 https://doi.org/10.34028/ijqa/5/2/223

Using Security Centre in Indoor Internet of Things

Ghassan Samara
Faculty of Information Technology
Zarqa University
gsamarah@zu.ed.jo

Hussam Abu Munshar
Faculty of Information Technology
Zarqa University
Hussam_prog@yahoo.com

Ruzayn Quaddoura
Faculty of Information Technology
Zarqa University
ruzayn@zu.edu.jo

Received :11/04/2022 Accepted :27/07/2022

Abstract:

The Internet of things (IoT) facilitated various aspects of people's daily lives. In simple terms, the IoT refers to the connection of sensors, actuators, and devices to a network by which they can interact with each other and their users. It is a practical model that works on connecting a group of sensors and actuators that form a network that works to carry out several tasks, such as collecting information from the surrounding environment and processing it and providing the beneficiary of the network with this critical information is used in many cases in making important decisions and missions. Over time, the importance of IoT will increase due to its use in many fields. This technology is expected to become an essential milestone in developing many sectors and sciences.

Therefore, to benefit from IoT technology, security in the IoT must focus on raising its efficiency. The security of IoT is a big challenge because of its complexity, heterogeneity, and a large number of related resources. It is necessary to improve security protocols to guarantee IoT connection and ensure all devices in this network are trusted and prevent an attacker from accessing any device in the network because these attacks penetrate privacy and expose the personal property to damage.

This research introduces a new framework to improve the confidentiality, integrity, authenticity, and availability of IoT devices in indoor environments, by forcing new devices (IoT-MD), middleware (Security Centre SC), and protocols (add a new authorized device and IoT Traffic Control Protocol IoT-TCP).

Security in IoT will be guaranteed by using this framework which enforces isolation between the IoT devices and networks to prevent unauthorized IoT devices. Moreover, prevent attacks in the IoT indoor environment.

Keywords: Internet of Things, Security Centre, Indoor IoT.

Introduction:

Internet of things (IoT) is an essential part of scientific research. IoT is sensors and actuators in virtually any industry that can be connected and collect data over any network to cloud platforms and backbends. IoT is devices with limited sources that are used to collect information from the surrounding environment [1]. [2]. IoT is witnessing an accelerated development due to the benefit it achieves in many fields and helping humans know all the information about the surrounding environment and control it [3][4]. and [5]. Internet of things is used in many fields, such as intelligent buildings and cities, health care, monitoring the weather, traffic and humans and the ocean, monitoring natural phenomena, and maritime navigation, in addition to military uses[6] [7] [8] [9].

This is done by collecting data from the environment, sending it to the base for processing, and using it to make decisions by actuators and users [10].

Smart devices like computers and smartphones can execute security features built into them, like firewalls, anti-virus, and other security software, that can guarantee safety in data transition, which is generally missing in various IoT devices already in the market [11] [12]. [13]. On the other hand, the IoT application is not a standalone application; it is an assembled product that includes work from many individuals and industries, starting from sensing to the applications, several different products and technologies are being used [14].

These include many devices and many communication standards like cellular networks, WiFi, IEEE 802.15.4, fixed cable, Bluetooth, etc. [14, 15, 16, 17, and 18]. To improve the compatibility of connectivity, various connectivity technologies are being used in IoT devices like Zigbee Zonal Intercommunication Global-standard Battery Economical Efficient, 6LOWPAN IPv6 over Low-Power Wireless Personal Area Networks, wireless HART, Z-Wave, Bluetooth, NFC near Filed Communication, RFID radio frequency identification, etc. [19].

The big challenge in the IoT is security, security in adding a new device, and data transfer between devices and IoT controllers. The dangers of IoT attacks are accessing any device in the network and opening or controlling doors, devices and machines, or modifying cameras, and the risk of attacking private information and data that violates privacy [20].

