

Received January 22, 2021, accepted February 1, 2021, date of publication February 8, 2021, date of current version March 1, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3057655

Web of Things: Security Challenges and Mechanisms

RUHMA SARDAR  AND **TAYYABA ANEES** 

School of Systems and Technology, University of Management and Technology, Lahore 54770, Pakistan

Corresponding author: Tayyaba Anees (tayyaba.anees@umt.edu.pk)

ABSTRACT Web of things (WoT) is an improved and most promising infrastructure of the internet of things (IoT) which permits the smart things to not only integrate to the internet but also to the web. It allows the users to share and create content as well as provide capabilities for data aggregation and analysis through a network to become part of the World Wide Web (W3). Despite these advances, it has shown several security challenges that need to be addressed for the successful deployment of WoT on a commercially variable and large scale. In this paper, authors have analyzed the most noticeable security challenges related to WoT such as unauthorized access, eavesdropping, denial of service attack, tempering, and impersonating, through an analysis of already published empirical studies. Further, we have discussed some of the available mechanisms to overcome security related issues while taking into account the network size and mobility. Authors have used Threat analysis and attack modeling methods to inform the users about defensive measures and to prevent security threats from taking advantage of system flaws. Authors have provided the necessary insight into how security can be improved by using certain existing mechanisms and algorithms. The findings of the study revealed that security mechanisms to secure WoT are still immature and future research is required to resolve these challenges.

INDEX TERMS Web of things, Internet of Things, security challenges, security mechanisms, World Wide Web, security analysis, attack modeling.


I. INTRODUCTION

In this modern era, the internet is connecting more and more things to the global network and in this network, the web provides a universal platform for sharing resources, archiving and publishing services, etc. In WoT “things” refers to the physical or abstract objects and “web” refers to these objects that are accessible via web services, such as HTTP and API’s scripting can be used at protocol and service layers respectively for embedding complex and smart real-life realities with it [1].

WoT is expected to make accessibility of smart things easy and promote by combining novel values of web resources to physical world entities (sensors, appliances, and smart objects). It offers us the exciting capabilities to change the world and add quality to our lives just as the web is doing for the past 20 years. The relationship between WoT and IoT is just the same as the relationship between the web and the internet. WoT is supported by IoT at the network layer which is meant to provide any device like phones, laptops,

routers, computers, and many more with an IP address. Meanwhile, WoT signifies IoT at the application layer with the purpose to provide an electronic device like QR, Bluetooth, beacons, etc. with URL. Web of things can be defined as maximizing the present and evolving techniques by using web tools and provide the improvement of IoT scenarios to simplify the creation of IoT applications. By abstracting all the complexity and several transport protocols behind in the IoT, WoT provides the benefit to the developer to only focus on their applications without worrying about how devices and protocols work.

The OSI (open systems interconnection) has a seven-layered architecture to establish many standards and protocols for the internet. Similarly, WoT architecture has four layers namely; the Accessibility layer, Sharing layer, Composition layer and Findability layer, to organize the cluster of web tools and protocols into a valuable framework to connect anything or objects to the web. The main purpose of designing WoT’s architecture is to expedite the incorporation of smart objects with the available services on the web and to assist the implementation of web applications by using smart objects/things. The presented layers of the WoT

The associate editor coordinating the review of this manuscript and approving it for publication was Qing Yang .

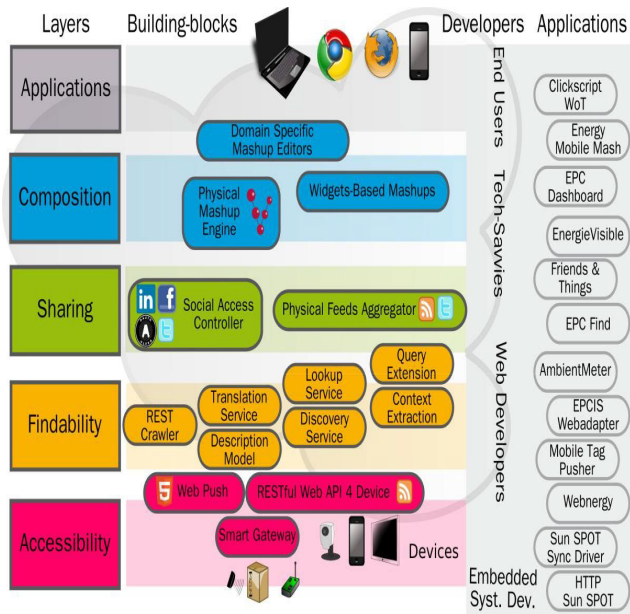


FIGURE 1. Architecture layers of the web of things [3].

architecture are not fully strictly designed and are not particularly hidden from the previous layers as shown in Figure 1 [3]. Instead, architecture should be seen as a multi-service network which step by step, simplifies the implementation of applications using smart objects. WoT design provides services that address each layer needed to look smart as high-end web citizens. However, applications can be assembled on the top of the respective layer offered by the implementation of the service or more of their combination depending on the specific application use-case. But, integrating applications by using smart features in their intuitive OS (operating system), libraries and protocols still need certain skills as well.

The objective of all WoT-building platforms is the basis for bringing this development closer for the hobbyist and web developers with technical expertise and thereafter brings the development and implementation of IoT applications closer to end-users by enabling them to create simple applications tailored to their needs.

Several new web/internet-based technologies like semantic web, service-oriented web, cloud computing, IoT and WoT make the cyber world not only a hot topic for researchers but also a global network of partnerships and collaborative places where many organizations, communities and organizations are established. The cyber-world to the social world is expanding constantly. The pioneering idea of connecting real-world things to the World Wide Web started around 2000. But in 2002, the authors proposed the cool town project by linking physical entities with web pages to get information and connected services [2].

Both IoT and WoT perceptions envision a world where communication can be made anywhere and anytime but these perceptions cannot be organized in the real world without facing critical aspects such as trust, security, and privacy. Smart things are almost covering all aspects of our daily life.

The number of devices connected to the WoT is increasing exponentially. In 2015, 15.41 billion devices were connected to the web and in 2025 it is expected that 75.44 billion devices will be connected to WoT [4] as illustrated in Figure 2.

Unfortunately handling security and privacy in these connected devices is extremely challenging because of four aspects. The first aspect is the heterogeneous nature of the IoT because it consists of an unlimited number of various devices with different protocols, interfaces, and requirements. The second aspect is insufficient resources as IoT objects have limited available resources. The third aspect is authentication and identification. Usually, ID's were linked to individuals to check whether they can perform a certain action or not [5]. In the digital and physical world objects are capable of behaving both by themselves or someone else. There is a need to handle identity management problems and find a solution securely to handle the identity of objects and the authorization process. Till now many researchers have put their efforts to investigate identify management threats but still, a shared definition of an object's identity is missing [6]. The fourth aspect is privacy as WoT is considered as a most interconnected system where information is coming from different sensors installed in different places like schools, universities, hospitals, homes, and parks, etc. also, information flows from device to device to the web. Such information can affect an individual's life and can pose critical privacy hazards. These aforementioned challenges motivated us to investigate the security challenges as it is one of the major problems to handle and previous studies on the WoT are few and still not very mature.

In this paper, the authors have investigated the trade of security threats to improve the security of WoT because current web authentication schemes like OAuth, JWT are inadequate for WoT applications as these schemes cannot provide protected ownership transfer of online personal data.

The rest of the paper is structured as follows: Section 2 presents the research contributions of this study. Section 3 presents the literature review. Section 4 describes an overview of the integration of smart things with the web. Section 5 describes the research methodology of our study. Section 6 presents the discussion and in the last section 7, discussed the conclusion and future work.

II. RESEARCH CONTRIBUTIONS

The main contribution of this work is threefold: (a) Authors have identified the main issues of the WoT in terms of security; (b) Authors have used threats analysis and attack modelling methods to inform the users about defensive measures and to prevent security threats from taking advantage of system flaws (c) Further, Authors provided the necessary insight into how security can be improved by using certain mechanisms and algorithms.

III. LITERATURE REVIEW

IoT is a term used for building a connection between different objects, systems, things, people, or applications and

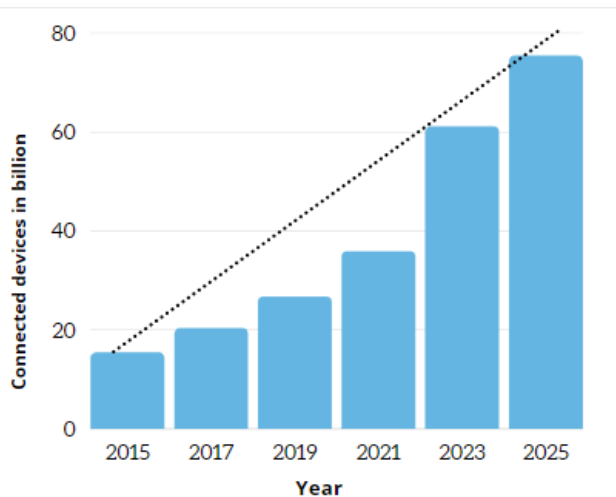


FIGURE 2. Connected in billion from the year 2015 to 2025.

controlling them from a web browser or mobile application. But, creating a single communication platform that tries to communicate with multiple subjects is challenging. The Semantic Web of Things is a current domain of exploration for integrating semantic web-based technologies with the IoT. It can also be considered as a change of the Web of Things (WoT) by including semantics. The SWoT targets the ability to exchange and use information between data and ontology. However, WoT allows control and access over IoT applications and resources by using conventional web technologies such as JavaScript, PHP, or HTML 5.0. In WoT, any device can be accessed by using web standard protocols. All these three technologies also include some security and privacy issues because, a large number of interconnected devices produce scalability, heterogeneity, and multiple interoperability issues. In this section, the authors have reviewed already published studies with the perspective of identifying security challenges in the WoT, SWoT, and IoT.

WoT lets users interconnect and share information. The social web of things are also an emerging concept of WoT. Privacy threats related to social WoT are discussed in every layer of architecture such as management, discovery, synchronization, privacy, walled-off internet and understanding of WoT and IoT further authors also suggested solutions for overcoming them [7].

The integration of WoT with wireless sensor networks provides the capabilities to connect real-life physical objects with a unified system. While integrating, serious issues raised over the access of individual information related to smart things and individual privacy [8]. The authors proposed that it is possible to strengthen the security of the environment by applying security instruments such as authentication protocols, built resilient and well-tested code, manipulating encryption technology, and by doing security level checks upon APIs.

