ISSN 2349-6193
Impact Factor: 2.805

IJESMR
International Journal OF Engineering Sciences & Management Research

ROBUST IOT SECURITY FRAMEWORKS: ADDRESSING IMPLEMENTATION AND NETWORK CAPACITY CONSTRAINTS

[1]Sri Bhargav Krishna Adusumilli, [2]Harini Damancharla
[1]Senior Software Engineer, Research Scholar,
[2]Senior Software Engineer, Research Scholar,
[1]sribhargav09@gmail.com, [2]damanharini@gmail.com
[1]https://orcid.org/0009-0005-4059-387X, [2]https://orcid.org/0009-0000-3899-3325

Keywords: cloud computing; IoT; cloud security; access control list; simple network monitoring protocol; Amazon Web Service (AWS); moving target defense (MTD)

ABSTRACT

This paper proposes a solution for ensuring the security of IoT devices in the cloud environment by protecting against distributed denial-of-service (DDoS) and false data injection attacks. The proposed solution is based on the integration of simple network management protocol (SNMP), Kullback–Leibler distance (KLD), access control rules (ACL), and moving target defense (MTD) techniques. The SNMP and KLD techniques are used to detect DDoS and false data sharing attacks, while the ACL and MTD techniques are applied to mitigate these attacks by hardening the target and reducing the attack surface. The effectiveness of the proposed framework is validated through experimental simulations on the Amazon Web Service (AWS) platform, which shows a significant reduction in attack probabilities and delays. The integration of IoT and cloud technologies is a powerful combination that can deliver customized and critical solutions to major business vendors. However, ensuring the confidentiality and security of data among IoT devices, storage, and access to the cloud is crucial to maintaining trust among internet users. This paper demonstrates the importance of implementing robust security measures to protect IoT devices in the cloud environment and highlights the potential of the proposed solution in protecting against DDoS and false data injection attacks.

INTRODUCTION

Although we refer to *the* Internet of Things (IoT) as if it formed a system, this terminology is not entirely correct and does reflect modern developments. Precursors of the IoT enjoyed various names such as Pervasive Computing, Ubiquitous Computing or Machine-to-Machine Communications (the latter taking a more network centric view) and sought to convey the idea that computation could occur anywhere. Indeed, the IoT is not just a collection of "things", nor a well defined system formed of things, but the instrumentation of the entire physical space surrounding us with an Internet connected digital interface and computational capabilities that increasingly comprise decision making and even learning. We often talk of *"smart"* things whether it is, for example, smart-meters, smart-buildings or, smart-toys. Again this only reflects that all objects that we are accustomed to in our physical spaces now comprise a digital component able to perceive the physical world through sensors and to control it through actuators. This point is particularly important when it comes to security. Compromising the security of the digital interface of a physical object impacts its physical behaviour and security, and the threats to be considered do not all originate in the digital (cyber) space but may start by exploiting their physical vulnerabilities or the trusting nature of their human users. Having made this point, this paper adopts commonly accepted terminology and refers to IoT Systems, Devices, Networks or Environments, bearing in mind that it is only a digital (cyber) perspective on the entirety of the physical world that surrounds us, which interconnects the physical world to the resources of the digital space.

The number of IoT devices is continuously increasing, and this trend is set to continue. In their latest report, IoT Analytics estimated that in 2022, the global number of connected IoT devices grew to 14.4 billion, which is a 18% increase compared to 2021, and by 2025, IoT Analytics predicts that there likely to be around 27 billion IoT connections (Sinha, 2021). In some respects, this may turn out to be an underestimate. On one hand the size of the devices is continuously reducing as well as their power consumption. On the other the (wireless) network connectivity is increasing, e.g., the deployment of 5G (Wasicek, 2020). Finally, devices are increasingly capable of learning and autonomous decision making. These trends will lead to more devices being used to monitor the physical world at a finer level of granularity and provide increasingly complex systems that optimise our usage of resources, personalise the services that are offered to us and, hopefully, increase our quality of life.

ISSN 2349-6193
Impact Factor: 2.805

IJESMR
International Journal OF Engineering Sciences & Management Research

However, adding an IoT device to a system is also adding an opportunity to compromise that system for a malicious actor. Any device connected to the Internet can be attacked from any other Internet location. Furthermore, in contrast to traditional computers or cloud servers securely hosted in offices or secure physical locations, IoT devices are deployed in the physical environment and can also be subjected to direct connections and physical attacks. Considering their vulnerability, a direct consequence of adding many IoT devices to our systems is that the attack surface of the IoT systems is also increasing exponentially. Faster interconnections, and rapid response also mean that compromises can spread faster and wider within the systems making them more difficult to protect and dependent on rapid response to a compromise to maintain their resilience. As well as making systems more robust to adversarial threats "by design", it is also necessary to deploy response techniques that can hinder the progress of an attack as well as responses that enable an adaptation (re-configuration) of the system and its recovery to maintain the system's function even when the systems have been partially compromised.

