https://doi.org/10.48009/2_iis_2020_93-101
Issues in Information Systems
Volume 21, Issue 2, pp.93-101, 2020

ANALYZING COLLEGE STUDENTS' PRE-KNOWLEDGE AND POST-KNOWLEDGE OF EMBEDDED SOFTWARE SECURITY AND ITS IMPACT TOWARDS FUTURE INTERNET OF THINGS (IOT) DEVELOPMENTS

Mel Tomeo, Miami Dade College, mtomeo@mdc.edu
David Hertz, Pittsburgh Technical College, hertz.david@ptcollege.edu
John J. Scarpino, Pittsburgh Technical College, scarpino.john@ptcollege.edu
Lee Cottrell, Pittsburgh Technical College, cottrell.lee@ptcollege.edu
Wilfred Mutale, Pittsburgh Technical College, mutale.wilfred@ptcollege.edu

ABSTRACT

The purpose of this study is to compare the results between two different colleges regarding how college students in Computer Programming (CP) and Information Technology (IT) perceive security issues related to how the Internet of Things (IoT) plays a role in their majors. Security issues within the IoT are part of the challenges facing this ubiquitous emerging technology implementing embedded software applications. In this paper, we analyzed the results from the study of students' pre-knowledge and post-knowledge on the impact of security issues in the IoT embedded software applications. This study was conducted as a collaborative initiative between two colleges, Miami Dade College (MDC), located in Miami, Florida, and Pittsburgh Technical College (PTC), located in Pittsburgh, Pennsylvania. The findings indicated that students believed exposure of private information was important to IoT security and that IoT vulnerabilities have changed over the last 5 years.

Keywords: Embedded Software Security, IoT Applications, Software Security, Application Security, Software Vulnerability, IoT Security

INTRODUCTION

The Internet of Things (IoT) concept was first created by Kevin Ashton in 1999 (Ashton, 1999). Since then, it has gained enormous attention due to rapid technological advancements and the amount of convenience that could be added to an individual's lifestyle (Celik, Fernandes, Pauley, Tan, & McDaniel, 2019). According to Amer and Alqhtani (2019), there are 30 billion connected IoT devices with approximately 200 billion connections worldwide. Specifically, in China, there are currently 15 billion IoT devices, and the number is expected to continue to increase as new technology is being created (Amer & Alqhtani, 2019). The majority of these IoT devices and applications were not designed to handle the security and vulnerability attacks that they are encountering.

Mahmoud, Yousuf, Aloul, and Zualkernan (2015) defined the IoT as "a collection of many interconnected objects, services, humans, and devices that can communicate, share data, and disseminate information to achieve a common goal in different areas and applications" (p. 1). IoT applications can be found in many industries of the world, such as transportation, agriculture, healthcare, energy production, and distribution (Ammar, Russello, & Crispo, 2018). IoT applications could transform current lifestyles by making intelligent devices perform daily tasks faster, giving individuals the ability to spend time on more important matters. Examples of popular IoT applications that are changing lifestyles are smart homes and smart transportation (Mahmoud et al., 2015). The era of IoT is changing individuals' lives due to the significant benefits that IoT applications can provide. This increase in IoT brings many new security threats, making IoT applications vulnerable (Yu, Sekar, Seshan, Agarwal, & Xu, 2015). Within IoT applications, an individual's personal information can be collected automatically, tracked, and monitored (Celik et al., 2019). The security of the user's personal information on an IoT device is very important because their private data is being shared among various types of other IoT devices (Razzaq, Gill, Qureshi, & Ullah, 2017). IoT devices currently have a higher rate of cybersecurity attacks compared to a traditional network, resulting in increasing security protocols (Tariq et al., 2019).

The following will present a review of the literature to give a better understanding of the importance of this study. Previous studies focused on IoT applications regarding their security and impact on society will be discussed. The methodology of this study will be described, followed by the results. Finally, the limitations, conclusions, and future recommendations on how to extend this study will be offered.