Web traffic logs, in the WOT environment, provide valuable information about how people interact with smart objects

through web servers. These web access logs play a significant role in building security management for applications. For this purpose, the authors introduced an algorithm named request dependency graph to investigate the behavior of clients by graphing the relation between HTTP requests to access web requests [9]. The authors performed experiments on a dataset collected from real-world cellular IoT networks and the achieved results show a higher accuracy rate which indicates that a dependency graph is a suitable tool for mining web usage.

Fast production of IoT technologies might become the cause of weak IoT networks extremely pruned to privacy and security threats [10]. The authors identified some security vulnerabilities by building three different IoT use-cases in case of personal information leakage, sensitive user information leakage, and unauthorized execution of functions by using cheap and commercially available standard products and services. Results of the use cases showed that IoT privacy and security protocols are always not well defined by manufacturers and consumers that leads to inadvertent tracking of user behavior and identity if devices are not built with privacy and data is not classified as sensitive.

The evolution of WoT is combined with semantic web technologies to make a vulnerable semantic web of things and highlights gaps in the domain such as technical interoperability, syntactical interoperability, and semantic interoperability [11]. Also, the authors discussed important security issues like confidentiality, integrity, trustworthiness, authentication, availability, and authorization of WoT with IoT constraints.

Problems including legal issues, privacy, and security to provide identity among existing off the shelf technologies are provided in [5]. Also, the researchers presented a briefcase study namely InterDataNet, which is a framework for WoT and is implemented in the smart cities of Spain, Santander to apply security solutions to the real use case to evaluate their strengths and weaknesses.

In the IoT environment privacy, security, and trust issues for both information and devices are proposed in [12]. Furthermore, concise security issues related to IoT are reviewed in [13] by analyzing security properties and requirements for four architectural layers namely the network layer, support layer, perceptual layer, and application layer.

The authors in [14] discussed security issues for three layers of IoT architecture namely application, perception, and transportation layer and for securing IoT, they presented various IoT security threats such as confidentiality, availability, integrity, authentication, and non-repudiation as well as discussed possible solutions to tackle these threats for IoT's successful utilization on a commercially large scale.

Some key challenges of IoT like authentication, authorization, confidentiality, and integrity have been discussed in [12]. Basic security principles and resource constraints for authentication in IoT have been proposed in [15]. This study concluded that non-repudiation and responsibility are feasible for IoT's cyber-crime environment in applications such as forensics, cyber-crime investigations, and many



FIGURE 3. Overview of WoT [18].

others. Depth analysis of features of IoT such as autonomy, pervasiveness, and ubiquity has been discussed in [16]. Also, security issues were analyzed for every architectural layer of IoT with a special focus applied to the requirements for the availability of data, confidentiality, and integrity.

We have also conducted a primary study on the web of things findability taxonomy and challenges in [17]. However, this paper is considerably different from our previous study [17] in the following aspects: (1) Authors in [17] focused on finding the dynamic searching problem of the WoT while we are concerned about finding the security challenges in the domain of the WoT; (2) we are identifying the existing security mechanisms to establish secure WoT while authors in [17] investigated the current trends and research gaps of the WoT; (3) The focus of the authors in [17] is on the find layer while in this paper, we focused on the share layer as it is responsible for the sharing of data in a secure way.

IV. INTEGRATING SMART THINGS TO THE WEB

There are two options for connecting smart devices to the web; indirect integration and direct integration as demonstrated in Figure 3 [18].

As shown in Figure 3, home appliances can be viewed as direct integration and RFID can be viewed as indirect integration with an RFID reader and an embedded server. In general, the system can not only rely on one method but can use both integration methods as a hybrid.

A. DIRECT INTEGRATION

To integrate things with the web, it is first required that all objects are addressable such as every object must have one IP address when linked with the web.

In the application layer, WoT also requires communication and collaboration. The web server must be embedded in such a way that businesses can communicate and interact with the web language defined by web protocols. Most devices will be IP enabled and can be integrated with web services through the development of computer technology and communication technology. Therefore, these devices can communicate directly with other devices from any terminal with web

browsers. Standard web functionality such as POST and GET can also interact with other devices.

Several pioneer solutions have been developed to directly connect smart objects to the web. IP-enabled sun SPOT with a web server is presented in [19]. Where each system in their prototype proposed its functionality over the web. In another proposed architecture, all small programming objects are integrated into the web, where the sensor details and applications of the sun SPOT are consistently displayed by web services [20].

A prototype used for programmable low-power Wi-Fi components to attach things to the web directly has been proposed in [21]. That prototype controls the interoperability of HTTP protocol and IEEE 802.11 access points.

B. INDIRECT INTEGRATION

All devices cannot be powerful enough to be integrated with web servers directly due to limited resources, such as RFID tags. Also, sometimes there is a need for smart devices to integrate directly with the web because of the power, security, and cost. In both cases, an indirect combination can be employed.

In this configuration, a middle proxy is located between the web and smart objects. This proxy is called a smart gateway. Smart things integrate with the smart gateway. Therefore, they shall understand the exclusive protocols of smart objects.

Several solutions to indirectly integrate smart objects with the web have been proposed already. To enable efficient query and to manage the sensor network, the HTTP 1.1 protocol is used for embedding sensor gateway. Smart sensor gateways for smart network management and sensing data aggregation is designed by [22]. In that paper authors also developed a Java applet to exchange data in a well-defined manner. Another implementation for smart gateways to web base integration and management of embedded devices has been proposed in [23]. The proposed gateway enables the sensor network to be accessed by a lightweight web service interface.

V. RESEARCH METHODOLOGY

The main objective of this paper is to investigate the security challenges faced by the WoT which have become threats not only to human lives but also have damaged the properties. The methodology starts with reviewing the present time applications of WoT and then empirically review the security challenges faced by the WoT. After that performed a threat analysis and attack modelling technique on a few of the identified security threats to discover the system vulnerabilities. Furthermore, provide some of the already proposed security mechanisms to improve these security challenges. In the end, we have provided a discussion section to discuss the findings of this study. Figure 4 demonstrates the research methodology of this paper.

A. APPLICATIONS

In present times, the WoT is applied in many real-life applications. Experts are constantly making good use of these

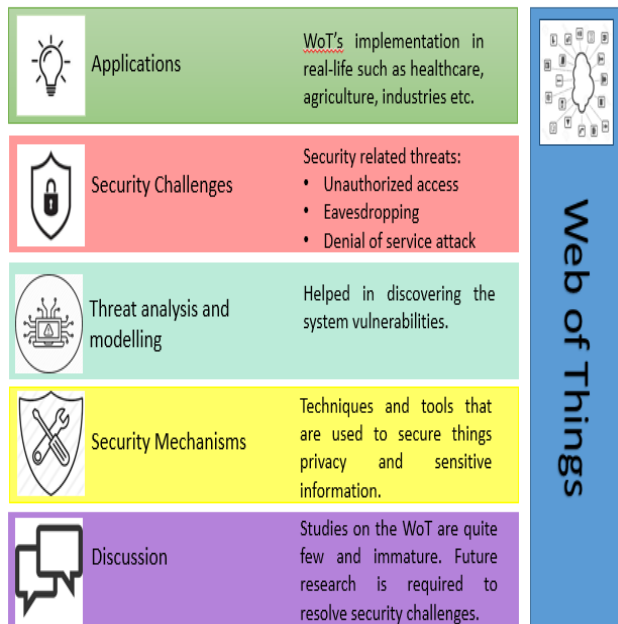


FIGURE 4. Research methodology.

technologies to cater to the need of the community. Various applications of the WoT are creating wonders for this real-world. Some of the researchers have used WoT and IoT in specific areas and different application domains to improve the daily lives of users [17], [24], [25]. In this section, after reviewing the WoT applications concisely, the authors listed the benefits and challenges of using WoT applications in Table 1.

Combining IoT with WoT could provide various benefits in the arena of IT (Information Technology). Authors in [26], used the combination of IoT and WoT in robotics and encountered various real-life examples such as sports, health, entertainment, culture, military, domestic supports and surveillance, etc. by using bibliographic research to examine the behavior of WoT. The general observation is that various major fields of the WoT/IoT in robotics are not being touched by the researchers yet.

The authors in [2], proposed a WoT case study in agriculture. In which they developed an ontology enabled architecture by using a range of fixed environment sensors and separate livestock monitoring techniques to increase the performance of land. The authors in [27], proposed a WoT architecture for connecting vehicles by interoperating ITS-G5 for data exchange between vehicles, processing, and storage units.

WoT facilitated devices that have improved flexibility and reliability in infrastructure operations by using associated sensors, meters to analyze data and lights to get the advantages of cost and manpower reduction and to enhance the safety of the cities [28], [29]. Before WoT, handling garbage was a big issue. Now garbage containers can be monitored to improve the waste management and trash collection route [30].

The development of the Internet of Medical Things has presented epic healthcare benefits such as management of disease, remotely monitoring the condition of the patient, treatment techniques and reducing the cost and errors. This change has greatly influenced the lives of patients and healthcare workers equally [31]. Also, some smart devices and sensors can be used to regularly monitor the temperature, heartbeat, and other health conditions of the patients.

It is also helpful in homes where the consumer appliances can be controlled remotely such as reducing water and electricity bills by monitoring meters of energy and water.

Rapid growth in the development of WoT devices worldwide has changed the day-to-day lives of consumers. However, some of the security, privacy, general and legal issues have also come to light due to some reasons. One of them is that the wide variety of the products and dealers are available in the market and the information about the security and privacy of WoT devices is not enthusiastically available to the user who want to consider it before buying. The Authors in [32], explored the security and privacy labels based on the series of surveys, interviews, users and with the help of 22 privacy and security experts and proposed a prototype for privacy and security labels to help buyers to make the right decision before purchasing items.

Another reason is, smart devices are transmitting a massive amount of data wirelessly to the cloud due to which WoT is facing more security challenges than ever before. There are many traditional security measure techniques to protect WoT but these existing techniques are not sufficient enough to tackle the different attack types and their severity. The authors in [33], [34], used Machine and Deep Learning (DL) procedures such as deep belief neural network, supervised and unsupervised learning techniques to enhance the security mechanisms in IoT, even in uncertain circumstances.

B. SECURITY CHALLENGES IN WOT

Sharing and openness are always conflicting when it comes to privacy, trust, and security. These are the main challenges in WoT that need extraordinary attention and needs to be further investigated. To understand them, let's take an example of something accessible on the web. Here privacy issue is related to the sharing of this item only to the authorized persons to access it. The security issue involves, who will have access to the object and what he can do with it. In the last, trust handle issue related to communication of different WoT entities on the web. On the web, things are shared and accessed among many users which makes it essential for the researcher to make WoT successful and well-known. Unfortunately, until now researchers dealt mostly with IoT issues [36]. Consequently, WoT security challenges are yet to be explored. In this section, identified the most challenging security threats and provide their summary in Table 2.

