Technoarete Transactions on Internet of Things and Cloud Computing Research
Vol-2, Issue-4, December 2022
e-ISSN: 2583-0805

Evaluating Present and Future Challenges in IoT Security

Muzammil Parvez M[1]*, Vishal Kumar[2]

[1] Department of ECE, KL University, India.
[2] Chandigarh University, India.
*Corresponding Author Email: [1] parvez190687@gmail.com

Abstract

The internet of things is presently faced with huge challenges which presently create a major effect on the present and future organizational development. IoT proceeds with high concentrated security and thus is mainly confirmed with the major development due to maintaining data security. Providing IoT security has been faced many challenges such as: in healthcare service, data analytics, information technology and agricultural issues. The government body has taken better chances under the construction of carelessness and various fraud activities. The strong passwords and security codes should be provided at the time of better processing. Lack of scalability, lack of government support, interoperability, security and personal privacy, lack of treating patients, design base challenges are major issues faced by managing IoT security. There is high cultural effectiveness and huge drastic changes have been faced by the organization as technical upgradation has not been done in any sector. Hence, security personnel and many important human resources should have a better impact on future development. The application of advanced technicians can have a better impact on future growth.

Keywords

Development, information, Internet of things, IoT security.

INTRODUCTION

Security on the internet of things is an important one which is conducted with specific confidential processes which allows better security of big data and large analytical computation. In recent days, usage of IoT is prioritised by many organisations to bring effectiveness in overall business operations [1]. However, sometimes outcomes from the usage of IoT reflect complications that may cause many issues to enterprises. The security in IoT is the most important which is directed towards privacy maintenance to have ethical business operations. Many enterprises have faced huge difficulties in providing securities in IoT. Big data analytics, computation and programming have faced the most challenging situation without satisfying security.

In recent times, the major security of IoT has been facing various challenges which may bring various obstacles in business conduction and transformation of various jobs. The Internet of Things (IoT) has faced various challenges such as: failing to get healthcare information, data analytics, information technology and agricultural issues [2]. The major security of IoT can proceed with minute and advanced processes which may not be possible in the recent trends due to the least number of proper techniques. There is a major lack in documentation and international data privacy regulation and lack of proper access. These issues happen due to lack of automation and careless activities.

The present challenges of IoT are mainly faced with the application of various devices such as artificial intelligence tools and less effective visibility. The present security issues of IoT are: limited security, lack of visibility, open-source code, weak password, unpatched vulnerabilities and vulnerable APIs [3]. IoT security is the robust activity which includes better protection of big data sets within a high volume. In this concern, manufacturing of IoT devices should be most satisfied to perform a great job. However, there are some problems faced by providing certain security as these transmitters and sensors are low cost which may not be fruitful in business operation. Hence low-cost devices create major obstacles which may not be efficient in creating better jobs.

MATERIALS AND METHODS

This article has been chosen for qualitative design to conduct a better approach in the evolution of major topics. Qualitative design in the study allows gathering non-numerical data or information which may get a better advantage in justification of a certain topic [4]. This type of research design allows the researcher to gather information based on present and future challenges of IoT which can make a perfect alignment to get better results in future investigation. In this concern, the researcher has collected secondary data which makes a better approach in proper justification. The researcher mainly gathers information about security challenges of IoT, present and future challenges which have been gathered from relevant peer-reviewed journals which can form feasible conditions to form justification.

The researcher should choose better qualitative design to get a fruitful way of justification and should not choose any other method of design which may create some obstacles. On the other hand, the researcher should choose a secondary data collection method which can form a better approach in evaluating the entire article regarding the major subject.

Technoarete Transactions on Internet of Things and Cloud Computing Research
Vol-2, Issue-4, December 2022
e-ISSN: 2583-0805

RESULTS

Security issues of IoT

The security challenges of IoT have not been constructed with keeping security protocols in mind. This particular aspect can be the myriad of IoT security challenges that can be able to guide a disastrous circumstance [5]. Additionally, several people do not understand the inherent issues with IoT devices. Threats and attacks typically humiliate fragmented or hardcore passwords to archive entry cards to IoT devices as well. These IoT device credentials are often retained as unencrypted within several types of databases, by making it easy for the hackers to steal the information in an easy way.

