ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

NEUMANN JÁNOS
FACULTY OF INFORMATICS

THESIS

OE-NIK Student's name: **Mousa, Ammar Abdulzahra**

2022 Student's registration number: **T/008802/FI120904/N**

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

NEUMANN JÁNOS
FACULTY OF INFORMATICS

Proactive Communication Threat Monitoring for Cloud Android

OE-NIK	Student's name:	**Mousa, Ammar Abdulzahra**
2022	Student's registration number:	**T/008802/FI120904/N**

Óbuda University
John von Neumann Faculty of Informatics
Institute of Biomatics and Applied Artificial Intelligence

DIPLOMA THESIS
TOPIC DESCRIPTION

Student name: **Ammar Abdulzahra Mousa**
Registration number: T/008802/FI12904/N
Neptun's code: [redacted]

Title of diploma thesis:

Proactive communication threat monitoring for cloud androids
Proaktív kommunikációs fenyegetésmonitorozás felhő alapú androidokhoz

Internal supervisors: Bence Tureczki, Dr. Katalin Szenes
External supervisor

Deadline: 15th of December, 2022

Topic description:

With the era of 5G and IoT, the development of computing and communication technologies arose the need to investigate the difficulties of the applications of different robots. The enormous computing capacity that is typically needed either by the 5G or by the IoT made it necessary to move the thinking systems of robots up into the cloud. We have chosen android robots as their thinking systems are more complex than those of the other robots.
Thus, the domain of the threats is partially moved up into the cloud, too. Having classified these threats, we can choose the most significant ones. Based on the professional literature, we have to find ways to monitor them.
This thesis will develop a proactive threat monitoring system to monitor and collect these threats.

The diploma thesis should cover:

- overview of the Security Information and Event Management (SIEM) systems,
- modeling an android communication network,
- build a cloud-based monitoring system to monitor and detect threats
  - system plan,
  - programming,
  - testing,
- results analysis & discussion,
- conclusion,
- upgrade options.

Ph.

ÓBUDAI EGYETEM * Neumann János Informatikai Kar. * 1. Budapest

.....
Dr. György Eigner
head of institute

Term of limitation: **15th of December, 2024.**

The diploma thesis is adequate and can be submitted:

.....
external supervisor

.....
Bence Tureczki
internal supervisor

.....
Dr. Katalin Szenes
internal supervisor

STUDENT'S DECLARATION

I the undersigned student hereby declare that this thesis is the result of my own work; I have disclosed the references and tools used in an identifiable manner.

The results indicated in my thesis completed may be used by the university and the institution announcing the task for their own purposes free of charge.

Dated: Budapest, 07.05.2022.

Mousa, Ammar Abdulzahra

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Neumann János Faculty of Informatics

Annex 9

CONSULTATION LOG

Student's name: Mousa Ammar Abdulzahra

Neptun code: [redacted]

Specialty: Computer Science Engineering

Phone number:

Mailing address (e.g. domicile): [redacted]

Degree project / thesis[1] title in Hungarian:

Proaktív kommunikációs fenyegetésmonitorozás felhő alapú androidokhoz

Degree project / thesis[2] title in English:

Proactive Communication Threat Monitoring for Cloud Androids

Institutional supervisors:

Dr. Katalin Szenes, Bence Tureczki

Please write the data in printed capital letters!

Occ.	Date	Content	Signature
1.	13/9/2021	Comparing AI-based communication design technologies	
2.	22/10/2021	Choosing a suitable Integrated Development Environment (IDE) for humanoid robot communication	
3.	27/10/2021	Elaborating the system plan and the test plans of the communication system to be developed	
4.	3/11/2021	Plan the configuration of the communication system to be developed for effective threat monitoring	

The Consultation log is required to be countersigned by either supervisor on a total of 4 occasions of consultation.

The student has complied with the requirements of the subject titled Degree project I / Degree project II (BSc) or Thesis 1 / Thesis 2 / Thesis 3 / Thesis 4[3], and is allowed to proceed for reporting / defense[4].

Dated: Budapest, December 15,..... 2021.....

.....

institutional supervisor

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Neumann János Faculty of Informatics

CONSULTATION LOG

Student's name: Mousa Ammar Abdulzahra

Neptun code: [redacted]

Specialty: Computer Science Engineering

Phone number:

Mailing address (e.g. domicile):

[redacted]

Degree project / thesis[1] title in Hungarian:

Proaktív kommunikációs fenyegetésmonitorozás felhő alapú androidokhoz

Degree project / thesis[2] title in English:

Proactive Communication Threat Monitoring for Cloud Androids

Institutional supervisor:

Dr. Katalin Szenes, Bence Tureczki

Please write the data in printed capital letters!

Occ.	Date	Content	Signature
1.	24/11/2021	TRANSACTION MANAGEMENT OF SCHEDULED TASKLISTS FOR HYBRID CLOUD ARCHITECTURES	
2.	1/12/2021	CUSTOMIZATION OPTIONS OF 3RD PARTY APPLICATION PROGRAMMING INTERFACES (APIS)	
3.	8/12/2021	EVALUATION OF THE EFFICIENCY OF CLOUD COMMUNICATION PROTOCOLS	
4.	15/12/2021	REVIEW OF MODERN PRESENTATION TOOLS AND TECHNIQUES	

The Consultation log is required to be countersigned by either supervisor on a total of 4 occasions of consultation.

The student has complied with the requirements of the subject titled Degree project I / Degree project II (BSc) or Thesis 1 / Thesis 2 / Thesis 3 / Thesis 4[3], and is allowed to proceed for reporting / defense[4].

Dated: Budapest, ... 2021.12.15.....

.....

institutional supervisor

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Neumann János Faculty of Informatics

CONSULTATION LOG

Student's name:	Neptun code:	Specialty:
Mousa Ammar Abdulzahra	[redacted]	Computer Science Engineering

Phone number: Mailing address (e.g. domicile):

[redacted]

Degree project / thesis[1] title in Hungarian:

Proaktív kommunikációs fenyegetésmonitorozás felhő alapú androidokhoz

Degree project / thesis[2] title in English:

Proactive Communication Threat Monitoring for Cloud Androids

Institutional supervisor:

Dr. Katalin Szenes, Bence Tureczki

Please write the data in printed capital letters!

Occ.	Date	Content	Signature
1.	7/2/2022	COMPARISON OF CLOUD EXPLOIT ENGINES	
2.	21/2/2022	ASSESSMENT OF BOT DEVELOPMENT PLATFORMS	
3.	28/2/2022	EVALUATION OF METALANGUISTIC TOOLS	
4.	7/3/2022	MULTIDIMENSIONAL VISUALIZATION OF THE RESULTS	

The Consultation log is required to be countersigned by either supervisor on a total of 4 occasions of consultation.

The student has complied with the requirements of the subject titled Degree project I / Degree project II (BSc) or Thesis 1 / Thesis 2 / Thesis 3 / Thesis 4[3], and is allowed to proceed for reporting / defense[4].

Dated: Budapest, ... 2022.05.06.....

.....

institutional supervisor

Abstract:

The study of proactive threat monitoring is a promising field of interest as it has great potential for communication network services in sectors like the commercial marketplace, government, military, and so on. From an economic, human resources, and sustainability standpoint, many enterprises and organizations are beginning to turn to the transition of their network infrastructures into cloud computing environments. IT (Information Technology) solutions offered by cloud computing companies promise to be more secure than those offered by other providers. Obviously, cloud computing protects computers from physical theft, but there are other critical considerations to address as well. It is the responsibility of cloud suppliers and customers to work together to ensure the security of their data in the cloud. "Azure by Microsoft, which holds the slogan of Invent with purpose, has become one of the most famous and biggest cloud computing providers" [1]. Azure has engaged a huge number of businesses and individuals to its services over the last few years. The security-related risks of the Azure cloud computing adoption can be crucial. To address these issues, a cost-effective and efficient monitoring solution is needed. The goal of this Thesis is to build such a threat monitoring system for the reconciliation of the occurrence of the most dangerous attacks against the androids. In the Thesis, we discuss threat monitoring using the android robot as an example. This involves the use of different IoT (Internet of Things) systems as components of the robots. In order to approach the human appearance, we put our robot into a cloud wireless environment. Because cyber-attacks are becoming more sophisticated, it is more important than ever to defend enterprise wireless networks and information systems. A threat monitoring system must be able to monitor enormous amounts of data generated from networks and identify threats. There is a growing interest in cloud computing solutions, but many businesses may not be aware of wireless security dangers and their potential integration with cloud computing security for vital systems. So, we discuss the most important aspects of wireless technology and its evolution here, too. In testing our proactive monitoring system against threats and vulnerabilities, we will depend on the exploit databases (Exploit Pack, Exploit Database and Rapid7) to test it. The exploit databases are a great tool for finding potential network vulnerabilities and keeping up with existing network attacks. The findings of my thesis during test our systems claims that the average time to fix the vulnerabilities in these exploits was 500 seconds for high, about the same for medium, and 650 seconds for low severity vulnerabilities. The average time involved the collection and reverse engineering of exploits, the download, and installation of the fixes, and the rescanning of the system components. In comparison, the manual collection of the same vulnerabilities took 8 working hours. The manual installation of the patches cost another 8 working hours. So, the AI (Artificial Intelligence) supported version was better in order of magnitude. Furthermore, during the manual process, several human errors were detected such as forgotten documentation, or downloading the wrong version of the patch.

The environmental factors and structure of the research:

Since over a decade ago, the majority of Internet-connected devices were PCs with a wired Internet connection. Nowadays, With the revolution of IoT and it is considered to be the future of Internet, no one is surprised that" things" communicate between themselves or connect to the Internet [2]. Android Robotic Sensor Networks, which are widely employed in the military, industry, agriculture, and health care, have grown in popularity as wireless networks and cloud systems have become more widely used. Even while these networks have become increasingly popular, they have also become targets for cyberattacks because of the valuable or essential data they carry. With the advancement of sensors, devices and algorithms in Robotics, new users are being brought from outside its traditional industrial and academic sectors. Robots to be utilized by more people, they must be able to connect with user devices (such as computers, tablets, smartphones, and smartwatches) to monitor, programming, and control tasks. IoRT (Internet of Robot Things) attempts to utilize recent communication technology in order to establish this connection. A major consideration for researchers and workers in this scenario is having access to robot software that works with a variety of user resources (devices and software). When it comes to robotics programming and application development, however, most academic software and distributed frameworks use Linux-based desktop OS (Operating Systems), such as Ubuntu.

It is becoming increasingly important to evaluate the security risks associated with the rapid growth of IoT applications as robotic sensors and devices become part of the Internet infrastructure. As more and more things become interconnected via the Internet, the severity of these problems will rise. The increased worldwide exposure to the Internet will actually expose more security problems. A hacker might exploit these security problems to get access to billions of IoT devices in an uncontrolled environment. When it comes to hacking and other forms of cybercrime the Internet of Things IoT will raise the number of attack surfaces.

"A study conducted by Hewlett Packard revealed that 70% of the most commonly used IoT devices contain serious vulnerabilities" [3]." IoT devices are vulnerable to security threats due to their design by lacking certain security features such as insecure communication medium, insufficient authentication and authorization configurations. As a matter of fact," [4].

The study is divided into five chapters, as shown:

In the first chapter, I will explain an overview of IoT and its challenges and then explain brief description about Android robot platforms, after that, I'll explain the cloud robotics and its benefits.

The second chapter will be explaining the Security and Threats Issues for cloud systems and listing the cloud security attacks and threats.

The third chapter will list the most important monitoring and security systems such as SIEM (Security Information and Event Management) and its benefits. Explaining Block Chaining Technology and its pros and cons. Also the related work of threat monitoring.

The fourth chapter will be about Android Communication Network. And explaining the Wireless Communication technology and its security issues, also will be displaying the evolution of wireless technology and its generations. Then displaying Android Robot Operating System Networks in cloud. Microsoft Azure IoT Hub and the enhanced protocols used to model the network will be described in detail.

The fifth chapter will be displaying Our Cloud Based Monitoring System**.** First, highlight the role of cloud computing in the security and privacy of IoT. And then Azure Sentinel as a cloud based monitoring system that I will use as a platform for monitoring
The Six-chapter will be presenting the steps for creating and preparing digital assistance (Land bot) that we named (Obuda bot), also presenting the Metrics and user's Log data of Obuda bot and also explaining REST APIs (Representational State Transfer Application Programing Interfaces) for Azure Sentinel and Landbot and also how to initiate integration between them.

The seventh chapter will present the Strategy of testing the proactive monitoring system based on exploits databases and also displaying the main Types of Exploits and making a comparison between the main exploit databases we will utilize, finally the Exploit Code for Testing Monitoring System and the result analysis.

Research goal:

With the development of computing and communication technologies in the era of 5G (5 Generation) and IoT led to arose many difficulties, the enormous computing capacity that needed by these new systems arose the need to move the thinking systems for Android robots up into the cloud. there are many communication threats in the cloud domain. The aim of this research is to develop a proactive threat monitoring system to monitor and collect communication threats for the cloud android systems.

Chapter 1: Application examples for cloud androids

1.1 Overview of the internet of things and its issues

The phrase IoT was coined in 1999, by Kevin Ashton, and was popularized by the Auto-ID Center's work.," a research group working in the field of networked RFID (Radio-Frequency Identification) and other emerging sensing technologies" [5]. At the time, however, the particular definition of IoT was not specified, and although there is a general consensus that IoT incorporates items and connectivity, the precise terms are still to be discovered. On the area of IoT, there are now basically two distinct groups of opinion. In the first framework, IoT is seen as a layer of digital communication on top of current systems and objects. Convergent advances on infrastructure, services, applications, and governance tools are seen as a controllable collection of IoT developments in this view. Existing economic models are expected to be disrupted by new entrants, as was the case during the switch from mainframe to Internet business models.
In the second approach, IoT is viewed as a disruptive convergence that will be impossible to manage with conventional tools because it will shift the focus from the supply chain to 'apps,' where data and noise are defined differently. The challenges we face are the same in each of these methods. The main difference will be in the approaches and solutions. In this thesis I will focus on the Technological challenges and the methods used to overcome it. IoT encompasses a wide range of technical advancements that are as disparate as they are numerous. Defining the borders of the term itself is difficult, if not impossible, due to the fact that the meaning itself is currently being debated. Considering that the Internet of Things is based on "interconnected smart objects," we have the option of focusing on communication technologies or the "smart object" perspective, which incorporates advances in energy harvesting and conservation as well as the miniaturization of printed circuit boards and the incorporation of transistors into common materials like plastic, wool, and metals.
There are several challenges facing IoT such as:

- **Scalability:** There will be billions of IoT devices. These will be far more networked objects than there are currently on the internet by many orders of magnitude, even though it is doubtful that all things would be connected in a mesh.

- **Security and privacy:** The problem of providing adequate security on devices with restricted capabilities must be addressed and solved effectively. In addition, it is necessary to build and utilize as a foundation for any future development technology architectures that respect privacy.
- **Communication mechanisms:** IoT is in a similar scenario to the beginning of the internet, where a variety of communication methods were utilised, but only a single reference model permitted the development of the Internet.

1.2 Android robots platforms

"The number of studies and researches made on robotics field involving ROS (Robot Operating System) has been increasing recently. ROS is a different operating system than the ones we are used to. It provides a structured communications layer above the host operating systems of a heterogeneous compute cluster" [6].

Many people start recognizing its advantages. In addition, systems with many robots and cooperative robots are now being developed based on this concept. It is easier to get started with ROS because of the large ROS community, which has already built a number of packages and is constantly available to solve problems. The peer-to-peer topology network must be established in order for this framework to be used to connect various systems together.

1.3 Cloud robotics

We are constrained by the CPU (Central Processing Unit), memory, and storage capabilities of a robot while utilizing it independently. To do kinds of complex tasks, you'll need a high-priced robot. The ultimate objective is to make robot ownership and use in daily life accessible to the general public. Achieving this aim would necessitate the development of personal robots that are both inexpensive and capable of connecting to the Internet, where they can take advantage of the vast computing, memory, storage, and data resources available online. Also as previously explained, a connectivity to the cloud may be established using an Android device Robot. And limitations prevent us from solving certain robotics difficulties. Many robot research platforms, despite their high price tags, simply cannot retain all of the data required to complete particular tasks. Cloud services can, however, be used by robots that are linked to the cloud. For example, User may use the Google Maps API (Application Programing Interface) to learn about the quantity of data stored on a cloud server.

Chapter 2: Security and threats issues

Cloud computing has grown significantly in recent years. In the modern era of IT technology, As the need for services or utility computing is increasing over the global internet. A number of businesses have been migrating to the cloud over the last few years, including Microsoft, Google, and others. When it comes to cloud computing, the software is no longer dependent on the operating system or the hardware, therefore if any of these fail, the software will immediately switch to other resources. This is not virtual computing. “The term ‘cloud’ is ‘remote data center’ it also has two meanings, the first is the access of information and data resources via the Internet using Web browser while the second is paying for the computing resources based on usage” [7].

One of the most difficult challenges in delivering powerful processing and storage as on-demand services is the security risk that results from resource sharing throughout the cloud. This is due to cloud computing's ability to increase efficiency and performance while simultaneously lowering expenses. Governments and enterprises throughout the world are implementing or migrating their IT infrastructures. Although cloud computing's features and quality service are improving, there are still a number of technological challenges that are delaying the widespread adoption of cloud computing.

Threats and attacks in the cloud systems are listed below:

- **Account and service hijacking:** Security experts consider it a severe threat. There is an assault on the cloud provider's infrastructure when an attacker attempts to hack into a web service located on the cloud provider's server.
- **Abuse and nefarious use of cloud computing:** Cloud computing power may be used to attack targets via spam and malware, such as a botnet, in this case. According to the CSA (Cloud Security Alliance), it is the cloud computing's greatest security risk.

- **Backdoor cchannel attacks:** When an effective user has high access to the VM(Virtual Machines) or the Hypervisor level, this type of attack occurs in the Iaas. Data security and service availability might be affected by this attack.

- **XSS (Cross Site Scripting) attacks:** is another name for it. It is one of the most effective web application security vulnerabilities that has been discovered to date. Java script language, which has the largest range of scripting, is usually applied in such attacks.

- **Cloud malware injection attack:** Malware, macules applications, and virtual machines may all be injected into the cloud infrastructure with this top cloud computing security list attachment.

- **Denial of Service attacks:** When a user tries to access a service through the server during a denial-of-service attack, the service is unavailable. They'll get a 404 error message stating that the service they're looking for is unavailable.

- **Zombie attack DoS(Denial-of-Service)/DdoS(Distributed denial-of-service)** At the Hypervisor, Network, or VM level it occurs in an indirect/direct manner. It might impact service availability and build a user account for fake service consumption.

- **Insecure application programming interface:** Using APIs, service providers offer their service to clients, encrypting the APIs with secure authentication and providing safe access control and activity monitoring techniques for the APIs themselves.

- **Man in the middle attacks:** While the consumer and service provider are unaware, a hacker establishes a direct link between the two parties in order to spy on their communications.

- **Metadata spoofing attack:** Web services providers transmit the metadata document to the client system, which contains all the service invocation information, such as the security requirements, message format and network location. It is the attacker's goal to alter the security rules and network references by reengineering the web service metadata descriptions.

- **Malicious insiders:** It's possible for an employee to gain access to a cloud service provider's virtual assets without sufficient security measures in place. Due to the employee's privilege not implementing in the cloud system and updating their responsibilities when their behaviour or job is altered, this threat may be more difficult to address.

- **Phishing attack:** Affected user privacy as well as data and information exposure by allowing users to browse a false web link placed on their **PCs(Personal Computers)** is the basis of this issue: That data is exposed via malicious code.

- **SQL(Structured Query Language) Injection attacks:** When hackers try to hit a website database by injecting SQL statements with malicious code, they can deactivate a website's security by exploiting the website inquiry techniques.

- **Shared technology's vulnerabilities:** This is a problem with cloud computing, which utilises the same infrastructure as the internet and is shared among cloud clients. As a result, the cloud will be used to solve all of the issues now plaguing internet infrastructures. As a result, the traditional computer components have not been adapted to work with cloud computing systems in this manner.

- **Sniffer attacks:** It's easy for hackers to read the contents of a network packet when no encryption measures were used to convey the data. Any one of these things could be used as a "sniffer."

- **Concerns about the virtual machine's security Manager:** Service providers must exercise extreme caution while providing VM technology-based services to their customers because to the potential for security vulnerabilities.

- **Unknown risk profile:** If the concentration is just on the capabilities and features that cloud services can provide, without any concern for the security technologies and producers that will be established, then this security issue will arise. The issue is which features may have access to third-party data and whether or not this data is published for whatever purpose they choose.

Chapter 3: Methods for monitoring systems' security

3.1 Security information and event management system

"Security Information and Event Management (SIEM) is a set of tools and services offering a holistic view of an organization's information security" [8].

SIEM tools provide:

- Real-time visibility into the security information systems of a company.
- Event log management that collects data from several sources.
- If-then rules applied to raw data from various logs and security sources are used to create correlations.
- A mechanism for automatically notifying users of security events. The majority of SIEM systems provide dashboards and other forms of instant alerting for security risks.

When two technologies are combined in SIEM, security information management (SIM) is used to collect log file data from which it is possible to analyze threats, while security event management (SEM) is used to monitor the system, notify administrators of critical issues and establish correlations between security events. Security information and event management could be divided into the following categories:

- **Data collection** – Data from all sources of network security information is fed into a SIEM solution that is designed to receive event data from all sources of network security information. Most existing SIEM products utilize agents to gather event logs from corporate systems, which are subsequently analysed, filtered and transmitted to the SIEM. There are certain SIEMs that enable for data collecting without the need of agents. For example, Splunk uses WMI to collect data on Windows without the need for a dedicated agent.
- **Policies** – The SIEM administrator creates a profile that specifies the behavior of existing systems under normal conditions and in the event of a security incident. SIEMs include pre-configured rules, alarms, reports, and dashboards that may be created to suit unique security requirements.
- **Data consolidation and correlation** – Log files are consolidated, parsed, and analyzed by SIEM systems. The raw data is then processed and correlation techniques are applied to integrate individual data occurrences into relevant security problems.
- **Notifications** – In the case that a SIEM rule is triggered, the system alerts the appropriate security staff.

3.2 Block chaining technology

A rising number of systems are utilizing blockchain technology in an effort to improve security. It's one of the best candidate technologies for storing an immutable log of transactions (a ledger) in a distributed network, creating a genuinely decentralized, trustless, and secure environment for transactions and related applications. "Trusted" here refers to the system's structure rather than its central authority or other participants in transactions being trusted. Blockchain technology also includes the concept of "smart contracts," which are essentially software components running on the Blockchain to implement agreements between two or more parties, automatically triggered when certain conditions are met. The use of smart contracts in Blockchain transactions is critical. As a result, proponents of blockchain Technology believe that it provides assurance in a widely distributed zero-trust environment: the need to evaluate the degree of trust one desires to invest in a third party to any transaction (for example, a bank in the case of financial transactions) is gone. This might be extremely valuable in the IoT environment, where devices from a variety of manufacturers with various data standards, accuracy, and other functional aspects are common. IoT devices and the data they create must be able to be trusted with an immutable record that can be seen by both the systems that consume the data and the devices themselves. Temperature, traffic speed, and occupancy are all examples of physical attributes that may be measured by several sensors in the same spot. Using a consensus method, Blockchain technology can allow parties to agree on which value from a set of values is utilized in any system.

3.3 Block chaining pros and cons.

Pros

1- Blockchain is working on the basis of **distributed ledger technology** without need for **centralized authority.** This unique feature giving leverage for blockchain to become the next generation of technology. Except private blockchain that may be utilize some aspects of centralization.

2- It enables set of peers for creating a **unified decentralized networks** for working together and communicate and sharing data and information by using **secure cryptographic protocols** and **consensus algorithms** for validation purpose.

3- Blockchain networks are **trustworthy and transparency** among other types of networks.
4- Blockchain supports **immutability**, which meaning that when the data once is written it cannot be erased or replaced
5- Blockchain supports **data integrity** thanks to **Immutability** and there is no chance of failure.
6- **Proofing of work** is one of consensus algorithm is used as evidence to validate the work. It's ensure there's no invalid transactions passing into the blockchain.
7- Each transaction can be **tracing, verifying by any one and backed** by creating a **Timestamps**.
8- The whole system of blockcain can adding values and bringing new features for **Transparency, Immutability and security.**

Cons

1- Blockchain cannot implemented on the business or organizations having private data and process at stack or critical. Therefore, it's evolved and we have different types of blockcain **(Hybrid, Federated)** to solve the problems of private organizations.
2- It's very hard to implement or maintain block chain.
3- Blockchain is **slowing** by verification, redundancy and consensus processes.
4- Block chain supports only two operations, Read and Write.
5- Blockchain have **high costs** when implementing (end to end) and maintaining because It's new technology and still evolving.
6- The blockchain is not suitable for storing a huge amount of numerical data that needs to be regularly used
7- Blockchain require large energy consumption.

3.4 Block chain protocols

A protocol is a collection of regulations that regulates how something works and how it is passed across devices. Code blocks known as protocols form the backbone of modern networking and security protocols. The framework provides the rules for data transport and represents how the devices respond to the information transmitted. There is a diversity of blockchain protocols, or "business blockchain protocols," that are now in use.

