ISSN: 2349 - 4891

International
Journal of Recent Research and Applied Studies
(Multidisciplinary Open Access Refereed e-Journal)

A Study on Smart way of Apprehensions on IoT Security and Privacy

Thrisha V.S.[1] and Vikas Reddy. S[2]

[1]Dept of CSE, S J C Institute of Technology, Chickballapur, India
[2]Assistant Professor, Dept of CSE, S J C Institute of Technology, Chickballapur, India

Received 02nd March 2021, Accepted 10st April 2021

Abstract

Number of internet connected devices is increasing as IoT is getting more prevalent. Volume of data collected by IoT sensors is very high and requires considerable resources for data processing like analytics. Internet of Things (IoT) is now in its initial stage but very soon, it is going to influence almost every day-to-day items we use . The more it will be included in our lifestyle , more will be the threat of it being misused . There is an urgent need to make IoT devices secure from getting cracked . Very soon IoT is going to expand the area for the cyber-attacks on homes and businesses by transforming objects that were used to be offline into online systems . Existing security technologies are just not enough to deal with this problem . Therefore Many technologies and methodologies have been introduced to provide more security and privacy for IoT devices .

***Key words**: IoT, Sensors, Data and Internet*

The Internet of Things (IoT) has been identified as one of the most disruptive technologies of this century . It has attracted much attention from society , industry and academia as a promising technology that can enhance day to day activities , the creation of new business models , products and services , and as a broad source of research topics and ideas . High severity security attacks to CNI concepts , such as data leakage , spoofing , disruption of service (DoS/DDoS) , energy bleeding , insecure gateways , etc., target sensitive information/data can disrupt the system availability and energy resources , can cause system blackouts and also other indiscriminate and long-lasting damage . The effects of these security issues may cause major interference to the operation of services (e.g. public transportation networks can be targeted to cause chaos during peak travel periods , attacks to power grids can result in wasting huge amount of energy and a possible blackout of the system , etc.) and therefore , require immediate attention .

Nowadays , the IoT as a buzzword is widely known , subsequent industry applications related to the IoT will arise , for example cyber-transportation systems (CTS), cyber-physical systems (CPS), and machine-to-machine (M2M) communications . As to the security , the IoT will be faced with more severe challenges . There are the following reasons: 1) the IoT extends the 'internet ' through the traditional internet , mobile network and sensor network and so on , 2) every 'thing ' will be connected to this 'internet ', and 3) these 'things ' will communicate with each other . Therefore , the new security and privacy problems will arise . We should pay more attention to the research issues for confidentiality , authenticity , and integrity of data in the IOT . Nowadays , the IoT as a buzzword is widely known , subsequent industry applications related to the IoT will arise , for example cyber-transportation systems (CTS), cyber-physical systems (CPS), and machine-to-machine (M2M) communications . As to the security , the IoT will be faced with more severe

Correspondence
Thrisha V.S. Dept of CSE, S J C Institute of Technology, Chickballapur, India

challenges . There are the following reasons: 1) the IoT extends the 'internet ' through the traditional internet , mobile network and sensor network and so on, 2) every 'thing ' will be connected to this 'internet ', and 3) these 'things ' will communicate with each other . Therefore , the new security and privacy problems will arise . We should pay more attention to the research issues for confidentiality, authenticity , and integrity of data in the IOT .

RELATED WORKS

[1] Pulse : An Adaptive Intrusion Detection for the Internet of Things . This paper signifies a brief description about emerging a new model that can forecast malicious behaviour and can notice hostile IoT junction on a network . Majorly very delicate individual data such as phone number , email address , codewords , passwords etc., is also provided over internet which is assembling them as a board for numerous attacks that take place through cybers . The information which we send from one device to another device has not been protected . To provide security to IoT devices , functioning of security management should be done in a proper way . One such security management declared here is Intrusion Detection Systems(IDS) which can progress the security reaction. Since IDS sensors can perceive network hosts and strategies, they can also be utilized to inspect the information that is existing inside the network packages , as well as to recognize the operating systems of services that are being manipulated . Here the foremost exploration has been undertaken to develop Pulse related IDS which will be functioned in two segments in which one of them regularly record the network traffic and it is generated automatically and protected by the log files . The other is used to deploy various outbreaks and additional malicious procedures such as web scrutinizing were systematized on the identical network however the system traffic was also documented .