Lack of security integration

The reason behind security norms of IoT devices is that there are various IoT devices, extending within the security systems which are not possible to maintain [6]. Lack of security integration can be an immersive challenge in the implementation of IoT devices.

Deficiency of visibility

Users of IoT devices often deploy it without having any sort of knowledge regarding the IT department and this can make a huge impact on the security protocols of IoT devices [7]. This lack of knowledge makes it impossible to have an adequate stock of what requires be securing and observing firmly.

Fragmented process of testing

There are plenty of IoT developers who do not take the charge of security and thus they fail to act impact fully with vulnerable testing to identify fragile traits within IoT devices.

Pause in Vulnerabilities

There are uncountable IoT devices which have unpatched vulnerabilities for several reasons, involving patches which have not been available and issues can be easily entered within the devices and can install the patches. This involves many issues in recent transactions and continuation of various business operations that lead to huge challenges at this time.

Weak passwords

Internet of things devices are mainly shipped with web default passwords and that may fall under the obstacle situation. Weak passwords are commonly easy to access by common criminals and many people who create fraud activities [9]. The fraud activity has increased at an alarming rate due to this type of weak passwords. This password should be conducted with various characters and lower-upper cases of passwords and these passwords should change within time.

Open-source code vulnerability

There are various firmwares which especially use open source code for vulnerable security systems. Open source code is determined with the code that is easy to identify which may not create a clear activity and this causes a huge adverse effect on the business operation. This process may not make an effective process due to lack of proper process.

The cyber security and major business operations should make proper cyber security and this has been getting huge issues in transaction of information and data. Therefore, future development may affect drastically and profitable growth may not proceed within this conduction. Hence, all the business operation and major programming computation should be secured with string password and key code.

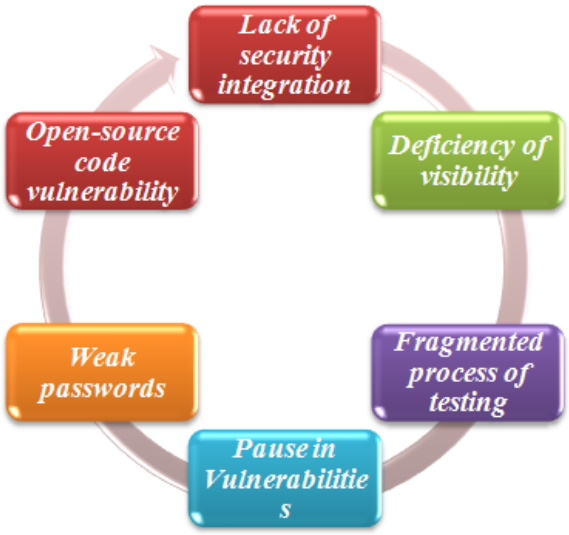

Figure 1: Security issues of IoT

Present challenges related to IoT security

Vast opportunities are provided to software and wearable devices by IoT in the field of communicating and sharing information on internet. A huge amount of private information is contained by this shared information; therefore, there is an immense requirement of maintaining a high security level of this data that is shared. The Internet of things is facing many issues in the areas which hamper privacy protection of any organization. There are many areas in which IoT has faced many challenges such as: in the civil society, private sector and in many public sectors [9]. Government body focuses on such issues, areas which may play a vital role in preventing IoT protection. Information technology is getting more negative as there is a lack of proper protection. Information technology mainly proceeds with various codes and key codes which may not be more protective and this is easily identified by any fraud individual. This hampers many areas such as the public and private sector. Hence, major obstacles have appeared in the business development process which may not be fruitful for recent trends.

Lack of proper upgradation and lacking in usage of new scalability may create a major challenge in providing security of IoT. There are some present challenges which hamper development work such as: lack of scalability, lack of government support, interoperability, security and personal privacy, lack of treating patients, design base challenges [10].

e-ISSN: 2583-0805

Huge network has been connected with billions of devices that need to be replaced with systematic development. A device or system that is highly present with the IoT process specifically needs a scalable aspect [11]. The raw data obtained from different types of devices and systems requires big data analytics and cloud storage. This raw data can be connected with each other to get a fruitful result, though this does not proceed in a systematic way as there is a lack of protection facility in IoT. Moreover, technology should be upgraded with various new implementations which mainly cause standardization in modern business construction.