The security and resilience of IoT environments is a complex topic that spans across the entirety of their life-cycle from design and realisation to their deployment, operation and decommissioning. In contrast to the other related surveys which fall short of outlining concrete coherent steps to mitigate the spread of attacks in an IoT environment, this survey explores security measures in IoT system that are applied throughout the life-cycle of the IoT devices starting from their design, to the moment when a device joins a network, while the IoT device operates in the network, and until it leaves (or is/removed) from the network and decommissioned. The survey discusses threat mitigation techniques applied across different IoT application contexts, and elaborates on how to apply each mitigation technique, its benefits and limitations and the extent to which progress has been reported in the literature. In essence, the discussed measures provide answers to the questions of how IoT device(s) connect and communicate with new devices and systems safely, starting from the moment when the IoT device(s) join the new environment, whilst operating in it, when an attack occurs, and until the device is removed/decommissioned or leaves the environment. This paper adopts a" defence in depth" strategy in discussing mitigation techniques proposed for the aim of controlling and slowing down the spread of threats in the IoT environment throughout the life-cycle of the IoT device. A defence in depth strategy to securing systems uses measures that aim to reduce systems vulnerabilities, contain threats, and mitigate attack effects if they occur, such that if an attacker manages to overcome one layer of defence, they still need to overcome the subsequent defence layers to compromise the system (Vacca, 2012). The challenges are being addressed in the design of individual devices and in the design and operation of deployments. Like in the case of enterprise or more traditional computing environments, new techniques are being developed to make devices more trustworthy and new techniques are being developed to make systems more resilient and trustworthy by detecting, mitigating and responding to threats at run-time.

The contributions of this survey are summarised as follows: i) This survey discusses the state of the art covered in previous surveys, whilst focusing on defending against threats rather than on the threats alone. A summary of the discussed topics in the prior surveys along with examples of mitigation techniques suggested are presented in Table 1. ii) This survey collates current research into risk and threat mitigations in the dynamic IoT environment, considering the mobility if the IoT systems, which is composed of several devices that join and leave a network dynamically. To achieve this, this survey provides an overview and presents these mitigation techniques uniquely throughout the life cycle of the IoT device, starting from its design, to the moment when a device joins a network, while the IoT device operates in the network, and until it leaves (or is removed) from the network and is eventually decommissioned, hence adopting a "defence-in-depth" approach. A taxonomy for the mitigation techniques discussed in this survey, and which are applied throughout the life-cycle of an IoT device is presented in Table 2. iii) This survey takes a more comprehensive and detailed step by analysing a broad variety of methods for accomplishing each of the mitigation steps, and elaborates on how to apply each mitigation technique across different IoT application contexts, its benefits, as well as highlighting their challenges, limitations, difficulty of implementation, and the extent to which progress has been reported in the literature. iv) This survey sheds a light on a rarely discussed method in literature, that is, exploiting the redundancy as an inherent nature of multi-sensor IoT applications to improve integrity and recovery, and discusses different methods on harnessing redundancy in inter-connectivity as a mitigation technique to reconfigure networks in response to security events and isolate compromised devices, whilst enabling the rest of the network to operate normally. v) The survey emphasises novel perspectives for the discussed mitigation steps, and reconnects them to the ground principles they seek to implement.

ISSN 2349-6193
Impact Factor: 2.805

IJESMR
International Journal OF Engineering Sciences & Management Research

This survey is structured according to the life-cycle of an IoT device in a dynamic context, i.e., before a device joins a system, when a device wants to join a system, while the device is in the system, when a cyber attack occurs, if the device has been compromised, and when the device leaves or is removed from the system. This structure is depicted in Table 2.

After summarising the aspects covered in prior surveys in Section 2, this survey discusses aspects of self-protection and self-defence in Section 3, in particular, techniques to secure the IoT device before and when a device join a new system. Techniques based on mediation are discussed in Section 4 as techniques to secure the IoT device and a system while the device operates in the system. Segmentation techniques are discussed in Section 5 as techniques to mitigate the impact of the attack on the system when a cyber attack occurs. Techniques based on redundancy and recovery are discussed in Section 6 as mitigation techniques to be applied when the device leaves or is removed from the system.

Research theme	Topics covered	Examples on mitigation techniques covered	Related surveys
IoT application domains	Industrial Control Systems (SCADA), SmartGrids, Intelligent Transportation Systems, E-Health and Medical IoT Systems, Smart Home and Automation IoT Systems	- Threats related, e.g., Secure remote access	Stellios et al. (2018)
		- Vulnerability related, e.g., Tamper resistance	
		- Connectivity related, e.g., Network segmentation	
IoT stack layers	1- Physical Layer, Data Link Layer, Network Layer, Transport Layer, Application Layer	1- Physical: spread-spectrum communication, MAC: Error correction codes, Network: Multi-path routing, Transport: security policies, Application: CoAPs	1-Butun et al. (2019)
	2- Sensing layer, Network layer, Middleware layer, Application layer	2- Using blockchain, using fog Computing, using machine learning, using edge computing	2-Hassija et al. (2019); Lu and Xu (2019)
	3- Perception layer, Network layer, Application layer	3-Perception: intrusion detection, Network: IPv6 and IPSe	3-Mohamad Noor and Hassan (2019)
IoT technologies (practical and technical)	1- ZigBee, BLE, 6LoWPAN, LoRaWAN.	1- ZigBee: trust centre, BLE: pairing using elliptic curve cryptography, 6LoWPAN: RPL, LoRaWAN: different keys to verify Message Integrity Code (MIC)	1-Meneghello et al. (2019)
	2- Case studies: EV charger, Itron Centron CL200 smart meter, Fitbit Aria, g Google's Nest Thermostat, Tesla Model S, Chamberlain MyQ, Parrot AR 2.0 Quadcopter, Edimax IP camera system	2- Additional parameter validation, tamper-resistant, encryption, chain-of-trust secure boot, Random Number Generators, Strong password, access restrictions, identity management	2-Alladi et al. (2020)
	3- Physical-based, e.g., RFID, Protocols-based, e.g., NFC,Bluetooth, Wifi, ZigBee, Network-based, e.g., RPL, 6loWPAN, TCP-UDP.	3- Physical: lightweight cartographic mechanisms, protocol based: error control mechanisms, network based: intrusion detection	3-Abdul-Ghani et al. (2018)
IoT device life cycle	1- Smart home environment: security of the development of IoT devices, integration of devices in home networks, usage until end-of-life	1- Minimum reliability, trust infrastructure, network segmentation, use gateways, vulnerability survey, software updates, remote protection, secure backup	1-Cedric Levy-Bencheton (2015)
	2- IoT supply chain: actors, processes and technologies	2- Product design: sabotage prevention, semiconductor fabrication: scrap management, component manufacturing: defective components, component Assembly: firmware access control, device programming: coding practices, distribution: tracking for registration, technical support: patches, recovery: data removal	2-Christina Skouloudi (2020)
	3- Smart environments: security Critical Information Infrastructures, Policies, Technical Measures	3- Security by design, trust management, firmware updates, authentication, cryptography, logging, end-of-life support	3-ENISA (2017)
Other themes	1- Certification	1- IoT device life cycle support	1-Matheu et al. (2020b)
	2- Artificial Intelligence	2- Naïve Bayes for intrusion detection	2-Kuzlu et al. (2021)
	3- Software Defined Networks	3- vFirewalls, vIoTHoneyNet, traffic filtering and isolation, vChannelProtection	3-Liu et al. (2023b)
	4- Blockchain	4- Trust management	4-Molina Zarca et al. (2019)

