International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 7, Issue 1, No 1, 2019. ISSN: 2348-6600
Reference ID: IJCS-349 PAGE NO: 2345-2351

A survey on security forthe Internet of Things using Particle Swarm Optimization

Dr.B. Indrani, Mrs. Ilakkiya

Assistant Professor, Department of Computer Science, Madurai Kamaraj University, Madurai.

Research Scholar, Department of Computer Science, Madurai Kamaraj University, Madurai.

indrani.phd@gmail.com, phd.ilakkiya@gmail.com

Abstract- Smart City paradigm is one of the emerging domain, in which the Internet of Things (IoT) has fueled the process raised widespread concern within the whole ICT community. The term IoT refers to the connecting sensors, man and the physical things with the assistance of networks or different communication technologies to build intelligent things to things network. The rapid large-scale deployment has faced several challenges, particularly in security and privacy problems for sensible, connected and mobile IoT devices and platforms. IoT has various characteristics from the conventional communication networks, associated with its specific options and threats. Especially, finding a solution for the security-related issues, when IoT nodes like physical things, client, servers, and objects with accuracy, confidentiality, reliability and novelty certification, and authorized. Of course, it's conjointly necessary to strike a balance between the supply and therefore the security and privacy protection for IoT. The special issue can specialize in the IoT devices and platforms with high security and privacy-protective technologies for dashing up technological progress and attracting new researcher's considerations regarding the growth during this field. In this paper, they discussed various challenges that are faced by IoT security are highlighted.

Introduction

IoT has become a vital part of the present era. It provides associate degree easy life with higher flexibility, easier management, and wide property through several applications. Security threat in IoT [5] has risen to potential vulnerabilities causes physical and financial loss. Being common and easier targets owing due to minimum consumption of power and lower processing capabilities, advanced firewall and availableness for service, IoT devices need advanced higher security to face different cyber attacks.

These rapid changes in technology have made tremendous implications for de-centralized manufacturing are expected to trigger the computer revolution. IoT devices have made a great impact on each and every customer. Telstra telecommunication from Australia said that the typical [7] Australian house in 2017 had thirteen web-connected devices by 2021 a typical home will occupy over 30%. It's forecasted that the collective worth of the sensible home one billion

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 7, Issue 1, No 1, 2019. ISSN: 2348-6600
Reference ID: IJCS-349 PAGE NO: 2345-2351

dollars of market penetration in the year 2021.

In this paper [16] they covered the potential security measures to stop the vulnerabilities attacks from cyber-criminals with added measures. They adopted 3 layer security in terms of device, communication and server security to protecting the attacks.

The researcher designed a cooperative resource planning for energy inhibited applications in a consistent and fault-free performance. Task scheduling algorithm with particle swarm optimization [1] helped to solve the resource allocation problem in diversified IoT based environment. They considered various metrics for measure the satisfy the standard in terms of service in terms of output and delay of task scheduling was considered.

IoT has many advantages [2] on devices handling, they are potential downsides that may be created once improper implementation of protocols was utilized to communicate the data among networks. As many thousands of physical devices hook up with the net daily, it's necessary to live the protection of those connections. Not uncommon to seek out, a preferred trade-off exists between security-implementation price and actual security levels. They analyzed enhanced security implementation of connected house electronic devices for higher safeguard the transmitted knowledge.

Speedy development in the embedded technology, the IoT becomes the foremost centered analysis trend [3] within recent years. It's a combination of technology into mobile crowd sensing networks ends up in several security challenges. Data privacy and genuineness are the two key security considerations in any IoT-based applications. Focal on these security problems, they designed a fresh cryptographic protocol to satisfy the present challenges.

