Indonesian Journal of Electrical Engineering and Computer Science
Vol. 26, No. 3, June 2022, pp. 1581~1588
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v26.i3.pp1581-1588

A survey of security and smart home automation based on internet of things technology

Sarah Mohammed Shareef[1], Zainab Adnan Abbas[2], Zahraa Mohammed Hilal[2]
[1]Department of Production Engineering and Metallurgy, University of Technology, Baghdad, Iraq
[2]Department of Registration and Students Affairs, University of Technology, Baghdad, Iraq

Article Info

Article history:

Received Aug 19, 2021
Revised Mar 14, 2022
Accepted Mar 30, 2022

Keywords:

Infrastructure
Internet of things
Security
Sensors
Smart home
System analysis

ABSTRACT

The internet of things (IoT) refers to the physical tools that are embedded with Internet, software, electronics, sensors and network connectivity. This involves many different systems, for example, healthcare, smart home and so on. The security problem of the IoT and the smart home infrastructure is considered, which has become an urgent issue due to the high popularity, low systemic research and the growth of threats to "us" (people seeking comfort) from "them" (surrounding things, which becoming increasingly intelligent, automated). The research is based both on a systemic, infrastructure understanding, and on an architectural, problem-oriented level. Key security risks for the infrastructure of various types-software and technical, technological, socio-psychological and others-were analyzed. The evolutionary problems of the internet of things and factors influencing the vulnerability of infrastructures have been investigated. In addition to traditional network security tasks, specific tasks (direct and reverse, for identification) are highlighted in IoT interactions and environments. This paper provides an overview of the related work in IoT, together with the open challenges and future research directions using Arduino platform (such as "thick server-thin client") to simulation modeling of time delay probability distribution based on identified simple model.

Corresponding Author:

Sarah Mohammed Shareef
Department of Production Engineering and Metallurgy
University of Technology-Iraq
Senaa Street Front of University of Technology
Email: sarah.m.ali@uotechnology.edu.iq

1. INTRODUCTION

The category "internet of things" (IoT) was entered by K. Auto-ID center in 1999 [1] for radio-frequency identification (RFID) of the goods connected to a network. IoT is a category that unites habitual for the person (works, rest) things and technologies in the uniform intellectual distributed infrastructure activated with the help of the Internet. The purpose is to improve life, comfort, opportunities and safety of the habitat [2], [3]. Intellectualization of habitual things and services raises consumer opportunities and the competitiveness of both things and a person. The basic principle of IoT "Turn on the device in the socket and use it comfortably". By 2025 all our environments from a kettle and video surveillance can become IoT points, and at the beginning of 2021 the world IoT market will exceed one half-trillion dollar, there will be more than 50 billion devices in the market [4].

In 2005 the International Telecommunication Union (ITU) announced the concept of pervasive networks. The internet of things is an environment in which things can obey and data about things can be processed to control devices that can learn. Implementation of IoT is well shown in Twine, the compact and low-power hardware, working together with the network software in real-time and allowing to make this concept a reality. IoT-system is implemented by the infrastructure formed of the following key elements, subsystems [5], [6]:

a) Sensors, infrared (sound, heat, and light) sensors for monitoring processes and operating modes, situations, for example, whether the owner has woken up and is it time to turn on the "warm floor in the bathroom";
b) Applications of intellectualization and algorithms for self-learning of subsystems of "smart" infrastructure, the creation of a unified, safe, intelligent and comfortable environment from things, processes and conditions of comfort familiar to humans;
c) Protocols, standards (for example, IEEE1888) for controling the network communication of sensors, remotely controlling them without the participation of an operator (host).

For example, sensors, responding to sound, can identify the source, the range of processes controlled by the owner using applications. This is how an ecosystem of things, people and processes (environment) is created, adaptive and analyzable, self-regulating with the help of data science (big data and data mining). It has a kernel-SMART house (often instead of SMART apply “intelligent” or just “smart”).

The SMART methodology is based on supporting specific, measurable, achievable, relevant, and time constraints. These criteria determine the emergence of a SMART environment at home and its effectiveness. There is always a SMART strategy for digital transformation through intelligent infrastructure (home, owner, and environment).

