Impacts Of Cyber Security In Iot-Based Cloud Computing

Lataben J Gadhavi[1] ,
Madhuri V Vaghasia[2]

[1]Lecturer, Information Technology Department,
Government Polytechnic Gandhinagar ,
latagpg@gmail.com
[2]Assistant Professor, Department of Computer Engineering,
LDRP-Institute of Research and Technology, Gandhinagar.
madhuri.vaghasia03@gmail.com

Abstract:

Cloud computing contributes the elastic and extensible architecture in which resources and data are scattered at different regions and accessible from anywhere. Cloud computing indicates applications and services to implement on a distributed computing network by applying virtualized resources. Meanwhile, industries have rapidly adopted cloud computing technology for secure and effective accessibility, improvement of performance and cost reduction. Moreover, incorporation of cloud computing and internet of things (IoT) has been enhancing in last decade. Hence, this expeditious evolution in the cloud computing technology raised numerous security issues and challenges. IoT with cloud demands exclusive security aspects to overcome the traditional security challenges.Technological advancements like smart cities and IoT needs protected cloud infrastructure to deploy secure system. The conclusion of the research paper comprise a comprehensive survey of facilitating cloud-based architecture of IoT , security models and classification of cloud security with IoT. To blend security in cloud computing, technological challenges and significant research gaps will be considered to highlight future research directions. This chapter presents security and privacy challenges with IoT-based cloud systems.

Keywords – Cloud-based IoT Platform, Security issues, Security challenges in IoT.

1. Introduction of IoT-based Cloud Computing

Upcoming era will be totally on skill-based-technology like (IoT), Open-Artificial Intelligence(AI) and Deep Learning & Machine Learning(ML). IoT is one of the booming technologies which are playing a vital role in transforming from conventional systems to smart system in homes, offices, public sectors, supply chain management etc. The future of Smart Computing will be completely based on Internet of Things (IoT). IoT term sounds as a critical part of changing "Conventional Innovation" from house to workplaces to "Cutting edge Wherever Figuring". "Internet of Things" is found as a connecting network exclusively. Nowadays, the potency and flexibility of IoT has been distorted. It is not only limited to experts but these days it is also being utilized even by layman. From the place of ordinary client, IoT has established the underpinning of advancement of different items like savvy residing, e-wellbeing administrations, computerization and, surprisingly, brilliant training. Also, according to business perspective, Internet of Things with cloud is being utilized in the business council, fabricating, and smart transportation and even in agricultural business [1].

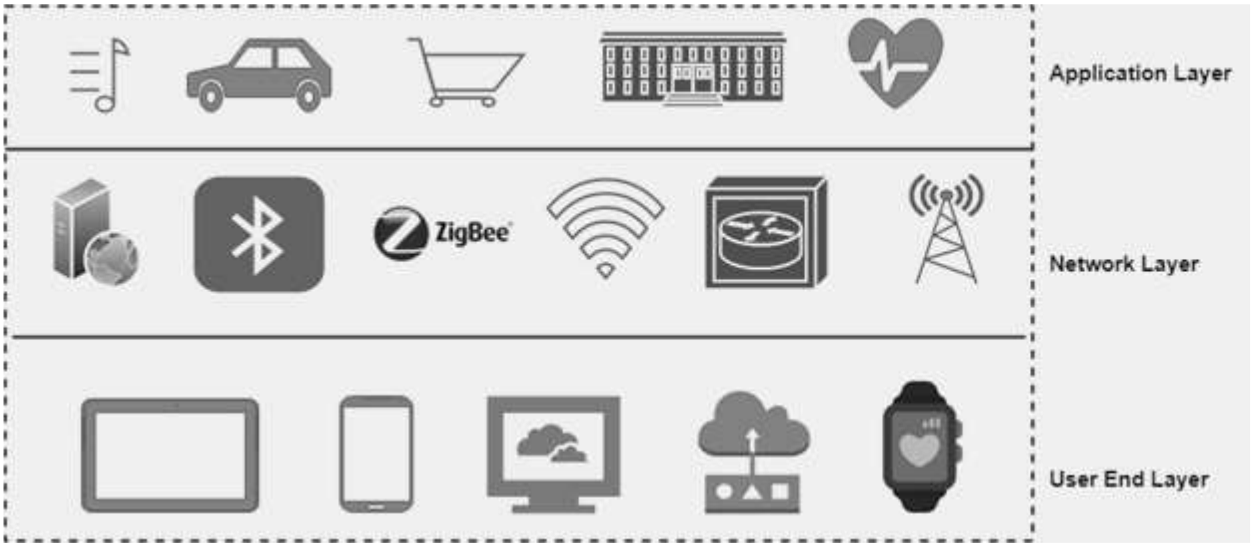

Figure-1 : Traditional Architecture of IOT[1]