The market predicted that in future the IoT will create a more than value one billion $ annually increased from the year 2017 onwards. From this concluded that as a result of data production at this stage are forty-four times bigger than in the year 2009, indicates the need for a speedy increase within the huge volume, rate and variety of knowledge. So IoT based smart sensible system generates a huge volume of knowledge typically known as big data analytics for processed by conventional data processing algorithms and applications. The problem was storing, process and visualizing this vast knowledge generated from IoT based mostly system was identified. However, there are extremely helpful data and then several potential values are hidden within the vast volume of IoT based mostly device knowledge. IoT based mostly device knowledge has gained a lot of attention from researchers in care, bioinformatics, data sciences, policy and call manufacturers in governments and enterprises. Nowadays, AI ways play a big role in varied environments as well as business observance, health care applications, manufacturing process development, research and development, share market prediction, business method, industrial

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 7, Issue 1, No 1, 2019. ISSN: 2348-6600
Reference ID: IJCS-349 PAGE NO: 2345-2351

applications, social network analysis, weather forecasting analysis etc.

The vast growth in IoT and cyber-physical systems (CPS) has made wider applications are developed and deployed in recent days. They matched the homogenous and heterogeneous application requirement in IoT and CPS in several resources constrained IoT devices are deployed, within which privacy and security have emerged as a giant challenges as a result of they need not been designed to possess effective safety features.

They are several security solutions are developed so far for internet-based applications, there major considerations relating to the resource-constrained environments in IoT for encryption, decryption, privacy and vulnerabilities attacks. To deal with these privacy-related security issues are challenging for researchers to develop resource inhibited environments in IoT.

Review of Literature

In IoT to face the cyber attacks with the help of safeguard, the Hardware-assisted defense mechanisms [5] were used. These did not want any additional layer of protection, especially in traditional software. To supply comprehensive security, several challenges like domain and over power consumption.

IoT helps to monitor and control the various physical objects. In this paper [6] suggested three-layered security implementation for the IoT operating mechanism. In this paper, the potential high-level security implementation has been prompt at the device level, communication level, and system level. They added the mandatory implementation of security observance and modify the protection implementations from time to time to forestall the attacks in IoT.

The protocol relies on two schemes namely encryption scheme and verifier signature scheme. The verifier signature scheme sends the signature without sends the original message. And this scheme [3] has so many advantages when compared with other related protocol schemes. This scheme was applied in various crowd sourcing applications for data authenticity.

The major problem in the existing system was a high process pairing price and unbalanced ROM [4] usage. Implementation result shows that the conventional security algorithm was an in-efficient and vulnerable attack made on the message and ID of the user. They adopting cost cut exercise in terms of quadratic residue that has signature verifies IoT devices with the help of cloud computing.

The planned signature does not con template ROM storage, and it's secure within the commonplace model supported the planned modified interactive quadratic residuosity assumption. Performance analysis and comparisons make sure that our theme is additional economical than earlier connected schemes.

Most of the internet-connected devices have poor in-built security measures and might

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 7, Issue 1, No 1, 2019. ISSN: 2348-6600
Reference ID: IJCS-349 PAGE NO: 2345-2351

reveal non-public knowledge and data that is harmful to customers. It's the same that privacy and security considerations are closely connected because the potential for security breaches has important ramifications for the privacy risks related to the planned theme.

The study [7] suggested that the present generation of IoT devices is susceptible to attack in a numerous way. It's a fancy downside, and there don't seem to be any "single bullet" solutions to create IoT devices safer or safer. This text sets the platform for a dialogue between customers, suppliers, regulators, and insurers of IoT devices to develop a suitable method to overcome this challenge.

The review [8] based on the security attacks in IoT supported by
machine-learning (ML) techniques are further classified as supervised, semi-supervised and reinforcement learning (RL).This article mainly focused on malware identification, secure offloading and authentication control to protecting the valuable data.

IoT based systems were more complicated objects that typically require de-centralized management. Swarm Intelligence [9] systems are de-centralized self-organized algorithm helped to resolve complicated issues with dynamic properties, incomplete data, and restricted computation capabilities.