Typical CIA (Confidentiality, Integrity, and Availability) security requirements should be employed in the IoT system [21]. It is necessary to improve security protocols to guarantee IoT connection to ensure that all devices in this network are trusted and would prevent an attacker from

accessing any device in the network and that attacks penetrate privacy and expose the personal property to theft and damage.

The IoT is essential in human life by providing the platform for exchange and communication between different devices without human intervention [22]. It is used now in many aspects of life like automation, home and office, industry, and autonomous vehicle (AV), at the same time, since this technology is used in various aspects and applications. In addition, [23] have suggested one of the most straightforward definitions that smoothly describe the IoT, as shown in Fig 1. It stated: 'The Internet of Things allows people and things to be connected anytime, anyplace, with anything and anyone, ideally using any path/network and any service [24].

Many challenges in IoT security must be overcome, which is considered a weak point like different types and brands used in IoT devices with different firmware. Usually, IoT uses a wired or wireless network that accepts authorized and unauthorized users to access IoT devices. There is no isolation between the IoT network and the wide-area network, leading to attacks. Most IoT devices are easy to install and configure by a user, leading to powerlessness in security protocols and authentication [21] [25], a different type of data transfer in LAN from other kinds of devices (control message, video, audio messages, and internet data browsing) this data exhibition to attack because it is not classified and not easy to know which is authorized access.

The security of IoT is a big challenge because of its complexity, heterogeneity, and a large number of related resources. The aggressor can attack the IoT system by damaging or tampering [26].

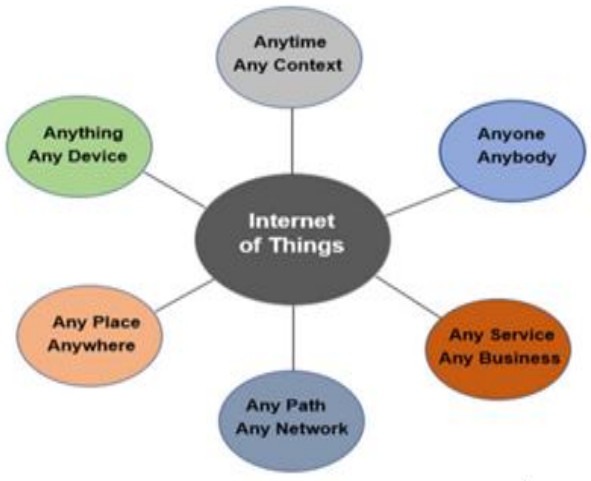

Fig 1: The IoT can connect anything anywhere using any path

This research demonstrates how IoT devices will transfer data under security rules. IoT data traffic includes; all data sent from IoT devices (sensors, actuators, users, cloud, and IoT controller) in the IoT network. This network has been shared with other types of data traffic. The variation of traffic types in the network has led to the rise of a wide range of attacks. Therefore, a protocol must be enforced to verify this data's source, authenticity, and security.

There are significant concerns about the security of IoT devices and potential threats to them. Security must be a cornerstone of the IoT systems. Such systems should be able to validate, authenticate, confirm, and encrypt data exactly [27][28].

2 Related Works:

Many papers discussed the issue of improving the IoT security domain. IoT-KEEPER [29] presents a system capable of detecting network attacks and enforcing necessary security measures to prevent IoT devices from performing these attacks. This system secures both network-local device-to-device (D2D) and remote device-to-infrastructure (D2I) communication of IoT.

IOT-KEEPER is a lightweight, hardware-agnostic solution which can be deployed using network gateways or single-board computers.

Protecting IoT environments against Traffic Analysis Attacks with Traffic Morphing [30] authors proposed using fake traffic to mask the real traffic generated by IoT devices, where the fake traffic is statistically similar to real IoT traffic. Therefore, the opponent cannot distinguish between real and fake traffic. Traffic diversion makes it difficult for Network Monitor to implement traffic analysis attacks effectively.