All kinds of things (a kettle, the conditioner, the video camera and others) if they are connected to SMART infrastructure of the house and the Internet can become the IoT nodes (access and reaction) in the smart home. For example, the conditioners operated by energy of sunshine are developed. There are achievements in the development of countering risks to the house and used IoT vulnerabilities, early control and protection against minor vulnerabilities, filtering “noise”, spoofing, network activity analysis (LOG, domain name service (DNS)), process masking, management substitution and other “innovations” IoT networks. Users also track “suspicious” activities, know the “standard methods” of fraudsters, resort to security outsourcing, cloud and fog computing.

The main problem in IoT networks is security, protection from intruders, they can harm not only things, but also a person, for example, by turning off a video surveillance system or a fire extinguishing system without permission. The study of IoT security is an urgent task, not only software-technical and technological, but also socio-psychological and cognitive. The task is complicated by the increase in the number of devices [7] connected to the IoT network and their variety and quantity on the market. Therefore in our article this problem is investigated (on examples).

2. RESEARCH METHOD

The methods of developing and researching the infrastructure of a smart house are based on equipment and systems that should ensure a high (by order of magnitude) increase in comfort, reliability, "obedience" of the house and things in it to residents. For example, the refrigerator "itself" will send an order to the chain store for products ending in it, even if the owner is not present. "Smart" at home is determined by functionality, intelligence, and the degree of automation. In particular, an intelligent light switch is a multi-channel mini-controller that controls a cluster of lamps and electrical appliances.

Intelligent automation of the house is based on network, internet control and control of the subsystems of the house: lighting, heating, blinds, ventilation, security and others. Therefore, the system equipment is subject to high requirements both in terms of functionality, capabilities, information exchange, and both home (internal) multimedia, and external abilities, for example, perimeter control of the house or mobile communication with residents in the office.

Typically, such equipment includes:

- "SMART" switches and lines;
- Motion sensors with applications;
- Electromagnetic switch-switches, regulators;
- Infrared and electromagnetic sensors, controllers controlled and controlled remotely (mobile);
- Cable, network equipment;
- Communication, distribution, and other equipment.

Common IoT architecture-three-level: levels of perception, network and application. At each level their own tasks, their own software and standards of security solutions. At the network level, heterogeneity of structures (variety of sensors, things, network technologies) and "power" (number of objects) of the system are important. Here, failures, distributed denial of service (DdoS) attacks (congestion in the network), poor real-time testing (poor use of environmental load simulators) is important.

There are also works involving more groups, for example, in the work [8] 5 classes are offered, with intermediate classes to the three classes of architecture indicated by us. All IoT applications can be combined, as in [9], into three groups: IIoT (industry); 2) EIoT (environment); 3) SOoT (society). Figure 1 shows the block diagram of the SMART-LPU system (environment).

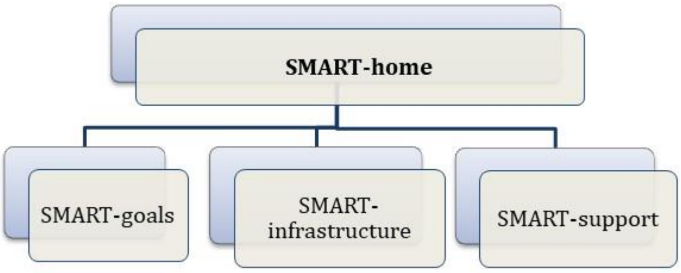

Figure 1. SMART-home

In a smart home, sensors and modules for various purposes are a full-fledged and unified subsystem for efficient functioning and control of the entire system. The reliability of a smart home depends on the relevance of the selection and installation of sensors, as well as directly the places of collection and selection, and analysis of primary data, for example, the conversion of electromagnetic signals to digital.

Sensors of different profiles are used:

- Analyzers for detecting instability (risk state, for example, CO2) and subsequent signaling;
- Radio frequency identification (RFID);
- Converting the Z-Wave signal to infrared;
- USN sensor networks (Ubiquitious Sensor Networks);
- Multisensory;
- Temperature;
- Central administration;
- Connections ("smart socket").