Integrate AI and IoT networks [10]are changing into a requirement for achievement in today's digital ecosystem that tends to businesses should move speedily to facing the challenges of combining AI and IoT take part in a catch-up in years to come back. The evolution of IoT and what however best will play a key in combining with AI will do for the business in the future.

Many of the IoT research work is based on the applications, routing and device search services. This work focused on building, implementing, and evaluating routing rul e for high scale wireless device networks for channel allocation. Particle Swarm improvement (PSO) combined with the gravitative search algorithm [12] was used to allocate the best channel bandwidth to all ways among the total allotted destination.

There are so many challenges faced [13] by IoT particularly in investment made on hardware. These devices carry with it energy modules, power management modules, RF modules and sensing modules.

Real-time chat with home appliances are sensible older dc motor over social
network from anyplace within the world. These devices communicate the current trend with Artificial Intelligence (AI) will give a choice. To produce a world wherever not solely humans, however devices even have their own social network platform wherever they able to communicate to performa certain action, similar to a person do a favor and monitor them with potency.

This paper [14] designed a novel paradigm which controls over the network with the help of AI. Social network like Face book, Twitter, Google Assistant, if needed, they able to change our alternative that is offered by AI. The paper brings associate approach towards bridging

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 7, Issue 1, No 1, 2019. ISSN: 2348-6600
Reference ID: IJCS-349 PAGE NO: 2345-2351

the gap between social networks and IoT, to connect the individuals with physical devices called as Social Internet of Things.

This paper [15] mainly focused on the attack model in IoT systems security solutions supported ML techniques has supervised, unsupervised and reinforcement learning. The machine learning was mostly based on authentication, access control, secure loading and malware virus detection for the purpose of safeguard the information privacy.

Smart cities are designed with the help of IoT technology that permits a massive range of devices to attach with one another. These physical devices are manufactured by different makers with different standards, that confront various interactive management
problems. Moreover, these devices can turn out giant amounts of information and expeditiously analyzing these data for intelligent services. They designed a completely unique artificial intelligence[16] based linguistics IoT designed to integrate heterogeneous IoT devices to support intelligent services.

There are various applications performed by IoT typically to find out skin cancer with a higher level of accuracy detected with the help of Support vector machine and PSO algorithm. It also creates Twitter Doctors Community [11] to send the patient's health condition to the dependent person. It recommends acceptable treatment for the patient and might act with patients with the help of IoT and conjointly enhancing security based mostly health care system within which the patient's condition is measured in a secure manner.

Another classic example of IoT in online shopping [17]is used for automated packing system. 3-D adaptive PSO algorithm is used for packing the products. It consists of four layers namely conversion, decision making, package management and application.

Conclusion

Hardware aided protection for the secure the IoT devices is still a challenge for further improvement in terms of their importance and flexibility over time and across multiclass attack vectors. And arose some question related to the security of IoT is needed to enhance and style acceptable security mechanisms with high accuracy and low overhead for light-weight IoT applications. In intrusion detection, the unsupervised learning algorithm misses the detection rates that don't seem to be negligible for IoT systems. Both supervised and unsupervised learning an algorithm fails to identify the intruder's attacks due to oversampling, inadequately trained data and dangerous feature extraction. They needed more reliable and secured security for backup and use the data.

References

1. Fadi Al-Turjman, Mohammed Zaki Hasan, Hussain Al-Rizzo, "Task scheduling in cloud-based survivability applications using swarm optimization in IoT", John Wiley & Sons, - *Trans Emerging Tel Tech*. 2018, pp. 1-20.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 7, Issue 1, No 1, 2019. ISSN: 2348-6600
Reference ID: IJCS-349 PAGE NO: 2345-2351

2. Erick Buenrostro, Daniel Cyrus, Tra Le & Vahid Emamian, "Security of IoT Devices, Journal of Cyber Security Technology", 2018, pp.1-13.

3. ArijitKarati, G. P. Biswas, "Provably secure and authenticated data sharing protocol for IoT-based crowdsensing network", *Trans Emerging Tel Tech*. 2018, pp. 1-22.