Bitcoin is the most well-known. The Bitcoin cryptocurrency was the impetus for the creation of the Bitcoin blockchain network. The blockchain network of the Bitcoin currency serves primarily as a repository for the cryptocurrency's value. Value may be passed from one person to another without anyone knowing who the other person is.

Ethereum is an open-source platform that may be used by anybody. Ethereum improves on the foundations of Bitcoin by offering a protocol that permits the establishment of small apps and the transfer of fundamental value. Finally, logic and code may be used instead of just fixed value transfers**.**

Ethereum and Hyper Ledger Fabric are good options if you plan to leverage blockchain for your own solution. Programmable blockchains may be put to many different uses. Smart contracts are used to embed business logic and information in general use protocols. The Ethereum protocol is the topic of this module**. Figure (1)** will illustrate the network of blockchain technology.

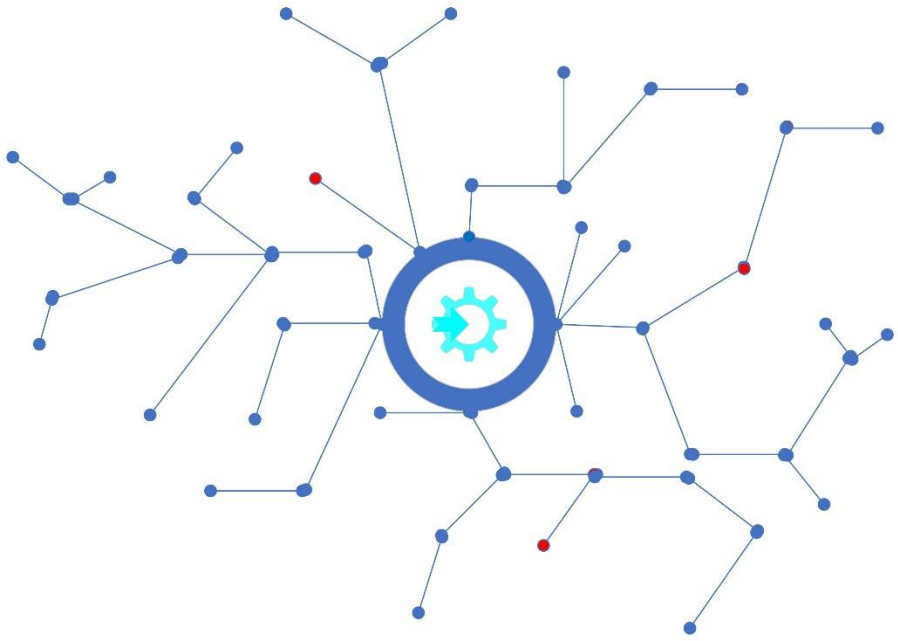


Fig. 1. Network of Block Chaining Technology [8]

3.5 Related work

Through a multitude of research investigations, numerous and diverse network monitoring and threat detection systems have been developed:

Bailey, Michael, et al [10]. "The internet motion sensor-a distributed blackhole monitoring system.". This paper introduces the IMS (Internet Motion Sensor), An Internet monitoring system that measures, characterizes, and tracks threats throughout the world. Components of the IMS architecture include three new elements. To begin, A global threat landscape is better understood thanks to a distributed monitoring infrastructure. Second, the interactivity provided by a Lightweight Active Responder is sufficient to distinguish traffic flowing through the same service regardless of the semantics of the applications. Third, a Payload Signatures and Caching technique prevent the recording of duplicate payloads, hence lowering overhead and helping to detect fresh and unique payloads. A three-year deployment of this system over different dark address blocks (varying from /24s to a /8) provides an opportunity to examine the system's architectural trade-offs. There are a wide variety of companies and a wide range of routable IPv4(Internet Protocol Version 4) ranges represented by these sensors. There are various notable Internet threats, such as Blaster (August 2003), Bagle backdoor scanning (March 2004), that the IMS may identify and describe from the data acquired from these installations (December 2003).

Wei Yu et al [11]. Founded a cloud computing based architecture for cyber security situation awareness. They propose a cloud computing based architecture for conducting cyber security situation awareness. Cloud computing with cost-effective data storage and stream processing techniques are used in particular to decrease operational delays. They propose a cloud-based threat detection system that incorporates both signature-based detection and anomaly-based detection in order to successfully detect threats. Attack scene analysis based on spatiotemporal correlation and visualization approaches is discussed to capture the informative properties of attacks. Lastly.

Zhijiang Chen et al [12]. also have founded A Streaming-Based Network Monitoring and Threat Detection System.

There is still a problem with managing massive amounts of network traffic data from corporate systems, while simultaneously providing real-time monitoring and detection, which was addressed in this study. A streaming-based threat detection system, in particular, was introduced and tested for its ability to quickly analyze very intense network traffic data in real-time, using streaming-based clustering algorithms to detect suspicious network behaviors. For network monitoring and intrusion detection, the system created incorporates the streaming and high-performance data processing capabilities of Flume, Sharp and Hadoop into cloud computing. a substantial volume of

streaming data can be dealt with by the created system without degrading detection accuracy or system performance, as shown by the results of the performance evaluation and experiments.

Luigi C. et al [13]. “Cloud security: Emerging threats and current solutions” Here, they present a detailed evaluation of the primary challenges to cloud computing adoption, and a thorough examination of the remedies currently being offered by the major suppliers. Additionally, the article provides an outlook on the (near) future prospects of cloud security research by providing a snapshot of the primary research trends and the most well recognized methodologies. Open Source and commercial cloud services are included in the research because they provide the "best of both worlds." Papers like this one help IT staff understand the security issues associated with cloud computing and analyze the advantages and drawbacks of current solutions in a short period of time.

Giampaolo Fiorentino et al [14]. "Blockchain: Enabling Trust on the Internet of Things," introduces Blockchain technology and highlights some of its adoption issues. Internet of Things (IoT) and how it has already been used to industries such as insurance, the pharmaceutical business, and the energy vertical are the topic of this article. Blockchain's technology is based on Distributed Ledger Technology. A whole peer-to-peer network is used to store the distributed ledger database, which is replicated and saved by all of the nodes. All the nodes in the network must be able to trust the transaction in order for DLTs to achieve consensus validation. "Internet of Transactions" can be used for blockchain implementations. Several businesses might benefit from the Blockchain's decentralization, immutability, auditability, and fault tolerance/resilience, which are all essential advantages. There are many difficulties and potential for Blockchain technology in the IoT setting that will be discussed in this chapter's conclusion.

Dutta, S. et al [15]. "Utilizing chatbots to increase the efficacy of information security practitioners". According to this article, chatbots may help information security professionals, such as security analysts and pentesters, in ways that go beyond the existing human-before-support mentality. Investigations into possibly harmful conduct and team security testing initiatives are examples of scenarios in which a chatbot might significantly improve the effectiveness and efficiency of a specific type of information security practitioner.

Chapter 4: Android communication network

4.1 Wireless Communication technology and its security issues

Internet of Things (IoT) and Android robot sensor networks have expanded to facilitate communication at any time and everywhere thanks to the development of wireless networks and the arrival of 5G networks in particular. It is predicted that new services and applications will be developed as a result of this change. If these sensing networks are not properly protected, they will be subject to a wide range of security risks and assaults. Communication signals travel across the air, making wireless networks less secure than wired networks. It can readily be intercepted through radio waves. Users of wireless technology face more risks and threats as the technology become more widely used, especially as the Internet of Things (IoT) revolution takes hold and wireless networks become the backbone for linking billions of devices and sensors. When wireless technology was originally launched, there were few risks. The new technology had not yet been adopted by hackers, and wireless networks were not widely available. In spite of this, wireless protocols and encryption methods are vulnerable to a wide range of threats and security hazards because of user and corporate IT laziness and ignorance. As wireless connection becomes more common, hacking techniques have gotten more complex and ingenious. The availability of free, easy-to-use Windows- and Linux-based hacking tools on the internet has made hacking considerably more accessible. When it comes to cloud computing security, many organizations may not be aware of wireless security issues and how they may potentially be integrated with cloud computing security [16]. So, we discuss the most important aspects of wireless technology, its evolution and the enhanced protocol used to overcome these challenges. **Figure (2)** will illustrate the vulnerabilities of wireless and cloud services and how to protect them.

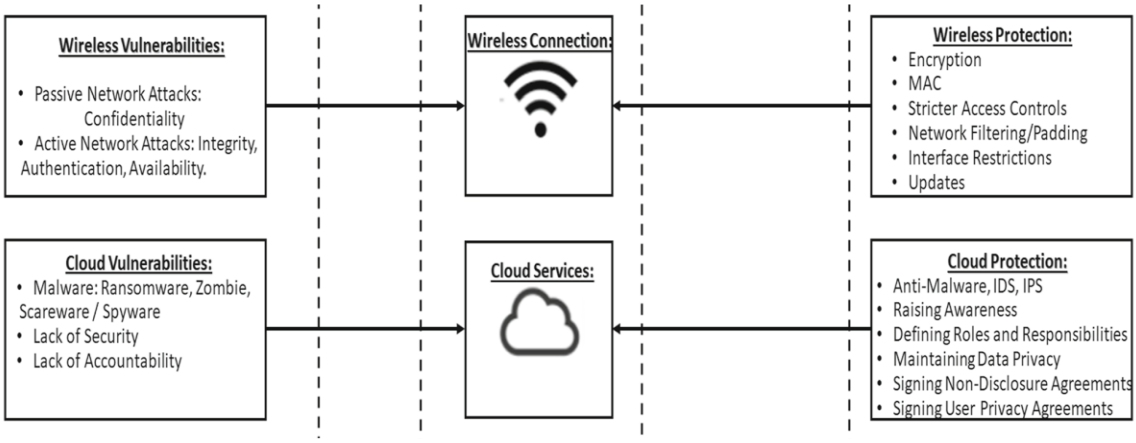


Fig. 2. Security vulnerabilities of Wireless and Cloud services

4.2 Evolution of wireless communication networks

From Alexander Graham Bell's phone experiments to the widely used W-CDMA (Wideband Code Division Multiple Access) network and the nearly achieved 5G mode of communications, we see new dimensions of emerging modern communications technology and revolution every year as illustrate in **Figure (3)**. This includes the ability to transfer a vast amount of data at a relatively faster rate with more security and intelligible forms and directions all over the world with limitless borders. It is clear that each generation of wireless mobile communication has and will continue to make a significant impact on today's voice/data network and Internet of Things (IoT).

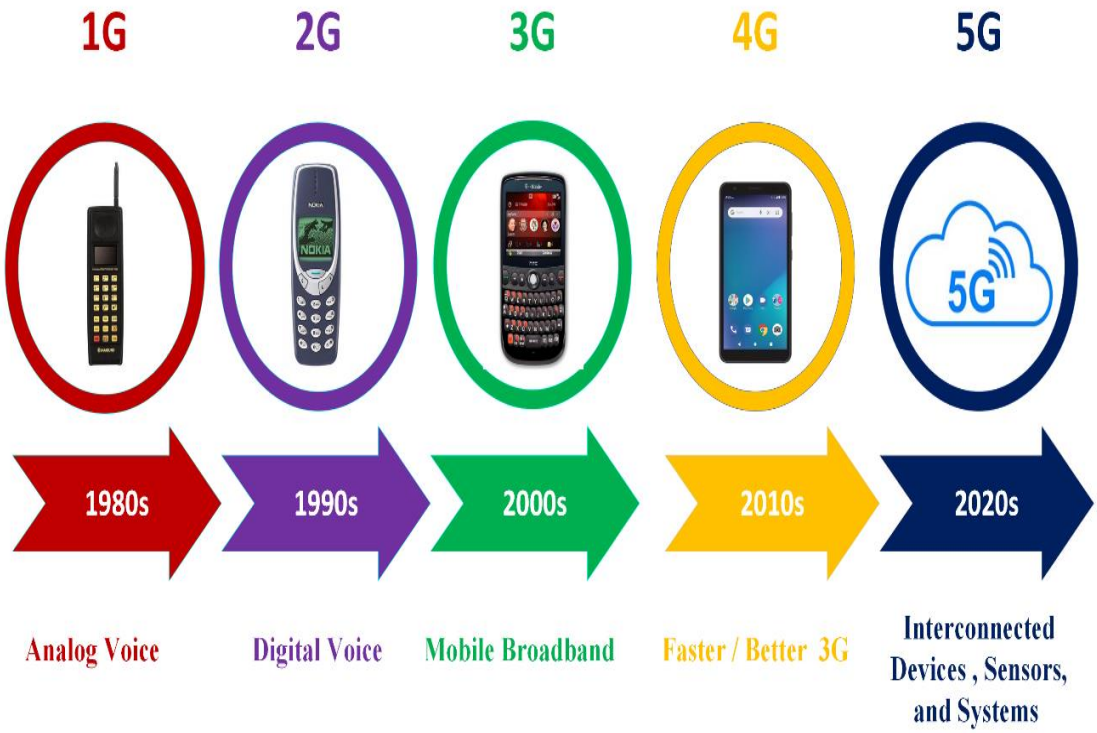


Fig. 3. Evolution of Wireless Communication Networks [17]

First generation (1G)

Analog radio technology meant that users could only make phone calls, neither send nor receive text messages on the first generation networks. A year after its introduction in Japan, the 1G network was rolled out in other regions, such as the United States, the UK and Australia. In order to make it work, cell towers were erected around the country, allowing for increased signal coverage. However, the network was unstable and had some security problems. For example, cell coverage would frequently decrease, other radio signals would interfere with it, and because of a lack of encryption, it might be simply hacked. These tools allow for talks to be heard and recorded with only a few clicks. **Figure (4)** will illustrate the architecture of first generation.

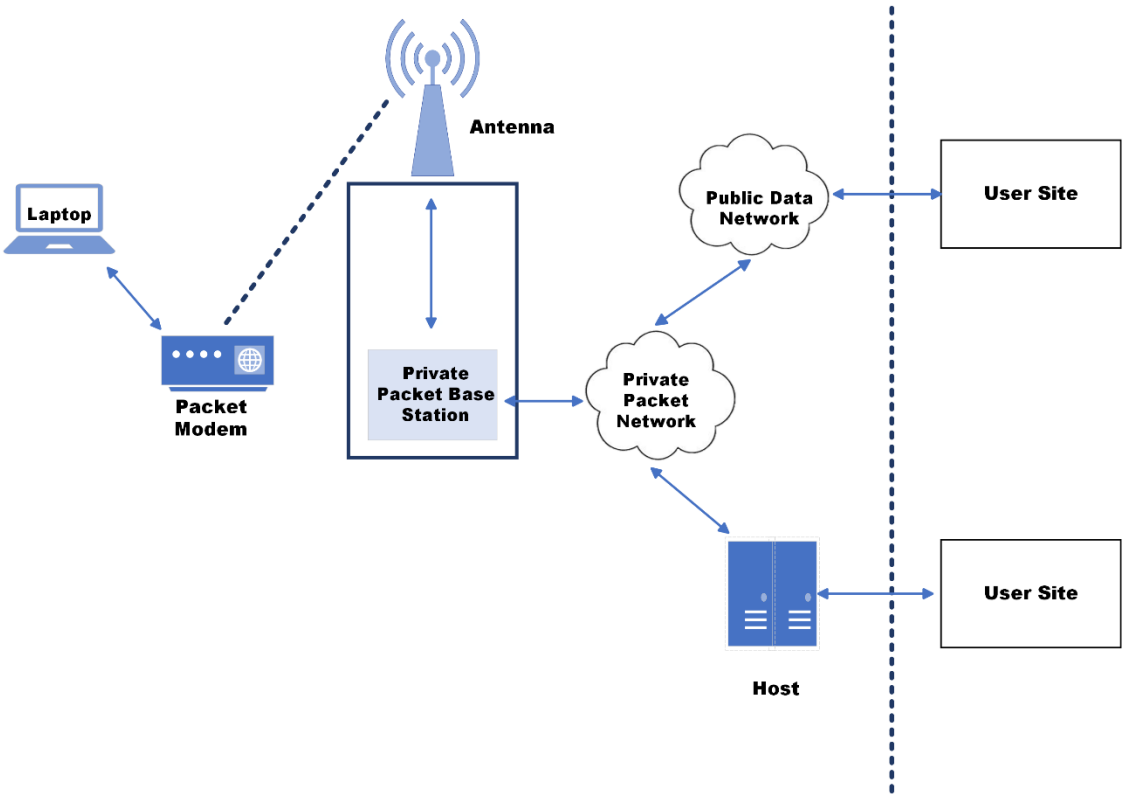


Fig. 4. 1G network architecture [18]

Second generation (2G)

Despite its problems, the 1G network lasted until 1991, when it was replaced by 2G. Digital signal, rather than analogue, was used in this new mobile network, which greatly enhanced security and also increased its capacity, Users were able to send and receive SMS and MMS messages on the 2G network, but they were unable to send or receive emails until the introduction of GPRS in 1997. **Figure (5)** will illustrate the architecture of second generation.

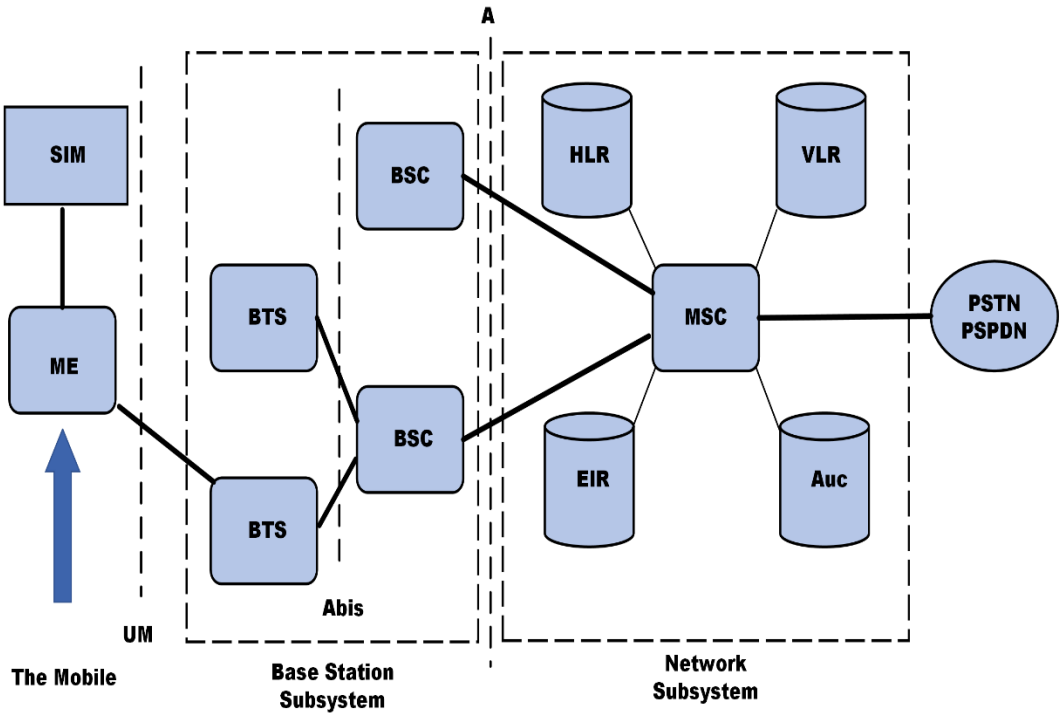


Fig. 5. 2G network architecture [18]

Third generation (3G)

Today, third generation networks are still in use when the stronger 4G signal is unavailable. Third Generation (or 3G) mobile phone connection and capabilities were revolutionised by 3G. Faster and more capable of transmitting data than the previous generation, 3G outperformed its predecessors. For the first time, people could video call, transfer files, access the internet, watch TV online, and play online games on their mobile devices.. As a result of the introduction of 3G, mobile phones become more than just a means of making and receiving phone calls and texts**. Figure (6)** will illustrate the architecture of third generation.

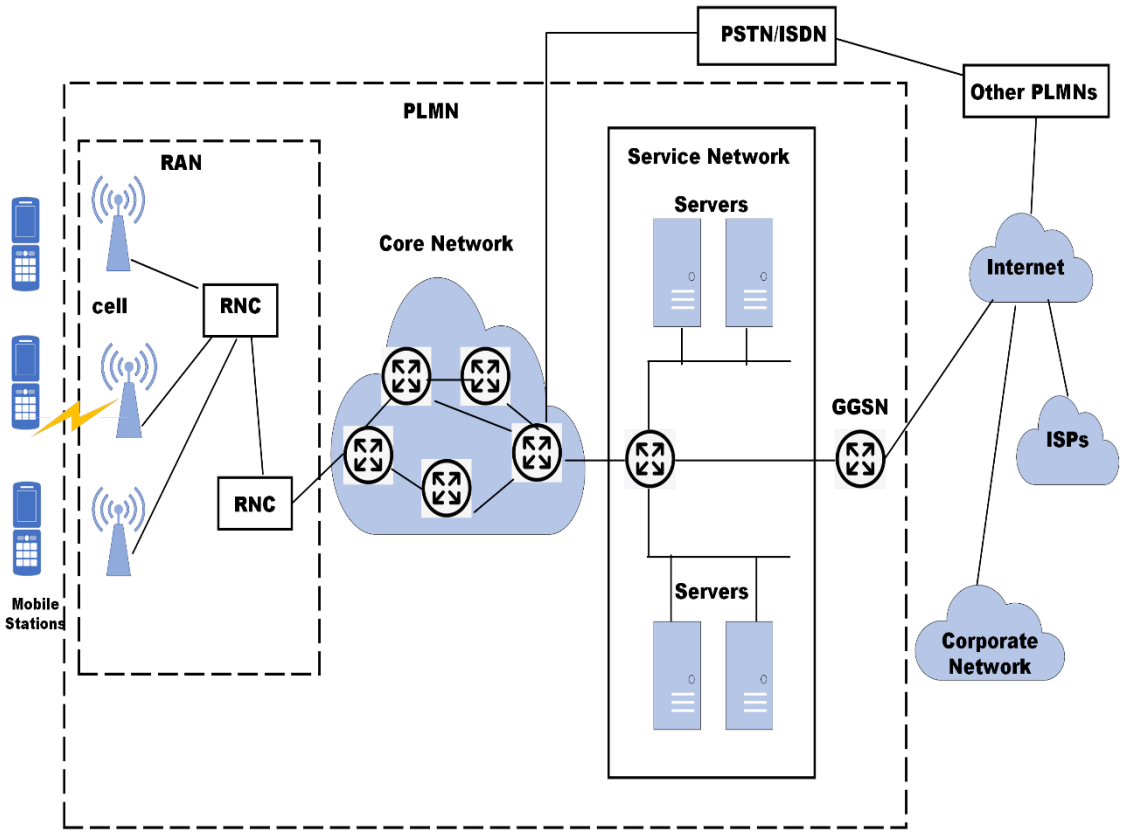


Fig. 6. 3G network architecture [18]

Fourth generation (4G)

In the midst of the 3G revolution, 4G was the next logical step forward. Compared to the 3G network, it is five times speedier and theoretically provides rates of up to 100Mbps. All new smartphones and tablets manufactured after 2013 should be able to connect to this network, which can also be used to link laptops and desktop computers. Improved security and latency (less buffering), improved audio quality, simple access to instant messaging services and social media, quality streaming and quicker downloads are all possible under 4G. **Figure (7)** will illustrate the architecture of fourth generation.

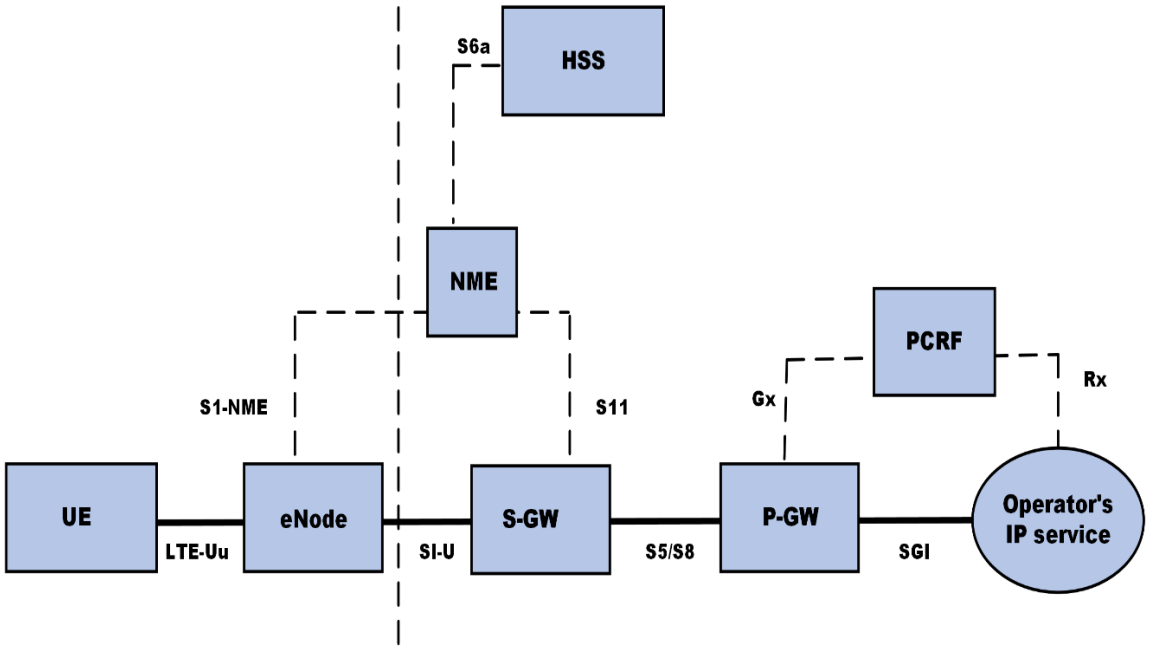


Fig. 7. 4G network architecture [18]

Fifth generation (5G)

For the mobile industry, 2020 is a target date for the delivery of 5G technology. Many analysts believe that the network will alter not just how we use our mobile devices but also how we connect our gadgets to the internet. Connected automobiles and smart cities, as well as IoT in the home and workplace, will be able to take use of the network's increased speed, security and capacity.

