IOT-BASED SMART ENVIRONMENTS: STATE OF THE ART, SECURITY THREATS AND SOLUTIONS

Ghizlane Ikrissi, Tomader Mazri
National School of Applied Sciences, University Ibn Tofail, Kenitra, Morocco – (ghizlane.ikrissi, tomader.mazri) @uit.ac.ma

KEY WORDS: Smart environments, IoT, Security threats, Countermeasures, Blockchain, Machine learning, smart city, smart home

ABSTRACT:

Smart environments provide many benefits to the users including comfort, convenience, energy efficiency, safety, automation, and service quality. The Internet of Things (IoT) has developed to become one of the widely used technologies in smart environments. Many security attacks and threats are generated by security flaws in IoT-based systems and devices, which may affect smart environments applications. As a result, security is one of the most important issues in any smart area or environment based on the IoT model. This paper presents an overview of smart environments based on IoT technology and highlights the main security issues and countermeasures in the four layers of smart environment IoT architecture. It also reviews some of the current solutions that ensure the security of information in smart environments applications.

1. INTRODUCTION

The smart environment is a term developed from the idea of Ubiquitous computing or physical word that contains numerous sensors, controllers, actuators and other computational elements that interact with each other to make people's lives more comfortable and smarter, facilitate communication and improve performance and quality of services. Briefly, the smart environment is the ability to get and apply knowledge independently in the surroundings (Ikrissi, Mazri, 2020).

The internet of things is one of the advanced technologies used in smart environments. It includes billions of smart "things" that are connected and capable of providing sensing acting and data processing capabilities to create value-added services for any application field (Patrono et al., 2020).

As one of the objectives of the smart environment is the improvement of quality of human life in terms of comfort and efficiency, the Internet of Things (IoT) paradigm has recently grown into technology for building and developing smart areas (Elrawy et al., 2018), which means that it becomes the key ingredient for the development of many smart environments such as smart cities, smart homes, smart campus, smart health etc, by automating things to communicate in a network to realize many services (intelligent identification, monitoring and tracking, automation, data management, green energy, etc.) (Ikrissi and Mazri, 2020b).

The advantages of IoT are nearly limitless and its applications are changing the way we live and work by saving resources and time. It also creates new opportunities for entities to collaborate on innovation, growth, and knowledge exchange (Deogirikar, Vidhate, 2017).

As the environments and applications become smarter, they are based on many resource-constrained IoT devices that are susceptible to a variety of vulnerabilities. All of this could put users' privacy at risk and lead to a slew of cyberattacks such as false data generation while manipulating sensing data, resulting in a loss of control over highly intelligent systems.

IoT technology, communication, and computation resources are used in smart cities to improve the quality of life and services available to citizens and urban environments. It can control objects in real-time and provide citizens with intelligent information in areas such as smart traffic management, smart transportation, traffic systems, and smart agriculture, etc (Al-Turjman et al., 2019).

Smart city applications can collect sensitive data, which may be vulnerable to a variety of security issues and threats that affect the privacy of the citizens. For example, users' location traces may be leaked by smart mobility applications. Also, Smart card services have a tendency to jeopardize citizens' card details and purchasing habits.

Furthermore, the smart home is regarded as an important domain in IoT applications; it is an interconnected environment in which various types of devices and things interact with one another via the internet. This contributes to home automation by making it smart and interconnected. In this smart environment, IoT can be used to remotely control electrical appliances to save energy, systems installed on windows and doors to detect intruders, and so on. Also, Monitoring systems are being used to track energy and water supply consumption (Hassija et al., 2019).

All the devices in a smart home environment are connected to the internet. As the number of devices in the smart home environment grows, so do the chances of malicious attacks. Smart home devices can now be accessed via the internet from anywhere at any time. As a result, the possibility of malicious attacks on these devices increases (Shouran et al., 2019).

In the Smart Agriculture domain, every aspect of traditional farming methods can be fundamentally improved by implementing IoT technologies in agricultural practices. IoT can help to improve several traditional farming issues, such as yield

optimization, drought response, irrigation, land suitability, and pest control (Ayaz et al., 2019).

