CLUSTERING BASED D2D GROUP COMMUNICATION METHOD

The clusters are formed from devices that are close and communicating with each other, for example, sharing data. The cluster carve up the broadcasting assets among additional devices in the scheme thus creating a mixed network system comprising directly communicate plans and plans having radio links to and from the base stations. In this type of a system the extra tackle is to make a decision when cluster shall use direct communication and when

conventional cellular radio links to communicate with each other. Here, in adding to cluster idea account we give new income to examine attainable scheme presentation when cluster message is integrated into a cellular network and especially into an interference limited system [11]. The results indicated that it is possible to improve system capacity with direct communication. Considering the mode selection procedure the results indicated that with small separation of cluster members the D2D operation mode can be selected for the cluster by default and reach the optimum system performance. When the separation is relatively large the cluster members are subject to increased interference from other users in the system and the gain from the short path loss compared to cellular mode is diminished.

3.2 FUZZY IDENTITY-BASED ENCRYPTION (FIBE) SCHEME

Fuzzy identity-based encryption (FIBE) is a good candidate for resolving this problem. However, existing FIBE schemes suffer from the following disadvantages: rely on random oracle models, merely secure in selective-ID model, long public parameters, and loose security reduction. In this process we propose a new FIBE scheme. Our scheme is secure in the full model without random oracles, and at the same time has a tight security reduction and short public parameters. This means that our scheme is quite suitable for secure transmitting data in IOT [12]. In addition, our scheme has the advantage of tight security reduction. Thus in contrast to previous FIBE schemes with loose security reduction, our scheme needs not to enlarge the keys size and cipher text sizes to obtain the same security level. Our scheme also enjoys the advantage of constant size of public parameters. All of these indicate that our FIBE scheme is more efficient that previous schemes, and hence is more suitable for secure IoT communications.

3.3 ENHANCED AUTHENTICATION PROTOCOL

To ensure system control security, the authenticity of the information source must be confirmed firstly. Although academic fields have already proposed some authentication mechanisms, there are not any mature authentication models which fully meet the IoT environment requirements [13]. It analyzes the pros and cons of some existing authentication mechanisms, proposes an enhanced bi-direction authentication mechanism for IoT control system, and discusses the proposed mechanism in detail, including the improvements measures, the authentication process and the authentication model. Finally, this paper presents the security analysis of the enhanced authentication model.

3.4 RSA ALGORITHM

Two-method proof defense format for the Internet of property (IoT) bottom on obtainable Internet principles, specially the Datagram convey coating safety (DTLS) process By relying on an documented usual, obtainable implementations, business technique and safety communications can be reuse, which enables easy security uptake [14]. Our proposed security scheme is therefore based on RSA, the most widely used public key cryptography algorithm. It is intended to job more than average announcement tons that offer UDP/IPv6 network for Low power Wireless Personal Area Networks (6LoWPANs). Our implementation of DTLS is presented in the context of system architecture and the scheme's feasibility (low overheads and high interoperability) is further demonstrated through extensive evaluation on a hardware platform suitable for the Internet of Things

3.5 AGGREGATED-PROOF BASED HIERARCHICAL AUTHENTICATION SCHEME (APHA)

An obtainable U2IoT supermarket (i.e., unit IoT and ubiquitous IoT), to denote an collective-proof base hierarchical validation drawing (APHA) intended for

the covered network. Concretely, 1) the aggregate-proofs are recognized for manifold target to attain back and onward nameless data broadcast; 2) the directed path descriptors, homomorphism functions, and Chebyshev disordered map are together practical for joint authentication; 3) different entrée authorities are assigned to achieve hierarchical access control. in the meantime, the BAN logic official psychoanalysis is perform to show that the future APHA has no clear safety defect, and it is potentially available for the U2IoT architecture and other IoT applications [15]. In the APHA, two sub-protocols are respectively designed for the unit IoT and ubiquitous IoT to provide bottom- up security protection. The proposed scheme realizes data confidentiality and data integrity by the directed path descriptor and homomorphism based Chebyshev chaotic maps, establishes trust relationships via the lightweight mechanisms, and applies dynamically hashed values to achieve session freshness. It indicates that the APHA is suitable for the U2IoT architecture.

