WJCMS

Wasit Journal of Computer and Mathematics Science

Journal Homepage: https://wjcm.uowasit.edu.iq/index.php/WJCM

e-ISSN: 2788-5879 p-ISSN: 2788-5879

Escalation of Security and Privacy in Internet of Things using Advanced IPv6 Based Security Mechanism

Prof.Dr.Sundresan Perumal[1,*]

[1]Information Technology Department, USIM University, Malaysia

*Corresponding Author: Prof.Dr.Sundresan Perumal

DOI: https://doi.org/10.31185/wjcm.Vol1.Iss1.7
Received: December 2020; Accepted: February 2021; Available online: March 2021

ABSTRACT: Kevin Ashton coined the phrase Internet of Things in 1999 with high performance implementation for corporate and social world. Thanks to the success of high-performing Internet of Things (IoT) whereby the tags and sensors are the foundation for IoT implementation of radio frequency identification with enormous implementation patterns. Real world objects and systems that are remotely managed using program- based tools may be outfitted with RFID tags. Radio frequency recognition devices may identify objects and sense information. Very thin micro-sized RFID chips that can attach remotely are built. The internet of things will cross over USD 267 billion in 2020. According to the report by Gartner, there would be $273 billion linked devices around the world in 2014. The quantity, which is equal to 8.4 billion goods, is 31% more than last year. This study examines security and productivity in the IoT. It is very popular to use Internet of Things (IoT) in robotics because of sensor sensors, advanced wireless technology and use of software programming. Both wireless IP-based systems come with built-in GPS modules. The utility of smart cities and home automation was increasingly accentuated by the appearance of vast databases of smart IP-based sensors. Within the scope of this study, one of the goals is to establish simulation trends that can cover protection weakness of the Internet of Things. In the novel, the simulation processes were implemented through Contiki Cooja and CupCarbon. The modern age is greatly being affected by impossibly sophisticated technical devices. It is treated under the umbrella of Internet of Things (IoT). Several applications are commonly using IoT linked technologies to a broad variety of purposes. IoT contains many other concepts such as universal computing, widespread computing, ambient computing, among several others. The work presents the implementation using high performance framework for the security in the IoT environment using security mechanism on IPv6.

Keywords: Internet of Things, IPv6, Contiki Cooja, IoT Security

1. INTRODUCTION

There are a number of problems that network protection administration needs to address. With the advent of Internet of Things, considerable work has been undertaken to establish protection and privacy measures as the networks became increasingly fragile. IoT vulnerabilities can be targeted using various forms of attacks at different stages. In this way, hackers will disrupt or incapacitate the Internet of Things or the IoT network. The attacks are top priority because they impact the whole network with the attacks at computer networks have been widespread in recent years [1].

Denial of Service assault is a process where the network is clogged by the malicious message. Here, the unauthorized customers cannot connect the network facilities. This is one of the main facets that fits with an IoT situation. This form of attack is risky because it becomes Distributed Denial of Service (DDoS) since it is in a state of diffusion. This assault is performed from different positions [2, 3].

*Corresponding author: sundresan.perumal@usim.edu.ma

Sybil assault impacts vehicular network by losing a number of energy. The intruder uses the session to exploit the identification. There are malicious nodes that claim to be recorded or initial root. Sybil assault relies on the intruder to build separate nodes to play the part of itself. This attacks may be identified using resource partitioning, which operates on the presumption that cars have minimal energy. This problem can be solved using public key cryptography through using peer's public key to encrypt and decrypt info.