Table-1

ISSN 2349-6193
Impact Factor: 2.805

IJESMR
International Journal OF Engineering Sciences & Management Research

IoT Device life cycle	Mitigation technique	Related studies and proposed work
Before a device joins a system	Device self-protection and self-defence	Sidhu et al. (2019); Hamadeh et al. (2017); Lu et al. (2020); Eldefrawy et al. (2012); Mohan et al. (2018); Dhavlle et al. (2021); Demme et al. (2013)
	- Hardware self-protection	
	- Software self-protection	Ravi et al. (2004); Zavalyshyn et al. (2020); Frank et al. (2018); Choi et al. (2018); Ankergård et al. (2021); Mercado-Velázquez et al. (2021); Navas et al. (2020, 2021)
	- Moving Target Defence	
If a device wants to join a system	Certification	Matheu et al. (2020b), Matheu et al. (2020b)
While the device is in the system	Mediation	Leo et al. (2014); Mahmoud et al. (2015); Davies et al. (2016); Chio et al. (2019)
	- IoT Edge	Zarpelão et al. (2017)
	- Continuous monitoring	Franco et al. (2021); Vetterl (2020); Pa et al. (2015)
	*Intrusion detection	Kuzlu et al. (2021); Chaabouni et al. (2019); Kumar et al. (2021); Meidan et al. (2018); Pacheco et al. (2019); Pauna et al. (2019)
	*Honeypots	
	*AI techniques for monitoring and detection	
When a cyber attack occurs	Device self-protection and self-defence	Sidhu et al. (2019); Hamadeh et al. (2017); Lu et al. (2020); Eldefrawy et al. (2012); Mohan et al. (2018); Dhavlle et al. (2021); Demme et al. (2013)
	- Hardware self-protection	Ravi et al. (2004); Zavalyshyn et al. (2020); Frank et al. (2018); Choi et al. (2018); Ankergård et al. (2021)
	- Software self-protection	Mercado-Velázquez et al. (2021); Navas et al. (2020, 2021)
	- Moving Target Defence	
If the device has been compromised	Device(s) isolation and system segmentation	Stellios et al. (2018); Xing (2021); Stergiopoulos et al. (2020); Luiijf and Klaver (2021)
	- Identifying and documenting IoT dependencies	Wasicek (2020); Osman et al. (2020); Mämmelä et al. (2016)
	- Micro-Segmentation	Baldini et al. (2020); García et al. (2019); Zarca et al. (2019)
	- Software Defined Networks (SDN)	
When the device leaves or is removed from the system	System availability and resilience	Laszka et al. (2018); Venkatakrishnan and Vouk (2016)
	- Diversity	Salayma et al. (2017); Illiano and Lupu (2015); Illiano et al. (2017)
	- Exploiting data correlation	Rosenberg and Reinhardt (2021)
	- Exploiting data overhearing	Li et al. (2017); Ar-Reyouchi et al. (2020); Liao et al. (2019); Lee and Lee (2020)
	- Network Coding (NC)	

Table-2

TECHNICAL BACKGROUND

The key security concerns in the IoT environment [6] are classified into implementation, privacy, network infrastructure, security threats, malware, authentication, and authorization-related challenges. Violation of IoT-related security focus merely related to the areas of privacy and confidentiality among heterogeneous management and network capacity constraints. Possible security issues include securing IoT architecture, active detection, and protection of DoS and DDoS, standards, methods, or tools for managing all user identity and objects. A few issues related to the private domain are personal information control, improvement of privacy technologies and related rules, protection of exchanged sensitive information over the communication medium, and confidentiality of stored messages. The widespread adoption of the cloud to effectively carry out the collection, storage, and analysis of IoT data paves the way for more associated open challenges [7], which disrupt authorized access, retrieval, and extraction of information from the cloud.