LITERATURE REVIEW

IoT's impact on an individual's safety, security, and privacy is a very sensitive and extremely complex topic. Due to the complexity of IoT applications, protecting these applications from cyber threats requires specific security measures (Yu et al., 2015). IoT applications have layers that are defined by functions and the devices that are used in that layer (Azza, Hanaa, & Elmageed, 2019). Security measures need to be implemented within each layer of an IoT application (Ning & Liu, 2012). An IoT application can be divided into three layers: perception, network, and application (Azza et al., 2019).

Khattak et al. (2019) described the perception layer to be the lowest, and it acquires data from the environment with the help of sensors. They explained that this layer is significant because it identifies other IoT applications within its surroundings. They used this layer in their study to detect, collect, and process information. Khattak et al. (2019) found this layer was important because it takes information and transmits it to the network layer. They suggested four main security objectives that should be taken into consideration during the implementation of security measures in this layer were authentication, data privacy of sensitive information, user anonymity, and risk assessment.

Bello, Zeadally, and Badra (2017) described the network layer as the middle, which receives information from the perception layer. They explained that this layer determines the route of how the sensor data will locate the different devices over the internet. Examples that Bello, Zeadally, and Badra gave in their study of these devices were hubs, routing devices, and a gateway. They found that these devices all operate using different communication technologies, resulting in the network layer playing a vital role in determining the correct route the sensor data will obtain. This network also handles any network congestion that the IoT application encounters. They suggested four main security objectives that should be taken into consideration during the implementation of security measures in this layer were intrusion detection, data encryption, routing security, and data integrity.

Swamy, Jadhav, and Kulkarni (2017) described the application layer as the top, which obtains information from the network layer. They explained that this layer delivers application services to the users. They conducted an exploratory study into understanding how this layer was related to the interface between the IoT application and the network. They found that the main purpose of the application layer was to create a smart application environment. They suggested five main security objectives that should be taken into consideration during the implementation of security measures in this layer were integrated identity identification, data encryption, firewalls, risk assessment, and intrusion detection.

Each IoT layer is vulnerable to security threats and attacks. Zeng et al. (2017) explored how these threats and attacks could be active or passive and could be developed from external sources or internal networks. They found that the difference between an active attack and a passive attack was that an active attack directly stopped the service. They explained that a passive attack could monitor and record IoT network information without interrupting the performance of the IoT application. An example that they gave was called the Denial of Service attacks (DoS). Zeng et al. (2017) described this intrusion as a threat that could occur at every layer of an IoT application. These attacks could make the IoT application unavailable to the users. Their results indicated that each layer had specific attacks that made it vulnerable, resulting in the need for security measures to be developed and implemented at every layer of an IoT application during its lifecycle.

IoT Security Challenges

Guo and Heidemann (2018) conducted an exploratory study into how security challenges of the IoT could be addressed by creating a set of development guidelines. These guidelines included topics such as checking for security vulnerabilities, securing the deployment of the application, ensuring continuity of secure development in cases of integrators, and ensuring continuous delivery. They found that implementing secure development guidelines across the development lifecycle of an IoT application could decrease security vulnerabilities and develop a more secure product. Their results indicated that guidelines could potentially help identity relevant assets, threats, risks, and attack scenarios throughout the development lifecycle of an IoT application. They suggested that these guidelines should not only focus on smart devices, network protocols, and communications, but also take into consideration the integrity of design principles throughout the software development lifecycle.

Saleh, Aly, and Omara (2016) conducted an exploratory study into how security challenges could be decreased with the use of cryptography and steganography techniques. They reviewed previous literature regarding how these techniques could be crucial when dealing with the user's authentication and data privacy. They found that one technique, called the "Galois cryptography" technique, which was used by Khari et al. (2019), was very useful due to its ability to encrypt confidential data that came from different medical sources. They also found that machine learning techniques could enhance the security of IoT devices.