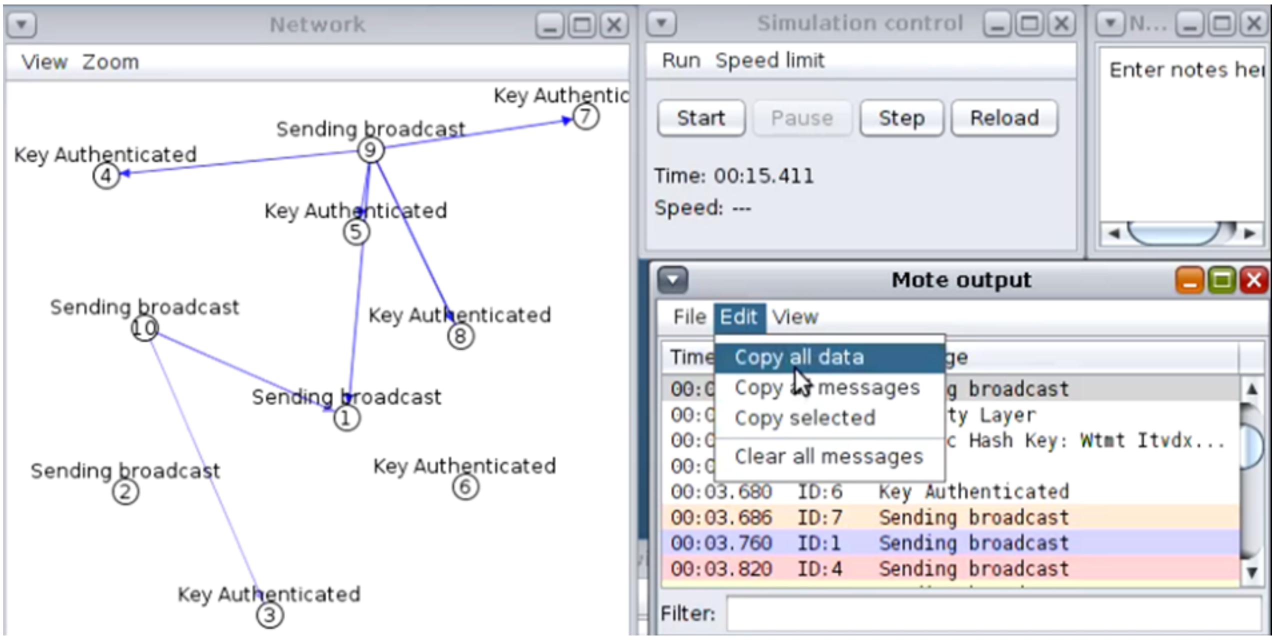
In this form of attack, the dissemination of messages happens via fake node. Any intruder will use the false identity to deliver the incorrect or harmful messages to any node without any suspicion. In such an attack, the identity of the system may be exploited to take the authentic and protected packets, which can be quite costly and catastrophic for the rest of the scenario [4].

Application Level Assault is a technique used in IOT that tamper the data and transfer to its target. Thus in IoV implementation, the free flow lane may be broadcasted as a congestion free lane. This traffic jam can be really heavy on that lane and can result in the disasters [5]. Protection and honesty of the contact link between device can't be violated. There is a need to incorporate IPv6 for Internet of Things situations of complex hybrid cryptography in the encryption techniques. The IPv6 dependent solution can be handled using completely secured algorithms that can't be intercepted. It is no longer enough to stop the attacks in IoT, IoT should also be safe against the intrusions.

2. RPL (ROUTING PROTOCOL FOR LOW-POWER AND LOSSY NETWORKS)

IoT is based on IPv6. This is mostly aimed at Low power Wireless Personal Area Networks convergence. (6LowPAN). The dynamic development of Destination-Oriented Guided Acyclic Graph (DODAG) has unidirectional and bi-directional communication capability. LUCC includes multi-factorial attributes that promote higher optimality. RPL allows each node in the framework to select whether packets will be sent upward or downward to their child nodes [6, 7].

Contiki is one of the several IoT powered Operating Systems that are accessible on the internet. Contiki Systems is fitted with Cooja Simulator which is used for program debugging as well as of sensor nodes for Internet of Things [8–10]. Contiki has created an exceptional IoT simulator Cooja which enables programmers to import and program huge quantity of IoT devices and gives relevant results from various algorithms. To access and track IoT devices remotely, back-end C programs and header files can be customized and recompiled. Contiki operates almost as seamlessly on IPv4 networks as well as IPv6 ones with the integration of lightweight protocols [11, 12].