The use of such advanced features in smart agriculture can assist in achieving high yields and saving farmers monetary losses. Controlling the weather can help to increase vegetable and crop yield and quality. Humidity and temperature control in grain and vegetable production can also assist in the prevention of fungus and microbial contaminants (Hassija et al., 2019).

Some IoT applications monitor the health and activities of farm animals by attaching sensors to the animals. If such applications are compromised, it may result in the theft of farm animals, as well as crop damage from adversaries (Hassija et al., 2019).

Another smart area is smart Grids which refers to a data communications network that is integrated with the power grid in order to collect and analyze data from transmission lines, distribution substations, and consumers (Ghasempour, 2019). Smart Grid is the most common application of smart metering, also there are some IoT applications that use this smart meter to measure electricity consumption, the weight of goods, the water pressure in water transport systems, optimize the performance of solar energy, monitor water, address the issue of electricity theft, and so on.

Despite this, smart metering systems are vulnerable to a wide range of physical and cyber-attacks. Some equipment is linked to smart meters, and the data collected from this equipment can be used to manage load and costs. An adversary's intentional intrusion into such communication systems may alter the collected information, resulting in monetary loss for service providers or consumers (Hassija et al., 2019).
As a result, security is critical in nearly all smart environments and IoT applications that have been or are currently being deployed.

As a result, the purpose of this paper is to present various IoT security attacks in smart environments, as well as some solutions based on the Internet of Things architecture, which is divided into four layers: (1) the physical layer, (2) the network layer, (3) the platform layer, and (4) the application layer (Figure 1).

The following is how the paper's content is organized: Section 2 includes the related works. Section 3 goes over some IoT security threats and countermeasures in smart environments. Section 4 discusses the primary solutions for dealing with these security threats and section 5 discusses the conclusions.

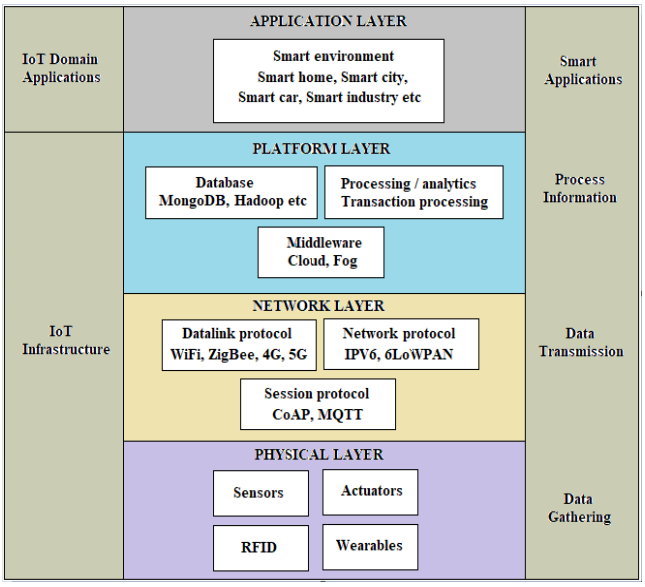

Figure 1. The IoT Architecture in Smart environments

2. RELATED WORKS

Many researchers investigate IoT security challenges and threats from a variety of perspectives. The authors (Nawir et al., 2016) studies IoT security issues in the health care, smart home, and transportation domains. In addition, because security is a major concern in the development of IoT, the paper discusses the vulnerability and Taxonomy of security attacks within IoT networks. It describes various types of IoT attacks such as Denial of Service, Spoofing, Replay Routing, Sybil attack, and so on. While The approach presented in (Gardašević et al., 2017)discusses the IoT system architecture in layers, including the design issues based on software and hardware components. It also identifies some IoT application domains, such as smart cities, healthcare, and agriculture, among others.

The researchers at (Alaba et al., 2017) investigate the state-of-the-art IoT security threats and vulnerabilities in application deployments such as smart environments, intelligent transportation, healthcare systems, and smart grid. They present an IoT security taxonomy based on current security threats in the contexts of application, architecture, and communication, as well as a comparison of potential IoT security threats and vulnerabilities, in order to propose some solutions for improving the IoT security architecture.

