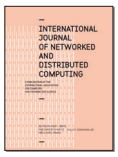
International Journal of Networked and Distributed Computing
Vol. **9**(**2-3**); April–July (2021), *pp.* 75–85
DOI: https://doi.org/10.2991/ijndc.k.210617.001; ISSN 2211-7938; eISSN 2211-7946
https://www.atlantis-press.com/journals/ijndc



Review

A Survey on Securing IoT Ecosystems and Adaptive Network Vision

Tejaswini Goli*, Yoohwan Kim

Department of Computer Science, University of Nevada, Las Vegas, Nevada 89154, USA

ARTICLE INFO

Article History

Received 15 December 2020
Accepted 08 June 2021

Keywords

IoT
security challenges
DDoS attacks
proximity-based authentication
adaptive networks
Machine Learning
IGMM
K-NN
SVM
Q-learning
Decision Trees
Honeypots

ABSTRACT

The rapid growth of Internet-of-Things (IoT) devices and the large network of interconnected devices pose new security challenges and privacy threats that would put those devices at high risk and cause harm to the affiliated users. This paper emphasizes such potential security challenges and proposes possible solutions in the field of IoT Security, mostly focusing on automated or adaptive networks. Considering the fact that IoT became widely adopted, the intricacies in the security field tend to grow expeditiously. Therefore, it is necessary for businesses to adopt new security protocols and to the notion of automated network security practices driven by analytic and intelligence, to ensure a prompt response to attacks there by protecting the privacy and data integrity of users. The main prospect of this paper is to highlight some extensive reviews on standardizing security solutions by means of adaptive networks, a programmable environment that is driven by analytical and intelligence which expands on the autonomous networking concepts and transforms static networks into a dynamic environment. Furthermore, this paper also inspects some of the Machine Learning techniques that can be used to enhance security and compares different techniques to find the best fit to IoT.

1. INTRODUCTION

Internet-of-Things (IoT) consists of physical devices embedded with sensors, computing power, and hardware connected to the internet that collects and shares data without human interaction. It is estimated that IoT would expand to more than 40–50 billion devices. All these devices are connected through internet with each other hence all these devices and the communication networks should be secured to safeguard user data. Although many vendors affirm that their technologies are secured and protected, yet devices are still vulnerable to various types of sophisticated attacks and threats because of resource constraints of the devices and the petty security standards that are normally more prone to attacks when compared to modern computer systems [1]. Additionally, extreme reliance on the blocking and prevention mechanisms with well-known security practices normally yield ineffective results since attacks are more dynamic in nature.

Additionally, Traditional security measures are no longer enough to secure IoT, especially IoT applications and devices cannot rely on blocking mechanisms or reacting to the incident after they have been attacked. Research of adaptive models in the IoT ecosystem will provide a good foundation for security techniques and application of best practices in variety of use cases. This could provide an environment to look for general and standardized security decisions that suit the high demand of dynamic IoT applications and smart devices. There were numerous research studies and research lately on adaptive security in the field of IoT [2–4]. We intend to achieve this goal by doing a comprehensive survey on available adaptive security measures in the IoT world, additionally we will try to explore the existing application or internet security domain and try to see if some of these security practices can fit into the IoT space.

The numerous existing researches, on network security mainly focus on different mechanisms which are blocking nature or reacting after it has happened and most of them have not particularly focused on adaptive and automated network. Enterprises need to build a comprehensive security model which is adaptive in nature that can adapt to moving perimeters and dynamics on a network. Adaptive security can mirror the environment, migrate, and evolve as things change. Adaptive network security is an implementation of security system that analyzes patterns and user activities [3], instead of focusing entirely on device logs. In contrast to traditional security models, this approach outlines some proposals to make the development ecosystems dynamic. It empowers the organizations to be apprehensive of newly materializing threats and apply required preventive counter measures. Coupling security automation with Machine Learning (ML), ensures a speedier response to attacks. The previous research primarily missing the network security concerns and the strategies to mitigate risks using adaptive network security practices which are critical for a user centric IoT-based service.

*Corresponding author. Email: golit1@unlv.nevada.edu

2. IoT SECURITY FRAMEWORK

Since network is now the focal point for IoT security, we will try to spotlight the network security in detail, and we believe understanding network vulnerabilities that exist in the current IoT world will help us to adapt today's constantly shifting ecosystems as well to its security challenges. Moreover, it helps in learning new strategies to mitigate or cease exploits from such vulnerabilities. This paper does a survey covering various security challenges, solutions and covering few design aspects of IoT security and recommendations.

2.1. Internet-of-Things Network Security Challenges

- ***Data security and privacy:*** Data privacy and security is the biggest issues in this interconnected world. Data is constantly shared, stored and used by large companies using various IoT devices. Cached data which is no longer needed must be wiped out securely.
- ***Small scale IoT attacks:*** Attackers trying to target with attacks that are small enough to allow the data leak rather than targeting huge volumes of information together since many organizations are engaged with necessary counter measures to avoid security attacks. Small scale attacks are the most often breaches and very difficult to detect and would pose challenges to enterprises. Printers and cameras are the most common enterprise technologies that hacker would target [5].
- ***Rise of botnets:*** The increasing Botnets is imposing a severe challenge in IoT industry and mitigating such threats would require a well-designed security strategy. Botnets by attacking connected devices and by infecting malware, Hackers then try to take control of the devices using a command-and-control authority [5].
- ***Insecure communication:*** Common attacks in this category include interception, modification, false data injection, DoS, and replay attacks [6]. Most of the devices communicate or share message through the network without encryption. So, there should be enough encryption among the cloud services and devices used by enterprises. There should be mutual authentication—where two entities communicating must prove their identity to each other. Here the some of the vulnerabilities in this category.

  i. **Unauthenticated communications:** IoT enterprise applications sends out security patches to mitigate threats when some of the devices get comprised without enough security policies, but this approach could fail since the update mechanism could be disengaged. Also, many IoT devices do not even use authentication to communicate or transmit data.

  ii. **Unencrypted communications:** Most of the existing IoT devices shares data in unencrypted format, instead of encrypted data. These transmissions of data can be interpreted by an attacker over the network. Encryption is the method of obfuscating or encoding data using cryptographic algorithms, that is encrypted data (referred to as cipher-text) [7].

  iii. **Lack of mutual authentication and authorization:** IoT devices that allows an unauthorized third party to alter its code or configuration, or grant access to its data, is a vulnerability [8]. It can reveal the owner's availability which makes it easier for installation or operation of malware, or it let the functionality of the IoT to be compromised.

- ***Lack of network isolation:*** Since IoT devices connect to the same network where a lot of other devices are connected and exchange data over the network it is easy for attacker to hijack all devices on the network when one device security is compromised.
- ***Lack of secure update mechanism:*** Most of the IoT devices lack the feature of Over the Air (OTA) firmware shown in Figure 1 which helps in sending major/minor upgrades to fix bugs and vulnerabilities and ensure reliability and scalability of the device. Without OTA automatic upgrades it is highly impossible to fix compromised devices. These upgrades can range from hardware to device operating systems updates.

2.2. Existing Countermeasures in IoT Security

There are several IoT security measures which are essentially determined by many factors and distributed across these four major stages: Predictive, Preventive, Detective and Retrospective. We will try to highlight and present some of the existing IoT security counter measures under different categories of Security levels, confidentiality, Availability, Authorization, and Integrity.