There are various approaches and systems of hardware [10], information, logical and technological solutions of the smart house class, for example:

- X10/S10-communication through existing power networks [11];
- Z-Wave-wireless communication (in particular, at a frequency of 868.42 MHz, [12]);
- ZigBee-ultra-low power wireless secure networks [13];
- Beckhoff-productive communication by open standards [14];
- Arduino-accessible, with minimal financial expenses, constructive and quickly mastered (programmable) communication [15].

Gartner publishes the annual technology maturity cycle report, which chronologically reflects innovative technologies and research. Now IoT has a "peak of expectations." IoT-a network concept, a paradigm of interactions of things (between themselves and with the environment). The goal is to use Internet networks and IT infrastructure to go beyond ordinary internet interactions. In the interests of the end user of the service, for example, smart-home, and production (IIoT).

Each has the properties of emergence [16], [17]. A quick, complex response is needed to events (often touch, WSN) and data (often disparate). For example, in the thermal control system of a smart home or video tracking. This takes into account the security of the entire IoT environment-a thing, a host and a system. This will require new perspectives not only on safety policy, but also on resource provision, profitability and environmental friendliness. For example, air conditioning in a smart home poses urgent tasks to improve the efficiency of air conditioning using solar panels, and removing hot air outside.

To go to industry 5.0 [18] "The internet of things" (internet of things, IoT) which is often identified with SMART processes is necessary SMART-support on evolutionary and self-organizational processes [19] and the internet of knowledge (IoK) [20]. In a narrow meaning, SMART stands for self-monitoring, analysis and reporting technology. With support for big data, data mining, Periodic limb movements in sleep (PLMS) (application software for product lifecycle management) and technology of digital manufacturing and industrial internet. Projects of the industry 5.0, intellectual infrastructure of people, robots, productions, processes and objects are also considered by many, for example, in [21]. In addition to traditionally solved network problems (combining heterogeneous networks, and blocking), specific problems are also solved in

IoT interactions-both direct and reverse, identification, parametric control. For example, the following problems can be solved [22], [23]:

a) Collisions of "things", data, routes, in particular, the discrepancy between the current commands and the conditions of the prophetic (environment);

b) Connecting things with an acceptable time delay, consistent with the dynamic parameters of virtual channels and routes;

c) Evolutionary capacity of the IoT-environment, "threshold capacity" of a cluster of things and alternatives of routes in network, the system analysis and synthesis, modeling of interactions.

They can communicate with cloud services, distributed devices, monitor parameters (Big Data), and contact emergency services if necessary [24], [25] as shown in Figure 2.

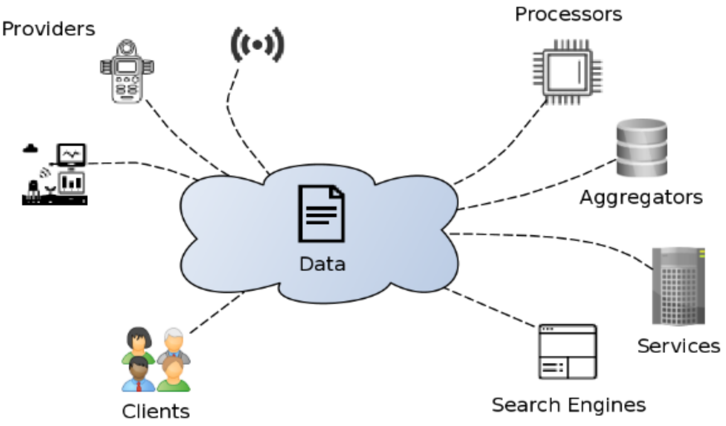

Figure 2. Using a typical cloud-based framework

3. DISCUSSION OF INFRASTRUCTURE AND SOLUTION

3.1. System-evolutionary analysis and self-organization of IoT in the modern industrial world (Industry 4.0)

IoT-distributed touch and network (sensors, network providing) and infrastructure's infological level (data, algorithms, models) of interactions and services in "space of things" (physical devices) and "space of people" (work, rest, the house, sport, and training). Therefore, it requires a systematic approach to research, systems analysis and synthesis. We carry out this analysis based on the P2P (point-to-point) model of interactions.