1) UNAUTHORIZED ACCESS

While access to a variety of WoT networks can be found on many end-user devices such as tablets or smartphones but

TABLE 1. Web of things real-life examples.

Application area	Features	Benefits	Challenges
Smart infrastructure	Use data to manage traffic. Keeps citizen safe and clean. Used to control pollution.	Improves flexibility and reliability [28]. Manpower reduction [29]. Environment improvement by reducing noise and pollution [39]	Fast and ultra-efficient risk decision devices. Lack of suitable tools to handle largely generated data [40]. Software complexity.
Smart education	Connect students from all over the world. Provide a safe and secure environment for students for learning. Transform learners to creators [63].	Energy efficiency improvement [39]. Cost-effective. Improves management and administration [41].	Security and privacy. Security. Better management. Minimization of cost [41].
Agriculture	Monitoring soil condition and moisture level. Optimized Watering plans. Fertilizing land.	Maximize yield production while using fewer resources [42]. Cost-effective. Delivers high-quality crop production [42]. Better monitoring of climate conditions for increased crop production.	Continuous availability of the internet. Adopting the use of technology is more challenging for urban. Lack of technical knowledge among farmers [43].
Healthcare	Use of smart biomedical devices. Continuous monitoring of patients [44]. Personalized medications [44]. Vehicle to vehicle communication. Safety of the driver.	Disease prevention and risk monitoring [44]. Cost-saving. All around the technological enhancement. Early detection and prevention of illness.	Personal sensitive data security. Difficulties with regular update [44]. Handling of huge data generated. Scalability. Data interpretation.
Connected cars	Internet connectivity in cars [45]. Google to earth navigation system [45].	Provide safety. Traffic management. Sustainability.	Costly [45]. Security. Lack of infrastructure.
Environment monitoring	Monitoring air pollution [46]. Ozone level. Monitoring humidity, temperate, and fine dust particles.	Early detection of tsunami and earthquakes. Monitoring air and water conditions.	Energy efficiency [46].
Industries	Predictive maintenance [44]. Maintenance scheduling [44]. Energy competence.	Cost-efficient. Optimization of manufacturing load [47].	Fault tolerance [44]. Distributed computation.

these devices can be caught stealing or being stolen and the use of these devices by illegal users leads to unauthorized access to the WoT network. It usually happened when somebody tries to gain access to a program, server, website, service, server other systems by pretending someone else with the use of other's accounts or other methods. For instance, if someone continued to keep guessing the password or username that did not belong to them until they did so, this was done deliberately as unauthorized access. It can also happen when a user tries to access an application area where it should not be found.

To prevent unauthorized access, when attempting to access the unauthorized area, access should be denied and an unauthorized access message should be displayed [51]. Unauthorized access is divided into five common types namely; tailgating, door pooping levering doors, keys, and access cards [52].

Tailgating is the most common type of unauthorized access, which occurs when one or more unauthorized persons follow an authorized user over the gate. One way to prevent queuing is to provide training to all users to ensure awareness and safety. Similarly, propping doors is another common way for unauthorized users to gain access to the site and inadvertently create a dangerous situation for people and resources within. It is surprisingly easy to open the levered door by using something as small as screwdrivers or as large as a crowbar. Keys also pose a major problem if stolen, lost, or loaned out. It is often impossible to track lost keys. Like keys, access cards have also the potential to be lost or stolen by an unauthorized person [45].

In June 2006, PayPal was attacked by unauthorized users which affects the web application security by creating a cross-site scripting flaw. It happened when attackers redirected the PayPal visitors to the page warning that their accounts

had been compromised. And send application users to the phishing site that asked for their PIN, social security number, credit card number, and other personal data and let hackers execute malicious scripts in the browsers. This attack affected over 200 million users [15].

2) EAVESDROPPING

An eavesdropping attack is also known as a snooping and sniffing attack. It spreads when someone tries to steal the information that smartphones, tablets, computers, or other devices transmit over the network. A snooping attack takes the benefit of unsecured network communications to access the being received and sent through the web. This type of attack is difficult to detect because it does not cause any transmission to appear to be behaving aberrantly.

Some researchers proposed a model to prevent eavesdropping attacks [46], [47]. In IoT, any device having computing and sensorial can communicate with each other. Among all obtainable technologies, fifth-generation systems are the main dynamic force for the actualization of the IoT concept due to its heterogeneous and broadcast environment of radio propagation. In this network securing security assurance is a challenging task. To overcome this problem one way is to expose communication to eavesdroppers with unknown locations and numbers. An analytical method was proposed to examine eavesdropping in a wireless network of things which were considered with the randomness of channels with effects of path loss, shadowing, and Rayleigh fading effect [46]. Researchers also used transmission protocol multi-hop communications which are designed to randomize and forward relay strategy [47].

A most typical example of eavesdropping in a warehouse can be shown in Figure 5, in which each product is attached with an RFID tag, which can interact with RFID readers. In this system communication is taking place between RFID tags and readers can be easily wiretapped because of its complexity to apply anti-eavesdropping countermeasures.

3) DENIAL OF SERVICE ATTACK

A denial of service (DoS) attack occurs when an authorized user could not access devices, network resources, or other information systems resources due to the malicious actions of cyber threat actors. It may affect many services like online accounts, email, websites, or other services that depend on the affected network. DoS situation is accomplished by overflowing the targeted network with traffic until the target is crashed to block access to authorized users [39]. This attack can affect an organization with both cost and money while its services and resources are not reachable.

4) TEMPERING ATTACK

The WoT Tempering attack relies on the management of barriers between the server and the client to amend application data, such as product permissions, quality and user credentials. Typically, this information is stored in cookies,

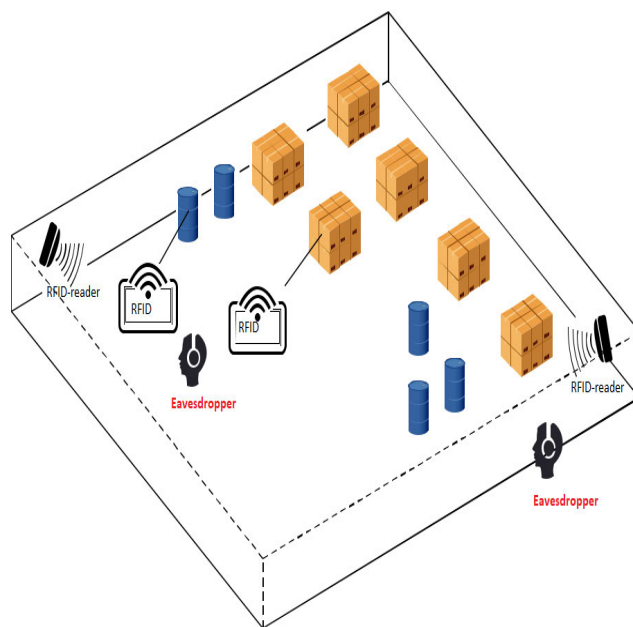


FIGURE 5. Eavesdropping attack in the WNoT [53].

which are hidden from URL query strings which are used to increase the control and functionality of the application.

A tempering attack can be obtained by an attacker who wants to harm a third party using a man in a middle attack or can be a malicious/medium person who wants to modify the application for his benefit. In both cases, some tools are used to prevent tampering attacks like Web Scarab and the Paros Proxy. The success of a tempering attack depends on the integrity and logic verification mechanism error.

5) IMPERSONATING

Among all types of attacks, impersonating is an interesting evolving category. These attacks are an adversary and can successfully assume the identity of the legitimate user also they can obtain his/her secreted information in a communication protocol. Impersonating is used for sharing sensitive information such as intellectual property, financial data, payroll information, or revealing login credentials that attackers can use to hack into a company's computer network. Some examples are CEO fraud and business email compromise.

C. SECURITY THREAT ANALYSIS AND ATTACK MODELLING

Threat analysis is a legal process of identifying, documenting and minimizing the system security threats and threat modeling is a technique of accessing and documenting the security risks related to the application which also includes understanding the enemy's intentions in attacking an interest-based system. This allows to compute threats and also helps in discovering the system's vulnerabilities. A threatening model is very useful if done in the initial stage of the system deployment and then, when the system is changed and requirements

TABLE 2. Summary of Security threats related to IoT and WoT.

Threats	Property Violated	Internet of Things	Web of Things
Unauthorized access	Authorization	Unauthorized access is an application layer security threat. Where an application may have various users and have different access rights. Appropriate authentication and access control mechanisms are still required at the application layer [48].	Unauthorized users in WoT can gain access to a service, program, server, or website through someone else account by changing the state of the different authentication and authority methods and they can forward it to the anticipated devices. E.g. in smart homes, the privacy of the user might be compromised by unlocking certain rooms in the home.
Eavesdropping	Authentication	Eavesdropping is a network layer security threat. Where someone tries to steal the information that smartphones, tablets, computers, or other devices transmit over the internet. Every type of attack starts with information sniffing by using some tools like sniffer packets [48].	This is a man-in-the-middle type of attack where privacy might compromise when traffic is flowing between the different objects. Through this, an attacker can gain access to the victim's credentials by accessing login information, password and credit card number.
DoS attack	Availability	Dos is also a network layer security threat A service in which works become unavailable usually because of the infrastructure that cannot cope due to the overload of traffic. This attack is more dangerous than others because it is implemented successfully on smart cars, which can cause the loss of life [48]. Solutions for mitigation and DoS detection are still ineffective and need attention.	DoS is the most common and easiest attack to implement on the devices. They can be intended in various ways that could reduce the speed and capacity of the system to perform expected results. In wireless system examples of the DoS are flood, collision and jamming signals. In February 2000 yahoo, amazon, CNN and some other websites were the victims of such an attack [50].
Tempering attacks	Integrity	The tempering attack is not in the domain of IoT.	Modifying something in the data, disk, memory, or elsewhere without the consumer's authorization.
Impersonating things	Confidentiality	Not in the domain of IoT.	Impersonating happens when an attacker act as someone else. It can disclose personal information or can send malicious code.

are better defined, the list of the threats and vulnerabilities can be updated according to the need of software.