IoT Sentinel [25] uses traffic traces from IoT devices captured during device setup to identify device model and manufacturer information. This information is later used to set up (one-time) network access control for identified devices. Since IoT Sentinel uses traffic traces collected during device setup, it cannot identify, and set up access control of, IoT devices that have already been used.

Integration of Block chain and Internet of Things (IoT) [22] according to the research results, although IoT-block chain integration brings many benefits in different areas, its realization faces many challenges. This study reviewed recent developments and solutions in static and dynamic categories.

This study also analysed the challenges and areas for future research. The IoT has recently penetrated various industries and is directed towards being smarter. In addition, industry owners have become more aware of the benefits of block chain systems over time. If the IoT-block chain integration challenges are met, integrating these two technologies can greatly affect all aspects of industries and people's everyday lives.

AuDI [31] has recently proposed identifying device-type information by analyzing the packet timing information from IoT traffic.

Kitsune [32] [33] is a lightweight, online anomaly detection technique which uses an ensemble of auto encoders for anomaly detection.
Secure box traffic analysis [14] is performed remotely by transmitting a secure code to an authorized user to obtain the privilege, resulting in latency problems. According to the current article, a strategy for boosting security in both device-to-device connections and devices-to-IoT controller connections is proposed to reduce communication overhead while simultaneously increasing the scalability property of the IoT system at any time.

4 The Proposed Framework:

This research divides the framework into three categories hardware (IoT devices, IoT management devices), middleware (Security Centre SC), and protocols such as the Internet of things traffic control protocol IoT-TCP.
The IoT management device IoT-MD is a smart server with sufficient memory, a fast processor, and high storage capacity with uninterruptible power supply UPS. This device manages all IoT system components (devices, network, gateway, and users). It will work as a fog computing platform for IoT administrators, IoT-admin, IoT-admin responsible for controlling all IoT devices, adding/removing devices and users, specifying users' privilege and reviewing the log file and Security Centre SC.
The Security Centre SC is a middleware in IoT management device IoT-MD, the mediator between IoT devices, and is responsible for receiving, decrypting, and sending data between IoT devices, using compatible encryption algorithms for each IoT device.
The IoT-TCP (traffic control protocol) is the first protocol in SC responsible for receiving and decrypting cipher text from the sender device to ensure that the message is from an authorized device, encrypting messages and resending them to the receiver IoT device. If the message is from an unauthorized device, it will be.
The second protocol in SC is to add New Authorized IoT Device (add NA-IoT-D), which is responsible for adding new IoT devices into the system. The third protocol in SC is a key selection responsible for selecting the key in data encryption operation. The SC includes database tables such as (table of keys, messages table, etc.). However, our proposed framework is scalable and it utilizes any cryptography algorithm.
Fig 2 illustrates suggested frameworks for IoT systems, which will be discussed in this part. And we will explain how data will be transferred between IoT devices using IoT-TCP; add NA-IoT-D, Security Centre SC, table of keys TK, and key selection, which will guarantee security in the IoT system.

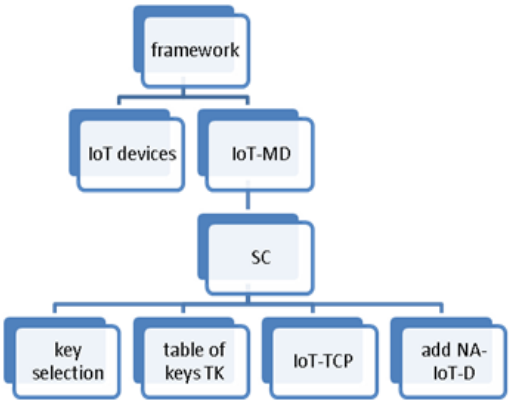

Fig 2 Proposed frameworks for IoT system

4.1 Security Centre SC:

This section has demonstrated how data will be transferred between IoT devices under security rules. IoT data traffic includes all data sent from IoT devices (sensors, actuators, users, cloud, and IoT controller) in the IoT network. This network has been shared with other types of data traffic such as internet browsing data, cellular device data, etc. The variation of data traffic types in the network has led to the rise of a wide range of attacks. Therefore, a protocol must be enforced to verify this data's source, authenticity, and security.
SC is the mediator between IoT devices and is responsible for receiving, decrypting, and sending data between IoT devices, using compatible encryption algorithms for each IoT device.