The purpose is intellectualization (improvement of comfort and safety, stability) of a situation of rest, work, the house and consumer qualities and opportunities of ordinary things and safety. Sensors, monitors, by means of the IoT-standard (IEEE1888) conduct remote control and management of network of things, modes, and situations. For example, if sensors of a system of video surveillance recorded the suspicious movement and it is necessary to send the SMS to the owner to office. There is a lot of things, they are various-from simple motion sensors in the system of video surveillance to the devices making an intelligent solution.

SMART-subsystems will be in the lead: cities, industry, health care, housing, and car. Traffic is threatened by avalanche danger though IoT uses, generally wireless technologies of IEEE standards are Wi-Fi 802.11, Zig Bee 802.15.4, and Blutheoth 802.15.1. Standards are focused on lower power consumption, energy efficient protocols and low cost of network services. IoT base as it is told, divide into three categories: industrial-smart-factory ("the smart enterprise"); social-smart-town ("the smart city"); household-smart-home (smart home). Also intermediate levels which we don't consider so far are possible.

The transition to the IoT paradigm initiates the reengineering of administrative (special social) procedures, industries and societies, especially education. We need not only competent, but also creative, “flexible” (self-learning) specialists and even housewives. The key factors that increase the complexity of the safe functioning of IoT systems, energy saving, development by the inhabitant, data protection and identification of legal ones, may be difficult authorization (authentication), diagnostics of "things", operations with cryptographic keys. The owner of these, inter-legal communications, management (OS, SIEM) and other factors. Although IoT is not a standardized, universal concept, there are verified (tested) models for the interactions of IoT systems.

Industry 4.0 is positioned as a post-industrial production based on a global infrastructure for making production decisions that increase the effectiveness and quality of products at the “vertical” (“horizontal”) levels of time thanks to digital technologies, analytics and intellectualization of processing systems in a broad sense (data, products). The SMART subsystem and infrastructure elements are implemented everywhere-smart cities, smart homes, smart roads, smart transport, smart contract, smart clinic, and smart data processing (based on data mining). It is necessary to systematically analyze, try to predict the evolutionary potential of the IoT.

Obviously, over time, the evolution of the IoT will require the involvement of models of the P4P, and M4M class. When the IoT becomes self-organizing, high-speed, scalable, secure, and resistant to attacks, failures of elements (and even subsystems), a "dense" and "almost everywhere compact" network with a mesh topology, then there will be functionality, a hosted service available in cloud computing and fog computing. Interactions are formed and implemented at the following architecture levels:

- Interactions in the real mode with an environment (sensors, locks, protocols, networks);
- Transport network platforms;
- Services of data-logical and analytical support of secure interactions;
- Applications (on scopes of application, distributed horizontally and vertically, especially corporate).

We will consider coordinated with a system task of this section, a problem of modeling of behavior in the environment of IoT.

3.2. Modeling of IoT systems and solutions based on sockets

First, make a general note of the vulnerability analysis models. There is a general theorem (Harrison, Ruzzo, Ullman, 1976) on the intractability of the computer security problem, but the take-grant model has advantages. It is used when analyzing access rights according to the access graph (nodes-objects or subjects IoT, arcs correspond to access rights). Graph conversion rules are applied to determine whether such rights can be obtained. We believe that an extended version of the model can consider information flows in systems with a distinction of rights. It confirms/refutes the degree of security of the system according to the requirements regulations.

So, the graph model is given by a finite oriented weighted graph without loops:

$$G = < S, O, E >,$$

where O is the set of objects IoT, S is the set of subjects, $E \in OxOxR$ is the arcs of the graph. In the model, there are two basic rules, Apply, Allow, and two non-basic rules, create, restrict, which can be described syntactically as:

Apply (r, x, y, s);
Allow (r, x, y, s);
Create (r, x, s);
Limit (r, x, s);
($r \in R$, $s \in S$, $x,y \in O$).

Each rule is associated with a "safety" score (weight value), which can be constant, depending on the rank (specificity) of the rule, on the number of participants applying this rule, on the degree of interaction of objects. The cost (safety) of the entire path on the graph is determined by the sum of the safety estimates of all applied rules. By using them, we reproduce the state of the system for various access rights, this gives analytics, an assessment of possible threats.

