International Journal of Engineering Applied Sciences and Technology, 2019
Vol. 4, Issue 3, ISSN No. 2455-2143, Pages 164-166
Published Online July 2019 in IJEAST (http://www.ijeast.com)

INTEGRATION OF IOT AND CLOUD COMPUTING SECURITY CHALLENGES

S.Brintha Rajakumari,
Associate Professor, Dept. of CS,
BIHER, Chennai

V.Janani
MPhil Scholar,
Department of CS,
BIHER, Chennai

Abstract- **The recent emergence of Internet of Things has refashioned user's perception over the internet and the real world by means of omnipresent spatially distributed devices with fixed identification and sensing capabilities. Integration of distributed and dynamic IoT with the innovative deployed architecture of cloud computing, molding the latter as the intermediate layer between sensor and application. This paper focus is on the integration concepts and possibility of security challenges of ClouT (Cloud of Things).**

Keywords: **Internet of Things, ClouT, Security, Heterogeneity, Reliability, Integrity, Inter-operability, and Monitoring.**

I. INTRODUCTION

Past few decades of human life is filled with wireless communication across the world. The recent attempts of innovations are completely on developing resources which should be shared and used among networks in large scale. Cloud computing provides application delivered as a service over internet and these services are delivered on-demand to the users. It acts as a resource pool with rapid elasticity or expansion when needs increase. Miorandi et al (2012) described swarming with bunch of security risk like data privacy, excluding vulnerability, relentless service, data adequacy. Shrewd customers raise tough questions, before committing to cloud vendors. In Information of Things (IoT) extended internet technologies are used to interconnect smart objects by Jon Brodkin. (2008). When interconnection of smart devices are considered there exist immense communication between people to device (or) device to people (or) device to device. The prime behavior of IoT are collecting and sending information across objects and receiving and acting on such information. IoT should provide heterogeneous communication, ensure privacy protection, Bootstrapped security domain. In this paper, the flow begins with overview of cloud computing, IoT and kernels at security issues faced when integrating these two massive system.

II. CLOUD COMPUTING

Cloud computing furnish application as a service over internet. A person or organization pay recursively to access a software and its function remotely as a web based service. This software delivery method is known as Software as a Service (SaaS). Platform as a Service (PaaS): Development platforms such as operating system software, a database, web development tools and web service software were provided to customer, whose control is limited to configure and manage these cloud hosted application presented by Daniele (2012). Organization or user pay only for computing resources (server, storage, networking delivery) they use, this featured service is known as Infrastructure as service (IaaS). These services are provided to customers as they are scalable, low in cost, secure convenient, immensely available, accepts rapid elasticity and expansion described by Nandhini (2016).

Michael et al (2010), has mentioned ten obstacles and opportunity to overcome those obstacles. Service availability to customer in single cloud, data lock-in for every individual customers, data confidentiality and audibility, storage expandability, any customer delinquency can affect reputation of other users, are some risk mentioned in the article. Dimitrios et al (2012) have given a comprehensive review on security risk and requirements to overcome those risk in application, virtual and physical level. Interception, data interruption, privacy breach, impersonalize, session hijacking, modification of data at rest and in transit, are service attacks at software level. Programming flaws, software interruption, defacement, connection flooding, disrupting communications are service attacks possible at platform and infrastructure level.

III. INTERNET OF THINGS

An internet protocol shuttles its service to a diverse network through IoT gateway to a smart sensor like, smart cities, Wi-Fi routers, industries and robotics. The smart object or a thing should possess a set of physical features unique identifier, computing capabilities, should sense physical phenomena.

International Journal of Engineering Applied Sciences and Technology, 2019
Vol. 4, Issue 3, ISSN No. 2455-2143, Pages 164-166
Published Online July 2019 in IJEAST (http://www.ijeast.com)

When focusing on IoT sensors, it conquer the word 'Things' in IoT. Consist of energy module, RF module (manage signals), sensing module (manage sensing through active and passive sensing device). It fills the cleft between virtual and physical world with set of characteristics such as sensing, actuation, embedded information processing, RFID, homogeneous protocol ecosystem, unified interface for application.