4.1.1 Add New Authorized IoT Device:

This step is important in the IoT framework to determine a new IoT device type. This information will be used later by SC, such as encryption algorithm, MAC address, and device identifier. This step configures a new device with network settings such as device IP address, SC IP address, and SC time and date.

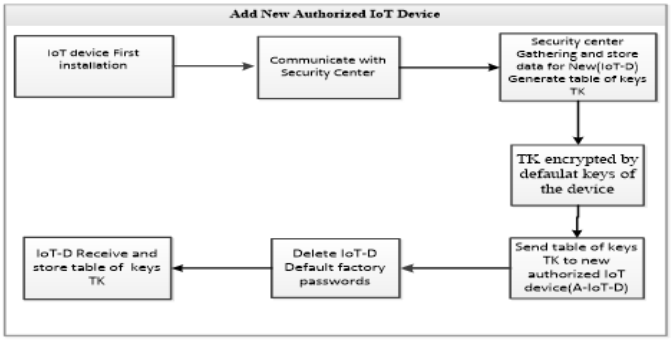

Fig 3 Add New Authorized IoT Device

As illustrated in Fig 3, the first step is adding the new IoT device to the network by configuring the IP and SC IP addresses. Then the device communicates with the SC. SC will receive device information that will be used later to detect the device's authenticity. Then SC will generate a table of random keys TK to be used by the encryption algorithm. The default keys of

the device will encrypt this table, and then it will be stored in SC and sent to the device. These keys will be used to decrypt messages in sending and receiving data between the device and the SC.

Each device has been designed with default factory passwords and resets figuration instructions, weakening IoT security. The next step is to delete the default factory passwords and stop resetting instructions.

Finally, a table of keys TK has been saved in the IoT device and SC to enable communication between the device and the SC confidentially and reliably; this protocol uses one key in each message transaction.

4.1.2 Internet of Things Traffic Control Protocol IoT-TCP:

The main purpose of this protocol is to identify attacking messages originating from unauthorized devices and allow heterogeneous IoT devices to deploy encryption algorithms with the help of the SC, which is the middleware between IoT devices.

IoT-TCP is responsible for receiving and decrypting the cipher text from the sender device to ensure that the message is from an authorized device and then encrypting messages and resending them to the receiver IoT device. If the message is from an unauthorized device, it will be deleted. As shown in Fig 4, the data (cipher text) sent from the IoT device to the security Centre SC will be decrypted. This message, which uses Sender Private Key SPK, has been dedicated to the sender's IoT device. Suppose that the message rises from an authorized sender. In this case, the decryption operation will be valid, so the message will be saved in a database and encrypted using the Receiver Private Key RPK dedicated to the destination. Otherwise, if this message has risen from an unauthorized sender, the decryption operation will be invalid; the SC will gather fingerprinting of the message or traffic behaviour and add labels (addresses, port, etc.) to machine learning ML will delete the message.