Modeling of IoT systems is often focused on simulation models. In addition to the above formal mathematical description of the model, you can build problem-oriented. Consider one of these useful models, although it is impossible to predict complex, poorly structured and formalized systems and processes with classical models. Many factors affect: delays, traffic, unequal potential, and dynamically changing value.

The density of the time delay probability distribution is the main "generator" of the simulated processes (or sockets IoT), for example, it is approximated for the Xiaomi socket with a distribution function (semi-experimental dependence) of the form:

$$F(x;\alpha;\beta) = x^{\beta}/(x^{\beta}+\alpha^{\beta})\ ,$$

where,

$$\alpha = 8.4;\ \beta = 21;\ \gamma = -2.5041.$$

For the broadlink outlet, you can take the logonormal distribution function with the appropriate parameters when sending packets to the outlet. The density of the distribution of sockets and things (IoT), and especially the risks in real mode, is even approximately impossible to describe functionally. Therefore, instead of experimental dependencies, we propose to clearly identify the species dependence for assessing the risks of IoT vulnerability:

$$r(x) = \prod_{i=1}^{m} \left(\sum_{j=1}^{k_i} \alpha_j {x_i}^{\beta_j} \right)^{\frac{\gamma_i}{\beta_i}}.$$

where $x_i(t)$ is the i-th vulnerability factor; α_j - an indicator of the importance of taking into account flaws by x_j (if the remaining factors are considered optimal), β_i, γ_i- parameters reflecting the degree of influence of the factor (self-organizational qualities of things).

There are significant differences in the traffic of IoT devices that are not predicted during traffic jumps. This makes it difficult to model IoT security management processes. But here standard solutions also help. Consider one of them.

3.3. Standard Arduino platform IoT and solution

As standard solutions and IoT management tasks for Smart-home, we specify the following key tasks:

- Forecasting and planning of energy costs;
- Temperature control;
- Control of the condition in the room (air, light, presence);
- Prevention of communication failures (leaks, faults, hydraulic impacts).

The use of sensors in the smart home system gives residents, maintenance staff and guests the following key advantages:

- Controlled comfort (illumination, temperature, and humidity);
- Temporary or long-term benefits (savings and ergonomic);
- Guaranteed safety measure (control and warning);
- Economy (energy and time).

IoT does not provide system security completely, there are enough vulnerabilities. The safety problem is solved at all levels, but it is important to start with the level of sensors, and nodes. There are more risks and their diversity. For example, power failures, overloads, failures, incorrect routing, foreign sensors, "copiers" and forwarding, internet collisions, and "backdoors". The greatest safety risks are possible at the lower level (perception level).

We emphasize the proposed Arduino solution. It is a client-server, such as "thick server-thin client": collection, analysis, preliminary calculations are performed by a remote server, and Arduino and mobile applications are processing, connecting to the server for messages about changes in the house (lighting, temperature, and humidity). The server interactively sends information to the database and to the user (home owner) in a visual form. In interactive mode, for example, up and down movement is regulated, the smart home is controlled on the Arduino platform, scalable without skills. The digital infrastructure of the house is aimed at developing and using new opportunities and the best options for a comfortable stay in the house. Such options should be supported by the principle: "host access to infrastructure at any point, with any resource, at any time, for any purpose." The environment allows you to analyze and control the "Smart House" and the environment, for example, video surveillance, energy costs, and environmental condition.

4. CONCLUSION

Internet of things and smart-home have become promoted and popular concepts of a new consumer-level infrastructure, new requirements for the comfort of life. With the promotion of IoT, potential innovations are "growing." The usual form of the Internet goes into its modified and integrated version. The consumer IoT provides an opportunity to improve comfort and quality of life (fitness tracker, and smart-watch). They help collect and analyze data on physical activity, sleep quality of the user.

The further development of IoT is the key to the transition to Industry 4.0 and systems that were impossible without the maximum level of automation (intelligence) and direct interactions of machines, sensors, devices with each other and with the user. The introduction of smart devices and controllers improves the quality of management and improves the security policy of the environment. The consequence is to reduce risks, errors and increase competitiveness.