The authors in (Tweneboah-Koduah et al., 2017) present some IoT service domains and applications such as smart homes, smart grids, smart cities, and so on. They also discuss some cybersecurity challenges and present a taxonomy of cybersecurity attacks in which they discuss six types of vulnerabilities (IP misconfiguration, injection, Memory corruption, Code execution, DoS, CSRF, and XSS) with the corresponding threat vectors including physical network attack, software attack, device attack, data attack, and web interface attack.

The paper (Vashi et al., 2017), provides an overview of IoT

architecture in the smart world, which can be explained using five layers (Perception layer, Network layer, Middleware layer, Application layer, and Business layer), and then discusses security challenges and issues in these IoT architecture layers.

In (Varshney et al., 2019), the authors discuss the privacy and security challenges and attacks encountered while developing an IoT network. The taxonomy of these security attacks is based on a three-layer architecture (perception layer, network layer, and application layer), with each layer containing some security issues that can be distinguished by its technologies and functions. They also highlight some security measures proposed by various researchers to deal with IoT security breaches.

According to (Hassija et al., 2019), any IoT application is built on a four-layer architecture: sensing layer, network layer, middleware layer, and application layer. Each of these layers in an IoT application contains many devices and technologies that can cause a variety of security issues and threats. The paper discusses some security attacks in each layer and highlights in detail the four major classes of IoT security solutions which are: machine learning-based solutions, fog computing-based solutions, blockchain-based solutions, and edge computing-based solutions.

Another IoT Security Architecture with five layers is presented in (Pal et al., 2020), which includes device sensing, network management, service composition, application, and user interface layers. For each layer, the authors present the various components, main functionalities, and general security issues. and they categorize IoT attacks and security threats into five categories: communications, services/devices, mobility, users, and resource integration.

3. IOT SECURITY THREATS IN SMART ENVIRONMENTS

As previously stated, (Figure1), the IoT architecture of smart environments is made up of four layers. Each of these layers employs various technologies, which introduce a variety of issues, security attacks and threats. This section presents different security issues in IoT for these four layers (Figure2).

3.1 Security threats at the physical layer

The physical layer (the sensing layer) is the architecture's lower layer. This layer contains a variety of devices such as actuators and sensors, that gather data and send it to the architecture's upper layer.

The most common attacks on the physical layer are hardware attacks. The following are some security threats that can be found at this level of the architecture:

3.1.1 Sleep deprivation attack: The Internet of Things (IoT) employs a large number of devices that are powered by replaceable batteries to ensure high performance and to extend their lifetime. Adversaries can exploit this to increase the power consumption of the sensor nodes by keeping them awake or by running infinite loops in the devices using malicious code (Ikrissi and Mazri, 2020b). A dead battery causes a denial of service from the nodes in the IoT application (Hassija et al., 2019).

3.1.2 Capturing & Fake node injection: Attackers may attempt to capture, replace a node in the IoT system with a malicious node, or inject a fake or malicious node between network nodes. The attacker then takes control of the new node, which appears to be a part of the system, and gains access to the network, allowing him to control all network data flow. This could compromise the overall security of IoT applications (Khan and Salah, 2018).

3.1.3 Malicious code injection attack: In this attack, the attacker injects malicious code into the node's memory. It may use malicious code to force nodes to perform unintended functions or even gain access to the entire IoT system (Ahemd et al., 2017).

3.1.4 Eavesdropping attack: IoT applications are based on many nodes that are deployed in open environments. As a result, they are vulnerable to eavesdroppers. During various phases, such as data transmission or authentication, attackers may eavesdrop and capture data (Hassija et al., 2019).

Some physical layer countermeasures to mitigate such attacks include ensuring the authentication of devices. This means that the physical devices in IoT networks must authenticate themselves before sending and receiving data in order to be correctly identified in the system. As a result, no malicious devices will be able to access the network.

Furthermore, in an IPSec Security channel, we can differentiate between two secure functions: authentication and encryption. This mechanism can be used to prevent eavesdropping and node tempering attacks through encryption. As a result, the receiver can distinguish whether the sender of the data onto IP is real or fake.

In order to maintain data confidentiality, integrity, and privacy, some security techniques such as cryptography, error detection, and risk assessment must be used to avoid data security violations in IoT-based smart environments.