The goal of this paper [8] is to identify the security challenges and key issues that are likely to arise in the IoT environment in order to guide authentication techniques to achieve a secure IoT service. Denial-of-service (DoS) [9] is considered to be the most dominant and devastating in the IoT environment. The attackers could be using flooding attacks in order to exhaust system resources such as CPU, memory, and bandwidth. With the adoption of numerous techniques, the attacker's target is to flood the network with bogus packets [10,11,12] and hence block legitimate or trusted users from utilizing the usual services.

Replay attack [13] targets the authentication and key exchange-related protocols in order to capture or store either a whole session or a fragment of a session in legitimate traffic. On gaining trust over the public network, the attacker sends the captured message in order to indicate participation in the original session. A replay attack is mentioned as a security weakness or vulnerability in the authorization procedure for accessing stored data. To handle a replay attack, the current scenario uses three types of solutions, including timestamp, nonce, or challenge-response mechanisms. The freshness of a message is identified and tracked by using the concept of timestamp, where the purpose of the nonce is the generation of random digits and comparing the same for granting access. Challenge-response measures attempt to test the pre-shared secret values between the user and the target system or entity.

ISSN 2349-6193
Impact Factor: 2.805

IJESMR
International Journal OF Engineering Sciences & Management Research

The password-guessing attack [14,15] occurs by overhearing the communication channel by exploring weaknesses in numerous authentication protocols. This type of attack could take place either in online or offline mode. The attacker will be able to guess all possible passwords in order to succeed in the authentication process. The main aim of a spoofing attack is to make the servers trust that the attacker is one of the authorized entities.
Various categories of distributed denial-of-service (DDoS) attacks, along with their impact on IoT devices, are discussed [16], along with detailed mitigation models. It deliberately discusses the classification of different intrusion detection systems, anomaly detection techniques, different intrusion detection models related to datasets, various machine learning and deep learning methods for pre-processing data, and malware detection is carried out. Most of the security challenges are specific to the issues related to IoT devices and are listed below in Figure 1.

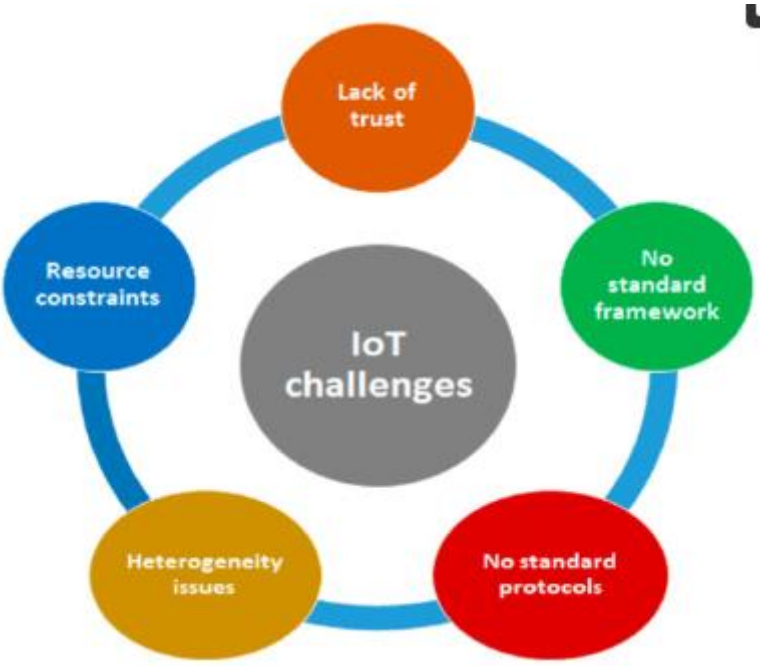

Figure 1. IoT challenges.

here are many categories of DDoS attacks specific to IoT devices namely, TCP SYN flood, tear drop, Smurf, ping of death, and botnet attacks. The main classification of DDoS includes reflection and amplification attacks. The main difference between these two attack categories could be analyzed by observing the size of request and response packets. The size of the response is *nn* times bigger than the request size in an amplification attack, whereas the size of the response is equal to the request size in reflection-based attacks. Attackers will be utilizing common vulnerabilities for launching DDoS attacks:

- Insecure connection;
- Weak password;
- Firmware updates;
- Software vulnerabilities;
- Data handling-related vulnerabilities.

Various anomaly detection techniques [17,18] used for detecting the presence of malware in IoT devices are signature-based detection and anomaly-based detection. The former detection pattern is not a successful one as the bots keep on changing their signature pattern, while the latter helps in tracking behavioral changes between the normal and botnet traffic. Other approaches related to community-based anomaly detection [19,20,21] focus on identifying bots based on the communication graph. A bad neighborhood is one of the methods utilized in phishing and spam detection to identify the cluster of IP addresses that performs malicious activities over a period of time.

ISSN 2349-6193
Impact Factor: 2.805

IJESMR
International Journal OF Engineering Sciences & Management Research

DIMENSIONS OF SECURITY THREATS IN IOT

The security threats and challenges associated with IoT are more prevailing as, according to a recent survey of IoT analytics, by 2025, there will be 30.9 billion [22] connected devices in the world. The increasing security vulnerabilities and cyber-attacks block many users from utilizing IoT devices. IoT-related security problems are more prevalent in healthcare and logistic-related domains [23]. The security challenges associated with IoT data while operating in a cloud environment could be generalized based on the analysis of common threats prevailing in the current scenario, which are listed below:

- Software vulnerabilities;
- Firmware vulnerabilities;
- Insecure communication channel;
- Data leaks from IoT systems;
- Malware risks;
- Cyber-attacks.