Interoperability in various sectors is still disintegrated as there is a lack of standard technological upgradation. Technologies always need to be standard and should be converged [12]. This can make a better effect on building up a common framework which is related to IoT. This standardization process is still lacking in the devices and various careless activities have been showcased in the formation of technological upgradation. Interoperability within legacy devices is especially considered as a critical position and has also hampered much internal connectivity. This situation has made obstacles in reaching the major goal of the company which is incorporated with smart objectives.

Government body does not give more attention to the protection of various major trends and this has lacked under recommendation of security of IoT. The government body and regulatory body have not been setting up accurate safety rules rather working with easy maintenance. Regulator body has a responsibility in maintaining the security of IoT with protecting various information of many people [13]. The lack of proper protection, treatment based on the technological process cannot continue at a particular system and also resulted in huge risk on major operations. There are various less modification devices of IoT which is now connected with major objectives and this can make huge technological error and theatre various patients.

Basic technological design has also been affected in the way of limited protection and this may increase unpredictable results in major works. The technical upgradation is an important part in the way of major development which is designed by various frameworks and new analytical processes to have a feasible effect on organization [14]. Recent graph has highlighted that there are huge challenges faced with the huge procedure of security protection of IoT. There are huge challenges depicted in the recent year, in which transportation and logistics have faced huge challenges with huge amounts of money being spent. This resulted due to a major lack of security within the inter-operational management.

API and cloud services have spent much in integration of major integration which may not be fruitful with careless activity. The industrial internet of things (IIoT) is expected to reach $123 billion in 2021 rather than 2020[15]. However, the personnel have not taken any step under better protection and securities which leads to a risk in organizational development. The lack of proper care and maintenance may sometimes create less effective emergence.

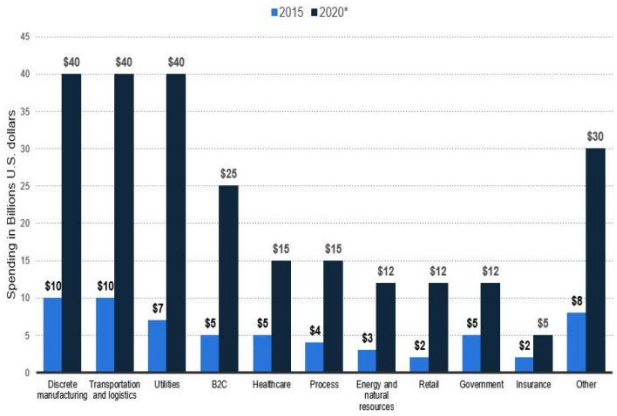

Figure 2: Spending internet of things worldwide from 2015 to 2020 (in billions of US Dollar)

Future challenges associated with IoT security

The lack of technological upgradation and major protection imitation may challenge many sectors. In this concern, there is major utilization of proper business models that may not be working out. The future of IoT may not be fruitful whether there is less potential activity in and strong protection in IoT. Hospitality services, agricultural development have loosened various information and this leads to major challenges in future establishment [16]. Increasing the rate of network agility, AI and automation technology can make huge chances to have secured diverse uses within a major scale. Government has taken various new integrations to have better facilities in connection with better criteria of people which may not be happening with the proper protection. This may cause huge challenges in developing major business activity.

IoT can leverage various empowerment activities in the establishment of networking establishments. Smart city application for citizen analysis has been created with specific application and adoption of new technology [17]. Hence, security should be provided with major specific knowledge to have opportunities. The IoT already transfers into the main security concern; this attentively makes various monitoring facilities to get minute information from every place. In this way many peers should be connected to enhance the rate of connection. However, some fraud activities never get into the certain integration rather this affects various organizational developments.

Connectivity is the major challenge in IoT procedures which make better connections between humans and various underlying technologies. Connectivity model is really sufficient in the business ecosystem which can make better connections within personnel and main trends of technology [18]. There is better peer-to-peer connection between major communication establishments which may emerge with IoT technologies which can make positive changes in the major business operation. The security limitation in major business development may not be created with the less effective security and this may receive huge challenges in profitable

e-ISSN: 2583-0805

return in future. The future growth may not be continued with less effective scalability and this creates huge risk on the major establishment.