In this section, the authors described some of the security threats analysis and attack's modelling. Modelling of the attack is shown via sequence diagrams and mitigation measures. The purpose of threat modelling is to provide a good understanding of the vulnerabilities posed by the system and helps in taking safety measures in case of a system attack.

1) DENIAL OF SERVICE ATTACK

Dos is an attack on the cloud service. An attacker deploys Dos by flooding the target system with unwanted network traffic until the system is either broken or useless. The attacker aims to prevent legal users from accessing the services and information. Cloud services flouting the updated data by user and hiding the lost information can also be considered as a Dos attack.

a: THREATS LEADING TO DENIAL OF SERVICE

These are some of the common reasons for DoS attacks:

Robbery by using the threat of a DoS attack: The attacker may aim to directly benefit from his perceived ability to disturb the object's services by demanding payment to avoid the attack.

Cybercrime and Turf wars: Teams and individuals engaged in internet-based risk activities can use DoS as weapons

against infrastructure and operations against each other, holding appropriate business on fire.

Competitive business practices: Cybercriminals sometimes offer DoS services to take competing websites and otherwise interfere with their operations.

Punishment for unwanted actions: DoS attacks may be intended to punish the victim by denying the need for robbery or causing disruption to the attacker's business model (e.g., spam shipping operations).

Expressing anger and criticism: Attackers can use DoS attacks as a way to criticize a company or government organization for displaying unpopular political or national, economic, or financial behavior.

Training ground for other attacks: Attackers may sometimes point to an organization where they are better prepared for DoS tools and future attack skills, which will be targeted at other victims.

Interruption from other malicious actions: Enemies may launch DoS attacks just to keep an eye on other intruders on their site.

Autonomy: Some disruptions to leisure time and service are the results of non-hazardous actions performed by organizational staff by mistake (e.g., server configuration problem).

DoS is also possible in the cloud services because of the improper design techniques of the cloud applications. Attacks can occur due to the limited storage space available

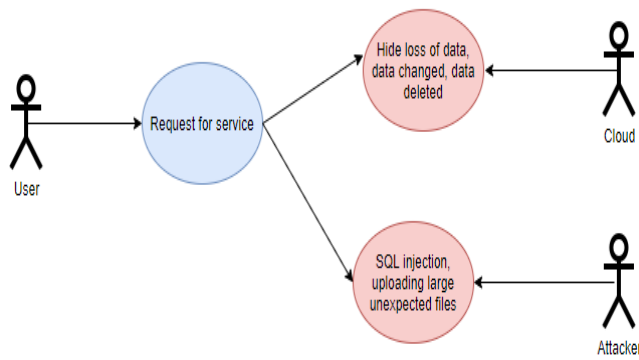


FIGURE 6. Denial of service attack use case diagram.

in the cloud. For this reason, the cloud deletes the files and doesn't allow updates. The attack can also happen when an unexpected and largest file uploaded by the attacker and overwriting data results in rejection of service attacks because existing data has been deleted and new data is being added to the cloud.

Use case diagram of the DoS attack is shown in Figure 6. In which, an attacker uses a cloud system and introduce vulnerabilities to prevent legal users to access cloud services. Legitimate users request services from the cloud and an attacker performs unpleasant activities such as buffer overflow, SQL injection, on or by uploading malformed packets which creates a lot of traffic in a communication channel of the cloud service provider. Similarly, in cloud performs other functions such as hiding the loss of data or data deletion and make more space for customers' threats to the request of data posed by the user. In such cases, the cloud is interrupted from providing the services to the legitimate users thus, causing a DoS attack.

b: DENIAL OF SERVICE ATTACK THREAT MODELLING

Figure 7 illustrates the DoS attack by using a sequence diagram. The user sends his/her relevant information to the cloud as proof of identity and once confirmed it is given authorized access to the encrypted data and cloud access policy. Then authorized and legitimate user requests for access of data stored in the cloud. However, the cloud couldn't provide a service to the user because unexpected activities are performed by the attacker such as SQL injection, large file uploading and buffer overload.

2) IMPERSONATING THINGS

An impersonating attack occurs when the attacker successfully takes over the appearance of the legitimate groups in the communication protocol. To be effective, a person who disguises himself needs to study carefully what he wants to do. Impersonation attacks take many forms and can point to both individuals and business organizations.

a: THREATS LEADING TO IMPERSONATION

These are some of the common reasons for impersonating things:

Steal sensitive information: Malicious attackers employ packet spoofing tools to capture the data packets in a network to steal or extract sensitive information like username, password, or use credit card numbers.

Criminal purposes: The attackers are usually after the sensitive business and financial information that can be later sold for criminal purposes.

Figure 8 shows a use case diagram of the eavesdropping attack which shows the activities of the invaders such as sniffing and monitor the communication mode. In the communication channel, the attacker accesses private data during the transmission of the packets and manipulates them to threaten legitimate users. The confidentiality and security of the encrypted data are then designed and sent to the destination by the source.

b: IMPERSONATING THINGS THREAT MODELLING

Figure 9 illustrates the impersonation attack by using a sequence diagram. The user sends his/her relevant information to the cloud as proof of identity and once confirmed it is given authorized access to encrypted data and cloud access policy. Then authorized and legitimate user requests for the access of data stored in the cloud. After that, the cloud over the verification of authentication initiates the transfer of the requested data over the communication link. The attacker who was also there monitor the link which holds the transmitted data disrupts or alters all information. It also monitors corrupted data of the legitimate users which could impede normal function. Alternatively, when a legitimate user sends some data to store over the cloud tempering attack can also occur. As a result, when some other user tries to access the data which was originally sent by the owner, he/she is given corrupted data.

3) UNAUTHORIZED ACCESS

Unauthorized access is when a person tries to access the website, program, server, or system by using some else's credentials or by using other methods. It could also occur if a user tries to attempt access to the area of the system that they should not be accessing. For instance, if a person keeps guessing the username and password for an account that is not their account until and unless they gain access, this act is considered unauthorized access.

a: THREATS LEADING TO UNAUTHORIZED ACCESS

These are some of the common reasons for unauthorized access:

Stealing user credentials: Engineering attacks especially phishing scams, in which an attacker sends messages to legitimate parties, usually with the intent to steal user credentials.

Vulnerable accounts: Attackers often seek out a compromised system, endanger it, and use it to access other secure programs

Internal Threats: A malicious intruder can use his position to gain unauthorized access to company systems

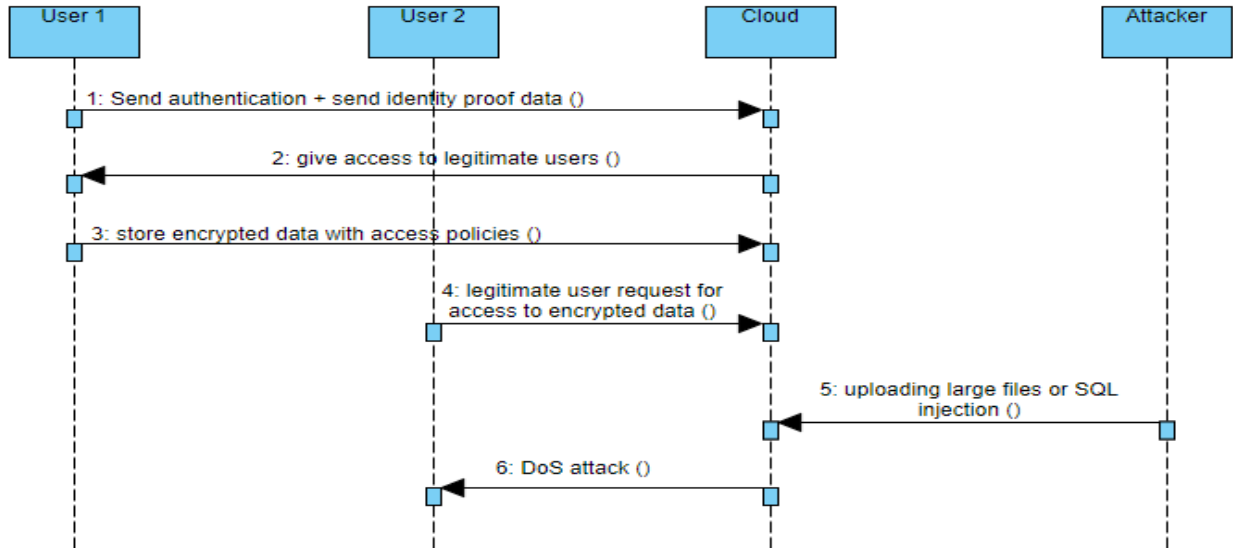


FIGURE 7. Sequence diagram for illustrating Dos by an attacker.

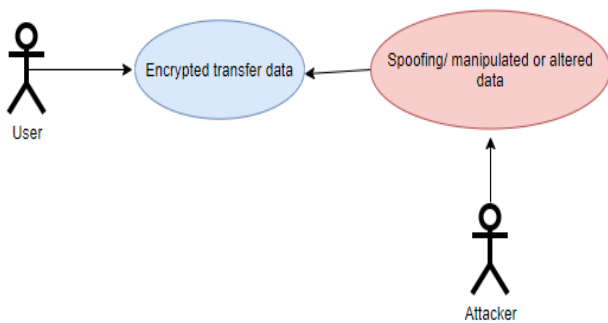


FIGURE 8. Impersonate attack use case diagram.

Zeus malware: An attacker uses botnets to gain unauthorized access to financial systems by stealing guarantees, banking details and financial data.

The phishing attack is one kind of unauthorized access that is used to steal someone’s personal information. Figure 10 shows a use case diagram of the phishing attack where an attacker sends a legitimate-looking website URL to the user. The user recognized the URL and graphical interface and then enters his/her username and password which may be directly taken to the phisher server and saved in their database. Later the attacker may steal the user’s social security numbers, business information and other personal information by using legitimate user’s credentials.

b: UNAUTHORIZED ACCESS THREAT MODELING

Figure 11 illustrates the phishing attack by using a sequence diagram. The user requests for the webpage but the phisher will send the URL of their own deployed web page which

is the same as the original page with some slight differences and hard for the user to find out. Suddenly, when the user recognizes the page with the phisher provided link they will believe it as an original page and unknowingly user enters their credentials and the phisher page loads successfully by storing the user’s sensitive information in the attacker’s database.

D. SECURITY MECHANISMS

Security mechanisms are technical tools and techniques which are used to secure things, their privacy and sensitive information from being accessed, modified and avoid being copied by an unauthorized person. A mechanism might operate by itself or by combining with others, to provide a specific service. They can be implemented in any layer but, in general, our analysis indicates that implementing security mechanisms in the initial levels of the protocols can secure high-level protocols. For instance, a link-layer encryptor can protect IP as well as ARP packets. In this section, the authors reviewed the four currently proposed architectures for securing the web of things.

