VFAST Transactions on Software Engineering
http://vfast.org/journals/index.php/VTSE@ 2023, ISSN(e): 2309-3978, ISSN(p): 2411-6246
Volume 11, Number 1, January-March 2023 *pp:85-100*

Humanoid Robots: Cybersecurity Concerns And Firewall Implementation

Safa Munir*, Kashaf Khan, Dr Naeem Aslam, Kamran Abid, Mustajib-ur-Rehman

Department of Computer Science, NFC Institute of Engineering and Technology, Multan, Punjab, Pakistan
*Corresponding author email: 2k20mscs105@nfciet.edu.pk

ABSTRACT

Technology has grown more important in our lives, and scientists are developing new products to make people's life easier and more pleasant. One of these innovations is the humanoid robot. The use of humanoid robots in our daily lives is expanding at an unprecedented rate as robots are being used in different aspects of life. The market is becoming more automated and optimized, Robotics serves as one of the primary instruments used for these reasons. Yet, security continues to pose a concern for robotics. As humanoid robots begin to function "in the open," we must assess the threats they will confront. Through the literature review, researchers found that security assessments were not performed on the robots which cause the robots to be weak against cybersecurity attacks. In this research, we perform different security assessments to identify the vulnerabilities in humanoid robots. Furthermore, different metrics were used to check and perform security assessments on the robot as well as the results of security assessments has been shown. It was shown that humanoid robots are vulnerable as anyone will be able to hack the login credentials of robot's website as well as there are some open ports in the robot's network which can be used by the hackers to exploit robot's working. Based on the results of assessment methods and our findings, we gave the firewall framework which will be helpful to protect the humanoid robot against those security vulnerabilities and attacks.This firewall framework will be able to protect the humanoid robots in aspects of both network and website/webpage exploitation.

KEYWORDS

Humanoid robots, cybersecurity, vulnerabilities, threats, assessment, firewall

JOURNAL INFO

HISTORY: Received: February 02, 2023 Accepted: March 27, 2023 Published: March 31, 2023

1. INTRODUCTION

Technology has a significant impact on our lives, both personally and professionally. Currently, technology may mean many different things. The phrase "technology" brings up thoughts of a wide range of products, including pcs, cellphones, and tablets. Technology may evoke visions of the internet, knowledge, or technological achievements. It might be a restricted perspective, but technology covers numerous imaginative answers to basic problems that humankind has faced all through history [1]. The role and impact of technology are expanding with time [2]. Technology everywhere around the globe has been employed to aid human being's life, ranging from the smallest basic advances to complex systems that operate completely independently of human expertise. Technology has revolutionized society in several ways; it helped early humans to farm their food, travel huge seas, and connect people on a global scale. The change from manual to technological problem-solving methodologies evolved simply because technology simplifies work [3]. Scientists and engineers are working hard to improve our quality of life through various innovations and technologies.

The field of robotics is not a recent one, it is a great invention as they are machines that help us in various industries. Robots are used in different fields and domains [4]In the early 1950s, the first robot was created, which resulted in the establishment of the Robotics industry. Robots help businesses and people to minimize expenses and do particular jobs in a quicker, more accurate, and more dependable way. They are frequently employed in industrial production, the defense sector, health care, education, and in different organizations [5]. The increased attention reflects a significant shift in robot skills over the last few centuries. Developing autonomous, adaptable, and multifunctional robots was a big engineering barrier, but great advances have been accomplished. Robots are capable of doing a broad range of operations with minimal human assistance, like welding, printing, and packing. These characteristics distinguish robots from prior waves of automated processes. Many individuals are concerned that as machines replace humans on more duties, large-scale job losses are on the horizon. [6]. The idea of controlling autonomous robots has been dramatically and intriguingly altered with the advent of social humanoid robots. Autonomous robots are often made to function as autonomously and distant from humans as possible, frequently carrying out jobs in dangerous and hostile conditions (such as clearing minefields, checking oil reserves, or discovering other planets). Other uses of autonomous robots include cleaning floors and delivering hospital meals, but there is still little interaction between humans and robots in these duties. The creation of robots that

can interact and collaborate with humans as a companion, rather than as a tool, is being driven by a wide variety of application areas (social, entertainment, medical services, etc.). According to studies by Reeves and Nass (1996) in the area of human-computer interaction (HCI), People generally approach computers in the exact manner they view humans. Possibly the best candidates for this are humanoid robots. Due to their comparable morphologies, they are able to communicate in ways that support human communication styles naturally. Examples include speech, posture, ability, and face and body language. It is not unexpected that research like this has had a significant impact on efforts in building technologies that collaborate with humans as collaborators and communicate with them [7]. The humanoid robot is an emerging field in Robotics. It plays a key role in robotics research. Since, Humanoid robots can move, behave, and interact like humans, they will eventually replace humans in certain difficult or dangerous tasks [8]. These robots are designed to communicate with humans and understand their emotions. Also, these robots are expected to work closely with humans in the everyday world. Humanoid robots like Pepper and Robovie [9] are utilized in public settings and can provide supervision, however, it is not their main function. They could play a role in interacting with people in public areas. ASKA is a robot receptionist, Pepper assists autistic patients and plays a role in educational institutions, whereas Geminoid has operated in a store [10]. The production and usage of robots are increasing day by day. More than 40 million robots are believed to have been sold between 2016 to 2019 [11]. Moreover, both the public and commercial sectors are making major investments in robotic technology. According to reports, robotics investment reached $188 billion globally in 2020 and is continuing to rise over the following years. Over the next five years, South Korea intends to invest $450 million in robotics. Alibaba and Foxconn recently gave Softbank $236 million for its robotics group. In the last two years, UBTECH Robotics has raised $120 million [12]. As robot knowledge is now employed in a variety of diverse industries, determining the actual number of automation industries is currently impossible [13]. Automation robots are playing a vital role in manufacturing large products. The core purpose of these robots is to lessen the need for human labor. Artificially intelligent robots are now able to complete tasks more quickly, safely, and effectively. Manufacturing, building, transportation, and quality control are a few examples of these vocations. Robots are deployed in risky environments to carry out risky activities. They are also more adept than humans in performing repeated jobs with the same quality and precision [14]. Hospital, surgical, and medical robots have all been built using robot technology [15]. Advanced therapeutic robots can perform Cardio-Pulmonary Resuscitation (CPR) and are utilized to accurately execute minor operations [16]. Robots are utilized in agriculture because they are more effective and efficient in conserving resources and labor. When working in a big farming area takes at least twelve personnel and many days, but robots are employed to do various jobs quickly. This improves agricultural cultivation, crop monitoring, harvesting, etc [17]. Emergency robots are capable to locate defenseless individuals who have been trapped or lost at some place due to flooding. Robots designed for disaster relief may do tasks and access areas that people cannot. Robots are being used in a variety of police roles, such as when it comes to disarming or eliminating offenders in situations deemed too risky and potentially fatal for devoted humans. The police's deployment of a robotic system outfitted with a C4 explosion as well as activating it to eradicate the Dallas shooter is a well-known application of this technology [14]. Although these robots are extremely important to our daily lives, there are several issues with their deployment in key infrastructure. The primary issues here are security, authenticity, and reliability. As Robots are playing an important role in our lives, in homes, and different fields and industries. Hence, it is important to configure the security of robots and to make the robots secure and safe so that they will not have a negative effect in our environment. If not, they will turn into deadly machines that may wreak havoc and seriously hurt both the environment and the people they are supposed to benefit [12].