2.2.1. Confidentiality

Authentication of devices in IoT is often not given enough importance when compared to application or user authentication methods that are common today due to IoT device resource limitations, network transmission capacity, or the lack of user interface. Many IoT devices are equipped with inexpensive sensors and insufficient security protections and are generally more prone to attacks than personal computers or smart IoT systems shown in Figure 2. The first issue stemming from it is that these devices are less capable than the laptops and desktops which can be protected with access controls and have antivirus software installed. The second issue is that IoT devices are using new connectivity protocols like Wi-Fi, Bluetooth, Zigbee and others that are not secured by traditional security systems. The last issue is that most of these devices do not have a way to patch or update security issues they are discovered. These devices are designed to be running all the time and there is no user interaction or interface which essentially the main areas where there are high chances of compromising security and to enforce strong protection rules, we would need a strong device authentication mechanism.

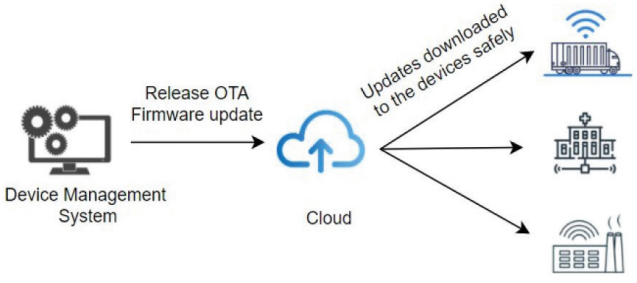


Figure 1 | Security patch upgrade using OTA through cloud.

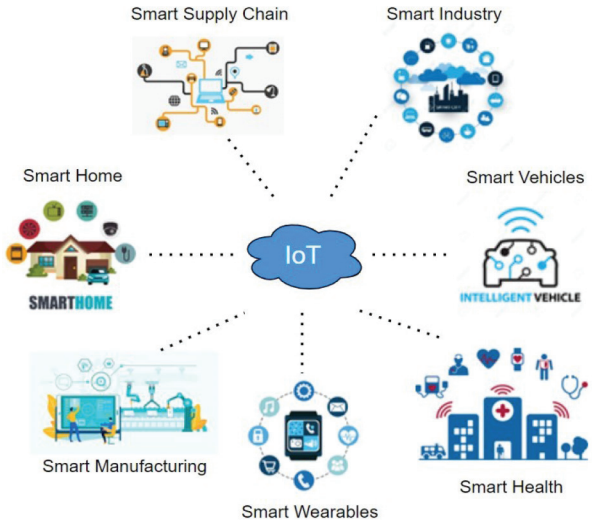


Figure 2 | IoT smart network.

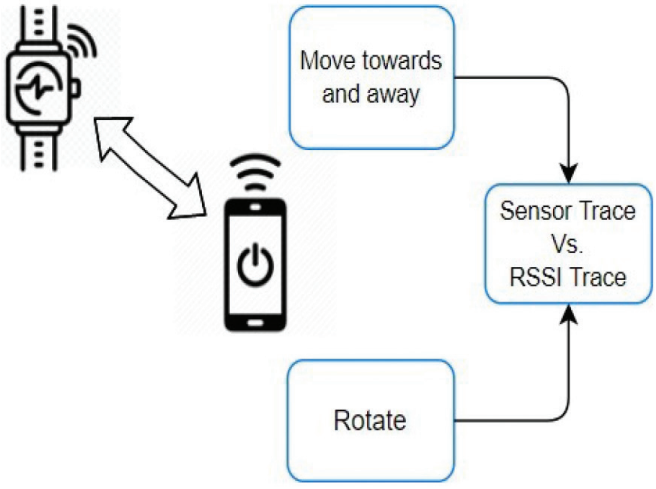


Figure 3 | Proximity-based authentication.

Let us take Smart home scenario as an example to illuminate authentication of IoT devices and potential faults. First and foremost, the step to enable any smart devices is to connect device to the internet by authenticating the device with home Wi-Fi (e.g., connecting smart switch to Wi-Fi router) as depicted in Zhang et al. [8]. While connecting, an attacker in the proximity can perform either a passive attack (by sniffing all message exchanged over the Wi-Fi), or by imitating the home automation device an attacker can connect to Wi-Fi router. Hence, sensitive information can be accessed such as Wi-Fi password or gaining access to network which allows the intruder to peek into the whole world of IoT network.

Several IoT device vendors take advantage of smartphones to input Pre-Shared Key (PSK) as a solution to authentication of IoT device problem. IoT devices collect PSK through smartphone and completes authentication with Wi-Fi router once after the connection between smartphone and IoT device is established. Hence, now the complication is shortened to IoT device and smartphone from IoT device and the Wi-Fi router authentication. And there were many cryptographic solutions proposed to pair smart phone and IoT devices securely but unfortunately, many traditional cryptographic techniques, such as the Diffie–Hellman protocol, by themselves are insufficient for securely pairing devices that spontaneously come into wireless contact.

The other problem as highlighted in Zhang et al. [8] is even if the home device had additional enough protection rules to secure the password using encryption, still it is not sufficient in protecting passwords. As home device is an embedded system, it is highly possible to read out the home device firmware and take binary analysis (by using firmware analysis tools) to retrieve the secrets. So, indeed the protection rules implemented by home device is not sufficient to fix the vulnerability. Also, an attacker can mimic the IoT device through transmitting same Service Set IDentifier (SSID) and Media Access Control (MAC) address.

As an alternative it was suggested to use a two-step authorization using biometrics verification in Farooq et al. [9], to ensure authentication which essentially is a preventive security measure but the drawback with this approach is mostly the IoT devices are heterogeneous and cannot support same level of communication required for authentication because of hardware constraints. For example, home devices such as smart switches and Router do not have the same set of authentication capabilities.

The shortcomings of IoT device hardware mentioned above can be conquered by using a proximity-based IoT device authentication called Move2Auth in Zhang et al. [8], in which the user operates few gestures in front of IoT device to authenticate securely while the IoT device is broadcasting radio signals as illustrated in Figure 3. Smartphone matches sensor trace with Received Signal Strength indicator (RSSI) trace to resolve if the device is within the proximity.

In the proximity-based authentication, there is no need of manual entry of passwords and this solution is not sensitive to eavesdropping attacks. Using Move2Auth [8], we combine large RSSI-variation detection, and a comparison between RSSI trace and smartphone's sensor trace, to execute reliable proximity detection, where RSSI variation detection can adequately mark off whether devices are with in proximity or far away, and the comparison between RSSI trace and smartphone's sensor trace can counterattack against potential intruder who can promptly tune transmission capacity. Aforementioned method is easier to use and strongly secured. The basic advantages of this technique are it does not require any added hardware on the devices besides the radio signals that is anyhow used for communication. The only drawback with this approach is the accuracy of proximity-based authentication to adapt to the advancing dynamic nature of malicious attack, which can be improvised by using an adaptive security model as mentioned in our Section 3.

2.2.2. Availability

Availability is among the most important security models that ensures the target IoT systems, devices and networks are working as expected and allow authorized users to access data at any time. Although the data is essential component of IoT, IoT devices and other services must be available too when needed in the IoT network. Distributed Denial-of-Service (DDoS) attack are the most common attack that targets Availability of service and network.

Let us investigate additional details of DDoS attacks and some of the existing countermeasures to it.