For IoT, three levels of data processing and reaction generation are systemic: a) object competencies (on things, interactions, response); b) transmission stability (network communication protocols, encryption, security); c) mining (neuro-computation, fuzzy data, and noise filtering and object identification). Last one remark. We have not addressed the above legal issues closely related to the security issue. But they are relevant, legislative initiatives are needed that regulate the procedure for using and protecting the collected information, moving to private clouds that belong to the user himself and are placed with him (on his equipment). After all, given the decrease in the cost of equipment (some already cost a couple of dollars), on which you can deploy your cloud and lower the entry threshold for its configuration, this option is seen as the most promising.

Technical unification and technological standardization require new approaches from IoT to the concept of infrastructure security. In the future, soon, IoT can directly influence life, social, state evolutionary goals and strategies, tactics. A systematic and evolutionary analysis is needed, taking into account the information and state, personal security of IoT users. It is necessary to model, test and verify such systems at all levels.

REFERENCES

[1] K. Ashton, “That internet of things,” *RFID Journal*, vol. 22, pp. 97-114. 2009, Accessed: Sep. 26, 2018. [Online]. Available: http://www.rfidjournal.com/articles/view?4986.

[2] K. A. Palaguta, I. S. Shubnikov, and A. L. Safonov, “Handbook of the module smart house,” *Kniga*, p. 184, 2016.

[3] M. N. Sokolov, K. A. Smolyaninova, and N. A. Yakusheva, “Internet of things security problems: Overview,” *Cybersecurity Issues. Special issue*, vol. 5, no. 13, pp. 33-35, 2015.

[4] J. Rozhkova, “The internet of things: Market forecasts,” Accessed: Jul. 11, 2021. [Online]. Available: https://www.likeni.ru/analytics/internet-veshchey-prognozy-po-razvitiyu-rynka.

[5] G. Quandeng, “Construction and strategies in IoT security system,” *Green Computing and Communications (GreenCom) IEEE International Conference on and IEEE Cyber*, Physical and Social Computing, 2013, pp. 1129-1132, doi: 10.1109/GreenCom-iThings-CPSCom.2013.195.

[6] Z. Baoquan, Z. Zongfeng, and L. Mingzheng, “Evaluation on security system of internet of things based on fuzzy-AHP method,” *(ICEE) International Conf.*, 2011, pp. 1–5, doi: 10.1109/ICEBEG.2011.5881939.

[7] N. S. Korshunov and M. V. Verba, “Analysis of internet of things security problems,” (in Russian), *Int. J. Humanit. Nat.Sci.*, vol. 1, no. 2, pp. 93-95, Jan. 2019, doi: 10.24411/2500-1000-2019-10540.

[8] Z.-K. Zhang *et al.*, “IoT security,” *SOCA'14: Proceedings of the 2014 IEEE 7th International Conference on Service-Oriented Computing and Applications*, Nov. 2014, pp. 230–234, doi: 10.1109/SOCA.2014.58.

[9] C. Perera, “Context aware computing for the internet of things: A survey,” *IEEE* Commun. *Surv. Tutor.*, vol. 16, no. 1, pp. 414-454, 2014, doi: 10.1109/SURV.2013.042313.00197.

[10] I. M. Kuznetsov, “IoT and smart home management systems,” no. 2, 2017, Accessed: Jul. 11, 2021. [Online]. Available: http://journal.mrsu.ru/arts/iot-i-sistemy-upravleniya-umnym-domom.

[11] Protocol X10: General Information. Accessed: Aug. 9, 2021. [Online]. Available: http://janto.ru/repository/smart-home/platform-l-x10.html.

[12] Z-Wave Plus™ Certification, Accessed: Aug. 10, 2021. [Online]. Available: https://z-wavealliance.org/z-wave_plus_certification.

[13] What is ZigBee, Accessed: Aug. 10, 2021. [Online]. Available: https://zigbeealliance.org/solution/zigbee.

[14] TwinCAT-solutions for IoT and Industry 4.0, Beckhoff Automation GmbH & Co. Germany. Accessed: Aug. 10, 2021. [Online]. Available: https://www.beckhoff.com/TwinCAT-Industry40, doi: 10.1016/S1365-6937(21)00192-1.

[15] M. Riley, “Getting started,” in Programming Your Home Automate with Arduino, Android, and Your Computer, Jacquelyn Carter, Ed., Dallas, Texas, USA: The Pragmatic Bookshelf, pp. 19-26, 2012.