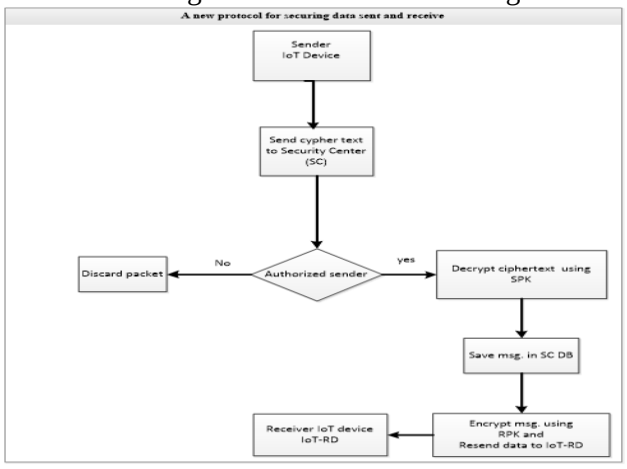

Fig 4 Flowchart for A new protocol for securing data transfer

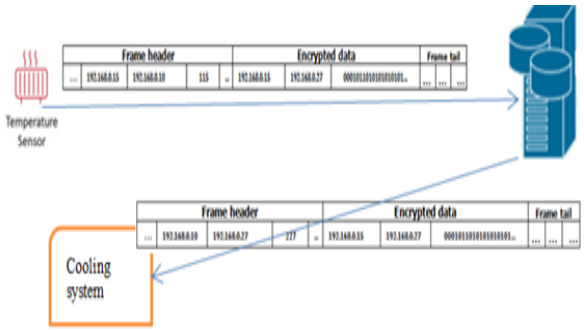

Fig 5 sending data between IoT devices

For example, if the temperature sensor detects that the room temperature is more than 25 degrees, it will send a message to the SC after checking that it is from an authorized device. In this case, the message will be sent back to the cooling system as a cipher message using PRK dedicated to the cooling system, as shown in Fig 5.

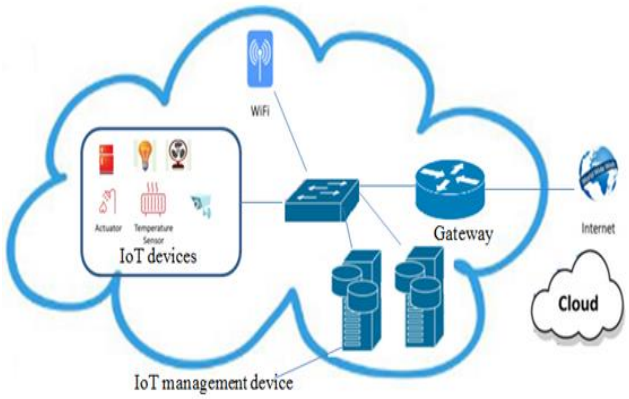

Fig 6 suggested framework for the indoor IoT system

Fig 6 describes the indoor IoT architecture and the connections between the IoT components; because the IoT-MD is a critical device, the backup IoT-MD device will be added to the system.

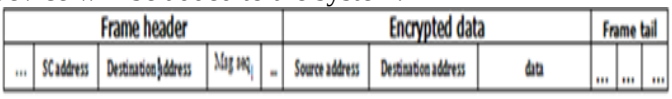

Fig 7 IoT data frame from IoT device

Fig 7 describes the IoT data frame in the suggested framework, which is presented with an example earlier in Fig 7. This message has been used to send data between IoT devices. In the header field, the destination address is the IoT-MD address because all messages will be sent to SC firstly in the IoT-MD, and then SC will send them to an actual destination IoT device.

Fig 8: IoT data frame from SC

Fig 8 describes the IoT data frame which has been resent from SC to the IoT device. The sequential message Meg_Seq is a counter of messages sent from

the sender to the SC. This counter has been used in key selection.

4.1.3 Key Selection:

The main objective of this work is to investigate methods for improving security in indoor IoT systems, despite the security weakness of the IoT device and the difference in manufacturers, device capabilities, and encryption algorithms.

As mentioned in adding a new authorized IoT device section, SC will generate a table of random keys TK, which allows heterogeneous IoT devices to deploy encryption algorithms.

Differences in IoT devices led to differences in encryption algorithms, as mentioned in the encryption algorithms section in Chapter 2. Hence, an intermediary must handle different encryption algorithms and transfer data between IoT devices. So, there is no imposition of any data encryption algorithms; choosing the encryption algorithms depends on the IoT devices' capabilities. SC in this framework is the mediator between IoT devices and is responsible for data decrypting and encrypting between IoT devices, using compatible encryption algorithms for each IoT device.