DDoS attacks: By definition, distributed DoS attack is outlined by a definitive effort to avoid the authentic users from consuming the services striking the target services with tremendous traffic. DDoS attacks are the leading threats in the modern internet and IoT era. And it is quite notable that in recent times, hacker's frequency using IoT devices as an army of bots to target network, services and even the internet by introducing DDoS attacks. The special example we always can refer to is the popular Mirai Bot Attack explained in Figure 4. By leveraging the shortcomings of IoT devices mentioned earlier, attackers were able to successfully compromise many IoT devices such as surveillance cameras or smart switches and used them to bombard the victims with DDoS traffic. This has been described and demonstrated very extremely well in Gallopeni et al. [5].

There are various types of DDoS attacks. Some of them are:

- **Syn flood attacks:** This is a DoS attack where an intruder swiftly opens a connection to the target server and will never send an Acknowledge (ACK) back to the target. The targeted server waits for the ACK response from the requester and go into waiting state that results in utilizing server resources as demonstrated in Figure 5. Such utilization of resources will result in making the target system to be unresponsive to verified and authenticate users or traffic.

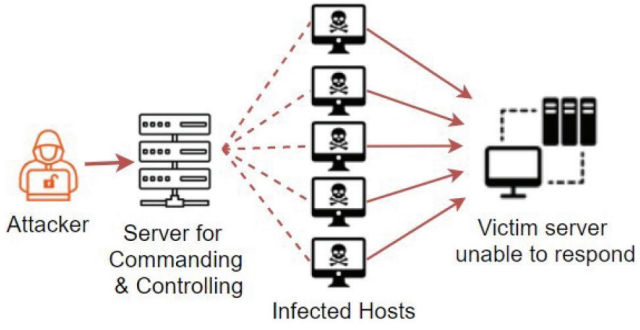


Figure 4 | Mirai Bot attack 2016.

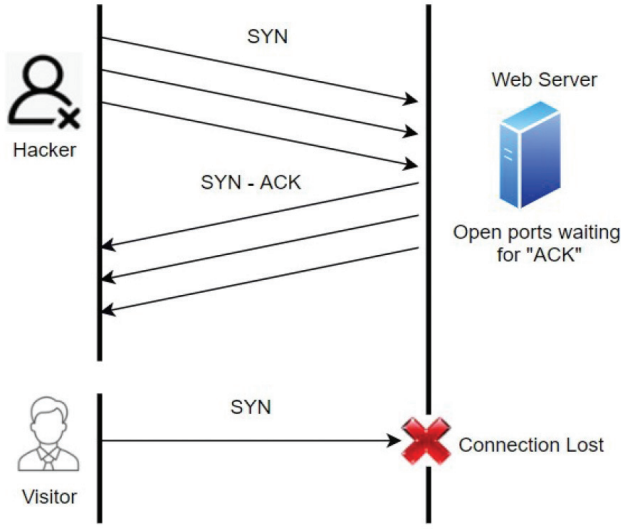


Figure 5 | SYN flood attack.

- **Ping flood attacks:** This is a DDoS attack where attacker send a constant sequence of Internet Control Message Protocol (ICMP) echo ping requests to a target server's network and the target server becomes busy in responding to such requests with ICMP Echo Reply packets.

  Target server's network becomes very busy processing them and the legitimate users cannot connect to the target server. In a way attacker achieves what he wants by introducing delays into the network as shown in Figure 6.

- **UDP flood attacks:** DDoS attack when the intruder sends enormous number of UDP packet messages to target server to make the target server busy until it reaches the server's request threshold and ultimately push the target server to go into a busy state and rejects all the legal traffic. As demonstrated in Figure 7 legitimate users or requests perceive this as server timeout or service is unavailable.

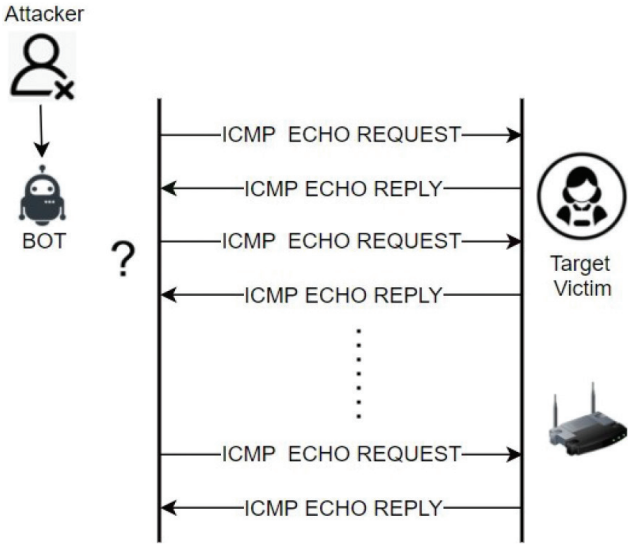


Figure 6 | Ping flood attack.

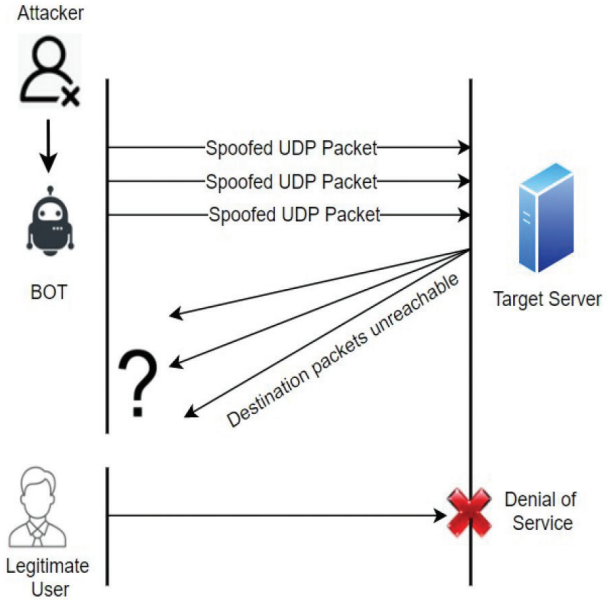


Figure 7 | UDP flood attack.

Syn Flood Attacks are the most common DDoS attack among all. Figure 8 shows the pictorial representation of various DDoS attacks depicted in pie chart using the 2018–2020 statistics [6]:

Intrusion Detection System (IDS): IDSes can identify the attack traffic and help in decreasing the attack surface. It analyzed the network traffic to identify and detect any suspicious behavior and takes necessary actions to contain the attack. Generally, there are two known types of IDS as described in Shurman et al. [10]:

- **Anomaly based:** In Anomaly IDS method, the technique followed to detect attacks is by comparing the past traffic pattern and its behavior with the current normal traffic and this type is commonly used mechanism to detect new type attacks. However, it is known to be a mechanism that creates a lot of false positive alarms.
- **Misuse based or Signature based:** This type uses a signature-based comparison to detect anomalies in the traffic and yields no false positive alarms, but new attacks are unidentified since signature of that pattern does not exist in the signature repository. Widely used to detect known attack with precision but would not work for detecting new attacks.