3.2 Security threats at the network layer

This layer is reliant on basic networks such as communication networks the internet and wireless sensor networks, etc. Its primary function is to transmit the data collected from the physical layer to the computational unit for processing (Al-Turjman et al., 2019).

The following are the major network layer security issues:

3.2.1 DDOS attack: In an IoT network, this attack aims to disrupt server availability through a flood of impersonated requests from distributed IoT devices on the communication channel (Vishwakarma and Jain, 2020). The network layer of the IoT is vulnerable to them due to the complexity and heterogeneity of IoT networks. Many IoT devices used in IoT applications are not securely configured, making them easy targets for DDoS attacks on target servers.

3.2.2 Routing attack: In this attack, malicious nodes in an IoT may attempt to redirect routing paths during data transmission, or create routing loops, allowing or dropping movement, sending

false error messages, and so on, which can cause the system to become convoluted (Hassija et al., 2019).

3.2.3 Sniffing attack: it is an attack that involves listening in on network packets. This attack is very common in wired and wireless networks, and it jeopardizes communication confidentiality. This attack can be carried out by an attacker using a compromised device or by directly capturing packets from the shared medium. Partially topological information, routing information, and data content may be obtained from sniffed packets (Kamble et al., 2017).

3.2.4 Traffic analysis attacks: In this attack, the attacker first obtains network information by using port scanning or packet sniffers, then he analyses the network traffic from user devices in order to get sensitive information about users. This is a passive attack that is difficult to detect (Hafeez et al., 2019).

Authentication mechanisms and encryption processes are two network layer countermeasures used to prevent unauthorized access to data on sensor nodes.

Besides that, ensuring routing security by utilizing a variety of secure routing algorithms is necessary to guarantee the confidentiality of data transferred to and from various sensor nodes in IoT. For example, using multiple paths provides secure routing, that fixes the errors of the networks and improves the system performance. Ad hoc (AOMDV) is a secure routing protocol that can deal with a variety of attacks, including wormhole attacks.

3.3 Security threats at the platform layer

It serves as an intermediary layer between the network and application layers. When IoT devices connect and communicate with one another, they generate a variety of services. The PLATFORM layer's function is to provide powerful computing storage capabilities, which means that it can store the information of the lower layer in databases and also retrieve, process, compute, and decide based on the computational results (Kumar and Smys, 2018).

This layer is vulnerable to a variety of attacks that can infect the middleware and take control of the entire IoT application. Here are some examples of attacks in the middleware layer.

3.3.1 Cloud malware injection: Using cloud malware injection, an attacker can gain control, inject malicious code, or inject a virtual machine into the cloud. The attacker impersonates a legitimate service by attempting to create a virtual machines instance or a malicious service module. In this manner, the attacker gains access to the victim's service requests and captures sensitive data that can be modified as desired (Hassija et al., 2019).

3.3.2 SQL injection: The attacker enters a SQL query into an unprotected field, which is then processed by a SQL database. This type of threat exists in all types of systems, including IoT. The main issue with SQL injection is that it can lead to privilege escalation, granting the attacker greater access to the system (Rizvi et al., 2018).

3.3.3 Storage attacks: In smart environments based on IoT there are large amounts of data containing the user's vital information that needs to be stored in the cloud or just on storage devices, both of which can be attacked and the data compromised or changed to incorrect details. The replication of data, combined with the availability of data to various types of people, results in a larger surface area for attacks (Kumar et al., 2016).

3.3.4 Side-channel attacks: This type of attack is based on discovering information by analyzing exposed side properties of the algorithmic implementation, such as power consumption, processing timing, associated sounds etc. This type of attack could occur as a result of a lack of secure methods for processing and storing IoT data, such as storing unencrypted data in the cloud or on IoT objects (Abdulghani et al., 2019).

Platform layer security concepts include the use of Web application scanners and web firewall applications, which aim to identify and detect various attacks and threats in the web application. In addition, cryptography techniques and Heper safe can be used to keep memory pages from being tampered with and provide data protection in the platform layer.

Moreover, to ensure data security and prevent confidential information leakage in the cloud, it is important to use fragmentation redundancy. Scattering implies that data on the cloud should be divided and allocated in different fragments or parts for storage in servers.

