Security Challenges observed in IoT-Enabled Cloud Infrastructure: A Review

Ravi Jadhav[1] and Harshad Ithape[2]

[1]Senior Product Manager-Amazon, [2]Senior Software Engineer (DevOps)- Capital One, USA

Email Address- [1]ravjadha5@gmail.com, [2]harshad.ithape@gmail.com

Abstract:

This review work consists of the analysis based upon the challenges faced in the field of security which caused because of the devices that are enabled through IOT with cloud infrastructure. This paper is regarding the process of identification of the challenges occurred in the security apart from the risk which is involved while dealing with IOT devices in the environment of cloud and this includes privacy of data, controlling of access, process of authentication apart from the encryption. This paper is also regarding the examining different technologies which are generally used to sort out the challenges faced. The blockchain and edge computing is the technology that can be considered to solve some of the challenges. The paper also includes some of the recommendations to sort out the challenges in the field of security in terms of the cloud infrastructure which is IOT enabled. This paper also discusses the need for the procedure for standardization, to improve the awareness apart from the education while the development in the field of the security is need of an hour. Overall this work consists of providing a good resource for the researcher, academicians which are interested to work in field of security for IOT enabled cloud infrastructure.

Keywords: IOT, cloud computing, security challenges, privacy and data integrity.

1. Introduction

The internet of things is in you concert and because of which the device is and the sensors are able to communicate effectively with each other as well as with the cloud. When the integration of devices under IoT and infrastructure of the cloud has enabled continuous communication of the data as well as the processing. Because of this process it is found that there are different

challenges introduced in security [1]. The challenge in the security particularly for the case of IoT enabled infrastructure of the cloud is the new concern in these years. Therefore it is very important to understand the different challenges which are to be sorted out very efficiently and therefore the review process is carried out [2].

There are different research papers on the security challenges particularly for the IoT enabled cloud in first structure are carried out. Some of the research paper included different kind of review on the challenges faced in the security for the case of infrastructure of the cloud through IoT [3]. The researchers have analysed different issues in the security particularly the device is which are IoT enabled as well as with cloud infrastructure apart from integration of this both [4]. There are different security traits apart from security attacks since the device which are IoT enabled and with the cloud infrastructure. Some of the researcher have evaluated the existing solution which can be carried out for sorting out such kind of challenges [5].

The present work consist of the impact of emerging technology is particularly artificial intelligence and blockchain on cloud infrastructure as well as security of it when IoT is involved. This paper also consist of certain recommendations as well as future directions so that that can be enhanced in the security of this challenges. This work is considered to be a good resource for researcher as well as practitioner whose interest is in the field of cloud infrastructure security when IoT is involved.

2. IoT devices security challenges

There are different security challenges in the case of device is which are enabled with IoT and researchers or consistently working on the challenges as well as solutions. The researcher have carried out comprehensive review in the case of different challenges faced in the security when the cloud infrastructure is consists of IoT [6].

There are certain work carried out in the case of IoT privacy and the security apart from its challenges and solutions. It is very important to understand the different challenges faced in the security when internet of things is involved. Different solutions have also been addressed by some of the researcher. Is very important to analyse the risk which consisted in the case of devices which are IoT enabled. Some of the work also discusses related to the mitigation of certain risk in such cases [7].

A good review is also carried out on the security challenges which are particularly involved in the case of internet of things. There are different security threads as well as vulnerability for the case of internet of things device and therefore it is very important to analyse the risk to the privacy of the data apart from its confidentiality and integration of it [8].

The research work related to the privacy as well as security challenges in the case of smart home environment when studied in depth and analysis is performed. It was found that there are certain risk associated with the different internet of things enable devices when particularly used in smart homes. Risk also found in case of devices for the case of smart home devices, smart thermostats and different security cameras [9]. The potential privacy trades as well as security threads are found to be very important and need to be resolved [10].

The work was also carried out for the different security challenges in the case of IoT enabled cloud computing. Different security challenges have been analysed appropriately when the internet of things is involved in the cloud computing. Work was also carry doubt for the risk involved in the data breaching process, unauthorised access to the data apart from tempering process of the data [11]. The work also carried out of security of internet of things and the challenges involved in it. The different potential solutions have been discussed to resolve such kind of challenges.

3. Cloud infrastructure security challenges

The adoption of cloud computing has become a very fast process and nowadays it has become the focus of research. Cloud infrastructure has advantage including different range for the benefit to the organisation, this also include scalability apart from effectiveness in the cost. Since there are different benefits it has lead to the challenges in the security. Many organisations are moving towards cloud computing and its application it is a need of an hour to review comprehensively the security involved in cloud infrastructure.

From the research work it was observed that there are different security traits to the cloud in first structure and this involve cyber criminals, internal traits apart from occasional bleaching of the data. It was observed that the primary is security challenges included breaching of the data apart from unauthorised access as well as not secured API. It was ensured that the security and privacy related to the information which is very sensitive has to be stored in the cloud so that the customer as well as take holders can have the trust.

Some of the research work included the different risk in the security and in particular to the cloud virtualization. This also include vulnerability and unauthorised access to be machine which are virtual. The work also consist of the potential impact of these challenges in the security particularly on the cloud providers as well as the customers of the cloud provider.

The research work also consist of examining different challenges in the security when faced by public cloud providers apart from the customer of the providers. Different security risk have been identified and they are associated with the services of public cloud.

The research was carried out related to the security challenges for the case of different layers of the network in cloud computing. Different security thread serve in identified as well as the vulnerability which is associated when the cloud computing consists of many layers. The threads associated with the different layer particularly physical layer and network layer apart from application layer. Some of the security solutions as well as best practices have been identified so that the security risk can be resolved veryffectively.