Some of the examples of Anomaly-based IDS model is using the parameters such as login location, login times and activities of the user to find anomalies in the network traffic by comparing it with the previous patterns. These can be automated by using network monitoring tools but collecting new data and feeding to the IDS model is a big challenge as there are so many attacks that happens every minute and due such huge data it is not easy for the monitoring tools to find the anomaly spontaneously. Since these models are static in nature, Section 3 proposes some of the Machine Learning techniques in association with adaptive security methods in improving the IDS countermeasure accuracy rate and identifying any intrusions and making it almost dynamic.

2.2.3. Integrity

Let us look at some of the traditional cryptographic methods such as Data Encryption Standard (DES), Advanced Encryption Standard (AES), Triple DES (TDES) and (Rivest–Shamir–Adleman) is an asymmetric cryptographic algorithm (RSA) as a countermeasure to ensure Data security and integrity during the transfer of data through communication channel. First and foremost, all these models would require reasonable memory and CPU processing power. It was found in recent times that DES is vulnerable to attacks and experts have found various flaws in the cipher design. It is well known AES is the much-used scheme and most efficient scheme that uses a symmetric cipher as suggested by authors in Farooq et al. [3] and Farooq and Faisal Aslam [7]. AES method is also adapted and recognized by US federal government. AES Cryptographic scheme is very easy to implement and uses symmetric, round-based algorithm with various sizes of key. Standard AES implementation would require more hardware resources and again that could very well be a drawback for some of the IoT devices with resource limitations. There are various new schemes introduced recently especially for securing IoT communication channels such as eXtended TEA (XTEA), SPEK and Location-Exposure Algorithm (LEA). This is certainly a debatable topic and various research has been done [11,12] to compare and find the most suitable cryptographic schema for IoT devices. So, for simplicity let us assume here that the IoT devices nowadays comes with efficient and large resources and we are considering AES method here as AES proven to be most efficient cryptographic scheme per [12]. Even though AES cryptographic scheme is a suitable candidate it is still not dynamic in nature that it is not suitable for the dynamic nature of attacks. An Adoptive model of AES scheme is shown in Section 3.

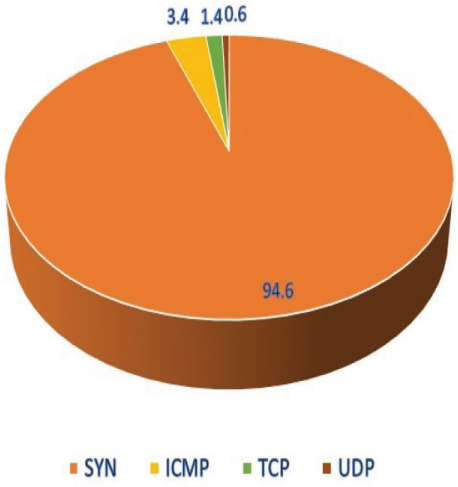


Figure 8 | 2018–2020 statistics depicting various DDoS attacks.

2.3. Threat Model

Sun Microsoft [13] lists the following as the objectives of Adaptive Security Architecture. Our threat model approach follows these objectives:

- Reduce threat amplification: Restricts the potential spread of a pandemic in a monoculture.
- Shrink the attack surface: Make the target of an attack smaller.
- Decrease attack velocity: Slow the rate of attack.
- Reduce remediation time: Respond to an attack quickly.
- Facilitate the availability of data and processing resources: Prevent or contain attacks that try to limit resources.
- Promote correctness of data and the reliability of processing resources: Respond to attacks intended to compromise data or system integrity.

Threat model here is represented in three-dimensional notion as shown below in Figure 9 and revolves around three basic security services i.e., Confidentiality, Integrity, Availability (CIA). One of the dimensions represents Assets such as hardware, firmware, operating system, and application software that talks about various asset categories in which the attack can happen. The other dimension denotes breadth of the attack which are IoT device ecosystem, network, and cloud network.

Confidentiality denotes that only the authorized person can view the sensitive information, integrity guarantees accuracy and completeness of the data during storage or during data transmission, and availability denotes that the data is available always for the customers and businesses who would need it. If hackers find ways to compromise these three parameters, they can steal the data and

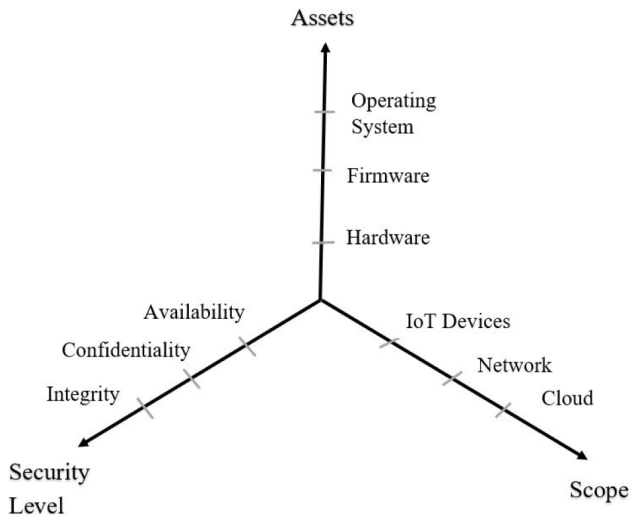


Figure 9 | Proposed IoT threat model, with threats along three dimensions: Assets, Security Level, and Scope.

could put it to wrong usage. This will in the end damage users' trust and could remarkably impact business operations.

3. ADAPTIVE NETWORK SECURITY

In this fast-growing IoT environment especially, devices and device network are constantly being exposed to security threats. Traditional security measures no longer applicable or sufficient for IoT security practices, especially IoT devices cannot rely on blocking mechanisms or reacting to the incident after they have been attacked which cause loss in revenue. To counter these cyber threats, we need advanced security platforms that has capability to adapt to the changing environment of dynamic threats and implement adaptive response mechanisms. If a security model is implemented with pre-established security measures, then it is referred to as a static security method whereas if a security model that can watch, identity, rectify and revise a security risk steadily and provide revised fixes dynamically or mitigate the attack then the mechanism is considered dynamic which is mostly achieved through adaptive security mechanisms. Also, we have seen some of the existing countermeasures in Section 2.2 and has few drawbacks such as not static nature of the security measure in the current IoT.

Adaptive network security is the concept to deliver continuous monitoring and scrutinize the network for anomalies, and vulnerabilities during the data transmission by automating various strategies and best practices. Whenever a threat is detected, the system enforces appropriate counter measures that block the attack.

Like any other security framework Adaptive security is classified into four major stages:

- **Predictive:** This stage produces alerts about external events also forecasts new attacks by monitoring activities of the attacker. Additionally, it contributes data that can be leveraged further to enhance the detective and preventative layers, consequently creating an entire loop for an adaptive security.

  i. One of the traditional approaches is simulating various attacks using some of the tests such as penetration tests that facilities with knowledge on the target's network security and its efficiency rate by mimicking an attack.

  ii. Artificial Intelligence (AI) driven networks that can learn the intent of network behaviors, deliver predictive analysis, and provide recommendations to the problems or threats so detective and preventive layers can enhance security measures.

