On the Feasibility of DoS Attack on Smart Door Lock IoT Network

Belal Asad and Neetesh Saxena

Department of Computing and Informatics, Bournemouth University, UK
belal_ea@hotmail.com
School of Computer Science and Informatics, Cardiff University, UK
nsaxena@ieee.org

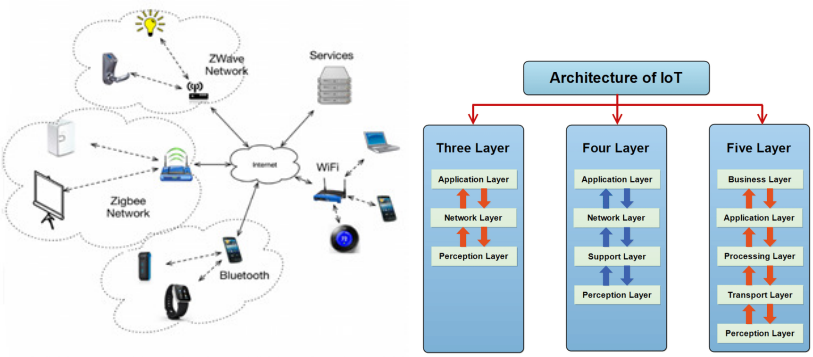
Abstract. The Internet of Things (IoT) is one of the most extensive technological evolution of the computing network. This technology can transform the physical world into a virtual world for testing and emulation to evaluate the key issues present in the physical devices. This work aims to explore the security in IoT devices and demonstrates the security gaps in the behavior of the smart door lock. In this paper, we conducted two surveys to gather consumers' requirements about the IoT devices as to whether they do understand the security risks involves with these devices. Further, we carried out a denial of service attack on a smart lock device to demonstrate that such devices are not secure. This work also highlights the security weakness and suggest guidelines to improve the overall system using cloud and edge computing and authentication and access control-based solutions.

I Introduction

The Internet of Things (IoT) is a new revolution of the networking technologies that uses the advantages of the wireless sensors network. The IoT platform has several types of applications that diversified in all areas of every-day life and several types of communication technologies are required to allow the connection between the IoT devices. The communication technologies could be divided into four different fields: the technology used to connect the IoT devices to the network, technology used for data collection and changes detection, technology to make these devices take action, and technology used to make the small devices have the ability to interact and connect. The massive connectivity in one platform makes this platform risky in security aspects. IoT platform needs to be flexible, extendable, and acceptable to mobility that allows the network and different devices the ability to communicate. All previous requirements make the security of the IoT network more challenging. Nowadays, IoT devices are involved in our daily life and deal with sensitive data through smart homes, smart gates, cars, etc. Such data needs to be protected.

The IoT technologies' deployments have been increased in the last few years, so the associated challenges and issues have also increased. The connection between people and objects can be made through any path, network, and service, as shown in Fig. 1(a). Using different types of technologies on a single platform creates several threats. There are many ways to attack this vulnerable system, such as accessing personal information, disabling the connection, and destroy the process of the device by loading massive fake data. One of the applications of the smart city is a smart

home and its smart appliances and devices, such as an intelligent gate or door. The business layer is not a part of the original IoT architecture, but it is considered under a five-layer architecture, as shown in Figure 1(b).



(a) IoT network [5]. (b) Three forms of IoT architecture [10].

Fig. 1. Internet of things network and three forms of architecture.

This work aims to identify the security issues challenges, as well as analyzing the most recent used security techniques. Secondly, it is to understand how the IoT devices' security work and behave through the network, and thirdly, it is to know how to develop a secure smart door and how the current technologies can be a benefit.

We summarize our contribution to this work as follows. (1) Investigated the currently used technologies and systems, also captured the reviews and opinions, (2) design and build a small emulation smart door system for Denial of Service (DoS) attack evaluation, (3) design the test cases on the emulation system, and (4) evaluate and analyze the results of the attacked system and suggest improvements.

The rest of the section of this paper is organized as follows. Section 2 starts with related work. This section helps to understand the current security issues in IoT platforms, as it presents the IoT architecture following it by the current security features and requirements. Furthermore, this section ends up with smart cities security, which illustrates the security risks and challenges for smart cities. Section 3 presents the results and evaluation of the work. Section 4 offers analysis and discussion around the findings and observations. Finally, Section 5 summarizes the conclusion.

2 Related Work

This section explores the identification of IoT technologies and illustrates the persistent inadequacies of currently available systems. The scope of the work starts with the modern IoT architecture, followed by the security issues and their requirement in each level of the architecture. Also, it shows the critical security

challenges in the IoT system. Finally, it ends up with the authentication and authorization in the IoT followed that with the current security risks in smart cities.