Bertino (2016) investigated how simple IoT security measures could be implemented to help decrease the challenges and threats that organizations encounter daily. One measure that was explored was related to understanding how an organization could implement employees into making sure that the software running on all IoT devices was authorized. A second measure that was investigated was how employees should authenticate the IoT application through the network when it was first turned on before collecting or sending data. A third measure that was suggested would be to implement a firewall within the IoT application to filter unwanted threats directed at the device. A fourth measure that was explored was related to the IoT applications being updated with the most current patches.

Importance of Embedded Software Security

Software is the building block of every IoT application; it enables the IoT's functionality and provides the ability to add features to the IoT application. Frazelle (2019) conducted a systematic literature review into how firmware can be vulnerable to an IoT application. Frazelle described firmware as a type of software that allows a device to operate and interact with other parts of the application. Frazelle explained that firmware is important due to it having the most access to privileged information. IOT devices could use the same firmware as a Personal Computer. Frazelle found that firmware could be an attractive target for a hacker on many levels because it had access to all parts of the computer. Frazelle found in the literature review that compromising the firmware on a device could provide a permanent backdoor because the firmware was usually not rewritten when a device was restarted.

Perumal and Manohar (2017) investigated how embedded software security should move to the forefront during the software development life cycle. They believed that having this type of mindset would protect the data within the application and protect the user interfaces from the very beginning stages of development. They found that one way of improving embedded software security was by creating a five-step checklist that could be implemented during the development of an IoT application. This five-step checklist would consist of:

1. All unnecessary programs should not have the ability to execute.
2. All data must be private, and programs should not be allowed to expose information to each other.
3. All information should be verified.
4. All devices should be secured during boot time and require validation before transmitting or receiving data.
5. All programs should be able to encounter anomalies and handle the issues.

Future of IoT Developments

Badran (2019) investigated the different security requirements for IOT devices in the United Kingdom, European Union, Australia, and Canada. Badran's investigation revealed that each country had a different set of security requirements for IoT devices. This investigation led Badran to propose a universal five-level classification system for IOT device security. This system would classify devices based on the impact on the consumer and their private data if the device was compromised. Badran's results indicated that a gap in the literature revealed the need for a set of security requirements for all IoT devices to follow. The set of requirements should be accessible to consumers.

Hewitt (2016) suggested that a future development regarding IoT applications could be the idea of having a backdoor into IoT applications. A backdoor could essentially allow security agencies of each country the ability to monitor and control IoT devices in their own country. Hewitt believed that this could lead to the exchange of surveillance information with other countries. A possible problem with this future development is that security agencies would have the ability to access and control large numbers of devices with the possibility to abuse surveillance and control capabilities. Having a backdoor would also create a security issue and could cause IoT applications to be vulnerable.

RESEARCH METHODOLOGY

The main research question that this study addressed was: Does introducing the importance of embedded software security and its impact on IoT applications change the students' conception of software application security? The two specific research questions that this study addressed were:

RQ1: By educating the participants on the importance of embedded software security and its impact on IoT applications, will users have a new conception towards reducing the possibilities of encountering IoT security vulnerabilities?

RQ2: By comparing the same data set of students from two different colleges but in two different time settings, will there be a significant change of conceptual view from before being introduced to embedded software security and its impact on IoT applications to after they have completed their learning?

Research Instruments

All the constructs were measured with previously validated instruments. In this study, two surveys were conducted on students pursuing associate degrees. The instruments used in the study were a series of survey questions that were measured on a 4-point Likert-type scale in which 1 denoted "strongly disagree (SD)," 2 denoted "disagree (D)," 3 denoted "agree (A)," and 4 denoted "strongly agree (SA)." The participants for the surveys were sent a link through email to access the questionnaire between February 2020 and March 2020. The targeted participants were students who were in their freshman year. Participants were given an introduction and the purpose of the survey before being asked to take it. Participants were expected to fully understand the purpose of the survey and agree to the terms and conditions before proceeding to completing the survey. IRB approval was obtained prior to recruitment of subjects.