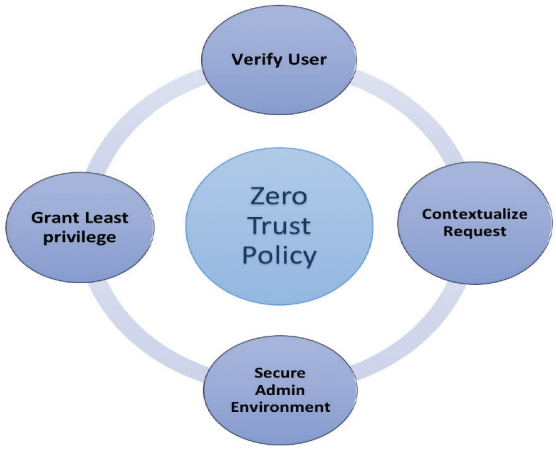


Figure 10 | Zero trust security model.

- **Preventive:** Helps to create products, processes, and policies that can counter-attack any cyber-attack. This approach sometimes would mean if there were suspicious behavior detected even though there is no real threat, still the security policies enforce remediation steps such as re-login or to reauthenticate. One of the security models which serves as a full preventive strategy is "zero trust security model" as shown in Figure 10, in which all devices need to be authenticated and authorized whenever they access applications or data.

Businesses would need more resilient and reliable security strategies to avoid malicious activity or unauthorized access. Building inspection points into popular junctions to spot in network attackers as they navigate your systems. Creating security rules and policies to identify and deny traffic that moves through the inspection points.

Zero trust security model in Figure 10 means that none on the network can be trusted and required to go through identity verification that claim access to resources. Also, with on the assumption that all user behavior cannot guarantee their security, we should identify the devices, users, and environment during data use. With zero trust, least-privilege is not only applied to who is accessing the data, but also what—which services, devices, or connections—where, and when, which greatly reduces attack surfaces, giving defenders a narrower scope of focus.

- **Detective:** This stage identifies various attacks which are not seized by the preventative layer. Detective phase of Adaptive security helps in reducing the time to detect a threat and thereby limiting possible risks from becoming actual risks.

- **Retrospective:** Last stage in the adaptive security model depicts more in detail, contemplate the threats that were not identified in earlier stages. During retrospective analysis, further incidents or attacks can be countered using the forensic or post incident data.

It has been a challenge for the network engineers in the IoT world to identify and trouble shoot issues manually as there are so many security threats or issues a NetOps engineer to investigate manually. From the Cisco survey report [6] in Figure 11 it was found that about 33% of the times a NetOps engineer need to spend time on identifying and troubleshooting network issues, 30% in detecting vulnerabilities and threats to take remediation steps and rectify such issues, and 37% in analyzing and exploring advancements in automation.

3.1. Machine Learning in the Adaptive Security

In the hybrid and dynamic network of IoT, it has been a challenge to choose policies and protocols to setup a trade-off in the process securing IoT devices. IoT devices need to adopt and identify key parameters in the security protocols in the dynamic networks world where ML could be beneficial. Machine Learning is data-driven learning approaches helps in decisions making with no pre-programmed systems. Security processes are automated by using ML training data sets, therefore making the security monitoring with no human intervention.

The first step to adopt Machine Learning is to audit everything over the network. This auditing logs should be made available for the ML systems to parse and train to detect any vulnerabilities and suspicious activity. By using Machine Learning, security systems can analyze suspicious behavioral patterns by accessing massive databases and detect new threats. Machine Learning analyzes old data and then comes out with the optimal counter measures for both the present and the future (sometimes). It relieves Network operators from manually analyzing thousands of log files. By using old data, it tracks and identifies user activity patterns and additional entities such as applications, devices, and networks. System thereby compares user and entity activities and identify irregular or inconsistency patterns. For instance, enterprises can see if users executing activities that they do not generally do. Alert triggers raised to inform enterprises or the legit users about the Suspicious behavior or unusual activities. Various Machine Learning techniques are elaborated and discussed in Section 3.2.

Sometimes over reliance on the old data produces very high false alarms or will rationally results in not sufficiently detecting potential threats. Since new type of attacks and techniques are involved and the type of attacks evolve over the time, it is very much necessary to transition from static and one time created data sets toward more dynamically generated data sets that are modifiable, reproducible, and extensible. So, we have inspected a mechanism in our Section 3.3 in which honeypots are used to log and collect latest network data for the ML systems to consume and train from.

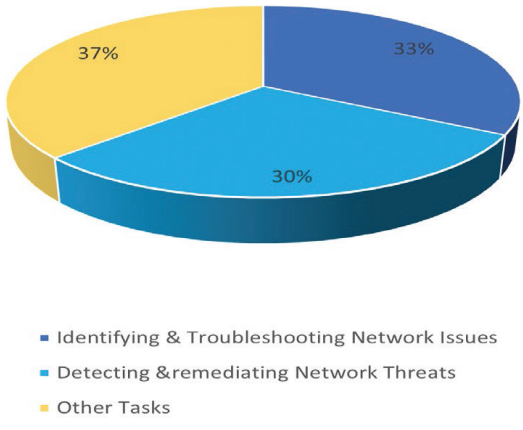


Figure 11 | Cisco network security report.

3.2. Approaches to Adaptive Network Security

We have seen some of the existing countermeasures in our earlier sections (Section 2.2) and highlighted few limitations for example we have seen why most of the traditional countermeasures are static in nature and why not all of them can best fit in the current IoT context. In adaptive network security we will see how to leverage some of the ML techniques to collect information on the latest attacks and make decisions to counterattack. For details of the attack taxonomy, we refer the readers to Hossain et al. [14] that describes various potential attacks in IoT. Here we will try to inspect some of the countermeasures grouped by security services (CIA triad) using adaptive security and Machine Learning.

3.2.1. Confidentiality and authentication

In Section 2.2 we identified proximity-based authentication approach is the best solution with a limitation of not able to adapt to the changing dynamic nature of malicious attacks. Using Machine Learning data, we can implement adaptive framework to detect unusual activity based on the previous login times, location and other activities taken place and block the authentication. Various learning-based authentication techniques are applicable to IoT devices however since Unsupervised learning techniques like IGMM and Q-Learning techniques [15] are ideal to be used for proximity-based authentication without compromising the location information of the devices as shown in Xiao et al. [16] we will try to inspect them.

- **Infinite Gaussian Mixture Model (IGMM):** IGMM technique is a non-parametric Bayesian method used mostly in the proximity test and the IGMM takes multiple radio sources into account and provides flexible proximity range control [17]. To identify spoofers outside the proximity range, the Model proximity will be adjusted to compute RSSI trace and ambient signal's packet arrival time intervals [16,17]. In IGMM model, the proximity-based authentication and session key establishment are implemented based on location tags. So basic idea in this model is to make it difficult for the attacker to construct the location tags if the signals are sent from multiple radio sources. Also, each radio client will create a public location tag using the MAC addresses of the packets, RSSI, and sequence numbers. Additionally, all the clients keep a secret location tag that consists of packet arrival time details to generate the session keys. Accuracy of authentication will be improved with the use of IGMM technique. In comparison with the Euclidean distance-based authentication which is mostly used to detect the spoofing attacks [16,18] IGMM technique used in proximity authentication scheme trim down the

error rate to 5% by 20%. This technique is strong enough, and the spoofers/Eavesdroppers cannot really intrude outside the proximity range easily.

In IGMM the ML system would need below data points for training exercise that can be collected during the authentication process:

(i) IP addresses and MAC addresses.

(ii) IoT User Agent header

(iii) Known or unknown device (from the cookie out of earlier authentication activity.

(iv) Authentication time.

(v) Previous authentication time.

(vi) Time since the previous authentication.

(vii) Whether from a trusted network or untrusted network.