4. Manoj Kumar, Harsh Kumar Verma, GeetaSikka, "A secure lightweight signature based authentication for Cloud-IoTcrowdsensing environments", *Trans Emerging Tel Tech*. 2018, pp.1-15.

5. Fahim Rahman, Mohammad Farmani, Mark Tehranipoor, and YierJin, "Hardware-assisted Cybersecurity for IoT Devices", IEE 18th International Workshop on Microprocessor and SOC Test and Verification, 2018, pp. 51-56.

6. Tamanna Siddiqui and SaifSaffahBadrAlazzawi, "Security of Internet of Thing", International Journal of Applied Science – Research and Review, Vol.5, Issue No.2:8 ,2018, pp. 1-4.

7. Vijay Sivaraman, Hassan HabibiGharakheili, Clinton Fernandes, Narelle Clark, and Tanya Karliychuk, *"Security and Privacy Implications",*IEEE Technology and Society Magazine, 2018, pp. 71- 79.

8. Liang Xiao, Xiaoyue Wan, Xiaozhen Lu, Yanyong Zhang, and Di Wu, "IoT Security Techniques Based on Machine Learning", IEEE SIgnalProcESSIngMagazInE, 2018, pp. 41-49.

9. OuardaZedadra, Antonio Guerrieri, Nicolas Jouandeau, GiandomenicoSpezzano, Hamid Seridi, Giancarlo Fortino, "Swarm intelligence-based algorithms within IoT-based systems: A review", *Journal on Parallel Distributed Computing, 2018, pp. 1-38.*

10. VenkateshNaganathan, Rajesh Rao K, "The Evolution of Internet of Things: Bringing the power of Artificial Intelligence to IoT, its Opportunities and Challenges", *International Journal of Computer Science Trends and Technology (IJCST) – Volume 6 Issue 3, May - June 2018, pp. 94-108.*

11. X Josephine Meena and S Indumathi, "A secure IoT based skin cancer detection scheme using support vector machine and particle swarm optimization algorithm", *International Journal of Engineering Research and Science & Technology, Vol. 6, Issue no. 2, 2017, pp.30-40.*

12. ShilpaBisen,PSO-GSA Tuned Dynamic Allocation in Wireless Video Sensor Networks for IOT", International Research Journal of Engineering and Technology, Vol: 4 IssueNo.07, 2017, pp. 1949-1954.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 7, Issue 1, No 1, 2019. ISSN: 2348-6600
Reference ID: IJCS-349 PAGE NO: 2345-2351

13. Ajish K S, Athira Prem, Reshma R, Minu Lalitha Madhavu, "Survey on Security Issues of Internet of Things (IoT)Devices", International Research Journal of Engineering and Technology, Vol 4 Issue no 11, 2017, pp. 1297-1299.

14. Anjan Chatterjee, "Artificial Intelligence based IoT Automation: Controlling devices with Google and Facebook", International Research Journal of Engineering and Technology, Vol: 5 Issue No.4, 2018, pp. 1437-1442.

15. Liang Xiao, Xiaoyue Wan, XiaozhenLu,Yanyong Zhang, Di Wu, "IoT Security Techniques Based on Machine Learning", arXiv:1801.06275v1, 2018, pp. 1-20.

16. Kun Guo, Yueming Lu, Hui Gao and Ruohan Cao, "Artificial Intelligence-Based Semantic Internet of Things in a User-Centric Smart City", MDPI *Sensors* 2018, pp. 1-22.

17. Tzuu-Hseng S. Li, Chih-Yin Liu , Ping-HuanKuo, Nien-Chu Fang, Cheng-Hui Li , "A Three-Dimensional Adaptive PSO-Based Packing Algorithm for an IoT-Based Automated e-Fulfillment Packaging System", IEEE ACCESS, 2017, pp. 9188- 9205.