Some incidents indicate that robots are a serious threat if they are launched without considering their negative effects. In 1979, the first human fatality caused by an industrial robot occurred. In order to physically count the components within a big shelving unit, a 25 y/o production staff Robert Williams of Ford Motor Company casting plant was requested to scale it [18]. Williams was standing when a robot arm used for parts retrieval discreetly approached the young guy, struck him in the head, and instantaneously killed him. Williams died on the ground, afterwards his corpse was discovered by anxious coworkers. Williams was unprotected since there were no barriers in place. Williams was unprotected since there were no barriers in place. There were no alerts to warn him of the coming arm, and there was no way to control the robot to behave differently around people. The next robot tragedy happened in 1981 and in identical conditions. Once more, a robot arm accidentally killed a man by failing to detect him. The robot pinned Kenji Urada against machinery with broken gears, trapping him there which results in his death [19]. A lady was murdered in 2015 in Cusseta, Alabama when an industrial robot restarted unexpectedly. During shooting practice in 2007, a malfunctioning robot cannon resulted in the deaths of 9 soldiers and severe injuries to another 14 soldiers. Even though these occurrences were unintentional, they sufficiently illustrate the grave possible consequences of robot errors [12]. Different operating systems are used by advanced robots. Not decades back, robot operating systems (ROS), platforms, and software were not open source, built by each firm separately and available exclusively within that company. But, with the emergence of generally available robot-specific operating systems such as free and open-source ROS, the situation has altered [20]. ROS (Robot

Operating System) is an open-source platform that assists researchers and programmers in the creation and use of code amongst robotic systems. It is also a worldwide open-source society of researchers, programmers, and enthusiasts that work to improve, make robots more approachable, and introduce them to everyone. It has been embraced by some of the most well-known organizations in robotics. The majority of the firms use ROS since it is easily deployed or a branch of ROS in some manner. And the number of use cases is still expanding. ROS is utilized in a variety of sectors, including farming, medical equipment, and household appliances, and is expanding to incorporate all types of automated use cases. These are a few of the firms that publicly use ROS today, and the list is growing and diversifying all the time [21]. It decreased the barrier of entry into robots for small businesses and individuals. Non-robot OS are often modified with some additional bespoke programs built to provide the needed robot capabilities. Because robots have comprehensive operating systems, they can be subject to the same kind of cyberattacks that the systems are exposed to today. Nevertheless, due to the availability of some specific sophisticated capabilities, such as autonomy of movement, actual actuators, various sensors, and cameras, robot cybersecurity is more challenging issue. Another aspect is the existence of many communication channels extending from the internet and different operating modes. All of this adds up to make robot security a far more challenging problem than conventional IT security. The threat landscape is vast, and as with any cyber-physical system, the consequences might be serious, even fatal, especially in essential applications [20]. Robotic problems include a variety of factors that might take advantage of any weakness in security to attack both robotic applications and systems. Robotic systems are widely supported by the intellectual and physical skills of aged and handicapped people, as well as ordinary human associates, in current history [22], [23]. Personal and professional automated systems as robots are fast evolving, and so security improvement is critical. Robots coexist in community hubs alongside people in a variety of settings, including residences, workplaces, and even key infrastructures such as airlines and institutions. As a result, their safety and protection are critical, especially as their competency is rising as well as they have been designed to function independently of human assistance [24]. Manufacturers' concerns, and current requirements, are primarily concerned with safety.

Security is not regarded as an important issue. Many of these robots' design is the best demonstration of how insufficient security has been addressed. Unprotected, dangerous, unsecured, and/or public robots result in a variety of bad results for organizations [25]. Security is not an item, but rather a procedure that must be evaluated regularly as systems develop and cybersecurity issues emerge. This is especially important given the rising complexities of such systems. Modern autonomous robots are complicated, which results in vast potential vulnerabilities and a multitude of new threat vectors, making the employment of old methodologies problematic. Overall, this generates the research questions: What is the current state of protection in robotics? and how can we increase security measures in robots the most? [26] As Eduardo B. Fernandez mentioned, a significant portion of technologies and robotic applications have faults, defects, and weaknesses that attackers may readily exploit [27]. Addressing these weaknesses and vulnerabilities, though, does not represent a straightforward or full answer to the issue. Vulnerabilities are becoming more numerous and severe and trying to protect devices and networks that contain risky software is an unproductive strategy to resist intruders [28]. The majority of commercial, domestic, and business robots are unprepared for cyber threats and exploitable weaknesses. Robot security flaws are a major source of concern for producers, developers, and people who interface with them in critical applications as in hospitals. Robots operate in intimate, full contact with kids, older individuals, and people with impairments in a medical environment, and it might be uncertain to the potential customer if the robot is performing well or is under threat [29]. The truth is that insufficient attention has been paid to well-known security vulnerabilities that have previously shown to be disastrous on the eve of past advances in artificial intelligence, Like the rise of commercial digital networks and the acceptance of the net. Unfortunately, we are seeing an increase in the number of robot companies taking risks and rushing their products to market without proper security considerations. Furthermore, it is typical for manufacturers that lack effective security policies to be unsure of how to handle vulnerability reports. Most of them are unlikely to have an effective framework in place to address concerns, much alone offer security updates to clients. If lessons are not learned and robot producers do not prioritize security today, it will come back to haunt them later [25]. Robots are exposed to a variety of vulnerabilities [30], [31] which can impair their connection, efficiency, procedures, and reliability. Multiple flaws in the operation of robots can render them dangerous to humans. Robotic devices are prone to numerous wired/wireless connectivity exploits such as replay, man-in-the-middle, spying, probing, spoofing, and so on due to a lack of fundamental security precautions. Adopting new security precautions before thoroughly evaluating them can have an impact on the operation of both robotic applications and gadgets. Application security app that has not been examined and assessed for programming or usability problems could also influence the performance of the robots. Hence, testing is important prior to deployment. Robots are also vulnerable to update bugs, which can lead their devices and system software to behave differently as a result of the new version, such as the loss of unrecorded data, the stoppage of an existing procedure, and so on [14]. Attackers often use malicious code or directly penetrate distant devices by utilizing existing vulnerabilities and defects in infrastructure, programming, and protocols. Defenders must uncover flaws and faults before attackers in order to combat attackers and

avoid a device from being exploited. To do so, vulnerability ideas must be extensively explored, and vulnerability assessment must be utilized to analyze system vulnerabilities as a prospective threat actor [32]. A vulnerability scanner uses advanced technologies to identify security flaws and gaps that might enable an attacker to obtain unauthorized access to systems and devices [33].

A method of demonstrating entire system protection is to undertake penetration testing with preexisting tools to detect shortcomings [34], [35]. Penetration testing is conducted manually or automatically using technology solutions. In any case, the procedure comprises acquiring data about the intended system before the examination (reconnaissance), recognizing potential open ports, trying to break in and communicating back the discoveries. The primary goal of penetration testing is to identify security flaws [36]. Penetration testing examines the device to assess how well it performs in the context of network security, and how effectively it is secured concerning security measures. Also, it involves ethical hacking of the system to determine how sensitive it is to network attacks like DoS. The primary goal of the testing process is to access a system and examine its holes and protection mechanism so that it will help to improve the security weaknesses they have left in the defensive system to guarantee that the system is secure from any external malware that could attempt to violate the security of the system and gain unauthorized access to the information. It has the potential to mishandle the information and destroy the communication system [37]. Thorough penetration testing raises awareness and lowers intrusion threats [34], [38]. There are several penetration testing tools in the market, some of which may be customized to increase efficiency. The usage of each tool is dependent on the circumstances or system being examined. These tools have specialized goals, in addition to guides and instructions on how to operate them, as well as tutorials on different sites. Without becoming an expert in the industry, one may simply discover a variety of examples to replicate and GUI tutorials to do a penetration test. Approval is required to conduct a penetration test on any external system or network. However, one may construct as many virtual computers as he wants on his system and performance testing [36]. Moreover, the security of robots should be ensured through different angles and perspectives. Cybersecurity is also known as the security of devices and the security of information technology. It is the protection of data or device against theft or other harm to the devices, product, or information present on hardware [39]. Hence, Security is all about how well these robots are protected from various types of cyber threats, such as insecure communication, authentication issues, missing authorization, etc [14]. Several major cybersecurity issues were discovered in technology from several suppliers, including Pepper and Nao robots of Softbank Robotics, Alpha 1S robot of UBTECH Robotics, and certain ROBOTIS robots. These robots were created for both corporate and domestic use [12]. As traditional industrial robot applications usually do not include any interaction with the external world, cybersecurity has traditionally been neglected when creating or deploying robots. Yet, with the prevailing situation toward networked robots, a platform that is unsuited for this trend confronts all of the risks associated with networked robots. In general, modern robots are simple targets also for inexpert attackers as cybersecurity accomplishments that are effectively implemented in the IT industry over previous decades, such as proxy servers, protected terminals, or encoded transmission, remain frequently absent from a robotic platform. Furthermore, in roboticist education, a protection approach is rarely addressed [40]. Generally, cybersecurity for robots is based on IT security approaches. Furthermore, there is some robotics expertise that requires further attention [41]. This results in two security-related concerns. First and foremost, robotic systems can be directly controlled. We frequently discover exposed networks or connections in robotics, which an intruder may simply compromise. This is particularly troublesome for robotic systems that travel spontaneously in restricted regions. Furthermore, robots have a substantial influence on the physical security of the individuals in their vicinity. Typically, robot safety rules are highly tight in order to avoid any individual injury caused by a robot. Unfortunately, many of the needed safety-critical systems may be wirelessly assaulted, essentially leaving the safety procedures ineffective [40]. Every cyber-attack in the Robotics industry involves either a terminal point breach or an internet interaction attack. A terminal point breach prevents a supervisor from commanding the robots, but an internet information exchange attack allows the attacker to snoop or implant malware into the network. Accessibility is essentially a basic metric for comparing the intensity of two attack paths. Physical access exploits are substantially more practical than endpoint compromise attempts since they are more network connection reliant [42]. If a robot gets hacked, it can be used by a third party that can take advantage by communicating with the robot through TCP. These people could use 3D cameras and microphones to keep an eye on people. It will affect you in public and private places like airstrips, industrial areas, schools, and also hospitals. The backup device can also simply fake login credentials, access encrypted data of the robot, hack other linked devices, and even physically damage humans. Moreover, a hacked robot that is employed, as in a residential space or, worst, in a public place such as an airport, may have serious negative effects on people's safety, particularly when it is simple to remotely convert it into a weapon that can be used to carry out hostile behavior [43]. A compromised robot might also reveal the robot owner's online platforms, app shops, and cloud services. This implies that an intruder can acquire access to confidential personal information, such as passwords and usernames. Malicious instructions may be sent to robots through smartphone platforms or microcontroller boards. Cell devices might be used to launch assaults on robots; if a user's smartphone is compromised, the robot can also be hacked. Similarly, an