- **Q-Learning-based authentication:** Q-learning is a re-enforcement learning technique [15] model and has been commonly used in improving authentication efficiency [18,19] which will help in building the IDS model. The value function V exploits each state quality and, in the Q-function assigns a value to every action has taken by agent at all different states. For this reason, Q is often referred as action value function. Where Q-learning works from the experience replay what it gathers after some time of execution. The efficiency of Q-learning technique in the authentication technique entirely depends on the training data and also depends on the RSSI traces of the radio signals and empowers devices to enhance authentication accuracy and efficiency. For instance, from Xiao et al. [19], the Q-learning-based authentication trims down the error rate of average authentication by 64.3% to <5%.

There are other methods such as deep neural network and 'Distributed Frank-Wolfe' [20] methods to increase the accuracy of the authentication, but we propose IGMM, or Q-learning-based authentication since both suits the approach of proximity-based authentication [17] and yields better accuracy results.

3.2.2. Availability

We have seen in Section 3.2 that DDoS attacks are the most common ones that targets availability service and we have also seen the drawbacks of existing IDS mechanisms (anomaly and signature-based IDS systems). Anomaly-based IDS models create false positive alarms and whereas signature-based IDS model does not guarantee detection of new attacks (only to detect known attacks. So, in our adaptive security approach we will try to inspect some of the models using Machine Learning models or any other models, one example could be Hybrid IDS model to overcome the limitations of individual IDS types.

- **Hybrid IDS using known-attack signature database (KAS-DB):** The hybrid approach proposed in Shurman et al. [10] is an integration of both anomaly- and signature-based IDS models to overcome the drawbacks in each of the IDS model that we discussed earlier. In this model all the patterns will be tracked and stored in KAS-DB, so even if an attacker IP (new IP address) without being detected using the IDS model the signature of the packet gets compared with the signatures in the KAS-DB and if found (known attack), blocks the packet and the signature gets stored in KAS-DB if not the behavior pattern of the attack gets monitored using the anomaly-based IDS to see whether there are any unusual patterns in the packets or not and the signature gets updated in KAS-DB and Log DB if a new attack is found so all the data will be used for future attacks. Even though this approach will reduce false positives drastically and helps in identifying new attacks with precision, the proposal did not outline how well it can perform in IoT ecosystem per [10]. Since multiple layers of IDS detection models are used in here most likely the performance of the IDS model will impact and this may ultimately impact the packet transfer rate.

- **Anomaly Detection-IoT (AD-IoT) system using Random Forest Machine Learning Algorithm:** AD-IoT proposed in Alrashdi et al. [21] by authors is an intelligent anomaly IDS method based on Random Forest Machine Learning technique to identify threads and decrease false positives. Random Forest is a predictive modelling data analysis approach which is also mainly used for data exploration, where it generates several trees by recursive partitioning method and then it aggregates its results. This is more advanced IDS system than the traditional IDS models or the signature-based IDS systems which does not best fit to detect unknown attacks. Although this model performs better than all other machine techniques used such as "Decision Tree, *k*-Nearest Neighbor" but the only drawback could be the intrusion detection has to be detected in fog nodes instead of cloud layers, this may help in some of the IoT systems where fog nodes are deployed but since the fog node is still emerging and has a long way to go, this model is not preferred.

- **Support Vector Machines (SVM):** SVM is a supervised learning ML method used for classification of data and is used to detect DDoS attacks with associated learning algorithms [22]. SVM has been extensively used to detect invasions as a classical pattern recognition tool where the principle of DoS attack generally utilizes the lack of effective authentication mechanism for management frames and control frames and the defects of Carrier-sense multiple access with collision avoidance (CSMA/CA) mechanism. SVM gets trained with both normal and intrusive data both [23]. SVM identifies a support vector and allows maximum space called hyperplane. An attacker can send a normal connection request through many forged illegal management frames and control frames, which will significantly increase the probability of the attack node accessing the wireless attack communication channel, thereby making the wireless access point unable to provide normal service or access due to access overload. The purpose of continuously occupying the communication channel for a long time affects the normal communication between other legitimate clients and the wireless access point.

  Using SVM algorithm, a new model is built which elects new candidates in at least one category, by constructing a non-probabilistic binary linear classifier. This model exhibits some examples both mapped and just as points in space, so that the samples in the other categories are split by a transparent gap as large as possible [23]. This method then try to map more samples into that same space and try to predict which category it fits into by matching the side of the gap they fall. SVM model adopts the principle of structural risk minimization, which establish good rationalization ability and promotes prediction accuracy. Even though SVM yields good classification accuracy results it suffers from memory and performance [24].

- ***k*-Nearest neighbors (*k*-NN) IDS method:** *k*-NN's method is another alternative to SVM to identify DDoS attacks. *k*-NN model is a type of supervised ML technique and used for both classification as well as regression problems like SVM. In IDS the *k*-NN is used to classify intrusion data. A class is classified through the vote of its neighbors so that a class is promoted as mostly widely used class within *k*-NN. Once the classification is done the *k*-NN value is derived. Several research were conducted on *k*-NN model [23,25] and proven to be efficient mechanism than "Naive Bayesian" and SVM. The accuracy of *k*-NN model count on the quality of training data, moreover the storage and computing costs are very high when the volume of data is huge since *k*-NN must compute Euclidean distance [26].
- **Decision tree IDS method:** Decision tree is the non-parametric supervised learning algorithm used in both classification and regression tasks [27]. Decision tree IDS method is a general, predictive model and a greedy approach that uses divide and conquer method. It follows a top-down approach starting from root node and traverse through all non-leaf nodes by primarily choosing an attribute to test the sample data. While traversing through all non-leaf nodes the training sample gets divided furthermore into sub-samples where each sub sample have a new leaf node [28]. The same process is repeated until a specific condition is met. Choosing test attribute and a strategy on how to divide samples are very crucial in the process of creating a decision tree. Generally, users not required to know a lot of details about the learning process in Decision tree. C4.5 algorithm [29] is the most regularly used decision trees. In decision tree IDS model, first decision tree is constructed from the training data and then classification rules are extracted as by traversing through all the paths from root to leaf in which each branch denotes a test output so, the decision tree can be converted into IF ELSE a conditional rule. These classification rules are used in the IDS model to determine network behavior. Experiment in Wang et al. [28] shows decision tree IDS model yields better accuracy. In some other experiments [24] it was proven that the accuracy rate of decision tree is 98.11 using various feature selection techniques.

From the experiments [26] it was proven the accuracy rate of decision tree to be 99.95% using the NSL-KDD dataset when Random Forest method is applied to find the best features. In further experiments [30] when multiple decision trees also referred as "hybrid decision tree" model is used, the accuracy and precision rate is improved drastically since hybrid decision tree is a combination of three decision trees used for classification. That is, the first decision tree observes the entire dataset of the training phase and constructs its model [30]. Then, the tree is evaluated with the same training set. Subsequently, those samples that the first tree failed to classify correctly are more likely to be selected to enter the second tree. Those [28] appeared to be more difficult in the first and second classifiers were more likely to enter the third tree.