Mitigation of security issues of IoT

Security issues should be mitigated with the help of proper steps and a secure system that can control every personal information and data. A security analytics infrastructure has been reduced due to careless activity of government and organizational personnel. The analytical infrastructure has reduced, which is related to the Internet of things, this is required in collection of compilation, analysis of data, multiple sources of IoT and threat intelligence [19]. All the organizational personnel and many business activists should go forward with the idea of maintaining a big data set and huge logical programming. In this way, major business activity should look at the securing major connection, identification of high risk features, focusing on the major quality, upgradation of devices, getting certification process and purchasing secured SMART devices [20]. There should be a sedentary networking facility that affects major business development.

Any business activity may be connected with the secured formation of a major connector which can provide better connection between humans and machines. The security network should be within the effects and that is able to protect major business activities [21]. The encryption of networking activity can provide potential effects which threaten pass codes and key codes. On the other hand, business activities can keep away from fraud personnel's. This is able to protect every objective and potential business growth that is the major vitality to form potential risk with major recommendation. The high risk can be identified with application of various instruments and this should be successful and hidden with all conditions.

Many accessible devices can be detected with specific cameras, microphones, automatically saving cards and recording facilities. The major features that can make proper protection and security with the action and adoption of new technology can have a better effect on IoT technologies [22]. Cameras, microphone are the main features to have prep identification of high risk areas and this is able to connect any type of devices without knowing people. There are many applications which can also be connected with high standardization of technological development. The organization should take some steps with reliable guidelines which specifically proceed with a secured designed report, such as: Passwords of consumers should be unique and should be set with a universal setting of the factory. In addition, IoT devices should display certain contacts and this can promptly report major incidents. On the other hand, manufacturers of IoT must be displayed with a certain application of timings with minimum length that can make connections between devices and major updates.

The certification of IoT can only be acquired with proper terminologies that should be examined a lot to ensure protection of IoT applications. Cloud credentials can be able to provide better security and also assessing particular risks which form potential management [23]. Hence, every human resource personnel in the organization should be aware of certain risk factors that have been faced by interoperation; therefore, this technology can apply easily for certain mitigation. On the other hand, smart protection is ensured with application of antivirus software at the time of privacy setting. This can maintain the entire activity related to technological development. In addition, internet connection is an important one to have a proper process with another board. This is considered with the IoT worth which can result as a major organizational favour.

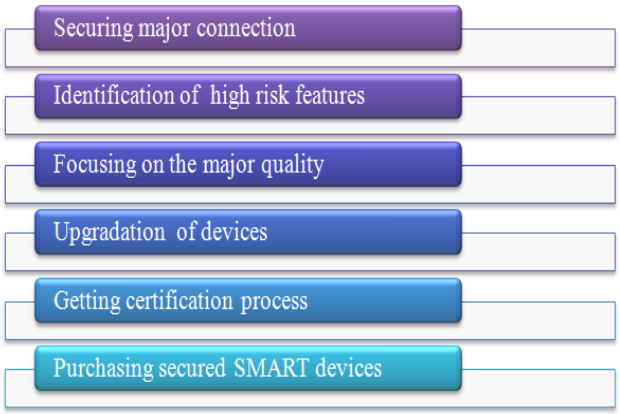

Figure 3: Mitigation of security issues of IoT

DISCUSSION

In the present challenges of IoT, there are a huge amount of drastic issues that have been faced by many organisations. There is much private information contained in the part of main requirement and this is highly being shared within the level of shared data. There are many areas which have been stated in recent reports that are: in the private sector, public sector and in the civil society. The negotiation level of government in the way of confirmation of security is required with negative growth. In the past trends of major upgradation regulation bodies have taken a step on the proper level of positive identification which is immensely concerned with security and privacy checking out. These activities have not been highlighted in major establishments as there is a huge obstacle in the business development process.