5G offers a lot of potential for security, and it's a lot better than 4G. In 5G, there are significant security gains. Anti-tracking and spoofing features, which make it more difficult for bad actors on a network to identify and control individual device connections, are among the most common. In order to do this, 5G encrypts more data, so that less of it is available to be intercepted by anyone. In addition, 5G is a far more software and cloud-based system than prior wireless networks, which will allow for greater monitoring to discover any threats. Network slicing—segmenting the system into many virtual networks that can be managed and configured independently—will also be possible with this technology. This means that separate "slices" might have different specialized security for different sorts of gadgets. **Figure (8)** will illustrate the architecture of fifth generation.

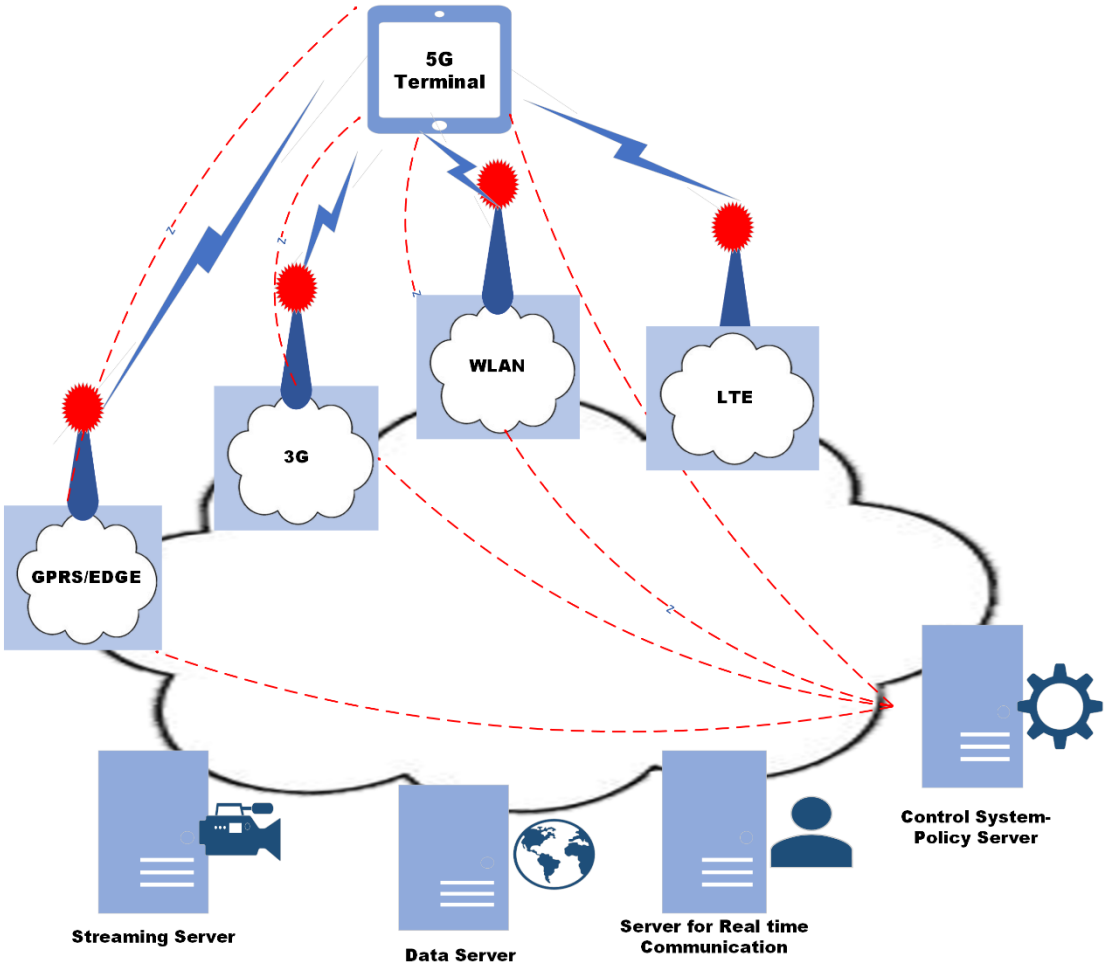


Fig. 8. 5G network architecture [18]

4.3 Android robot operating system networks in cloud

It has always been the goal of IT engineers to construct a high-performance and dependable network. When everything else fails, cloud computing appears to be the answer. In the near future, cloud computing will change the computer industry. As 5G and Internet of Things (IoT) technology develops, it will be necessary to move the new technology's thinking system to the cloud because of the sheer amount of smart devices and Android Robotic sensors that will be linked via this new communication technology. **Figure (9)** will illustrate the architecture of cloud computing.

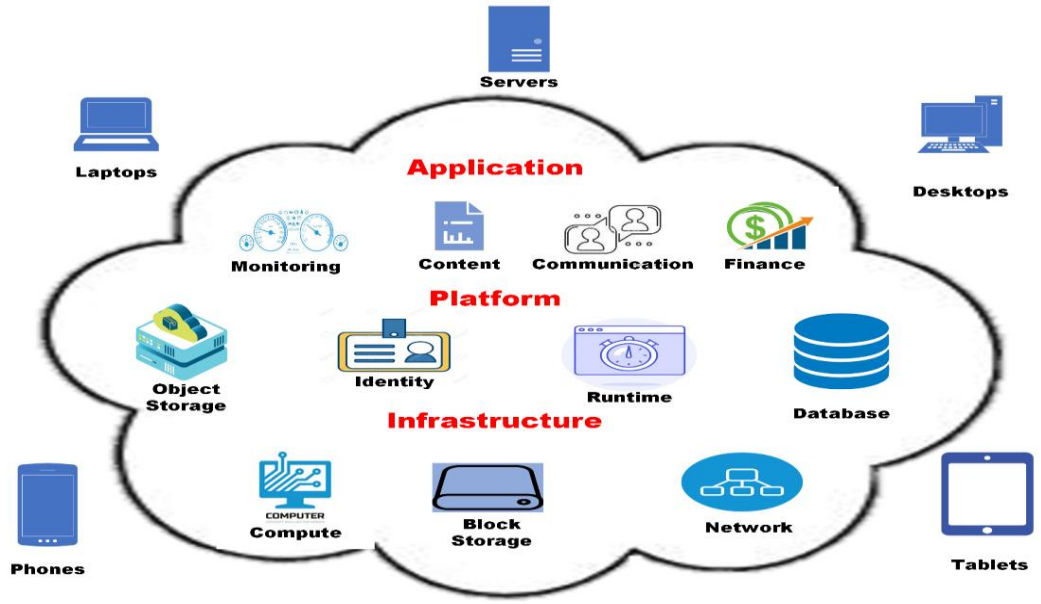


Fig. 9. Cloud Computing [19]

There are numerous amazing tools and Robotics middleware that can act as communication distributed networks in cloud based systems. The term "middleware" refers to the software that resides between an operating system and the application that uses it. Middleware is essentially a hidden translation layer that enables remote apps to communicate and handle their data. "Plumbing" simply means connecting two programs so that data and databases may flow through a "pipe". A user's profile can be used to return dynamic web pages depending on a user's form submissions, for example, using middleware. Common middleware frameworks for research and development on robotics platforms, such as the ROS (Robot Operating System) and YARP (Yet Another Robot Platform) are presently implemented in hundreds of robots worldwide. If you want to connect your ROS apps to the cloud, you may use ROS bridge, which lets you publish and/or subscribe to topics from any non-ROS client. Through the internet, communications are structured in JSON (JavaScript object notation) Any non-ROS client, from any platform that understands JSON, can communicate with a ROS-based robot. To facilitate interoperability across applications, messaging frameworks are often included in software applications. JSON The type of middleware a company chooses to

deploy depends on the type of service they are using and the type of information they need to convey. Authentication, transaction management, message queues, applications servers, web servers, and directories are all examples of this type of technology. By connecting ROS robots to Android and Google's cloud services, android provides another cloud-based method. In order to do this, the Rosjava and android core packages are used, which implement ROS in Java and Android. Android Apps that can communicate with ROS-enabled robots may be created by combining these two technologies together.

ROS networks may be used as a distributed computing platform. Nodes in a running ROS system can be dispersed among a number of computers. It is possible for any node in the system to communicate with any other node at any moment, depending on how the system is set up. Distributing robot software over several networked components in a ROS application, each component functions as a server or client and concurrently publishes and receives robot data. **Figure (10)** will illustrate the ROS network.

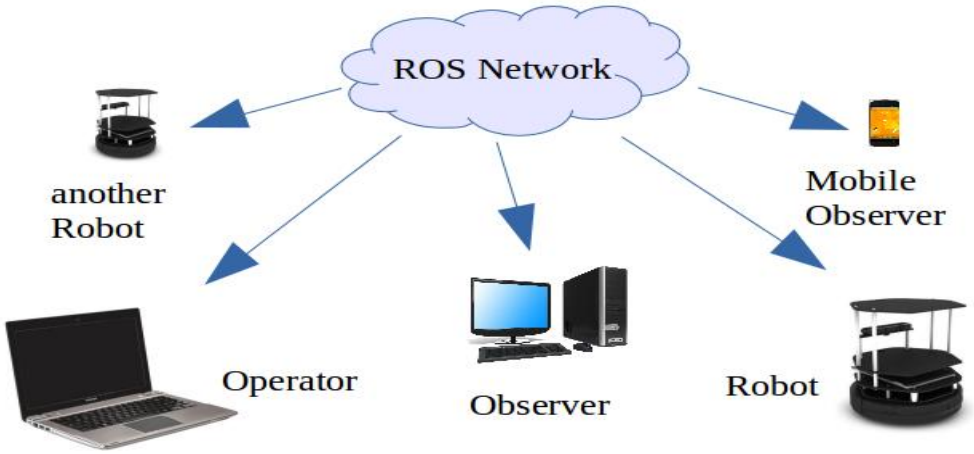


Fig. 10. The ROS network [20]

4.4 Network modeling

Microsoft Azure platform will be used in my thesis to represent the network. Connecting computers and apps is the primary role of the Azure network. Microsoft Azure's network features give a variety of alternatives for connecting the outside world to Microsoft Azure's services and capabilities. Azure networking facilities have the following services:

- **Azure Virtual Networking:** Allows inbound VPN (virtual private network) connections to be established between VMs.
- **Azure Load Balancer:** Working on connection balancing at the application's endpoint.
- **Azure VPN Gateway:** Using a high-performance VPN Gateway to connect to Azure Virtual Networks.

- **Azure Content Delivery Network (CDN):** On a worldwide scale, delivering information with high bandwidth.
- **Azure ExpressRoute:** A secure, high-bandwidth connection to Azure is recommended.
- **Azure Network Watcher:** Monitor and diagnose network issues with the help of a software tool for analysis .

4.5 Azure internet of things hub and private link

Azure IoT Hub is a cloud-hosted managed service that serves as a central messaging node for communications going both ways between an IoT app and the connected devices. It is capable of securely and reliably connecting millions of devices and the backend solutions that support them. An IoT Hub may be linked to almost any device. Device-to-cloud telemetry, uploading data from devices, and request-response ways to manage your devices from the cloud are all supported by the service. Monitoring is also supported by IoT Hub, allowing you to keep tabs on the creation, connection, and failure of devices. You may create scalable, full-featured IoT solutions with IoT Hub's features, such as industrial equipment management, asset tracking in healthcare, and office building utilization monitoring. Private Link and Managed Identity are supported by IoT Hub for virtual networks. By default, IoT Hub's hostnames lead to a public endpoint with an internet-routable IP address. It is possible for IoT devices on wide-area networks and on-premises networks to reach this public IoT Hub endpoint shared by several clients [21]. **Figure (11)** will illustrate Azure IoT Hub.

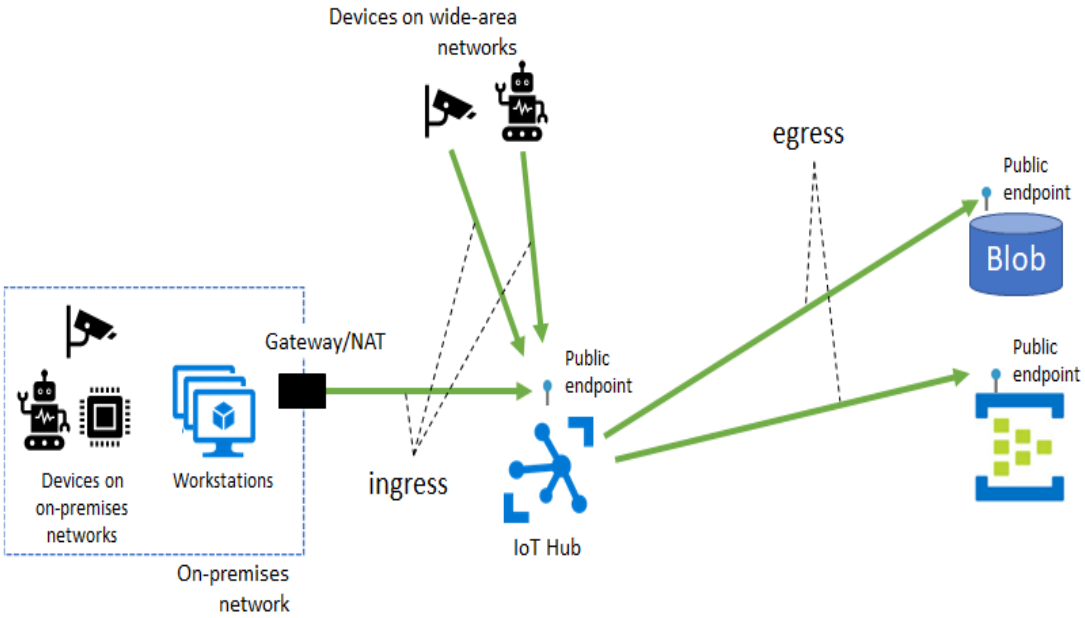


Fig. 11. Azure IoT Hub. [22]

Services like message routing, file upload, and bulk device import/export all need communication between IoT Hub and a customer-owned Azure resource across its public endpoint. The egress flow from the IoT Hub to client resources is made up of all of these connections. IoT Hub and other Azure resources may require a VNet (Azure Virtual Network) that you own and control in order to limit access. Reasons for these include:

- Creating a private network for your IoT hub by blocking it from being exposed to the public internet.
- Enabling private connectivity from your on-premises network assets to ensure that your data and traffic is routed directly to the Azure backbone network.
- Preventing the exfiltration of sensitive information from on-premises networks.
- Using private endpoints to adhere to well-established patterns of connection throughout the whole Azure network.

Use Azure Private Link for IoT Hub ingress and Trusted Microsoft Services exception for IoT Hub egress connectivity, respectively, in order to fulfil these aims. An Azure resource can be accessed using a private endpoint, which is an IP address assigned to a customer-owned VNet. Your IoT Hub may communicate with your VNet's services via a private endpoint set up with Azure Private Link, which does not need the traffic to be delivered to the IoT Hub's public endpoint. Similarly, your on-premises devices may connect to your VNet and IoT Hub via Virtual Private Network (VPN) or ExpressRoute peering (via its private endpoint). IoT Hub IP filter and public network access toggle can be used to restrict or totally prevent connectivity to your IoT hub's public endpoints. Using a private endpoint, devices may still connect to your Hub. This arrangement is primarily intended for on-premises devices. In a wide-area network, this design is not recommended. **Figure (12)** below illustrates Azure private link.

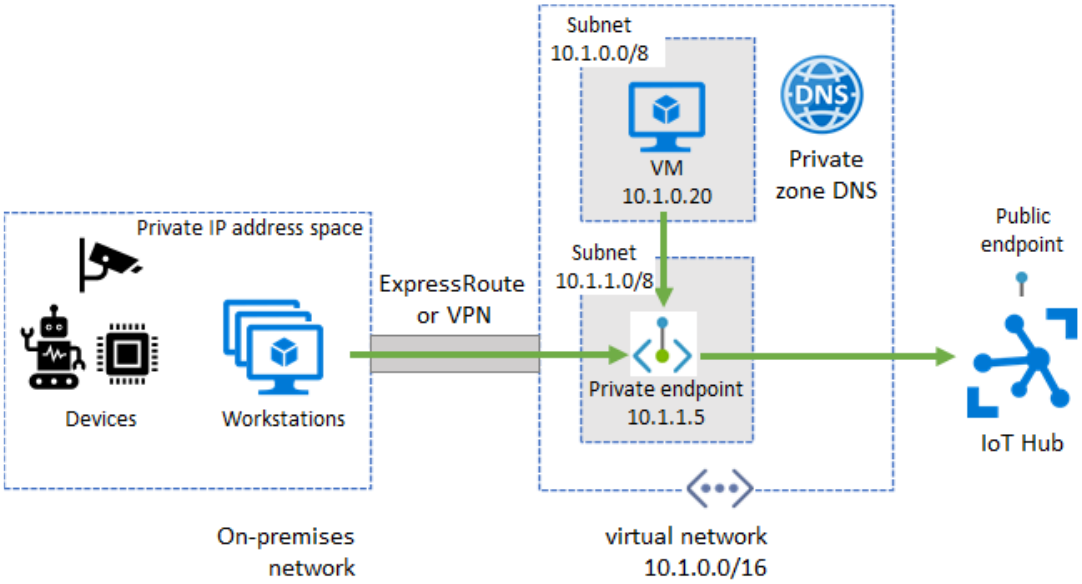


Fig. 12. Azure Private Link [22]

The following conditions must be satisfied before you may proceed:

- In order to construct a private endpoint, an Azure VNet with a subnet has been set up.
- If you have on-premises devices that need to connect to your Azure VNet through a VPN or ExpressRoute private peering, do so.
- IoT Hub device APIs (such device-to-cloud communication) and service APIs may be accessed via the private endpoint (like creating and updating devices)

4.6 Enhanced protocols used

To exchange data from a remote place, Internet of Things (IoT) devices require a message and connectivity protocol. Many Robotic Android sensors and end devices will be able to link to the Internet and cloud services through the Internet of Things (IoT). To connect to the Internet and cloud, these devices can either use cellular technologies like 5G or connect over a LAN (Local Area Network) that includes a gateway. All Robotic Android sensors and end-devices should be able to communicate with the Internet and the cloud, regardless of the wireless technology used to establish the network. By transmitting the data to a private web server accessible over the Internet or using the cloud, this may be performed. Data may be received, stored, analyzed, and processed on a cloud system like Microsoft Azure. In addition, they function as distant data repositories. IoT networks are built using current technologies, although research organizations are focusing on modifying protocols for the IoT to improve communications and security. Our description will include existing IoT protocols and the most appropriate protocols for connecting Android robotic sensors to the cloud.

IoT networks are governed by a wide range of different standards agencies. The IEEE (Institute of Electrical and Electronics Engineers), IETF (Internet Engineering Task Force,) and ITU (International Telecommunication Union) are among the most prominent organizations in the field. Wireless connection and Robotic Sensors should support the same communication protocols as the entire design. Although we've done our best to keep the list up-to-date, new protocols are always being developed and may appear in the future**. Table (1)** below illustrate the enhanced protocols for IoT.

1-	**MQTT**	Message Queue Telemetry Transport.
2-	**AMQP**	Advanced Message Queuing Protocol.
3-	**HTTPS**	Hypertext Transfer Protocol Secure
4-	**Websockets.**	Web socket

Table (1) Enhanced protocols for IoT

To send and receive data to and from the Azure IoT Hub in the cloud, remote IoT networks at the edge are linked to a local IoT gateway device. The upgraded MQTT, AMQP, WebSockets, and HTTPS protocols are supported by the Azure IoT Hub for cloud communication. **Figure (13)** describe the location of these protocols in the OSI (Open Systems Interconnection) and TCP/IP (Total Control Protocol/Internet Protocol) communication models.

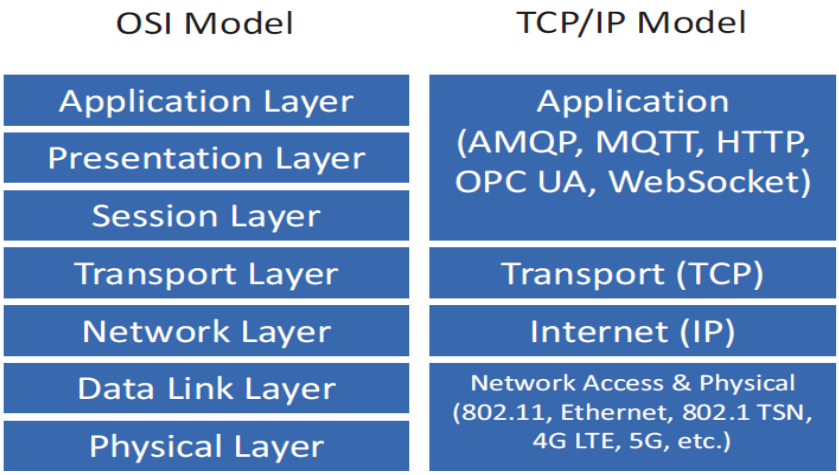


Fig.13. IoT protocols in OSI and TCP/IP models

For the sake of standardization, most businesses prefer to link their devices to the cloud using a single protocol. The following are some of the features of such a protocol:

- Small code footprint (to make it easy to implement in small devices)
- High security
- Low power consumption
- Low bandwidth consumption
- Low latency
- Use of a publish/subscribe ("pub/sub") pattern

Microsoft Azure, Amazon Web Services, and Google CloudPlatform support **MQTT,** which meets all of these criteria. In IoT projects, MQTT is a data-centric protocol that is widely used to connect to remote sites with restricted network capacity. To connect sensors on oil pipelines to communications satellites, the MQTT protocol was first created in 1999.

AMQP is the second protocol The operation of message-oriented middleware may be determined using the application-layer protocol. AMQP was built with the following major criteria in mind: (Security, Reliability, Interoperability, Standard, and Open).

Chapter 5: Cloud based monitoring system

5.1 The Role of cloud computing in internet of things security and privacy

As technology advances and data is sent online, it creates weaknesses and opens the door to cyber-attacks. In cloud storage and networking, security and privacy are critical concerns. The internet of things is made possible because of the cloud computing environment. Servers, apps, and other storage devices were all part of the cloud computing technology, which relied on a virtual connection. Cloud-based data may be accessed and changed without the use of any physical resources. End-node IoT devices, which deliver information and services via information and communication technology, are vulnerable to cyber-attacks because they lack intelligence and resources

IoT plays a huge role in enabling mobility. However, without adequate protection, its abilities would be rendered null and void. Preventive, investigative, and remedial controls provided by the cloud have improved the security of IoT. Security precautions have been bolstered through the usage of effective authentication and encryption mechanisms provided. In addition, biometrics have made it feasible for IoT gadgets to manage and secure user identities. The cloud's security makes this feasible.

As in the previous chapter, this thesis will be using Microsoft Azure as a cloud platform and Azure Sentinel as solution for the challenges of privacy and security in the cloud and IoT.

Many benefits may be gained by implementing a hybrid cloud strategy. Especially when selecting Microsoft Azure, this is much more true. Using Azure Hybrid Cloud can provide a number of advantages for enterprises especially for security purposes.

1- You may easily move and manage your data.

2- Build secure hybrid networks in a short time.

3- whole company should have access to enterprise-level security safeguards.

4- Assist in securing one-time passwords.

5- Take advantage of the public cloud's performance and scalability.

6- increase productivity and lower expenses.

5.2 Azure sentinel as a threat monitoring system

With Azure Sentinel, you can access and analyze data from a variety of sources, not only from Microsoft sources. It is difficult to keep track of many workloads' security status in a cloud environment. Azure Sentinel, a cloud-native security information event management (SIEM) and SOAR (Security Orchestration Automated Response) system from Microsoft, is highly scalable. Azure Sentinel provides a single solution for alert detection, threat awareness, proactive hunting, and threat response across the whole company. When it comes to dealing with ever more complex assaults, increased alert volume, and lengthy resolution times, Azure Sentinel provides a birds-eye perspective of the whole company. For example, Log Analytics and Logic Apps are directly integrated with Azure Sentinel, which is built on the whole spectrum of Azure services. In addition to providing Microsoft's threat intelligence stream, Azure Sentinel allows you to put your own threat intelligence into the system. **Figure (14)** will illustrate the main functions of Azure Sentinel.

- **Collect data at cloud scale** both on-premises and in different clouds, across all users, devices, apps, and infrastructure.
- **Detect previously undetected threats** Microsoft's analytics and unrivalled threat intelligence help decrease false positives.
- **Investigate threats with artificial intelligence** at a massive scale, relying leveraging Microsoft's years of cyber security research.
- **Respond to incidents rapidly** built-in automation and orchestration of routine. chores.