1) IDENTITY MANAGEMENT

Identity management describes the management of devices, services, an individual’s identity, authentication, and authorization [56]. In any application and system, managing identity is an important aspect. Personal information such as ownership, identification, and social security should be secured from unauthorized access. Therefore, several studies have been published to control identity management issues [56], [57], [58], [69].

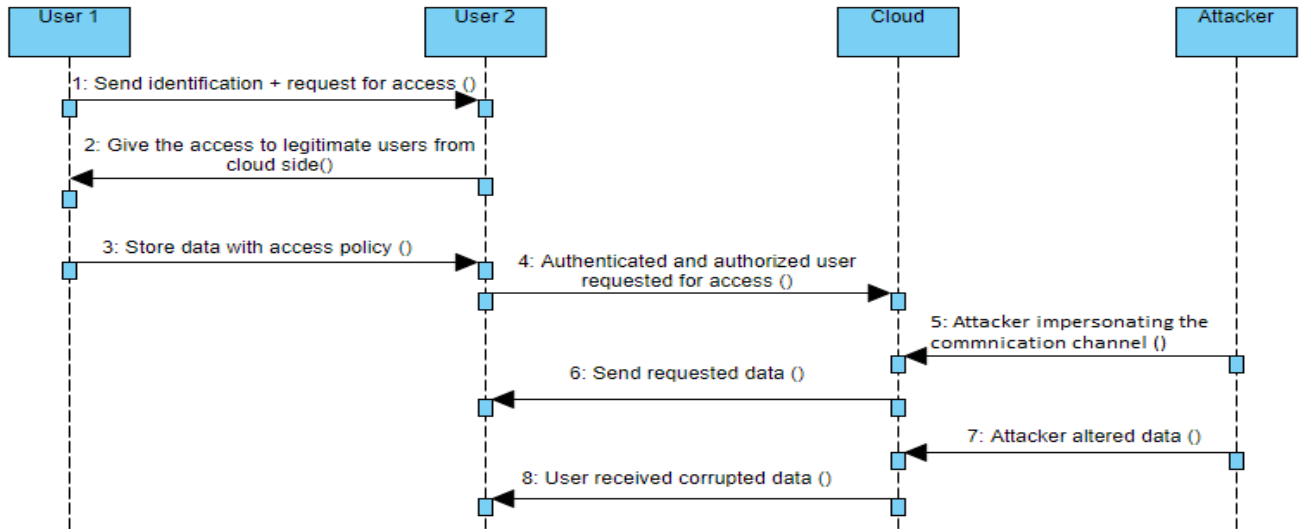


FIGURE 9. Sequence diagram for illustrating Impersonating things by the attacker.

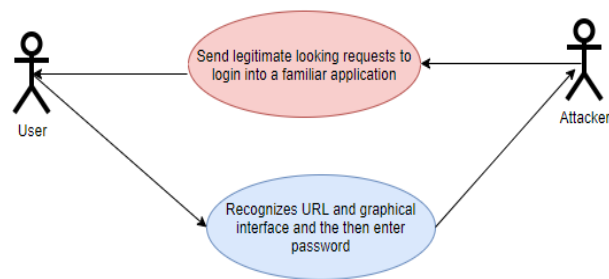


FIGURE 10. Phishing attack use case diagram.

Identity management establishes the rules for identifying entities in a specified method. The system controls an individual’s rights by providing authentication or by restricting them. Defining policy in identity management is also important to check whether the user is authorized to the network or not and which access rights he/she has under certain conditions. In WoT architecture, identity management is composed of three components: service provider, identity provider, and user. Some of the existing identity management models are briefly discussed in Table 3.

2) DATA CONFIDENTIALITY AND INTEGRATION

Ensuring data confidentiality is important for WoT systems because any failure can seriously create privacy issues. Therefore, it is imperative to protect the communication between different WoT modules, to maintain data integrity, confidentiality and to prevent third parties from snooping on information exchanges between different modules of the system.

Using encryption in WoT to solve this problem can be problematic because cryptographic computations require a

TABLE 3. Existing models of identity management.

Identity management model	Description
User-centric model	This model provides the solution to solve the user identification problem by providing the individual full transaction control. The identity provider can also provide a user with one or more identities such as confidentiality, integrity, and unlink-ability.
Centralized federation model	In this model unique trusted identity information (idP) provider is responsible for the provision and collecting of individuals with ID. Although this idP faces the problem of one point of failure because if this part fails it becomes the cause of the failure of the whole identity management system's failure.
Decentralized federation model	The services of an identity information provider are distributed across several idPs of different domains. Therefore, in this model, a person does not have full control over his or her details and information can be disclosed to a third party without the consent of the person.

lot of power and money which is not always available on smart devices [59]. Cryptographic algorithms are divided into two main categories as discussed below in Table 4.

3) AUTHENTICATION AND AUTHORIZATION

As smart things are part of the World Wide Web (www) and can be easily opened by anyone it is important to allow flexible and elegant access control only to recognized modules in an open system such as WoT.

Due to smart objects inhibited nature, it might not be possible to apply traditional cryptographic algorithms and protocols. To solve this problem most of the distributed

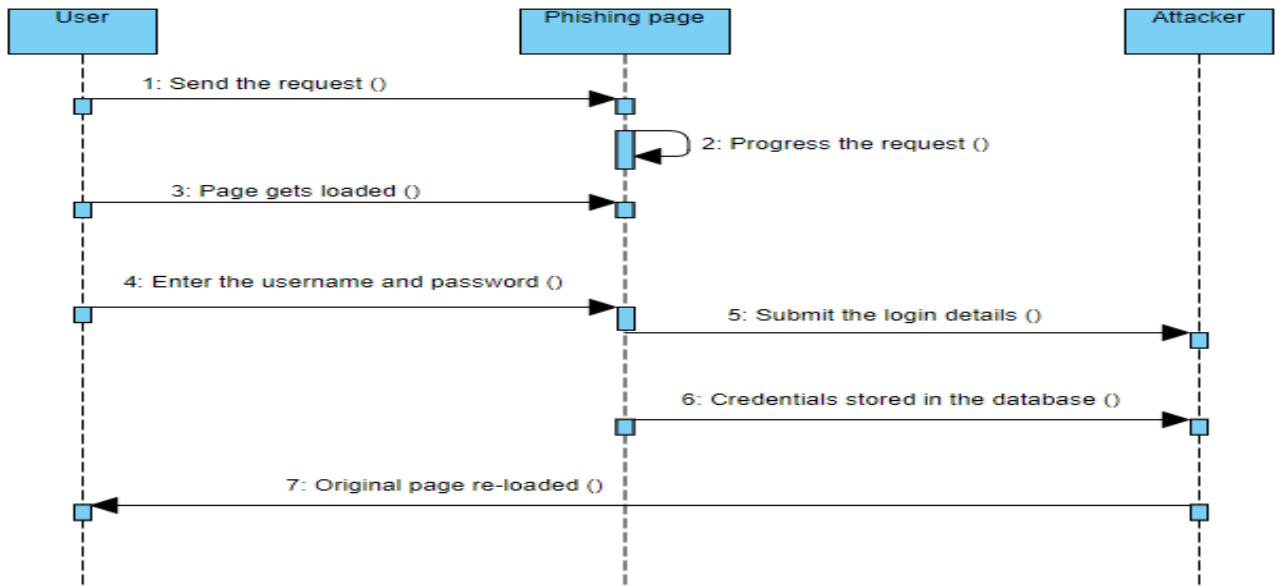


FIGURE 11. Sequence diagram for illustrating Phishing attack.

TABLE 4. Cryptographic algorithms.

Protocols	Description
Symmetric protocol	In this algorithm, the key is shared between the entities to encrypt and decrypt data. The main drawback of this algorithm is the requirement of accessing the private shared keys between involved parties. However, the symmetric algorithm is less resource consuming than asymmetric protocols.
Asymmetric protocol	In this algorithm, private or public keys are shared for encrypting and decrypting data. The encrypting entities use the public key of the receiver to encrypt data and to decrypt data the receiver uses a private key. A public key is not kept secret but private keys are kept secret and they are not available to anyone except the owner.

authorization architectures have been proposed, where the back-end server deals with intricate tasks that require resources for processing while restrictive objects need to deal with minimal messages.

The back-end server is mostly situated between the requester and the smart objects. However, smart things also need to be able to distinguish the difference between different requests coming from different modules and be able to use the right authentication decision.

Simultaneously, few lightweight cryptographic protocols like OAuth, SEA, and PRESENT have been built specially to satisfy this purpose [60]. Establishing a secure DTLS router between different resource-constrained modules and allowing for the distribution of complex cryptographic data between external devices is another proposed solution for

CoAP authentication and the DCAF accreditation framework [61]. These processes can be used to transfer authenticity between communicating peers and authorization management to trustworthy third parties with more computational money, power and strength.

These constrained nodes should be present in various aspects of daily life so that a large amount of information is provided and protected from various susceptible attacks. Authorization and authentication are required for the safety of WoT. Figure 12 shows an overall authentication architecture which is proposed by [62]. Exclusively for constrained environments another authentication and authorization architecture, is proposed by [63]. In which complex security management tasks are assigned to a third entrusted party or they can get help from less restricted actors in the system. In the proposed structure, each device is given a restricted level. Complex security functions such as managing keys, enforcement authorization policies are performed on the behalf of respective managed nodes by the authorization manager also called less constrained nodes. The components included in this architecture are described in Table 5.

4) ACCESS CONTROL

The purpose of traditional access control is to protect data on the basics of attributes and identity of users. In general, access control is used to protect system resources, back end, and front-end data by using limits on what users can do, who can access the data, what resources they have, and what activities are allowed to be performed on the data.

Access control protects the data from unauthorized users from making changes, viewing, and copying. Figure 13 summarizes the basic architecture of access control.