Lack of proper protection and less effective technological upgradation cannot make a huge feasible condition. The devices can get a huge negative effect that fails to meet reliable treatment of major device modification. Technological upgradation is the major effect on creating certain development and thus can form proper culture to maintain security [24]. In this concern, API and cloud technology and high priority of services have much to spend on internal activity. These activities in modern technological implementation have not been properly regarded as there is less effective adoption from main business activity. IIoT is expected to reach towards $123 billion in 2021 rather than previous year. This resulted in the application of innovative

e-ISSN: 2583-0805

technological implementation which can form organizational development.

There is a lack of technological upgradation as there is limited sect oral integration which is not giving importance to major business models. Hospitality services, agricultural development have loosened various information and this leads to major challenges in future establishment. Increasing the rate of network agility, AI and automation technology can make huge chances to have secured diverse uses within a major scale. Increasing the rate of network agility can make better results for careless processes which have come to be a risk factor on operational management. Moreover, there is an increasing rate of artificial intelligence and automation technology. Connectivity can be the better aspects which can make logical connectivity that impact with the major effect on organizational availability.

The connectivity is mainly referred to as the peer-to-peer connection between two different systems which also maintain analytical infrastructure that can easily make advanced construction. The future growth can be done with the help of effective scalability and this conducts less effective risks as the major trends of development. On the other hand, scalability is not upgraded as there is less impact on future production hence many business operations have been disconnected towards the security analysis. Moreover, major security has not been done with organizational personnel and main business personnel; hence future activity has remained closed. The business personnel and various activities should look forward to SMART integration with the help of application of logical programming.

There should be a huge facility of secondary networking that can impact major business development with better security possibilities. The integration of business activity can advance from a technological upgradation which can be protective with investigating high risk factors. Cameras, microphone are the main features to have an effective investigation of high risk areas and this is able to connect any type of devices without knowing people. There are many applications which can also be connected with high standardization of technological development; hence human resources activity should be prioritized with desired application.

CONCLUSION

The Internet of things has major challenges in the major security and maintenance of privacy which may not be fruitful in recent trends. Technological upgradation is also highlighted with aligning the IoT which is vital for the growth of business. There are several present challenges faced by providing proper security in IoT which has made specific challenges in the future organizational growth. Many organizations have not properly upgraded technology which can make huge turnover many businesses. On the other hand, the government does not make better connections with maintaining fruitful security in IoT. The application of cloud technology can give better chances of having effective facilities in privacy maintenance. However, easy passwords and key codes make the fraud personality feasible. This has resulted in a drastic view on organizational growth.

The present security issues of IoT are: limited security, lack of visibility, open-source code, weak password, unlatched vulnerabilities and vulnerable APIs. Moreover, the security of IoT has made robust creation in the way of data transaction and protection of big data sources. The big data sources have been getting into huge manufacturing facilities along with protection of various logical functions and programming. IoT devices have barely proceeded with low cost strategy which in the present situation may not make faithfulness towards the major trends. Hence, many fraud activities have been highlighted with greater effects on organizations. The article has mainly highlighted security issues in which lack of security integration, fragmented process, pause of vulnerability, weakening of key codes and deficiencies of visibilities has been stated.

Open source codes are also highlighted with application of various business operations and this cannot make proper creativity in future business. The business operation in recent trends is mainly done with cloud technological processes along with new implementation. However, there is less connection between major trends and a culture of strong security. Hence major business may not be feasible rather this may affect future development. Recent graphical representation has shown long term integrity with spreading in IoT which has created a huge effect on business development. In this concern, connectivity is an important component within the adoption of several technological procurements. However, there should be a proper system in the application of security in IoT and passwords should be strong which may not be used by any fraud personality.

REFERENCES

[1] Henriques, David, et al. "How IT Governance can assist IoT project implementation." *International Journal of Information Systems and Project Management* 8.3 (2020): 25-45..

[2] Sinha, Bam Bahadur, and R. Dhanalakshmi. "Recent advancements and challenges of Internet of Things in smart agriculture: A survey." *Future Generation Computer Systems* 126 (2022): 169-184.

[3] Rondon, Luis Puche, et al. "Survey on enterprise Internet-of-Things systems (E-IoT): A security perspective." *Ad Hoc Networks* 125 (2022): 102728.

[4] Johnson, Jessica L., Donna Adkins, and Sheila Chauvin. "A review of the quality indicators of rigor in qualitative research." *American journal of pharmaceutical education* 84.1 (2020).