2.1 Network Security in IoT and IoT Architecture

In recent days, the industrial companies propose several applications related to the IoT based on cyber-physical systems (CPS) and machine to machine communications (M2M). These fields also deal with their sensitive data [4]. The IoT platform faces more security issues challenges than the traditional Internet-based systems due to the reason that the IoT platform works and extends the Internet through sensor networks, traditional Internet, and mobile networks to provide flexibility and scalability [3]. Therefore, new algorithms and technologies need to be developed to achieve higher satisfaction for security requirements. The information security of the system in the traditional Internet must be compatible with several critical properties such as undeniability, confidentiality, integrality, and identification. The IoT platform is based on the conventional Internet, but it will be applied to critical and sensitive areas of the national economy, for example, smart transportation, and health care systems. Thus, the security of information and network in the IoT platform require higher availability and dependability [2]. In general, the IoT architecture consists of three different main layers and these layers simplify into four layers [7], as shown in Figure 2. This addresses the IoT levels (perception, network, and application) and most modern architecture with four layers (perception, network, support or processing, and application); each of these layers has its security and management issues.

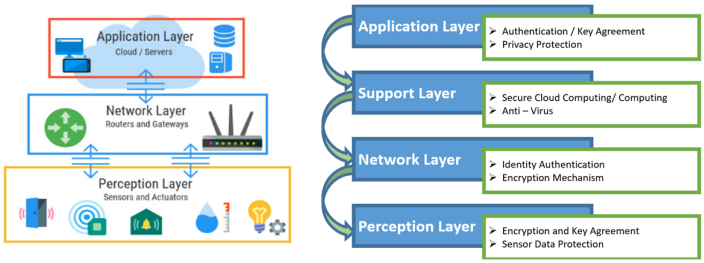


Fig. 2. Internet of things architecture [10].

2.2 Security Features

Network security issues can create troubles in building a secure preserved IoT system. This section explores the security problems in each layer of the IoT architecture as follows:

Perception layer. This layer consists of simple nodes (sensors) with short of power and storage capacity; consequently, applying the traditional security algorithm is impossible [3]. The most security issues in this layer are related to sensors, whereas

this layer consists of sensors such as the global positioning system (GPS), wireless sensor networks (WSNs), and radio-frequency identification (RFID), etc., therefore, this layer is the main target of attackers [13]. Further, the key security issues in this layer are as follows:

i) False sensor data: The IoT systems depend on the sensors to collect information from the physical world to enhance the experiences of the IoT applications [9]. The attackers can control the demands of the IoT devices by altering the sensor data. The false sensor data or fake data can be injected through communication mediums, physical access, or the sensors of the IoT devices. The attackers can take advantage of the power analysis on IoT devices, as the power analysis using an encryption algorithm can detect details about the encryption process in the IoT system such as key size, block size, also the existent encryption key. The attacker can use the captured information to encrypt fake data and substitute the authentic data on the device [9]. Consequently, the false encrypted data can be injected in the communication medium to change the actual action of the system. The security issues of RFID technology are also related to false sensor data. RFID is contactless technology depends on identifying the target tag signal, the identifying process does not need manual involvement [3]. RFID is widely used in harsh environments that reveal many problems such as (1) *Conflict collision*: passing the information to the reader from multiple RFID tags simultaneously causing the reader to get incorrect data. (2) *Uniform coding*: Currently, there is no internationally uniform encoding standard for RFID tag [3]. This problem may cause other issues such as errors that occur during the reading process and authorize the reader to obtain the correct access information to the tag [3].

ii) Malicious Sensor Commands: Several sensors embedding in the IoT devices open away to transmit malicious commands to activate malware that might be implemented in the victim's device. The IoT sensors can be used to create communication channels between devices peripherals [10]. These channels aim to transmit malicious commands or to change the sensor parameters such as light intensity [9]. Since the light sensor can differentiate the intensity of the light source, it is easier for the attacker to transmit a bitstream via light source by turning it on and off, as the IoT devices decode the light intensity change as a bitstream [10].

iii) Eavesdropping: Eavesdropping refers to a type of unauthorized real-time attack where the attacker tries to steal the information that is transmitted over a network through private communications such as video conferences, phone calls, or text messages [10]. The malicious app records the audio, video, or saves texts by exploiting the audio sensors or messages sensors. In this type of attack, the attacker can save the recorded voice or listen to the conversation in real-time [9].