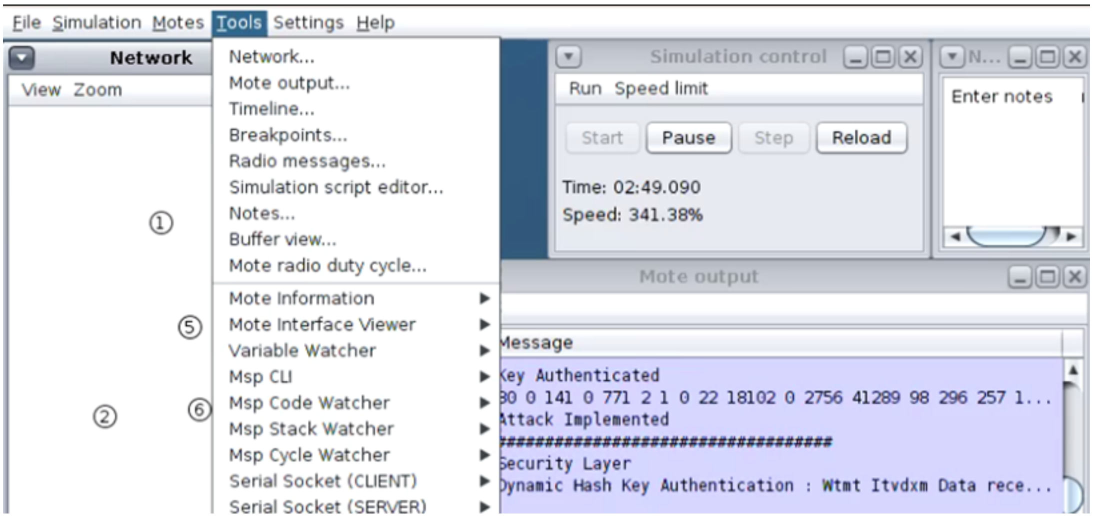
Time: 00:15.411
Speed: ---

```
Time                 ge
00:0                 g broadcast
00:0                 ty Layer
00:0                 c Hash Key: Wtmt Itvdx...
00:0
00:03.680  ID:6    Key Authenticated
00:03.686  ID:7    Sending broadcast
00:03.760  ID:1    Sending broadcast
00:03.820  ID:4    Sending broadcast
```

FIGURE 1. **Formation of Network and Simulation**

Figure 1 portrays the various Internet of Things (IoT) motes in Cooja Simulator with a complex encryption method. The way outcomes can be evaluated after the simulation. Both the data contact and signals are processed in the Mote and can be analyzed using graphs.

When the simulation is done, the network log files of operation and the data transmission will be checked. In the Log Data Recorder Window, the log data can be evaluated in depth using many available analytics methods [13].

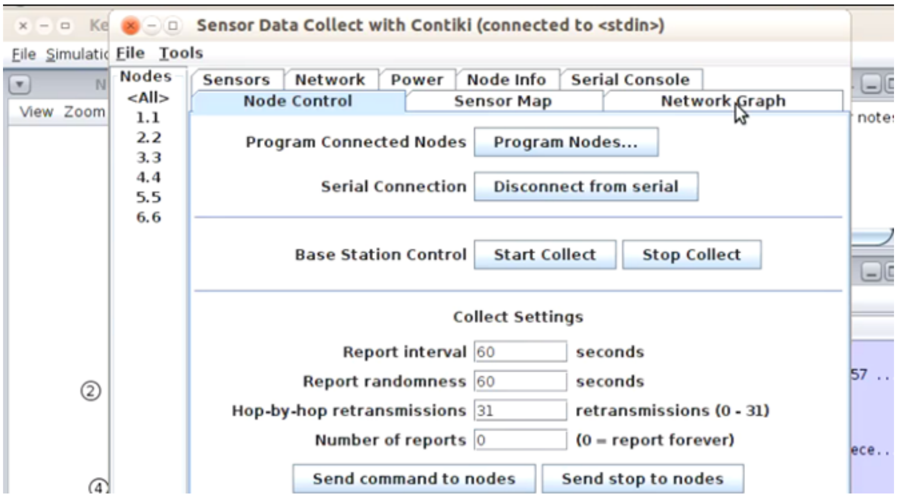


Time: 02:49.090
Speed: 341.38%

```
Key Authenticated
30 0 141 0 771 2 1 0 22 18102 0 2756 41289 98 296 257 1...
Attack Implemented
######################################
Security Layer
Dynamic Hash Key Authentication : Wtmt Itvdxm Data rece...
```

FIGURE 2. **Log Evaluations from Simulation**

Figure 2 reflects Cooja Simulator. The instrument used in Cooja IoT Simulator is useful to analyse the health of the human mote. In the Cooja dashboard, you can view IoT control software. Collect View uses AI to examine activities of the Internet of Things motes [14, 15].