attacker may use a compromised phone to conduct assaults against the owner's cellphone. As many robots use pc operating systems, a number of the threats and weaknesses within these operating systems are also applicable to robotics [12]. The MITM attacks also affect the performance of robotic systems and steal data. It takes place when an attacker is proficient in paying close attention to and eavesdropping on the interaction between two robots or endpoints, altering the message, and injecting it without detection. The attacker can thereby influence the interaction between these lawful entities. System weaknesses include the failure to keep program and system software upgrades, as well as security fixes, up to date to ensure a secure and up-to-current robot system. As a result, there are also setup and database risks [14]. Denial of Service exploits is a form of attack that seeks to deplete a connection until the system fails. These assaults occur when cybercriminals tried to overload a local network using emails till it breaks, generating vital aggravation for customers as well as the capability to use facilities. While DoS attacks use a single targeted system, the attacks employ a "botnet," which is a network of infected computers capable of performing numerous tasks all at once. DDoS attacks are extremely aggravating because they can last anywhere from some days to many weeks, disrupting activities and depriving individuals of access to critical information. These security concerns are now being discussed internally by robot makers and end users, and researchers of both the robotics and cybersecurity areas agree. Robot manufacturers, however, seize the opportunity of a rapidly expanding market and launch their devices there without giving security enough thought [25].

The primary goal of this research is to identify the security vulnerabilities and cybersecurity constraints as well as limitations in robots using different metrics. Furthermore, it proposes an adequate framework of the firewall to protect the robot from these security issues. The contribution of researchers is to test some of the possible vulnerabilities that robots face nowadays. Moreover, it provides a firewall framework to protect the robot from these vulnerabilities.

- Testing is performed to find the vulnerabilities regarding the robot's security
- Different metrics and tools are used to identify and verify the vulnerabilities
- Results are obtained by testing the robot's security
- Firewall framework is given to protect the robot from security vulnerabilities and loopholes

2. LITERATURE REVIEW

Humanoid Robots are supposed to become human friends because they are expected to work in a close relationship as their structure is built-in that way. The advantage of HR is that they can act like a human in any environment and are helpful in different fields [44].

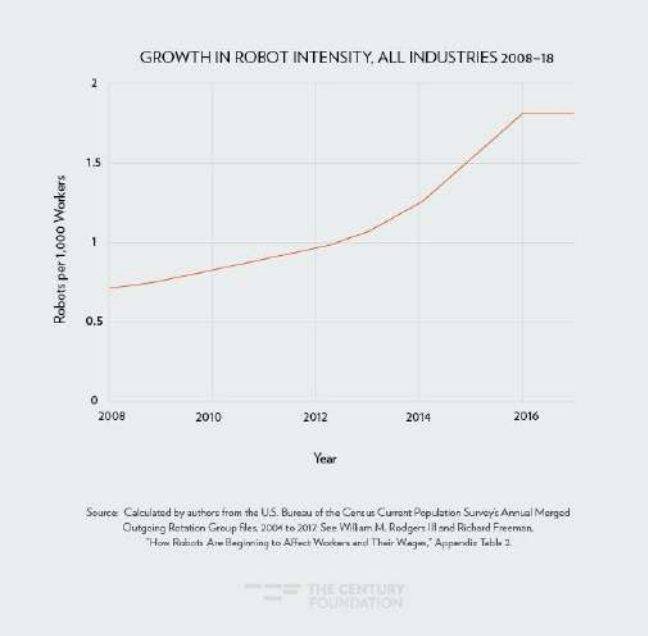


Figure 1 Development of Robot Activity in Environment

A. State-of-Art

HR (Humanoid Robot) is primarily a whole great package, but it contains some downsides. These downsides are referred to as security vulnerabilities. In computers, security also refers to cybersecurity [1]. It is the technique used to protects data and information from unauthorized users, intruders, and hackers. It is a shield that protect data from being theft and stolen. As AI advances, the concept of domestic appliance robotics is turning into a reality. Manipulation methods that might be utilized to specifically target these robots must be extensively researched.

Table 1 Literature Review

Paper Title	Publication Year	Issues and Challenges	Proposed Solution	Gap
A Case Study on the Cybersecurity of Home Appliance Robots [45]	2022	Cybersecurity of robotics	Vulnerability assessment and analysis	Framework for protection of robot from vulnerabilities is needed

Cybersecurity Issues in Robotics [46]	2021	Cyberattacks and threats in Robotics	Just Overview of Countermeasures	Efficient and effective solution is required
Introducing Robot Security Framework [41]	2021	Security and Integrity of Robots	Overview of Robot Security Framework	Testing and Improvement is needed
A new paradigm of threats in robotics behaviors [47]	2021	Intentional and Unintentional Physical Attacks as well as Intentional and Unintentional Programming Attacks	Prevention, Detection and Mitigation	Need solution to avoid Vulnerability problem in robots
Robotics Cybersecurity: Vulnerabilities, Attacks, Countermeasures and Recommendation [14]	2021	major security flaws, risks, concerns, and their consequences, as well as the primary security breaches in the robotics realm	Overview of several threats, vulnerabilities. Moreover, overview of techniques and suggestions against security	Identification of vulnerabilities, Robotic security framework is required
Robot Cybersecurity: A Review [26]	2021	Cybersecurity issues in robotics	Only identification	Need of complete secure architecture
Cybersecurity of Robotic Systems: Leading Challenges and Robotic System Design Methodology [24]	2021	Robotic system cybersecurity	Framework for the robot system security with IoT	Framework that can quickly detect the robotic threats and vulnerabilities
The Cybersecurity and the Care Robots: A Viewpoint on the Open Problems and the Perspectives [48]	2021	Cyberattacks	Only Identification	A suitable countermeasure required
Cybersecurity Attacks on Robotic Platform [49]	2019	Security Vulnerabilities Analysis, attacks on robots, Penetration testing	CIA model	Multistate approach is needed
Robot Hazards: From Safety to Security [25]	2019	Safety and Security of robots	Only identification	Require secure framework for robots against security issues
Adding Salt to Pepper [43]	2018	Security Vulnerability Analysis and Penetration Testing	Identification as well as Limited Countermeasure	Improvement required in countermeasure against robotic vulnerabilities
A Case Study on Cybersecurity of Social Robots [45]	2018	Cybersecurity Vulnerabilities due to lack of Authentication	Only Identification	Adequate countermeasures are required to avoid cybersecurity vulnerabilities
Cybersecurity Risks in Robotics [50]	2018	Cybersecurity risks and threats	Identification of Vulnerabilities and mitigating the threats	Need security framework to overcome the security threats
Hacking Robots Before Skynet [12]	2017	Cybersecurity Vulnerabilities in robotics and cyberattacks	Provided basic recommendation for vendors	Still there is a need of adequate countermeasure

B. Firewalls

To overcome the issues of system security vulnerabilities and cybersecurity attacks, a security mechanism is necessary such as firewalls. A firewall is a critical security component that serves as a separation between internal networking and the outer world. Over the previous four decades, firewall designs have evolved

tremendously. A firewall is a protection system that monitors both outgoing and incoming traffic to find and prevent dangerous data packets based on specified criteria, enabling genuine information to access your private network. Firewalls can be deployed as hardware, software, or frequently your initial protection against threats, attacks, and hackers who try to get a connection to one's company's inner infrastructure [51]. Firewalls are categorized as either software or hardware firewalls, depending on how they are built. Every firewall has a distinct purpose yet performs identical functions. But it is recommended that you have both for better safety [52]. As it is above mentioned that robots came across different vulnerabilities and threats. Therefore, different countermeasures were taken in the past to solve these issues. In this research, researchers have done the testing on the robotic system to find its loopholes. As robots are based on LINUX hence, all testing is done on the LINUX environment. The results of testing showed that a security framework is required to handle the vulnerabilities of the robots. The researchers have provided a firewall framework that will help the robotic systems to be safe and secure from different vulnerabilities and threats.