Transportation layer. The transportation layer is highly sensitive to attacks, as the environment of this layer has prominent security problems, especially regarding authentication and integrity. This layer deals with issues that occur in the network layer as well. This part presents the common security issues as follows:

i) Daniel of Service (DoS) Attack: A DoS attack aims to prevent users from accessing the system by disabling the devices. The IoT devices can easily be affected by DoS attacks due to the constraints on time, energy consumption, and memory

constraints [15]. By flooding the target with redundant requests makes the use of that target difficult or impossible for all or some users.
ii) Man-in-the-Middle (MITM) Attack: MITM is an attack where the attacker secretly relays, intercepts, and alters the communication between two devices. Since the attacker has access to control the communication, therefore he can change the information between the devices according to his needs [16].
iii) Storage Attack: The exchanged information in the communication between IoT devices usually stored in a storage environment such as storage devices or cloud, both storage environments able to be attacked by attackers. This attack is critical, especially in smart city applications, as the attacker can change the user's information to incorrect details [10].

Processing layer. The processing or support layer is taking place between the transportation layer and the application layer. Sometimes, this layer itself is considered as a part of the transportation layer as it deals with exchanged information in the communications between two devices, as well as it deals with the storage environments. Consequently, the security issues at this level are related to security issues at transportation processing. The common security issues and attacks are as follows:
i) Malware: This attack base on such applications as viruses, spyware, Trojans horses, worms, and adware to collaborate with the system. It uses the executable form of scripts, contents, and codes to act against the system's requirements and steal the confidential information [19].
ii) Exhaustion: An attacker here uses attrition of the previous attack to disturb the processing of the IoT structure. In the IoT network, it could be a result of such attacks that impoverish the system resources.

Application layer. The application layer is the terminal and user-centric layer of IoT architecture which performs diverse tasks for the users. Therefore, this layer has many different issues but the security issue comes as the main problem. Minutely, when the IoT is used to construct the smart home, it originates several vulnerabilities [10]. The devices used in smart homes are small and have weak resources such as low memory and computational power [11]. Common security issues in this layer are listed below:
i) Malicious Code Attack: This attack considers as an application security threat that cannot be discovered or controlled by the antivirus software. The attackers can attach the malicious code in any part of the software to damage the system. Furthermore, the attached code could activate by itself or could require action from the user [10].
ii) Cross-Site Scripting: This attack allows the attackers to inject client-side scripting in a trusted site used by other users. A cross-site attack gives full validity to the attackers to change the contents and illegally use the original policies.

Business layer. The business layer acts as a manager for the whole system; therefore, the vulnerabilities in this layer permits the attackers to misuse the application by averting the business logic [10]. Mainly, most of the security issues at this level are weaknesses in an application that come as a result of a cracked or truant security

control. The most dangerous security problem at this level is a zero-day attack [20]. The zero-day attack is an unknown security hole or problem which is exploited by an attacker to create complicated problems before the victim can detect it. This vulnerability enables the attacker to control the application without the user's knowledge and consent [20].

In addition to these security problems, the IoT system requires different communication technologies to achieve the purpose of the IoT existence. Each technology of these communication technologies has several security features and also provides security protocols, as well as these technologies that have some drawbacks which make the security more challenging in IoT [18]. Table 1 shows the different communication technologies used in IoT and illustrates the characteristics with the drawbacks for each.

Table 1. Different Communication Technologies Used in IoT [1]

Technologies	Mechanism	Security	Applications	Characteristics	Drawbacks
ZigBee	Wireless	Encryption and Integrity	Home and Industry	Low consumption and Cheap	Fixed key
RFID	Frequency waves	Encryption (AES, DES)	Health care	Data capturing with no duplication	Lack of a uniform coding and no authorization
Bluetooth	Wireless	Encryption and Authentication	PDA, Mobiles and Laptops	Cable replacement and Low cost	Blue jacking, Bluesnarfing
Wi-Fi	Radio Signals	Authentication and Authorization	PC, Phones and Cameras	Faster, Secure and Convenient	Eavesdropping
WSN	Wireless	Key, Encryption and Authentication	Buildings and Health care	Low Cost, Power, and Resilience	DOS attack
5G Network	Wireless	Authentication and Authorization	Phone, IoT and Multimedia	Faster, Secure and Convenient	Distributed DoS

2.3 Security Challenges in the IoT

IoT security is an active research field. Various issues in different security aspects require solutions at diverse levels of security. The challenges in the security aspects of IoT could be divided into two main parts, as follows:

Security challenges: The evolution of IoT technologies and the increasing number of connected devices to the IoT network increases the potential security threats [17]. As the IoT ameliorates the companies' productivity and improves the quality of human lives, it will increase the potential opportunities for cybercriminals and hackers. The latest studies disclose that more than 70% of the conventional used IoT devices have serious vulnerabilities [17]. The IoT will stay escalate over time; consequently, even by collecting all the security mechanisms of each layer and putting them together will not introduce reliable security for the IoT network [1]. The IoT applications are supporting several sensitive infrastructures such as health care, smart grid, and banking systems, which require a high level of security.