The research work was carried out on clouds strike which is depending up on Chaos engineering for the case of security in cloud infrastructure. It was observed that the different concept of cloud engineering and application for the security of cloud infrastructure have been discussed.

Different issues related to the security, data privacy, loss in the data, denial of service attacks apart from malware attacks are discussed in depth. The discussion models carried out for the case of different trades related to the cloud infrastructure and its include insider threat apart from external attack as well as the issues in the regulatory compliance.

4. Internet of Things

The work was carried out so that the IoT devices particularly commercial purpose and industrial purpose are analyzed in terms of the security for the hardware as well as software. The detailed procedure has been identified so that the home automation can be smoothly run and a smart meter considered so that the security established [12].

The research work carried out to provide identification of the risk involved in the security particularly when IoT devices are involved. The security procedure when adopted in the work was related to the protocols of the communication. Some of the attacks on the on the IoT devices are also discussed, the reason behind it was discussed too [13].

It was observed that the security in IoT devices found to have the scope in almost four different dimensions. The scope of security consists of the tasks in terms of the sensors which are trusted, process of computing, process of privacy apart from the digital information. The new technology was discussed for the protection of IoT devices, the sensors and actuators played crucial role in the security [1].

Fig.1: Internet of Things (IoT)

The IoT components considered to be very cost effective and the method of communication based upon the wireless technology used so that the connection is possible. The safety issues are identified especially in terms of the cybercrimes apart from the attacks on the security. IoT devices are becoming targets very easily due to such vulnerability [14].

The work was carried out for the development of the srcipts that can have automation for the testign of security as per every four dimensions of the threats earlier identified by the authors. The test devices are put in the market so that the security of the devices can be tested effectively. It was proposed to give the star based system of the security [15].

From the research work it has been proposed that the protection for IoT based devices is essential and need to in conjunction with the solutions based upon the different network levels. This shall helpful for monitoring the activity of network so that the suspicious threats can be detected. The networking technology is very helpful to sort out the threats [16].

When the SDN gateway was used so that the monitoring related to the traffic possible particular to the IoT enabled devices the successful detection of the TCP engaging attacks observed. The ICMP flood engaging attacks are also blocked when the SDN gateway was used. The secure integration was possible in the IoT enabled devices [10].

The security manager as used in the work so that the determination of the type of risk in the security can be observed effectively. The work regarding the installation of different updates regarding the software, it was found that the authentication process can be strong when filtering the traffic. The design is very helpful for the protection against harm IoT devices [17].

The security landscape for the case of IoT is considered to be the trending research work when carried out in the proper direction. The enhancement is very necessary for the speed to counteract the possible threats. It was observed that consumers need to be aware and responsible for the different regulations given by government.

5. Industrial Internet of Things

Internet of things is considered as very booming field since it is related to the internet connection and the device using it. Therefore the infrastructure need to be supported such new devices so that the proper efficiency and flexibility is possible [18].

Industrial internet of things (IIoT) is considered to be a stage where the different sensors need to have interface on the connection of internet. This is very important to live good and feasible life. This technology is considered to be very fast and new and therefore much research work is needed in this regard [19].

The main objective of IIoT is considered to be achieving the efficiency which is high in operation, more production and the management should also be improved. The process of the customization should be improved apart from the monitoring different application can be very intelligent process so that the production of shops on the floor apart from the health of machines can be very extrapolative [20].

The new and innovative trends in the field of Industry 4.0 and IIoT gives the business models to the industry which are very new and noble. The experience to the user is very decent as the connection is very strong and the device in terms of IoT gives good response.

When the coupling process is carried out in the components of the industry then there are many benefits to the industry apart from the different challenges in the security of it. Industrial internet of things gives different challenges to the industry. The components found to have good life compared with the consumer internet of things [21].

Industrial automation and control system are found to be very different from the general digital network e.g. environment related of ICT. When the good connection is vey needed then the architecture with different zones have been used, this give the protection to the components of the system related to core control. When the technology of IoT was adopted and deployed then changes are made to the architecture [22].

The manufacturing process when depends upon the cloud then it has given many advantages to the industry. The process has enabled the access the resources of the manufacturing, the trusted platform is very important to have the transactions in terms of the users and service providers. The work consisted of the platform named BPIIoT based upon the industrial internet of things and technology of block chain [23].

A innovative concept was put forward for the environment of industry when the IIoT which was defined through software placed so that the network can become enough flexible. The IoT enabled devices can be managed properly and the platform for the exchange of information is available through the proposed concept [24].

Sine there are many number of sensors and the devices which IoT enabled the production of the big data can be observed. The processing of such big data is very much complex and the storage facility is very limited. The analytics related to the bog data is important for the provision of the intelligence of the level in case of customer and operation [25].

When the internet was used for the different devices of computing it was observed that he life of people get changed drastically. The communication became more reliable and trusted, therefore the industrial revolution is booming in these days [26].

Industrial internet of things found to be very new way of generation where the system of industry get connected. The earlier focus was on the health of the machine apart from the maintenance of machines. Now the focus of the industry is on the analyzing process of data related to the industry of production [27].

6. Internet of Medical Things

The health sector unit is also adopting internet of things very rapidly. The process of monitoring the signals of biomedical is possible since the use of smart sensors and the devices which are IoT enabled used in the sector. When this smart devices used in the sector of medical then the term called internet of medical things is coined particularly if the human intervention is minimum [28].

The monitoring of the patients is nowadays carried out remotely and even for the very complex diseases the IoT is playing a vital role. The diagnosis of the patients is effective and precise and this ultimately lead to the saving of a life. There are some challenges in the field of internet of medical things. Security is also playing a crucial role in this system [29].