When adding a new IoT device, a table of keys TK will be created by SC, which has several keys compatible with encryption algorithms used in IoT devices. These keys will be used in sending and receiving operations.

When the SC receives the data frame from the IoT device, the key selection protocol will select the key from the TK assigned to the IoT device by defining the key index using this equation.

$$key_{index} = (Msg\_Seq) \bmod (total\_of\_keys)$$

The total_of_keys is the number of keys generated from SC when adding an IoT device and saved in TK.

5 Conclusions and Future Works:

In this research, the primary goal was achieved to develop a network attack detection approach based on new security policies (IoT-TCP), with the help of the security Centre SC, that ensures that IoT devices do not receive any data from an unauthorized device in the IoT system and that heterogeneous IoT devices can deploy encryption algorithms with the help of the SC.

More research should be done on using the security Centre SC in the IoT system. In addition, machine learning should be used to monitor IoT networks and analyze and classify data traffic to prevent attacks.

References:

1. Samara, G. and Aljaidi, M., “Efficient Energy, Cost Reduction, and QoS Based Routing Protocol for Wireless Sensor Networks”. International Journal of Electrical & Computer Engineering (2088-8708), 9(1). 2019.
2. Samara, G., Alsalihy, W.A.A. and Ramadass, S., “Increasing Network Visibility Using Coded Repetition Beacon Piggybacking”. World Applied Sciences Journal, 13(1), pp.100-108. 2011.
3. Samara, G. and Blaou, K.M., “Wireless Sensor Networks Hierarchical Protocols”. In 2017 8th International Conference on Information Technology (ICIT) (pp. 998-1001). IEEE. 2017.
4. Samara, G., Al-Okour, M. “Optimal Number of Cluster Heads in Wireless Sensors Networks Based on LEACH”, International Journal of Advanced Trends in Computer Science and Engineering, 9 (1), pp. 891–895, 2020.
5. Samara, G. and Aljaidi, M., “Aware-Routing Protocol Using Best First Search Algorithm in Wireless Sensor”. Int. Arab J. Inf. Technol., 15(3A), pp.592-598. 2018.
6. Khanna, A. and Kaur, S., “Evolution of Internet of Things (IoT) and Its Significant Impact in the Field of Precision Agriculture”. Computers and Electronics in Agriculture, 157, pp.218-231. 2019.
7. Samara, G., Albesani, G., Alauthman, M., Al Khaldy, M., “Energy-Efficiency Routing Algorithms in Wireless Sensor Networks: A Survey”, International Journal of Scientific and Technology Research, 9(1), pp. 4415–4418. 2020.
8. Samara, G., Wireless Sensor Network MAC “Energy-Efficiency Protocols: A Survey”. In 2020 21st International Arab Conference on Information Technology (ACIT) (pp. 1-5). IEEE. 2020.
9. Samara, G., Ramadas, S., Al-Salihy, W.A.H. “Safety Message Power Transmission Control for Vehicular Ad Hoc Networks”. Journal of Computer Science, 6 (10), pp. 1056–1061. 2010.
10. Samara, G. and Alsalihy, W.A.A., “A New Security Mechanism for Vehicular Communication Networks”. In Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec) (pp. 18-22). IEEE. 2012.
11. Samara, G., Al-Salihy, W.A. and Sures, R., “Efficient Certificate Management in VANET”. In 2010 2nd International Conference on Future Computer and Communication (Vol. 3, pp. V3-750). IEEE. 2010.
12. Samara, G., Abu Salem, A.O. and Alhmiedat, T., “Dynamic Safety Message Power Control in VANET Using PSO”. World of Computer Science & Information Technology Journal, 3(10). 2013.
13. M Khatari, G Samara, “Congestion Control Approach Based on Effective Random Early