3 Results and Evaluation

This section aims at detailing the results obtained from the online survey, the investigation of the current technology, analyzing the used technology, and the findings from the emulation system. Furthermore, this section presents the evaluation of the entire results to propose an improved solution. This section presents aims through three main sub-sections as follows: 1) capturing stakeholders' requirements and their opinion, 2) designing and building the system, and 3) evaluations.

3.1 Capturing Stakeholders Requirements and their Opinion

Stakeholders Identifications. The stakeholders are people who are looking to acquire this system and are actively involved in the work. Therefore, stakeholders are the user of this system and whose interests could be affected by the work, either positively or negatively [52]. The stakeholders' identification process could be done through several techniques such as consultation with organizations involved in the work, consultation with people planning to acquire such systems, and consultation with expert people working in the same field. To achieve this aim, the following potential objects have been suggested: the potential users for this technology, the available technologies to build such systems, and the system's behavior under an attack. Different potential objects and stakeholders identified within the work domain are potential users, expert people in technology, Arduino as an available technology to build the system and implement a DoS attack to analyze the system's behavior under attack.

The above stakeholders and objects can be categorized according to the method of gathering the information. The potential users and the expert people were considered as one category, where their information and requirement can be gathered via surveys or interviews. The third category's information and requirements can be extracted by studying the current researches, similar experiences, and analyzing the experts' reviews. Finally, the last object's requirements and information can be collected by implementing the real types of attacks and analyzing the findings. In order to identify the potential users' requirements and experts' reviews and their opinions, two online surveys were performed. The first survey was aimed at potential users. It focused on gathering the basic requirements that users expected from the smart locks and looks at their concerns about the security aspects. The targeted group was chosen randomly from different backgrounds and various ages, and the targeted group consisted of thirty-three participants. To gain respondents, the survey took up to three minutes to complete and gave four optional questions for who's interested in technical aspects. The structure of the survey consisted of seventeen questions, thirteen compulsory questions, and four optional questions. The questions were designed to get different requirements according to the differences of the responders' backgrounds. The first block of the survey addresses the countries, and the age ranges for the participants. Figure 3 shows the different backgrounds of the participants involved.

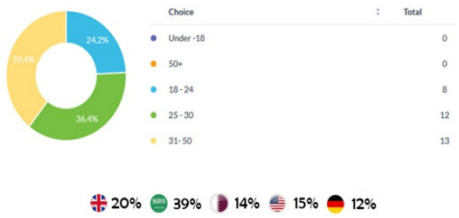


Fig. 3. Participants' backgrounds.

As can be seen from Figure 3, the participants from different countries and their ages range from 18 to 50. A large proportion of who is interested in this technology is between the age of 25 to 50. Therefore, the people who have responsibilities or families to take care of are more interested in such systems. The next block consists of two questions that aimed to find out if the participants have already dealt with such systems. Figure 4 shows people's awareness of these technologies.

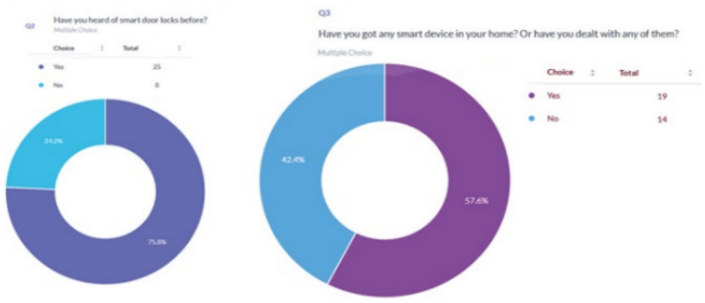


Fig. 4. Participants' awareness of smart devices.

Fig. 5. The outcome of the participants' expectations.

As can be seen in Figure 4 that 75.8% of the targeted group heard about the smart lock technology, and 57.6% of them have dealt with different IoT devices such as Apple HomePod, A/C, Smart TV, wall switches, and smart door lock. Only one participant out of 33 has dealt with the smart door lock. The next block of questions aimed to understand why the participants want to use the smart locks, what do they expect the smart lock would do for them and how much that will cost to have a smart lock. Figure 5 addresses the outcome of the participants' expectations.

Table 2. Participants' Satisfaction.

Question	**Participants responds**		
Are you confident when you use the internet?	18% have no confidence while using the internet	55% have average level of confidence while using the internet	27% have high level of confidence while using the internet
How critical are the privacy issues in IoT (Internet of Things) to you?	18% consider the privacy is a not critical issue in the IoT	52% consider the privacy is a critical issue in the IoT	30% consider the privacy is a very critical issue in the IoT
If the product were available today, how likely would you be to buy the product?	29% of participants are not likely to gain this technology.	61% of participants are moderately likely to gain this technology.	10% of participants are strongly likely to gain this technology.