The possible causes for the occurrence of such threats in IoT-associated cloud environments are due to the following:

- Lack of computational capacity;
- Poor access control techniques;
- Limited budget to carry out testing;
- Limited budget to ensure firmware security;
- Lack of regular patches;
- Lack of periodic upgrades;
- Technical limitations of IoT devices;
- Unavailability of software updates for older IoT devices;
- Ineffective protection from physical attacks.

One of the most dangerous threats which happen due to an insecure communication medium is the Man-in-the-Middle (MiTM) attack. On installing malware or by changing the device's functionality, MiTM is launched if the device does not use any encryption or authentication mechanisms. Man-in-the-Middle (MiTM) attacks are a significant threat to the security of IoT systems due to their reliance on insecure communication mediums. These attacks involve the attacker intercepting and altering communication between two parties without their knowledge or consent. This can be accomplished by installing malware on a device or altering its functionality. IoT systems are particularly vulnerable to MiTM attacks because they often lack robust encryption and authentication mechanisms. As a result, attackers can easily intercept and modify communication between devices, making it difficult for users to detect and prevent these attacks. IoT systems are prone to various cyber-attack categories, as depicted in **Figure** 2. Application attacks target vulnerabilities in the software or firmware of an IoT device. This can include SQL injection, cross-site scripting, and command injection attacks. Physical intrusion involves physically accessing an IoT device to extract information, install malware, or disrupt its operation. An attacker may use tools like lock picking or physical access to the IoT device to perform these attacks.

Device spoofing involves tricking a device into connecting to a fake device or network, allowing the attacker to intercept or modify communication. This can be done through a technique known as "rogue access points" or "evil twin" attacks. Denial of sleep involves preventing IoT devices from entering a low-power state, which can cause them to consume more energy and potentially shorten their lifespan. Denial of service involves overwhelming a device or network with a flood of traffic, making it inaccessible to legitimate users. This can be done through a distributed denial-of-service (DDoS) attack, where multiple devices are used to flood the target. These attacks are often interconnected, with one layer of security being compromised, providing an easy pathway for a DDoS attack to be launched.

ISSN 2349-6193
Impact Factor: 2.805

IJESMR
International Journal OF Engineering Sciences & Management Research

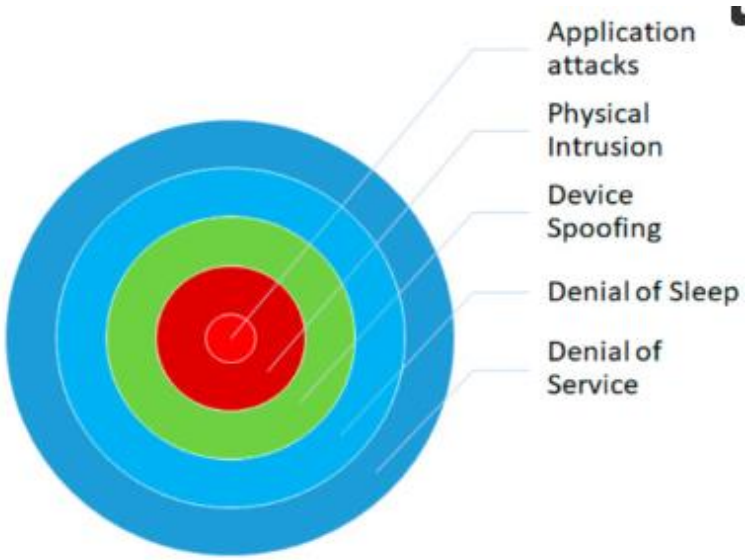

Figure 2. Cyber-attacks in IoT environment.

On careful analysis and deep inspection of existing cyber-attacks, general attacks, and device-specific threat categories of IoT in a cloud environment, the below structure, as depicted in Figure 3, is formulated. Irrespective of the type of cyber-attack in the cloud-assisted IoT environment, the below steps remain the same.

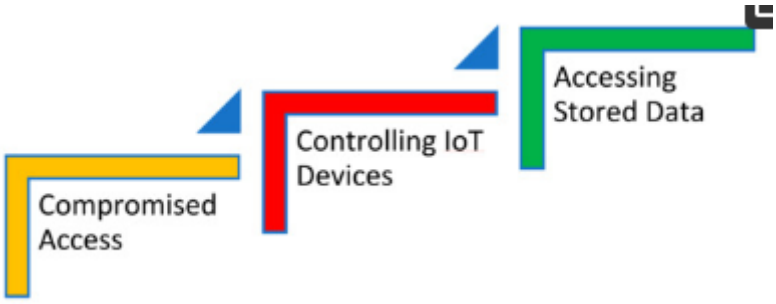

Figure 3. Stages of IoT threats in general.

Among other attack categories in the IoT environment, DDoS seems to be more prevalent, which is evident from the below statistics depicted in Figure 4. DDoS is more devastating as it makes the complete IoT devices inaccessible and unavailable for the legitimate user community. The prevalence of DDoS attacks in IoT platforms and their underlying structure are depicted in Figure 4 and Figure 5. Figure 4 clearly illustrates the bandwidth affected in the IoT platform due to the launch of a DDoS attack. The ultimate reasons for DDoS attacks are the insecure communication medium and unsecured data in a cloud environment. The proposed works address both by formulating an efficient architecture.