[2] DEMO : An IDS Framework for Internet of Things, This paper signifies a brief description about Empowered by 6LoWPAN , Intrusion Detection System (IDS) for IoT by familiarizing current open code methodologies . In order to simplify this, an evolving technique represents an IDS background for IoT , authorized by IPv6 that has short control over the private area network (6LoWPAN) devices. It is a criss-cross code of behaviour that describes summarization and caption firmness mechanism and also it is a stimulating protocol which acts as a backbone for the recognition of IoT in a reserve controlled atmosphere and these strategies are susceptible to outbreaks that are obtained from both the wireless sensor networks and the Internet protocols . The projected IDS outline which comprises of a recording machine and an exposure engine has been combined into the system framework that is established inside the EU FP7 project 'ebbits ' and a crowding attack is originated by means of Graphical User Interface(GUI) that displays actual disruption probability of channels particularly planned and unifiedv by the Frequency Agility Manager (FAM). A penetration testing (Pen Test) system has been developedv to estimate the presentation of the applied IDS framework and this penetration testing outline is based on Metasploit . The tests conducted discovered that the projected outline indicates the positive consequences of confirmation of better-quality security in 6LoWPANs .

[3] Emerging "Cyber Hygiene " Practices for the Internet of Things (IoT): Professional Issues in Consulting Clients and Educating Users on IoT Privacy and Security , This paper signifies a brief description about today's computing technologies in workplaces and households (the latter including frequently changing passwords and installing malware protections). This paperv explores the various rolesv of healthv professionalsv, insurancev agentsv, marketersv, lawyersv, financial specialists , and other professionals who are working with clients and consumers during this period in which IoT devices are evolving rapidly and the IoT-produced data's privacy and other legal statuses are still murky . Roles of technology developers and implementers may also shift as IoT data are retainedv for an assortmentv of technicalv vand diagnosticv purposesv butv are laterv requestedv or subpoenaed for specific investigations or legal proceedings . The paper will also outlinev vthe needsv for inputv to publicv vpolicy discoursev by communications professionals who have some insights as to how IoT advances may impact their clients and society as a whole . In the near future , education and communications professionals may also empower households by designing instructional materials for use in establishing cyber hygiene routines and resolving IoT-related concerns .

[4] Authentication of IoT Device and IoT Server Using Secure Vaults, This paper signifies a brief description about Mutual authentication between IoT devices and IoT servers is an important part of secure IoT systems . Single password-based authentication mechanisms , which are widely used , are vulnerable to side-channel and dictionary attacks . In this paper , we present a multi-key (or multi-password)

based mutual authentication mechanism . In our approach , the shared secret between the IoT server and the IoT device is called secure vault , which is a collection of equal sized keys . Initial contents of the secure vault are shared between the server and the IoT device and contents of the secure vault change after every successful communication session . We have implemented this mechanism on an Arduino device to prove our algorithm is feasible on IoT devices with memory and computational power constraints .

[5] Ensuringv compliance of IoT devices with their Privacy Policy Agreement , This paper signifies a brief description about the study the security issues of IoT devices due to the sensitive information they carry about their owners . Privacy is not simply about encryption and access authorization , but also about what kind of information is transmitted , how it used and to whom it will be shared with . Thus IoT manufacturers should be compelled to issue Privacy Policy Agreements for their respective devices as well as ensure that the actual behavior of the IoT device complies with the issued privacy policy . In this paper , we implement a test bed for ensuring compliance of Internet of Things data disclosure to the corresponding privacy policy. The vfundamental approach used in the test bed is to capture the data traffic between the IoT device and the cloud, between the IoT device and its application on the smart-phone, and between the IoT application and the cloud and analyze those packets for various features. We test 11 IoT manufacturers and the results reveal that half of those IoT manufacturers do not have an adequate privacy policy specifically for their IoT devices. In addition, we prove that the action of two IoT devices does not comply with what they stated in their privacy policy agreement.