3.6 SECRET SHARING SCHEME

A story continuous authentication follows for the Internet of belongings base on clandestine distribution system. This procedure provide secure and efficient authentication for frequent communication transmissions in short session time intervals. The procedure introduce a work of fiction employ of clandestine distribution system, that is, the clandestine is second-hand as an authenticator and the share are used as authenticator tokens [16]. Each token is an outcome of a function of time that binds the secret share to a specific point in time during the session such that the share can only be revealed in that specific time. The share can be linked back to the secret and, hence, the message source can be authenticated. Security evaluation of the protocol shows that it fulfills the stated security requirements and addresses the listed attacks. Performance evaluation of the protocol shows that it is lightweight in terms of computation and communication costs, thus addressing the resource-constrained IoT endpoints.

3.7 MAXIMIZATION LIKELIHOOD ALGORITHM

With the fast growth of the Internet of gear (IoT), edifice IoT system with tall quality of service (QoS) has become an urgent requirement in both academia and production. In the measures of house IoT system, QoS-aware examine variety is an significant unease, which require the ranking of a set of functionally similar services according to their QoS values. Utmost probability (AML) estimator has the best presentation for small time example wideband basis manner opinion. But for a long time, the heavy computational load of maximizing the multivariate, highly non-linear likelihood function prevented it from popular use. Using this algorithm improve the security process in IOT techniques.

3.8 COMPARATIVE STUDY OF DIFFERENT ALGORITHMS

Table 1

Name of the Algorithm	Merits	Demerits	Focus Area
Clustering Based D2D Group Communication Method [10]	1 It reduces the transmission delay 2. Use of cluster overcomes the problem of node failure problem	1. If one node fails it can lead to whole communication failure 2. Less feasible process 3. Less reliability	Direct communication between two devices using cluster
Fuzzy Identity-Based Encryption (FIBE) Scheme [11]	1. Secure in selective-ID model. 2.It provide high security process 3. High efficient process	1.Need to enlarge the key size for security purpose 2.Large error tolerance 3. Diffie–Hellman exponent problems	Fuzzy identity-based encryption to provide security in IOT environment
Enhanced Authentication	1. Large feasible security		It enhances the working of

Protocol [12]	2. Large authentication process 3.Effective process	1. Higher computing and Large storage capacity 2.Replication of each devices can lead to cost problem	two way communication protocol which solve the old issues
RSA Algorithm [13]	1.Provides end to end security 2.Data updating mechanism and security involved to tackle attacks like Meet in middle	1.Generating key by using RSA is heavy task 2. Dynamic update can handle key protection against eavesdropping	A standard based security architecture with two-way authentication for the IoT.
Aggregated-Proof Based Hierarchical Authentication Scheme (APHA) [14]	1.Gives Proof of authentication for devices 2. To achieve hierarchical access control 3.High security protection process	1.Attacker can overwhelm such a server by flooding it with connection requests 2. It severe security challenges, and there are potential vulnerabilities due to the complicated networks	Authentication protocols are popular to address security and privacy issues in the IoT, and should be designed considering the things' heterogeneity and hierarchy.
Secret Sharing Scheme [15]	1. provides secure and efficient authentication 2. for frequent message transmissions in short session time intervals	1. Problem can be raised when we are using for the multi factor or multilayer 2. Ineffective process	A novel continuous authentication protocol for the Internet of Things based on secret sharing scheme
Maximization likelihood algorithm	1. Improve security process 2. Reduce non linear problem 3.Highly effective process and low cost	----	The IoT gateway has better computational performance and battery power than the IoT device, so employing a well-known security algorithm is possible

IV. CONCLUSION

"Things" that are connected to each other with the help of internet faces various security issues, authentication issues, data integrity, accesses policies and so on. Integration of cloud computing and the Internet of Things represents the next great leap forward in the future Internet. Users are getting involved in IOT paradigm which increases the User to User, User to Machine, and Machine to Machine interactions. Moreover, Cloud platforms need to be enhanced to support the rapid creation of applications, by providing domain specific programming tools and environments and seamless execution of applications, harnessing capabilities of multiple dynamic and heterogeneous resources, to meet QoS requirements of diverse users. To this purpose, it is observe that various security measures have been done for securing devices, secure routing, and clustering concept for efficiency in communication. In this concept we have surveyed the aspects of the IoT with emphasis on what is being done related to secure and efficient communication and what are the issues that require further research. Future work will be focus on how devices can be identified to provide required quality of service based on their working capabilities and performance regarding their storage and transmitting capabilities with respect to secure transmission.