3.2.3. Integrity

We have seen in our Section 2.2 the proposed solutions [12] do not acknowledge the heterogenous type of IoT devices and proposes single AES implementation. That kind of approach is not suitable to all IoT devices owing to the varied limitations of resources on the device and the static nature of the model. So, now we try to inspect the model proposed in Farooq et al. [3], another model in Farooq and Faisal Aslam [7] which is an adaptive approach that considers five different implementations of AES schemes. Farooq et al. [3] proposed a solution to find the suitable scheme for the IoT device based on the device resource and throughput needs. An optimization function designates a value for each one of the available AES schemes results in a resource to throughput weighted distribution. Graph theory approach adapted in Farooq et al. [3] to find the correct match of AES scheme using the weighted bipartite graph which is a graph whose vertices can be divided into two separate disjoint sets, i.e., A, B and all the edges connect vertices between A and B sets. All the edges in a Bipartite graph points in one direction that is A $\rightarrow$ B.

From the research [3] it was proven that this approach yields better throughout results and more dynamic in nature. So, as mentioned in the adaptive approach a specific scheme of AES is chosen from various AES schemes [7] based on the IoT device hardware or resource by using Hungarian algorithm [31]. It was proven that this technique will help in minimizing the IoT device resource usage and proven to be dynamic in nature [3]. Results from both the Hungarian algorithm and the earlier discussed random and greedy approaches were compared and the results depicts this proposed framework yields 11% and 17% enhanced average throughput, 3% and 13% enhanced resource usage results when compared to the random and greedy approaches [3].

3.3. Use of Honeypots in IoT to Collect Train Data for Machine Learning Systems

All in all, each Supervised and unsupervised learning typically fails to spot the attacks because of the insufficient training data, and not enough class features. And at the same time there is a need of monitoring attacks at real time and learn about new attacks and malware. Therefore, always there is a need of designing backup security solutions and integrate with ML schemes to provide stable and secure IoT services. Here honeypots can play an important role, honeypots as its name suggests, used for luring in attackers with an intention to observe and analyze their method of launching an attack by capturing information about the attacking agent like malware for a DDoS attack [32]. It is a device capable of getting compromised on the behalf of the main server by simulating any vulnerability which can easily be exploitable by an attacker. Either they can be used for carrying out any research to get knowledge of possible threats and shortcomings in the system called as Research Honeypots [32,33], or they can be used for protecting the company's assets from the attacks in real time to improve the overall security called as Production Honeypots. Honeypots are quite effective in dealing with Zero-Day DDoS attacks without compromising IoT devices.

The collected information in the form of log file in Figure 12 can be used as input to the Machine Learning model which will solve the problem of insufficient training data and such data sets collected at runtime is used as input to various ML models to advance more in network security. Most of the data sets collected using honeypots, are preferable to unsupervised learning algorithms as there is no human intervention in the process because an expert is needed to form the rules and assign the labels accordingly for supervised learning algorithms.

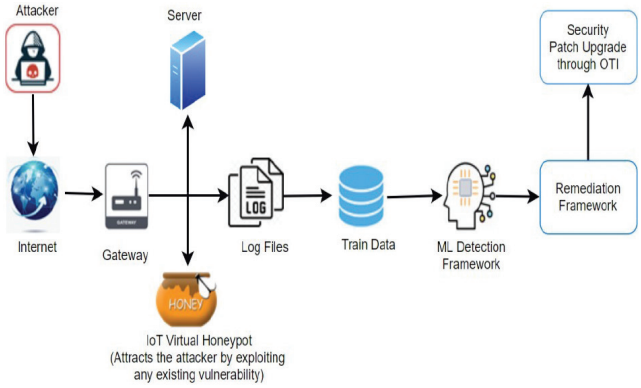


Figure 12 | Honeypot design used in conjunction with ML framework and remediation framework.

3.4. Benefits and Drawbacks of Adaptive Network Security using Machine Learning

3.4.1. Benefits

- Adaptive security or network vision leverages old and real time network data to apply advanced analytical and machine learning processes which can detect security breaches to larger extent.
- Helps in mitigating the attack and reducing the area of attack by providing dynamic resolutions.
- Security threats are detected nearly at real time and dealt with efficiently by automated processes.

3.4.2. Drawbacks

- Even though the existing training datasets would help in analyzing security threats and detecting vulnerabilities, it requires more accurate and latest data sets to be used by ML systems since ML systems lacks improvement even with experience and creativity. This can be mitigated by using honeypots described in Section 3.3.
- If Malicious insiders can exploit and manipulate the existing old training data used in the machine learning techniques, then it would be challenging for adoptive network systems to detect or trace the data manipulation changes.

3.5. Examples

- Let us take the example of high-profile Mirai botnet attack Figure 4 in 2016 [11], during which the malware involved would continuously scan the internet for the IP address of IoT devices, such as security cameras and digital video recorders, and then "enslave" them for use in a widespread DoS attacks on various web sites. If we apply adaptive network security measures in such scenario the predictive stage would keep a track of network traffic and can help detect the issue in first place using the detective stage. Once the issue is identified an automated process will kick in to block those IP addresses as a defensive mechanism. Shape security tool is a good example as a defensive mechanism tool for Bot attacks.
- Another example where we can apply Adaptive security strategies in IoT is if a IoT device is compromised and security patch upgrade is restricted by stopping the IoT devices. An Automated signal will be sent to the device to reboot and apply an essential security patch. Even some Automated diagnosis scripts can be written to diagnose the device health which can also detect a hung, wedged device and instantly cycle power to the unit.
- Automate the process of detecting common WAN problem or any outage's and provide instant diagnosis with the supporting data or configuration updates to speed recovery and facilitate carrier resolution.

4. CONCLUSION

Many enterprises are becoming dynamic in the IoT ecosystem, so do the potential risks. We started with investigating various security challenges in the IoT ecosystem, and the current available solutions furthermore examined why the post-incident approaches and the static security methods in the traditional security architecture do not withstand the dynamically changing threats. We then examined how to counterattack these cyber threats by materializing adaptive responsive mechanisms or adaptive security framework, where systems can continue to evolve and ensure to have required policies, processes and procedures primed to defend IoT devices and networks from the threat landscape. We have surveyed that by using some of the Machine learning models such as IGMM and Q-learning models we can ensure confidentiality of the IoT devices and networks that also produce better results in blocking any eavesdropping attacks. In another survey of IDS model using *k*-NN's or Hybrid Decision Trees the accuracy of intrusion detection and the performance is proven to be improved that helps immensely in implemented adaptive network security. The other survey is on how to ensure integrity of data over communication channel while exchanging data between devices in IoT networks using AES algorithm and the adaptive model of Advanced AES which finds the suitable AES schema dynamically based on the IoT resource type. Also, we believe the proposed honeypot model will help in improving the accuracy of training data and help in collecting newer attack patterns at near real times which will help greatly the ML techniques in the adaptive security approach.

CONFLICTS OF INTEREST

The authors declare they have no conflicts of interest.