Mirza et al (2017) presented the platform of IoT expanded as any industries, smart homes, medical devices the security requirement is focused. As devices are interconnected data authentication, access control, client privacy, and resilience to attacks are the challenges to be considered. Sujithra et al (2016) described security layered architecture is deployed. The local and national application security system is invoked. In the former, concealed messages are transferred between nodes, and the latter is secured by authentication firewall, selective disclosure as it deal with small scale communication. Network layer has wired and wireless levels of security. The perception layers are the actual sensors mostly hardware based layers and its security issues: device should be tamper proof, avoid man in middle attack, bootstrapping and authenticated access needed.

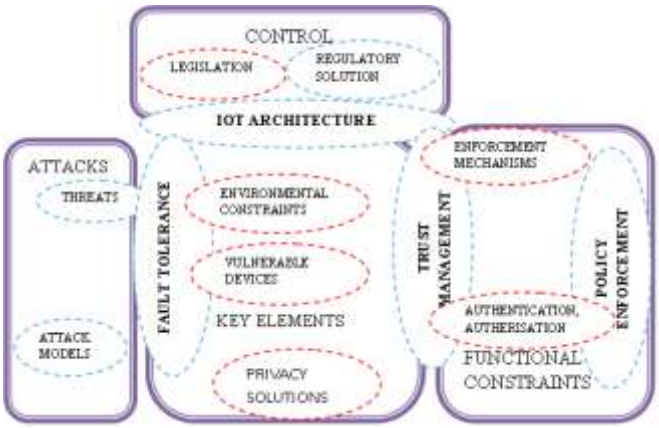

Fig. 1: IoT security challenges and solutions

IV. CLOUT-SECURITY CHALLENGES

Cloud computing and Internet of Things the contemporary massive subject in IT environment. The concept of integrating cloud and IoT brings common advantages leading to convenient and cost effective communication, information sharing and reusing of application software. Cloud happen to be an intermediate layer between application and object or a sensor, hence known as cloud of things (ClouT). In ClouT third parties like sensors look-in data aggregation, sharing resources, data integration, tracking and monitoring. Yu Liu et al (2015) have described upgraded ClouT services like sensing, actuation, sensor event, database, Ethernet, identity and policy management and video surveillance as a service. The ClouT provide anything and everything over internet storage, service, and application energy efficiency and so on. The concept of mobile cloud computing exist by fusing mobile computing and cloud computing to make mobility of cloud based software, platform and infrastructure presented by Christos(2016). The smart sensor or object can be ambulatory and so cloud is merged together for efficacious upshot. The IoT security challenges and solutions is in figure 1.

Everton et al (2016) and Jatinderet al (2015) presented he cloud and IoT architecture are not homogeneous, hence integration of these two can be made at different levels such as software, platform, middleware and framework. The core feature of IoT is sensor or smart object, these sensed information are made available for the software components running over the cloud. The on-demand feature of cloud annex to browser and mobile device to integrate, manage and monitor IoT devices at real-time described by Jun Zhou et al (2017). Listed below security challenges of ClouT based on heterogeneity, reliability, integrity, interoperability, and monitoring.

Heterogeneity: Considering cloud architecture classification as public, private, and hybrid cloud, huge data placed on public cloud requires various preventive techniques, as different users access those data for processing. In private cloud, data encryption is limited to trustworthy IoT objects. 'Things' are heterogeneous, which takes advantage of protecting, sharing, generating, consuming data of various level of sensitivity. Privacy concern is important in such sharing, cloud detach such flaw by aggregating the data to be used on-demand with set of privacy for the range of 'things'. Scaling is factual provocation to cloud based architecture and leads to availability issues, in such cases IoT aid in queuing system, customizing architecture, etc.

Reliability: A set of introverted IoT users add or remove all forwarding layer to reduce number of intermediate transmitter between them to slow down the performance of cloud. IoT sensor share data in cloud which may be relevant to number of application, so each sensor maintain an encryption standard, or each call it revokes all keys and updates a new set of key for applications and provide to other smart users on-demand (cloud).