[5] Jurcut, Anca, et al. "Security considerations for Internet of Things: A survey." *SN Computer Science* 1 (2020): 1-19.

[6] Khan, Muhammad Amir, et al. "An Adaptive Enhanced Technique for Locked Target Detection and Data Transmission over Internet of Healthcare Things." *Electronics* 11.17 (2022): 2726.

[7] Yadav, Chandra Shekhar, et al. "Malware Analysis in IoT & Android Systems with Defensive Mechanism." *Electronics* 11.15 (2022): 2354.

e-ISSN: 2583-0805

[8] Olofinbiyi, Sogo Angel. "Cyber insecurity in the wake of COVID-19: a reappraisal of impacts and global experience within the context of routine activity theory." *ScienceRise: Juridical Science* 1 (19) (2022): 37-45.
[9] Hess, David J. "Incumbent-led transitions and civil society: Autonomous vehicle policy and consumer organizations in the United States." *Technological Forecasting and Social Change* 151 (2020): 119825.
[10] Gupta, Medini, et al. "A systematic review on blockchain in transforming the healthcare sector." *Transformations Through Blockchain Technology: The New Digital Revolution* (2022): 181-200.
[11] Pal, Shantanu, et al. "Security requirements for the internet of things: A systematic approach." *Sensors* 20.20 (2020): 5897..
[12] Ning, Huansheng, et al. "A Survey on Metaverse: the State-of-the-art, Technologies, Applications, and Challenges." *arXiv preprint arXiv:2111.09673* (2021).
[13] Cheryl, Barr-Kumarakulasinghe, Boon-Kwee Ng, and Chan-Yuan Wong. "Governing the progress of internet-of-things: ambivalence in the quest of technology exploitation and user rights protection." *Technology in Society* 64 (2021): 101463..
[14] Gupta, Anchal, Rajesh Kr Singh, and Shivam Gupta. "Developing human resource for the digitization of logistics operations: readiness index framework." *International Journal of Manpower* 43.2 (2022): 355-379..
[15] ENTERPRISE TECH. “10 Charts That Will Challenge Your Perspective Of IoT's Growth”. *Forbes*. 6 June ,2023. https://www.forbes.com/sites/louiscolumbus/2018/06/06/10-charts-that-will-challenge-your-perspective-of-iots-growth/.
[16] Jamader, Asik Rahaman. "A Brief Report Of The Upcoming & Present Economic Impact To Hospitality Industry In COVID19 Situations." *Journal of Pharmaceutical Negative Results* (2022): 2289-2302..
[17] Bellini, Pierfrancesco, Paolo Nesi, and Gianni Pantaleo. "IoT-enabled smart cities: A review of concepts, frameworks and key technologies." *Applied Sciences* 12.3 (2022): 1607..
[18] Chen, Chun-Liang. "Value creation by SMEs participating in global value chains under industry 4.0 trend: Case study of textile industry in Taiwan." *Journal of Global Information Technology Management* 22.2 (2019): 120-145..
[19] Shim, Jung P., et al. "The Internet of Things: Multi-faceted research perspectives." *Communications of the Association for Information Systems* 46.1 (2020): 21..
[20] Da Xu, Li, Yang Lu, and Ling Li. "Embedding blockchain technology into IoT for security: A survey." *IEEE Internet of Things Journal* 8.13 (2021): 10452-10473..
[21] Cole, Rosanna, Mark Stevenson, and James Aitken. "Blockchain technology: implications for operations and supply chain management." *Supply Chain Management: An International Journal* 24.4 (2019): 469-483..
[22] Sinha, Bam Bahadur, and R. Dhanalakshmi. "Recent advancements and challenges of Internet of Things in smart agriculture: A survey." *Future Generation Computer Systems* 126 (2022): 169-184..
[23] Alwaheidi, Mohammed KS, and Shareeful Islam. "Data-Driven Threat Analysis for Ensuring Security in Cloud Enabled Systems." *Sensors* 22.15 (2022): 5726..
[24] Alzahrani, Bandar, et al. "How ready is higher education for quality 4.0 transformation according to the LNS research framework?." *Sustainability* 13.9 (2021): 5169.