In a one of the articles circulated that25 highly predicted best tendeliberate innovations for the year 2020 along with cloud based services predicted to grow by 20% in 2021. The cloud computing first applied in 1990s to refer to distributed computing platforms [2]. In 2006 AWS (Amazon Web Service) has introduced Elastic Compute Cloud (EC2)[3]. Similarly, Google has released beta version of Google App Engine in 2008 [4]. In 2008, NASA had launched Open Nebula which was earliest open source s/w used for deployment of hybrid and private clouds [5].Microsoft Azure was released in 2008 by Microsoft [6]. Other such examples are OpenStack, IBM smart cloud.

2. Issues and challenges for secure cloud infrastructure

There are four main levels that should be considered while planning and pertaining security in cloud IAAS, for data level, network, application, and host level. At each level all the components are should be considered while providing security to cloud infrastructure. As this technology is adaption is increasing beside the fame of cloud computing technology, issues of security are also increasing. Though cloud computing has so numerous compensation, it is also susceptible to different kinds of attacks. Attackers are finding many loop holes in the existing cloud services. The following are the problems in the various layers of cloud system.

2.1 Issues at Data level :

Data breaches, crypto jacking, Distributed Denial of service (DDos) data loss, data virtualization, data segregation, data integrity, data confidentiality and data availabilityare the major issues found at this level.

2.2 Issues at Application-level:

Major issues that come up at application level are related to availability, unauthorized access, authentication and access control, resource issues.

2.3 Issues at Network level :

Network level issues involve attacks on confidentiality, availability and integrity.

3. Characteristics of attacks based on Cloud IoT

Security is major concern expected by the end users. So, it is the responsibility of the service provider to solve it to maintain reliability and confidentiality. However in past few years so many organizations have been shifted there applications, data and business over the cloud platform. Due to that attackers have diverted their focus and they find it a new way of making cyber attacks. Figure 2 represents the components of cloud, vulnerabilities and attacks that can be the loopholes in the cloud based systems. Investors of cloud platforms are worrying the most during investment in cloud based services. This is happening because users' data is used by third party wanders without knowledge of user.

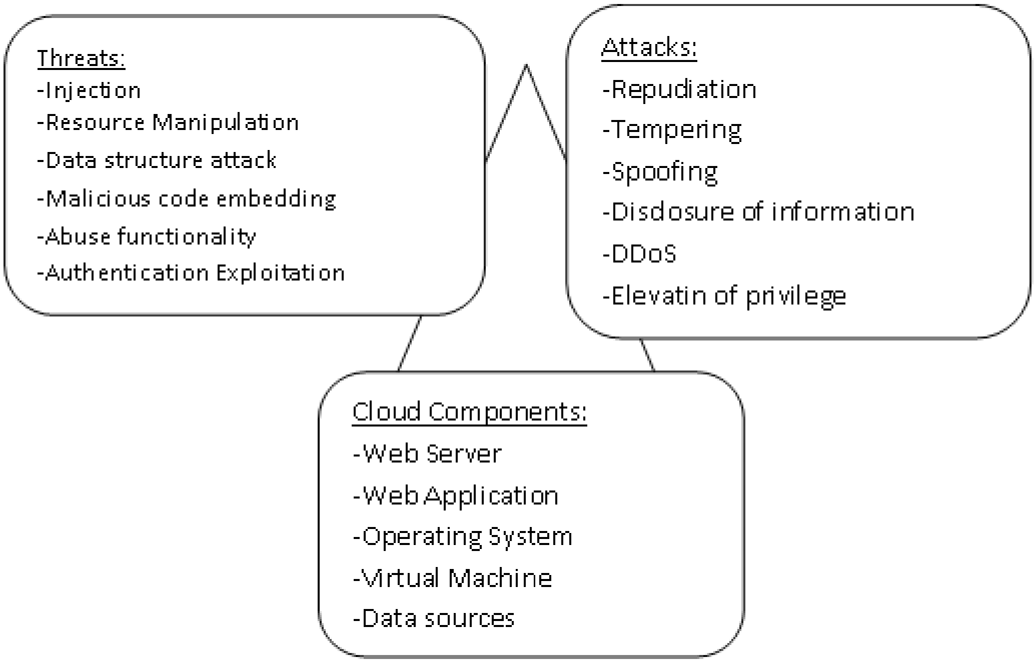

Figure-2: Threats, Attacks and Cloud Components on Cloud

Cloud platform in IoT is helping to collect, store and use data as a supporting platform. A centralized cloud server is provided along with computing resources which are available 24X7. Fog computing and cloud computing are suitable platforms to collect and transmit a huge data created by Internet of Things devices. Due to all these reasons data breaches are possible in this kind of environment. Following table gives the summarised information about the types of attacks [7,15].