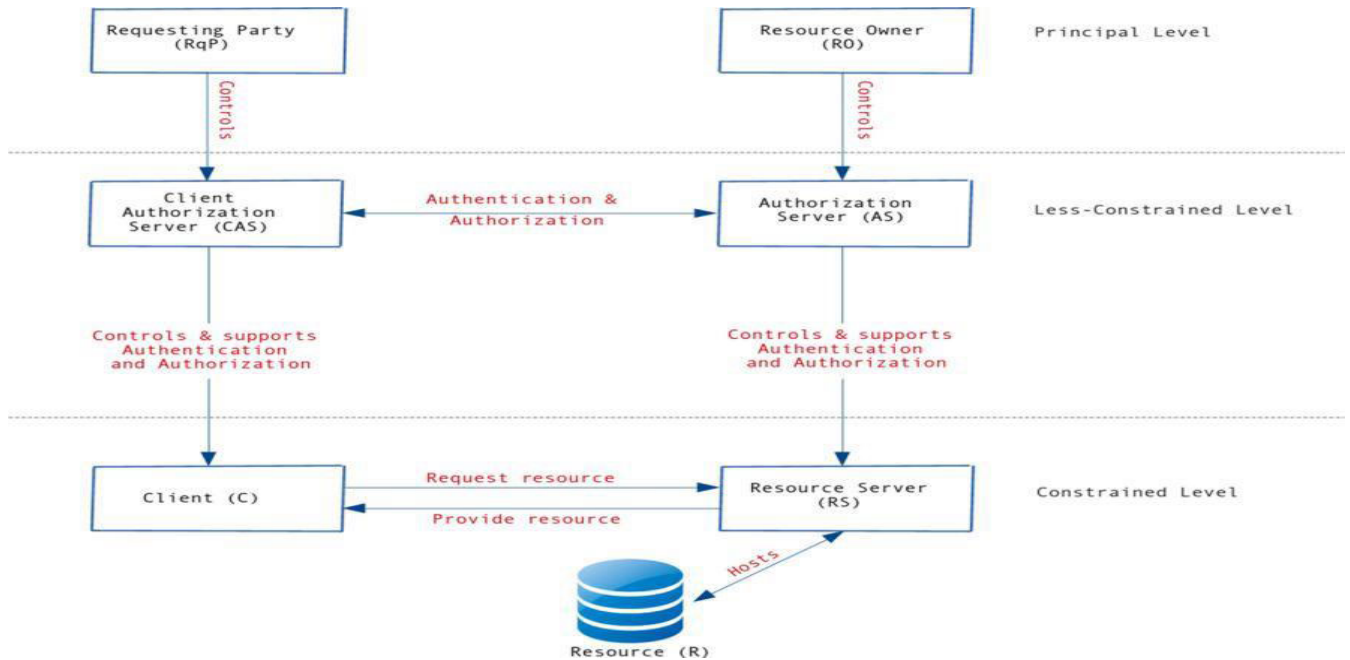


FIGURE 12. Overview of authentication architecture [63].

TABLE 5. Deployed components of authentication architecture.

Component	Role
Resource server (RS)	It is responsible for representing and hosting a resource. It can be a less controlled expedient.
Client (C)	A client is an endpoint to request the resource server. It can be a restricted device or not.
The authorization server (AS)	It is responsible for approving or creating authorization and authentication data for the resource server. It also plays the backup part of the resource owner. It is a less restricted device of the architecture
The client authorization server (CAS)	It is responsible for receiving and building authentication and authorization data. It also plays the backup role of the requesting team to handle client access requests. It is also a less constrained device of the architecture
Resource owner (RO)	This principle owns and controls the resources and also grant permission to use a mechanism like OAuth and user-managed access.
Requesting party (RqP) principal	This policy governs the client which governs customer requests and the acceptance of feedback received. It can be either RO or RqP.

Where an entity X requires access to entity resources Y, this request must be passed to a security guard who will grant access or not. Denial of access has two additional steps, if the number of attempts by the same user reaches the limit the system will automatically block that request or may ask the user to resubmit the access request.

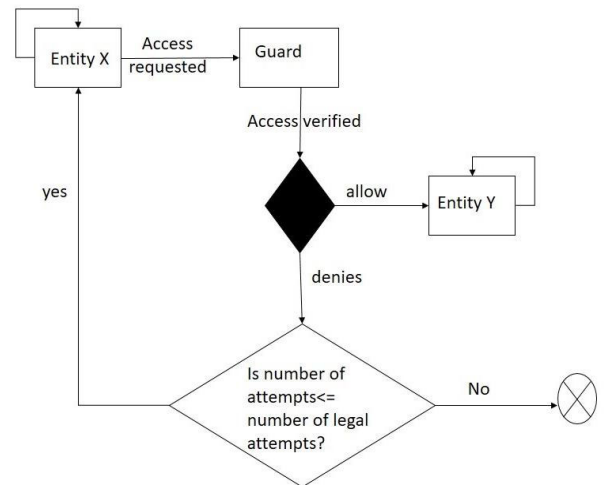


FIGURE 13. The basic flow of access control.

The WoT framework allows smart objects to exchange information with each other. Though, some security preventions need to be set before exchanging information through the web. Certain threats regarding access control for the object’s information and resources are unwanted data sharing, diver’s attacks, and malicious clients, etc. Here, the question is how to allow smart devices to access client secure resources in such an environment.

To answer that question, many access control standard authorization models have been proposed. Such as role-based access control, attribute-based access control, dynamic authorization, and multilevel security using information flow

TABLE 6. Architectures of implementing access control.

Architecture	Description
Distributed model	In this architecture access control server verifies the authenticity of the user and gives him/her the appropriate access token to access resources temporarily or permanently depending on the police deployed.
Centralized model	In this architecture, users are requested to use resources from the Access Control Server which carries them to the correct destination. Also, there is no direct interaction between the parties connected.

respectively in [64]–[67]. The selected models proposed; there are two methods to use to control web access to objects as discussed in Table 6.

In real life, access control architectures can be employed by using both distributed and centralized models. Implementing centralized models in WoT is quite interesting as all the network complexity is carried by the server but, this could create various problems for instance single point of failure, impersonation and privacy problems because all the eventual responses and requests are monitored by the server. On the other hand, the distributed model provides better privacy and system stability but it could be difficult to implement.

VI. DISCUSSION

Instead of the vast connectivity of the smart devices to the WoT, users are still concerned about sharing their personal information with Smart things also about who is accessing their data. They want to have complete control over their data and have adequate security procedures to defend data inside or outside the structure.

There are three ways in which WoT poses a threat. Firstly, the excessive use of internet-connected devices that means the consumer's private data can be connected in powerful and new ways. Though it can be used to build a better user experience, it also means the companies that have access to this data and wants to steal it, can help them to steal user's behavior through innocuous tools and it can be used for marketing purposes. Secondly, WoT devices don't just allow hackers to access an individual's data and behavior also provide a way to reduce the structure of the internet. In 2016, a botnet that took advantage of a large number of IoT devices was created by scanning the internet effectively for devices which had default password and usernames. These devices were infected by the malware called Miri, which became the largest denial of service attack ever, that have access over vast areas of the internet, including Netflix, CNN, and Twitter [68]. Lastly, the risk is related to confidentiality associated with potential physical threats. When we begin the hypothesis of "smart cities", the risks caused by WoT devices are exacerbated where the digital ecosystems of entire cities are interconnected. So that it is necessary to identify

and handle threats for the successful implementation of WoT economically. Privacy and security issues to provide identity among existing WoT technologies is presented in [5]. The author also provided a framework that was implemented in smart cities to evaluate the strength and weaknesses of the proposed framework. The integration of smart things with WoT raised privacy issues but the security issues that the smart cities will face were not mentioned in this study.

In this study, a concern of the authors was to identify different types of issues that occurred while connecting smart things to the internet through the web. Such as unauthorized access, denial of service attack, tempering, impersonating, and eavesdropping. Among all attacks, unauthorized access is considered more dangerous because an attacker can access all sensitive personal information and caused huge losses. Famous websites like PayPal, Myspace, Orkut (Google's social media platform), amazon, and TweetDeck (an application in Twitter) had been affected by hackers in the past [39].

It is possible to strengthen the security of the environment by applying security mechanisms such as authentication protocols, built resilient and well-tested code, manipulating encryption technology, or by putting security level checks on APIs [8]. The focus of that study was to find the privacy issues find the lightweight privacy solution that can be implemented in a heterogeneous environment. The authors also incorporate existing security and privacy measures developed by investigators by the researchers. Four main aspects are; identity management, access control, data confidentiality and integration, authentication, and authorization. Different security mechanisms have been introduced by the scientific community which can help secure data. Recently, the authors in [71], showed how to secure data transfer protocols. They also proposed the group key transfer protocol. To do so, they created a variation of the Diffie-Hellman algorithm, designed for one-to-one interaction. The motive for this policy is to keep the key updated, its privacy and authentication. Two security mechanisms were proposed to protect the privacy details of the legitimate users by the authors in [72]. The first scheme focuses on computer efficiency over time and the second provides better protection at accounting costs. They used proxy-based additive homomorphism by re-encrypting and design these two privacy schemes. Authors in [74], developed the alternatives of the Map-Reduce paradigm. Then they complied with HIPAA. They also used an OpenSSL encryption packet to ensure maximum disability and extra security to the data. The literature comparison of different security mechanism techniques is given in Table 7.

Some of the mechanisms and algorithms to improve security information are Biometrics, access cards, keys, FIDO authentication, matching against a database and Public key infrastructure based methods. Table 8 summarizes the existing security mechanisms with security measures. Based on this study, the authors' findings are that the most lacking WoT security mechanisms are authentication and authorization as the increased number of WoT devices make it critical to

TABLE 7. Comparison of different security mechanisms with literature.

Publication	Problem Tackled	Security Mechanism
[7]	Lightweight privacy solution	authentication protocols and manipulating encryption technology
[69]	Data integrity verification	Authenticator based data integrity verification techniques
[70]	Data integrity	Sensitive data segment
[71]	Secure transfer of the data	Diffie Hellman algorithm variations
[72]	Supply information security to trusted users	Proxy-base additive homomorphism
[73]	Leakage of Encryptor	CP-ABE scheme
[74]	Security of data levels	OpenSSL encryption package
[75]	Provide security in monitoring the patients by using remote devices	ElGamal algorithm

TABLE 8. Security measures and associated mechanisms.

Security Measure	Associated Security Mechanisms
Access Control	Biometrics, VPN, Passwords and keys, Reference monitor, Time limits, User permissions, Multilevel security
Identity Management	Biometrics, Access cards, Logging and auditing, Intrusion detection systems
Data Confidentiality and Integration	User permissions, Secure channels, Alarms
Authentication and authorization	One-time password, FIDO authentication, Matching against a database, Public key infrastructure based

secure authentication. After authentication, access control mechanisms must be solved as anyone should not have access to everything. Currently, there is no perfect security mechanism that can be used to ensure full security in the system. Technology has taken a huge step forward over the years, which could help build high-performance technologies that are currently in use due to the computer load they need. However, this technology is the same for hackers, which means they need less time to find the keys.