[6] Five Acts of Consumer Behaviour: A Potential Security and Privacy Threat to Internet of Things, This paper signifies a brief description about The existing security and privacy preserving solutions proposed for IoT-enabled consumer products overlook communal vact of a consumer behaviour. They lack support in case when IoT Consumers borrow , rent , gift , resale and retire their IoT-enabled electronic products . In this paper , we attempt to highlight IoT consumer's security and privacy violation through seemingly five different angles . We also speculate that IoT products or devices , even after their End of Life (EOL), i.e. "IoT waste ", could become an attractive gateway for cyber criminals to access private information . Consequently , we present some recommendations in this regard.

[7] Blockchain : A Game Changer for Securing IoT Data , This paper signifies a brief description about The safety of blockchain has its origin from cryptography which exploits the technology's dispersed nature that affords the fundamentals for its security. Blockchain technology comprises of four major mechanisms namely network of nodes, Distributed database system, Shared ledger and cryptography which helps in preserving the record of each and every operation performed on the network and these operations are implemented on the blockchain platform by considering three different domains called public, consortium area and private. IoT is profited by the services offered by the blockchain technology through APIs thatv are existing by the nodes of the network . In order to connect multiple block chains , if artificial intelligence is added to the IoT location that is connected to blockchain network it creates a Decentralized Autonomous Organization (DAO)which runs without considering human involvement . By increasing the safety of roads, cars and homes, to fundamentally improving the manufacture and consuming the products, IoT solutions provide valuable information and insights that improve the mode of working and implementing and this outcome depends on ensuring the integrity and confidentiality of IoT solutions and data while justifying cybersecurity risks.

[8] Blockchain Enabled IoT Edge Computing, This paper signifies a brief description about The distributed nature of blockchain do not depend on a central point of control and a lack of a single authority makes the system fairer and considerably more secure. The technique in which the information is documented onto a blockchain characterizes its most revolutionary quality and its value of decentralization. Edge computing is a dispersed Information technology (IT) architecture in which client data is managed at the margin of the network, as close to the initiating source as possible. The architectural model involves the components like blockchain network, client or requester, resource lender and worker nodes and as soon as the transaction application is successfully recognized by the blockchain network and the resource provider will start processing the job by appealing occupation of specific scripts on one of the worker nodes. It empowers analytics and information gathering to arise at the source of the data and it also helps to face numerous challenges like validation of results, Reward system, packaging and distribution. Blockchain based resource sharing solution can help edge and fog architecture to address their scaling requirements. Edge level video storage that has searchable indexed storehouse for the video content and a basic form of this use case is distinguishing the dissimilar objects that are existing in video settings by means of deep learning and image classification techniques and this processing will be executed over worker nodes given by resource providers.

[9] When Internet of Things Meets Blockchain:

Challenges in Distributed Consensus, This paper signifies a brief description about IoT and blockchain ledger security is a method that is used to track-and-trace an IoT aided dispersal mechanism which comprises of two chief distributed consensus called Proof of Work (PoW), Proof of Stake (PoS) which plays a dynamic role in sustaining a solitary version of blockchain register among all manipulators. A DAG (Direct Acyclic Graph) based consensus mechanism utilises MCMC(Monto Chain Monto Carlo)tip selection algorithm which permits the operators to interpolate their blocks into blockchain at any period, as long as they process their previous transactions and it consists of two distinctive approaches named as Tangle and Hashgraph. Tangle is a DAG grounded distributed ledger for recording communications and it agrees assorted divisions eventually got merged into the chain, resulting in broad output and whereas hashgraph privileges to support an extra data which outfits a gossip protocol that is somewhat blockchain does not do and this is the segment where nodes reciprocate the statistics with other nodes to build and to resolve the data production.

[10] A Survey on Consensus Protocols in Blockchain for IoT Networks, This paper signifies a brief description about the several circumstances on which the usage of blockchain can afford the declaration of data integrity and safety for IoT networks and it can be explained by concentrating on recently functioned consensus and that is parallelly associated with the real time instances of resource controlled IoT devices and its network. The implementation is basically conducted on various means of recent consensus protocols in blockchain for IoT networks which in result delivers the respectable alternate resources in which the secluded blockchain and tangle can be employed. When compared to all the previous implementations revealed are appeared to be justifying and satisfactory since they get interrelated to the current limitations of blockchain technology and all these constraints says about the various mechanisms on which high security can be provided to IoT devices through the platform of blockchain. Since, no constraint has been successfully justified the current usage of all the limitations on IoT devices and to overcome this situation a blockchain based IoT platform has to be planned which is based on large scale with less potential. This mode of utilization of IoT network on blockchain should be operated and organized by a framework which consists of a cross framework, that means a framework that consists of numerous existing methodologies by which the security can be provided in a high range or it should contain newly developed framework with modernized methods that are applicable for constrained IoT devices and its networks.

