IJIREEICE

ISSN (Online) 2321-2004
ISSN (Print) 2321-5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

Vol. 7, Issue 10, October 2019

Study on Comparative Security Analysis of IoT Frame Work

Abdul Ohab[1], Md.Tahasin Abid[1], Utpal Chandra Das[2], Md. Zahirul Islam[3], Amir Sohel[4]

B.Sc. in ETE, Department of Electronics and Telecommunication Engineering,

Daffodil International University, Dhaka, Bangladesh[1]

Research Assistant, Department of Electronics and Telecommunication Engineering,

Daffodil International University, Dhaka, Bangladesh[2]

Assistant Professor, Department of Electronics and Telecommunication Engineering,

Daffodil International University, Dhaka, Bangladesh[3]

B.Sc. in CSE (Computer Science and Engineering), Daffodil International University, Dhaka, Bangladesh[4]

Abstract: The Internet of Things (IoT) gadgets have turned out to be well known in various spaces, for example, electronics Health (e-Health), e-Home, online business, and e-Trafficking, and so forth. With expanded arrangement of IoT gadgets in reality, they can be, and now and again, as of now are liable to malicious attacks to trade off the security and protection of the IoT devices. While various analysts have investigated such security difficulties and open issues in IoT, there is a deplorable absence of an orderly investigation of the security challenges in the IoT scene. In this report, we go for connecting this gap by directing a careful investigation of IoT security difficulties and issues. A definite investigation of IoT attack surfaces, frameworks, security issues and has been presented. A brief summary of comparison among the IoT frameworks those can provide countermeasures against various security attacks in IoT also been addressed

Keywords: IoT, Attack, Security, Frame Work, Investigation

I. INTRODUCTION

The Internet of Things (IoT) plays out a staggering capacity in all parts of our regular day to day existences. It covers numerous fields which incorporate social insurance, autos, stimulations, business home gear, sports, homes, and so forth. The inescapability of IoT facilitates a couple of typical exercises, advances the manner in which individuals have cooperation with the earth and environment, and enlarges our social communications with other individuals and items. This all-encompassing vision, be that as it may, raises additionally a couple of concerns, similar to which level of wellbeing the IoT ought to give? Also, how it gives and ensures the confidentiality of its clients?

Developing applications for the IoT can be an extreme mission because of a few thought processes; (I) The high multifaceted nature of apportioned figuring, (ii) The shortage of general indications or structures that handle low stage correspondence and improve unreasonable dimension usage, (iii) Multiple programming dialects, and (iv) Diverse correspondence conventions. It incorporates engineers to control the framework and manage both programming and equipment layers together with keeping up all functional and non-valuable programming program prerequisites. This intricacy has achieved a short development as far as presenting IoT programming structures that deal with the previously mentioned difficulties.

Exceptionally nowadays, various IoT systems had been discharged by method for the main investors in the IoT space and by utilizing the examinations network with a reason to help and make it smooth to extend, convey and hold IoT bundles. Every member built his technique depending on his vision closer to the IoT worldwide [1]. On this, we look at the homes of a subset of IoT structures, focusing on explicitly their assurance includes and limiting limit of numerous danger. The picked set of IoT plat-forms1 comprises of AWS IoT from Amazon, ARM bed from ARM and distinctive accomplices, Azure IoT Suite from Microsoft, Brillo/Weave from Google, Calvin from Ericsson, Home Kit from Apple, Kura from Eclipse, and Smart Things from Samsung.

IJIREEICE

ISSN (Online) 2321-2004
ISSN (Print) 2321-5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

Vol. 7, Issue 10, October 2019

II. IOT ATTACK AND RESPONSE

2.1 AWS framework

Dos attack: AWS offers flexible infrastructure and offerings that assist customers to enforce strong DDoS mitigations and create enormously to be had application architectures that comply with AWS first-rate Practices for DDoS Resiliency. These include offerings inclusive of Amazon route fifty-three, Amazon Cloud Front, Elastic Load Balancing, and AWS WAF to manipulate and take in traffic, and deflect undesirable requests. These services combine with AWS shield, a managed DDoS safety service that offers continually-on detection and automatic inline mitigations to protect internet applications strolling on AWS. This document describes not unusual DDoS attack types and offers AWS customers with satisfactory practices and strategies for defensive programs from a DDoS attack [1].