One of the solutions to security systems can be got by combining all the existing algorithms and mechanisms altogether. But, it seems that things are highly dependent in situations where it has to apply, in some places security is needed to protect the database while others protect the keys that encrypt the data being stored. To take full advantage of the future power of the WoT, governments and manufacturers have begun to put their efforts into innovating new technologies to enable the security of connected devices without disrupting user experience or adding additional costs and processes.

VII. CONCLUSION

WoT is transforming the IoT as the web has transformed computing over the last decade. This prototype of networking has been employed in every part of our lives ranging from smart cities to agriculture and industries but, connectivity between different devices is creating many security and trust problems. So, In this paper, highlighted the major security issues such as unauthorized access, tampering, impersonation, DoS, and snooping. After that applied threats analysis and attack modelling method to some of these highlighted security threats on security threats to find system vulnerabilities that can be helpful to protect the system from future attacks. Among all issues, handling unauthorized access is considered a major threat to WoT connected devices. To secure WoT communication between different devices further highlighted some of the security mechanisms such as access control, identity management, confidentiality, and integration, authorization and authentication.

Authors have used Threat analysis and attack modeling methods to inform the users about defensive measures and to prevent security threats from taking advantage of system flaws. Authors have provided the necessary insight into how security can be improved by using certain existing mechanisms and algorithms.

In our findings, security models are still immature and further research is required for ensuring security in WoT. In the author's opinion by ensuring things security, users' trust in the connected WoT devices can be achieved that can in return provide greater benefits such as reusability, easy access to information, and cost-effectiveness.

In the future, privacy and trust issues related to WoT can be identified to make communication between different objects of the environment easily.

REFERENCES

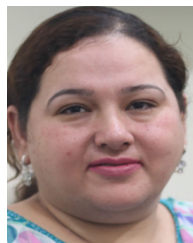
- [1] D. Raggett, "The Web of things: Challenges and opportunities," *Computer*, vol. 48, no. 5, pp. 26–32, May 2015.
- [2] T. Kindgerg, J. Barton, J. Morgan, G. Becker, D. Caswell, P. Debaty, G. Gopal, M. Frid, V. Krishnan, H. Morris, J. Schettino, B. Serra, and M. Spasojevic, "People, place, things: Web presence for the real world," *Mobile Netw. Appl.*, vol. 7, no. 5, pp. 365–376, 2002.
- [3] D. Guinard, "A Web of things application architecture: Integrating the real-world into the Web," ETH Zürich, Zürich, Switzerland, 2011.
- [4] I. billions and Statista. (2018). *IoT: Number of Connected Devices Worldwide 2012- 2025* | Statista. [Online]. Available: <https://www.statista.com/statistics/471264/iotnumberofconnected-devices-worldwide/>
- [5] M. S. Ferdous and R. Poet, "A comparative analysis of identity management systems," in *Proc. Int. Conf. High Perform. Comput. Simul. (HPCS)*, Jul. 2012, pp. 454–461.
- [6] L. Catuogno and S. Turchi, "The dark side of the interconnection: Security and privacy in the Web of things," in *Proc. 9th Int. Conf. Innov. Mobile Internet Services Ubiquitous Comput.*, Jul. 2015, pp. 205–212.
- [7] S. Mishra, S. Jain, C. Rai, and N. Gandhi, "Security challenges in semantic Web of Things," in *Proc. 9th Int. Conf. Innov. Bio-Inspired Comput. Appl. (IBICA)*, Kochi, India, Dec. 2018.
- [8] W. Shafik and S. M. Matinkhah, "Privacy issues in social Web of things," in *Proc. 5th Int. Conf. Web Res. (ICWR)*, Apr. 2019, pp. 208–214.
- [9] J. Liu, C. Fang, and N. Ansari, "Request dependency graph: A model for Web usage mining in large-scale Web of things," *IEEE Internet Things J.*, vol. 3, no. 4, pp. 598–608, Aug. 2016.

- [10] C. Koliás, A. Stavrou, J. Voas, I. Bojanova, and R. Kuhn, "Learning Internet-of-Things security 'hands-on,'" *IEEE Secur. Privacy*, vol. 14, no. 1, pp. 37–46, Jan. 2016.
- [11] D. Miorandi, S. Sicari, F. D. Pellegrini, and I. Chlamtac, "Internet of Things: Vision, applications and research challenges," *Ad Hoc Netw.*, vol. 10, no. 7, pp. 1497–1516, Sep. 2012.
- [12] S. Babar, P. Mahalle, A. Stango, N. Prasad, and R. Prasad, "Proposed security model and threat taxonomy for the Internet of Things (IoT)," in *Proc. Int. Conf. Netw. Secur. Appl.* Berlin, Germany: Springer, 2010, pp. 420–429.
- [13] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the Internet of Things: A review," in *Proc. IEEE Int. Conf. Comput. Sci. Electron. Eng. (ICCSEE)*, vol. 3, Mar. 2012, pp. 648–651.
- [14] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: Perspectives and challenges," *Wireless Netw.*, vol. 20, no. 8, pp. 2481–2501, Nov. 2014.
- [15] E. Oriwoh, H. Al-Khateeb, and M. Conrad, "Responsibility and Non-repudiation in resource-constrained Internet of Things scenarios," in *Proc. Int. Conf. Comput. Technol. Innov. (CTI)*, 2016, pp. 1–7.
- [16] T. A. Ahanger and A. Aljumah, "Internet of Things: A comprehensive study of security issues and defense mechanisms," *IEEE Access*, vol. 7, pp. 11020–11028, 2019.
- [17] M. R. Faheem, T. Anees, and M. Hussain, "The Web of things: Findability taxonomy and challenges," *IEEE Access*, vol. 7, pp. 185028–185041, 2019.
- [18] D. Zeng, S. Guo, and Z. Cheng, "The Web of things: A survey," *J. Commun.*, vol. 6, no. 6, pp. 424–438, 2011.
- [19] D. Guinard and V. Trifa, "Towards the Web of things: Web mashups for embedded devices," in *Proc. Workshop Mashups, Enterprise Mashups Lightweight Composition Web (MEM), Proc. WWW (Int. World Wide Web Conf.)*, Madrid, Spain, vol. 15, 2009, p. 8.
- [20] O. Akribopoulos, I. Chatzigiannakis, C. Koninis, and E. Theodoridis, "A Web services-oriented architecture for integrating small programmable objects in the Web of things," in *Proc. Develop. E-System Eng.*, Sep. 2010, pp. 70–75.
- [21] B. Ostermaier, M. Kovatsch, and S. Santini, "Connecting things to the Web using programmable low-power WiFi modules," in *Proc. 2nd Int. Workshop Web Things (WoT)*, 2011, pp. 1–6.
- [22] K.-I. Hwang, J. In, N. Park, and D.-S. Eom, "A design and implementation of wireless sensor gateway for efficient querying and managing through world wide Web," *IEEE Trans. Consum. Electron.*, vol. 49, no. 4, pp. 1090–1097, Nov. 2003.
- [23] V. Trifa, S. Wieland, D. Guinard, and T. Bohnert, "Design and implementation of a gateway for Web-based interaction and management of embedded devices," Inst. Pervasive Comput., ETH Zurich 2 SAP Res. CEC Zurich, Zürich, Switzerland, 2009, pp. 1–14.
- [24] M. S. Dawood, M. J. Margaret, and R. Devika, "Review on Applications of Internet of Things (IoT)," *Int. J. Adv. Res. Comput. Eng. Technol.*, vol. 7, no. 12, pp. 1–6, 2018.
- [25] P. Goyal, A. K. Sahoo, T. K. Sharma, and P. K. Singh, "Internet of Things: Applications, security and privacy: A survey," in *Proc. Mater. Today*, May 2020, doi: 10.1016/j.matpr.2020.04.737.
- [26] A. Kamilaris and N. Botteghi, "The penetration of Internet of Things in robotics: Towards a Web of robotic things," 2020, *arXiv:2001.05514*. [Online]. Available: <http://arxiv.org/abs/2001.05514>
- [27] K. Taylor, C. Griffith, L. Lefort, R. Gaire, M. Compton, T. Wark, D. Lamb, G. Falzon, and M. Trotter, "Farming the Web of things," *IEEE Intell. Syst.*, vol. 28, no. 6, pp. 12–19, Nov. 2013.
- [28] A. Heil, M. Knoll, and T. Weis, "The Internet of Things—context-based device federations," in *Proc. 40th Annu. Hawaii Int. Conf. Syst. Sci. (HICSS)*, Jan. 2007, p. 58.
- [29] S. Fang, L. Xu, Y. Zhu, Y. Liu, Z. Liu, H. Pei, J. Yan, and H. Zhang, "An integrated information system for snowmelt flood early-warning based on Internet of Things," *Inf. Syst. Frontiers*, vol. 17, no. 2, pp. 321–335, Apr. 2015.
- [30] J. Poncela, P. Vlacheas, R. Giuffreda, S. De, M. Vecchio, S. Nechifor, and P. Demestichas, "Smart cities via data aggregation," *Wireless Pers. Commun.*, vol. 76, no. 2, pp. 149–168, 2014.
- [31] F. Alsubaie, A. Abuhusseini, V. Shandilya, and S. Shiva, "IoMT-SAF: Internet of medical things security assessment framework," *Internet Things*, vol. 8, Dec. 2019, Art. no. 100123.
- [32] P. Emami-Naeini, Y. Agarwal, L. F. Cranor, and H. Hibshi, "Ask the experts: What should be on an IoT privacy and security label?" 2020, *arXiv:2002.04631*. [Online]. Available: <http://arxiv.org/abs/2002.04631>
- [33] S. M. Tahsien, H. Karimipour, and P. Spachos, "Machine learning based solutions for security of Internet of Things (IoT): A survey," *J. Netw. Comput. Appl.*, vol. 161, Jul. 2020, Art. no. 102630, doi: 10.1016/j.jnca.2020.102630.
- [34] N. Balakrishnan, A. Rajendran, D. Pelusi, and V. Ponnusamy, "Deep belief network enhanced intrusion detection system to prevent security breach in the Internet of Things," *Internet Things*, Sep. 2019, doi: 10.1016/j.iot.2019.100112.
- [35] S. K. Datta, R. P. F. da Costa, C. Bonnet, and J. Haerri, "Web of things for connected vehicles," in *Proc. W3C Track, 25th Int. World Wide Web Conf. (WWW)*, Montreal, QC, Canada, Apr. 2016.
- [36] H. HaddadPajouh, A. Dehghantanha, R. M. Parizi, M. Aledhari, and H. Karimipour, "A survey on Internet of Things security: Requirements, challenges, and solutions," *Internet Things*, 2019, Art. no. 100129, doi: 10.1016/j.iot.2019.100129.
- [37] N. A. A. Bakar, W. M. W. Ramli, and N. H. Hassan, "The Internet of Things in healthcare: An overview, challenges and model plan for security risks management process," *Indonesian J. Elect. Eng. Comput. Sci.*, vol. 15, no. 1, pp. 414–420, 2019.
- [38] S. Li, H. Song, and M. Iqbal, "Privacy and security for resource-constrained IoT devices and networks: Research challenges and opportunities," *Sensors*, vol. 19, no. 8, p. 1935, Apr. 2019.
- [39] J. Mack, Y. H. F. Hu, and M. A. Hoppa, "A study of existing cross-site scripting detection and prevention techniques using XAMPP and Virtual-Box," *Virginia J. Sci.*, vol. 70, no. 3, p. 1, 2019.
- [40] Y. Mehmood, F. Ahmad, I. Yaqoob, A. Adnane, M. Imran, and S. Guizani, "Internet-of-Things-based smart cities: Recent advances and challenges," *IEEE Commun. Mag.*, vol. 55, no. 9, pp. 16–24, Sep. 2017.
- [41] M. Abdel-Basset, G. Manogaran, M. Mohamed, and E. Rushdy, "Internet of Things in smart education environment: Supportive framework in the decision-making process," *Concurrency Comput., Pract. Exper.*, vol. 31, no. 10, p. e4515, May 2019.
- [42] B. B. Lin, "Resilience in agriculture through crop diversification: Adaptive management for environmental change," *BioScience*, vol. 61, no. 3, pp. 183–193, Mar. 2011.
- [43] A. A. R. Madushanki, M. N. W. A., and A. Syed, "Adoption of the Internet of Things (IoT) in agriculture and smart farming towards urban greening: A review," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 4, pp. 11–28, 2019.
- [44] S. Tian, W. Yang, J. M. L. Grange, P. Wang, W. Huang, and Z. Ye, "Smart healthcare: Making medical care more intelligent," *Global Health J.*, vol. 3, no. 3, pp. 62–65, Sep. 2019.
- [45] M. Gerla, E.-K. Lee, G. Pau, and U. Lee, "Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds," in *Proc. IEEE World Forum Internet Things (WF-IoT)*, Mar. 2014, pp. 241–246.
- [46] M. Ibrahim, A. Elgamri, S. Babiker, and A. Mohamed, "Internet of Things based smart environmental monitoring using the Raspberry-Pi computer," in *Proc. 5th Int. Conf. Digit. Inf. Process. Commun. (ICDIPC)*, Oct. 2015, pp. 159–164.
- [47] W. Qin, S. Chen, and M. Peng, "Recent advances in industrial Internet: Insights and challenges," *Digit. Commun. Netw.*, vol. 6, no. 1, pp. 1–13, Feb. 2020.
- [48] Y. Mehmood, F. Ahmad, I. Yaqoob, A. Adnane, M. Imran, and S. Guizani, in *Proc. Int. Workshop Secure Internet Things*, 2014, pp. 35–43.
- [49] I. Ali, S. Sabir, and Z. Ullah, "Internet of Things security, device authentication and access control: A review," *Int. J. Comput. Sci. Inf. Secur.*, vol. 14, no. 8, Aug. 2016.
- [50] F. Lau, S. H. Rubin, M. H. Smith, and L. Trajkovic, "Distributed denial of service attacks," in *Proc. Int. Conf. Syst., Man Cybern. Evolving Syst., Hum., Organizations, Complex Interact.*, vol. 3, Oct. 2000, pp. 2275–2280.
- [51] Y. Ashibani and Q. H. Mahmoud, "A user authentication model for IoT networks based on app traffic patterns," in *Proc. IEEE 9th Annu. Inf. Technol., Electron. Mobile Commun. Conf. (IEMCON)*, Nov. 2018, pp. 632–638.
- [52] (2015). *Security*. [Online]. Available: <https://www.securitymagazine.com/articles/86650-common-types-of-unauthorized-access-and-how-to-combat-them>
- [53] X. Li, H. Wang, H. N. Dai, Y. Wang, and Q. Zhao, "An analytical study on eavesdropping attacks in wireless nets of things," *Mobile Inf. Syst.*, vol. 2016, pp. 1–5, Jan. 2016.
- [54] Q. Xu, P. Ren, H. Song, and Q. Du, "Security enhancement for IoT communications exposed to eavesdroppers with uncertain locations," *IEEE Access*, vol. 4, pp. 2840–2853, 2016.
- [55] I. Alqassem, "Privacy and security requirements framework for the Internet of Things (IoT)," in *Proc. Companion 36th Int. Conf. Softw. Eng.*, May 2014, pp. 739–741.
- [56] T. U. Khan, "Internet of Things (IOT) systems and its security challenges," *Int. J. Adv. Res. Comput. Eng. Technol.*, vol. 8, no. 12, pp. 1–12, 2019.