REFERENCES

[1] N.M. Karie, N.M. Sahri, P. Haskell-Dowland, IoT threat detection advances, challenges and future directions, 2020 Workshop on Emerging Technologies for Security in IoT (ETSecIoT), IEEE, Sydney, NSW, Australia, 2020, pp. 22–29.
[2] M. Hamdi, H. Abie, Game-based adaptive security in the internet of things for ehealth, 2014 IEEE International Conference on

Communications (ICC), IEEE, Sydney, NSW, Australia, 2014, pp. 920–925.
[3] U. Farooq, N. Ul Hasan, I. Baig, N. Shehzad, Efficient adaptive framework for securing the Internet of Things devices, J. Wireless Com. Network. 2019 (2019), 210.
[4] E.K. Wang, T.Y. Wu, C.M. Chen, Y. Ye, Z. Zhang, F. Zou, MDPAS: Markov decision process based adaptive security for sensors in internet of things, in: H. Sun, C.Y. Yang, C.W. Lin, J.S. Pan, V. Snasel, A. Abraham (Eds.), Genetic and Evolutionary Computing, Springer, Cham, 2011, pp. 389–397.
[5] G. Gallopeni, B. Rodrigues, M. Franco, B. Stiller, A practical analysis on Mirai Botnet traffic, 2020 IFIP Networking Conference (Networking), IEEE, Paris, France, 2020, pp. 667–668.
[6] S. Cook, DDoS attack statistics and facts for 2018-2021, Available from: https://www.comparitech.com/blog/information-security/ddos-statistics-facts/.
[7] U. Farooq, M. Faisal Aslam, Comparative analysis of different AES implementation techniques for efficient resource usage and better performance of an FPGA, J. King Saud Univ. Comput. Inf. Sci. 29 (2017), 295–302.
[8] J. Zhang, Z. Wang, Z. Yang, Q. Zhang, Proximity based IoT device authentication, IEEE INFOCOM 2017 - IEEE Conference on Computer Communications, IEEE, Atlanta, GA, USA, 2017, pp. 1–9.
[9] M.U. Farooq, M. Waseem, A. Khairi, S. Mazhar, A critical analysis on the security concerns of internet of things (IoT), Int. J. Comput. Appl. 111 (2015), 1–6.
[10] M.M. Shurman, R.M. Khrais, A.A. Yateem, IoT denial-of-service attack detection and prevention using hybrid IDS, 2019 International Arab Conference on Information Technology (ACIT), IEEE, Al Ain, United Arab Emirates, 2019, pp. 252–254.
[11] I. Makarenko, S. Semushin, S. Suhai, S.M. Ahsan Kazmi, A. Oracevic, R. Hussain, A comparative analysis of cryptographic algorithms in the internet of things, 2020 International Scientific and Technical Conference Modern Computer Network Technologies (MoNeTeC), IEEE, Moscow, Russia, 2020, pp. 1–8.
[12] D.A.F. Saraiva, V.R.Q. Leithardt, D. de Paula, A.S. Mendes, G.V. González, P. Crocker, PRISEC: comparison of symmetric key algorithms for IoT devices. Sensors (Basel) 19 (2019), 4312.
[13] R. Nataraj, Adaptive security architecture, Available from: https://medium.com/@rk-root/adaptive-security-architecture-4c152a0164a.
[14] M.M. Hossain, M. Fotouhi, R. Hasan, Towards an analysis of security issues, challenges, and open problems in the internet of things, 2015 IEEE World Congress on Services, IEEE, New York, NY, USA, 2015, pp. 21–28.
[15] D. Pandey, P. Pandey, Approximate Q-learning: an introduction, 2010 Second International Conference on Machine Learning and Computing, IEEE, Bangalore, India, 2010, pp. 317–320.
[16] L. Xiao, Q. Yan, W. Lou, G. Chen, Y. Thomas Hou, Proximity-based security techniques for mobile users in wireless networks, IEEE Trans. Inform. Forensics Security 8 (2013), 2089–2100.
[17] P.M. Varela, J. Hong, T. Ohtsuki, X. Qin, IGMM-based co-localization of mobile users with ambient radio signals, IEEE Internet Things J. 4 (2017), 308–319.
[18] L. Xiao, X. Wan, X. Lu, Y. Zhang, D. Wu, IoT security techniques based on machine learning: how do IoT devices use AI to enhance security?, IEEE Signal Process. Mag. 35 (2018), 41–49.
[19] L. Xiao, Y. Li, G. Han, G. Liu, W. Zhuang, PHY-layer spoofing detection with reinforcement learning in wireless networks, IEEE Trans. Veh. Technol. 65 (2016), 10037–10047.
[20] L. Xiao, X. Wan, Z. Han, PHY-layer authentication with multiple landmarks with reduced overhead, IEEE Trans. Wirel. Commun. 17 (2018), 1676–1687.
[21] I. Alrashdi, A. Alqazzaz, E. Aloufi, R. Alharthi, M. Zohdy, H. Ming, AD-IoT: anomaly detection of IoT cyberattacks in smart city using machine learning, 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), IEEE, Las Vegas, NV, USA, 2019, pp. 305–310,
[22] V. Justin, N. Marathe, N. Dongre, Hybrid IDS using SVM classifier for detecting DoS attack in MANET application, 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), IEEE, Palladam, India, 2017, pp. 775–778.
[23] R. Ravinder Reddy, B. Kavya, Y. Ramadevi, A survey on SVM classifiers for intrusion detection, Int. J. Comput. Appl. 98 (2014), 38–44.
[24] P. Illavarason, B. Kamachi Sundaram, A study of intrusion detection system using machine learning classification algorithm based on different feature selection approach, 2019 Third International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), IEEE, Palladam, India, 2019, pp. 295–299.
[25] K. Rani, H. Roopa, V. Vani, Prediction of network intrusion using an efficient feature selection method, 2019 International Conference on Intelligent Computing and Control Systems (ICCS), IEEE, Madurai, India, 2019, pp. 597–601.
[26] W. Zhou, Y. Cao, H. Qi, J. Wang, An effective network intrusion detection framework based on learning to hash, 2019 IEEE International Conference on Smart Internet of Things (SmartIoT), IEEE, Tianjin, China, 2019, pp. 489–493.
[27] I. Ramadhan, P. Sukarno, M.A. Nugroho, Comparative analysis of K-nearest neighbor and decision tree in detecting distributed denial of service, 2020 8th International Conference on Information and Communication Technology (ICoICT), IEEE, Yogyakarta, Indonesia, 2020, pp. 1–4.
[28] J. Wang, Q. Yang, D. Ren, An intrusion detection algorithm based on decision tree technology, 2009 Asia-Pacific Conference on Information Processing, IEEE, Shenzhen, China, 2009, pp. 333–335.
[29] S.L. Salzberg, C4.5: programs for machine learning by J. Ross Quinlan. Morgan Kaufmann Publishers, Inc., 1993, Mach. Learn. 16 (1994), 235–240.
[30] S.M. Taghavinejad, M. Taghavinejad, L. Shahmiri, M. Zavvar, M.H. Zavvar, Intrusion detection in IoT-based smart grid using hybrid decision tree, 2020 6th International Conference on Web Research (ICWR), IEEE, Tehran, Iran, 2020, pp. 152–156.
[31] G.A. Mills-Tettey, A. Stentz, M.B. Dias, The dynamic Hungarian algorithm for the assignment problem with changing costs, Technical Report, Robotics Institute, Carnegie Mellon University, Pittsburgh, PA, 2007.
[32] C. Musca, E. Mirica, R. Deaconescu, Detecting and analyzing zero-day attacks using honeypots, 2013 19th International Conference on Control Systems and Computer Science, IEEE, Bucharest, Romania, 2013, pp. 543–548.
[33] R. Vishwakarma, A.K. Jain, A honeypot with machine learning based detection framework for defending IoT based Botnet DDoS attacks, 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), IEEE, Tirunelveli, India, 2019, pp. 1019–1024.