Blueborne attack: The vulnerability placed over approximate 5 billion devices at capability threat, with many yet opens to these flaws. These days, Armis Labs has opened that a predicted 20 million Amazon Echo are at risk of attacks through the BlueBorne exploit. Researchers delivered that attackers can take whole control of the device within the case of the Amazon Echo.
No longer all BlueBorne vulnerabilities (there have been over eight) have an effect on the device.
Amazon Echo is at risk of CVE-2017-1000251 (RCE flaw in Linux Kernel) and CVE-2017-1000250 (data leak inside the SDP Server). Researchers introduced that attackers can take entire control of the tool within the case of the Amazon Echo.

Jamming: Wireless networks provide a wide range of services which is never so easy by any other medium, its mode of working tends it to have many security breaches. In the modern era of communication, trillions of profitable vital information is available on the internet and they are accessible through this open medium. Such vital information can be achieved through intentional interference or jamming. There have a shield technique to prevent jamming and different avoidance techniques. [2]

Remote access using telnet: with a view to supplying an oversaw administration encounter, Amazon RDS does now not give shell get right of the section to in DB examples, and it limits get passage to specific framework systems and tables that require propelled benefits. Amazon RDS encourages access to the database on a DB case the use of any favored sq. server control studio. Amazon RDS does not allow guide have got admission to in a DB occurrence through telnet, secure shell (SSH), or windows remote registering device association.[3]

Exploit kit: For an attacker, breaching a system is about exploiting its weaker spots. Cloud environments shift these weaknesses dramatically. Some traditional attack vectors become very difficult to exploit and thus less important, while many new vectors open up. This presents new challenges for security teams, as they have to model their security very differently from traditional data centers. EC2 instances, RDS, Amazon Redshift, etc.: customers can control on which VPC or subnet to launch these resources, thus controlling

Access to the resources. Aws VPC defines an excellent perimeter that provides security groups for firewalling. [4]

Man –in-the-middle attack: Man in the middle (MITM) attacks. All the AWS APIs are to be had through SSL protected endpoints which provide server authentication. Amazon EC2 AMIs automatically generate new SSH host certificate on first boot and log them to the instance's console. You may then use the secure APIs to call the console and access the host certificate earlier than logging into the instance for the primary time. [5]

We chose the above systems dependent on the resulting criteria: (I) The notoriety of the transporters inside the product program and gadgets ventures, (ii) The assistance of expedient utility enhancement and the quantity of uses on the store, (iii) The inclusion and usage of the structure, and it' s notoriety in the IoT commercial center.

Ransomware: Unsecured Amazon s3 buckets are prime cloud target for ransomware attacks. Misconfigured s3 buckets are a too-common problem among Amazon web services (aws) users and security researchers are taking notice. Noted security researcher Kevin Beaumont has warned that publicly writable s3 buckets could be used by criminals in ransom attacks. [6]

Side channel attack: Updated kernels for Amazon Linux AMI 2017.09 (alas-2018-1058), Amazon Linux AMI 2018.03 (alas-2018-1058), and Amazon Linux 2 (alas-2018-1058) are to be had within the respective repositories. As a standard security excellent exercise, we recommend that clients patch their operating systems or software program as applicable patches grow to be available to deal with emerging side-channel problems.[7]

IJIREEICE

ISSN (Online) 2321-2004
ISSN (Print) 2321-5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

Vol. 7, Issue 10, October 2019

2.2. ARM mbed

DoS attack: Little, low-vitality gadgets like sensors and surveillance cameras are the greatest unmistakable a piece of IoT, and that they're legitimate in ARM's wheelhouse on the grounds that the overwhelming weight in low-vitality chips. Anyway, the association featured a cloud-based SaaS displaying rather than chips or edge gadgets themselves. IoT depends upon on once more end aptitudes as parcels as feature gadgets, and the association wants to assume a job in it all. The SaaSstage, known as mbed Cloud, handles gadget association and setup, encryption-key provisioning, and firmware refreshes. [8].