Table 3. The Optional Questions.

Question	**Participants responds**	
Do you aware there is a general lack of security in the design of the leading IoT devices components.	65% of the participants aware that there is a general lack of security in the design of the leading IoT devices components	35% of the participants aware that there is a general lack of security in the design of the leading IoT devices components but they do not know about them in details.
How much do you aware of Memory Attacks?	29% of the participants aware about the memory attacks.	71% of participants not aware about this type of attacks.
Do you know most of IoT devices such as Arduino has Denial Of Service and Overflow Vulnerability?	15% of the participants know that Arduino devices has Denial of Service and Overflow vulnerabilities.	85%participants do not know about these vulnerabilities.

Table 4. The Additional Survey.

Question	**Expert 1**	**Expert 2**	**Expert 3**	**Expert 4**
Developing Arduino Experience (in years)	5	6	4	6
Academic specialisation	BSc. software engineering	BSc. Electronic engineering	MSc. computer science	BSc electrical engineering
number of completed projects	78 mini projects and 7 robotics.	103 mini projects and 2 complicated projects.	50 mini projects.	97 mini projects, 6 robotics and 1 complicated project.
Do you know about security issues in Arduino?	I know that the security in Arduino is weak.	DDoS attacks issues	None.	limited resources
How do you secure your projects?	Depends on the cloud computing security only	Connecting the device to internet through remote server.	None.	Depends on the service provider
Have any of your projects been hacked?	None.	Two of them under university experiments	I never connected my projects to the internet.	no security tests have been applied to my projects
Do you take security aspects in count while you are building your projects?	No	No	No	No
Will you be interested in using a secure system in your future projects?	Yes	Yes	partly	Yes
Do you aware of Memory Attacks?	No	Yes	No	Yes
Do you know Arduino has Denial Of Service and Overflow Vulnerability?	No	I know that it has denial of service vulnerability but not overflow.	No	Yes

From Figure 5, it can be stated that the potential users' expected full control of the 'smart' device at a low price. In contrast, only 36% of them feel comfortable when using their phone as a key. The next set of questions show the reason why only 36% would like to use their phone as a key. Table 2 reflects that 61% of the participants are moderately likely to gain a smart lock. This percentage comes as a result of their satisfaction with the privacy of the internet in general. The optional questions were intended to understand the scientific background of the participants. Answered these questions, seventeen participants had technical certificates such as electronic engineering, network engineering, computer engineering, computer science, and PhD in cybersecurity. Table 3 illustrates the optional technical questions and shows that security issues are unknown to many people. Moreover, a large number of people who have a certificate in related areas are not aware of these issues. The answers to the first survey were a strong motivation to perform an additional survey. The second survey targeted four experts in Arduino to understand how well they know and able to avoid the available security issues. Table 4 illustrates the additional survey questions and the experts' answers. It reflects several aspects of the Arduino's experts. 100% of the experts do not take into consideration the security aspect while they are doing

their works. Moreover, 90% of them put the security responsibility on the service provider or the remote server; as well as most of them were not aware of the most critical vulnerabilities in Arduino. However, all experts are interested to use a secure system for their future works.

3.2 Designing and Building the System for Evaluation

In order to specify the requirements to propose an improved system, this section identifies the smart locks' key requirements followed by available types and then investigates the security vulnerabilities in Arduino. Furthermore, this section addresses the challenges and requirements to build a system for the evaluation. This section aims to understand and match the requirements extracted from the questionnaires and previous studies.

The Smart Door Identification and Types. In a smart home, the smart door is a door fitted with an electronic and mechanical device that allows a homeowner to control the door wirelessly. The user can wirelessly verify and unlock the door by using a smart key such as a smartphone or a key fob instead of the traditional keys. The common types of smart locks include password-based (2013), social networking site-based (2015), door phone-based (2013; 2019), and combined systems (2018).

Arduino. Arduino is an open-source programmable circuit board. This programmable board can be integrated into several complicated experiments. Arduino board contains a programmable microcontroller to sense and control objects in the physical world. Arduino's flexibility makes it a popular choice for building IoT devices. Arduino UNO, one of the most popular Arduino boards. To further study the proposed security mechanisms and its efficiency on the vulnerabilities, an emulation system was built and tested in this work. The following sections illustrate such requirements followed by the results.

The System Requirements. To know the requirements of the system, the experiment's scheme needs to be detailed. The emulated system considered different technology-based mechanisms such as cloud computing and fog computing. However, Figure 6 addresses the scheme for the emulated system. The smart lock controller connecting to the edge device (Laptop) which acts as a gateway. To connect the IoT device to the Internet, the edge device connects to a remote server, which makes the mobile able to control the smart lock [21]. This system implements different security mechanisms such as cloud interface access and local authorization. Thereafter, we have used the Blynk application to run the experiments.