3.4 Security threats at the application layer

This is the top layer of the secure IoT architecture, and it is responsible for providing users with intelligent and smart applications and services based on their needs. Smart environments, such as smart cities, smart homes, transportation, utilities, and healthcare, are examples of these applications.

The security issues in this layer are specific to various applications; they may be related to privacy issues, data theft, and so on. Some of these security threats are listed below:

3.4.1 Reprogram attack: in some environments, a network programming system can be used to remotely reprogram IoT objects. If the process of programming is not protected, an attacker could use it to take control of a large portion of the IoT network (Abdul-Ghani et al., 2018).

3.4.2 Sniffing attack: In this type, the attacker introduces a sniffer application into the IoT system to force an attack on it, which could gain network information, resulting in a corrupted system and allowing the attacker access to confidential user data if sufficient security protocols are not in place to prevent it (Swamy et al., 2017).

3.4.3 Data thefts: IoT applications use, produce, and deal with a large amount of critical and private data, which is vulnerable to a variety of attacks. The adversary may use an insecure procedure or some data processing algorithms to steal users' confidential data, which may result in catastrophic damage.

3.4.4 Service interruption attacks: are also known as DDoS attacks or illegal interruption attacks. In this attack, the hacker logs into the system and pretends to be an authenticated user to disrupt the network's normal operation and prevent legitimate users from using the services (Swamy et al., 2017). This is one of the system's most serious and dangerous issues.

The most commonly used mechanisms in the application layer to protect data security and privacy are authentication, integrity, and encryption. They protect data from being hacked or stolen by preventing unauthorized access to it.

Furthermore, intrusion detection processes in this layer provide many security solutions to various attacks by producing alarms whenever malicious actions are performed in the system. An Intrusion Prevention System, also identifies security threats based on a variety of monitoring features and then blocks or remediates a detected threat. Besides, the use of ACLs can control traffic access and monitor access requests from multiple users in the IoT system. Firewalls are another process that is used to filter packets and block unauthorized users.

Some software, such as anti-spyware, anti-virus, and anti-adware, can provide security and ensure the dependability, integrity, and confidentiality of IoT data.

Application layer	**Malicious scripts** **Service interruption** **Data thefts** **Sniffing attack** **Reprogram attack**	**Data security** **Anti-viruses** **Anti-spyware** **Firwalls & ACLs**
Platform layer	**Man in the middle** **Cloud malware injection** **Side-channel attacks** **Storage attacks** **SQL injection**	**Hyper safe** **Homomophic encryption** **Web application scanners** **Fragmentation** **Redundancy scaterring**
Network layer	**Wormhole attack** **Routing attack** **Trafic attack** **DDOS attack** **Jamming attack**	**Routing protocol** **Routing security** **Data privacy** **Authentication** **Hello flood detection**
Physical layer	**Malicious code injection** **Faake node injection** **Sleep Deprivation** **Eavesdropping** **Jamming attack** **Social Engineering**	**Data privacy** **Secure booting** **Data integrity** **Risk assessment** **Device authentication** **Secure physical desing**

Figure 2. Security threats in IoT architecture layers

4. SECURITY SOLUTIONS FOR IOT-BASED SMART ENVIRONMENTS

In the previous session, we presented some countermeasures for dealing with security attacks in the IoT Architecture layers. In this section, we will look at some additional security and privacy solutions used to combat various threats and attacks in smart environments.

4.1 Lightweight Cryptography

Smart environments contain a great number of devices that store data transmitted through the IoT network, making this data vulnerable to a variety of security and privacy violations. This necessitates the use of encryption mechanisms to ensure the integrity and confidentiality of information. it is also a critical element for trusting transactions in smart environments.

However, due to the IoT device's limited computational capability, power resources, and memory, it is difficult to use traditional cryptographic algorithms that require intensive resources. So many researchers presented in (Bhardwaj et al., 2017) and (Dhanda et al., 2020) study and develop lightweight cryptography as a solution to the security problem of resource-constrained devices in IoT, as well as to maintain data security and authentication.

4.2 Blockchain

Blockchain is a P2P (peer-to-peer) centralized, distributed and public decentralized technique for storing agreements, sales, contracts and transactions across many computers. It is essentially a chain of blocks in which digital data is stored in a public database. Blockchain is designed specifically for cryptocurrencies such as Litecoin and Bitcoin.