Jamming attack: An embedded sensor hub microcontroller intended to help sensor organize applications with serious security requests is exhibited. It includes a low power 16-bit processor center upheld by various equipment quickening agents intended to perform complex activities required by cutting-edge crypto calculations. [9].

Remote access using telnet: In arm mbed, there is an access of remotely login. Data is encrypted when access. There is a password to log in. The HTTPS server makes use of the ARM mbed TLS software program component to allow secure communication. [10].

Man in the middle attack: ARM's "mbed TLS" programming system might be deceived into a validation sidestep and needs a fix. Made by methods for PolarSSL, which was gotten in February by methods for ARM, mbed is a crypto library intended to make it simple for inserted framework designers to include SSL/TLS capabilities to their items. ARM's embedded TLS can fixes man-in-the-middle attack. [11]

Replay attack: The BLE Gateway and BLE Sensor is an endeavor at alleviating the defenselessness to replay attack when utilizing reference point type ads. It's composed for nRF51822 equipment with no locally available NVRAM. [12].

Side channel attack: Side channel attack can be entered into the cloud.but can be detected. There using the mbedTLS functions of AES256-GCM. [13].

2.3. Azure IoT suite

DoS attack: Application layer assurance with purplish azure web application firewall. Protection against the unanticipated expenses of a ddos attack. [14].

Blueborne attack: To abuse the vulnerability, the aggressor should be inside the physical closeness of the focused on the client, and the client's PC needs Bluetooth empowered. The attacker would then be able to start a Bluetooth association with the objective PC without the client's information. [15]

Jamming attack: In azure IoT suite, there have a security protocol that can fix the jamming attack. [16]

Remote access using telnet: If an IoT Gateway is deployed within the industrial plant and if a few application crashes in Gateway or a few need of login to the gateway. If so, Azure IoT edge must permit users to remotely log in to the IoT gateway the use of ssh/telnet. This can be very easy to reveal the status and debugging/protection. [17]

Sybil attack: The enterprise makes use of machine studying structures to assist prevent cyber assaults or to mitigate ability damage have to they succeed. Every day, Microsoft's account protection structures automatically locate and prevent greater than 10 million attacks from tens of hundreds of locations, even if the attacker has legitimate credentials. [18]

Man in the middle attack: Numerous Microsoft Azure IoT SDKs are inclined to a security weakness that may enable aggressors to direct ridiculing attack. A man-in-the-middle attack can misuse this issue to lead caricaturing attack and perform unapproved activities. [19]

Replay attack: Microsoft engineers have pooled their endeavors to propose an assurance against what are known as "replay attack". These will be happen when an aggressor takes something like an injured individual's Author token and utilizations it to mimic them to get to generally anchored assets. [20]

Ransomware: Microsoft antimalware products had been up to date with signatures for this threat which includes windows defender antivirus. These submit summarizes measures that azure clients can take to prevent and stumble on this threat through azure security. [21].

IJIREEICE

ISSN (Online) 2321-2004
ISSN (Print) 2321-5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

Vol. 7, Issue 10, October 2019

Side channel attack:
Microsoft has sent alleviations over all the cloud administrations. The foundation that runs azure and confines client remaining burdens from one another is ensured. This implies a potential attacking utilizing a similar foundation can't attack any application utilizing these vulnerabilities.
[22].

2.4. Brillo/weave

DDos attack: Google released Brillo/Weave platform for the rapid implementation of IoT applications. From the last few years our favourite searching site google was attacked by Distributed denial of service or DDos .A DDos attack is an attempt to make an online service unavailable overwhelming it with traffic from multiple sources. They can have a huge impact if businesses aren't adequately prepared. As a google cloud customer we are protected by default to this type of attack. As the scale of our infrastructure enables us to simply absorb many of them. For context a huge attack last year had a strength of around one terabit per second (1Tb/sec) .The whole internet has a bisection bandwidth of 200Tb/sec. Now when we compare this to a single Google data center which has a bisection bandwidth of 1,300Tb/sec.
We can see Google already built in level of internal capacity multiple times doubt of any traffic load we anticipate. When there is an attack, Google have time to isolate it and address it but Google don't stop there. In Google cloud platform customers benefit directly from Google central dose mitigation service that provide an additional multi tear multi-layer protection and further reduces the risk to services running behind of Google front end. When the system detects an attack is taking place it can configure load balancers to drop or throttle traffic associated with the attack. [23].