Table-1 Summary of attacks based on Cloud IoT

IoT based Cloud attacks	**Explanation**
DOS attack	Attacking on network or computing device that make unreachable touser
Information Loss	Poor handling of data leads to data loss
Service or Account Hijacking	Aim to stole Information by the system attack
Malicious Insider	Malicious activity is done by the insider only
Insufficient diligence	Lack of cloud knowledge increases the risk of attack
Shared technology	The device is used on shared basis that leads to several types of attack
API technology	Attacks to depict APIs or software
Maltreatment and disreputable utilization of cloud system	Use of cloud system for immoral purpose

4. Impacts of cyber security in cloud and IoT

Quite possibly of the biggest concern in the current cyber security era is the IoT. As this is one of the leading technology, it comes with various challenges and issues[8]. So, it is advisable to work under the guidance of cyber security experts from the beginning of the implementation processs[23-26].

By involving the security experts from other specialist organization, assures that the products are secure before going to a scale in the market[12-13]. Organizations can also teach their customers about possible threats and the steps to secure the system under the advice of security experts.

This is also true that IoT is not fully developed till, they may or may not come with all security concerns. Some the IoT devices are very low powered so that they may not connect with other devices. All these loopholes leads to data breaches and attacks. One side IoT offers so many advantages to public sectors, healthcare application and helps to grow the business. Its interconnected nature also increases the risks of cyber security repudiation[14,19-22].

As we keep on adding devices in IoT network, the better the opportunity for attackers to access data and use it for malicious purpose. A weak network may also be the threat for the national security. Impacts of cyber security in IoT and Cloud Computing is discussed in the following section[9].

- **Rise in Connectivity:** Day by day more number of devices are joining the IoT network. Increase in number of devices can become vulnerable for the attackers.
- **Importance of Data:** Data has the super power in today’s era and hence plays a vital role. And this is the reason that attackers are targeting these data.
- **More ways to attack:** As new devices are joining the network connection, it also increasing the ways to attack the network.
- **Atomization:** IoT offers fully automated and remotely operated services to the users. These services need individual security methods also that is lacking currently.
- **In-built securityfeatures:** Currently IoT based appliances lack in-built security features. Third parties are providing security to the IoT appliances now a days. They are mostly used for specified devices or protecting whole network from unauthorized access.

Different ways to handle the security issues are:

- Correct maintenance of data collected from various IoT devices as per the lifecycle of data and its characteristics that reduces the risk level at certain point.
- Access privileges must be given to users to access the data to make it more secure.
- Central monitoring interface can also help to detect unauthenticated access and malicious activity.
- Specific purpose firmware and software usage to find out loopholes and make it correct on timely basis.
- Timely data backup with up gradation in software can also prevent the IoT system form potential cyber-attacks.

5. Classification of issues

Major security issues and challenges in cloud infrastructure are recognized and considered in the following division. Somewhat wrong happens to digital resource resided on the cloud platform. These resource can be a software, platform, infrastructure, data, business reputation[11].

Security issues are classified into four categories: (i) issues with security of data, (ii) issues of network and security service, (iii) security of application, and (iv) security issues of people-related. This classification has been done based on the latest attacks identified on cloud based platforms. A short summarization of each type is given following section and a summary is given in the figure-3[1],[10,16-18].

Issues with security of data: Covers the data security issues associated to data access, breaches, backup, integrity, storage and location.

Issues of network and security service: Includes insiders' risk, virtualization, account hijacking, multitenancy issues.

Issue of application security: This issue includes cloud based software applications like malicious insiders' development, User Interface issues, malware injection etc.

People-related security issues: These issues include human resource, legal issues like copyrights, compliance issues and trust management issues.