Blockchain technology can be an essential key to controlling, managing and most importantly, resolving many IoT security issues. The transmitted data through the IoT devices and connected to the blockchain network is cryptographically signed and proofed by the true sender, who has a unique Global Unique Identifier and public key, which ensure the data integrity and authentication. Besides, all transactions made from or to an IoT device are registered on the blockchain distributed ledger and can be tracked in a secure manner (Khan, Salah, 2018).

Furthermore, by providing logic and de-centralized authentication rules, Blockchain smart contracts can guarantee single and multiparty authentication to an IoT device (Khan, Salah, 2018).

4.3 Machine learning

Machine learning is an artificial intelligence subset that aims to develop and create systems that can learn from previous experiences. It is one of the powerful techniques that has been used to create an intrusion detection system that plays a critical role in detecting malicious activities in the IoT network.

Many machine learning (ML) techniques can be used to create IDS models for securing networks in IoT environments. Some of these techniques have been presented in numerous studies. For example, in (Alsheikh et al., 2014), the authors investigate the benefits of using machine learning technology to provide security in WSNs. In addition, in (Aminanto et al., 2018) a novel model based on ML algorithms was developed to detect numerous attacks in Wi-Fi networks. Furthermore, some ML techniques, such as supervised and unsupervised learning, are used in (Miller, Busby-Earle, 2016)to detect the presence of a botnet.

4.4 Biometrics

One of the secure authentication solutions used in IoT-based smart environments is biometric recognition. This technology is based on human physiological traits and behavior, which are used to recognize people based on their faces, fingerprints, iris, DNA, gait, voices, handwritten signatures, and other characteristics.

We can divide identity issues in smart environments IoT systems into two categories: (1) identification and (2) authentication. Biometric security is used to protect the user's identity and to ensure the security of the authentication and recognition process.

The authors in (Obaidat et al., 2019), discuss some advantages of the biometric security system in various IoT applications. It can obtain more accurate and secure information than a password or PIN-based security system; it can also ensure accountability and scalability; and, most importantly, biometric information cannot be guessed or stolen, ensuring identity security.

5. CONCLUSION

Smart environments have the ability to improve people's quality of life and well-being. IoT as a one of advanced technologies implemented in smart environments (Smart home, smart city, smart car etc), can enable software, wearable devices, and other objects to communicate and share information over the internet.

Despite this, the IoT system and devices are vulnerable, insecure, and incapable of self-protection and defense for a variety of reasons, including limited resources in IoT devices, development and deployment issues, a lack of secure software and hardware design, and the diversity of IoT resources.

As a result, smart environments have become vulnerable to a wide range of security threats that put data privacy at risk of violations by malicious persons. All that makes security and privacy issues a major concern that requires efficient and effective solutions that must ensure the authentication, availability, integrity and confidentiality of data transmitted in the IoT network.

As a consequence, it is important to take into account the security and privacy threats when designing and implementing new smart systems. in this paper, we investigated and discussed security threats in various layers of IoT architecture. Then, we presented some solutions and mechanisms for securing Smart environments based on IoT technology.

REFERENCES

Abdul-Ghani, H.A., Konstantas, D., Mahyoub, M., 2018. A Comprehensive IoT Attacks Survey based on a Building-blocked Reference Model. International Journal of Advanced Computer Science and Applications (IJACSA) 9. https://doi.org/10.14569/IJACSA.2018.090349

Abdulghani, H.A., Nijdam, N.A., Collen, A., Konstantas, D., 2019. A Study on Security and Privacy Guidelines, Countermeasures, Threats: IoT Data at Rest Perspective. Symmetry 11, 774. https://doi.org/10.3390/sym11060774

Ahemd, M.M., Shah, M.A., Wahid, A., 2017. IoT security: A layered approach for attacks defenses, in: 2017 International Conference on Communication Technologies (ComTech). Presented at the 2017 International Conference on Communication Technologies (ComTech), pp. 104–110. https://doi.org/10.1109/COMTECH.2017.8065757

Alaba, F.A., Othman, M., Hashem, I.A.T., Alotaibi, F., 2017. Internet of Things security: A survey. Journal of Network and Computer Applications 88, 10–28. https://doi.org/10.1016/j.jnca.2017.04.002