The gap is identified between the doctor, patient and service providers in the healthcare system. Internet of things in this sector proved to be a bridging this gap through innovative system. The work became very smooth and precise when the IoT enabled devices and systems used [30].

The devices enabled through IoMT is majorly consists of AI which is used for monitor the health of patients consistently. There are many smart devices like robots and assistant which gives important services to the patients. The epidemic disease can also controlled and checked when such systems are involved and work efficiently [31].

The different challenges are faced in the internet of medical things, the issues related to the safety, secured connection and reliable system need to be fixed. The different practical applications related to the process of democratization in the case of devices used in the medical industry are to be checked [32].

It was observed that the scalability is major issue for the system assisted with the blockchain technology. Saturation was observed with the increasing number of patients under this technology. It was observed that every device is not possible to make SDN based technology. Therefore the important data gathering is the challenge in this field [33].

The different solutions in case of security using the algorithms that are cryptographic and lightweight have been studied. The reduction in the overhead was also studied, the proper detection system is needed for cooperating with the honeypots which are having very dynamic shadow [34].

The internet of medical things consists of the requirement of big data, very high speed and life of battery should be sufficient so that the connection can be reliable. When the IoMT introduced with 5G technology then the diagnosis and treatment of the patients is possible with ease [35].

It was observed that the security is not easy to inspect since there is increase in the use of mobile and the solution related to tele-medicine. The reason behind increase in the problem of healthcare is use of Bring Your Own Device system. The data used by patients and doctors became a target for the hackers or security attackers [36].

The security of the connected devices used in the medical has been the issue and therefore the new technology related to the agent driven was developed. The use of machine learning apart from the algorithms of regression used for detection of invasion in the network. The simulation of network from the hospital topology was carried out for performing experiments [37].

7. Internet of Things in Smart cities

The review work was carried out on the internet of things related to smart cities, in this work the different technologies related to communication so that the services for the people are also studied. The urban internet of things was studied in terms of the protocols and different architecture [38].

The overview was put forward in terms of the IoT involved in smart cities, the analytics of the big data also considered to be part of the system. The improvement in the infrastructure and the transportation services are possible due to use of IoT [39].

The city when connected with the advance infrastructure apart from ICT services then the smart city can become more advance with more intelligence involved in it. The modern technologies are also to be included so that the communication can be very strong through IoT [40].

The review work was carried out to check the real time monitor process of the infrastructure involved in the smart cities. The other technologies are also introduced in terms of the cloud computing and wireless communications to be used in the IoT enabled system of smart cities [41].

The federated smart city platform developed in the research work, the experimental program was carried out. Smart waste management system was experimentally tested. The use of IoT in this

technology found to be good for the peoples in smart city of Europe. The main thing involved is the middleware supporting semantic system of interoperability related to the resources [42].

There are many applications in smart cities which are possible due to Internet of things, the increased demand of people are also getting fulfilled. The energy demand increasing when IoT enabled applications are used, IoT enabled devices are in increasing due to such demand. The solutions need to be focused on proper utilization of energy [43].

The case study consists of the utilization of GreenIoT platform in city Uppasala of Sweden country. The concept of interoperability is considered to be important as IoT devices are scaling up. The notion related to interoperability and open data used in the case study [44].

The security issue in smart cities was studied and sensing scheme was proposed which called as RealAlert which was depending upon the secured policy and trust. The trustworthiness have been studied in case of data used in IoT and devices. The history of collection of data and reports studied thoroughly. It was observed that the trust in the proposed scheme can be accurately measured [45].

The modeling of heterogeneity was proposed in the study, the data streams related to IoT and challenges in it also studied. The project named as VITAL and this is a open source platform to be used in case of internet of things. The rapid development of the platform and application for smart cities evaluated [46].

The semantic framework was proposed so that proper integration is possible of IoT and techniques of machine learning when this is to be used in smart cities. The different case studies were evaluated for proper working of the framework. The approach was also studied so that scalability can be achieved, the platform work efficiently [47].

8. Cloud computing security

Cloud computing is a new technology and it was observed that the current technology and current computing technology is turning into solutions based on the utility. There are several benefits and this includes computing resources which are configurable, saving effectively and the flexible services [48].