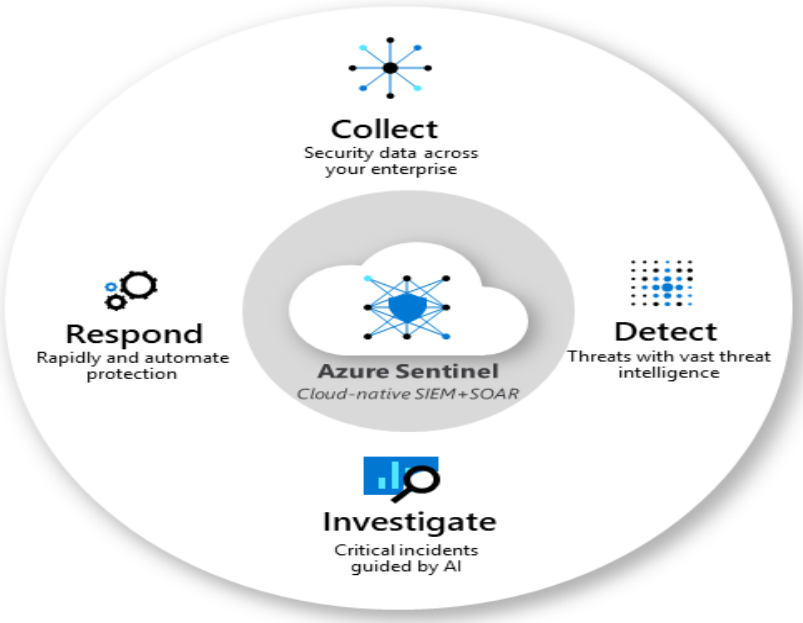


Fig.14. Microsoft Azure Sentinel main functions [23]

Because Azure Sentinel is a component of Azure, you must have an active Azure subscription before you can deploy it. Similarly, to any other SIEM, Azure Sentinel needs to store the data that it collects from the many data sources that you configure. This data will be stored in your specified Log Analytics workspace by Azure Sentinel. Create a new workspace or utilize one that already exists. However, because alert rules and investigations do not operate across workspaces, it is suggested that you create an Azure Sentinel-specific workspace. The workspace is only accessible if you have at least contributor access to the subscription.

5.3 Architecture of azure sentinel

Azure Sentinel's architecture may be better understood by first examining the many components that make up the system. An overview of the key Azure Sentinel components may be seen in **Figure (15)** below.

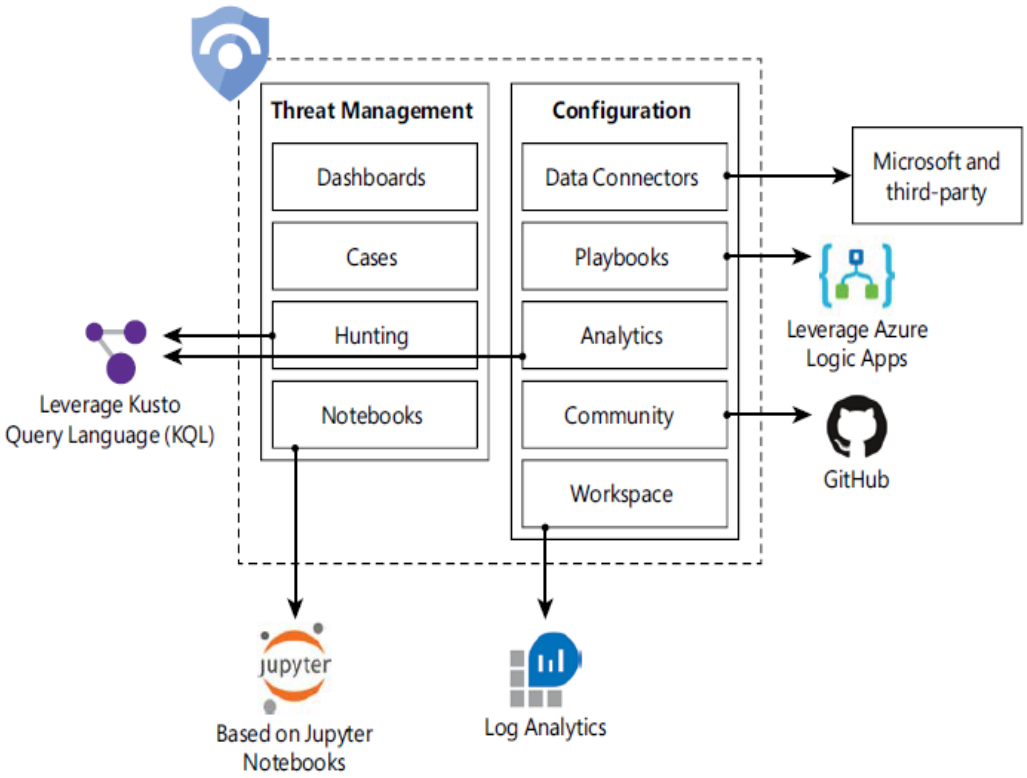


Fig.15. Major components of Azure Sentinel [24]

The components shown in Figure (15) are presented in more detail below:

Dashboards: Data visualisation for your linked data sources is provided through built-in dashboards, allowing you to delve deeper into the events created by those services.
Cases: A case is a collection of all the evidence pertinent to a certain inquiry. One or more alarms depending on your defined analytics can be included in the notification.

Hunting: Investigators and security analysts who need to keep an eye out for potential dangers may find this to be a useful tool. A query language called Kusto is used to power the search function KQL (Kusto Query Language).

Notebooks: You can do more with the data you get from Azure Sentinel by combining it with Jupyter notebooks. A variety of libraries for machine learning, visualisation, and data analysis is included in the notebooks feature.

Data Connectors: Connectors for Microsoft and partner solutions are available to help with data intake.

Playbooks: there are Playbooks that may be used to automate actions when Azure Sentinel issues an alarm. You can automate and orchestrate processes and workflows with Azure Logic Apps, which are used in Playbooks.

Analytics: You may use Kusto Query Language to build custom alerts in Analytics (KQL).

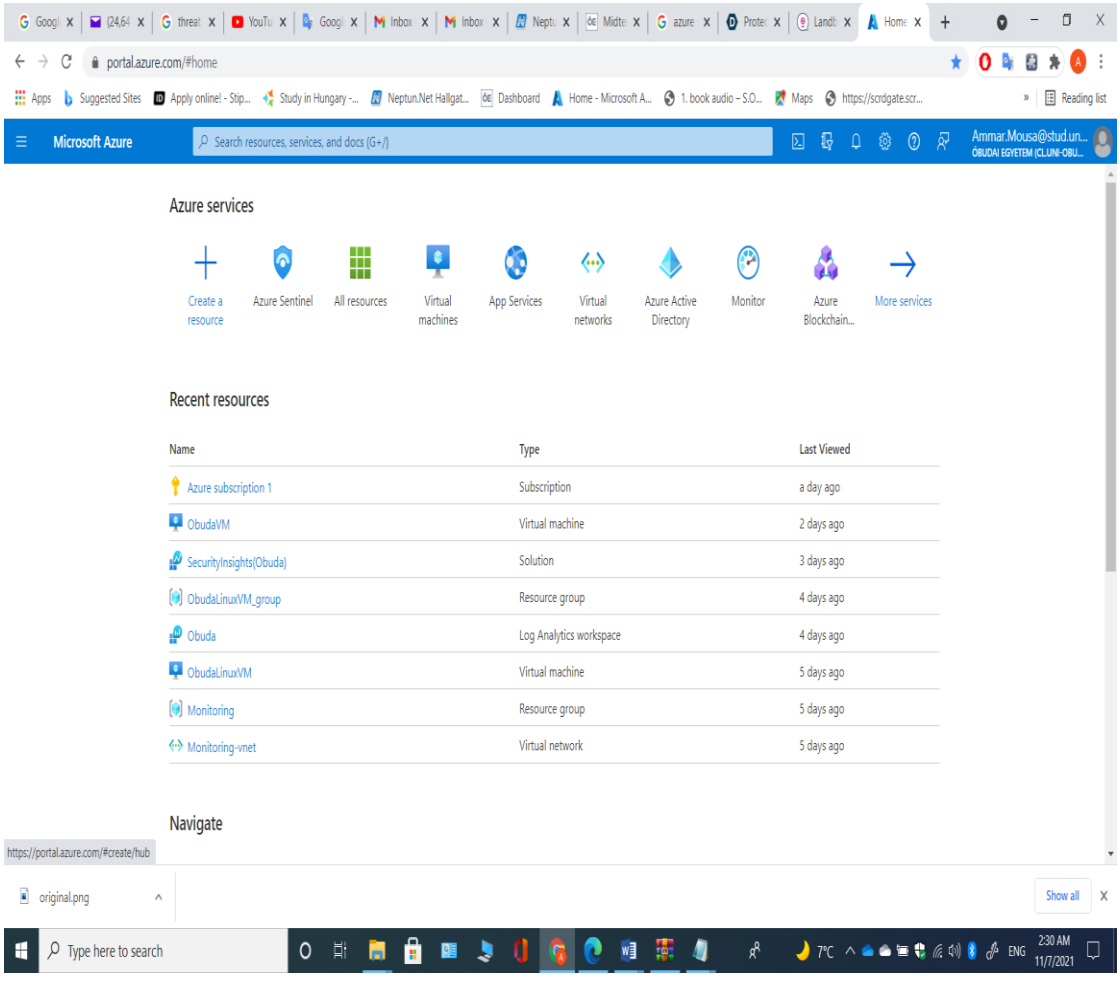
Community: If you're interested in creating alerts and responding to risks in your environment, the Azure Sentinel Community page on GitHub has Detections based on several data sources. Hunting query examples, playbooks, and other artefacts may be found on the Azure Sentinel Community website.

Workspace: Data and configuration information may be found in a Log Analytics workspace, which is just a container. This container is used by Azure Sentinel to store the data it receives from various data sources.

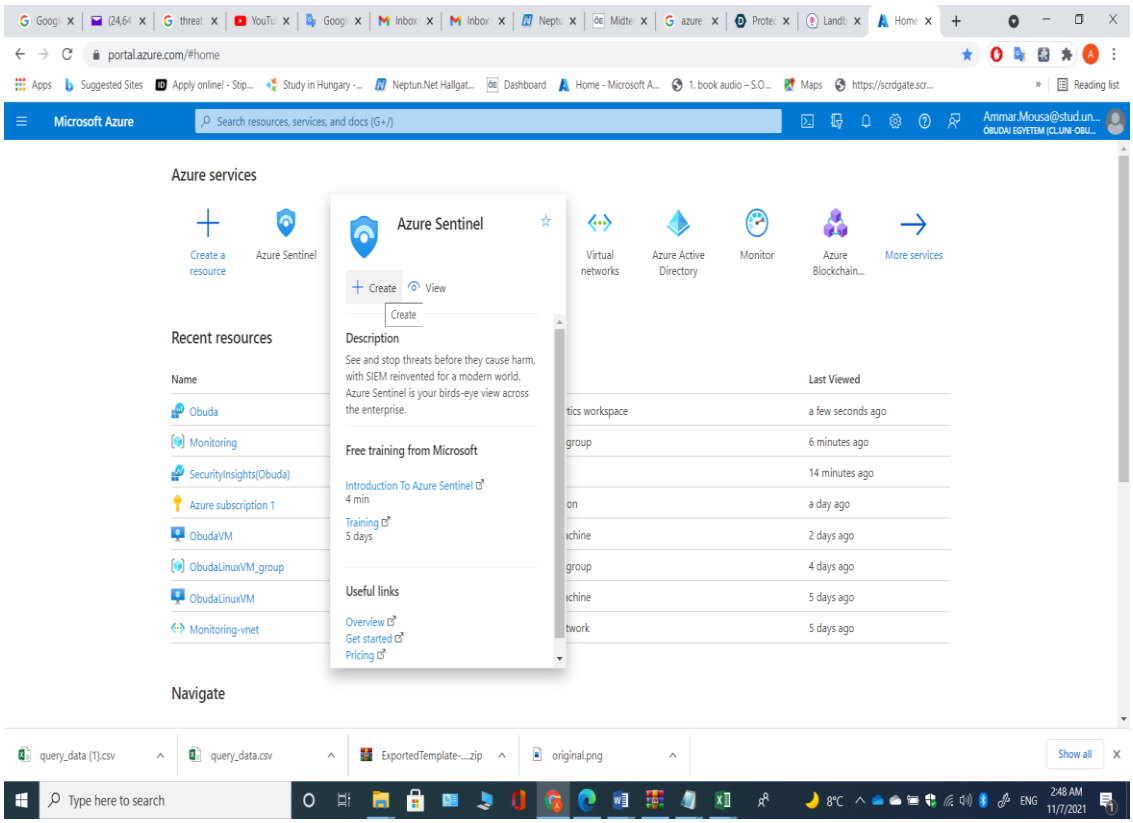
5.4 Creating and preparing azure sentinel

Because Azure Sentinel is a component of Azure, you must have an active Azure subscription before you can deploy it. Azure Sentinel, like any other SIEM, need a place to save the data it gathers from the many data sources you set up for use. Your specified Log Analytics workspace will be used to store this data. You have the option of setting up a whole new workplace or utilizing an already existing one. However, because alert rules and investigations do not operate across workspaces, it is highly advised that you have an Azure Sentinel-specific workspace set aside just for this purpose.

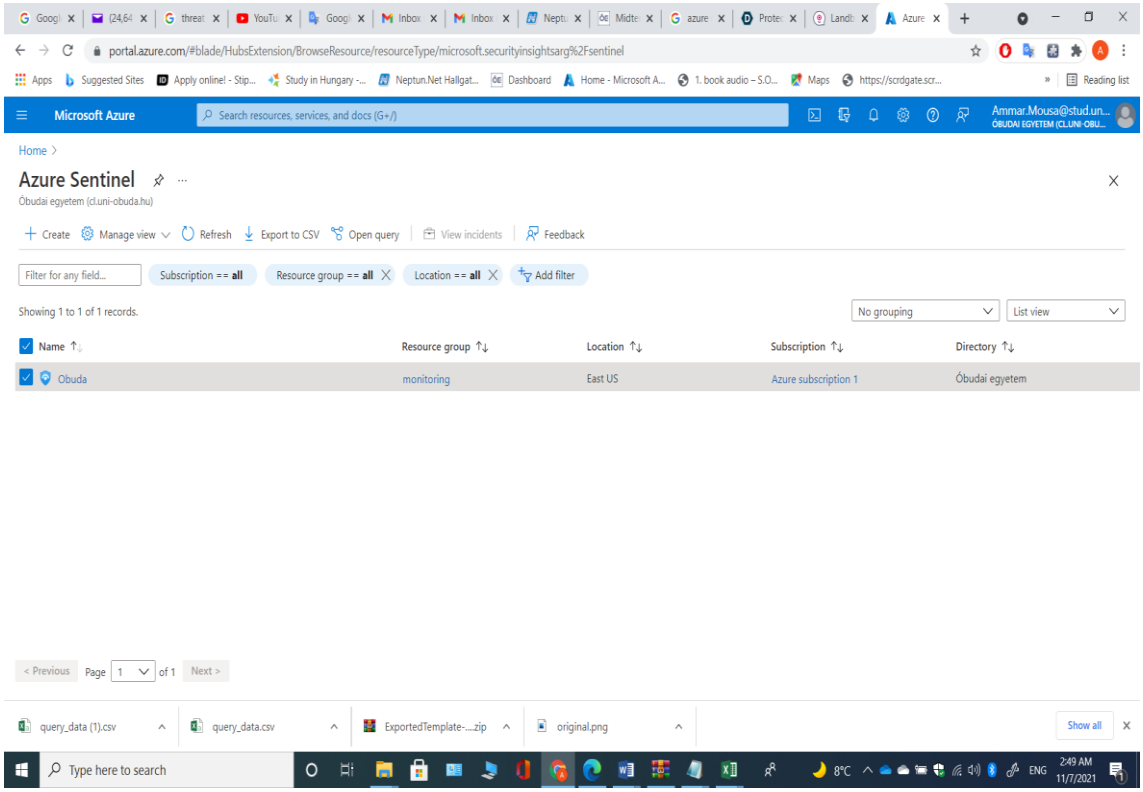
The following screens (a-k) illustrate my Azure account and the steps for creating Azure sentinel and Log Analytics workspace



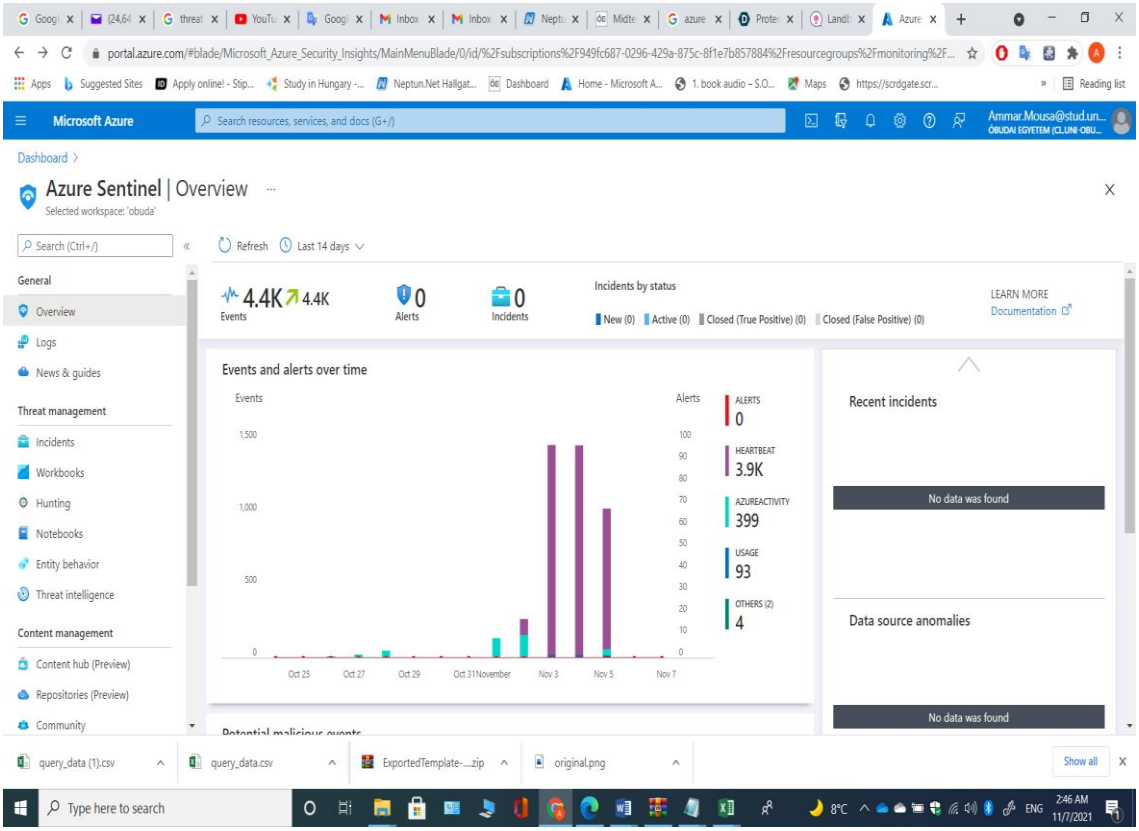
(a)


portal.azure.com/#home
Microsoft Azure
Search resources, services, and docs (G+/)
Azure services
Create a resource
Azure Sentinel
Virtual networks
Azure Active Directory
Monitor
Azure Blockchain...
More services
Recent resources
Name
Last Viewed
Obuda
Monitoring
SecurityInsights(Obuda)
Azure subscription 1
ObudaVM
ObudaLinuxVM_group
ObudaLinuxVM
Monitoring-vnet
a few seconds ago
6 minutes ago
14 minutes ago
a day ago
2 days ago
4 days ago
5 days ago
5 days ago
Azure Sentinel
Create
View
Description
See and stop threats before they cause harm, with SIEM reinvented for a modern world. Azure Sentinel is your birds-eye view across the enterprise.
Free training from Microsoft
Introduction To Azure Sentinel
4 min
Training
5 days
Useful links
Overview
Get started
Pricing
Navigate
query_data (1).csv
query_data.csv
ExportedTemplate-....zip
original.png
Show all
Type here to search
2:48 AM
11/7/2021

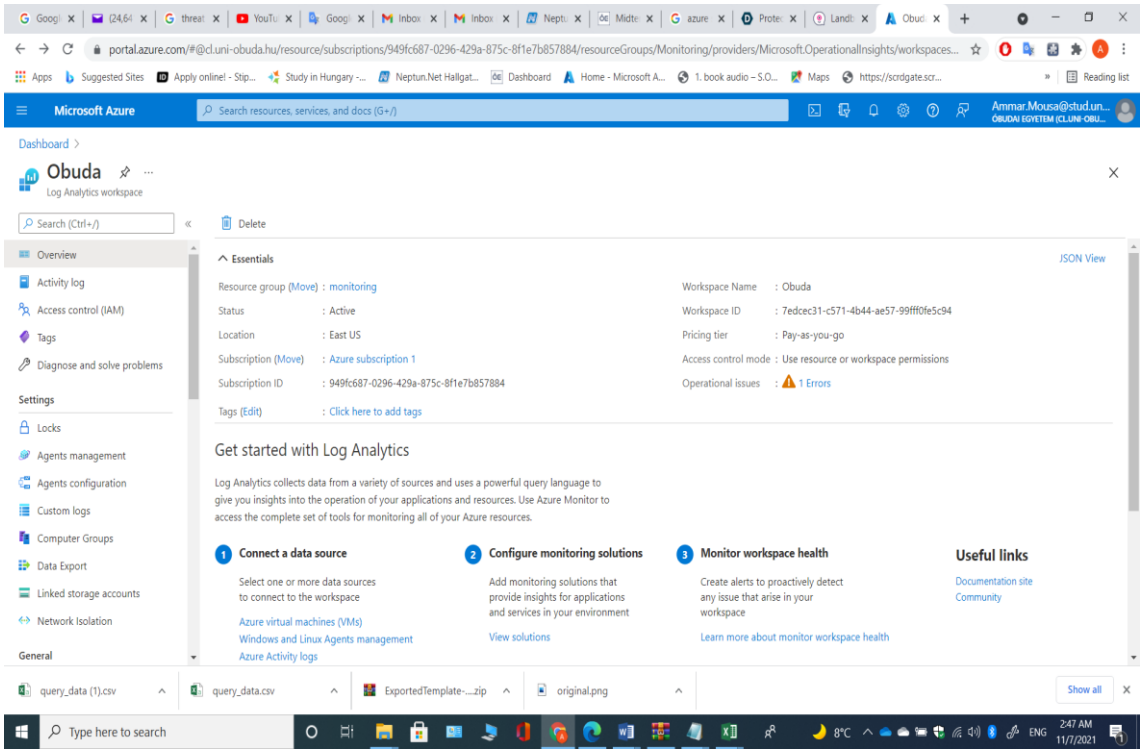
(b)


portal.azure.com/#blade/HubsExtension/BrowseResource/resourceType/microsoft.securityinsightsarg%2Fsentinel
Microsoft Azure
Search resources, services, and docs (G+/)
Home
Azure Sentinel
Obudai egyetem (cl.uni-obuda.hu)
Create
Manage view
Refresh
Export to CSV
Open query
View incidents
Feedback
Filter for any field...
Subscription == all
Resource group == all
Location == all
Add filter
Showing 1 to 1 of 1 records.
No grouping
List view
Name
Resource group
Location
Subscription
Directory
Obuda
monitoring
East US
Azure subscription 1
Obudai egyetem
< Previous
Page 1 of 1
Next >
query_data (1).csv
query_data.csv
ExportedTemplate-....zip
original.png
Show all
Type here to search
2:49 AM
11/7/2021

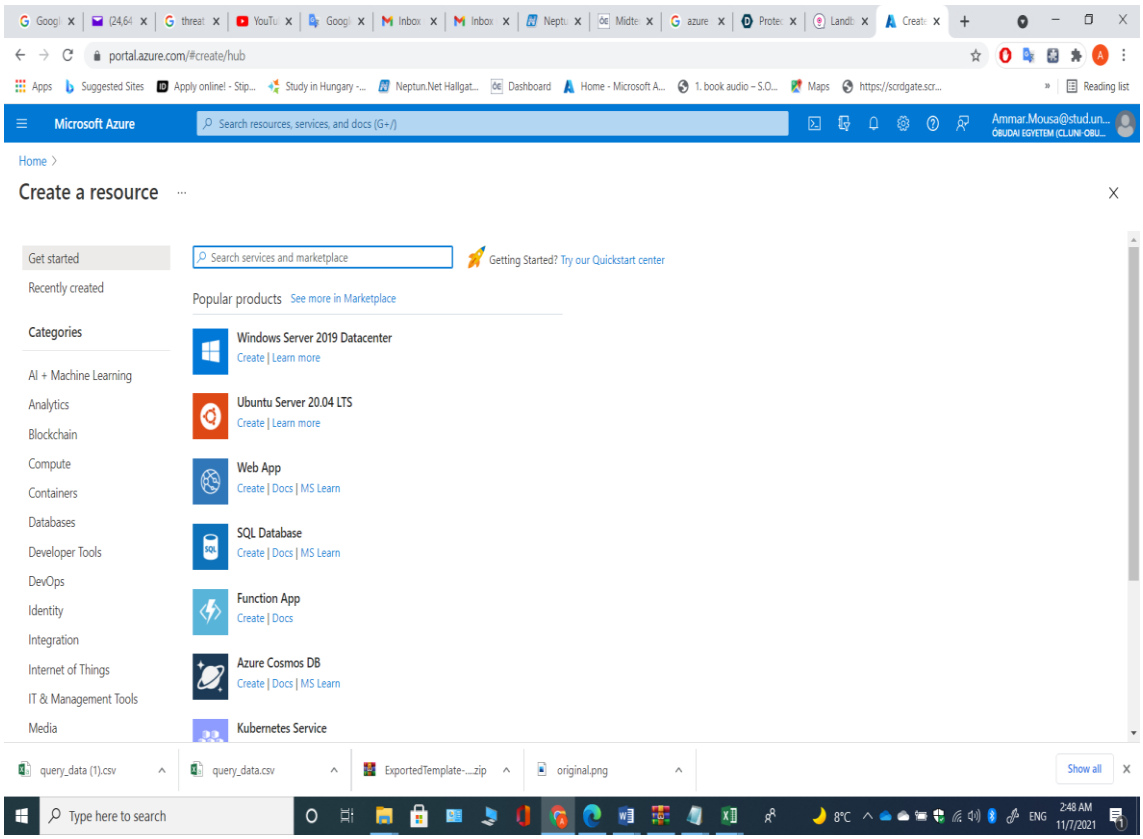
(c)