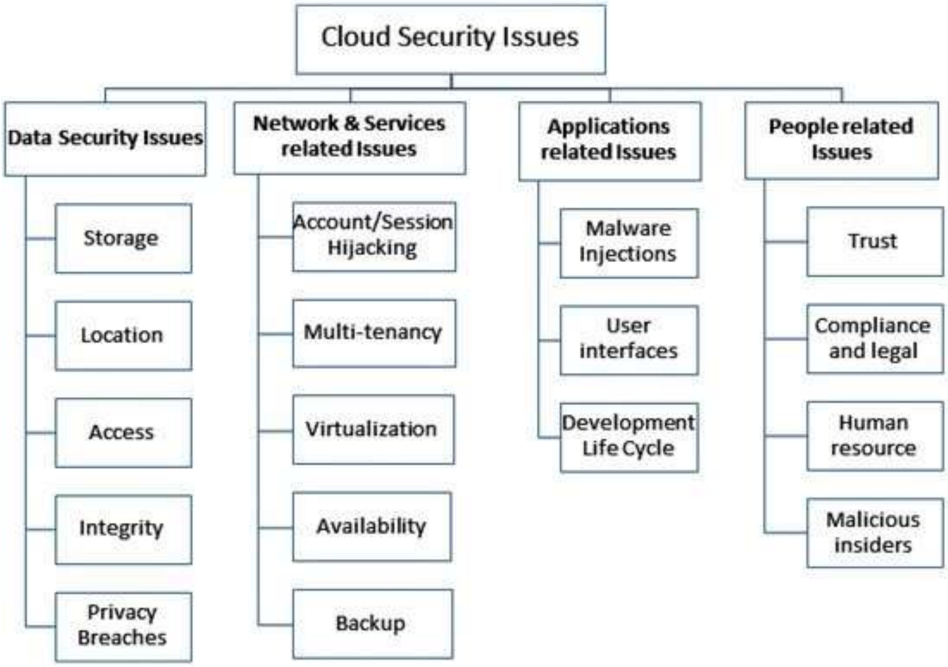

Figure-3: Classification of security issues in IoT system [1]

6. Future directions

The paper includes issues of cloud security with IoT applications. In the expectations work the authors may include the current cloud platforms security issues and also gives the logical solutions to overcome these issues to improvise the cloud security. Researchers can also learn the most current cloud security model and discuss its analysis, review current security issues and challenges of cloud computing platform like encryption, authentication, VM security and sharing of resources.

Along with the technological advancements like IoT, Fog computing, 4G and 5G applications, smart cities applications need more capable data storage and processing environment. All above technologies require an efficient cloud infrastructure and data security to protect it from all kind of attacks.

Blockchain based log security in cloud platform is also a future direction of research that offers the security to cloud user logs by block chain system to make the cloud system breach less and increases users' trust for cloud platforms.

7. Conclusions

Last one decade remains full of technological advancement but it is also a revolutionary period for the software industries, organizations and for the attackers. High speed internet applications based on cloud are the gifts to the society that brought new threats and challenges in terms of cloud platform security. This research includes the common cloud platform architecture and its exploitation models and ordinary possible attacks. Security issues and challenges are also classified in four different categories. Also given various challenges that require to be mentioned in the upcoming research soon.

References

1. Ahmad, W.; Rasool, A.; Javed, A.R.; Baker, T.; Jalil, Z. Cyber Security in IoT-Based Cloud Computing: A Comprehensive Survey. Electronics 2022, 11, 16.
2. Mohiyuddin, A.; Javed, A.R.; Chakraborty, C.; Rizwan, M.; Shabbir, M.; Nebhen, J. Secure Cloud Storage for Medical IoT Data using Adaptive Neuro-Fuzzy Inference System. Int. J. Fuzzy Syst. 2021, 1–13.
3. Ikram, A.A.; Javed, A.R.; Rizwan, M.; Abid, R.; Crichigno, J.; Srivastava, G. Mobile Cloud Computing Framework for Securing Data. In Proceedings of the 2021 44th International Conference on Telecommunications and Signal Processing (TSP), Brno, Czech Republic, 26–28 July 2021; pp. 309–315.
4. Larsson, L.; Henriksson, D.; Elmroth, E. Scheduling and monitoring of internally structured services in cloud federations. In Proceedings of the 2011 IEEE Symposium on Computers and Communications (ISCC), Kerkyra, Greece, 28 June–1 July 2011; pp. 173–178.
5. Al-Khafajiy, M.; Baker, T.; Asim, M.; Guo, Z.; Ranjan, R.; Longo, A.; Puthal, D.; Taylor, M. COMITMENT: A fog computing trust management approach. J. Parallel Distrib. Comput. 2020, 137, 1–16.
6. Rao, P.M.; Saraswathi, P. Evolving cloud security technologies for social networks. In Security in IoT Social Networks; Elsevier: Amsterdam, The Netherlands, 2021; pp. 179–203
7. Gadhavi, Lata, Bhavsar, Madhuri. Adaptive cloud resource management through workload prediction. Energy Systems. pp.1-23(2019).
8. Alghofaili Y, Albattah A, Alrajeh N, Rassam MA, Al-rimy BAS. Secure Cloud Infrastructure: A Survey on Issues, Current Solutions, and Open Challenges. Applied Sciences. 2021; 11(19):9005.
9. Lata Gadhavi, Madhuri Bhavsar, Proposed methodology to strengthen the performance of adaptive cloud using efficient resource provisioning, Advances in Intelligent systems and Computing, Proceeding of IEMIS-2018, Springer (2018), pp. 217-226.
10. Lata Gadhavi, Madhuri Bhavsar, Prediction based efficient resource provisioning and its impact on QoS parameters in the cloud environment, International Journal of Electrical and Computer Engineering (IJECE), Volume 8, No 6,(2018),5359-5370.
11. Yu Y, Hu L, Chu J. A Secure Authentication and Key Agreement Scheme for IoT-Based Cloud Computing Environment. Symmetry. 2020; 12(1):150.
12. Anuradha, M.; Jayasankar, T.; Prakash, N.; Sikkandar, M.Y.; Hemalakshmi, G.; Bharatiraja, C.; Britto, A.S.F. IoT enabled

