International Journal of Psychosocial Rehabilitation, Vol. 24, Issue 09, 2020
ISSN: 1475-7192

SECURING HAZARDOUS IoT SENSOR DEVICE WITH PATCH MANAGEMENT USING TWO PHASE AUTHENTICATION

A.Suresh1, Prof.G.T.Naidu2

[1]*Research Scholar, Rayalaseema University, Kurnool, Andhra Pradesh, India., allu.sbabu@gmail.com*
[2]*Dept.Of.Physics, Sri Krishnadevaraya University, Anantapur-515001, Andhra Pradesh, India, goneguntlanaidu@yahoo.co.in*

Abstract:

Security in IoT security is the novelty zone concerned about defending linkeddigital media and systems in Internet of things (IoT). IoT comprised with adding web ease of use to an agreement of consistentbuildin gadgets, with advanced mechanical machines, items, creationswith add on's digital content. Every "thing" as digital media is given an identifier and the ability to naturally transform information over information system. Permitting digital gadgets to edge with the web frees them up to various genuine weaknesses on the off probability that they are not properly secured. Secure IoT has been converted into the examination subsequent to various majorevents where a characteristic IoT gadget was utilized to invade and assault the bigger system. Actualizing hazardous safety efforts is basic to assurance the wellbeing of IoT gadgets associated with them. This work addresses IoT patch management is implemented in hazardous IoT devices that enhances automatic security as it seems to be crucial. The vulnerabilities in IoT rise when the IoT devices are updated. Using patch management the IoT devices uses two phase authentication for ensuring the devices are secured and free from vulnerabilities. The security is evaluated based on the device security implication and the device performance is degraded when there is a security flaw.

Keyword: *IoT security, Patch management, IoT gadgets,Two phase authentication*

1. INTRODUCTION

The difficulties faced with IoT gadgets needs advanced security measures that have its head and tail towards current information security. Since the latest IT trends has security breaches and need to be improvised as the extended security is implemented in hazardous devices. Furthermore, the focus of IoT in the current IT trends has its own market and the extended security reaches the peaks creates a new pathway in information security.

A significant approach in IoT security[1] based on its utilization of current security measures with password based which has its own demerits. Despite changing password frequently is considered to be one of the approaches in security measures and its not sufficient for extended security.

Another basic feature of the IoT media based on its security doesn't hold firm secure measures by highlighting its advance features. An instance with IoT security breach, the sensor is validated with the basic secure principles that cut hold its viable breach and provide instant security for the device. The accessibility of the sensor is also bounded with the secure features that provide overall accessibility. Building a secure network for IoT makes the system more perfect and doesn't need to be secured individually as block.

2. Survey

Associating digital media resources with intrinsically deals with latest and future IoT [2] network is another security challenge. Replacing the changing IoT and its framework that is associated with the innovation is cost-restrictive and it is replaced by the huge numbers of benefits will be retrofitted with savvy sensors. Nevertheless, as inherited and

Received: 10 Jul 2020| Revised: 20 Aug 2020| Accepted: 02 Sep 2020

extensive IoT resources that presumable have not been refreshed or ever had protection from present day dangers, the assault surface is extended. Such data's are stored in vast IoT cloud store [4].

While dealing with current secure feature and its updates, numerous frameworks are incorporatedwith the assistance of time span. For inherit and new resources, security may misswhen addon assistance isn't included. In extent, the increasing IoT gadgets[5] remain in the system for a long time that holds valid security measures that are tested simultaneously.

IoT security is likewise under attackwith the nonexistence of advanced industry-acknowledged principles whereasabundant IoT securities structures are prevails and exist but none proven to be secure enough for providing utmost security. Vast industries and its organizations have their own meticulous principles, excluding hazardous sections, for example, the recent IoT sensor in hazard section and its extension and exclusion, contradictory guidelines from industry establishment. The collection of these guidelines makes it hard for the current frameworks and in addition it guaranteesmutual operation between the devices.

The technical and operation innovation of the various security enhancements in current technological growth paves way for the trust and enforcement and finally provide assurance for extending the security zones once proven to be secure and viable.It is also referred as secure domain extension system where a secure zone is extended to other with the same principles by considering the amount of hazard in that particular zone.

3. Existing Method

The security experts already stated the growth of IT sectors and the inventions to be happened in the future gadgets. As the growth of IoT [3] which is also a notable part in the future innovations confirms the statement and the extensive need of security in this field. The need of secure mechanism justifies even further when the electronic Medias are scammed and published with unwanted content to loot the information. As the IoT inventions are widespread and every device in future has IoT sensor and this makes the statement more clear about the need of security in IoT sensor.