[16] A. A. Sherstobitova, M. O. Iskoskov, V. M. Kaziev, M. A. Selivanova, and E. N. Korneeva, “University financial sustainability assessment models,” *Smart Innovation, Systems and Technologies*, vol. 188, pp. 467-477, 2020, doi: 10.1007/978-981-15-5584-8.

[17] M. A. Elizarov, “Models and algorithms of information interaction in internet of things networks,” Ph.D. dissertation, Dept. Tech. Sci., S-Petersburg Univ., S-Petersburg, p. 18, 2017.

[18] K. Manganello, “Will industry 5.0 really be revolutionary?” 2019, Accessed: Feb. 15, 2021. [Online]. Available: https://www.thomasnet.com/insights/will-industry-5-0-really-be-revolutionary.

[19] V. M. Kaziev and B. V. Kazieva, “The internet of things and the vulnerability of their and Us interactions,” *Collection of Scientific Works of the III International Scientific and Practical Forum* (November 16-21, 2020) ‘Russia, Europe, Asia: Digitalization of Global Space’, Nevinnomyssk, pp. 318-321, 2020.

[20] G. B. Evgenev, “Industry 5.0 as the integration of the internet of knowledge and the internet of things,” *Ontology of Design*, vol. 9, no. 1, pp.7-23. 2019, doi: 10.18287/2223- 9537-2019-9-1-7-23.

[21] N. I. Cherepanov, “Principles and approaches of application of industry 5.0 at the enterprise,” *Innovation and Investment*, no. 9, pp. 144-147, 2019.

[22] T. M. Tatarnikova and M. A. Elizarov, “Procedure for resolving conflicts in the RFID system,” *News of Universities. Instrumentation*, vol. 60, no. 2, pp.150-157, 2017, doi: 10.17586/0021-3454-2017-60-2-150-157.

[23] S. A. Soldatov, “Internet of things,” *Corporate Information Systems*, vol. 9, no. 1, pp. 47-52, 2021.

[24] T. M. Tatarnikova and M. A. Elizarov, “Simulation model of the virtual channel,” *Scientific and Technical Bulletin of Information Technologies, Mechanics and Optics*, vol. 16, no. 6, pp. 1120-1127, 2016, doi: 10.17586/2226-1494-2016-16-6-1120-1127.

[25] M. R. Schurgot, D. A. Shinberg, and L. G. Greenwald, “Experiments with security and privacy in IoT networks,” *Worldof Wireless, Mobile & Multimedia Networks (WoWMoM)*, 2015 *IEEE 16th International Symposium*, pp. 1-6, 2015, doi: 10.1109/WoWMoM.2015.7158207.

BIOGRAPHIES OF AUTHORS

Sarah Mohammed Shareef her M.Sc. degree in University of technology-2018. Baghdad, Iraq, and her B.Sc. from Al-Rafedain University-Iraq in 2006. Professionally she has worked in ministry of higher education-Baghdad-2008 before moving to the academia, currently works at Department of production Engineering and Metallurgy in University of Technology-Iraq, since 2010. Her research interested in computer interaction. She can be contacted at email: sarah.m.ali@uotechnology.edu.iq.

Zainab Adnan Abbas received the B.Sc. degree in computer science from the University of Baghdad, Iraq, the M.Sc. degree in fundamental information and information technology from the South Ural State University, Russia. She works at the Department of Registration and Students Affairs, University of Technology, Iraq, since 2005. She used to hold several administrative posts. She is currently teaching in the departments of University of Technology/undergraduate studies in addition to the administrative posts. She can be contacted at email: Zainab.A.Abbas@uotechnology.edu.iq.

Zahraa Mohammed Hilal her B.Sc. degree in computer science from the University of Baghdad, Iraq, and her M.Sc. degree in fundamental information and information technology from the South Ural State University, Russia. She works at the Department of Registration and Students Affairs, University of Technology, Iraq, since 2005. She used to hold several administrative posts. She is currently teaching in the departments of University of Technology/undergraduate studies in addition to the administrative posts. She can be contacted at email: Zahraa.M.Hilal@uotechnology.edu.iq.