The purpose of the survey was to collect data and analyze the results to compare the students' perceptions of IoT application security before and after being introduced to the security proactive controls. Surveys and questionnaires are widely used in research to target a specific population with designed questions to measure and collect data pertaining to a specific topic (Alvarado, León, & Colón, 2016). This technique provides precise calculations of the variables that are being used in the study.

Questionnaire Development

The questionnaire was divided into three main categories. The first category was the student's opinion on the importance of IoT security risks when developing software applications. The second category was the student's opinion on the importance of embedded software security and its impact on IoT applications' embedded software. The third category was the student's understanding of the timeframe of addressing and implementing security features in the life cycle of a software development project.

Questionnaire Testing

A pretest was conducted on a group of participants to complete the questionnaire by themselves, without intervention or support from the researcher. The pretest was given to two different groups, participants from Miami Dade College (MDC) and Pittsburgh Technical College (PTC). The reason for doing this was to help validate the questions on the questionnaire. This test was conducted through a survey questionnaire created on www.surveymonkey.com. A link to the questionnaire was sent to the participants through email with an introduction text explaining the terms and the estimated time of completion. The researchers used SurveyMonkey due to its reputation of stability and for the simple appearance of the interface that it provides. SurveyMonkey uses traditional web widgets such as checkboxes and radio buttons. This interface helped reduce the amount of instructions on how to reply to the questions. Surveymonkey was chosen by the researchers due to the built-in functions to analyze the results of the data collection. These tools have been tested and validated by previous studies. The tools that were provided by Surveymonkey were at no cost to the participants or researcher.

Questionnaire Deployment

The approach to invite participants to the survey was done online through the college's email service. The invitation had an important role as an initial contact with the participants because it explained the purpose of the research, the researchers, the colleges that were involved, and the average time that would be spent to complete the questionnaire. SurveyMonkey.com provided the header of both the pre-knowledge and post-knowledge survey questionnaire for the participants. This helped show the participants that the research was focused on a specific part of the student population at the colleges.

RESULTS

At PTC, the first questionnaire was taken by 36 students enrolled in the Associate of Science (A.S.) degree in Computer Programming in the School of Information Systems and Technology. The students who participated in this questionnaire were in their second quarter term (first six months of enrollment). The first questionnaire was emailed in March 2020, and the second questionnaire was emailed later in the same month. The data was collected until April 1, 2020. The second questionnaire was taken by 17 of the 36 students who previously took the first questionnaire. These 36 students were educated on the importance of embedded software security and its impact on IoT applications.

At MDC, the first questionnaire was taken by 19 students enrolled in the Associate of Science (A.S.) degree in Game Development and Design at Miami Animation and Gaming International Complex. The students who participated in this questionnaire were in their second or third semester. The first questionnaire was emailed in March 2020, and the second questionnaire was emailed later in the same month. The data was collected until April 1, 2020. The second questionnaire was taken by 17 of the 19 students who previously took the first questionnaire. These 19 students were educated on the importance of embedded software security and its impact on IoT applications.

Findings

The following statements in the questionnaire on the pre-knowledge and post-knowledge related to the importance of embedded software security and its impact on IoT applications were given to the participants of this research study:

RQ1: I consider the possible security risks when developing IoT applications.
RQ2: I feel that secure programming is a requirement for software developers to implement.
RQ3: I take a different approach of developing code when it will be used for an IoT application.
RQ4: I believe that exposure of private information is the highest-ranking vulnerability of an IoT application.
RQ5: I believe that insufficient logging and monitoring is the highest-ranking vulnerability of IoT.
RQ6: I think IoT security attackers have many different paths through IoT to cause harm to an organization.
RQ7: I believe that common security IoT and software vulnerabilities have changed over the last 5 years.
RQ8: I believe that IoT security can be implemented at all levels of development.
RQ9: I believe that the requirements of the application should be completed before security concerns are addressed.
RQ10: I believe that security requirements should be implemented through the development of an IoT application.