Blueborne attack: Google related android device can minimize the BlueBorne attack. [24]
Below is a list of android devices that have the ability to stand against the blueborne attack:

- .Nexus 5X
- .Nexus 6P
- .Nexus 6
- .Nexus 9

Jamming Attack: Mobile jamming attack is a power wasting denial-of-service attack. The mobile jamming protecting method works multi topologies scheme to reduce the mobile jamming attack so the affected area also be reduce. [25]

Remote access using telnet: There is remote access in google but the hacker can't do anything because the data being encrypted.

Sybil attack: Existing decentralized defences have largely been designed for peer-to-peer networks but not for mobile networks. That is why a new decentralized defence for portable devices and call it MobID. The idea is that a device manages two small networks in which it stores information about the devices it meets: its network of friends contains honest devices, and its network of foes contains suspicious devices. By reasoning on these two networks. [26]

Exploit Kit: Exploit kit have some program interface which permit non-technical clients to through unclean attacks for stealing corporate and personal data. Google cloud can minimize this problem by default. [27]

Man in the middle attack: Google related application like google chrome can recognize man in the middle attack automatically. Google chrome warn the clients when 3rdparty software try to hack the web connection or something other data. [28]

Replay attack: To keep away from this kind of attack is all about having the right method of encryption. Google already released encryption at rest in google cloud platform and G suite encryption to prevent this attack on google cloud. [29]

Ransomware: Google related android device can also prevent the ransomware attack by having antivirus like Bitdefender, Kaspersky, M-cafe, and AVG etc. [30]

Side channel attack: Side channel attack can be removed by some steps, Eliminating the arrival of private data or confirming this data is random to private information.
Electrical cable molding and separating to dissuade control checking assaults and also emanating a station with commotion. [31]

IJIREEICE

ISSN (Online) 2321-2004
ISSN (Print) 2321-5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

Vol. 7, Issue 10, October 2019

2.5. Ericsson/Calvin

DDos attack: An effective way to improve the resilience of the centralized control plane and prevent the spread of DDoS control-plane attacks to the rest of the network is to rate-limit NEs in terms of bandwidth and resource consumption – such as CPU load, memory usage, and API calls. [32]

Remote access: Remote access is a product developed by Ericsson to offer video/sound conferencing, screen recording, screen capture, and cloud-based storage together with the additional usefulness of "automatic" checklist, genuine time bookmarking, accessible hyperlinked work area of substance, commented on screen catches, connections to supplemental material.
Ericsson's workers, suppliers and customers can utilize the product program as a way to associate and lead classes for VPWs and distinctive meetings.

Man in the middle attack: Something like 76 famous applications on Apple's iOS stage are vulnerable attack that could enable programmers to block and take information without being taken note.

Replay attack: Home kit device can prevent replay attack by default.

Ransomware: Apple says I-cloud won't be hacked by a ransomware attack. Cause the device had remotely locked in exchange for ransom. [33]

2.6. Apple homekit

DDos attack: Apple was generally late to the table with its HomeKit smart home stage. It was inventin 2014, and the first HomeKit-suitable smart device didn't begin rolling off until a year later. A major piece of that delay was likely the security requests AAPL put on producers, including the additional expense of an authentication chip every device requires. [34]

Blueborne attack: The older model of apple device can't take away the BlueBorne attack. Below a list of the oldest device that can't discover this assault. [35]

- iPhone 4S and older
- iPad (third generation) and older
- iPad mini (1st generation) and older
- iPod touch (fifth generation) and older
- Apple TV (third generation) and older

However in the more moderen version device can detect BlueBorne attack

Remote access using telnet: In apple home kit Device has remotel access. A center hub is set up to the home kit device. Byutilizing the home application the client can oversee or control the home kit accessories by iOS device or mac.

Man in the middle attack: The first-rate way to stay away of this will be to rotted the device and manually in capacitatessl take a look at or update the embedded declarations with burpsuite's. This will be require a notably extra complex size of attack and if the device is jailbroken/rotted there are different attack vectors to ponder.