Table 2 Characteristics of Firewall Types

Firewall	Purpose	Advantage	Disadvantage
Packet-Filtering Firewall	enables packets to travel over the network and manages the way they travel using a set of rules [53]	-effective and fast header filtering -single router is needed	-time consuming -prone to IP spoofing
Stateful Inspection Firewall	monitor how packets of data are routed via firewall and analyzes the status of active connections [54]	-examine packet headers as well as payloads -maintain a record of overall session	-DDoS assaults are possible -there isn't any authentication option
Web Application Firewall	secures online applications by filtration, inspection, and restricting harmful HTTP/S communication, and prevents unauthorized content from exiting the app [55]	-less complex -secures web application	-not much secure -not helpful against other threats
Application Proxy Firewall	protects the network against future attacks by safeguarding the clients identify and other dubious information [52]	-limit connectivity with other networks to keep information secure -maintain user privacy	-Additional setting is required to guarantee total encryption -performance may decrease
Circuit-Level Firewall	monitors connections and encounters at OSI model's session layer [51]	-data encryption and IP protection are provided -examine TCP handshakes	-no data filtering -no application layer protection

3. METHODOLOGY

As robotic systems play such an essential part in people's lives, it is critical to ensure that they are safe and cannot hurt people. Without a question, one of the most crucial notions in our everyday lives is security [56]. To make the robots secure and safe so that they will not have a negative effect on our environment, it is necessary to take suitable countermeasures and do a security assessment of robots.

A. Assessment Methods

A feasible assessment for security issues that appear in any robot or Humanoid Robot is categorized into two parts:

1. Automated Assessment
2. Manual Assessment

In the Automated Assessment section, *Nmap* is used for port scanning. It shows all the open ports which can be used by an attacker to attack our robot or system. Whereas in Manual Assessment, different tools are used as *Ettercap*, *Wireshark,* and *Hydra*. These tools are used to how that user's information can be stolen by unauthorized users and hackers. As robotic systems use Robot Operating Systems (ROS) which are based on Linux [57]. Hence, the testing to check the vulnerability status of a robot is done using Kali Linux and its result can be seen in the "*Results and Discussions"* section. The below flowchart shows the overall scenario of this research and the security assessments:

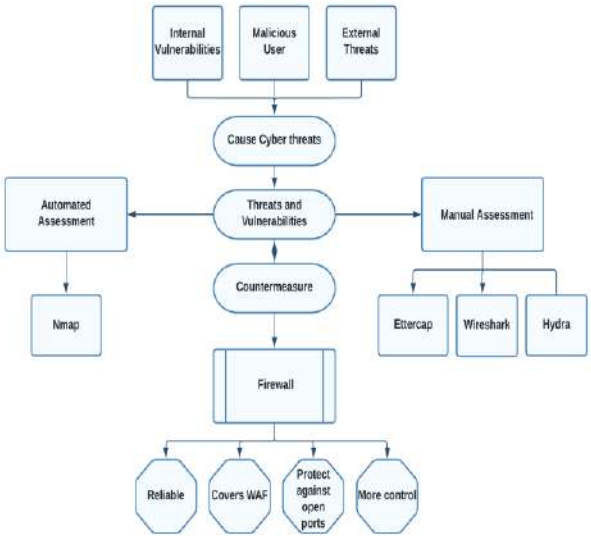


Figure 2 Flowchart of Security Assessment

B. Firewall Configuration

A firewall includes some terms that are used to understand it's working. Some of them are:

IP addresses

Every device on the internet has assigned a unique address known as an IP address. They are made up of 32 bits. A typical IP address looks like this: 216.27.61.137. Such as, if a single IP address just outside of the business reads an unusually large quantity of data from such a host, the firewall may block all communication from and to that address [58].

Protocols

It is the pre-defined means by which someone who wants to use a facility communicates with that facility. The "someone" might be a person, although it is most typically a piece of code or software [58]. A few typical protocols for which investigators can configure firewall filtering include:

IP- known as Internet Protocol. It is the primary method of delivering data through the internet [58].

HTTP- known as Hypertext Transfer Protocol [58]. It is used to build websites and web pages.

TCP- known as Transmission Control Protocol. It is used to separate and change data as it flows through the Internet [58].

UDP- known as User Datagram Protocol. It is used for the content which doesn't necessitate responses, such as broadcasting video and audio files [58].

Ports- A port is a number issued to a connectivity terminal to detect it and deliver data to a certain service. A port is a unitary concept that defines a certain activity or kind of communication service at the system level, in an OS [58].

These terms are used in testing and finding the robot's vulnerabilities (Results and Discussion section). Two major vulnerabilities are found in the robot which can be exploited by the hacker are:

- Open ports on the network: unnecessary ports should be closed or blocked, so that hackers will not be able exploit them and harm the robot
- Login credentials: as robots have a login site inside them and they are connected to computers, so that only authorized persons can give them commands. However, after testing, it was shown that login credentials of the robot are not secure and anyone can steal them.

Following are the steps to secure the robot from these vulnerabilities by using the firewall:

Steps to use a Firewall to Close/Block open ports on the network:

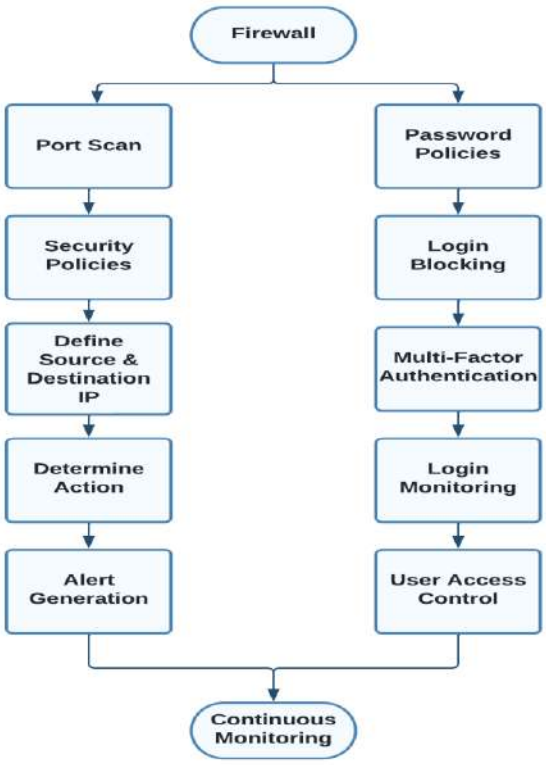
- Conduct a thorough port scanning of all the devices and services on the network to identify which ports are open and need to be closed or blocked.
- Create a security policy on the firewall to block traffic on the open ports. This can be done by configuring the firewall to drop packets that match a specific set of rules.
- Define the source and destination IP addresses and port numbers that the firewall should block, based on the results of the inventory.
- Determine the appropriate action for each port and protocol, such as blocking, logging, or allowing restrictions.
- Configure the firewall to generate alerts when traffic attempts to access blocked ports, to allow for quick response to potential security threats.
- Continuously monitor and update the firewall's security policies and settings to ensure that the network remains secure against new threats.

Steps to use a Firewall to secure Login Credentials:

- Implement strong password policies for all users, including requiring users to use complex passwords and regularly changing them.
- Configure the firewall to block login attempts from known malicious IP addresses or those that have attempted too many failed logins attempts in a short period of time.
- Implement multi-factor authentication (MFA) on the firewall to provide an additional layer of security for login credentials.
- Monitor login attempts and generate alerts for any suspicious activity, such as repeated failed login attempts or login attempts from unexpected locations.
- Implement user access controls and permissions to ensure that users only have access to the resources

they need to do their job.

- Continuously monitor and update the firewall's security policies and settings to ensure that the



network remains secure against new threats.

Figure 3 Working of Firewall

4. RESULTS AND DISCUSSIONS

The security assessment is done in two ways and its results are shown below which shows that robots have security vulnerabilities, and it was necessary to have a theoretical framework to overcome security issues.