Faced Challenges. During the process of building the emulated system, the process faced critical challenges such as unknown errors while programming the board, errors while connecting the controller to the edge device, and difficulties while analyzing the security aspects. This section illustrates these challenges in two categories as follows:

Construction stage challenges. The first challenge appeared while uploading the code to the controller, an error message appear, and the serial port turned into disable mode. Figure 7 shows the error that occurred. This challenge was resolved by ordering a new Arduino board. The error occurred because of the damage that happened to a chip responsible for converting the USB port to a serial port. Another error was occurred to prevent the application to run the servo motor code. This challenge was resolved by replacing the library and the servo parameters.

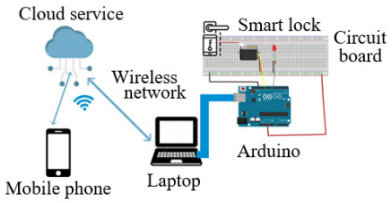


Fig. 6. Emulated system setup.

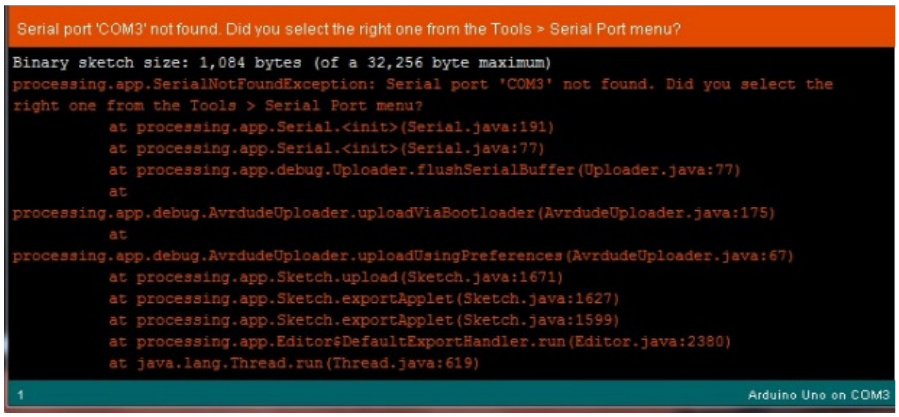


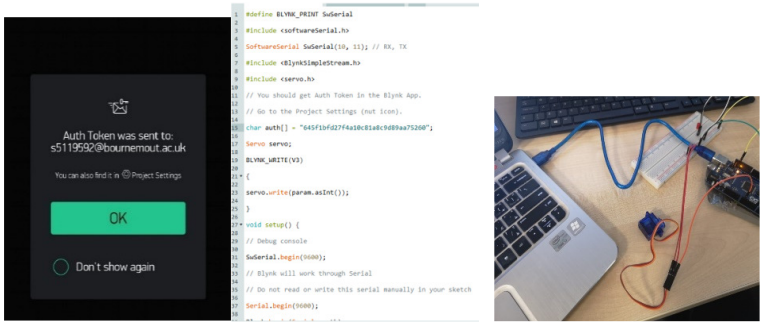
Fig. 7. Error message and disabled port.

Implementation phase challenges. The challenge faced here was a technical issue. The system was freezing when the sniffing command was calling Wireshark to capture packets. No error messages appeared at this stage. The challenge here has been resolved by updating the operating system.

3.3 Evaluation: Findings and Examination Results.

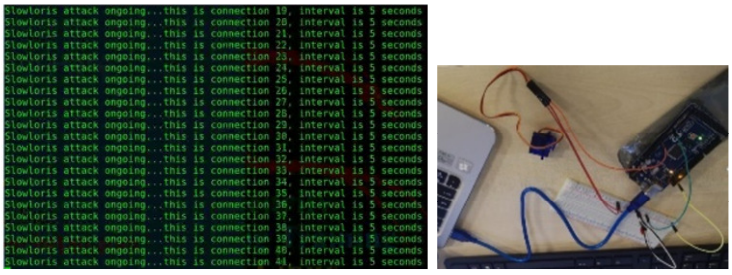
This section illustrates the findings which are shown through figures. Blynk application is used in the smartphone to communicate with the remote server. The Blynk sends a specific Auth code to each user in order to protect the controller from unauthorized devices. Figure 10 shows the application and its interface. The aim of

this experiment is not to show how to build the smart lock but to show the security issues in the smart lock. Figure 8(a) shows the code built for this task whereas Figure 8(b) shows the setup in working mode before implementing the DoS attack. The next stage of this experiment is to implement a DoS attack and analyze its outcome. The DoS attack was implemented on the system by using Pentmenu scripts in the Kali Linux environment.