Microsoft Azure
Search resources, services, and docs (G+/)
Dashboard
Azure Sentinel | Overview
Selected workspace: 'obuda'
Search (Ctrl+/)
Refresh
Last 14 days
General
Overview
Logs
News & guides
Threat management
Incidents
Workbooks
Hunting
Notebooks
Entity behavior
Threat intelligence
Content management
Content hub (Preview)
Repositories (Preview)
Community
4.4K 4.4K
Events
0
Alerts
0
Incidents
Incidents by status
New (0)
Active (0)
Closed (True Positive) (0)
Closed (False Positive) (0)
LEARN MORE
Documentation
Events and alerts over time
Events
Alerts
ALERTS
0
HEARTBEAT
3.9K
AZUREACTIVITY
399
USAGE
93
OTHERS (2)
4
Recent incidents
No data was found
Data source anomalies
No data was found
Oct 25
Oct 27
Oct 29
Oct 31
November
Nov 3
Nov 5
Nov 7
query_data (1).csv
query_data.csv
ExportedTemplate-....zip
original.png
Show all
Type here to search
8°C
ENG
2:46 AM
11/7/2021

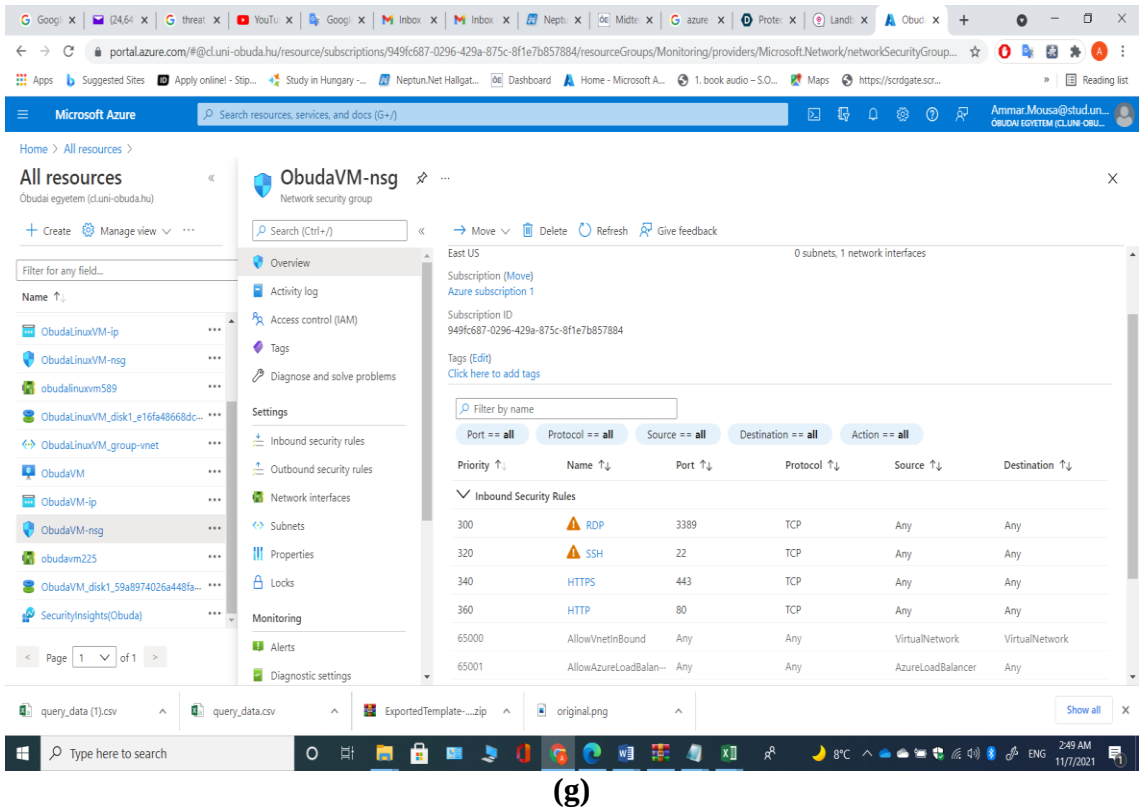
(d)


Microsoft Azure
Search resources, services, and docs (G+/)
Dashboard
Obuda
Log Analytics workspace
Search (Ctrl+/)
Delete
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Locks
Agents management
Agents configuration
Custom logs
Computer Groups
Data Export
Linked storage accounts
Network Isolation
General
Essentials
JSON View
Resource group (Move) : monitoring
Status : Active
Location : East US
Subscription (Move) : Azure subscription 1
Subscription ID : 949fc687-0296-429a-875c-8f1e7b857884
Tags (Edit) : Click here to add tags
Workspace Name : Obuda
Workspace ID : 7edcec31-c571-4b44-ae57-99fff0fe5c94
Pricing tier : Pay-as-you-go
Access control mode : Use resource or workspace permissions
Operational issues : 1 Errors
Get started with Log Analytics
Log Analytics collects data from a variety of sources and uses a powerful query language to give you insights into the operation of your applications and resources. Use Azure Monitor to access the complete set of tools for monitoring all of your Azure resources.
1 Connect a data source
Select one or more data sources to connect to the workspace
Azure virtual machines (VMs)
Windows and Linux Agents management
Azure Activity logs
2 Configure monitoring solutions
Add monitoring solutions that provide insights for applications and services in your environment
View solutions
3 Monitor workspace health
Create alerts to proactively detect any issue that arise in your workspace
Learn more about monitor workspace health
Useful links
Documentation site
Community
query_data (1).csv
query_data.csv
ExportedTemplate-....zip
original.png
Show all
Type here to search
8°C
ENG
2:47 AM
11/7/2021

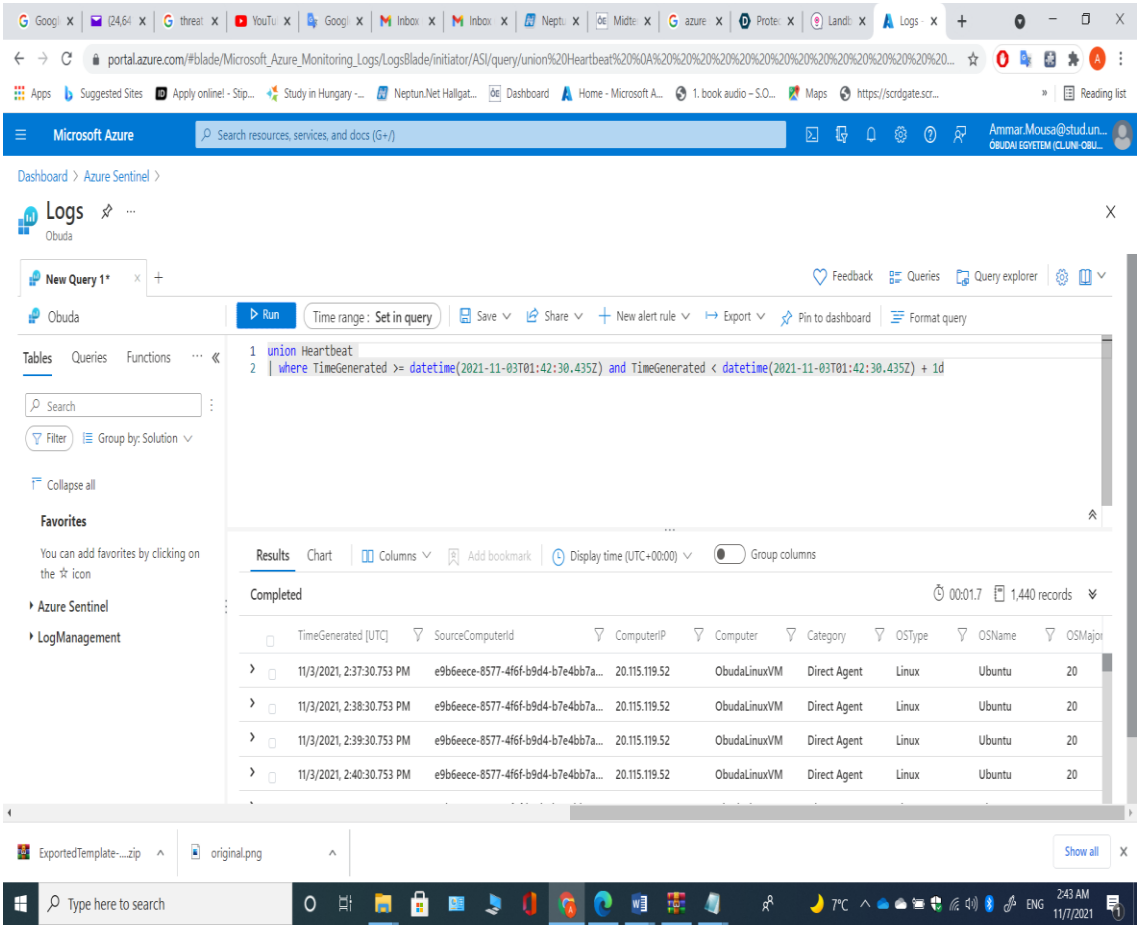
(e)


portal.azure.com/#create/hub
Microsoft Azure
Search resources, services, and docs (G+/)
Home
Create a resource
Get started
Recently created
Categories
AI + Machine Learning
Analytics
Blockchain
Compute
Containers
Databases
Developer Tools
DevOps
Identity
Integration
Internet of Things
IT & Management Tools
Media
Search services and marketplace
Getting Started? Try our Quickstart center
Popular products See more in Marketplace
Windows Server 2019 Datacenter
Create | Learn more
Ubuntu Server 20.04 LTS
Create | Learn more
Web App
Create | Docs | MS Learn
SQL Database
Create | Docs | MS Learn
Function App
Create | Docs
Azure Cosmos DB
Create | Docs | MS Learn
Kubernetes Service
query_data (1).csv
query_data.csv
ExportedTemplate-....zip
original.png
Show all
Type here to search

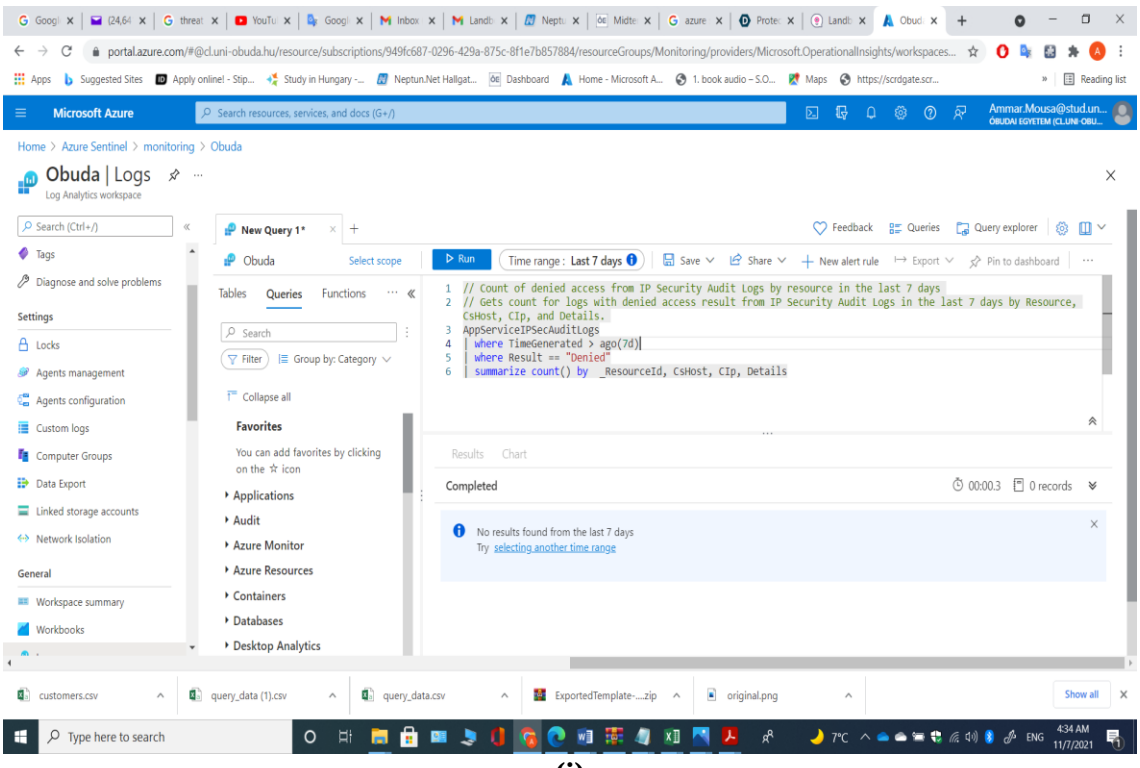
(f)


portal.azure.com/#@cl.uni-obuda.hu/resource/subscriptions/949fc687-0296-429a-875c-8f1e7b857884/resourceGroups/Monitoring/providers/Microsoft.Network/networkSecurityGroup...
Microsoft Azure
Search resources, services, and docs (G+/)
Home > All resources
All resources
Óbudai egyetem (cl.uni-obuda.hu)
Create
Manage view
Filter for any field...
Name
ObudaLinuxVM-ip
ObudaLinuxVM-nsg
obudalinuxvm589
ObudaLinuxVM_disk1_e16fa48668dc...
ObudaLinuxVM_group-vnet
ObudaVM
ObudaVM-ip
ObudaVM-nsg
obudavm225
ObudaVM_disk1_59a8974026a448fa...
SecurityInsights(Obuda)
Page 1 of 1
ObudaVM-nsg
Network security group
Search (Ctrl+/)
Move
Delete
Refresh
Give feedback
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Inbound security rules
Outbound security rules
Network interfaces
Subnets
Properties
Locks
Monitoring
Alerts
Diagnostic settings
East US
0 subnets, 1 network interfaces
Subscription (Move)
Azure subscription 1
Subscription ID
949fc687-0296-429a-875c-8f1e7b857884
Tags (Edit)
Click here to add tags
Filter by name
Port == all
Protocol == all
Source == all
Destination == all
Action == all
Priority
Name
Port
Protocol
Source
Destination
Inbound Security Rules
300 RDP 3389 TCP Any Any
320 SSH 22 TCP Any Any
340 HTTPS 443 TCP Any Any
360 HTTP 80 TCP Any Any
65000 AllowVnetInBound Any Any VirtualNetwork VirtualNetwork
65001 AllowAzureLoadBalan... Any Any AzureLoadBalancer Any
query_data (1).csv
query_data.csv
ExportedTemplate-....zip
original.png
Show all
Type here to search

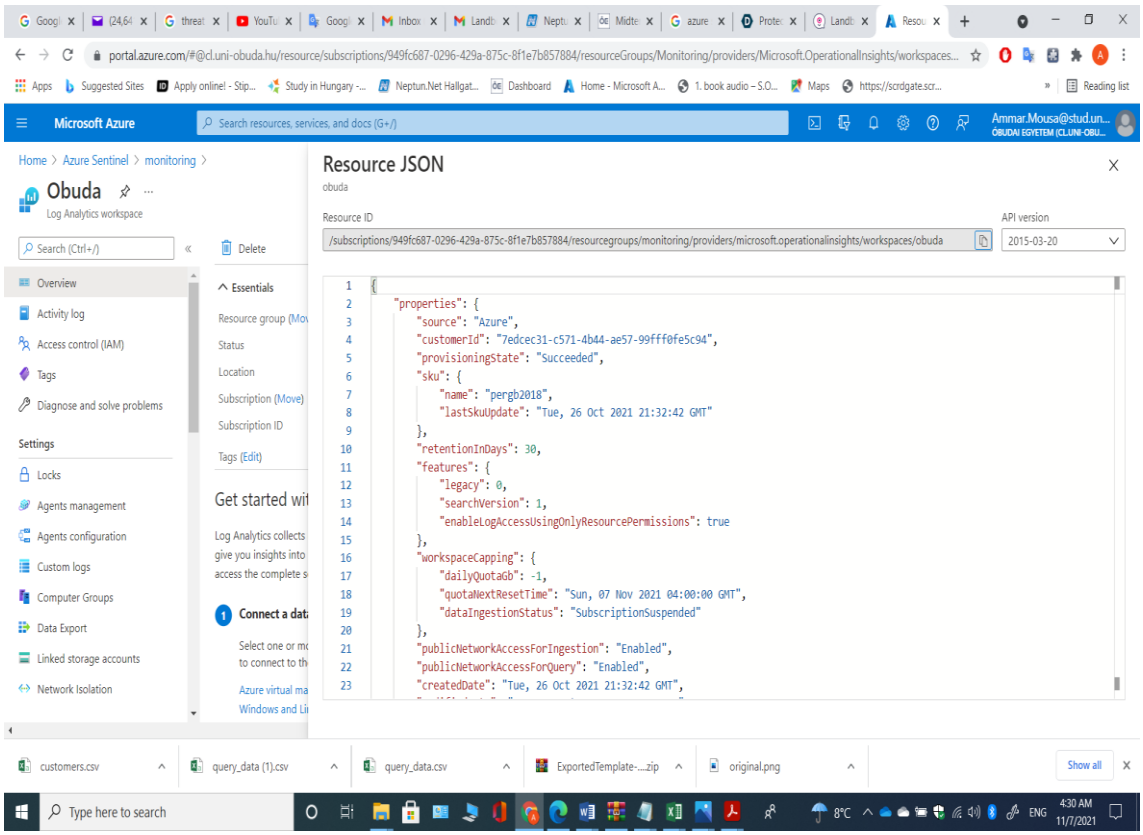
(g)


Microsoft Azure
Search resources, services, and docs (G+/)
Dashboard > Azure Sentinel >
Logs
Obuda
New Query 1*
Feedback
Queries
Query explorer
Run
Time range : Set in query
Save
Share
New alert rule
Export
Pin to dashboard
Format query
Tables
Queries
Functions
Search
Filter
Group by: Solution
Collapse all
Favorites
You can add favorites by clicking on the ☆ icon
Azure Sentinel
LogManagement
1 union Heartbeat
2 | where TimeGenerated >= datetime(2021-11-03T01:42:30.435Z) and TimeGenerated < datetime(2021-11-03T01:42:30.435Z) + 1d
Results
Chart
Columns
Add bookmark
Display time (UTC+00:00)
Group columns
Completed
00:01.7
1,440 records
TimeGenerated [UTC]
SourceComputerId
ComputerIP
Computer
Category
OSType
OSName
11/3/2021, 2:37:30.753 PM e9b6eece-8577-4f6f-b9d4-b7e4bb7a... 20.115.119.52 ObudaLinuxVM Direct Agent Linux Ubuntu 20
11/3/2021, 2:38:30.753 PM e9b6eece-8577-4f6f-b9d4-b7e4bb7a... 20.115.119.52 ObudaLinuxVM Direct Agent Linux Ubuntu 20
11/3/2021, 2:39:30.753 PM e9b6eece-8577-4f6f-b9d4-b7e4bb7a... 20.115.119.52 ObudaLinuxVM Direct Agent Linux Ubuntu 20
11/3/2021, 2:40:30.753 PM e9b6eece-8577-4f6f-b9d4-b7e4bb7a... 20.115.119.52 ObudaLinuxVM Direct Agent Linux Ubuntu 20
ExportedTemplate-....zip
original.png
Show all
Type here to search
2:43 AM
11/7/2021

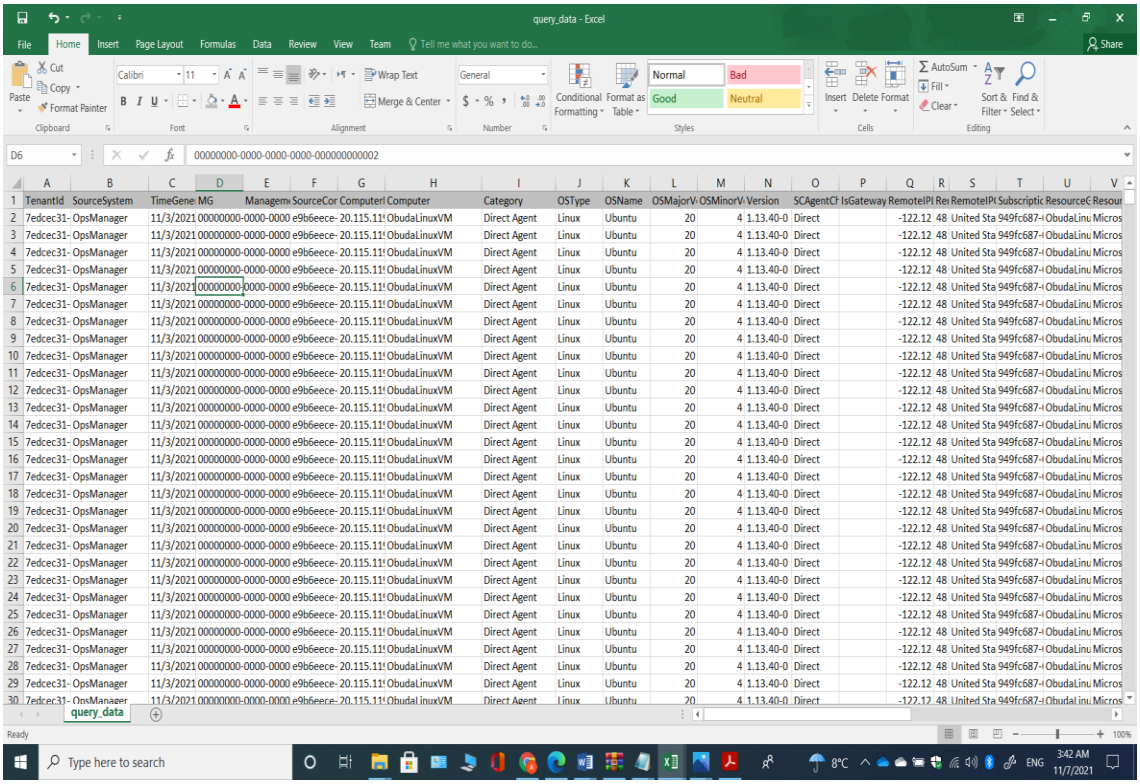
(h)


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Azure Sentinel > monitoring > Obuda
Obuda | Logs
Log Analytics workspace
Search (Ctrl+/)
Tags
Diagnose and solve problems
Settings
Locks
Agents management
Agents configuration
Custom logs
Computer Groups
Data Export
Linked storage accounts
Network Isolation
General
Workspace summary
Workbooks
New Query 1*
Obuda
Select scope
Run
Time range : Last 7 days
Save
Share
New alert rule
Export
Pin to dashboard
Feedback
Queries
Query explorer
Tables
Queries
Functions
Search
Filter
Group by: Category
Collapse all
Favorites
You can add favorites by clicking on the ☆ icon
Applications
Audit
Azure Monitor
Azure Resources
Containers
Databases
Desktop Analytics
1 // Count of denied access from IP Security Audit Logs by resource in the last 7 days
2 // Gets count for logs with denied access result from IP Security Audit Logs in the last 7 days by Resource, CsHost, CIp, and Details.
3 AppServiceIPSecAuditLogs
4 | where TimeGenerated > ago(7d)
5 | where Result == "Denied"
6 | summarize count() by _ResourceId, CsHost, CIp, Details
Results
Chart
Completed
00:00.3
0 records
No results found from the last 7 days
Try selecting another time range
customers.csv
query_data (1).csv
query_data.csv
ExportedTemplate-....zip
original.png
Show all
Type here to search
4:34 AM
11/7/2021

(i)


Microsoft Azure
Search resources, services, and docs (G+/)
Ammar.Mousa@stud.un...
ÓBUDAI EGYETEM (CI.UNI-OBU...
Home > Azure Sentinel > monitoring >
Obuda
Log Analytics workspace
Search (Ctrl+/)
Delete
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Locks
Agents management
Agents configuration
Custom logs
Computer Groups
Data Export
Linked storage accounts
Network Isolation
Essentials
Resource group (Mov
Status
Location
Subscription (Move)
Subscription ID
Tags (Edit)
Get started wit
Log Analytics collects
give you insights into
access the complete s
Connect a data
Select one or mo
to connect to th
Azure virtual ma
Windows and Li
Resource JSON
obuda
Resource ID
/subscriptions/949fc687-0296-429a-875c-8f1e7b857884/resourcegroups/monitoring/providers/microsoft.operationalinsights/workspaces/obuda
API version
2015-03-20
{
"properties": {
"source": "Azure",
"customerId": "7edcec31-c571-4b44-ae57-99fff0fe5c94",
"provisioningState": "Succeeded",
"sku": {
"name": "pergb2018",
"lastSkuUpdate": "Tue, 26 Oct 2021 21:32:42 GMT"
},
"retentionInDays": 30,
"features": {
"legacy": 0,
"searchVersion": 1,
"enableLogAccessUsingOnlyResourcePermissions": true
},
"workspaceCapping": {
"dailyQuotaGb": -1,
"quotaNextResetTime": "Sun, 07 Nov 2021 04:00:00 GMT",
"dataIngestionStatus": "SubscriptionSuspended"
},
"publicNetworkAccessForIngestion": "Enabled",
"publicNetworkAccessForQuery": "Enabled",
"createdDate": "Tue, 26 Oct 2021 21:32:42 GMT",
customers.csv
query_data (1).csv
query_data.csv
ExportedTemplate-....zip
original.png
Show all
Type here to search
4:30 AM
11/7/2021

(j)


query_data - Excel
File
Home
Insert
Page Layout
Formulas
Data
Review
View
Team
Tell me what you want to do...
Share
Cut
Copy
Format Painter
Paste
Calibri
11
Wrap Text
General
Merge & Center
Conditional Formatting
Format as Table
Normal
Bad
Good
Neutral
Insert
Delete
Format
AutoSum
Fill
Clear
Sort & Filter
Find & Select
Clipboard
Font
Alignment
Number
Styles
Cells
Editing
D6
00000000-0000-0000-0000-000000000002
TenantId SourceSystem TimeGene MG Managem SourceCor Computer Computer Category OSType OSName OSMajorV OSMinorV Version SCAgentCh IsGateway RemoteIPI Rer RemoteIPL Subscriptic ResourceG Resour
7edcec31- OpsManager 11/3/2021 00000000-0000-0000 e9b6eece- 20.115.11 ObudaLinuxVM Direct Agent Linux Ubuntu 20 4 1.13.40-0 Direct -122.12 48 United Sta 949fc687-(ObudaLinu Micros
query_data
Ready
Type here to search
3:42 AM
11/7/2021

(k)

Chapter 6: Establishing the digital assistance architecture

6.1 Creating a cloud landbot (Obuda bot)

Although chatbots are becoming popular, not all of their security concerns have been satisfactorily addressed. Chatbots are used for a variety of purposes, including retail, banking, meal delivery, healthcare, and more. The problem is that it adds an extra security risk and presents major security difficulties that must be addressed. [25]

This cloud-based chatbot system enables small and medium businesses to develop conversational websites, landing pages, surveys, and lead generation chat-bots that communicate with consumers more effectively and increase conversion rates. I made a survey Landbot (Obuda bot) about Microsoft Azure cloud system throw-out the following steps:

1- Set Up Free Landbot Account Using your email.