Ransomware attack: Apple has launched security update iOS 10.3.2 and macOS 10.12.5 on may additionally 15th that rolled out over 20 security fixes for iPhones and iPads and 30 protection someplace for Mac. The cyber-attack is extreme sufficient to make Apple patch up the vulnerability in iBooks for iOS and macOS. As soon as being attacked, iOS isn't as that secure as the customers have considered ever. New update is available now. So we can update to the latest iOS or macOS to fix the bugs.

2.7. Smartthing/Samsung

DDos attack: Watched a development of new reflex and improvement DDoS ambushes manhandling Internet of Things devices like smart things on Samsung which that mishandles correspondences traditions. The data is as per the revelations of the report starting late issued by Arbor Networks related to DDoS ambush saw in Q3 2014. The SSDP tradition misused by peril performing craftsmen are routinely used by such gadgets to speak with every other and to encourage practices

IJIREEICE

ISSN (Online) 2321-2004
ISSN (Print) 2321-5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

Vol. 7, Issue 10, October 2019

with various types of hardware. The IoT gadgets revealed on the Internet are engaged by horrendous performing craftsmen that exchange off them to sort out critical real assaults against big business targets. [36, 37]

Blueborne attack: The BlueBorne weakness licenses remote software engineers to broaden full control upon Bluetooth-enabled gadgets withal while it isn't coordinated with the developer's gadget or perhaps set to definable mode. It's prepared to affect cell phones, medications, pcs, or possibly IoT contraptions. A settle for the BlueBorne weakness end up settled with the Sept 2017 assurance rebuilding, be that as it may, Samsung has ceased the territory on its gadgets with the August 2017 security fix. These updates are incorporated into microcode shapes that contain the letter 'I' inside the penult position. [38]

Jamming attack: Experts found a blemish in the crucial ZigBee sorting out tradition that would allow attackers to stick correspondences on the framework in the midst of a break-in, thusly keeping security alarms from initiating. Samsung issued a fix for customers two or three months sometime later. [39]

Remote access using telnet: Samsung's execution for the Android Radio Interface Layer (RIL), that handles interchanges for modem. At the same time as identifying Samsung's RIL to make its very own substitution, Kocialkowski determined the product utilizes the Samsung IPC convention to actualize RFS directions and perform far flung I/O sports. Which usage the Samsung IPC conference, for maximum part Intel XMM6160 and Intel XMM6260 modems. [40]

Expliot kit attack: Investigators from Austria's Graz Technical college, who found that they may abuse the Meltdown weakness to attack Samsung gadgets. [41]

Main in the middle attack: As per varela's exploration the MITM assault can screen the correspondence among the Samsung pc and Samsung servers enabling the aggressor to block a demand for an xml paper that take on the model id for which the drivers are being asked. Samsung executed a figured correspondence between the instrument and its servers and furthermore a confirmation system. [42]

Relay attack: Samsung FAQ secured. "Samsung Pay and our associates respected this power hazard worth offered them to a super degree low likelihood of a productive token exchange assault. [43]

Ransomware: Bug in Samsung they can’t minimize Ransomware Attacks. [44]

Side channel attack: Samsung built up any other rendition of a side channel attack to split the worldwide AES-CCMkey that Philips makes use of to encode and verify new firmware. [45]

5.8. Kuru/Java

DDos attack: Memory and CPU advantages woodstox-focus asl are vulnerable against refusal of organization dos attacks. That shortcoming can be initiated when xml with a broad number of segments qualities or settled creates are passed to readerconfig.java causing CPU and memory usage. [46]

Blueborne attack: The blueborne strike vector has a couple of series. Inside the primary spot hacker uncovers dynamic Bluetooth relationship round which separate. Gadgets have ability to analysed paying little mind to whether they may be not appropriate to discoverable mode. Resulting hackers gets the instrument's macintosh clue which is a first class identifier of that express device. Which means of experimenting with the device the hacker can recognize out which working procedure his harmed individual is using and manage his experience in like manner. The hacker will by then abuse feebleness inside the execution of the Bluetooth convention to monstrous degree. [47].