(a) Blynk application interface and code. (b) Smart door emulation system.

Fig. 8. Blynk application interface and experimental setup.



(a) Running a DoS attack. (b) Disabled device after the attack.

Fig. 9. DoS attack successful attempts.

Figure 9(a) shows the attacking process for DoS attack as Slowloris. Slowloris is a type of denial of service attack that targets a single machine to take down another machine's web server with minimal bandwidth on unrelated services and ports. Figure 10 shows several packets that are sent to this device to perform a denial of service attack. Several attempts were made in a very short time. Different sources with different IP addresses were configured in the Linux environment to target a smart lock device (IP address 192.168.1.25) over the transmission control protocol (TCP). Each packet sent was 54 bytes in length. The application was running on

source ports ranging from 9506 to 9522, whereas the destination port was fixed as 80. After flooding the network with these packets, the IoT device stop working correctly. As shown in Figure 9(b), due to flood of the number of packets targeted to a single device in a very short time could result in disabling the device, and hence, denial of the service is performed (device does not respond). Thereafter, all the packets were also monitored using Wireshark to detect this DoS attack traffics. In this section, we demonstrated how to perform an attack over a smart lock. It also reflects that such smart devices can be hacked because they do not contain sufficient security to make the device secure against potential threats. As per these results and findings, the next section analyses all requirements to propose the improved system.

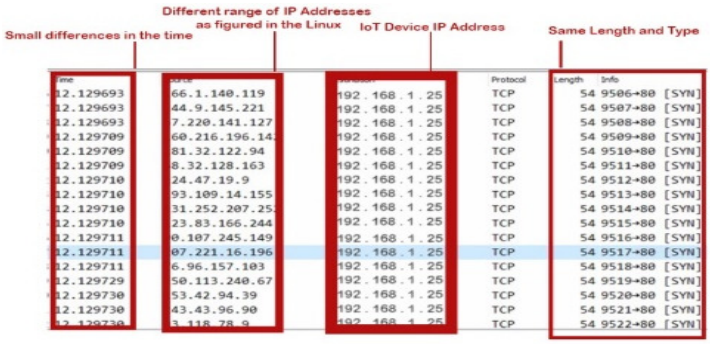


Fig. 10. DoS attack successful attack detection.

4 Analysis and Proposal for Improved System

This section aims to analyze the survey responses, the investigation of the build systems, and the experiment's results. The analyzation process aims to study the established investigation of available smart locks and the emulated experiment. Consequently, the analyzation process could be detailed as follows:

Stakeholders' and experts' opinions. According to the surveys, the targeted stakeholders are two different categories as follows:
Random public: This diversity provides a general idea of the requirements and available security concerns that people have. Most of the respondents were aged between 25 to 50 that makes the answers more accurate. More than 57% of the participants dealt with IoT devices as well as more than 70% of them want a smart lock which has full control of the door. On the other hand, 61% of them not very likely to get such a smart lock system. The reasons behind lie behind two reasons: 1) 65% of them are not very confident using it and 2) lack of security in the IoT devices.
Experts: The answers to this survey show the massive gap between IoT developers and IoT security. Some of them aware of the lack of security in IoT but never considered security aspects.

The investigation of available smart locks. The investigation of the available smart locks covers most aspects of the stakeholders' requirements. Most of them are offering semi-full control of the door. On the other hand, the security aspects still weak and need some enhancements. Moreover, the most commonly used technology in smart lock shows several security vulnerabilities which make the IoT security a critical issue in the smart home. We have demonstrated one attack on such a smart lock.

Proposal for an improved system. We proposed an improved system that combines three different mechanisms to avoid different security issues. Each IoT device in this architecture connects to the cloud through three different stages. Firstly, the IoT device connects to the edge device to enhance computation speed and protect the private information in a personal device [8]. Secondly, the edge device connects to the Internet through a local substation for authentication and authorization purposes [20]. Finally, the substation connects to the cloud through the central station. The proposed architecture keeps each specific group of IoT have their authentication and authorization station. All the devices from all different substations can communicate through the central station according to their roles [14]. Hence, this can avoid such attacks by placing authentication and access control based security controls. Furthermore, the smart lock in this architecture can provide different types of controls based on the users' needs. The smart lock in this architecture is based on the combined system of smart locks [6]. The built system used fog computing as a gateway to the Internet that offers the system more secure. Furthermore, the cloud system provides the owner with an authentication key which saved in his edge device [21]. The use of fog computing and the authentication key secure the controller from unauthorized users. However, the results of the experiment show the weakness of the authorization system used in the remote server and the edge device. The attacker did slowdown the smart lock performance without been blocked from the server. The experiment shows critical problems related to authentication and denial of service that can be avoided in the enhanced system.