Report interval 60 seconds
Report randomness 60 seconds
Hop-by-hop retransmissions 31 retransmissions (0 - 31)
Number of reports 0 (0 = report forever)

FIGURE 3. **Cooja Implementation Analytics**

Figure 3 shows how the IoT Simulation mechanism can be evaluated and prediction is possible on different parameters. The network graph of sensor nodes in Figure 4 can be viewed in Cooja's Collector View dashboard [16].

In Figure, the findings and parameter-based comparisons of various data had shown in the table format. It provides the person IoT programmer with the opportunity to analyze all nodes in collected community on several variables.

The Serial Console Tab as seen in Figure displays the data transfer file, and the authentication logs. Figure shows a mechanism where attack and authentication behavior allow the developer to assess the protection of device real time sensors [17].

In Figure, all the parameters including LPM, CPU, Radio Listen and Radio Send are used during the IoT simulation. The main outcomes in the graph are compatible and the strength in the low integrity mode is in the credibility mode. He loves listening to radio nearly all the time [18].

6LoWPAN is one of the popular and useful software with free and open source library used for network analysis. The sniffing module is integrated with the features that can plot the search results on various forms such as in text or graph. This tool facilitates continuous intrusion estimation tracking and review of traffic connected via 6LoWPAN with graphical user interface (GUI). Foren6 is strong enough to conduct real-time RPL analyses and document the details [19, 20].

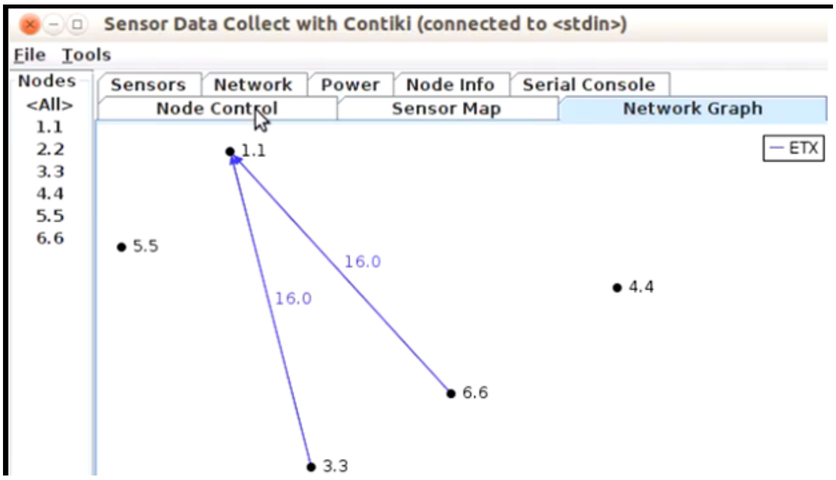
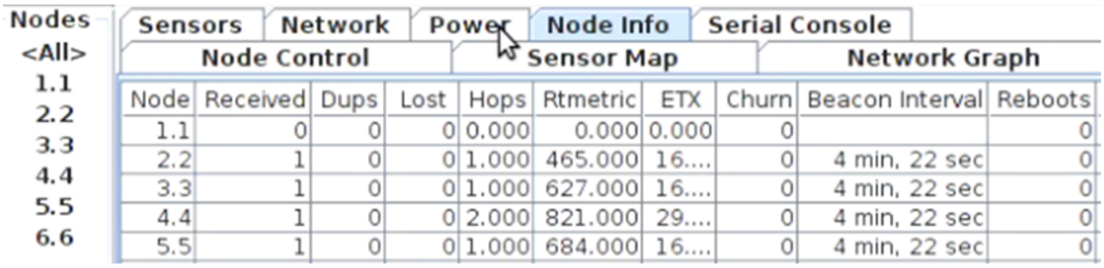
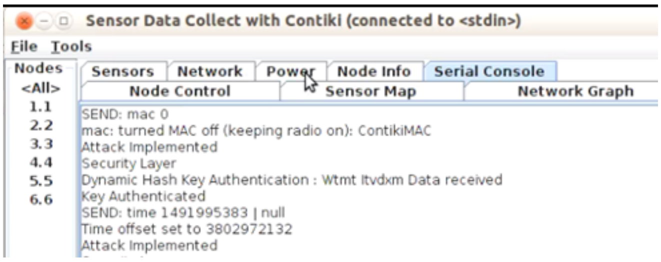