- [57] M. Trnka and T. Cerny, "Identity management of devices in Internet of Things environment," in *Proc. 6th Int. Conf. IT Converg. Secur. (ICITCS)*, Sep. 2016, pp. 1–4.
- [58] P. Mahalle, S. Babar, N. R. Prasad, and R. Prasad, "Identity management framework towards Internet of Things (IoT): Roadmap and key challenges," in *Proc. Int. Conf. Netw. Secur. Appl.* Berlin, Germany: Springer, 2010, pp. 430–439, 2010.
- [59] A. Salleh, K. Mamat, and M. Y. Darus, "Integration of wireless sensor network and Web of things: Security perspective," in *Proc. IEEE 8th Control Syst. Graduate Res. Colloq. (ICSGRC)*, Aug. 2017, pp. 138–143.
- [60] M. M. R. Abdmeziem, "Data confidentiality in the Internet of Things," Ph.D. dissertation, Dept. Inform., Univ. Sci. Technol. Houari Boumediene, Ezzouar, Algeria, Apr. 2016, doi: [10.13140/RG.2.2.19150.87366](https://doi.org/10.13140/RG.2.2.19150.87366).
- [61] (2012). *The OAuth 2.0 Authorization Framework*. [Online]. Available: <https://tools.ietf.org/html/rfc6749>
- [62] S. Gerdes, O. Bergmann, and C. Bormann, "Delegated authenticated authorization for constrained environments," in *Proc. IEEE 22nd Int. Conf. Netw. Protocols*, Oct. 2014, pp. 654–659.
- [63] S. El Jaouhari, A. Bouabdallah, and J. M. Bonnin, "Security issues of the Web of things," in *Managing the Web of Things*. San Mateo, CA, USA: Morgan Kaufmann, 2017, pp. 389–424.
- [64] E. Barka, S. S. Mathew, and Y. Atif, "Securing the Web of things with role-based access control," in *Proc. Int. Conf. Codes, Cryptol., Inf. Secur.*, Cham, Switzerland: Springer, 2015, pp. 14–26.
- [65] M. A. Al-Kahtani and R. Sandhu, "A model for attribute-based user-role assignment," in *Proc. 18th Annu. Comput. Secur. Appl. Conf.*, Dec. 2002, pp. 353–362.
- [66] J. Liu, C. Liu, D. Jiao, and J. Chen, "The research of a multi-factor dynamic authorization model," in *Proc. IEEE 9th Int. Conf. E-Bus. Eng.*, Sep. 2012, pp. 201–205.
- [67] A. C. Myers and B. Liskov, "A decentralized model for information flow control," *ACM SIGOPS Operating Syst. Rev.*, vol. 31, no. 5, pp. 129–142, Dec. 1997.
- [68] The Cloudflare Blog. *Inside the Infamous Miri IoT Botnet: A Responsive Analysis*. Accessed: Feb. 6, 2021. [Online]. Available: <https://cloudflare.com>
- [69] C. Liu, C. Yang, X. Zhang, and J. Chen, "External integrity verification for outsourced big data in cloud and IoT: A big picture," *Future Gener. Comput. Syst.*, vol. 49, pp. 58–67, Aug. 2015.
- [70] S Subashini, V Kavitha, "A metadata based storage model for securing data in cloud environment," in *Proc. Int. Conf. Cyber-Enabled Distrib. Comput. Knowl. Discovery*, Oct. 2011, pp. 429–434.
- [71] C. Hsu, B. Zeng, and M. Zhang, "A novel group key transfer for big data security," *Appl. Math. Comput.*, vol. 249, pp. 436–443, Dec. 2014.
- [72] Z. Yan, W. Ding, V. Niemi, and A. V. Vasilakos, "Two schemes of privacy-preserving trust evaluation," *Future Gener. Comput. Syst.*, vol. 62, pp. 175–189, Sep. 2016.
- [73] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring data storage security in cloud computing," in *Proc. 17th Int. Workshop Qual. Service*, Jul. 2009, pp. 1–9.
- [74] G. Zhou, D. Zhang, Y. Liu, Y. Yuan, and Q. Liu, "A novel image encryption algorithm based on chaos and line map," *Neurocomputing*, vol. 169, pp. 150–157, Dec. 2015.
- [75] D. Thilakanathan, Y. Zhao, S. Chen, S. Nepal, R. A. Calvo, and A. Pardo, "Protecting and analysing health care data on cloud," in *Proc. 2nd Int. Conf. Adv. Cloud Big Data*, Nov. 2014, pp. 143–149.



RUHMA SARDAR was born in Pakistan. She received the master's degree in software engineering from the University of Management and Technology, Lahore, Pakistan, in 2019, where she is currently pursuing the Ph.D. degree in computer science. She is currently working as a Senior QA Engineer with Quarrio Software House, Lahore. Her research interests include deep learning, the web of things, the Internet of Things, web services, quality assurance, and software fault tolerance.



TAYYABA ANEES was born in Pakistan. She received the Ph.D. degree from the Vienna University of Technology, Vienna, Austria, in 2012. Her Ph.D. dissertation is in the area of service-oriented architecture and web services availability domain. She has worked as a Project Assistant with the Vienna University of Technology for four years. She is currently working as the Program Head Software Engineering/an Assistant Professor with the Software Engineering Department, School of Systems and Technology, University of Management and Technology, Lahore. Her research interests include service-oriented architecture, web services, Web of Things (WOT), security, semantic web, software availability, software safety, software fault tolerance, and real-time data warehousing.

• • •