Jamming attack: optimal jamming attacks and system barrier approaches in remote sensor systems venture is a 2010 cse venture which is actualized in java stage. This task clarifies about sticking and barrier instrument is executed in java/osgi-base. [48]

Remote access using telnet: Apache active mqartemis is helpless against deserialization assaults. The jms self-command plots a get item technique on the javax.jms. Object message magnificence. The apache artemis execution of this technique permits the deserialization of things from untrusted assets. There are some spots within which apache artemis utilizes this get item approach. Those elements may also on this manner be defenceless against a distant code execution assaults. for this vulnerability to be exploited the sender of the listed off message must be confirmed and approved an honest thanks to sending the message to the artemis representative and influenced coaching device directions gift at the artemis magnificence manner.[49]

IJIREEICE

ISSN (Online) 2321-2004
ISSN (Print) 2321-5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

Vol. 7, Issue 10, October 2019

Exploit kit attack: We sort abuses in our malware reference book by the stage they target. For instance exploit java/cve-2013-1489.a is an adventure that objectives a helplessness in java. Basic vulnerabilities and exposures cve is utilized by numerous security programming merchants. The undertaking gives every defencelessness an extraordinary number for instance cve-2016-0778. The bit 2016 alludes to the year the helplessness was found. The 0778 is a one of a kind id for this explicit weakness. [50]

Ransomware: java is not defined via the manner wherein it acknowledges the files are defiled in its assault in order to be set apart with the report expansion '.java ' introduced as a ways as practicable of the prompted files' names. The java not-dharma ransomware changed into first seen from April of 2018 and the java not-dharma ransomware indicate to do a ransomware trojan assault like numerous ransomware. It is being utilized to target non-public ventures and internet servers right now. [51]

Side channel attack: Vulnerabilities in java/osgi bundle interactions assaults against java segments at the case of osgi group's scientific categorizations .a portion of the issues it addresses by changing the sort arrangement of java. [52].

Table.1comparative security's analysis

Attack/ Cloud	DoS/ DDoS Attack	Blue Borne	Jamming Attack	Remote access Using Attack	Sybil Attack	Exploit Kit Attack	Man in The middle attack	Replay Attack	Ransomware Attack	Side channel Attack
AWS(Amazon Web Service)	Yes	No	Yes	There Is no access	No Result	Yes	Yes	No Result	No	Yes
ARW mbed	Yes	No Result	Yes	No Data Encrypted	No Result	No Result	Yes	Yes	No Result	Attacked But can be deleted
Azure IoT Suite	Yes	No	Yes	Remoteley login	Yes	Yes	No	Yes	Yes	Yes
Brillo/ Weave	Yes	Yes	Yes	No Result	Yes	Yes	Yes	Yes	Yes	Yes
Calvin	Yes	No Result	No Result	Remotely login	No Result	No Result	No	Yes	Yes	No Result
Home Kit	Yes	Yes	No Result	Yes	No Result	No Result	No	No Result	Yes	No Result
Kura	Yes	Yes	Yes	Yes	No Result	No	Yes	Yes	No	No
Smarthing	Yes	Yes	Yes	No	No Result	Yes	No Result	No Result	No	No

III. CONCLUSION

The IoT market is growing rapidly and as a consequence, the attention has shifted from proposing single IoT elements and protocols towards application platforms in order to identify frameworks supporting the standard IoT suites of regulations and protocols. This study has covered a subset of commercially available frameworks and platforms for developing industrial and consumer-based IoT applications. The selected frameworks have the same design philosophy in terms of identifying cloud-based applications by centralizing distributed data sources. However, they followed various approaches in order to apply this philosophy. A comparative analysis of the frameworks was conducted based on the architecture, hardware compatibility, software requirements, and security. We highlighted on the security measures of each framework as verifying the various security features and immunity against attacks is one of the most important contemporary issues facing the Internet of Things.