FIGURE 4. Dynamic View of Network



Node	Received	Dups	Lost	Hops	Rtmetric	ETX	Churn	Beacon Interval	Reboots
1.1	0	0	0	0.000	0.000	0.000	0		0
2.2	1	0	0	1.000	465.000	16....	0	4 min, 22 sec	0
3.3	1	0	0	1.000	627.000	16....	0	4 min, 22 sec	0
4.4	1	0	0	2.000	821.000	29....	0	4 min, 22 sec	0
5.5	1	0	0	1.000	684.000	16....	0	4 min, 22 sec	0

FIGURE 5. Cavernous Node Evaluations



```
SEND: mac 0
mac: turned MAC off (keeping radio on): ContikiMAC
Attack Implemented
Security Layer
Dynamic Hash Key Authentication : Wtmt Itvdxm Data received
Key Authenticated
SEND: time 1491995383 | null
Time offset set to 3802972132
Attack Implemented
```

FIGURE 6. Key Exchange for Security and Privacy

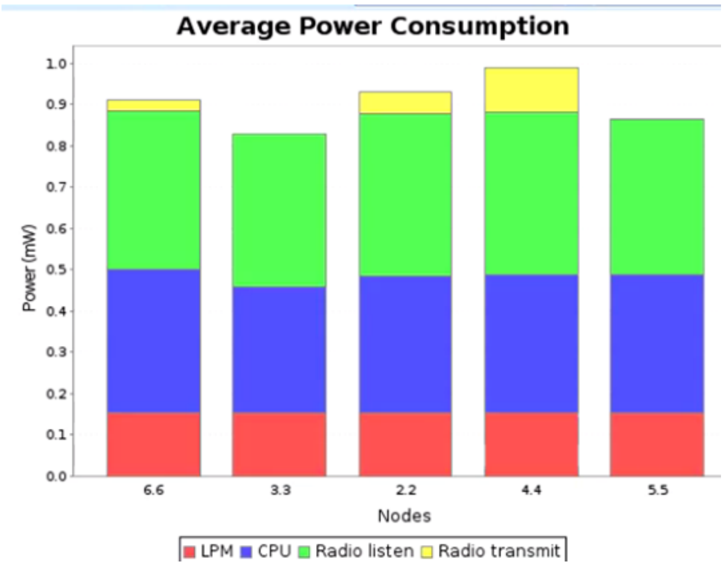


FIGURE 7. Power Evaluation Patterns

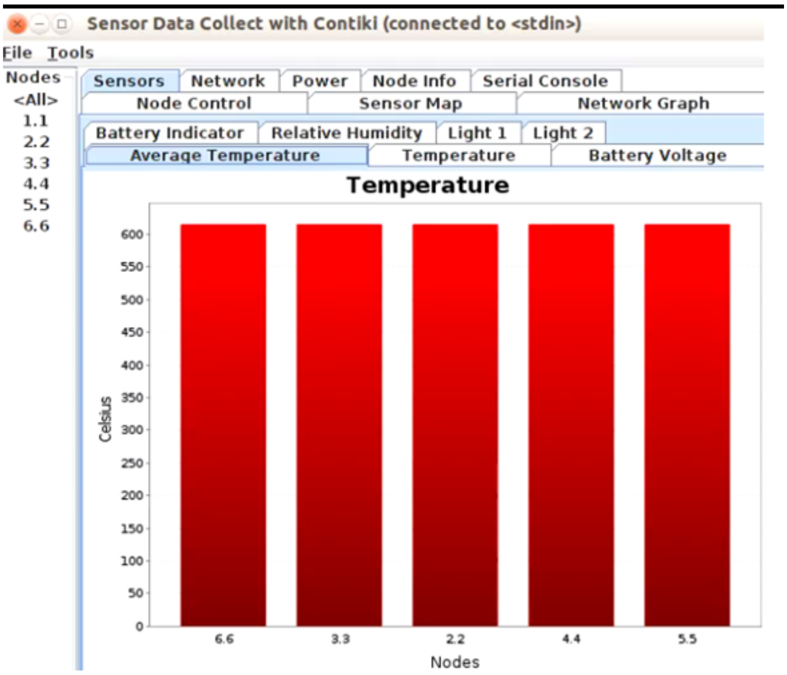
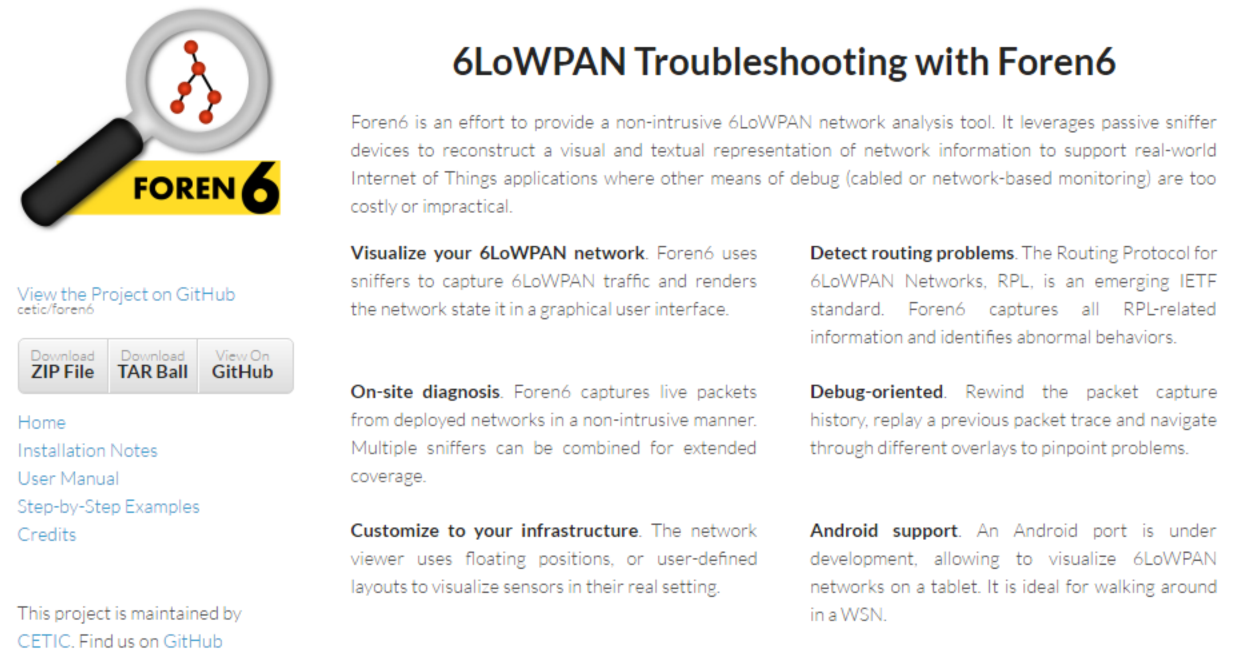


FIGURE 8. Temperature Patterns from Simulations



This project is maintained by CETIC. Find us on GitHub

6LoWPAN Troubleshooting with Foren6

Foren6 is an effort to provide a non-intrusive 6LoWPAN network analysis tool. It leverages passive sniffer devices to reconstruct a visual and textual representation of network information to support real-world Internet of Things applications where other means of debug (cabled or network-based monitoring) are too costly or impractical.

Visualize your 6LoWPAN network. Foren6 uses sniffers to capture 6LoWPAN traffic and renders the network state it in a graphical user interface.

On-site diagnosis. Foren6 captures live packets from deployed networks in a non-intrusive manner. Multiple sniffers can be combined for extended coverage.

Customize to your infrastructure. The network viewer uses floating positions, or user-defined layouts to visualize sensors in their real setting.

Detect routing problems. The Routing Protocol for 6LoWPAN Networks, RPL, is an emerging IETF standard. Foren6 captures all RPL-related information and identifies abnormal behaviors.

Debug-oriented. Rewind the packet capture history, replay a previous packet trace and navigate through different overlays to pinpoint problems.

Android support. An Android port is under development, allowing to visualize 6LoWPAN networks on a tablet. It is ideal for walking around in a WSN.

FIGURE 9. **9.6LoWPAN Framework**

In order to connect and use the USB serial machines, the Linux community, "dialout", is widely used. Initially, "Foren6" will be introduced as a root customer. If some other user account is used, then the user should be granted permission to use USB storage [21, 22].