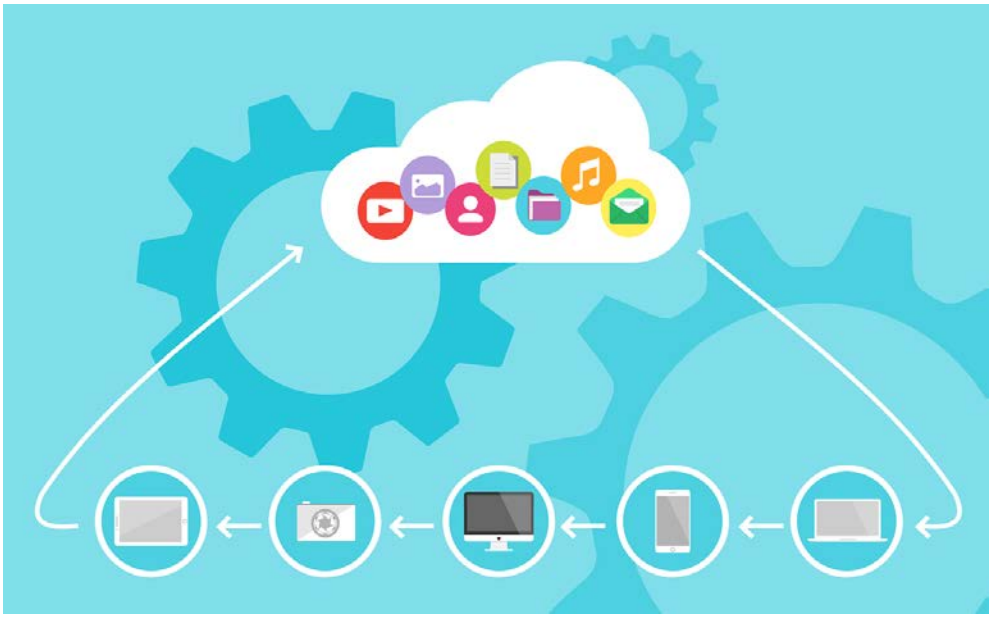

Fig.2: Cloud Computing

Cloud computing is considered to be the technology when adopted in the different models of business then much investment not needed and therefore organizations are adopting it rapidly. The adoption of the cloud models is considered to be important problem faced by an industry. Even the problem related to security is also need to be investigated properly.

There is also a technology known as edge computing comes under the cloud computing and it is responsible for process of data particularly sensitivity of time. This generally offers the ability of computing at the system's edge to the designers of applications and different services provider. The research work has to be related to current edge and its processing with the different methodology [49].

Table 1: Review on cloud computing security

Theme	Problem Identified	Solution Proposed	Reference
Cloud computing security problem	Model architecture, elasticity, multi-tenancy, stack with layer dependent	Based on cloud stakeholder perspective	[50]
Cloud computing security issues	Trust in third party	Cryptography, public key infrastructure in conjunction with SSO and LDAP	[51]
Cloud computing security problem and strategy	Privacy in the data and availability of services	Use of multiple security methods to solve problem	[52]

Cloud computing security consideration	Compromise in compliance integrity and data security	To apply firewall, detection of intrusion and prevention of intrusion, monitor integrity, inspection of log regularly	[53]
Cloud computing security trends and research directions	Provisioning of users in clouds with some mapping	Regulatory compliance by service providers of cloud with good norms of disclosure	[54]
Cloud computing security issues and challenges	Issues regarding security and challenges faced by CSP	Standards regarding security and model to manage properly	[55]
Cloud computing security management	Concern about ownership of data	Inclusion of identity and management regarding access, protocols and their standardization	[56]
Analysis of cloud computing security issues	Problems in cloud architecture, characteristics, its stakeholder and delivery	Solutions regarding security which is cloud aware and to secure model having dynamic data	[57]

Security support or IoT

IoT computing devices are considered as low cost and they are not powerful compared to laptop or desktop. Most of the IO T devices are considered as having low energy with the use of microcontroller having low end. It was observed that the Internet protocols which are existed are not design for these kind of embedded devices [58]. The different working group related to Internet engineering task force are created so that different problems can be easily tackled. There are some communication protocol with lightweight particularly in case of inhibited situation [59]. These environment include IPv6 for personal area network having little power without wire, also includes IPv6 for little power with routing protocol and lossy network apart from the protocol of inhibited presentation [60].

CoAP and security

CoAp is the term used to denote application layer protocol e.g. HTTP which is mostly designed in case of network having constraints. The user Datagram Protocol is considered by CoAP because of its suitability in case of connection having lesser bandwidth apart from the lesser computational power [61]. The encryption protocol used in case of HTTP is Transport Layer Security (TLS: RFC 5246), it was observed that there is much complexity involved in the

execution of TLS. CoAP services DTLS:RFC 63417 because of proper protocols in the security, it was also observed that this system is good at providing security as that of TLS [62].

Attacks on Cloud Platform

There are different three network based attacks consists of port scanning, Botnets and Spoofing attacks. Port Scanning is a kind of port based on a server and this used for penetrating to check implementation of service on the directed instrument. This type of system generally used for exposing the susceptibilities of the targeted device [63]. Botnets is used for thieving the data from a host device or instrument and then communication is implemented to the bot-master. Spoofing attacks is considered in the network imitate things in case of purpose having malevolent. Generally intrusion recognition system is used to handle such attacks [64].

The VM dependent attacks are easily found on the system of cloud infrastructure. There are four different type of VM dependent attacks i.e. cross VM side channel attacks, VM creation attacks, VM migration-rollback attacks [65] and VM scheduler centered attacks [66].

Some of the attacks on cloud platform are storage dependent attacks, there are two types of storage based attacks i.e. data scavenging and data deduplication attacks [67]. There are some attacks which are application dependent and this includes malware injection-steganography attacks [68], shared architecture attacks and webs services-protocol dependent attacks [69].

Cloud protection automation

The Alert Correlation, Assessment and Reaction module – next generation system (ACARM-ng) can be used for the generation of alerts and to have correlation [70]. The Suricata intrusion prevention system is considered as rule dependent engine which generally used for supporting the recognition of intrusion and inhibit through observing the traffic of network [71]. The Open Source SECurity (OSSEC) intrusion inhibition system is used for checking the network which are hosted discretely [72]. Snort is considered as network invasion inhibition system and this provides provision for packet sniffing modes apart from the packet logging modes which in addition to the investigating the method of NIDS. The Next Generation Intrusion Detection Expert System (NIDES) is used for the accomplishment on the host system, so that the investigation of activities from the user get collected for the target desktops [73]. There is eXpert-BSM software which is considered to be recognition system of invasion and it is host dependent, this uses the information base for the revealing of the invasions and generation of

alarm particularly on the system of Sun-Solaris dependent. There is also a Fail2ban software that generally uses the files of logging and usually identifies the configurations that resembles to the efforts of invasion [74]. There is a Prelude-OSS invasion recognition system and this is a kind open source form of the earlier mentioned Prelude software and this is used for providing backing of security event supervision. To perform the real time analysis for the events of intrusion then the Sagan software is very essential [75]. For the case of testing the integrity and analysis of logging apart from scanning the port there is IDS system which is host dependent, the invasion recognition system called Samhim is very helpful. If the intrusion are to be distinguished in term of observing real-time data then the Bro-IDS structure is used for analyzing the network.