2- Adding your name and company name and description about the company.

3- Choose Your Channel. And what you intend to use Landbot for such as (surveys & quizzes, internal communications, etc.).

4- After that describe your experience with using Chatbot (beginner, intermediate, advanced).

5- Select all tools you are currently using such as (google analytics, google sheets, WhatsApp business, salesforce, etc.)

6- You will see your canvas and then build a robot.

7- You can Optimize the Welcome Message. There are a lot of options to edit chat bot and make it more useful.

8- Add Your First Sequence. Drag from default to the next block for example (send a message).

9- Write a message for example (Awesome! You are here). you can add media again

10- You can add Ask a Question (what do you think of Microsoft Azure cloud system?).

11- After that you can drag out another one here and choose a button and you can ask for example (what do you want to do now?) and you can be adding buttons and selecting answers for example (watching a tutorial or subscribing in Ms. Azure).

12- In case selecting **watching a tutorial** you can drag other buttons and ask for example (what do you need to see?) and add buttons for many options, for example (How does Microsoft Azure work? Etc.)

13- For many options you can drag and choose a media and selecting YouTube after that add the URL for the video from YouTube.

14- In case selecting **subscribing in Ms. Azure** you can drag another button and add URL of Microsoft Azure home page.

15- After that drag and add a new button and ask for example (do you want to subscribe to Microsoft. Source newsletter?) and add two option buttons (yes, please) and (No, zero interest).

16- In case of **(No)** drag and adding message (I'm happy to have talked to you have a nice day).

17- In case selecting **(Yes)** You can add a **Question (Name)** followed by a message hello @name And also a **Question (Email).**

18- After that drag and **add buttons** and ask a question **(do you want to edit info?)**
And adding 3 buttons {(No everything is good), (yes, my name needs to edited) followed by a Question (Name), (yes, my email needs to be edited) followed by a Question for (Email)

19- After that drag and adding message (Excellent we are done and you receive an email from Microsoft) and all three buttons will be joining with these message.

20- Finally drag and add (send an email), in this step make the setting for your company email and also the email you will receive the reviews and information on it. **Figure (16)** will illustrate the flow chart of My Cloud bot (Obuda bot)

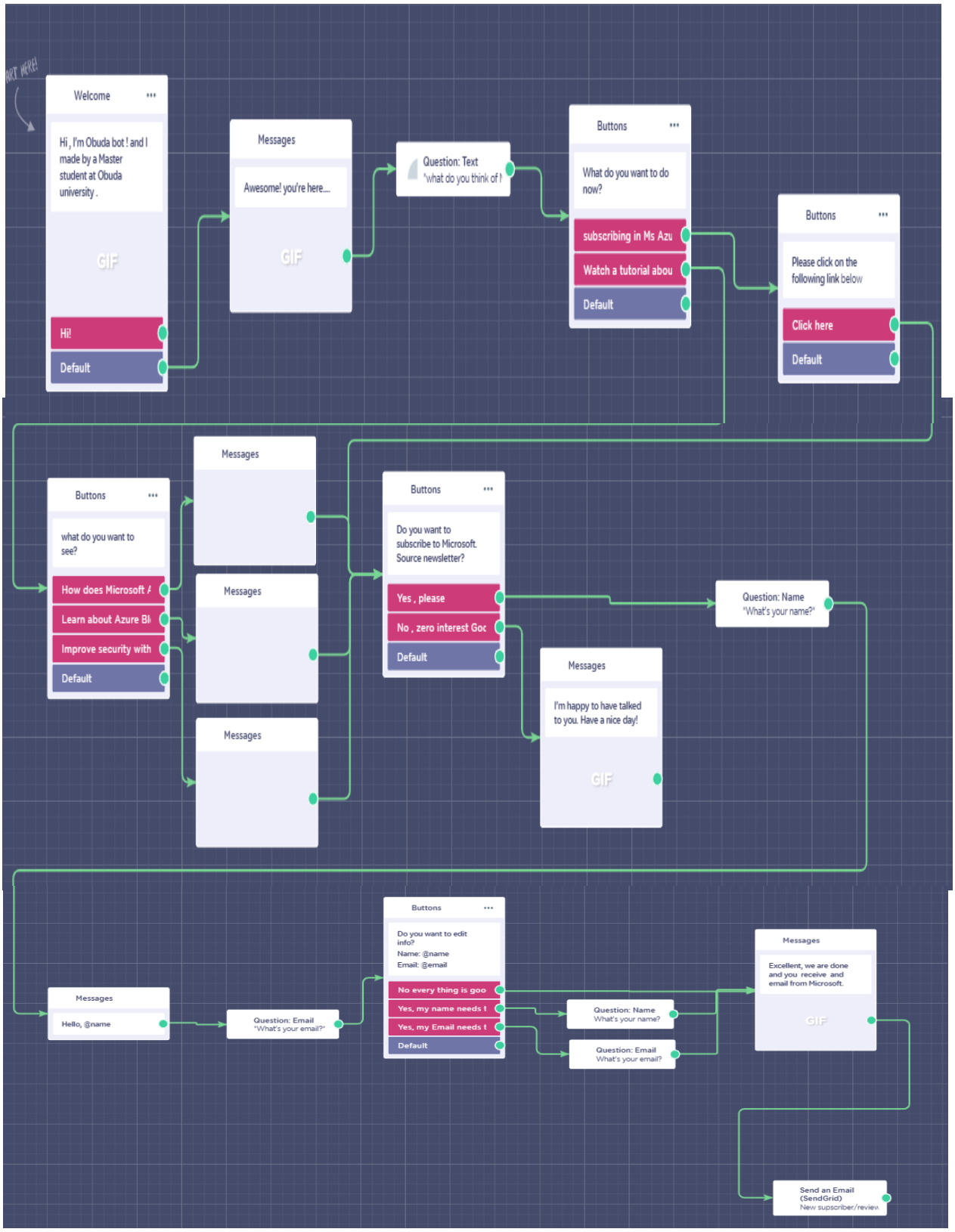
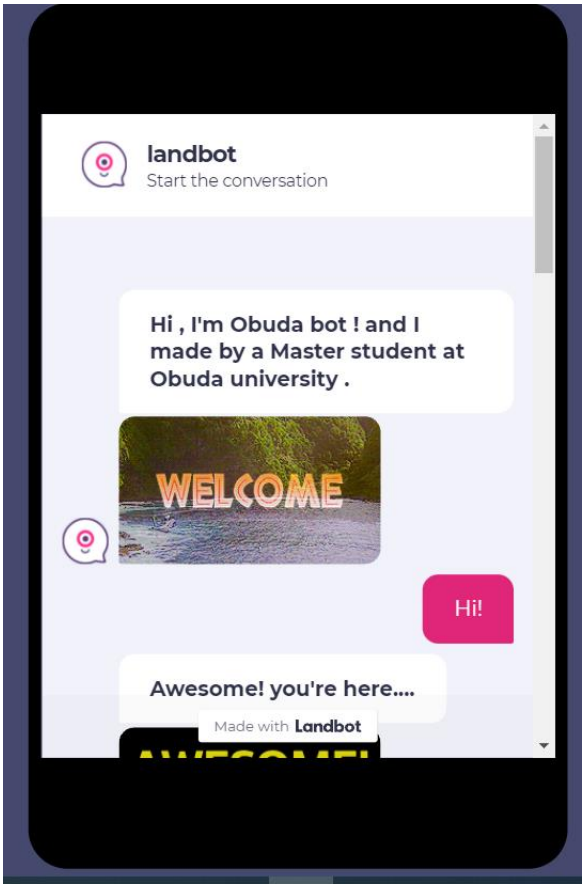


Fig.16. Flow chart of my cloud bot (Obuda bot)

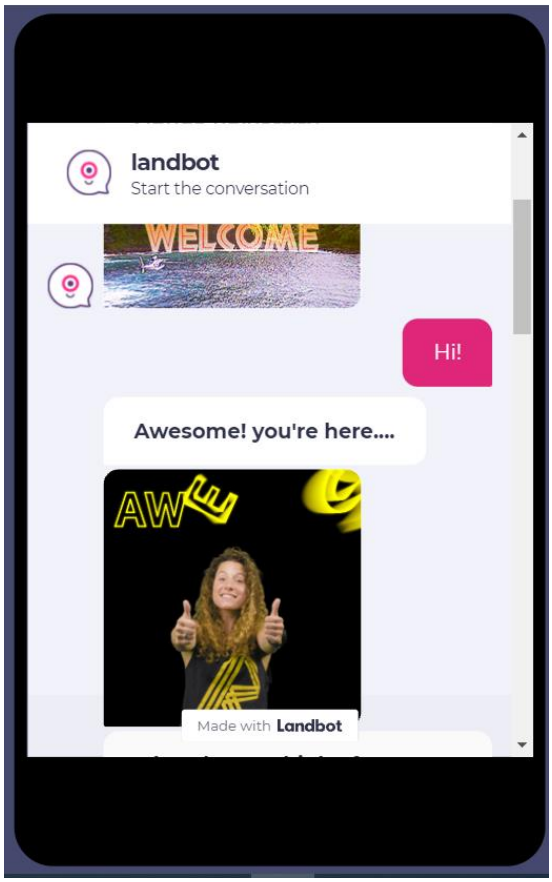
The following Code, link and screens(a-f) of my cloud bot (Obuda bot)

```
<script SameSite="None; Secure" src="https://static.landbot.io/landbot-3/landbot-3.0.0.js"></script>

<script>

  var myLandbot = new Landbot.Livechat({

    configUrl: 'https://chats.landbot.io/v3/H-1016611-U6VWXTQJHJOU6CL9/index.json',

  });

</script>
```

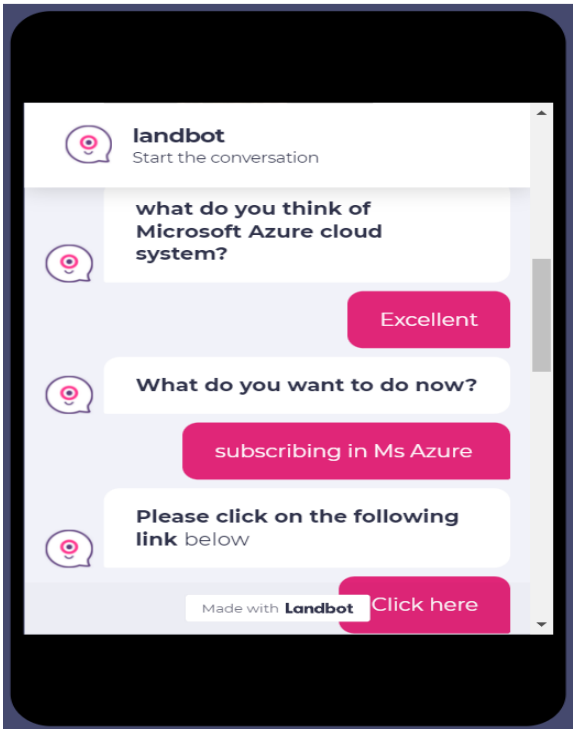
https://chats.landbot.io/v3/H-1016611-U6VWXTQJHJOU6CL9/index.html



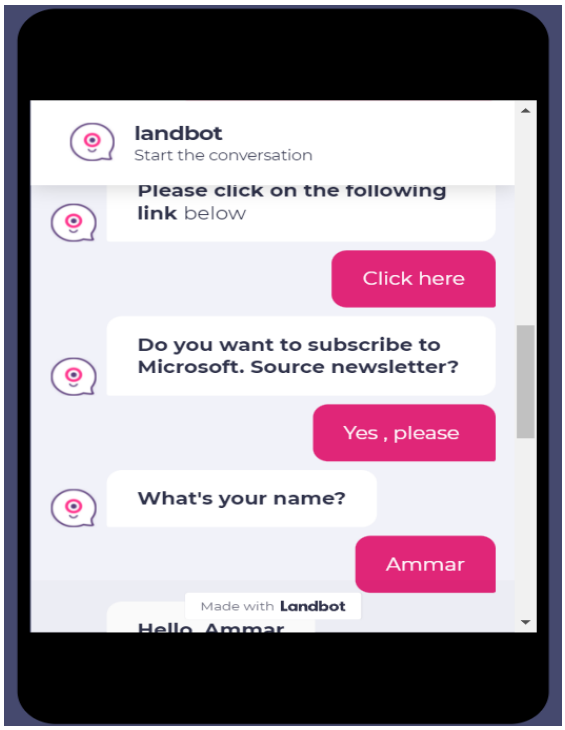
a



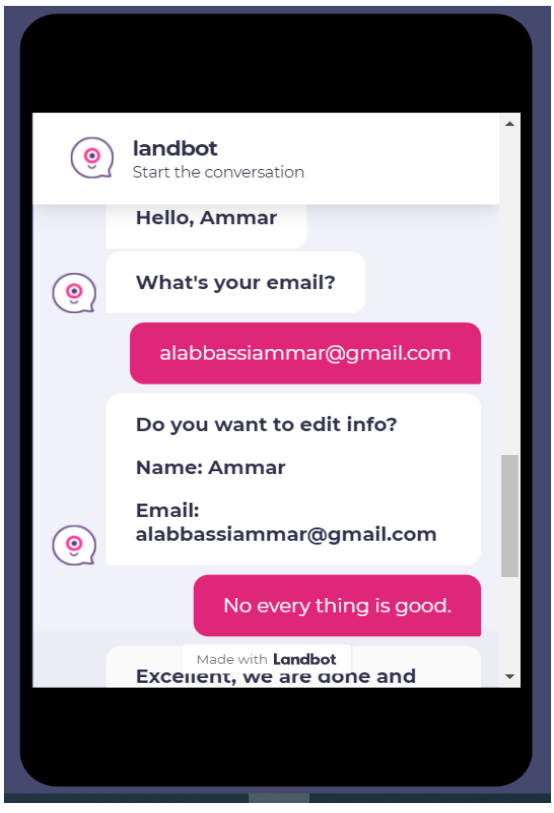
b


landbot
Start the conversation
what do you think of Microsoft Azure cloud system?
Excellent
What do you want to do now?
subscribing in Ms Azure
Please click on the following link below
Made with Landbot
Click here

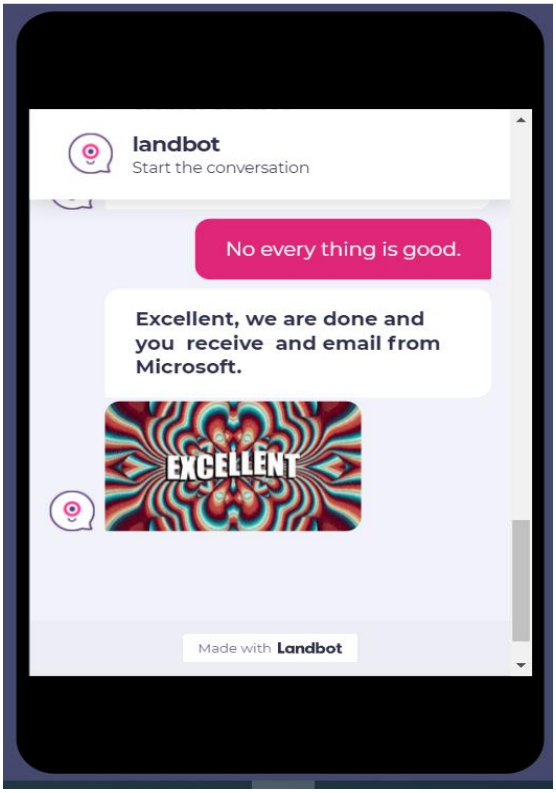
c


landbot
Start the conversation
Please click on the following link below
Click here
Do you want to subscribe to Microsoft. Source newsletter?
Yes , please
What's your name?
Ammar
Made with Landbot

d


landbot
Start the conversation
Hello, Ammar
What's your email?
alabbassiammar@gmail.com
Do you want to edit info?
Name: Ammar
Email: alabbassiammar@gmail.com
No every thing is good.
Made with Landbot

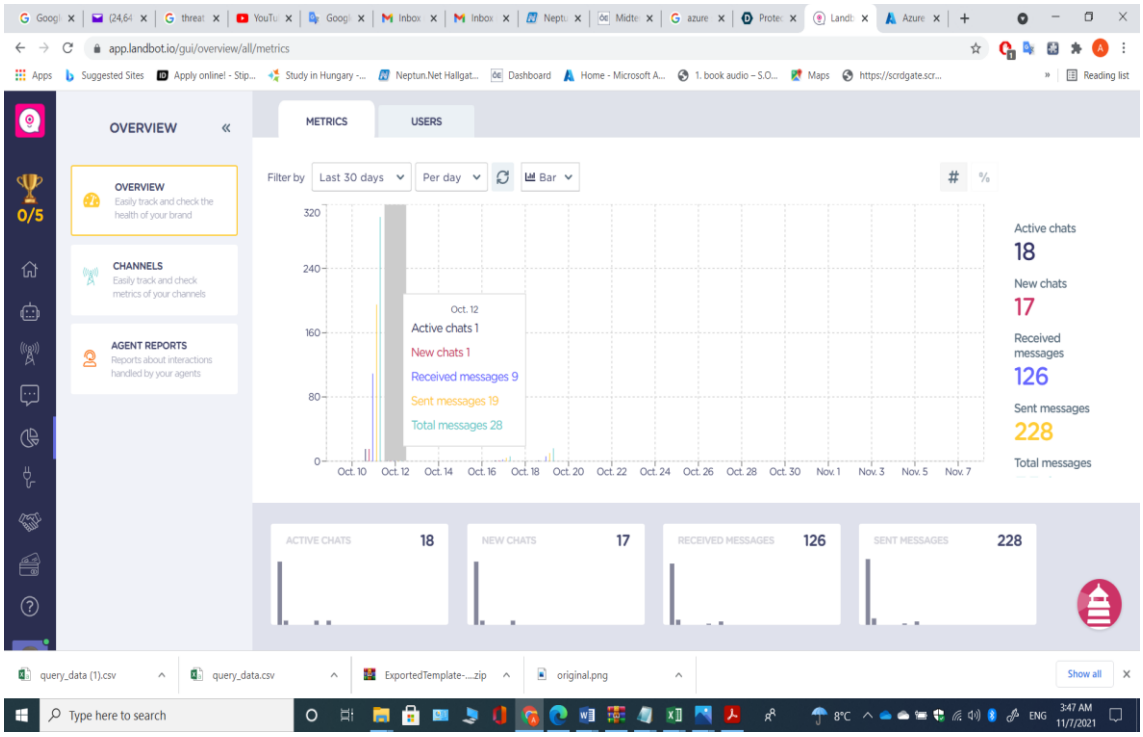
e


landbot
Start the conversation
No every thing is good.
Excellent, we are done and you receive and email from Microsoft.
EXCELLENT
Made with Landbot

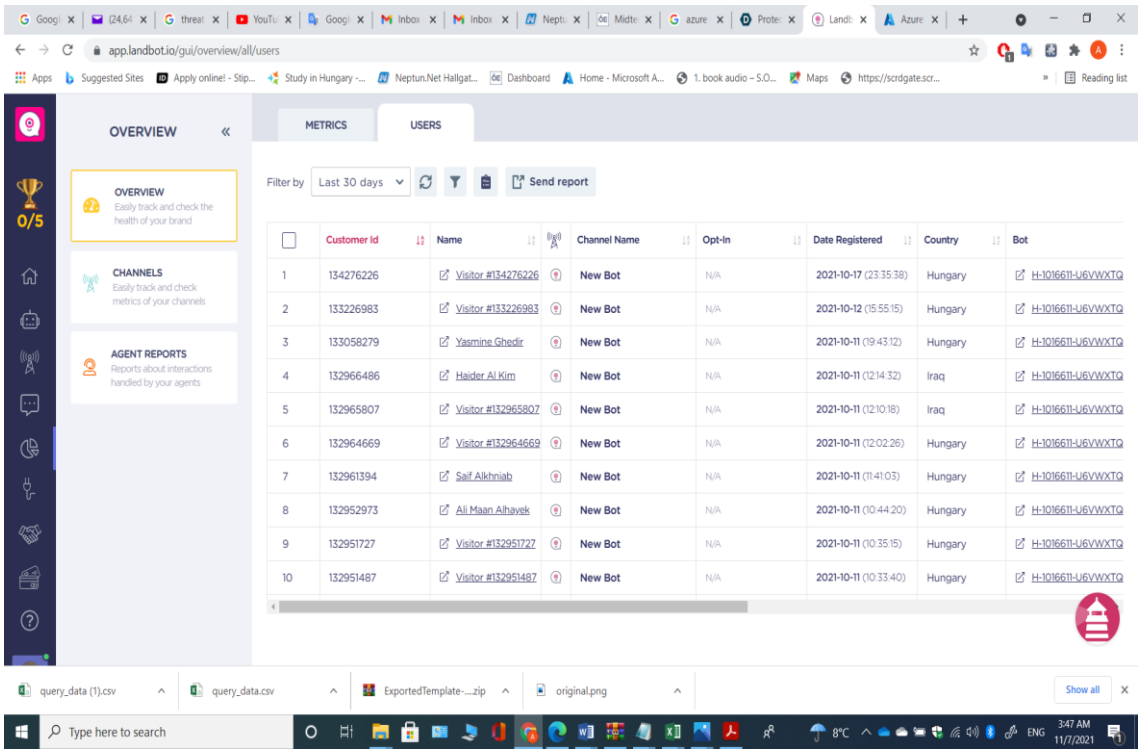
f

6.2 Metrics and user's log data of Obuda bot

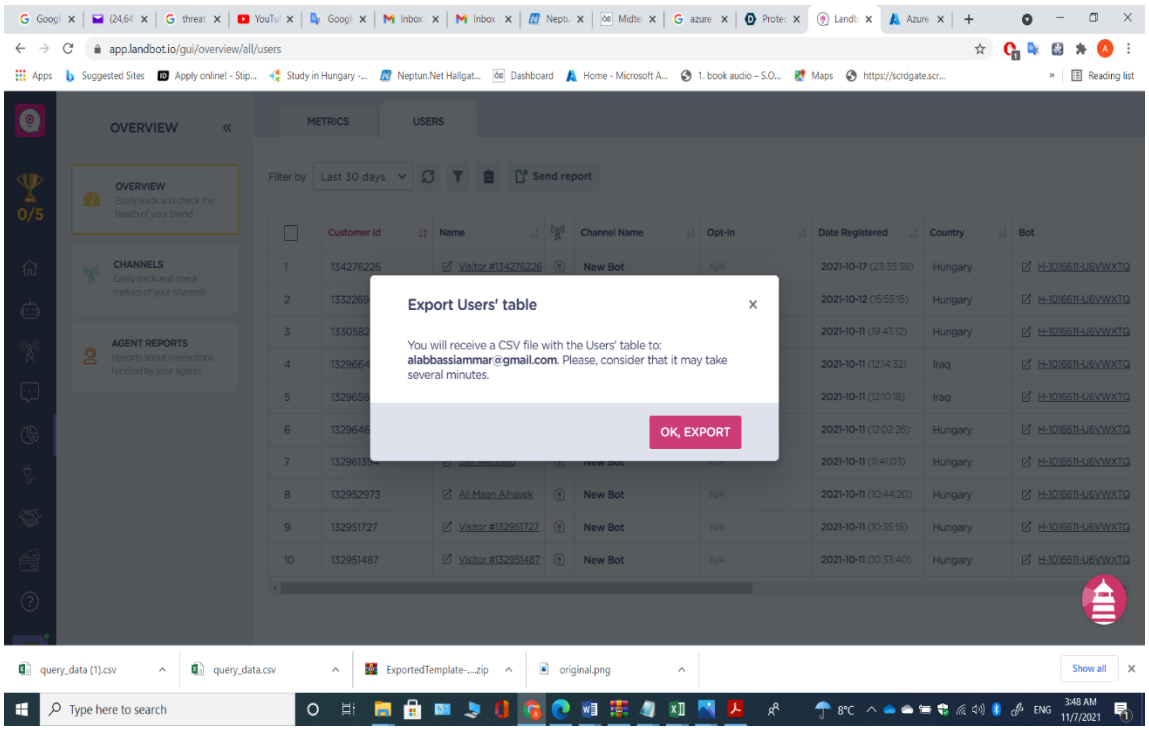
The following screens (a-h) illustrates metrics and user's log data of Obuda bot