cancer prediction system to enhance the authentication and security using cloud computing. Microprocess. Microsyst. 2021, 80, 103301.

13. Lata Gadhavi, Madhuri Bhavsar, Efficient and Dynamic Resource Provisioning Strategy for Data Processing Using Cloud Computing, International Review on Computers and Software (I.RE.CO.S.), Vol. 11, 691-700(2016).
14. Dang, L.M.; Piran, M.; Han, D.; Min, K.; Moon, H. A Survey on Internet of Things and Cloud Computing for Healthcare. Electronics 2019, 8, 768.
15. Renuka, K.; Kumar, S.; Kumari, S.; Chen, C.M. Cryptanalysis and Improvement of a Privacy-Preserving Three-Factor Authentication Protocol for Wireless Sensor Networks. Sensors 2019, 19, 4625.
16. Anand Nayar, Lata Gadhavi, Noor Zaman, Machine learning in healthcare: review, opportunities and challenges, Science Direct(Elsevier),2021, ISBN 978-0-12-821229- 5,pp.23-45
17. Gadhavi, L.J., Bhavsar, M.D. (2020). Efficient Resource Provisioning Through Workload Prediction in the Cloud System. In: Zhang, YD., Mandal, J., So-In, C., Thakur, N. (eds) Smart Trends in Computing and Communications. Smart Innovation, Systems and Technologies, vol 165. Springer, Singapore.
18. Chenghao Li, Steven C. H. Hoi , Peilin Zhao, Jianling Sun, Online ARIMA Algorithms for Time Series Prediction, Proceedings of the Thirtieth AAAI Conference on Artificial Intelligence (AAAI-16)(2016).
19. R.S. Shariffdeen, D.T.S.P. Munasinghe, H.S. Bhathiya, U.K.J.U. Bandara, and H.M.N. Dilum Bandara,Workload and Resource Aware Proactive Auto-Scaler for PaaS Cloud, IEEE 9th International Conference on Cloud Computing(2016).
20. Yi Han, Jeffrey Chan,Christopher Leckie, Analysing Virtual Machine Usage in Cloud Computing, IEEE Ninth World Congress on Services, pp.370-377(2013).
21. Yang Meng, Ruonan Rao, Xin Zhang, Pei Hong, CRUPA: A Container Resource Utilization Prediction Algorithm for Auto-Scaling Based on Time Series Analysis, pp 468-472, IEEE (2016).
22. R.S. Shariffdeen, D.T.S.P. Munasinghe, H.S. Bhathiya, D.K.J.U. Bandara, and H.M.N. Dilum Bandara, Adaptive Workload Prediction for Proactive Auto Scaling in PaaS Systems, IEEE(2016).
23. Rajkumar Buyya, Diana Barreto, Multi-cloud resource provisioning with Aneka: A unified and integrated utilisation of Microsoft Azure and Amazon EC2 instances, International

conference on computing and network communications (COCONET 15)(2015).

24. Michael Tighe, Michael Bauer, Topology and Application Aware Dynamic VM Management in the Cloud, J Grid Computing 15:273–294 (2017) .
25. M. Li, "Architecture design of IoT cloud platform for industrial monitoring," 2021 International Conference on Computer, Internet of Things and Control Engineering (CITCE), 2021, pp. 96-99
26. X. Zong, Y. Luan, H. Wang, and S. Li, “A multi-robot monitoring system based on digital twin,” Procedia Computer Science, vol. 183, pp. 94–99, 2021.