3. CONCLUSION

The Internet of Things (IoT) a global network of linked physical objects and records. The creation of Internet of Things has been accomplished thanks to the advancement of new technology and creative programs. The internet was born through the over-provision of mobile gadgets. The threats of IoT development in the internet of things have been seriously discussed and the industry and government are trying to develop international regulations to safeguard customers' privacy. In 1982, the concept of a pervasive machine network has already been raised as the revised delivery engine from Coca-Cola recorded its inventory and whether or not drinks were being constantly cooled. Kevin Ashton coined the word "Internet of things" to explain the underlying framework of the Internet. Large range of IoT-based applications was categorized into sectors of consumer use, industrial, manufacturing and infrastructure. The large variety of IoT technologies can make a huge effect on the market industry owing to the use of mobile devices. This sector has many study possibilities because of the rise of research equipment.

FUNDING

None

ACKNOWLEDGEMENT

None

CONFLICTS OF INTEREST

The author declares no conflict of interest.

REFERENCES

[1] V. Gampala, S. Inuganti, and S. Muppidi, "Data Security in Cloud Computing with Elliptic Curve Cryptography," *Int. J. Soft Comput. Eng*, vol. 2, no. 3, pp. 138–141, 2012.

[2] J. Vasseur, N. Agarwal, J. Hui, Z. Shelby, P. Bertrand, and C. Chauvenet *RPL: The IP routing protocol designed for low power and lossy networks", Internet Protocol for Smart Objects (IPSO) Alliance*, pp. 201–218, 2011.

[3] P.-P. Verbeek, *Moralizing Technology: Understanding and Designing the Morality of Things*. Chicago: The University of Chicago Press, 2011.

[4] O. Vermesan and P. Friess *Internet of things: converging technologies for smart environments and integrated ecosystems*, 2013.

[5] O. . Vermesan and P. Friess, *Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems (PDF)*. Aalborg, Denmark: River Publishers, 2013.

[6] M. A. Vieira, C. N. Coelho, D. Silva, D. C. D. Mata, and J. M, “Survey on wireless sensor network devices,” *Emerging Technologies and Factory Automation*, pp. 537–544, 2003.

[7] S. Vongsingthong and S. Smanchat, “Internet of Things: A review of applications & technologies" (PDF),” *Suranaree Journal of Science and Technology*, 2014.

[8] W. Trappe, R. Howard, and R. S. Moore, “Low-energy security: Limits and opportunities in the internet of things,” *IEEE Security and Privacy*, vol. 13, no. 1, pp. 14–21, 2015.

[9] J.-B. Waldner *Nanoinformatique et intelligence ambiante. Inventer l’Ordinateur du XXIeme Siècle. London: Hermes Science*, pp. 254–254, 2007.

[10] J.-B. Waldner *Nanocomputers and Swarm Intelligence. London: ISTE*, pp. 227–231, 2008.

[11] M. Wallace *Fragmentation is the enemy of the Internet of Things*, 2016.

[12] K. Walsh, “Nest Reminds Customers That Ownership Isn’t What It Used to Be,” *Electronic Frontier Foundation*, 2016.

[13] R. Want *An introduction to RFID technology*, pp. 25–33, 2006.

[14] R. . Want, B. N. Schilit, and S. Jenson, “Enabling the Internet of Things,” *Computer*, vol. 48, pp. 17384656–17384656, 2015.

[15] M. Ward, R. V. Kranenburg, and G. Backhouse, “RFID: Frequency, standards, adoption and innovation,” *JISC Technology and Standards Watch*, pp. 5–11, 2006.

[16] M. Ward *Smart devices to get security tune-up*, 2015.

[17] G. Webb *Say Goodbye to Privacy*, 2015.

[18] R. H. Weber and R. Weber *Internet of Things: Legal Perspectives*, vol. 9783642117107, pp. 59–64, 2010.

[19] M. Weiser, “The Computer for the 21st Century" (PDF),” *Bibcode:1991SciAm.265c..94W. doi:10.1038/scientificamerican0991-94. Archived from the original (PDF) on 11*, vol. 265, pp. 94–104, 1991.

[20] M. . Westerlund, Leminen, . Seppo, and M. Rajahonka, “Designing Business Models for the Internet of Things,” *Technology Innovation Management Review*, vol. 4, no. 7, pp. 5–14, 2014.

[21] K. Wieland, *IoT experts fret over fragmentation*. 2016.

[22] A. . Witkovski, Santin, . Altair, Abreu, . Vilmar, and J. Marynowski, “An IdM and Key-Based Authentication Method for Providing Single Sign-On in IoT,” *2015 IEEE Global Communications Conference (GLOBECOM)*, pp. 1–6, 2014.