A. Automated Assessment

Port Scanning:

First of all, an automated assessment will be done. This is the most essential step to ensure that every system is safe. The actual job starts after that. The term Port Scanning refers to the process of looking for open ports on a network and the services related to these ports. The attacker uses a bogus or fake command [59] to find out the open ports of a network and get information about them through which he can attack quickly. For this purpose, researchers use Nmap (Network Mapping) [60] which acts as a monitor, network scanner [61], or troubleshooter for both TCP and UDP devices. Nmap supports Linux as well as Windows and other operating systems. Nmap working on Windows is relatively more straightforward than Linux. It requires only a few clicks on shown options, but on Linux, a person needs to know sudo commands very well. To open a super user account, these steps need to be followed:

Application --> System --> Root Terminal

For the starter, researchers use the ls command to find the available live host on a network. If this command doesn't show the required network, then the sP or sn command will be used to ping all the addresses on the available network. It

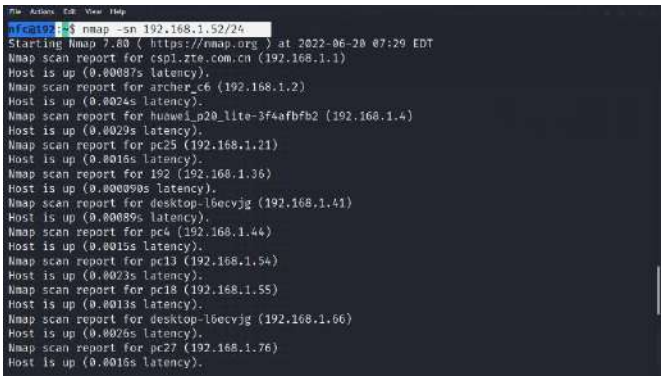


Figure 4 Ping All Connected Live Network Hosts

works well to find available hosts on a network. The *sn* command is used here.

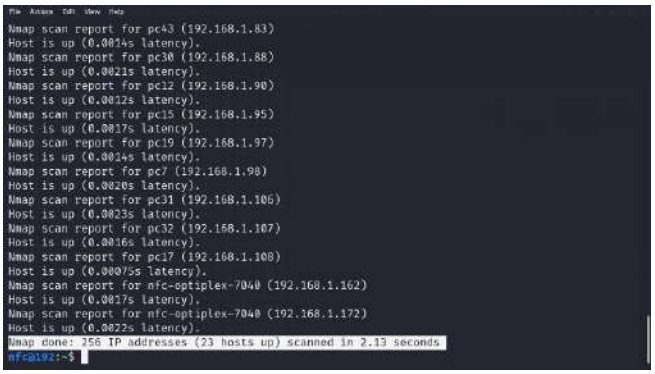


Figure 5 Live Network Host's Result

It became easy to scan all the open ports of available hosts [62]. At last, it shows all the details and status of ports as open, close, or filtered.

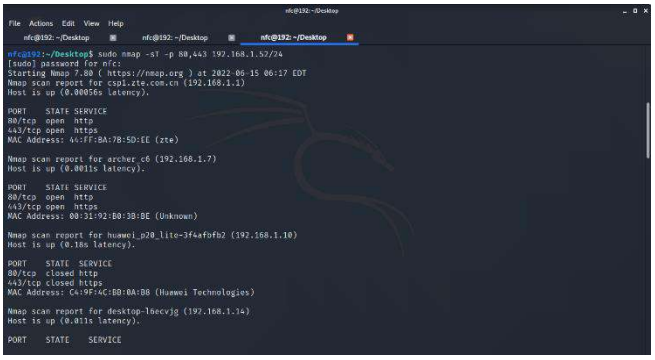


Figure 6 Network Ports Scan Result

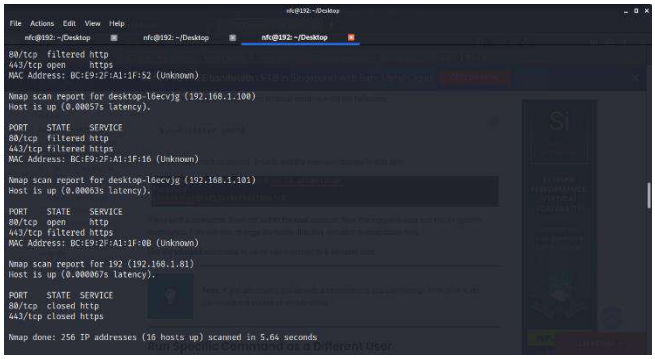


Figure 7 Network Ports Scan On Host

Port scanning results showed different ports. The ports numbers, their purpose and states are shown in the below tables:

Table 3 Port Numbers and Their Purpose

Port No.	***Purpose***
80	-World Wide Web HTTP -allows transmission of data in plain text -It is the standard network port for sending and receiving unfiltered web pages. -Unencrypted connection [63]
443	-Encrypted connection -Secured version of HTTP (HTTPS) -safe connection among the websites and the browser [63]

Table 4 Port Status and Their Purpose

Port States	***Purpose***
Open	shows that the targeted network is accepting connections actively [64]
Close	show that the request was received by the network, however there is no application "listening" to that port [64]
Filtered	show that requested packet has been transmitted but that the server did not reply and is not listening. It refers that the firewall has blocked that specific packet [64]

B. Manual Assessment

After the port scanning technique, a manual assessment should be done. Through port scanning, researchers get primary and logical security information, and in manual assessment, authors will use that information to critically analyze the robot. For this purpose, they will use.

Ettercap and ARP Spoofing:

Ettercap is available free online. This network security tool protects LAN (Local Area Network) from man-in-the-middle attacks (MitM) [65]. In Linux, click on applications, search Ettercap here, and click on it for further use. The primary Ettercap logo will appear on the monitor screen from which the real fun begins. Click on the network interface from the sniff menu and select the current network interface on which sniffing will be performed.

Figure 8 Network Interface of Ettercap

A text will be shown that says the sniffing process has been started. Before moving further on using Ettercap advanced features like MitM, Target, plugins, and host. It is necessary to find the targeted network. For finding out available network host scan is needed.

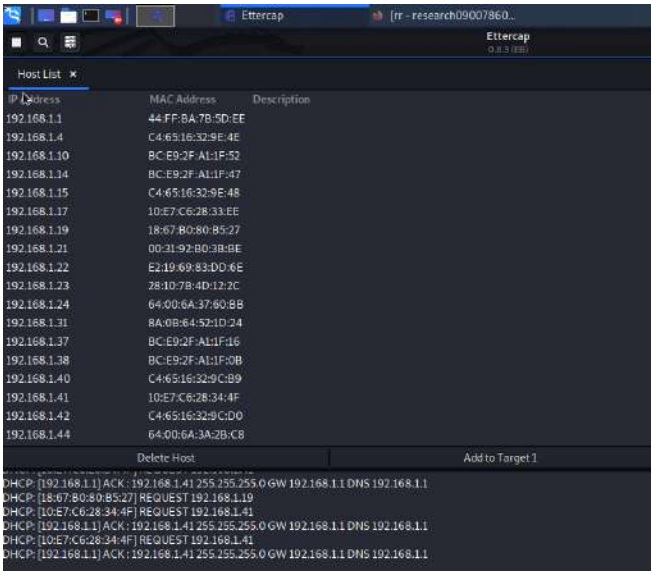


Figure 9 Host Scanning For Available Networks

Host scan will reveal the result of available networks and one can easily snoop into their activities by clicking on the view option. Furthermore, it displays view connection details which show the result of open and closed ports.

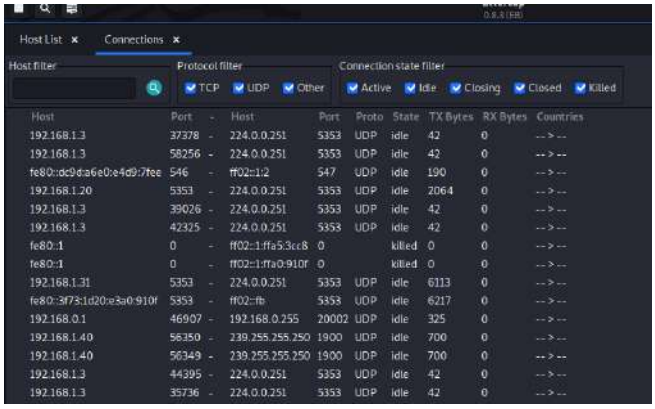


Figure 10 Results of Host Scanning

Now it depends on the user's choice whether he wants to perform MitM, spoofing or he wants to crack the password of available networks.