Detection and Fuzzy Logic", MAGNT Research Report, Vol.3 (8). PP: 180-193. 2015.
14. Hassija, C., Goyal, and Sikdar. Hassija V, Chamola V, Saxena V, Jain D, Goyal P, Sikdar B "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures". IEEE Access, 7, pp.82721-82743. 2019.
15. Alhmiedat, T. and Samara, G., "A Low Cost ZigBee Sensor Network Architecture for Indoor Air Quality Monitoring". International Journal of Computer Science and Information Security (IJCSIS), 15(1). 2017.
16. Salem, A.O.A., Samara, G. and Alhmiedat, T., "Performance Analysis of Dynamic Source Routing Protocol". Journal of Emerging Trends in Computing and Information Sciences, 5(2). 2014.
17. Salem, A.O.A., Alhmiedat, T. and Samara, G., "Cache Discovery Policies of MANET". World of Computer Science & Information Technology Journal, 3(8). 2013.
18. Alhmiedat, T.A., Abutaleb, A. and Samara, G., "A Prototype Navigation System for Guiding Blind People Indoors Using NXT Mindstorms". International Journal of Online and Biomedical Engineering (iJOE), 9(5), pp.52-58. 2013.
19. Samara, G., "Intelligent Reputation System for Safety Messages in VANET". IAES International Journal of Artificial Intelligence, 9(3), p.439. 2020.
20. Samara, G., "Lane Prediction Optimization in VANET". Egyptian Informatics Journal, 22(4), pp.411-416. 2021.
21. Atlam, H.F., Alenezi, A., Walters, R.J., Wills, G.B. and Daniel, J., "Developing an Adaptive Risk-Based Access Control Model for the Internet of Things". In 2017 IEEE international conference on internet of things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and ieee smart data (SmartData) (pp. 655-661). IEEE. 2017.
22. Samara, G. and Alsalihy, W.A.A., "Message Broadcasting Protocols in VANET". Information Technology Journal, 11(9), p.1235. 2012.
23. Harrison, M. V. O. F. P. G. P. G. S. S. H. B. A. J. I. S. M. M. "Internet of Things Strategic Research Roadmap". Cyber Resilience of Systems and Networks. Available at: http://link.springer.com/10.1007/978-3-319-77492-3_16. 2009.
24. Samara, G., "An Intelligent Routing Protocol in VANET". International Journal of Ad Hoc and Ubiquitous Computing, 29(1-2), pp.77-84. 2018.
25. Miettinen, M. et al. "IoT SENTINEL: Automated Device-Type Identification for Security Enforcement in IoT", Proceedings - International Conference on Distributed Computing Systems, pp. 2177–2184. doi: 10.1109/ICDCS.2017.283. 2017.
26. Deogirikar, J. and Vidhate, A. "Security Attacks in IoT: A Survey", Proceedings of the International Conference on IoT in Social, Mobile, Analytics and Cloud, I-SMAC 2017, pp. 32–37. doi: 10.1109/I-SMAC.2017.8058363. 2017.
27. Samara, G., Ramadas, S. and Al-Salihy, W.A "Design of Simple and Efficient Revocation List Distribution in Urban Areas for VANET's", (IJCSIS) International Journal of Computer Science and Information Security, Vol. 8, No. 1. 2010.
28. Samara, G., Alsalihy, W.A.H.A. and Ramadass, S., "Increase Emergency Message Reception in Vanet". Journal of Applied Sciences, 11(14), pp.2606-2612. 2011.
29. Hafeez, I., Antikainen, M., Ding, A.Y. and Tarkoma, S., "IoT-KEEPER: Detecting Malicious IoT Network Activity Using Online Traffic Analysis at the Edge". IEEE Transactions on Network and Service Management, 17(1), pp.45-59. 2020.
30. Hafeez, I., Antikainen, M. and Tarkoma, S., "Protecting IoT-Environments against Traffic Analysis Attacks with Traffic Morphing". In 2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops) (pp. 196-201). IEEE. 2019.
31. Marchal, S., Miettinen, M., Nguyen, T.D., Sadeghi, A.R. and Asokan, N., Audi: "Toward Autonomous IoT Device-Type Identification Using Periodic Communication". IEEE Journal on Selected Areas in Communications, 37(6), pp.1402-1412. 2019.
32. Mirsky, Y., Doitshman, T., Elovici, Y. and Shabtai, A., Kitsune: "An Ensemble of Autoencoders for Online Network Intrusion Detection". Machine Learning, 5, p.2. 2018.
33. Porkodi, S. and Kesavaraja, D., "Integration of Blockchain and Internet of Things". In Handbook of Research on Blockchain Technology (pp. 61-94). Academic Press. 2020.