V. REFERENCES

[1]. Prof. Anurag Shukla, Sarsij Tripathi "A Survey on Next generation Computing IoT Issues and Challenges" International Journal of Pure and Applied Mathematics, Volume 118 No. 9 2018, 45-64.

[2]. R. Shantha Mary Joshitta, L. Arockiam "Security in IoT Environment: A Survey" Journal of Information Technology & Mechanical Engineering - IJITME, Vol.2 Issue. 7, July- 2016, pg. 1-8

[3]. Marie-Aurélie Nef, Leonidas Perlepes, Sophia, and Panayotis K. Kikiras "Enabling QoS in the Internet of Things" CTRQ 2012: The Fifth International Conference on Communication Theory, Reliability, and Quality of Service.

[4]. Ravi C Bhaddurgatte, and Vijaya Kumar BP, SMIEEE "A Review: QoS Architecture and Implementations in IoT Environment" Research & Reviews: Journal of Engineering and Technology, ISSN: 2319-9873

[5]. Massimo Villari, Adnan Al-Anbuky, Antonio Celesti, Klaus Moessner et al presents "Leveraging the Internet of Things: Integration of Sensors and Cloud Computing Systems" Volume: 12 issue: 7, 2016

[6]. Diego Mendez, Ioannis Papapanagiotou, Baijian Yang "Internet of Things: Survey on Security and Privacy" Information Security Journal, Submitted on 6 Jul 2017 (v1), last revised 10 Jul 2017 this version, v2.

[7]. Carla Mouradian, Diala Naboulsi, Sami Yangui, Roch H. Glitho, Monique J. Morrow, and Paul A. Polakos "A Comprehensive Survey on Fog Computing: State-of-the-art and Research Challenges" IEEE Communications Surveys & Tutorials Volume: 20, Issue: 1, Firstquarter 2018

[8]. Hourieh KHODKARI, Saied Ghazi MAGHREBI "Necessity of the integration Internet of Things and cloud services with quality of service assurance approach" Vol. 85, 2016, p. 434 - 445

[9]. Gonçalo Marques, Nuno Garcia, Nuno Pombo "A Survey on IoT: Architectures, Elements, Applications, QoS, Platforms and Security concepts" Advances in Mobile Cloud Computing and Big Data in the 5G Era pp 115-130

[10]. M.Mullaiarasu , Dr S.Veni "Comparing and Analysis of Routing protocol in QoS of IoT" International Journal of Innovations & Advancement in Computer Science, IJIACS, ISSN 2347 – 8616, Volume 7, Issue 3, March 2018

[11]. Timo Koskela, Sami Hakola, Tao Chenand Janne Lehtomak "Clustering Concept using Device-to-Device Communication in Cellular System"

[12]. YANG Jin-cui, PANG Hao, ZHANG Xin "Enhanced mutual authentication model of IoT"

[13]. Thomas Kothmayr, Corinna Schmitt, Wen Hu, Michael Burning and Georg Carle" DTLS based security and two-way authentication for the Internet of Thing" Ad Hoc Networks, 2013 Zitiert von: 47 - Ähnliche Artikel - Alle 6 Versionen

[14]. Huansheng Ning, Hong Liu, Laurence T. Yang, "Aggregated-Proof Based Hierarchical Authentication Scheme for the Internet of Things", IEEE transactions on parallel and distributed systems, VOL. 26, NO. 3, pp. 657-667, MARCH 2015.

[15]. Yijun Mao, Jin Li, Min-Rong Chen, Jianan Liu, Congge Xie, Yiju Zhan"Fully Secure Fuzzy Identity-Based Encryption for Secure IoT Communications" Computer Standards & Interfaces, 25 June 2015

[16]. Omaimah Omar Bamasag, Kamal Youcef-Toum "Towards Continuous Authentication in Internet of Things Based on Secret Sharing Scheme".