Alsheikh, M.A., Lin, S., Niyato, D., Tan, H.-P., 2014. Machine Learning in Wireless Sensor Networks: Algorithms, Strategies, and Applications. IEEE Communications Surveys Tutorials 16, 1996–2018. https://doi.org/10.1109/COMST.2014.2320099

Al-Turjman, F., Zahmatkesh, H., Shahroze, R., 2019. An overview of security and privacy in smart cities' IoT communications. Transactions on Emerging Telecommunications Technologies. https://doi.org/10.1002/ett.3677

Aminanto, M.E., Choi, R., Tanuwidjaja, H.C., Yoo, P.D., Kim, K., 2018. Deep Abstraction and Weighted Feature Selection for Wi-Fi Impersonation Detection. IEEE Transactions on Information Forensics and Security 13, 621–636. https://doi.org/10.1109/TIFS.2017.2762828

Ayaz, M., Ammad-Uddin, M., Sharif, Z., Mansour, A., Aggoune, E.-H.M., 2019. Internet-of-Things (IoT)-Based Smart Agriculture: Toward Making the Fields Talk. IEEE Access 7, 129551–129583. https://doi.org/10.1109/ACCESS.2019.2932609

Bhardwaj, I., Kumar, A., Bansal, M., 2017. A review on lightweight cryptography algorithms for data security and authentication in IoTs, in: 2017 4th International Conference on Signal Processing, Computing and Control (ISPCC). Presented at the 2017 4th International Conference on Signal Processing, Computing and Control (ISPCC), pp. 504–509. https://doi.org/10.1109/ISPCC.2017.8269731

Deogirikar, J., Vidhate, A., 2017. Security attacks in IoT: A survey, in: 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC). Presented at the 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), pp. 32–37. https://doi.org/10.1109/I-SMAC.2017.8058363

Dhanda, S.S., Singh, B., Jindal, P., 2020. Lightweight Cryptography: A Solution to Secure IoT. Wireless Pers Commun 112, 1947–1980. https://doi.org/10.1007/s11277-020-07134-3

Elrawy, M.F., Awad, A.I., Hamed, H.F.A., 2018. Intrusion detection systems for IoT-based smart environments: a survey. Journal of Cloud Computing 7, 21. https://doi.org/10.1186/s13677-018-0123-6

Gardašević, G., Veletić, M., Maletić, N., Vasiljević, D., Radusinović, I., Tomović, S., Radonjić, M., 2017. The IoT Architectural Framework, Design Issues and Application Domains. Wireless Pers Commun 92, 127–148.

https://doi.org/10.1007/s11277-016-3842-3

Ghasempour, A., 2019. Internet of Things in Smart Grid: Architecture, Applications, Services, Key Technologies, and Challenges. Inventions 4, 22. https://doi.org/10.3390/inventions4010022

Hafeez, I., Antikainen, M., Tarkoma, S., 2019. Protecting IoT-environments against Traffic Analysis Attacks with Traffic Morphing, in: 2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops). Presented at the 2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), pp. 196–201. https://doi.org/10.1109/PERCOMW.2019.8730787

Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., Sikdar, B., 2019. A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures. IEEE Access 7, 82721–82743. https://doi.org/10.1109/ACCESS.2019.2924045

Ikrissi, G., Mazri, T., 2020a. A STUDY OF SMART CAMPUS ENVIRONMENT AND ITS SECURITY ATTACKS. ISPRS - International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences XLIV-4/W3-2020, 255–261. https://doi.org/10.5194/isprs-archives-XLIV-4-W3-2020-255-2020

Ikrissi, G., Mazri, T., 2020b. A STUDY OF SMART CAMPUS ENVIRONMENT AND ITS SECURITY ATTACKS. ISPRS - International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences XLIV-4/W3-2020, 255–261. https://doi.org/10.5194/isprs-archives-XLIV-4-W3-2020-255-2020

Kamble, A., Malemath, V.S., Patil, D., 2017. Security attacks and secure routing protocols in RPL-based Internet of Things: Survey, in: 2017 International Conference on Emerging Trends Innovation in ICT (ICEI). Presented at the 2017 International Conference on Emerging Trends Innovation in ICT (ICEI), pp. 33–39. https://doi.org/10.1109/ETIICT.2017.7977006