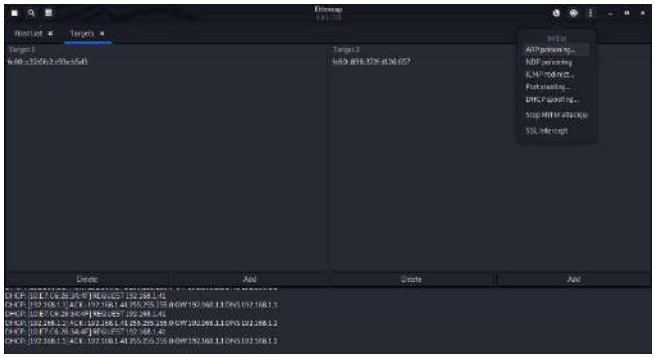


Figure 11 MITM Spoofing and ARP Poisoning

After performing ARP Spoofing, researchers cracked password and login credentials.

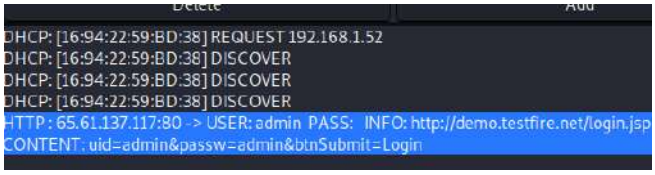


Figure 12 ARP Spoofing Results

ARP, which stands for Address Resolution Protocol also known as ARP poisoning. Attackers use this method to send spoof messages over LAN. This is most probably used to attack the MAC Address of the host [66].

Wireshark:

Like the ARP technique, there is another process used to analyze the network traffic and store data for offline analysis. This tool is named Wireshark [67]. Wireshark help in capturing network packets and show detailed data about that specific packet as much as it can [68]. Wireshark can easily be accessed in the application of Kali Linux. It is considered one of the best security tools of Kali Linux.

Moreover, it can be accessed by using the command prompt. To start working on this tool, simply click on Wireshark. It opens a welcoming window of Wireshark.

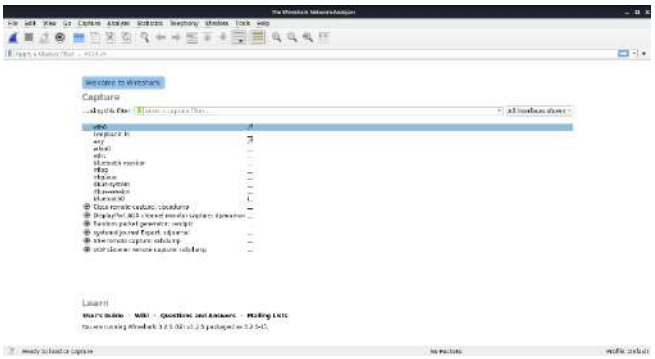


Figure 13 Wireshark Interface

It is quite easy to use, just choose desired network packet and start the process of capturing the details of that packet. Attackers use this software and crack info like usernames, passwords, and even users' bank balance information and use this info for their good.

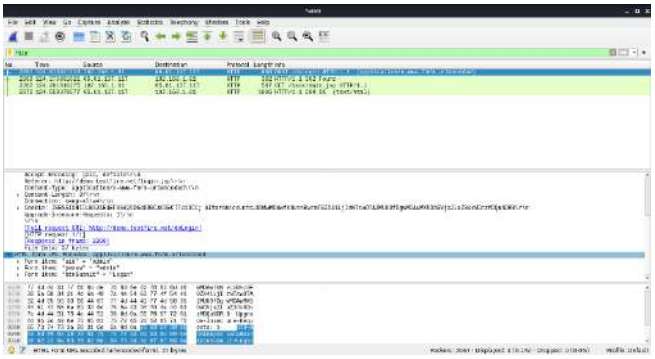


Figure 14 Scanning Results of Wireshark

Hydra:

A brute force attack was performed on a robot to check whether it had a secure system against the attack. For this purpose, Hydra is used, which is a dictionary attack tool, and researchers find out that after 1 to 5 minutes, any intruder can easily access the password and login information. Just like Wireshark, Hydra is also available in Linux beforehand. There is no need for any type of installation. Hydra [69] is present in two modes in Linux. It is Graphical and in Command form. For Graphical Interface, click on applications or type hydra. After that, select the Hydra *gtk* version. A window will appear.

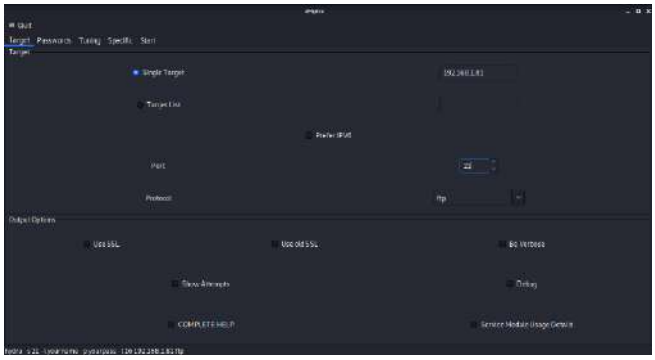


Figure 15 Graphical Interface of Hydra

Hydra allows login crack tool on a single target network, even on a target list that contains available networks in a system, and selects the desired port to find vulnerabilities. After that, select the preferred protocol for brute force attack. Set details about the username and password from the username and password list. Start the process by clicking on the start button after filling out all the required options. Wireshark provides an option to start and stop the attack and a save option.

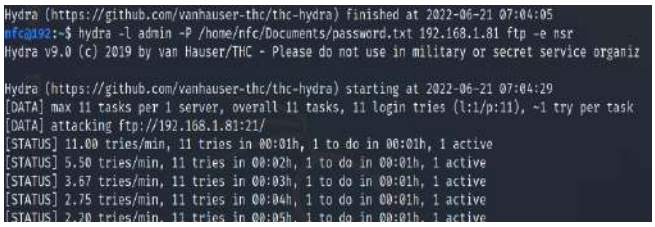


Figure 16 Password Cracking Process

Result will be shown like:

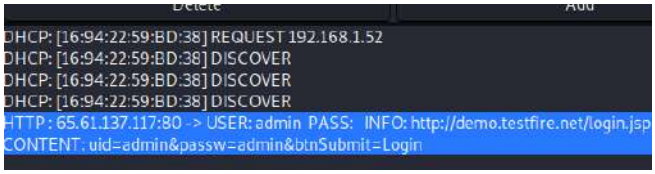


Figure 17 Password Cracking Result

It can be prevented by working in some common ways. They are:

- Enforcing a strong password of at least 9 to 13 characters, especially those with special characters.
- By installing Anti-Brute force Tool and by maintaining it too.
- And the most critical limit is connection rates because it prevents attack on a network.

The overall testing is done and their results are shown in the pictures. Hence, it is proved that the humanoid robots have some vulnerabilities which needs to be addressed. To make it more authentic and clear to understand, all the findings are discussed in the below table.

Table 5 Results of Assessment Methods

Assessment Method	***Tool***	***Purpose***	***Result***
Automated Assessment	Nmap	Port scanning	Shows open ports
Manual Assessment	Ettercap and ARP Spoofing	Used to analyze network traffic and to get access to user's login credentials	Shows login credentials as username and password
	Wireshark	To get detailed information about specific data and to access login information	Shows detailed information about specific data as well as login information
	Hydra	For cracking password	Shows password of the user

In the literature review, we have talked about different types of firewalls, their working and how efficient they are. In the methodology section, we have provided a firewall that will be helpful with robotic vulnerabilities as issues regarding open ports, and securing the login credentials of the user. Hence, the below table shows that our proposed firewall is better than the others as it keeps the robot safe from such loopholes.

Table 6 Comparison of Firewall Types

Packet Filtering Firewall	***Stateful Inspection Firewall***	***Web Application Firewall***	***Application Proxy Firewall***	***Next Generation Firewall (proposed firewall)***
simplest	Complex	Less complex	More complex	Less complex than other firewalls
basic	Better than Packet Filtering Firewall	basic	Better than stateful Inspection Firewall	advanced
Works at Network layers of	Works at Networ	Works at Applic	Works at Application layer	Works at Application layer of

OSI model	k layers of OSI model	ation layer of OSI model	of OSI model	OSI model but also monitor network traffic from layer1 to layer 7
Not particularly secure	Not efficient when it comes to exploiting stateless protocols	Only secure for web pages	Moderate security	Highly secure
Only effective for packet filtering	Vulnerable to DDoS attacks	Secure web pages	Less encryption	Covers deep inspection, spam filtering as well as includes features of different firewalls

5. CONCLUSION:

The robotics business is fast growing. Robots are being used in almost every aspect of our lives. Yet, the security of robots is still a concern. As robots are being a part of our daily life as well as their usage is increasing in different industries, hence it is necessary to highlight and overcome their security issues. It is important to make robots safer for mankind. Some of the causes for this is a lack of paperwork to assess the security of robots. We discovered that this issue exists in other growing security fields as well. In this thesis, we have performed different security assessments to check the security of robots. Furthermore, we have used different tools to analyze the vulnerabilities in the robots which can be exploited by the attacks and can affect the working of the robot.