9. Cloud computing and IOT solutions

The two technologies including cloud computing and IoT have already considered as a life's part. Nowadays the use of these technologies are increasing and becoming a part for technology in the future. Large number of applications are expected when the integration of IoT and cloud computing. The CloudIot paradigm was studied thoroughly in the research work [76].

The internet of things (IoT) and cloud computing is considered to be important in the case of manufacturing sector. The study was carried out in Cisco company which have improved the productivity when the cloud solutions enabled with IoT. There are many industries establishing roadmaps and also implementing for different opportunities in the market [77]. The main aim of integration of internet of things and cloud computing is the proper conjunction of the objects when used the network of wireless. The development of this integrating technology is spreading rapidly. The function of smart devices goes on improving and therefore becoming a challenge to resolve the security issues [78]. The review work was carried out in the paper and the name of integrating the technology of IoT and CC is considered as Cloud of things. Some of the major key problems have been identified in the case of Cloud of things. Some solutions are also included to resolve the problems stated [79].

Table 2: Review of cloud computing and IoT solutions

Theme	Applications	Solution	References

Integration of cloud computing and IoT	Smart grids, power sector	CloudIoT as platform for integration of cloud computing and IoT	[80]
Communication protocol for IoT and cloud computing	Fog system, cloud dependent IoT system	To include protocols in IoT, fog and cloud	[81]
Conceptual framework using IoT and Cloud computing	Healthcare system	Role of integrating IoT & CC	[82]
Efficient and scalable IoT service Delivery	Service delivery model	IoT PaaS architecture used, leverage of resources and middle service	[83]
Cloud computing for IoT	Smart devices	To provide storage remotely and accession to data without any kind of delay	[84]
Integration of IoT and cloud computing	Balanced Energy consumption	Use of Evolutionary algorithms considered as solution to be energy efficient	[85]

10. Recommendations

The security challenges have been analyzed properly in the present work related to cloud infrastructure and some of the solution existed, it is observed that the measures for addressing the challenges is very important. Some of the recommendations are as follows:

i. IoT enabled devices with integration of cloud infrastructure shall be designed so that the security as a important part. The security shall be considered at the different stages in the cycle of development i.e from the step of design to step of implementation.

ii. It is very important to make regular interval of updating and the process of patching so that it can be ensure vulnerabilities in security to be resolved at regular interval.

iii. Proper segmentation should be carried out in the networks so that prevention of unauthorized access is possible. Also this may lead to the breaches in the security in limited numbers.

iv. All the kind of data shall be encrypted properly in the transit and at the position of rest, this shall lead to the protection against unauthorized access.

v. The authentication process can be multi-factor so that the prevention of unauthorized access to IoT enabled devices can be done effectively.

11. Conclusions:

In conclusions the security challenges in involved in the internet of things and integration of cloud infrastructure have been presented in the present work. The attention is needed from the different researchers and practitioners in the problems faced in this field. The integration of some new technologies including fog computing apart from the blockchain technologies found to be very helpful to resolve some of the challenges faced. But there is need of an hour to develop more efficient and secured solution for the addressing dynamic field for internet of things enabled systems. The certain recommendation involve in term of adoption of different good practices apart from standardization and regular interval of auditing. The training can be given to the employees regarding the mitigation of some risks involved in the cloud infrastructure which is IoT enabled. Since the IoT enabled devices are increasing this has become very important for addressing the challenges involved in the security for ensuring integrity and confidentiality in the data apart from the system and data availability.

Bibliography

[1] T. Xu, J. B. Wendt and M. Potkonjak, "Security of IoT systems: Design challenges and opportunities," in *2014 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, 2014.

[2] T. Xu, J. B. Wendt and M. Potkonjak, "Security of IoT systems: Design challenges and opportunities," in *2014 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, 2014.

[3] M. Roopak, G. Yun Tian and J. Chambers, "Deep Learning Models for Cyber Security in IoT Networks," in *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, 2019.

[4] G. Nebbione and M. C. Calzarossa, "Security of IoT Application Layer Protocols: Challenges and Findings," *Future Internet*, vol. 12, 2020.

[5] C. Bodei, S. Chessa and L. Galletta, "Measuring security in IoT communications," *Theoretical Computer Science*, vol. 764, pp. 100-124, 2019.

[6] M. S. Hossain, G. Muhammad, S. M. M. Rahman, W. Abdul, A. Alelaiwi and A. Alamri, "Toward end-to-end biomet rics-based security for IoT infrastructure," *IEEE Wireless Communications*, vol. 23, pp. 44-51, 10 2016.

[7] W. Ahmad, A. Rasool, A. R. Javed, T. Baker and Z. Jalil, "Cyber Security in IoT-Based Cloud Computing: A Comprehensive Survey," *Electronics*, vol. 11, 2022.

[8] R. Agrawal, P. Verma, R. Sonanis, U. Goel, A. De, S. A. Kondaveeti and S. Shekhar, "Continuous Security in IoT Using Blockchain," in *2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2018.

[9] P. Bull, R. Austin, E. Popov, M. Sharma and R. Watson, "Flow Based Security for IoT Devices Using an SDN Gateway," in *2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud)*, 2016.