Khan, M.A., Salah, K., 2018. IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems 82, 395–411. https://doi.org/10.1016/j.future.2017.11.022

Kumar, R.P., Smys, S., 2018. A novel report on architecture, protocols and applications in Internet of Things (IoT), in: 2018 2nd International Conference on Inventive Systems and Control (ICISC). Presented at the 2018 2nd International Conference on Inventive Systems and Control (ICISC), pp. 1156–1161. https://doi.org/10.1109/ICISC.2018.8398986

Kumar, S.A., Vealey, T., Srivastava, H., 2016. Security in Internet of Things: Challenges, Solutions and Future Directions, in: 2016 49th Hawaii International Conference on System Sciences (HICSS). Presented at the 2016 49th Hawaii International Conference on System Sciences (HICSS), pp. 5772–5781. https://doi.org/10.1109/HICSS.2016.714

Miller, S., Busby-Earle, C., 2016. The role of machine learning in botnet detection, in: 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST). Presented at the 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST), pp. 359–364. https://doi.org/10.1109/ICITST.2016.7856730

Nawir, M., Amir, A., Yaakob, N., Lynn, O.B., 2016. Internet of Things (IoT): Taxonomy of security attacks, in: 2016 3rd International Conference on Electronic Design (ICED). Presented at the 2016 3rd International Conference on Electronic Design (ICED), pp. 321–326. https://doi.org/10.1109/ICED.2016.7804660

Obaidat, M.S., Rana, S.P., Maitra, T., Giri, D., Dutta, S., 2019. Biometric Security and Internet of Things (IoT), in: Obaidat, M.S., Traore, I., Woungang, I. (Eds.), Biometric-Based Physical and Cybersecurity Systems. Springer International Publishing, Cham, pp. 477–509. https://doi.org/10.1007/978-3-319-98734-7_19

Pal, S., Hitchens, M., Rabehaja, T., Mukhopadhyay, S., 2020. Security Requirements for the Internet of Things: A Systematic Approach. Sensors 20, 5897. https://doi.org/10.3390/s20205897
Patrono, L., Atzori, L., Šolić, P., Mongiello, M., Almeida, A., 2020. Challenges to be addressed to realize Internet of Things solutions for smart environments. Future Generation Computer Systems 111, 873–878. https://doi.org/10.1016/j.future.2019.09.033

Rizvi, S., Kurtz, A., Pfeffer, J., Rizvi, M., 2018. Securing the Internet of Things (IoT): A Security Taxonomy for IoT, in: 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE). Presented at the 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), pp. 163–168. https://doi.org/10.1109/TrustCom/BigDataSE.2018.00034

Shouran, Z., Ashari, A., Priyambodo, T.K., 2019. Internet of Things (IoT) of Smart Home: Privacy and Security. https://doi.org/10.5120/IJCA2019918450

Swamy, S.N., Jadhav, D., Kulkarni, N., 2017. Security threats in the application layer in IOT applications, in: 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC). Presented at the 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), pp. 477–480. https://doi.org/10.1109/I-SMAC.2017.8058395

Tweneboah-Koduah, S., Skouby, K.E., Tadayoni, R., 2017. Cyber Security Threats to IoT Applications and Service Domains. Wireless Pers Commun 95, 169–185. https://doi.org/10.1007/s11277-017-4434-6

Varshney, T., Sharma, N., Kaushik, I., Bhushan, B., 2019. Architectural Model of Security Threats theirCountermeasures in

IoT, in: 2019 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS). Presented at the 2019 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), pp. 424–429. https://doi.org/10.1109/ICCCIS48478.2019.8974544

Vashi, S., Ram, J., Modi, J., Verma, S., Prakash, C., 2017. Internet of Things (IoT): A vision, architectural elements, and security issues, in: 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC). Presented at the 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), pp. 492–496. https://doi.org/10.1109/I-SMAC.2017.8058399

Vishwakarma, R., Jain, A.K., 2020. A survey of DDoS attacking techniques and defence mechanisms in the IoT network. Telecommun Syst 73, 3–25. https://doi.org/10.1007/s11235-019-00599-z