The researchers also provided a firewall framework against those security vulnerabilities of the robot. The firewall framework will be helpful to make the robot secure and tells us how to handle the loopholes in robots regarding its security. This work is important as it gives a new and different approach to handle the vulnerabilities in robotics as well as it covers both aspects of network vulnerabilities and webpage vulnerability issues in humanoid robots. More work can be done in this field to combine some other robotic vulnerabilities and threats and make a framework that is more advanced and handle more security issues in the robots.

CREDIT AUTHOR STATEMENT

Safa Munir: Conceptualization, Methodology, Software **Kashaf Khan**: Visualization, Investigation. ***Dr Naeem Aslam:*** Supervision.**: Mustajeeb-ur-Rehman**: Software, Validation.: **Kamran Abid:** Writing- Reviewing and Editing

COMPLIANCE WITH ETHICAL STANDARDS

It is declare that all authors don't have any conflict of interest. Furthermore, informed consent was obtained from all individual participants included in the study.

REFRENCES

[1] Kaspersky, "What is Cyber Security? | Definition, Types, and User Protection," *AO Kaspersky Lab*. 2022. [Online]. Available: https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

[2] A. Lane, "What is technology? - OpenLearn - Open University," *OpenLearn*. 2019. [Online]. Available: https://www.open.edu/openlearn/science-maths-technology/engineering-and-technology/technology/what-technology

[3] Aiden Ford, "Technology Types & Uses | What is Technology? - Video & Lesson Transcript | Study.com," *Study.com*. 2021. [Online]. Available: https://study.com/academy/lesson/what-is-technology-definition-types.html

[4] P. Forbrig, "Challenges in multi-user interaction with a social humanoid robot pepper," *CEUR Workshop Proc*, vol. 2503, pp. 10–17, 2019.

[5] M. Chui, J. Manyika, and M. Miremadi, "Where machines could replace humans-and where they can't (yet)," *McKinsey Quarterly*, vol. 2016, no. 3, pp. 58–69, 2016.

[6] A. Zelinsky, "Robots at work," *Springer Handbook of Robotics*, pp. 1381–1384, 2016, doi: 10.1201/9781003214892-41.

[7] C. Breazeal, "Emotion and sociable humanoid robots," *International Journal of Human Computer Studies*, vol. 59, no. 1–2, pp. 119–155, 2003, doi: 10.1016/S1071-5819(03)00018-1.

[8] IEEE, "IEEE Robotics and Automation Society," *IEEE Transactions on Robotics*, vol. 33, no. 5. IEEE, pp. C3–C3, 2017. doi: 10.1109/tro.2017.2755362.

[9] T. Kanda, M. Shiomi, Z. Miyashita, H. Ishiguro, and N. Hagita, "An Affective Guide Robot in a Shopping Mall," *Human-Robot Interaction in Social Robotics*, pp. 52–74, 2017.

[10] G. Trovato, A. Lopez, R. Paredes, and F. Cuellar, "Security and guidance: Two roles for a humanoid robot in an interaction experiment," *RO-MAN 2017 - 26th IEEE International Symposium on Robot and Human Interactive Communication*, vol. 2017-Janua, pp. 230–235, 2017, doi: 10.1109/ROMAN.2017.8172307.

[11] World Robotics, "Executive Summary - World Robotics (Industrial & Service Robots) 2016," *World Robotic Report - Executive Summary*, pp. 11–18, 2016.

[12] C. Cerrudo, "Hacking Robots Before Skynet 1," *Cybersecurity Insight*, pp. 1–17, 2017.

[13] L. Pagliarini and H. H. Lund, "The future of Robotics Technology," *Proceedings of International Conference on Artificial Life and Robotics*, vol. 22, no. January 2017, pp. 29–32, 2017, doi: 10.5954/icarob.2017.is-1.

[14] J. P. A. Yaacoub, H. N. Noura, O. Salman, and A. Chehab, "Robotics cyber security: vulnerabilities, attacks, countermeasures, and recommendations," *Int J Inf Secur*, vol. 21, no. 1, pp. 115–158, 2022, doi: 10.1007/s10207-021-00545-8.

[15] R. A. Beasley, "Medical Robots: Current Systems and Research Directions," *Journal of Robotics*, vol. 2012, pp. 1–14, 2012, doi: 10.1155/2012/401613.

[16] J. Rosen and B. Hannaford, "Doc at a distance," *IEEE Spectr*, vol. 43, no. 10, pp. 34–39, 2006, doi: 10.1109/MSPEC.2006.1705774.

[17] F. A. Auat Cheein and R. Carelli, "Agricultural robotics: Unmanned robotic service units in agricultural tasks," *IEEE Industrial Electronics Magazine*, vol. 7, no. 3, pp. 48–58, 2013, doi: 10.1109/MIE.2013.2252957.

[18] B. Young, "The First 'Killer Robot' Was Around Back in 1979." 2018. [Online]. Available: https://science.howstuffworks.com/first-killer-robot-was-around-back-in-1979.htm

[19] R. Whymant, "From the archive, 9 December 1981: Robot kills factory worker | Japan," *The Guardian*. 2014. [Online]. Available: https://www.theguardian.com/theguardian/2014/dec/09/robot-kills-factory-worker

[20] O. Shyvakov and S. Maas, "Developing a security framework for robots," no. August, 2017, [Online]. Available: http://essay.utwente.nl/73371/1/Shyvakov_MA_EEMCS.pdf

[21] Canonical Ltd, "What is ROS? | Ubuntu." [Online]. Available: https://ubuntu.com/robotics/what-is-ros

[22] E. F. Villaronga, C. Millard, and Q. Mary, "Queen Mary University of London , School of Law Cloud Robotics Law and Regulation," no. January 2019, 2018, doi: 10.13140/RG.2.2.32883.17446.

[23] A. Tapus, J. Fasola, and M. J. Mataric, "Socially assistive robots for individuals suffering from dementia," *ACM/IEEE 3rd Human-Robot Interaction International Conference, Workshop on Robotic Helpers: User Interaction, Interfaces and Companions in Assistive and Therapy Robotics*, p. 3, 2008, [Online]. Available: https://robotics.usc.edu/publications/media/uploads/pubs/577.pdf%0Ahttp://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.124.7109&rep=rep1&type=pdf

[24] V. Dutta and T. Zielińska, "Cybersecurity of robotic systems: Leading challenges and robotic system design methodology," *Electronics (Switzerland)*, vol. 10, no. 22, pp. 1–24, 2021, doi: 10.3390/electronics10222850.

[25] L. A. Kirschgens, I. Z. Ugarte, E. G. Uriarte, A. M. Rosas, and V. M. Vilches, "Robot hazards: from safety to security," 2018, [Online]. Available: http://arxiv.org/abs/1806.06681

[26] V. Mayoral-Vilches, "Robot cybersecurity, a review," *International Journal of Cyber Forensics and …*, vol. x, pp. 1–19, 2022, [Online]. Available: https://conceptechint.net/index.php/CFATI/article/view/41%0Ahttps://conceptechint.net/index.php/CFATI/article/download/41/16

[27] E. B. Fernandez, "A methodology for secure software design," *Proceedings of the International Conference on Software Engineering Research and Practice, SERP'04*, vol. 1, no. January 2004, pp. 130–136, 2004.

[28] P. H. Meland and J. Jensen, "Secure software design in practice," *ARES 2008 - 3rd International Conference on Availability, Security, and Reliability, Proceedings*, pp. 1164–1171, 2008, doi: 10.1109/ARES.2008.48.

[29] E. Fosch-Villaronga and T. Mahler, "Cybersecurity, safety and robots: Strengthening the link between cybersecurity and safety in the context of care robots," *Computer Law and Security Review*, vol. 41, p. 105528, 2021, doi: 10.1016/j.clsr.2021.105528.

[30] A. Laitinen, M. Niemelä, and J. Pirhonen, "Demands of dignity in robotic care: Recognizing Vulnerability, Agency, and Subjectivity in Robot-based, Robot-assisted, and Teleoperated Elderly Care," *Techne: Research in Philosophy and Technology*, vol. 23, no. 3, pp. 366–401, 2019, doi: 10.5840/techne20191127108.