[10] P. Bull, R. Austin, E. Popov, M. Sharma and R. Watson, "Flow based security for IoT devices using an SDN gateway," in *2016 IEEE 4th international conference on future internet of things and cloud (FiCloud)*, 2016.

[11] S. Vashi, J. Ram, J. Modi, S. Verma and C. Prakash, "Internet of Things (IoT): A vision, architectural elements, and security issues," in *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, 2017.

[12] J. Wurm, K. Hoang, O. Arias, A.-R. Sadeghi and Y. Jin, "Security analysis on consumer and industrial IoT devices," in *2016 21st Asia and South Pacific design automation conference (ASP-DAC)*, 2016.

[13] F. Meneghello, M. Calore, D. Zucchetto, M. Polese and A. Zanella, "IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices," *IEEE Internet of Things Journal*, vol. 6, p. 8182–8201, 2019.

[14] R. Gurunath, M. Agarwal, A. Nandi and D. Samanta, "An overview: security issue in IoT network," in *2018 2nd international conference on I-SMAC (IoT in social, Mobile, analytics and cloud)(I-SMAC) I-SMAC (IoT in social, Mobile, analytics and cloud)(I-SMAC), 2018 2nd international conference on*, 2018.

[15] F. Loi, A. Sivanathan, H. H. Gharakheili, A. Radford and V. Sivaraman, "Systematically evaluating security and privacy for consumer IoT devices," in *Proceedings of the 2017 Workshop on Internet of Things Security and Privacy*, 2017.

[16] V. Sivaraman, H. H. Gharakheili, A. Vishwanath, R. Boreli and O. Mehani, "Network-level security and privacy control for smart-home IoT devices," in *2015 IEEE 11th International conference on wireless and mobile computing, networking and communications (WiMob)*, 2015.

[17] A. K. Simpson, F. Roesner and T. Kohno, "Securing vulnerable home IoT devices with an in-hub security manager," in *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, 2017.

[18] E. Sisinni, A. Saifullah, S. Han, U. Jennehag and M. Gidlund, "Industrial internet of things: Challenges, opportunities, and directions," *IEEE transactions on industrial informatics*, vol. 14, p. 4724–4734, 2018.

[19] P. K. Malik, R. Sharma, R. Singh, A. Gehlot, S. C. Satapathy, W. S. Alnumay, D. Pelusi, U. Ghosh and J. Nayak, "Industrial Internet of Things and its applications in industry 4.0: State of the art," *Computer Communications*, vol. 166, p. 125–139, 2021.

[20] W. Z. Khan, M. H. Rehman, H. M. Zangoti, M. K. Afzal, N. Armi and K. Salah, "Industrial internet of things: Recent advances, enabling technologies and open challenges," *Computers & Electrical Engineering*, vol. 81, p. 106522, 2020.

[21] M. Serror, S. Hack, M. Henze, M. Schuba and K. Wehrle, "Challenges and opportunities in securing the industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 17, p. 2985–2996, 2020.

[22] H. Boyes, B. Hallaq, J. Cunningham and T. Watson, "The industrial internet of things (IIoT): An analysis framework," *Computers in industry*, vol. 101, p. 1–12, 2018.

[23] A. Bahga and V. K. Madisetti, "Blockchain platform for industrial internet of things," *Journal of Software Engineering and Applications*, vol. 9, p. 533–546, 2016.

[24] J. Wan, S. Tang, Z. Shu, D. Li, S. Wang, M. Imran and A. V. Vasilakos, "Software-defined industrial internet of things in the context of industry 4.0," *IEEE Sensors Journal*, vol. 16, p. 7373–7380, 2016.

[25] M. H. ur Rehman, I. Yaqoob, K. Salah, M. Imran, P. P. Jayaraman and C. Perera, "The role of big data analytics in industrial Internet of Things," *Future Generation Computer Systems*, vol. 99, p. 247–259, 2019.

[26] Y. Liao, E. d. F. R. Loures and F. Deschamps, "Industrial Internet of Things: A systematic literature review and insights," *IEEE Internet of Things Journal*, vol. 5, p. 4515–4525, 2018.

[27] P. Lade, R. Ghosh and S. Srinivasan, "Manufacturing analytics and industrial internet of things," *IEEE Intelligent Systems*, vol. 32, p. 74–79, 2017.

[28] S. Vishnu, S. J. Ramson and R. Jegan, "Internet of medical things (IoMT)-An overview," in *2020 5th international conference on devices, circuits and systems (ICDCS)*, 2020.

[29] A. Ghubaish, T. Salman, M. Zolanvari, D. Unal, A. Al-Ali and R. Jain, "Recent advances in the internet-of-medical-things (IoMT) systems security," *IEEE Internet of Things Journal*, vol. 8, p. 8707–8718, 2020.

[30] G. J. Joyia, R. M. Liaqat, A. Farooq and S. Rehman, "Internet of medical things (IoMT): Applications, benefits and future challenges in healthcare domain.," *J. Commun.*, vol. 12, p. 240–247, 2017.

[31] F. Al-Turjman, M. H. Nawaz and U. D. Ulusar, "Intelligence in the Internet of Medical Things era: A systematic review of current and future trends," *Computer Communications*, vol. 150, p. 644–660, 2020.

[32] A. Gatouillat, Y. Badr, B. Massot and E. Sejdić, "Internet of medical things: A review of recent contributions dealing with cyber-physical systems in medicine," *IEEE internet of things journal*, vol. 5, p. 3810–3822, 2018.

[33] S. Razdan and S. Sharma, "Internet of medical things (IoMT): overview, emerging technologies, and case studies," *IETE technical review*, vol. 39, p. 775–788, 2022.