Below are four tables that display the results from two different colleges of students' pre-knowledge and post-knowledge regarding the importance of embedded software security and its impact on IoT applications security. Table one represents PTC students' pre-knowledge and table two represents PTC students' post-knowledge. Table three represents MDC students' pre-knowledge and table four represents MDC students' post-knowledge. The four tables are presented to compare the results between the two different colleges. It is important to notice the difference in participant size between the two colleges.

Table 1. PTC Students' Pre-Knowledge of IoT Software Application Security

RQ	SA	A	D	SD
RQ1	8	24	4	0
RQ2	22	14	0	0
RQ3	3	23	9	0
RQ4	18	15	3	0
RQ5	5	20	11	0
RQ6	18	16	2	0
RQ7	16	19	1	0
RQ8	10	21	5	0
RQ9	9	12	15	0
RQ10	11	22	3	0

Table 2. PTC Students' Post-Knowledge of IoT Software Application Security

RQ	SA	A	D	SD
RQ1	7	9	1	0
RQ2	10	7	0	0
RQ3	2	14	1	0
RQ4	9	7	1	0
RQ5	5	8	4	0
RQ6	8	9	0	0
RQ7	6	10	1	0
RQ8	8	8	1	0
RQ9	3	10	4	0
RQ10	10	6	1	0

Table 3. MDC Students' Pre-Knowledge of IoT Software Application Security

RQ	SA	A	D	SD
RQ1	10	7	2	0
RQ2	13	6	0	0
RQ3	7	10	2	0
RQ4	14	5	0	0
RQ5	9	9	0	1
RQ6	12	7	0	0
RQ7	11	7	1	0
RQ8	10	9	0	0
RQ9	6	8	4	1
RQ10	12	6	1	0

Table 4. MDC Students' Post-Knowledge of IoT Software Application Security

RQ	SA	A	D	SD
RQ1	14	3	0	0
RQ2	13	4	0	0
RQ3	9	5	2	0
RQ4	14	3	0	0
RQ5	10	6	0	1
RQ6	11	6	0	0
RQ7	11	4	2	0
RQ8	13	4	0	0
RQ9	10	2	3	2
RQ10	12	5	0	0

The results of the pre-test and post-test results show moderate improvement. On the pre-test, 90% of the respondents selected SA or A for RQ2, 4, 6, 7, 8, and 10. RQ2 had 100% of respondents selecting SA or A. On the pre-test, 89% of the respondents selected SA or A for RQ1. The results showed that in 7 of the 10 research questions, the participants had already agreed with the security concepts being tested. This may indicate that a previous exposure to security concepts in the programming curriculum exists. With pre-test scores this high, increases in post-test results will be moderate.

The post-test showed a moderate increase in respondents selecting SA or A for all questions except for RQs 2 and 7. RQs 2 and 7 increased from 3 to 10%. RQ7 decreased 5% from the pre-test to post-test results. RQ2 retained its 100% of respondents between both the pre-test and post-test. The results for RQ2 were extremely stable between the pre-test and post-test, with only a 4% increase in the number of respondents selecting SA between the pre-test and post-test.

RQ9 displayed the most room for growth. In the pre-test, only 64% of the combined participants selected SA or A. In the post-test, 74% of participants selected SA or A. This 10% rise ties for the highest increase for all the RQs. When the data was examined by school, PTC demonstrated an 18% increase in participants selecting SA or A. MDC participants selected SA or A, showing a decline of 3%, which indicated a significant difference in results.