In 2010, for instance, analysts uncovered the Stuxnet infection that was utilized to genuinely harm countrymen axes, with assaults beginning yet with the essential assault happening between years. Frequently thought to be probably the most punctual of IoT assault, Stuxnet is intentedto administrative and information control obtaining secure frameworks in mechanical power frameworks, utilizing malware to taint guidelines sent by operational rationale regulators.

The extensive Attack on modern digital media and its systems have just preceded, with malware, and few extensive attack on its system owing to its mechanical IoT frameworks.

The very first botnet and its impact happens with Inc Proof Point is identified by the IT experts declares the cost will be massive if it is extended without further control. Nearly 20% of the attack happens with digitial media irrespective of the impact with the PC interconnection.

The security specialist Charlie and Chris experimented this attack of the device fixed in a jeep by hacking its radio frequencies without driver intend. They also controlled vehicle wipers along with the climatic condition change. They concluded that when this control accessing is possible then the attack is also extended further to control overall devices. Also they have stated that when this attack is extended to widespread of overall vehicle control without user knowledge it leads to major hazard and using their experimental ways such attacks are saved in order to avoid the extensive of the attack.

Received: 10 Jul 2020| Revised: 20 Aug 2020| Accepted: 02 Sep 2020

One of the biggest BoTNet during the earlier stage of the impact is “Mirai” which attacked major French site on 2016 Septemeber. The attack happens with the major occupancy of 650 GB of data entering into the site and increasing 20% every seconds in order to take overall control. It is identified when analysis examine the server using DNS namespace conflict and further restricts its flows by controlling to spread to its nearby servers. When such attack happened the site remain non accessible for certain amount of time period and gives a clue how this Bot worked.

4. Proposed method

Securing IoT is a great challenge in any industry right from home automation extended till automation that happens with overall device control. The serious impact happens with the overall secure framework that does the job of controlling and transforming information exchange.

An assault debilitating the brakes of an associated vehicle, for instance, or on an associated wellbeing gadget, for example, an insulin siphon hacked to manage an excessive amount of patient consumption can be hazardous. Similarly, the assault on a defreeze framework lodging medication that is checked by its secure framework that destroys the practicality medication if warmthvacillate. Essentially, theattack on basic foundation - an oil well, vitality lattice or water flexibly - can also be more hazardous.

Different assaults, in any case, can't be thought little of. For instance, an assault against keen entryway locks might permit a robber to enter a shrewd home. Or then again, in different situations, the attack on 2013 executes security havoc in data penetration by declaring the malware by extending with the overall framework dealing with the current situation in order to extend its support.

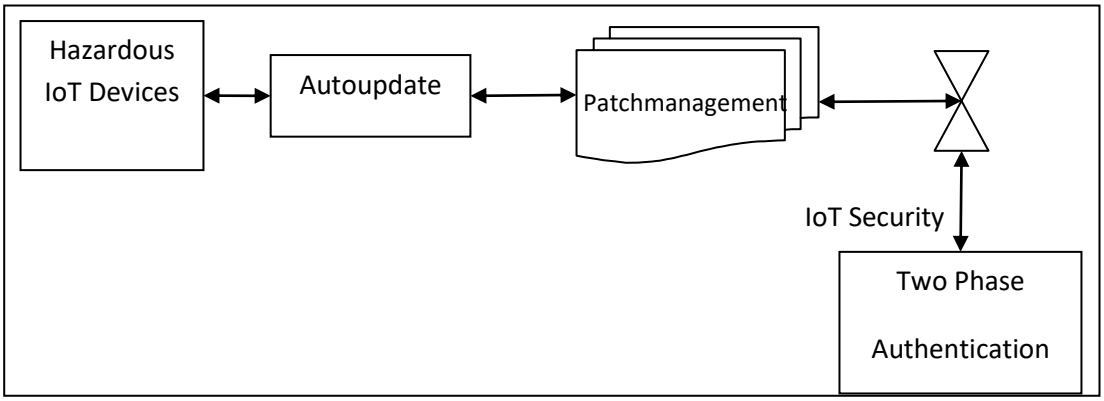

Figure 1: Auto-update in patch management

Figure 1 elaborates auto-update using patch management enclosing two phase authentication with IoT security mechanism. All IoT devices uses patch management for security enhancement that applied only at auto update. This validates all IoT devices with advanced security for providing security for the device along with its data.

The secure IoT[8] and its strategies differ based on its application and the environmental factors. In order to declare the system to be secure, the security measures should start from the sensor production level by carefully designing the system that it is meant to be. The following are the security measures to be done while producing IoT sensor for hazard protocols. The dynamic testing was done then and there in order to be the system to work safer for various attacks. With the proper

Received: 10 Jul 2020| Revised: 20 Aug 2020| Accepted: 02 Sep 2020

secure coordination and advancement more secure enhancement[6][7] are implemented in the system that works on various secure ground and with holds attacks that damages system and produce hazard.