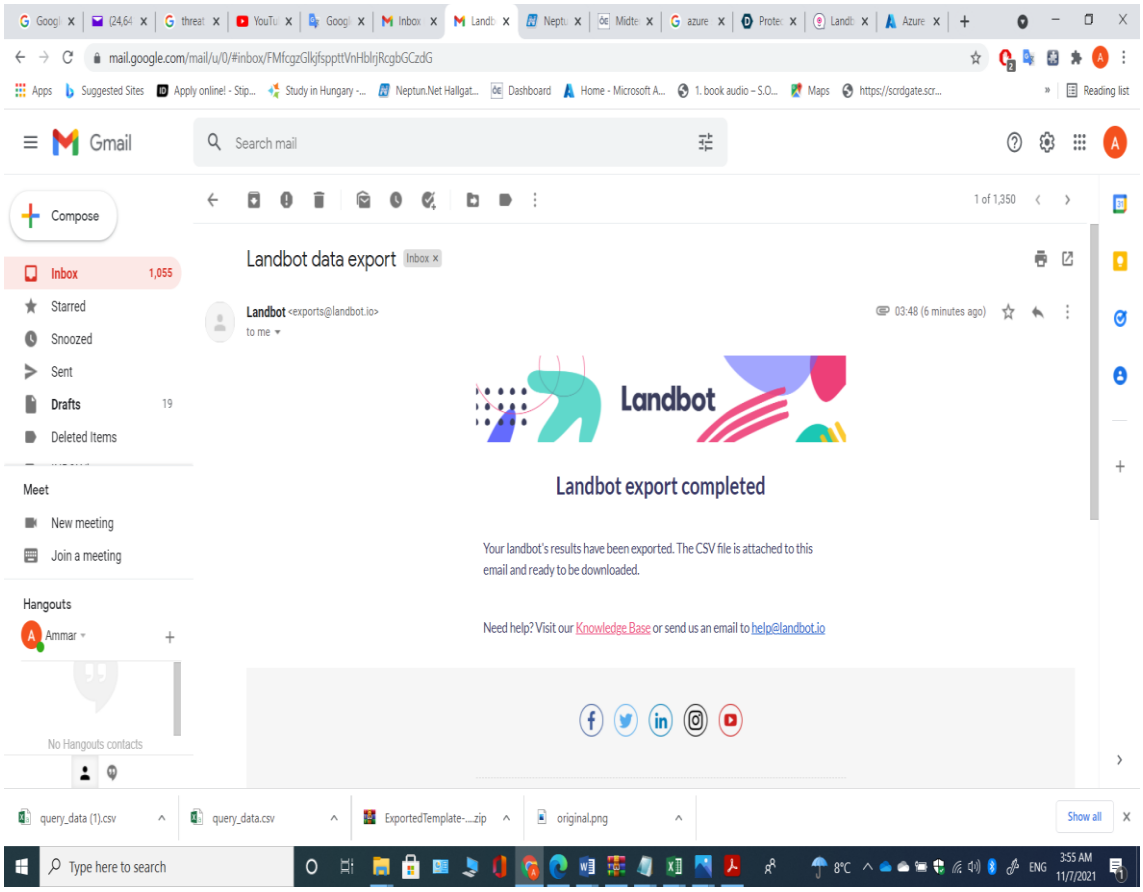
(a)



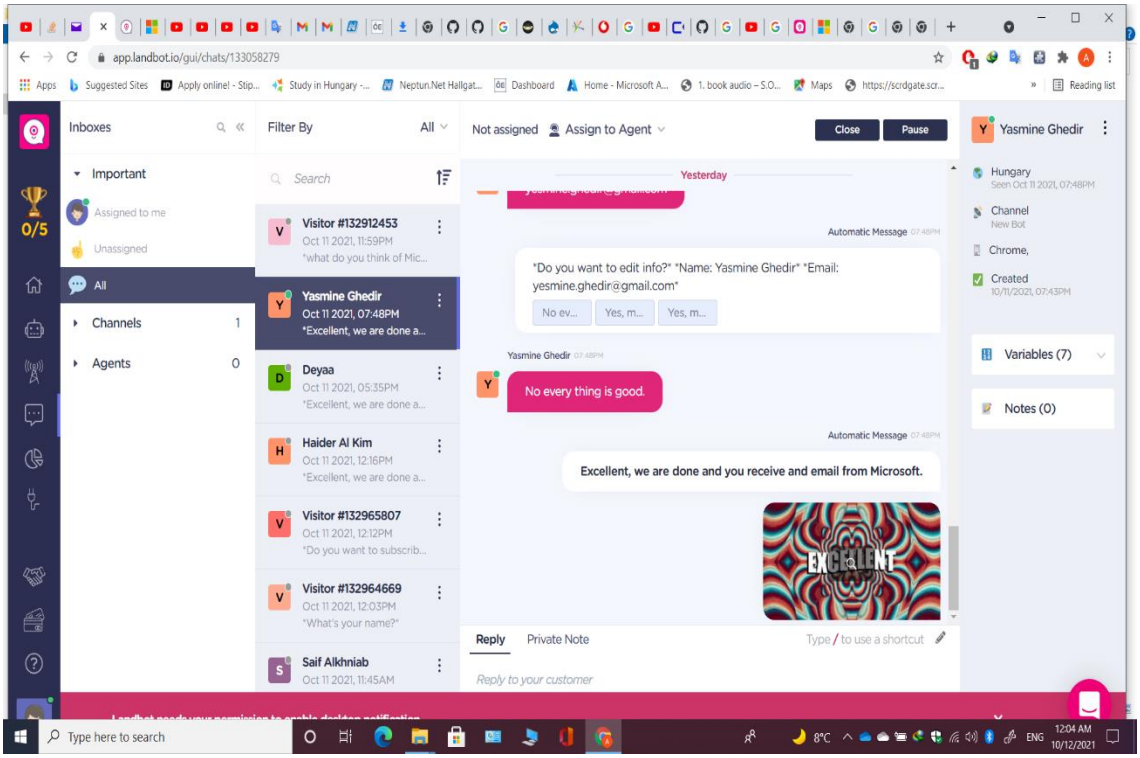
(b)


app.landbot.io/gui/overview/all/users
OVERVIEW
METRICS
USERS
Filter by
Last 30 days
Send report
Export Users' table
You will receive a CSV file with the Users' table to: alabbassiammar@gmail.com. Please, consider that it may take several minutes.
OK, EXPORT
query_data (1).csv
query_data.csv
ExportedTemplate-....zip
original.png
Show all
Type here to search

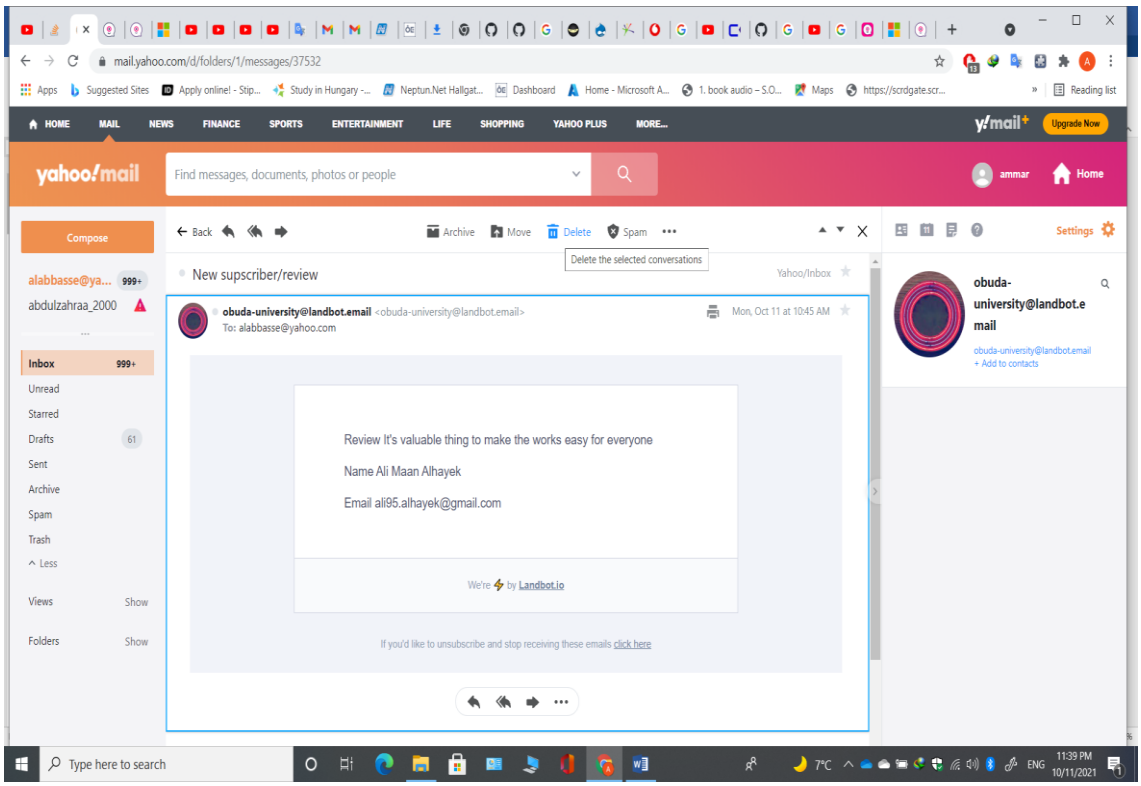
(c)


mail.google.com/mail/u/0/#inbox/FMfcgzGlkjfspttVnHblrjRcgbGCzdG
Gmail
Search mail
Compose
Inbox 1,055
Starred
Snoozed
Sent
Drafts 19
Deleted Items
Meet
New meeting
Join a meeting
Hangouts
Ammar
No Hangouts contacts
Landbot data export
Landbot <exports@landbot.io>
to me
03:48 (6 minutes ago)
Landbot
Landbot export completed
Your landbot's results have been exported. The CSV file is attached to this email and ready to be downloaded.
Need help? Visit our Knowledge Base or send us an email to help@landbot.io
query_data (1).csv
query_data.csv
ExportedTemplate-....zip
original.png
Show all
Type here to search

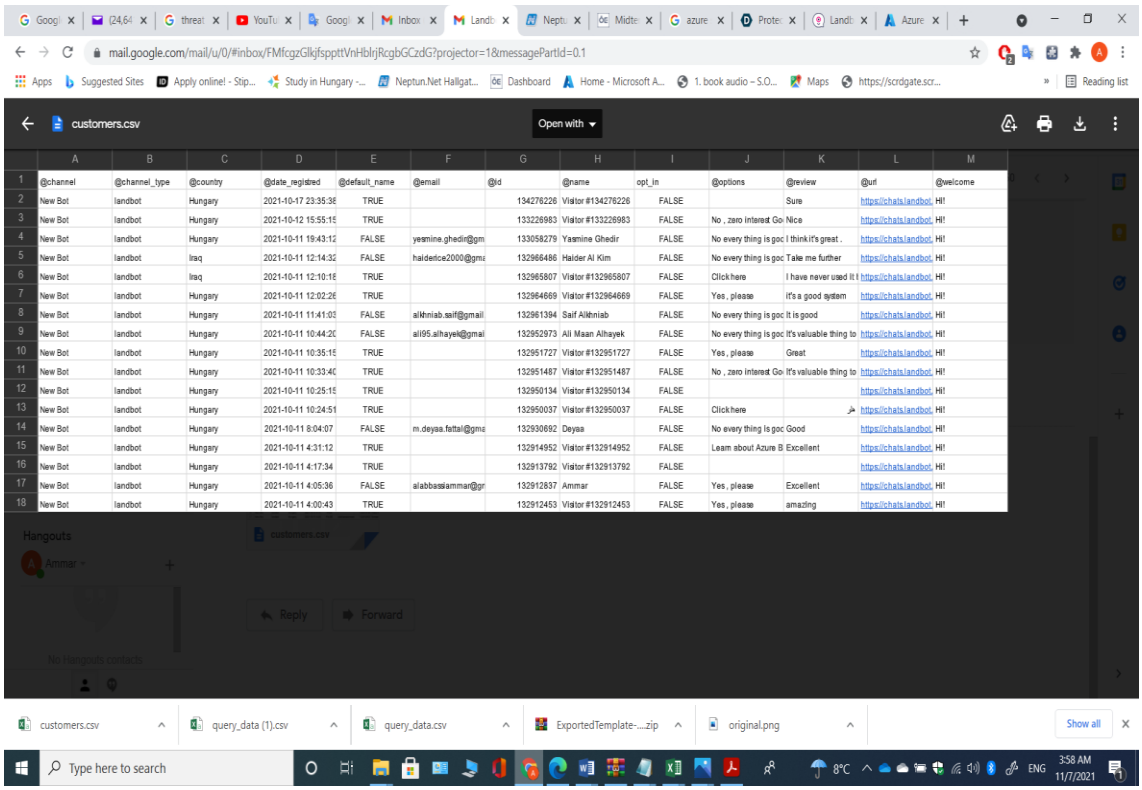
(d)


app.landbot.io/gui/chats/133058279
Inboxes
Filter By
All
Not assigned
Assign to Agent
Close
Pause
Yasmine Ghedir
Important
Assigned to me
Unassigned
All
Channels 1
Agents 0
Search
Visitor #132912453
Oct 11 2021, 11:59PM
"what do you think of Mic...
Yasmine Ghedir
Oct 11 2021, 07:48PM
"Excellent, we are done a...
Deyaa
Oct 11 2021, 05:35PM
"Excellent, we are done a...
Haider Al Kim
Oct 11 2021, 12:16PM
"Excellent, we are done a...
Visitor #132965807
Oct 11 2021, 12:12PM
"Do you want to subscrib...
Visitor #132964669
Oct 11 2021, 12:03PM
"What's your name?"
Saif Alkhniab
Oct 11 2021, 11:45AM
Yesterday
Automatic Message
"Do you want to edit info?" "Name: Yasmine Ghedir" "Email: yesmine.ghedir@gmail.com"
No ev...
Yes, m...
Yes, m...
Yasmine Ghedir
No every thing is good.
Automatic Message
Excellent, we are done and you receive and email from Microsoft.
EXCELLENT
Reply
Private Note
Type / to use a shortcut
Reply to your customer
Hungary
Seen Oct 11 2021, 07:48PM
Channel
New Bot
Chrome,
Created
10/11/2021, 07:43PM
Variables (7)
Notes (0)
Type here to search
8°C
ENG
12:04 AM
10/12/2021

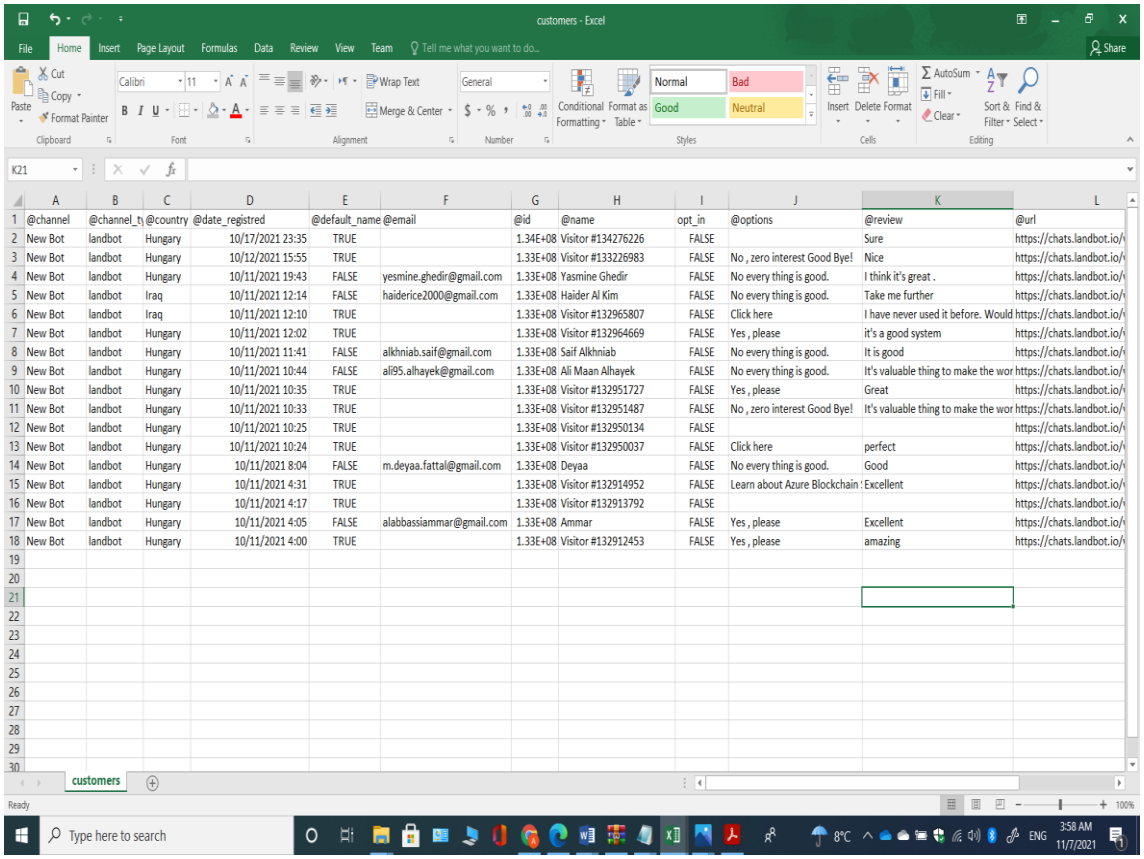
(e)


mail.yahoo.com/d/folders/1/messages/37532
HOME
MAIL
NEWS
FINANCE
SPORTS
ENTERTAINMENT
LIFE
SHOPPING
YAHOO PLUS
MORE...
Upgrade Now
yahoo!mail
Find messages, documents, photos or people
ammar
Home
Compose
Back
Archive
Move
Delete
Spam
Delete the selected conversations
Settings
alabbasse@ya... 999+
abdulzahraa_2000
New supscriber/review
Yahoo/Inbox
obuda-university@landbot.email <obuda-university@landbot.email>
To: alabbasse@yahoo.com
Mon, Oct 11 at 10:45 AM
Inbox 999+
Unread
Starred
Drafts 61
Sent
Archive
Spam
Trash
Less
Views Show
Folders Show
Review It's valuable thing to make the works easy for everyone
Name Ali Maan Alhayek
Email ali95.alhayek@gmail.com
We're by Landbot.io
If you'd like to unsubscribe and stop receiving these emails click here
obuda-university@landbot.email
+ Add to contacts
Type here to search
7°C
ENG
11:39 PM
10/11/2021

(f)


customers.csv
Open with
customers.csv
query_data (1).csv
query_data.csv
ExportedTemplate-....zip
original.png
Show all
Type here to search

(g)


customers - Excel
customers
Type here to search

(h)

6.3 Representational state transfer application programing interfaces

The important part is to determine the method of connecting Landbot to Sentinel. As known both of them are supported by a lot of REST (Representational State Transfer) APIs that I will use to create the connection between them.

An API, or application programming interface, is a collection of rules that describe how applications or devices can communicate with each other. APIs that satisfy the REST (representational state transfer) design principles are referred to as REST APIs or REST-compliant. As a result, REST APIs are often referred to as RESTful APIs [26]**. Figure (17)** illustrate how Link Azure sentinel workspace with syslog sources using API.

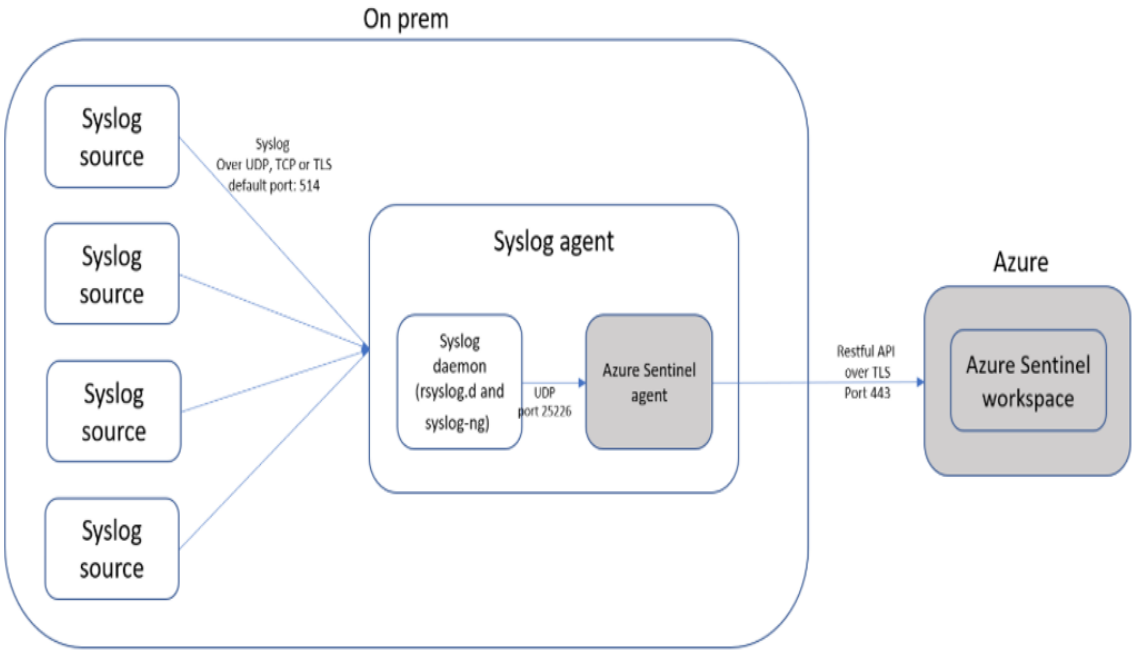


Fig.17. Link Azure sentinel workspace with syslog sources using API. [27]

6.4 How representational state transfer application programing interfaces work

As the name suggests, REST APIs interact via HTTP requests to conduct common database activities like creating, reading, updating, and deleting entries (CRUD). To retrieve data from a REST API, you use "GET" and "POST" requests; to add or remove data, you use "PUT" and "DELETE" requests. You can make API requests that utilize any of the HTTP methods. Similar to how a website functions in an internet browser with built-in HTTP capabilities, a properly designed REST API functions similarly.

When responding, information may be sent to a client in nearly any format, including JavaScript Object Notation (JSON), HTML, Python, or plaintext. In addition to being legible by people and machines, JSON is programming language neutral, making it a popular choice for data interchange. **Figure (18)** illustrate how Rest API work using HTTP and JSON methods.