استخدام مركز الأمان في إنترنت الأشياء الداخلي

غسان عبد الكريم سمارة
كلية تكنولوجيا المعلومات
جامعة الزرقاء
gsamarah@zu.ed.jo

حسام ابو منشار
كلية تكنولوجيا المعلومات
جامعة الزرقاء
Hussam_prog@yahoo.com

رزين أحمد قدورة
كلية تكنولوجيا المعلومات
جامعة الزرقاء
ruzayn@zu.edu.jo

الاستلام : 2022/04/11 القبول : 2022/07/27

المقدمة :

سهلت إنترنت الأشياء (IoT) جوانب مختلفة من حياة الناس اليومية. بعبارات بسيطة ، تشير إنترنت الأشياء إلى اتصال المستشعرات والمشغلات والأجهزة بشبكة يمكنهم من خلالها التفاعل مع بعضهم بعض. وهي نموذج عملي يعمل على ربط مجموعة من الحساسات والمشغلات التي تشكل شبكةً تعمل على تنفيذ عدة مهام مثل : جمع المعلومات من البيئة المحيطة ومعالجتها ، وتزويد المستفيد من الشبكة بهذه المعلومات الهامة. تُستخدم في كثير من الحالات في اتخاذ القرارات والمهام الهامة ، وبمرور الوقت ، ستزداد أهمية إنترنت الأشياء نظرًا لاستخدامها في العديد من المجالات. من المتوقع أن تصبح هذه التكنولوجيا علامة فارقة أساسية في تطوير العديد من القطاعات والعلوم.

لذلك ، للاستفادة من تقنية إنترنت الأشياء ، يجب أن يركز الأمن في إنترنت الأشياء على رفع كفاءتها. يمثل أمان إنترنت الأشياء تحديًا كبيرًا بسبب تعقيدها وعدم تجانسها ، ومن الضروري تحسين بروتوكولات الأمان لضمان اتصال إنترنت الأشياء والتأكد من موثوقية جميع الأجهزة الموجودة في هذه الشبكة ، ومنع المهاجم من الوصول إلى أي جهاز في الشبكة ، لأن هذه الهجمات تخترق الخصوصية وتُعرض الممتلكات الشخصية للضرر.

يقدم هذا البحث إطارًا جديدًا لتحسين السرية ، والنزاهة ، والأصالة ، وتوافر أجهزة إنترنت الأشياء في البيئات الداخلية ، من خلال فرض أجهزة جديدة (IoT-MD)، والبرمجيات الوسيطة ((Security Center SC، والبروتوكولات (إضافة جهاز معتمد جديد ، وبروتوكول التحكم في حركة مرور إنترنت الأشياء .(IoT-TCP).

سيتم ضمان الأمان في إنترنت الأشياء باستخدام هذا الإطار الذي يفرض العزل بين أجهزة وشبكات إنترنت الأشياء لمنع أجهزة إنترنت الأشياء غير المصرح بها. علاوة على ذلك ، منع الهجمات في البيئة الداخلية لإنترنت الأشياء.

الكلمات المفتاحيّة: إنترنت الأشياء, مركز الأمان , إنترنت الأشياء الداخلي.