ISSN 2349-6193
Impact Factor: 2.805

IJESMR
International Journal OF Engineering Sciences & Management Research

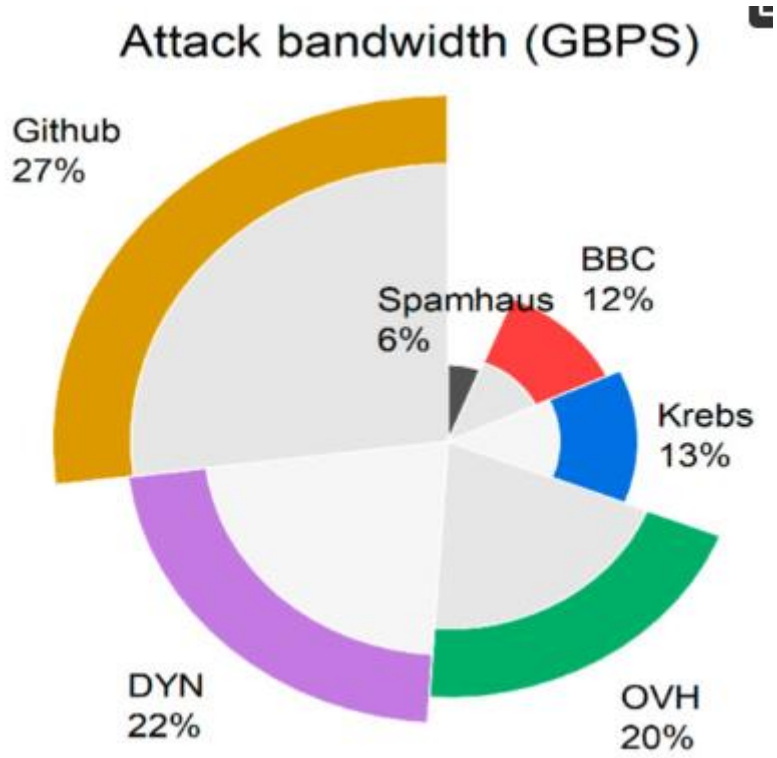

Figure 4. DDoS statistics in various IoT platforms.

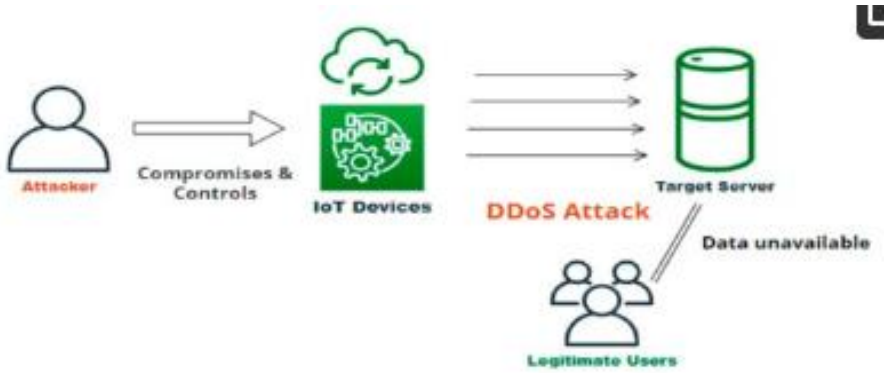

Figure 5. DDoS attack in IoT platform.

Due to the prevalence of DDoS attacks in IoT environments, this paper suggests the application of moving target defense strategies to make the attack target harder and to decrease the attack probability by applying various MTD techniques, diversity, and migration.

IoT Attack Mitigation Procedure Using ACL and MTD in AWS

The complete setup is configured in the Amazon Web Service (AWS) console to represent various proxy and web server configurations. For mitigation against DDoS, two levels of control measures are enforced by adopting the access control list in Level 1 and moving target defense-based migration concepts in Level 2. All the initial parameters specific to legitimate user requests are analyzed in detail, based on which the specific functionalities are identified in pre-defined ACL rules.

The main purpose of adding ACL rules in Level 1 is to filter DDoS attack traffic related to user-agent, header filed, request size, request count, and IP address. The requests which get validated and proven to be legitimate in Level 1 will be moved to Level 2. To secure the main or target server from crashing due to unwanted malicious

ISSN 2349-6193
Impact Factor: 2.805

IJESMR
International Journal OF Engineering Sciences & Management Research

incoming traffic, server hardening is carried out, which in turn decreases the DDoS attack probability by hiding the IP of the main server by maintaining servers in different availability zones and with the migration process. The target servers are made dynamic by applying the concept of MTD diversity. The location of the target server changes from time to time across various availability zones in order to withstand attacks by applying the concept of migration, which is depicted in Figure 6.