The two phase authentication works as follows

Phase 1: Device identification

The Hazardous devices are identified using pre embedded id like unique number along with device certificate with trust module using platform. In this work, Hazardous work needs more technological growth and IoT favors this technology to avoid the behavior aspects of IoT devices are identified with the device class. In extend the device class information generates hash file.

Phase 2: Ensuring security while device update

When the device is identified and verified, the authentication is set for ensuring the device requested for update. When the devices are recognized using authentication, the updation happens with user request. This avoid overall vulnerabilities happens when the device is updated automatically. Automatic update is the tedious process to avoid vulnerabilities.

5. 5. Results

$$HDIoT = \sum_{i=1}^{n} \sum_{j=i}^{m} D_i \quad [1]$$

$$SecHDIoT = \sum_{i=1}^{n} \sum_{j=i}^{m} D_i * S_j \quad [2]$$

Eqn [1] elaborates secure IoT hazardous device for enhancing secure device channels and Eqn [2] extends the security using two phase authentication for ensuring automatic device update for checking double check for providing at most secure channel.

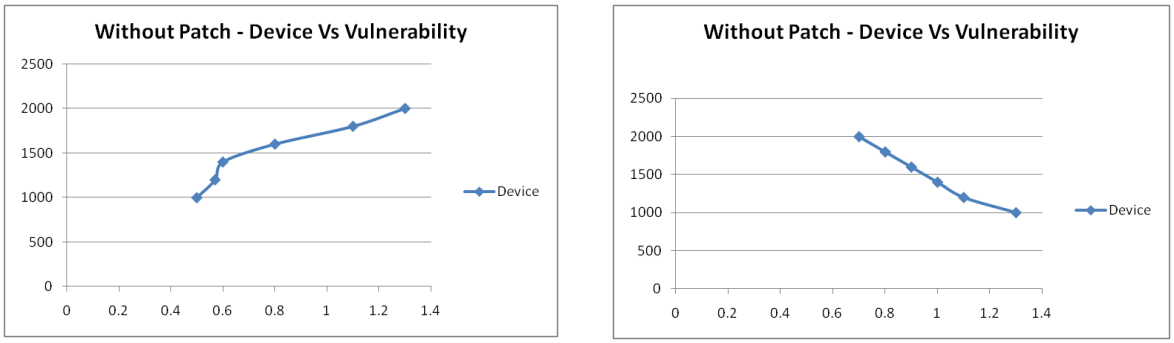

Figure 2: Comparison with / without patch

Figure 2 compares the difference between device and its vulnerability as the vulnerability decreased by increase in IoT device number using proposed approach using hash functions.

6. Conclusion

The work proposes a new style of secure mechanism for implementing security in automatic device update using two phase authentication as the secure lies only with application usage. Patches are compared with the automatic mechanism

for avoiding automatic device upgrading with secure mechanism. Such mechanism will enhance more security even when there is more increase in device number.

7. Reference

1. Khan, Minhaj Ahmad, and Khaled Salah. "IoT security: Review, blockchain solutions, and open challenges." Future Generation Computer Systems 82 (2018): 395-411.
2. Hassan, Wan Haslina. "Current research on Internet of Things (IoT) security: A survey." Computer networks 148 (2019): 283-294.
3. Hassija, Vikas, et al. "A survey on IoT security: application areas, security threats, and solution architectures." IEEE Access 7 (2019): 82721-82743.
4. Li, Xiang, et al. "Enhancing cloud-based IoT security through trustworthy cloud service: An integration of security and reputation approach." IEEE Access 7 (2019): 9368-9383.
5. HaddadPajouh, Hamed, et al. "A survey on internet of things security: Requirements, challenges, and solutions." Internet of Things (2019): 100129.
6. Zhang, Jiliang, and Gang Qu. "Physical unclonable function-based key sharing via machine learning for IoT security." IEEE Transactions on Industrial Electronics 67.8 (2019): 7025-7033.
7. Hou, Jianwei, Leilei Qu, and Wenchang Shi. "A survey on internet of things security from data perspectives." Computer Networks 148 (2019): 295-306.
8. Li, Fangyu, et al. "System statistics learning-based IoT security: Feasibility and suitability." IEEE Internet of Things Journal 6.4 (2019): 6396-6403.

Received: 10 Jul 2020| Revised: 20 Aug 2020| Accepted: 02 Sep 2020