Integrity: Trusted platform module offer promise by providing strong guarantees. In semi-trusted module, cloud makes a trust worthy gateway with the 'things' but try its best to access secret information of the sensors. Malicious model, completely hacks the information of the sensor. To overcome this three main privacy policy should be considered: input privacy, output privacy and function privacy.

Interoperability: secured communication has two main characteristics, maintain secrecy to prevent data leakage and from eavesdropping, and other is maintain data integrity. Node compromise attack: ClouT has a vast set of node to communicate with; any such smart object may be malicious one to hack secret information of all other nodes. Each node can maintain separate privacy key for intercommunication.

Monitoring: Identity privacy is the primary challenge of ClouT, where the unique identity of user to be secured and, on duplication by fraudulantation should be taken by authorities. Location privacy is an unfavorable issue of IoT as the smart users adopt to mobility, malicious hackers can easily access occasionally visited places of target nodes.

V. CONCLUSION

The real-time use of cloud to the distributed smart users made more feasible and flexible in IT environment. The integrated ClouT phenomenon ensures data privacy and integrity, secure communication, detect vulnerability, predict and pre-empt security issues, manage device update, authorize and authenticate devices. Before advent of ClouT, environment is narrowed and crisper. ClouT provides elaborated view of the network, makes a fill-in gateway between virtual world and real world. ClouT is a tropical topic in recent trends, this article helps to furnish my succeeding scrutiny on security issues in cloud computing.

VI. REFERENCES

[1] Miorandi, D, Sicari, S, De Pellegrini, F, & Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges, Ad Hoc Networks, vol 10 (7).

[2] Jon Brodkin. (2008). Gartner: Seven cloud-computing security risks", Network world.

[3] Daniele Miorandi, Sabrina Sicari, Francesco De Pellegrini, Imrich Chlamtac. (2012). Internet of things: Vision, applications and research challenges, Ad Hoc Networks, 10, (pp.1497 - 1516)

[4] T. Nandhini, M. Sajitha Parveen, B. Kalpana. (2016). A Survey on Internet of Things Architecture", World Scientific News 41,(pp.1 - 315).

[5] Michael Armbrust, Armando Fox, Rean Griffith,"A View of Cloud Compting", Communication of ACM, vol. 53, April 2010.

[6] Dimitrios Zissis, Dimitrios Lekkas. (2012). Addressing Cloud Computing security issues, Future generation computer system, 28, (pp.583 - 592).

[7] Mirza Abdur Razzaq, Muhammad Ali Qureshi. (2017). Security Issues in the Internet of Things (IoT): A Comprehensive Study, International Journal of Advanced Computer Science and Applications, vol. 8, No. 6.

[8] Ms. Sujithra, Dr. G. Padmavathi. (2016). IOT Security Challenges and Issues – An Overview, World Scientific News 41, (pp.1 - 315).

[9] Yu Liu, Beibei Dong, Benzhen Guo, Jingjing Yang and Wei Peng. (2015). Combination of Cloud Computing and Internet of Things (IOT) in Medical Monitoring Systems, International Journal of Hybrid Information Technology, vol.8, No.1 , (pp.367 - 376).

[10] Christos Stergiou a, Kostas E. Psannis, Byung-Gyu Kimb, Brij Guptac. (2016). Secure integration of IoT and Cloud Computing, Future Generation Computer Systems.

[11] Everton Cavalcante, Jorge Pereira. (2016). On the interplay of Internet of Things and Cloud Computing: A systematic mapping study", Computer Communications 89–90, (pp.17 – 33).

[12] Jatinder Singh, Thomas Pasquier, Jean Bacon, Hajoon Ko, and David Eyers. (2015). Twenty security considerations or cloud-supported Internet of Things, Internet of Things Journal, IEEE.

[13] Jun Zhou, Zhenfu Cao, Xiaolei Dong, and Athanasios V. Vasilakos. (2017). Security and Privacy for Cloud-Based IoT: Challenges, Countermeasures, and Future Directions", IEEE Communications Magazine.