IJIREEICE

ISSN (Online) 2321-2004
ISSN (Print) 2321-5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

Vol. 7, Issue 10, October 2019

REFERENCES

[1]. https://aws.amazon.com/answers/networking/aws-ddos-attack-mitigation/.[Accessed time: 6.19 PM 17-Nov-18]
[2]. https://www.amazon.co.uk/Enhanced-Dissembling-Schemes-Jamming-Prevention/dp/3659443727. [Accessed time: 6.37 PM 17-Nov-18]
[3]. https://vceguide.com/does-amazon-rds-allow-direct-host-access-via-telnet-secure-shell-ssh-or-windows-remote-desktop-connection/.[Accessed time: 8.18 PM 17-Nov-18]
[4]. https://securityboulevard.com/2018/03/new-attack-vectors-brought-by-the-cloud-and-aws/.[Accessed time: 9.28 PM 17-Nov-18]
[5]. https://d1.awsstatic.com/whitepapers/Security/Networking_Security_Whitepaper.pdf.[Accessed time:10.18 PM 27-Nov-18]
[6]. https://www.techrepublic.com/article/unsecured-amazon-s3-buckets-are-prime-cloud-target-for-ransomware-attacks/. [Accessed time: 10.23 PM 27-Nov-18]
[7]. https://aws.amazon.com/security/security-bulletins/AWS-2018-019/.[Accessed time:11.29 PM 27-Nov-18]
[8]. https://www.itworld.com/article/3136307/internet-of-things/to-solve-iot-security-look-at-the-big-picture-arm-says.html.[Accessed time: 12.12 AM 28-Nov-18]
[9]. https://www.researchgate.net/publication/301705986_An_Embedded_Sensor_Node_Microcontroller_with_Crypto-Processors.[Accessed time: 10.18 PM 02-Dec-18]
[10]. https://os.mbed.com/forum/mbed/topic/934/?page=1#comment-4523. [Accessed time: 10.21 PM 02-Dec-18]
[11]. https://www.theregister.co.uk/2017/08/31/arms_embedded_tls_library_patched_to_fix_mitm_bug/.[Accessed time: 11.38 PM 02-Dec-18]
[12]. https://os.mbed.com/users/electronichamsters/notebook/ble-advertisement-replay-attack--spoof-detection/.[Accessed time: 10.26 PM 03-Dec-18]
[13]. https://tls.mbed.org/discussions/crypto-&-ssl/aes-implementation-resistant-to-side-channel-analysis-attacks.[Accessed time:12.28PM 4.Dec.18]
[14]. https://azure.microsoft.com/en-us/services/ddos-protection/.[Accessed time: 10.26 PM 05-Dec-18]
[15]. https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8628.[Accessed time: 10.29 PM 05-Dec-18]
[16]. https://docs.microsoft.com/en-us/azure/iot-fundamentals/iot-security-ground-up.[Accessed time: 10.33 PM 05-Dec-18]
[17]. https://feedback.azure.com/forums/907045-azure-iot-edge/suggestions/34484857-remote-login-to-iot-gateway.[Access time:10.41PM 5.Dec.18]
[18]. https://www.networkworld.com/article/3067358/security/how-microsoft-keeps-the-bad-guys-out-of-azure.html.[Access time:10.49PM 5.Dec.18]
[19]. https://www.symantec.com/en/au/security-center/vulnerabilities/writeup/104070.[Accessed time: 10.57 PM 05-Dec-18]
[20]. https://www.theregister.co.uk/2018/10/10/token_binding_protocol_rfc.[Accessed time: 11.02 PM 05-Dec-18]
[21]. https://azure.microsoft.com/sv-se/blog/petya-ransomware-prevention-detection-in-azure-security-center.[Accessed time: 6.20 PM 08-Dec-18]
[22]. https://docs.microsoft.com/en-us/azure/virtual-machines/windows/mitigate-se.[Accessed time:6.28 PM 08-Dec-18]
[23]. https://cloud.google.com/security/.[Accessed time: 6.38 PM 08-Dec-18]
[24]. https://www.theandroidsoul.com/blueborne-attack-and-android-everything-you-need-to-know/.[Accessed time: 6.54 PM 08-Dec-18]
[25]. https://patents.google.com/patent/US20090325478.[Accessed time: 7.20 PM 08-Dec-18]