SL No	Technology	Advantage	Disadvantage
1	Intrusion Detection	Quick detection	No impact on traffic
2	Denial-of- service	Highly reliable	Loss of reputation
3	User education	Highly scalable	Increased accessibilty
4	Secure vault	High security	More attacks
5	GDPR	Better data security	High cost
6	DVR	High security	Low storage capacity
7	Blockchain	Good stability	Not ind estructible
8	Edge Computing	High speed and latecncy	High attacks
9	DAG	High speed and reliablity	Less scalable
10	Hyperledger	Good performance	Complex architecture

CONCLUSION

In this paper we have discussed different techniques to secure IoT devices. The best and shortest solution which we have obtained to solve the problem of security in IoT devices is providing several circumstances on which the usage of blockchain can afford the declaration of data integrity and safety for IoT networks and it can be explained by concentrating on recently functioned consensus and that is parallelly associated with the real time instances of resource controlled IoT devices and its network. Apart from this various solutions have been provided to solve different security issues.

REFERENCES

[1] Eirini Anthi, Lowri Williams ,Pete Burnap, “Pulse: An Adaptive Intrusion Detection for the Internet of Things” in School of Computer Science and Informatics, Cardiff University,2012.

[2] Prabhakaran Kasinathan, Gianfranco Costamagna, Hussein Khaleel, Claudio Pastrone, Maurizio A. Spirito,

" DEMO: An IDS Framework for Internet of Things" in CCS'13, November 4–8, 2013, Berlin, Germany. ACM 978-1-4503-2477-9/13/11.
[3] Jo Ann Oravec, "Emerging "Cyber Hygiene" Practices for the Internet of Things (IoT): Professional Issues in Consulting Clients and Educating Users on IoT Privacy and Security" in 978-1-5090-3042-2/17/$31.00 (c) 2017 IEEE.
[4] Trusit Shah ,S. Venkatesan, "Authentication of IoT Device and IoT Server Using Secure Vaults", in 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering.
[5] Alanoud Subahi, George Theodorakopoulos "Ensuring compliance of IoT devices with their Privacy Policy Agreement" in 2018 IEEE 6th International Conference on Future Internet of Things and Cloud.
[6] Wazir Zada Khan1, Senior Member, IEEE, Mohammed Y Aalsalem1, Member, IEEE, Muhammad Khurram Khan2, "Five Acts of Consumer Behaviour: A Potential Security and Privacy Threat to Internet of Things" in 2018 IEEE International Conference on Consumer Electronics (ICCE).
[7] Madhusudan Singh, Abhiraj Singh, Shiho Kim, "Blockchain: A Game Changer for Securing IoT Data", 2019.
[8] Pankaj Mendki, " Blockchain Enabled IoT Edge Computing", in ICBCT 2019, March 15–18, 2019, Honolulu, HI, USA © 2019 Association for Computing Machinery. ACM ISBN 978-1-4503-6268-9/19/03.
[9] Bin Cao, Yixin Li, Lei Zhang, Long Zhang, Shahid Mumtaz, Zhenyu Zhou, and Mugen Peng, "When Internet of Things Meets Blockchain: Challenges in Distributed Consensus".in 0890-8044/19/$25.00 © 2019 IEEE.
[10] Mehrdad Salimitari and Mainak Chatterjee, " A Survey on Consensus Protocols in Blockchain for IoT Networks" in arXiv:1809.05613v4[cs.NI] 19 june 2019.

Please cite this article as: Thrisha V.S. and Vikas Reddy. S (2021) **Study on Smart way of Apprehensions on IoT Security and Privacy .** *International Journal of Recent Research and Applied Studies*, 8, 4(6), 59-63.