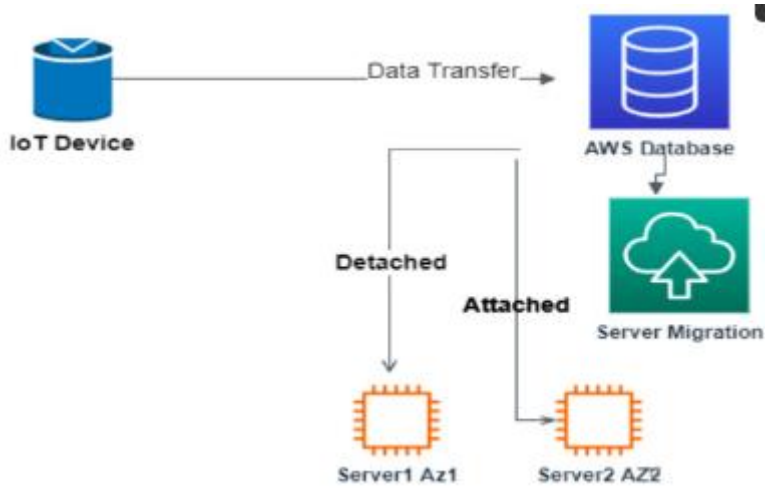

Figure 6. Securing IoT data in the cloud using MTD.

The AWS server instance plays a crucial role in maintaining the data that is transferred from IoT devices. In order to ensure the confidentiality of this data, the concept of server migration is applied. This is done to prevent an attacker from compromising the data by gaining knowledge of the IP address and other protection mechanisms of the server using port scanning tools.

The moving target defense (MTD) technique is applied to achieve more security by migrating the server instance from time to time. The migration process does not cause any delay or connection issues whenever there is a legitimate attempt because the AWS server instance in different availability zones alone remains attached or detached from the database instance. This is validated by the graph depicted in Figure 7 and Figure 8.

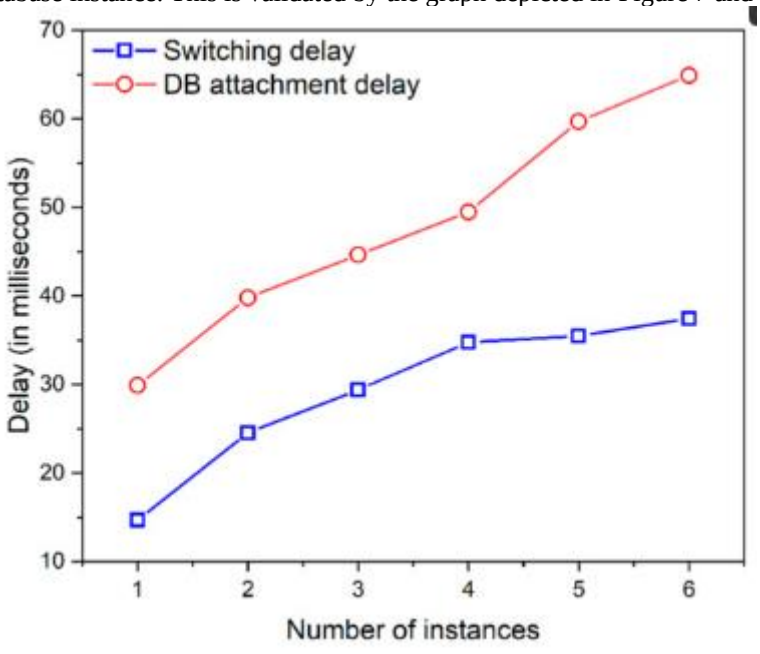

Figure 7. MTD delay estimation metrics observed in AWS.

ISSN 2349-6193
Impact Factor: 2.805

IJESMR
International Journal OF Engineering Sciences & Management Research

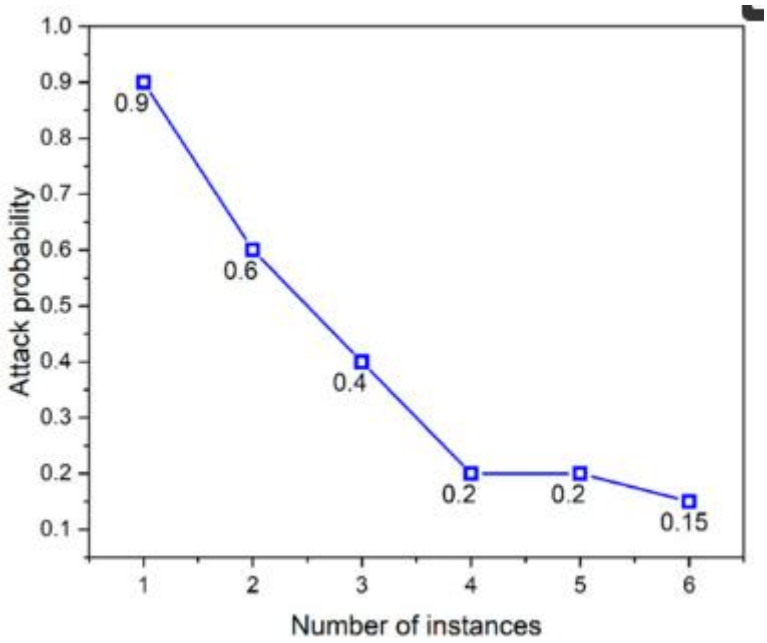

Figure 8. Attack probability on applying.

In Figure 7, the *x*-axis represents the number of instances chosen in AWS, and the *y*-axis represents the switching delay in milliseconds. The switching delay indicates the requests directed from one instance to another. The y-axis also represents the DB attachment delay in milliseconds which indicates the time taken to attach DB from one instance to another.