RQ3 also had very different results between colleges. The results showed a 10% increase in participants selecting SA or A between the pre-test and post-test. When the data was compared between each college, PTC showed a 22% increase in respondents selecting SA or A, while MDC demonstrated a 7% decline in respondents.

DISCUSSION

Three of the questions that increased from pre-test to post-test had disparate results. These questions were RQ9, 3, and 5; all demonstrated an overall increase from the pre-test to the post-test. The results were very different by school. For these three questions, PTC participants increased the number of SA or A choices, while MDC respondents decreased the number of SA or A choices. This may have indicated a difference in presentation or an implicit bias from the instructor.

In addition, this study concluded that teaching college students the importance of IoT application security is best implemented when students are educated about the possible threats that IoT applications can encounter throughout the development lifecycle. Introducing students to how IoT applications have been hacked and showing them statistics of organizations that have been impacted by data breaches indicated how this is a continuous problem in society. Students were educated about IoT applications that handle data such as credit card information, personal information, medical records, and bank information. The findings of this study indicated that the participants' pre-knowledge and post-knowledge of IoT application security changed after they were educated on the vulnerabilities and threats. Students' post-knowledge of IoT application security suggested that they were becoming aware of the importance of understanding the fundamentals of security in the software development lifecycle while developing an IoT application.

Limitations

The implementation of this study was not without certain limitations. The study was limited by the fact that it only focused on the measurement of students' pre-knowledge and post-knowledge of software application security through one delivery method. The study was limited in not being able to control a variety of major variables, such as learner characteristics, instructional method, teacher involvement, and student interactions. The results of this study were limited to a specific group of participants in two different colleges. These results should not be considered generalizable across different universities and countries.

Another limitation of this study was the size of the data sample. Further investigation is needed to establish if the same results can be duplicated through a larger data sample and applied across a broader context of universities. The participants being all first year and second year students in a computer-programming-related associate degree program may not have been a good representative sample of a broader university student population. Similarly, the instructor involved in the delivery method of the software application security vulnerabilities had a high degree of experience in

cybersecurity that may have influenced these results. Another limitation was the fact that limited insight into the participants' pre-knowledge and post-knowledge on software application security vulnerabilities was obtained.

CONCLUSION

In conclusion, the data indicated that the participants from the two schools felt that security within IoT was important when learning how to program. The participants from PTC showed a 22% increase in respondents selecting Strongly Agree or Agree, while the participants from MDC demonstrated a 7% decline in respondents selecting Strongly Agree or Agree regarding how they believed that the requirements of the application should be completed before security concerns are addressed. The data showed that the participants believed that secure programming is a requirement for software developers to implement.

A future study could be on the cultural and curriculum differences that play an impact on each school. The collected data indicated that students believed exposure of private information was important to IoT security due to the harm it could cause to an organization. The data showed that students believed that IoT vulnerabilities have changed over the last 5 years and that IoT security could be implemented at all levels of development regarding which security requirements should be applied throughout the development of an IoT application.

Previous literature review has shown that with the growth of technology and the adoption of IoT, students need to learn more about security impacts, design, architectures, and threats within the computer programming and information technology curriculum. Colleges and universities are being challenged to ensure that their students and curriculum are up to date with the latest threats within software. As IoT advances within personal, corporate, and manufacturing environments, increased risks will rise in its software and technology, requiring more security to prevent threats, bugs, and defects. Governments are continuously working on laws to fix and prevent the threats to IoT security. Individual software developers will need to be mindful of security while creating the code for IoT applications.

REFERENCES

Alvarado, F. C., León, M. P., & Colon, A. M. O. (2016). Design and validation of a questionnaire to measure research skills: Experience with engineering students. *Journal of Technology and Science Education*, *6*(3), 219-233.

Amer, M., & Alqhtani, A. (2019). IoT applications in Smart Hotels. *International Journal of Internet of Things and Web Services*, *6*.

Ammar, M., Russello, G., & Crispo, B. (2018). Internet of Things: A survey on the security of IoT frameworks. *Journal of Information Security and Applications*, *38*, 8-27.