[31] H. Choi, S. Kate, Y. Aafer, X. Zhang, and D. Xu, "Cyber-Physical Inconsistency Vulnerability Identification for Safety Checks in Robotic Vehicles," *Proceedings of the ACM Conference on Computer and Communications Security*, pp. 263–278, 2020, doi: 10.1145/3372297.3417249.

[32] Ö. Aslan and R. Samet, "Mitigating cyber security attacks by being aware of vulnerabilities and bugs," *Proceedings - 2017 International Conference on Cyberworlds, CW 2017 - in cooperation with: Eurographics Association International Federation for Information Processing ACM SIGGRAPH*, vol. 2017-Janua, pp. 222–225, 2017, doi: 10.1109/CW.2017.22.

[33] Wikipedia, "Penetration test - Wikipedia," *Wikipedia*. [Online]. Available: https://en.wikipedia.org/wiki/Penetration_test

[34] P. S. Shinde and S. B. Ardhapurkar, "Cyber security analysis using vulnerability assessment and penetration testing," *IEEE WCTFTR 2016 - Proceedings of 2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare*, 2016, doi: 10.1109/STARTUP.2016.7583912.

[35] M. R. Reddy and P. Yalla, "Mathematical analysis of penetration testing and vulnerability countermeasures," *Proceedings of 2nd IEEE*

International Conference on Engineering and Technology, ICETECH 2016, no. March, pp. 26–30, 2016, doi: 10.1109/ICETECH.2016.7569185.

[36] M. Denis, C. Zena, and T. Hayajneh, "Penetration testing: Concepts, attack methods, and defense strategies," *2016 IEEE Long Island Systems, Applications and Technology Conference, LISAT 2016*, 2016, doi: 10.1109/LISAT.2016.7494156.

[37] P. Vats, M. Mandot, and A. Gosain, "A Comprehensive Literature Review of Penetration Testing Its Applications," *ICRITO 2020 - IEEE 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)*, pp. 674–680, 2020, doi: 10.1109/ICRITO48877.2020.9197961.

[38] F. Holik, J. Horalek, O. Marik, S. Neradova, and S. Zitta, "Effective penetration testing with Metasploit framework and methodologies," *CINTI 2014 - 15th IEEE International Symposium on Computational Intelligence and Informatics, Proceedings*, pp. 237–242, 2014, doi: 10.1109/CINTI.2014.7028682.

[39] Bartleby, "Cyber Security _ Security And Security - 1880 Words _ Bartleby."

[40] Q. Zhu, S. Rass, B. Dieber, and V. M. Vilches, "Cybersecurity in Robotics: Challenges, Quantitative Modeling, and Practice," *Foundations and Trends® in Robotics*, vol. 9, no. 1, pp. 1–129, 2021, doi: 10.1561/2300000061.

[41] V. M. Vilches *et al.*, "Introducing the Robot Security Framework (RSF), a standardized methodology to perform security assessments in robotics," no. August, 2018, [Online]. Available: http://arxiv.org/abs/1806.04042

[42] R. Kumar, P. K. Pattnaik, and P. Pandey, "Detecting and mitigating robotic cyber security risks," *Detecting and Mitigating Robotic Cyber Security Risks*, no. March 2017, pp. 1–384, 2017, doi: 10.4018/978-1-5225-2154-9.

[43] A. Giaretta, M. De Donno, and N. Dragoni, "Adding salt to pepper a structured security assessment over a humanoid robot," *ACM International Conference Proceeding Series*, 2018, doi: 10.1145/3230833.3232807.

[44] Ashutosh Bhatt, "Humanoid Robots: An Overview," *Humanoid Robots: An overview*. 2011. [Online]. Available: https://www.engineersgarage.com/humanoid-robots-an-overview/%0Ahttps://www.engineersgarage.com/articles/humanoid-robots

[45] J. Miller, A. B. Williams, and D. Perouli, "A Case Study on the Cybersecurity of Social Robots," *ACM/IEEE International Conference on Human-Robot Interaction*, no. May, pp. 195–196, 2018, doi: 10.1145/3173386.3177078.

[46] G. Lacava *et al.*, "Cybsersecurity issues in robotics," *J Wirel Mob Netw Ubiquitous Comput Dependable Appl*, vol. 12, no. 3, pp. 1–28, 2021, doi: 10.22667/JOWUA.2021.09.30.001.

[47] M. Colledanchise, "Address behaviour vulnerabilities in the next generation of autonomous robots," *Nat Mach Intell*, vol. 3, no. 11, pp. 927–928, 2021, doi: 10.1038/s42256-021-00415-x.

[48] D. Giansanti and R. A. Gulino, "The cybersecurity and the care robots: A viewpoint on the open problems and the perspectives," *Healthcare (Switzerland)*, vol. 9, no. 12, pp. 1–12, 2021, doi: 10.3390/healthcare9121653.

[49] A. Bhardwaj, V. Avasthi, and S. Goundar, "Cyber security attacks on robotic platforms," *Network Security*, vol. 2019, no. 10, pp. 13–19, 2019, doi: 10.1016/S1353-4858(19)30122-9.

[50] I. Priyadarshini, "Cyber security risks in robotics," *Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications*, no. April, pp. 1235–1250, 2018, doi: 10.4018/978-1-5225-5634-3.ch061.

[51] G. Bonuccelli, "What Are the Basic Types of Firewalls?," *Parallels*. 2020. [Online]. Available: https://www.parallels.com/blogs/ras/types-of-firewalls/

[52] Javatpoint, "Types of Firewall - javatpoint." [Online]. Available: https://www.javatpoint.com/types-of-firewall

[53] Intellipaat, "What is Packet Filtering Firewall?" 2021. [Online]. Available: https://intellipaat.com/blog/packet-filtering-firewall/#no3

[54] GeeksforGeeks, "Types of Network Firewall - GeeksforGeeks." 2021. [Online]. Available: https://www.geeksforgeeks.org/types-of-network-firewall/

[55] Positive Technologies, "What is a Web Application Firewall (WAF): Definition & Guide," *Positive Technologies*. 2019. [Online]. Available: https://www.ptsecurity.com/ww-en/analytics/knowledge-base/waf-web-application-firewall/

[56] M. Simonyi, "What Is Security?," *Securing Windows NT/2000*, no. November, 2002, doi: 10.1201/9781420031461.ch2.

[57] J. C. (FORMERLY U. PLATFORM, "What Is ROS and Why It's Needed - JFrog Connect."

[58] P. Chakraborty, Md. Zahidur, and S. Rahman, "Building New Generation Firewall Including Artificial Intelligence," *Int J Comput Appl*, vol. 178, no. 49, pp. 1–7, 2019, doi: 10.5120/ijca2019919416.

[59] M. S. Kumar, J. Ben-Othman, K. G. Srinivasagan, and G. U. Krishnan, "Artificial Intelligence Managed Network Defense System against Port Scanning Outbreaks," *Proceedings - International Conference on Vision Towards Emerging Trends in Communication and Networking, ViTECoN 2019*, pp. 1–5, 2019, doi: 10.1109/ViTECoN.2019.8899380.

[60] nmap.org, "Nmap: the Network Mapper - Free Security Scanner," *Https://Nmap.Org/*. p. 1, 2021. [Online]. Available: https://nmap.org/

[61] N. El-nazeer and K. Daimi, "Evaluation of Network Port Scanning Tools," *Citeseer*, p. 1, 2011, [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.217.9175&rep=rep1&type=pdf%0Ahttp://docplayer.net/8252039-Evaluation-of-network-port-scanning-tools.html

[62] R. Turner, "A Practical Guide to Nmap (Network Security Scanner) in Kali Linux." 2016. [Online]. Available: https://www.tecmint.com/nmap-network-security-scanner-in-kali-linux/

[63] "Port 80 (tcp/udp)." [Online]. Available: https://www.speedguide.net/port.php?port=80

[64] Avast, "What is port scanning and how does it work? | Avast," *Avast*. [Online]. Available: https://www.avast.com/business/resources/what-is-port-scanning#pc%0Ahttps://www.avast.com/en-gb/business/resources/what-is-port-scanning

[65] E. Project, "ettercap."

[66] Radware, "ARP Poisoning."

[67] W. Foundation, "WiresharkÂů Go Deep," *Accessed*. [Online]. Available: https://www.wireshark.org

[68] V. KUMAR, "Using Wireshark filter ip address and port in Kali Linux 2021."

[69] sectools.org, "THC Hydra – SecTools Top Network Security Tools," *Internet*. 2016. [Online]. Available: http://sectools.org/tool/hydra/