5 Conclusion

IoT technologies are proliferating, and all modern countries around the world compete to convert into smart cities [12]. The work carried out highlighted the tendency for a further rise in IoT technologies, especially in smart homes and personal life. However, as the technologies spread quickly, the security issues increase as well. Therefore, this work aimed at analyzing and studying the security issues in a specific IoT device. Particularly, this work studied the security in the smart lock by following variable methods to gather the stakeholders' requirements and investigate the current smart lock by developing a setup. We demonstrated the insecurity (authentication issue and DoS attack possibility) present in a smart lock. The proposed architecture combines different security mechanisms to prevent the IoT device from several types of attacks. This work needs further studies to implement

and analyze other attacks on a real IoT device. The emulated system needs to do further tests and mount attacks to explore threats and enhance using fog computing.

References

1. Bhuvaneswari, V., Porkodi, R.: The internet of things (IoT) applications and communication enabling technology standards: an overview. In: International Conference on Intelligent Computing Applications, 324-329 (2014).
2. Weber, R.: Internet of Things – new security and privacy challenges. Computer Law & Security Review, 26(1), 23-30 (2010).
3. Suo, H., Wan, J., Zou, C., Liu, J.: Security in the internet of things: a review. In: Intern'l Conference on Computer Science & Electronics Engineering, 648-651 (2012).
4. Wan, J., Yan, H., Suo, H., Li, F.: Advances in cyber-physical systems research. KSII Transactions on Internet and Information Systems, 5(11), 1891-1908 (2011).
5. Desai, P., Sheth, A., Anantharam, P.: Semantic gateway as a service architecture for IoT interoperability. In: IEEE International Conference on Mobile Services. 313–319 (2015).
6. Divya, M., Rao, M.: Centralized authentication smart locking system using RFID, fingerprint, password and GSM. Intern'l J. of Engg. & Technology, 7(3.12), 516 (2018).
7. Jing, Q., Vasilakos, A., Wan, J., Lu, J., Qiu, D.: Security of the internet of things: perspectives and challenges. Wireless Networks, 20(8), 2481–2501 (2014).
8. Shi, W., Cao, J., Zhang, Q., Li, Y., Xu, L.: Edge computing: vision and challenges. IEEE Internet of Things Journal, 3(5), 637-646 (2016).
9. Kumar, A., Petracca, G., Aksu, H., Jaeger, T., Uluagac, S.: A survey on sensor-based threats to internet-of-things (IoT) Devices and Applications. arXiv, 14(1), 2-14 (2018).
10. Burhan, M., Rehman, R., Khan, B., Kim, B.: IoT elements, layered architectures and security issues: a comprehensive survey. Sensors, 18(9), 2796 (2018).
11. Khan, R., Khan, S., Zaheer, R., Khan, S.: Future internet: the internet of things architecture, possible applications and key challenges. In: 10th International Conference on Frontiers of Information Technology, Islamabad, 257–260 (2012).
12. Sethi, P., Sarangi, S.: Internet of things: architectures, protocols, and applications. Journal of Electrical and Computer Engineering, 20(9), 1-25 (2017).
13. Xiaohui, X.: Study on security problems and key technologies of the internet of things. In: International Conference on Computational and Information Sciences, 407-410 (2013).
14. Saxena, N., Choi, B., Lu, R.: Authentication and authorization scheme for various user roles and devices in smart grid. IEEE TIFS, 11(5), 907-921 (2016).
15. Prabhakar, S.: Network security in digitalization: attacks and defence. International Journal of Research in Computer Applications and Robotics, 5(5), 46-52 (2017).
16. Conti, M., Dragoni, N., Lesyk, V.: A Survey of Man In The Middle Attacks. IEEE communications surveys & tutorials, 18(3), 2027-2051 (2016).
17. Lee, I., Lee, K.: The internet of things (IoT): applications, investments, and challenges for enterprises. Business Horizons, 58(4), 431-440 (2015).
18. Al-Sarawi, S., Anbar, M., Alieyan, K., Alzubaidi, M.: Internet of Things (IoT) communication protocols: review. In: 8th International Conference on Information Technology (ICIT), pp.685-690 (2017).
19. Canzanese, R., Kam, M., Mancoridis, S.: Toward an automatic, online behavioral malware classification system. In: IEEE International Conference on Self-Adaptive and Self-Organizing Systems, 111-120 (2013).
20. Sharma, V., et al.: A consensus framework for reliability and mitigation of zero-day attacks in IoT. Security and Communication Networks, 17(1), 1-24 (2017).
21. Cai, Y., Genovese, A., Piuri, V., Scotti, F., Siegel, M.: IoT-based architectures for sensing and local data processing in ambient intelligence: research and industrial trends. In: IEEE Int. Instrumentation and Measurement Technology Conf., pp. 1-6 (2019).