[34] J.-P. A. Yaacoub, M. Noura, H. N. Noura, O. Salman, E. Yaacoub, R. Couturier and A. Chehab, "Securing internet of medical things systems: Limitations, issues and recommendations," *Future Generation Computer Systems*, vol. 105, p. 581–606, 2020.

[35] H. Magsi, A. H. Sodhro, F. A. Chachar, S. A. K. Abro, G. H. Sodhro and S. Pirbhulal, "Evolution of 5G in Internet of medical things," in *2018 international conference on computing, mathematics and engineering technologies (iCoMET)*, 2018.

[36] G. Hatzivasilis, O. Soultatos, S. Ioannidis, C. Verikoukis, G. Demetriou and C. Tsatsoulis, "Review of security and privacy for the Internet of Medical Things (IoMT)," in *2019 15th international conference on distributed computing in sensor systems (DCOSS)*, 2019.

[37] G. Thamilarasu, A. Odesile and A. Hoang, "An intrusion detection system for internet of medical things," *IEEE Access*, vol. 8, p. 181560–181576, 2020.

[38] A. Zanella, N. Bui, A. Castellani, L. Vangelista and M. Zorzi, "Internet of things for smart cities," *IEEE Internet of Things journal*, vol. 1, p. 22–32, 2014.

[39] Y. Mehmood, F. Ahmad, I. Yaqoob, A. Adnane, M. Imran and S. Guizani, "Internet-of-things-based smart cities: Recent advances and challenges," *IEEE Communications Magazine*, vol. 55, p. 16–24, 2017.

[40] Y. Qian, D. Wu, W. Bao and P. Lorenz, "The internet of things for smart cities: Technologies and applications," *IEEE Network*, vol. 33, p. 4–5, 2019.

[41] A. H. Alavi, P. Jiao, W. G. Buttlar and N. Lajnef, "Internet of Things-enabled smart cities: State-of-the-art and future trends," *Measurement*, vol. 129, p. 589–606, 2018.

[42] D. Bonino, M. T. D. Alizo, A. Alapetite, T. Gilbert, M. Axling, H. Udsen, J. A. C. Soto and M. Spirito, "Almanac: Internet of things for smart cities," in *2015 3rd International Conference on Future Internet of Things and Cloud*, 2015.

[43] W. Ejaz, M. Naeem, A. Shahid, A. Anpalagan and M. Jo, "Efficient energy management for the internet of things in smart cities," *IEEE Communications magazine*, vol. 55, p. 84–91, 2017.

[44] B. Ahlgren, M. Hidell and E. C.-H. Ngai, "Internet of things for smart cities: Interoperability and open data," *IEEE Internet Computing*, vol. 20, p. 52–56, 2016.

[45] W. Li, H. Song and F. Zeng, "Policy-based secure and trustworthy sensing for internet of things in smart cities," *IEEE Internet of Things Journal*, vol. 5, p. 716–723, 2017.

[46] A. Kazmi, Z. Jan, A. Zappa and M. Serrano, "Overcoming the heterogeneity in the internet of things for smart cities," in *Interoperability and Open-Source Solutions for the Internet of Things: Second International Workshop, InterOSS-IoT 2016, Held in Conjunction with IoT 2016, Stuttgart, Germany, November 7, 2016, Invited Papers 2*, 2017.

[47] N. Zhang, H. Chen, X. Chen and J. Chen, "Semantic Framework of Internet of Things for Smart Cities: Case Studies," *Sensors*, vol. 16, 2016.

[48] I. M. Khalil, A. Khreishah and M. Azeem, "Cloud Computing Security: A Survey," *Computers*, vol. 3, p. 1–35, 2014.

[49] U. A. Butt, M. Mehmood, S. B. H. Shah, R. Amin, M. W. Shaukat, S. M. Raza, D. Y. Suh and M. J. Piran, "A Review of Machine Learning Algorithms for Cloud Computing Security," *Electronics*, vol. 9, 2020.

[50] M. Almorsy, J. Grundy and I. Müller, *An Analysis of the Cloud Computing Security Problem*, 2016.

[51] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," *Future Generation Computer Systems*, vol. 28, pp. 583-592, 2012.

[52] W. Liu, "Research on cloud computing security problem and strategy," in *2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet)*, 2012.

[53] A. Tripathi and A. Mishra, "Cloud computing security considerations," in *2011 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC)*, 2011.

[54] S. Sengupta, V. Kaulgud and V. S. Sharma, "Cloud Computing Security–Trends and Research Directions," in *2011 IEEE World Congress on Services*, 2011.

[55] K. Popović and Ž. Hocenski, "Cloud computing security issues and challenges," in *The 33rd International Convention MIPRO*, 2010.

[56] S. A. Almulla and C. Y. Yeun, "Cloud computing security management," in *2010 Second International Conference on Engineering System Management and Applications*, 2010.

[57] A. Behl and K. Behl, "An analysis of cloud computing security issues," in *2012 World Congress on Information and Communication Technologies*, 2012.

[58] P. Thubert, *RFC 6282: Compression Format for IPv6 Datagrams over IEEE 802.15. 4-Based Networks*, RFC Editor, 2011.

[59] A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, J. P. Vasseur and R. Alexander, *RFC 6550: RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks*, RFC Editor, 2012.

[60] Z. Shelby, K. Hartke and C. Bormann, "The constrained application protocol (CoAP)," 2014.

[61] T. Dierks and E. Rescorla, "The transport layer security (TLS) protocol version 1.2," 2008.

[62] E. Rescorla and N. Modadugu, "Datagram transport layer security version 1.2," 2012.

[63] J. Soldatos, M. Serrano and M. Hauswirth, "Convergence of utility computing with the internet-of-things," in *2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, 2012.