[26]. https://www.mdpi.com/2073-8994/9/3/35.[Accessed time: 7.26 PM 08-Dec-18]
[27]. https://whatis.techtarget.com/definition/crimeware-kit-attack-kit.[Accessed time: 10.20 PM 08-Dec-18]
[28]. https://www.v3.co.uk/v3-uk/news/3017079/google-chrome-to-provide-man-in-the-middle-attack-warnings.[Access time: 10.22 PM 08-Dec-18]
[29]. https://en.wikipedia.org/wiki/Replay_attack.[Accessed time: 10.25 PM 08-Dec-18]
[30]. https://www.quora.com/Android-operating-system-How-do-I-block-Ransomware-attack-on-my-Android-tablet.[Access time:10.34PM 8.Dec.18]
[31]. https://www.jungledisk.com/blog/2017/12/28/be-aware-of-side-channel-attacks/.[Accessed time: 10.43 PM 08-Dec-18]
[32]. https://www.ericsson.com/en/ericsson-technology-review/archive/2015/identifying-and-addressing-the-vulnerabilities-and-security-issues-of-sdn.[Accessed time: 10.52 PM 08-Dec-18]
[33]. https://www.makeuseof.com/tag/cloud-drive-ransomware/.[Accessed time: 10.58 PM 08-Dec-18]
[34]. https://investorplace.com/2016/10/how-apple-inc-aapl-homekit-protects-against-ddos-attacks/.[Accessed time: 7.21 PM 14-Dec-18]
[35]. https://www.intego.com/mac-security-blog/what-is-blueborne-an-apple-device-faq/.[Accessed time: 7.27 PM 14-Dec-18]
[36]. https://www.cybercureme.com/bugs-in-samsung-iot-hub-leave-smart-home-open-to-attack.[Accessed time: 7.33 PM 14-Dec-18]
[37]. http://iotworm.eyalro.net/.[Accessed time: 7.43 PM 14-Dec-18]
[38]. https://www.sammobile.com/2017/09/25/samsung-rolls-security-patches-fix-blueborne-vulnerability/.[Accessed time: 7.48 PM 14-Dec-18]
[39]. https://www.techhive.com/article/3064372/home-tech/samsung-smartthings-vulnerability-lets-hackers-make-their-own-house-keys.html.[Accessed time: 9.33 PM 14-Dec-18]
[40]. https://www.zdnet.com/article/backdoor-in-samsung-galaxy-devices-allows-remote-access-to-data/].[Accessed time: 9.54 PM 14-Dec-18]
[41]. https://www.silicon.co.uk/mobility/smartphones/samsung-s7-meltdown-exploit-235753.[Accessed time: 8.20 PM 23-Dec-18]
[42]. www.securew2.com/blog/samsung-keyboards-vulnerable-to-man-in-the-middle-exploit.[Accessed time: 8.23 PM 23-Dec-18]
[43]. https://www.tomsguide.com/us/samsung-pay-tokens-vulnerable, news-23159.html.[Accessed time: 8.35 PM 23-Dec-18]
[44]. https://www.researchgate.net/publication/326609660_A_taxonomy_of_cyber-physical_threats_and_impact_in_the_smart_home.[Accessed time: 9.26 PM 23-Dec-18]
[45]. http://iotworm.eyalro.net/.[Accessed time: 10.25 PM 23-Dec-18]
[46]. https://www.sourceclear.com/vulnerability-database/security/denial-service-dos-memory-cpu/java/sid-833.[Access time: 10.34 PM 23-Dec-18]
[47]. https://security.stackexchange.com/questions/169527/what-is-blueborne-and-how-to-protect-myself.[Accessed time: 8.28 PM 25-Dec-18]
[48]. http://1000projects.org/optimal-jamming-attacks-and-network-defense-policies-in-wireless-sensor-networks-project.html.[Accessed time: 8.29 PM 25-Dec-18]
[49]. https://www.sourceclear.com/vulnerability-database/security/remote-code-execution-through/java/sid-2786.[Access time: 9.22 PM 25-Dec-18]
[50]. https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/exploits-malware.[Accessed time: 10.28 PM 25-Dec-18]
[51]. https://www.enigmasoftware.com/javanotdharmaransomware-removal/. [Accessed time: 10.45 PM 25-Dec-18]
[52]. https://crypto.stackexchange.com/questions/48867/timing-safety-in-jvm-languages/48877#48877.[Accessed time: 10.53 PM 25-Dec-18]