In Figure 8, the *x*-axis indicates the number of instances in AWS, and the *y*-axis indicates the attack probability reduction with an increase in the number of instances. It is observed that on increasing the number of AWS instances and applying the concepts of MTD, the attack probability is reduced to a minimum of 0.15% as the probability of occurrence of an attack. The chosen MTD method outperforms the existing schemes in reducing the attack probability from 0.5% to 0.15%, the switching delay reduced to 0.076 s from 1.2 s, and the DB attachment delay also decreased on comparing the existing literature from 1.4 s to 0.032 s.

Therefore, the methods applied in the proposed method are effective in mitigating the IoT-based DDoS and false data-sharing attacks with a considerable increase in performance metrics. The result shows that the MTD technique is effective in reducing the attack probability and improves the performance of the system by reducing the delay of switching and DB attachment.

CONCLUSIONS

IoT technology plays a vital role in today's digital, interconnected scenario. Ensuring the confidentiality and security of data from IoT devices is crucial for the success of the entire IoT model. In this paper, we discussed the detection and mitigation of DDoS and false data injection attacks in IoT environments. The detection of these attacks was carried out using simple network management protocol (SNMP) and kernel learning detection (KLD), whereas the mitigation was done using access control lists (ACL) and moving target defense (MTD) techniques. The proposed techniques were found to be more accurate and efficient than existing security techniques.

The focus of future work should be extended to the proposed techniques to detect and mitigate other types of IoT attacks. The communication channel is secured by maintaining ACL lists and SNMP monitors, while the stored data in AWS instances is maintained using MTD techniques such as diversity and migration. Both these techniques help in maintaining the dynamic IP address of the server and provide an added layer of security by not giving any clue about the location of the data. The processing delay due to migration is negligible, as evident from the experimental results discussed in the paper.

ISSN 2349-6193
Impact Factor: 2.805

IJESMR
International Journal OF Engineering Sciences & Management Research

In conclusion, the proposed techniques provide an efficient and effective solution for detecting and mitigating DDoS and false data injection attacks in IoT environments. The proposed techniques are not only accurate but also improve the performance of the system by reducing the delay of switching and DB attachment. As IoT technology continues to evolve and expand, it is essential to develop robust security mechanisms to protect against various types of attacks and ensure the confidentiality of data.

REFERENCES

1. Bhunia, S.S. & Gurusamy, M. (2022). "Dynamic attack detection and mitigation in IoT using SDN." In Proceedings of the 27th International Telecommunication Network Strategy and Planning Symposium.
2. Ferrag, M.A. et al. (2021). "Deep learning for cyber threat detection in IoT networks: A review." *Journal of Network and Computer Applications*.
3. Mrabet, H. et al. (2020). "A Survey of IoT Security Based on a Layered Architecture of Sensing and Data Analysis." *Sensors*.
4. "Dynamic attack detection and mitigation in IoT using SDN" (2023). *IEEE Xplore*.
5. S.S., & Gurusamy, M. (2022). "SDN-Enabled Hybrid DL-Driven Framework for the Detection of Emerging Cyber Threats in IoT." *MDPI Electronics*.
6. Aljughaiman, A. et al. (2022). "Cybersecurity Threats, Countermeasures and Mitigation Techniques on the IoT: Future Research Directions." *MDPI Electronics*.
7. Brajones, J.G. et al. (2023). "A comprehensive study of DDoS attacks over IoT network and their detection and mitigation using SDN." *Computers in Industry*.
8. "SDN-Based Prototype for Dynamic Detection and Mitigation of DoS attacks in IoT" (2022). *IEEE Xplore*.
9. "A Cognitive Digital Twin Architecture for Cybersecurity in IoT-Based Smart Homes" (2023). *Springer*.
10. Ferrag, M.A. et al. (2020). "Intrusion detection and mitigation in IoT using deep learning techniques." *Computer Networks*.
11. "Review of Botnet Attack Detection in SDN-Enabled IoT Using Dynamic Generative Self-Organizing Map" (2021). *MDPI Sensors*.
12. "Enhancing IoT network security through deep learning-powered Intrusion Detection Systems" (2022). *ScienceDirect*.
13. "Detection and Mitigation of IoT-Based Attacks Using SNMP and Moving Target Defense" (2021). *MDPI Sensors*.
14. "HybridRobustNet: enhancing detection of hybrid attacks in IoT networks" (2023). *Springer*.
15. "Cybersecurity for Industrial IoT: Threats, countermeasures and mitigation techniques" (2021). *ScienceDirect*.
16. "IoT Threat Detection Advances, Challenges and Future Directions" (2023). *IEEE Xplore*.
17. "Deep learning and hybrid models for IoT threat detection" (2023). *MDPI Electronics*.
18. "Protecting IoT devices using SDN-based dynamic threat detection and mitigation" (2022). *IEEE Communications Magazine*.
19. "A Survey on IoT Security using Machine Learning Approaches" (2020). *ACM Computing Surveys*.
20. "Detection of DDoS attacks in IoT using AI techniques" (2022). *IEEE Access*.
21. "A novel framework for dynamic detection and mitigation of cyber threats in IoT" (2023). *Elsevier Future Generation Computer Systems*.
22. "Cybersecurity in IoT: Detection and mitigation strategies using edge computing" (2022). *MDPI Sensors*.
23. "Securing IoT networks: A dynamic approach using blockchain and AI" (2021). *IEEE Internet of Things Journal*.
24. "Emerging trends in IoT security: Threat detection and mitigation" (2022). *Springer Nature*.
25. "A comprehensive review of IoT security frameworks for threat detection and mitigation" (2023). *Journal of Information Security and Applications*.