[64] K. Scarfone, P. Mell and others, "Guide to intrusion detection and prevention systems (idps)," *NIST special publication*, vol. 800, p. 94, 2007.

[65] H. Rong, M. Xian, H. Wang and J. Shi, "Time-stealer: A stealthy threat for virtualization scheduler and its countermeasures," in *Information and Communications Security: 15th International Conference, ICICS 2013, Beijing, China, November 20-22, 2013. Proceedings 15*, 2013.

[66] F. Zhou, M. Goel, P. Desnoyers and R. Sundaram, "Scheduler vulnerabilities and coordinated attacks in cloud computing," *Journal of Computer Security*, vol. 21, p. 533–559, 2013.

[67] D. Harnik, B. Pinkas and A. Shulman-Peleg, "Side channels in cloud services: Deduplication in cloud storage," *IEEE Security & Privacy*, vol. 8, p. 40–47, 2010.

[68] Y. Zhang, A. Juels, M. K. Reiter and T. Ristenpart, "Cross-Tenant Side-Channel Attacks in PaaS Clouds," in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, New York, NY, USA, 2014.

[69] G. Doychev, B. Köpf, L. Mauborgne and J. Reineke, "Cacheaudit: A tool for the static analysis of cache side channels," *ACM Transactions on Information and System Security (TISSEC)*, vol. 18, p. 1–32, 2015.

[70] B. lomiej Balcerek, B. Szurgot, M. Uchronski and W. Waga, "ACARM-ng: Next Generation Correlation Framework," *Building a National Distributed e-Infrastructure–PL-Grid*, p. 114–127.

[71] U. Lindqvist and P. A. Porras, "eXpert-BSM: A host-based intrusion detection solution for Sun Solaris," in *Seventeenth Annual Computer Security Applications Conference*, 2001.

[72] K. Hwang and D. Li, "Trusted cloud computing with secure resources and data coloring," *IEEE Internet Computing*, vol. 14, p. 14–22, 2010.

[73] R. Bray, D. Cid and A. Hay, OSSEC host-based intrusion detection guide, Syngress, 2008.

[74] H. Takabi, J. B. D. Joshi and G.-J. Ahn, "Securecloud: Towards a comprehensive security framework for cloud computing environments," in *2010 IEEE 34th Annual Computer Software and Applications Conference Workshops*, 2010.

[75] Z. Shen, L. Li, F. Yan and X. Wu, "Cloud computing system based on trusted computing platform," in *2010 International Conference on Intelligent Computation Technology and Automation*, 2010.

[76] A. Botta, W. de Donato, V. Persico and A. Pescapé, "Integration of Cloud computing and Internet of Things: A survey," *Future Generation Computer Systems*, vol. 56, pp. 684-700, 2016.

[77] D. Georgakopoulos, P. P. Jayaraman, M. Fazia, M. Villari and R. Ranjan, "Internet of Things and Edge Cloud Computing Roadmap for Manufacturing," *IEEE Cloud Computing*, vol. 3, pp. 66-73, 2016.

[78] C. Stergiou, K. E. Psannis, B.-G. Kim and B. Gupta, "Secure integration of IoT and Cloud Computing," *Future Generation Computer Systems*, vol. 78, pp. 964-975, 2018.

[79] M. Aazam, I. Khan, A. A. Alsaffar and E.-N. Huh, "Cloud of Things: Integrating Internet of Things and cloud computing and the issues involved," in *Proceedings of 2014 11th International Bhurban Conference on Applied Sciences & Technology (IBCAST) Islamabad, Pakistan, 14th - 18th January, 2014*, 2014.

[80] L. Bagherzadeh, H. Shahinzadeh, H. Shayeghi, A. Dejamkhooy, R. Bayindir and M. Iranpour, "Integration of Cloud Computing and IoT (CloudIoT) in Smart Grids: Benefits, Challenges, and Solutions," in *2020 International Conference on Computational Intelligence for Smart Power System and Sustainable Energy (CISPSSE)*, 2020.

[81] J. Dizdarević, F. Carpio, A. Jukan and X. Masip-Bruin, "A Survey of Communication Protocols for Internet of Things and Related Challenges of Fog and Cloud Computing Integration," *ACM Comput. Surv.*, vol. 51, 1 2019.

[82] S. Tyagi, A. Agarwal and P. Maheshwari, "A conceptual framework for IoT-based healthcare system using cloud computing," in *2016 6th International Conference - Cloud System and Big Data Engineering (Confluence)*, 2016.

[83] F. Li, M. Voegler, M. Claessens and S. Dustdar, "Efficient and Scalable IoT Service Delivery on Cloud," in *2013 IEEE Sixth International Conference on Cloud Computing*, 2013.

[84] H. Tyagi and R. Kumar, "Cloud Computing for IoT," in *Internet of Things (IoT): Concepts and Applications*, M. Alam, K. A. Shakil and S. Khan, Eds., Cham, Springer International Publishing, 2020, p. 25–41.

[85] A. Mebrek, L. Merghem-Boulahia and M. Esseghir, "Efficient green solution for a balanced energy consumption and delay in the IoT-Fog-Cloud computing," in *2017 IEEE 16th International Symposium on*

Network Computing and Applications (NCA), 2017.

[86] D. Serpanos, M. Wolf, D. Serpanos and M. Wolf, "Industrial internet of things," *Internet-of-Things (IoT) Systems: Architectures, Algorithms, Methodologies*, p. 37–54, 2018.

[87] S. Jeschke, C. Brecher, T. Meisen, D. Özdemir and T. Eschert, Industrial internet of things and cyber manufacturing systems, Springer, 2017.