Ashton, K. (1999). An introduction to the Internet of Things (IoT). *RFID Journal*.

Azza, A. A., Hanaa, F. M., & Elmageed, M. A. (2019). IOT perception layer security and privacy. *International Journal of Computer Applications*, *975*, 8887.

Badran, H. (2019). IoT security and consumer trust. In *Proceedings of the 20th Annual International Conference on Digital Government Research* (pp. 133-140).

Bello, O., Zeadally, S., & Badra, M. (2017). Network layer inter-operation of device-to-device communication technologies in Internet of Things (IoT). *Ad Hoc Networks*, *57*, 52-62.

Bertino, E. (2016). Data security and privacy in the IoT. In *EDBT* (Vol. 2016, pp. 1-3).

Celik, Z. B., Fernandes, E., Pauley, E., Tan, G., & McDaniel, P. (2019). Program analysis of commodity IoT applications for security and privacy: Challenges and opportunities. *ACM Computing Surveys (CSUR)*, *52*(4), 1-30.

Frazelle, J. (2019). Open source firmware. *Communications of the ACM*, *62*(10), 34-38.

Guo, H., & Heidemann, J. (2018). IP-based IoT device detection. In *Proceedings of the 2018 Workshop on IoT Security and Privacy* (pp. 36-42).

Hewitt, C. (2016). Security without IoT mandatory backdoors. *Using Distributed Encrypted Public Recording to Catch & Prosecute Suspects.*

Khari, M., Garg, A. K., Gandomi, A. H., Gupta, R., Patan, R., & Balusamy, B. (2019). Securing data in Internet of Things (IoT) using cryptography and steganography techniques. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *50*(1), 73-80.

Khattak, H. A., Shah, M. A., Khan, S., Ali, I., & Imran, M. (2019). Perception layer security in Internet of Things. *Future Generation Computer Systems*, *100*, 144-164.

Mahmoud, R., Yousuf, T., Aloul, F., & Zualkernan, I. (2015). Internet of things (IoT) security: Current status, challenges and prospective measures. In *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)* (pp. 336-341). IEEE.

Ning, H., & Liu, H. (2012). Cyber-physical-social based security architecture for future internet of things. *Advances in Internet of Things*, *2*(01), 1.

Perumal, K., & Manohar, M. (2017). A survey on Internet of Things: Case studies, applications, and future directions. In *Internet of Things: Novel Advances and Envisioned Applications* (pp. 281-297). Springer, Cham.

Razzaq, M. A., Gill, S. H., Qureshi, M. A., & Ullah, S. (2017). Security issues in the Internet of Things (IoT): A comprehensive study. *International Journal of Advanced Computer Science and Applications (IJACSA)*, *8*(6), 383-388.

Saleh, M. E., Aly, A. A., & Omara, F. A. (2016). Data security using cryptography and steganography techniques. *IJACSA) International Journal of Advanced Computer Science and Applications*, *7*(6), 390-397.

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)* (pp. 477-480). IEEE.

Tariq, N., Asim, M., Al-Obeidat, F., Zubair Farooqi, M., Baker, T., Hammoudeh, M., & Ghafir, I. (2019). The security of big data in fog-enabled IoT applications including blockchain: A survey. *Sensors*, *19*(8), 1788.

Yu, T., Sekar, V., Seshan, S., Agarwal, Y., & Xu, C. (2015). Handling a trillion (unfixable) flaws on a billion devices: Rethinking network security for the internet-of-things. In *Proceedings of the 14th ACM Workshop on Hot Topics in Networks* (pp. 1-7).

Zeng, X., Garg, S. K., Strazdins, P., Jayaraman, P. P., Georgakopoulos, D., & Ranjan, R. (2017). IOTSim: A simulator for analysing IoT applications. *Journal of Systems Architecture*, *72*, 93-107.