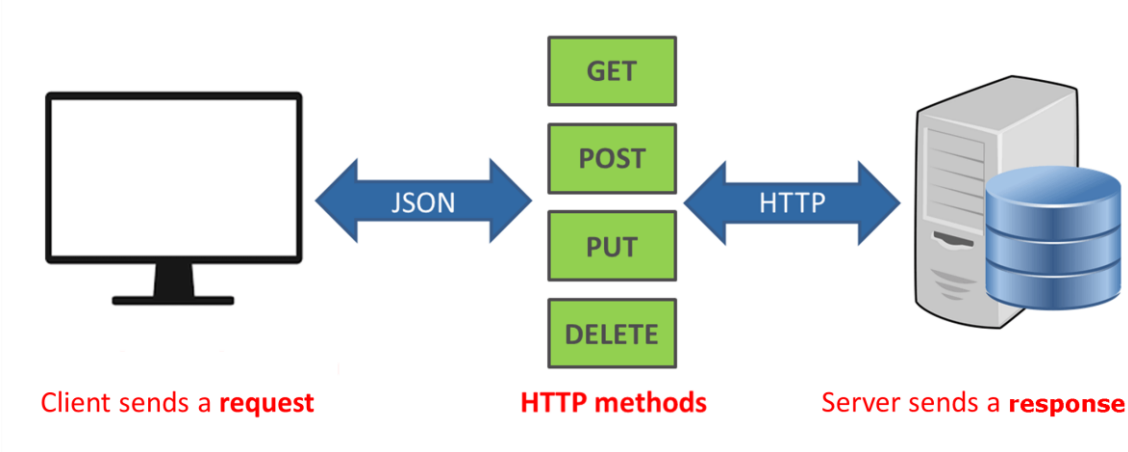


Fig. 18. Rest API work using HTTP and JSON methods [28]

I have collected and focus on **REST APIs** that listen to **HTTP requests** and respond in **JSON format** to perform standard database functions like **CRUD**

6.5 Azure sentinel representational state transfer APIs.

Azure Sentinel REST APIs allow you to create and manage data connectors, analytic rules, incidents, bookmarks and get entity information [29]. **Table (2)** illustrate Azure sentinel REST APIs.

No.	REST APIs	Description	URL	API Version
1-	**Create Or Update**	Creates or updates the data connector.	https://docs.microsoft.com/en-us/rest/api/securityinsights/dataconnectors#:~:text=OPERATIONS,Create%20Or%20Update,Delete,Delete%20the%20data	2020-01-01
2-	**Delete**	Delete the data connector.	https://management.azure.com/subscriptions/{subscriptionId}/resourceGroups/{resourceGroupName}/providers/Microsoft.OperationalInsights/workspaces/{workspaceName}/providers/Microsoft.SecurityInsights/dataConnectors/{dataConnectorId}?api-version=2020-01-01	2020-01-01
3-	**Get**	Gets a data connector.	https://management.azure.com/subscriptions/{subscriptionId}/resourceGroups/{resourceGroupName}/providers/Microsoft.OperationalInsights/workspaces/{workspaceName}/providers/Microsoft.SecurityInsights/dataConnectors/{dataConnectorId}?api-version=2020-01-01	2020-01-01
4-	**List**	Gets all data connectors.	https://management.azure.com/subscriptions/{subscriptionId}/resourceGroups/{resourceGroupName}/providers/Microsoft.OperationalInsights/workspaces/{workspaceName}/providers/Microsoft.SecurityInsights/dataConnectors?api-version=2020-01-01	2020-01-01

Table (2) Azure sentinel REST APIs

Example: Creates or updates a threat intelligence platform data connector. [29]

Sample Request (HTTP)

```
PUT https://management.azure.com/subscriptions/d0cfe6b2-9ac0-4464-
9919-
dccaee2e48c0/resourceGroups/myRg/providers/Microsoft.OperationalInsigh
ts/workspaces/myWorkspace/providers/Microsoft.SecurityInsights/dataCon
nectors/73e01a99-5cd7-4139-a149-9f2736ff2ab5?api-version=2020-01-01
```

Sample Response (JSON)

Status code:
200


```
{
  "id": "/subscriptions/d0cfe6b2-9ac0-4464-9919-
dccaee2e48c0/resourceGroups/myRg/providers/Microsoft.OperationalInsigh
ts/workspaces/myWorkspace/providers/Microsoft.SecurityInsights/dataCon
nectors/73e01a99-5cd7-4139-a149-9f2736ff2ab5",
  "name": "73e01a99-5cd7-4139-a149-9f2736ff2ab5",
  "type": "Microsoft.SecurityInsights/dataConnectors",
  "kind": "ThreatIntelligence",
  "etag": "\"0300bf09-0000-0000-0000-5c37296e0000\"",
  "properties": {
    "tenantId": "06b3ccb8-1384-4bcc-aec7-852f6d57161b",
    "tipLookbackPeriod": "2020-01-01T13:00:30.123Z",
    "dataTypes": {
      "indicators": {
        "state": "Enabled"
      }
    }
  }
}
```


Status code:
201


```
{
  "id": "/subscriptions/d0cfe6b2-9ac0-4464-9919-
dccaee2e48c0/resourceGroups/myRg/providers/Microsoft.OperationalInsigh
ts/workspaces/myWorkspace/providers/Microsoft.SecurityInsights/dataCon
nectors/73e01a99-5cd7-4139-a149-9f2736ff2ab5",
  "name": "73e01a99-5cd7-4139-a149-9f2736ff2ab5",
  "type": "Microsoft.SecurityInsights/dataConnectors",
  "kind": "ThreatIntelligence",
  "etag": "\"0300bf09-0000-0000-0000-5c37296e0000\"",
"properties": {
    "tenantId": "06b3ccb8-1384-4bcc-aec7-852f6d57161b",
    "tipLookbackPeriod": "2020-01-01T13:00:30.123Z",
    "dataTypes": {
      "indicators": {
        "state": "Enabled"
      }
    }
  }
}
```

6.6 Landbot representational state transfer APIs.

Landbot Web API utilizes resources like HTML pages and may be accessed via a simple HTTP protocol. Landbot API adheres to the REST typology (representational state transfer) since we do not keep any data internally between queries [30]. **Table (3)** illustrate Landbot REST APIs.

No.	REST APIs	Description	URL	API Version
1-	**Change**	Changes data of agent_id.	https://api.landbot.io/v1/agents/:agent_id/	Landbot V3 SDK
2-	**Create**	Create agent	https://api.landbot.io/v1/agents/	Landbot V3 SDK
3-	**Delete**	Removes agent_id	https://api.landbot.io/v1/agents/:agent_id/	Landbot V3 SDK
4-	**Get**	Returns agent data of agent_id	https://api.landbot.io/v1/agents/:agent_id/	Landbot V3 SDK
5-	**List**	Returns your agents data	https://api.landbot.io/v1/agents/	Landbot V3 SDK
6-	**Update**	Updates data of agent_id	https://api.landbot.io/v1/agents/:agent_id/	Landbot V3 SDK

Table (3) Landbot REST APIs

Example: Agents – create.

Sample request:

```
{
   "first_name": "Obuda",              * Required
   "last_name": "Landbot",               * Required
   "email": "ObudaLandbot @obudauni.com",          * Required
   "password": "202020212",            * Required
   "password_confirmation": 202020212"   * Required
}
```

Success response:

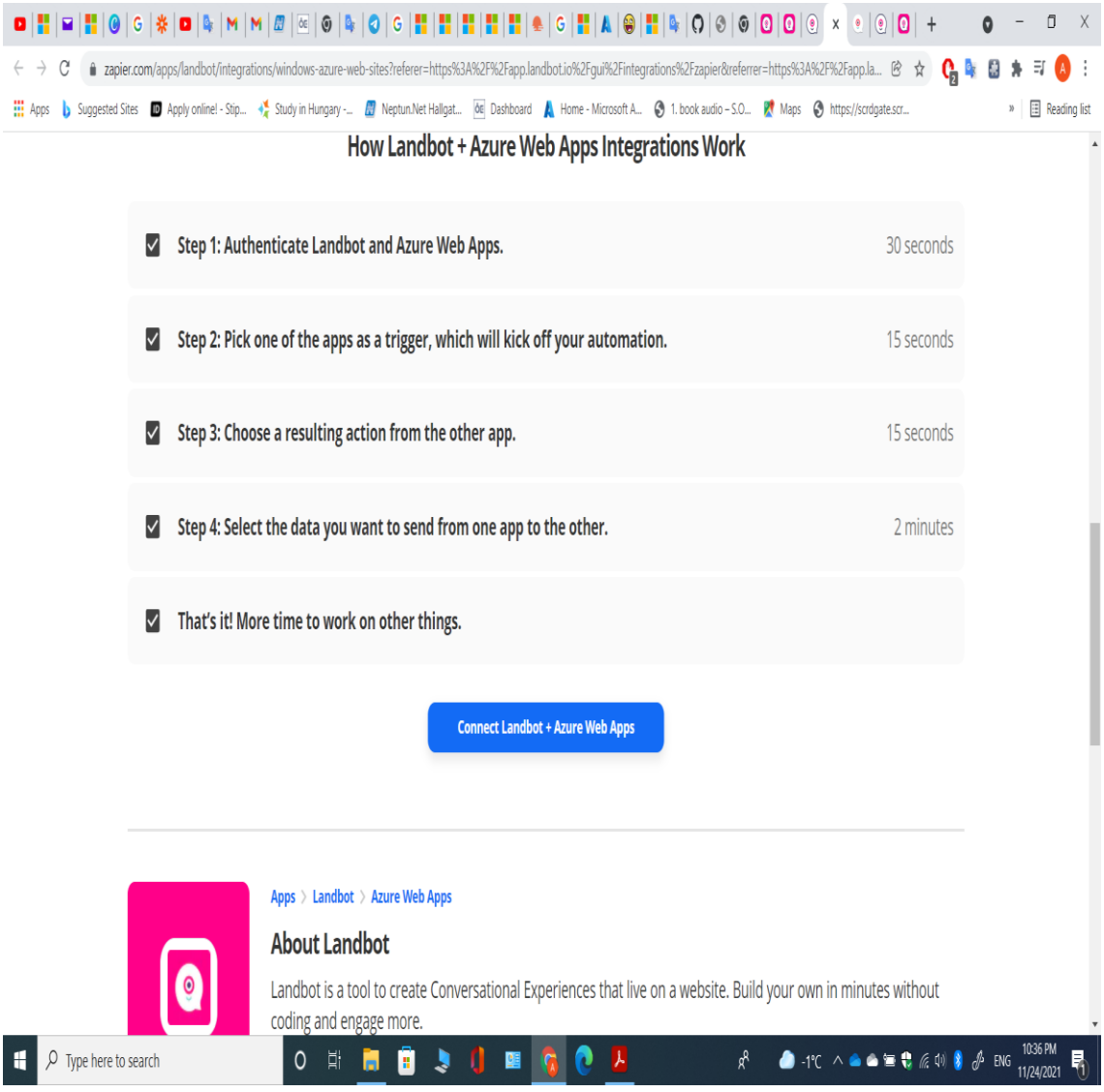
```
HTTP/1.1 201 OK
{
   "success": true,
   "paid": false,
   "agent":{
      "id": 10,
      "first_name": " Obuda ",
      "last_name": " Landbot ",
      "email": " ObudaLandbot @obudauni.com ",
      "status": "offline"
   }
}
```

Unprocessable entity:

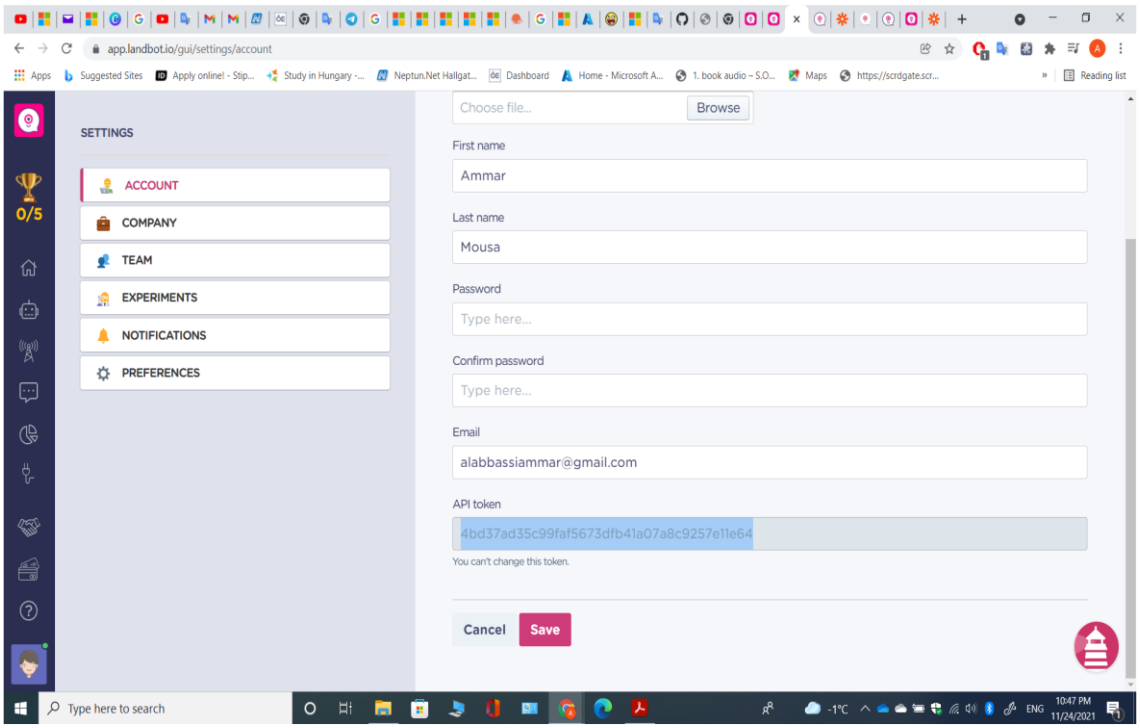
```
HTTP/1.1 422 Unprocessable entity
{
   'errors': {
      'first_name': ["This field is required"],
      'last_name': ["This field is required"],
      'email': ["This field is required"],
      'password': ["This field is required"],
      'password_confirmation': ["This field is required"]
   }
}
```

6. 7 Landbot and azure integration

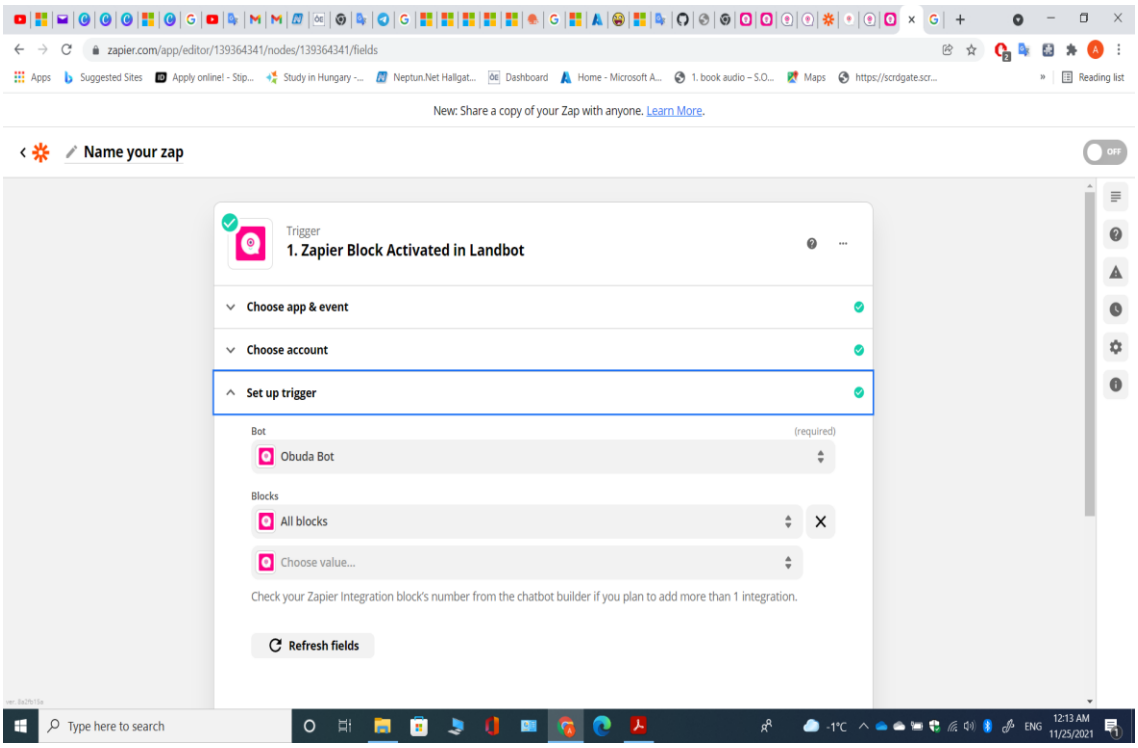
Without writing a line of code, we can use Zapier to automate the transfer of data between Azure and Landbot. The following screens(a-c) illustrate the steps for integration.



(a)


app.landbot.io/gui/settings/account
SETTINGS
ACCOUNT
COMPANY
TEAM
EXPERIMENTS
NOTIFICATIONS
PREFERENCES
Choose file...
Browse
First name
Ammar
Last name
Mousa
Password
Type here...
Confirm password
Type here...
Email
alabbassiammar@gmail.com
API token
4bd37ad35c99faf5673dfb41a07a8c9257e11e64
You can't change this token.
Cancel
Save
Type here to search

(b)


zapier.com/app/editor/139364341/nodes/139364341/fields
New: Share a copy of your Zap with anyone. Learn More.
Name your zap
Trigger
1. Zapier Block Activated in Landbot
Choose app & event
Choose account
Set up trigger
Bot
(required)
Obuda Bot
Blocks
All blocks
Choose value...
Check your Zapier Integration block's number from the chatbot builder if you plan to add more than 1 integration.
Refresh fields
Type here to search

(c)

Chapter 7: Testing system and results analysis

7.1 The Strategy of Testing System:

To test the proactive monitoring system that I made in the previous lectures against threats and vulnerabilities, I will be depending on the exploits databases to test my system. An exploit is any cyberattack that leverages a vulnerability in an application, network, operating system, or other hardware devices. In most cases, exploits come in the form of software or code that attempts to gain control of a computer or steal network information.

There is a difference between vulnerabilities and exploits. In fact, Vulnerabilities are weaknesses in a system or network's defenses that might be exploited by malicious individuals or hackers. So if a vulnerability is an open window into the system, an exploit is the rope or ladder the thief uses to reach the open window [31].

7.2 Main types of exploits:

There are two types of exploits: known and unknown:

a- **Known exploits:** Researchers in the field of cybersecurity have already made the discovery. Developers may provide fixes to close any holes found in the exploit, regardless of where the vulnerability originated: in software, OS, or even hardware. Users are given these updates as security measures. Keeping your devices up to date is essential for this.

b- **Unknown exploits or zero-day-exploits**: As soon as they identify a vulnerability, cybercriminals construct an exploit and utilize it to target their victims the same day. It is up to software developers and cybersecurity experts to find out how a zero-day exploit assault works and what can be done to fix it.

According to IT Security Database Site. A sample of Microsoft products' vulnerability data Shown in Figure (19). Statistical data about security vulnerabilities in this vendor's software products are readily available on:
https://www.itsecdb.com/vendor/26/Microsoft.html

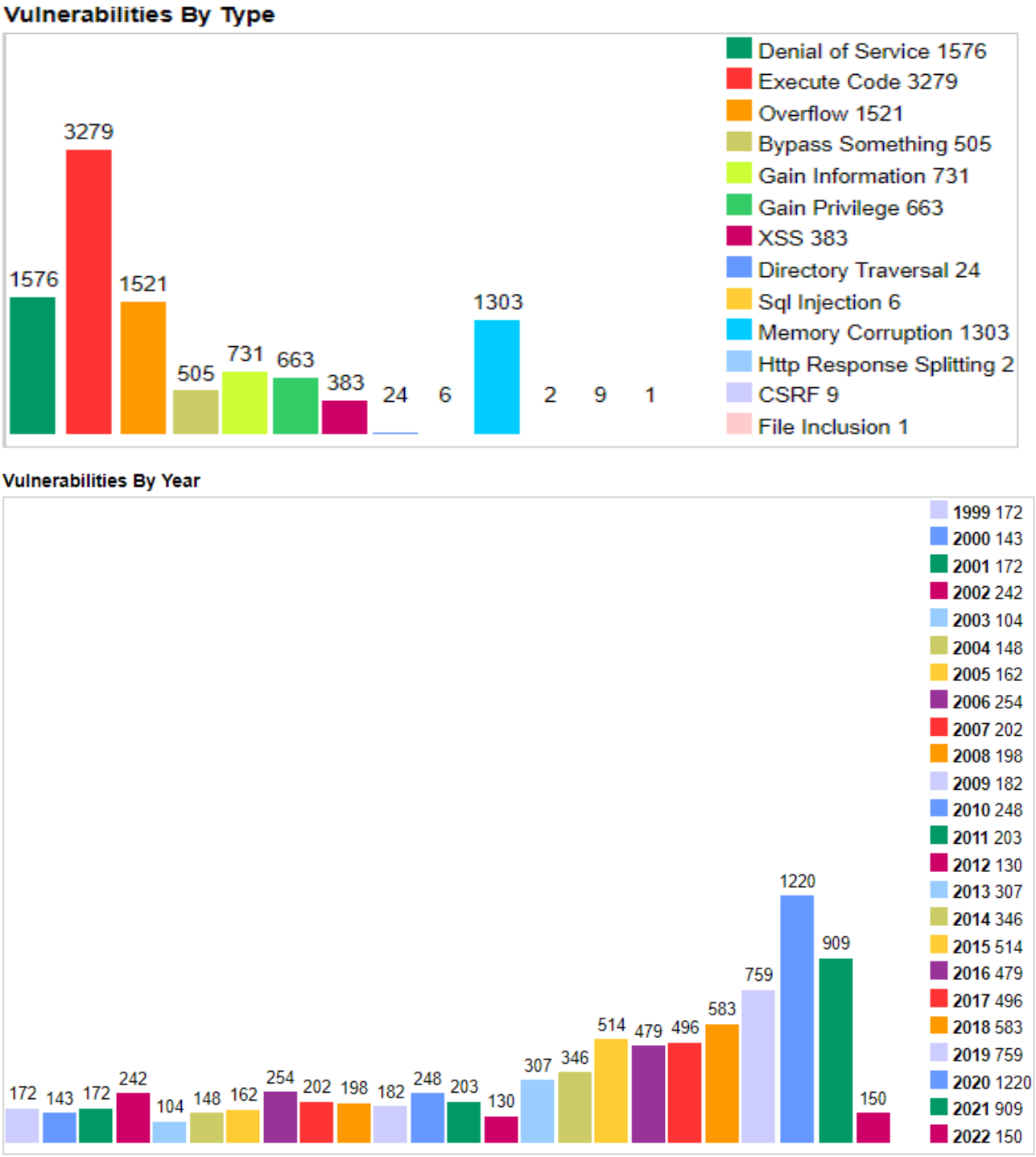


Fig. 19. Microsoft products Vulnerabilities by Type and Year

7.3 Exploit databases:

There are many excellent exploit databases that I will utilize to test my proactive system, the following description illustrate a comparison about three of them.

Exploit pack	Exploit Database	Rapid7
1- Summary		
Exploitpack is considered a multiplatform exploitation framework that contains more than 39,000 exploits, implants , and agents that are undetected and ready to assist you in gaining root access on your next target. [32]	Exploit Database was established as a resource for penetration testers and vulnerability researchers. It is considered a (CVE) Common Vulnerabilities and Exposures compliant repository of the publicly available exploits and their relevant susceptible software.[33]	Rapid7 was founded as a dependable solution, seamless controls under the slogan "**You Protect Our Future. We've Got Your Back**." and the strategic direction remain one step ahead of threats on your network. To help you quit putting out fires and concentrate on the real dangers. [34]
2- Who Founded It		
The Experienced software engineers and exploit writers created Exploit Pack as a small side project in **2007** to make security experts' work easier and free them up to do the vital things. As they though there is no tomorrow.	It was first founded by str0ke in **2004** An information and security training company called by Offensive Security maintains the Exploit Database as free service.	It was founded in **2000**, Rapid7 is the brainchild of Alan Matthews, Tas Giakouminakis, and Chad Loder, three software experts. Rapid7 was developed in response to client complaints that security was consider a difficult problem for their companies.

Exploit pack	Exploit Database	Rapid7
		
3- Location		
Amsterdam, Netherlands	New York City , United States	Boston, Massachusetts, US
4- Mission		
The goal of Exploit Pack is to process and exploit security vulnerabilities in a controlled environment, achieve access, and report issues so that you can protect against hostile systems. It's the optimal choice for both Red Teams and pentesters.	The main goal of Exploit Database to compile the most complete collection of exploits from direct contributions, mailing lists, and other public sources and provide them in a freely-available and searchable database	Security and data analytics are at the heart of Rapid7's mission to secure the information of commercial clients in a wide variety sectors via the provision of effective and dependable solutions.
5- Open Source or Restricted		
There are no restrictions on how you may use Exploit Pack, which is an open source GPLv3 security tool.	It is an independent and open source repository of software exploits and vulnerabilities.	Rapid7's Velociraptor is an open-source digital forensics and incident response (DFIR) tool.
6- Zero Day Exploit*		
Exploit pack Premium Pack get access to all zero-days exploits	Exploit Database support zero-days exploits	Rapid7 support zero-days exploits
7- Customer Services Support		
Yes, on their official website. https://exploitpack.com	Yes, it is supported by the main website of Offensive Security company. www.offensivesecurity.com	Yes, on their official website. https://www.rapid7.com

Table (4) Comparison Between Main Exploit Databases

7.4 Exploit code for testing monitoring system

My proactive monitoring system as shown in Figure(20),has multiple input levels and multiple inputs per level. At the level of basic search, the union of the exploit databases provides known vulnerabilities of system components.

Let {d1, d2, d3} be a set of vulnerability databases where "d1" is Exploit Pack, "d2" is Exploit Database, and "d3" is Rapid7. An exploit ("e") is an element of an exploit database ("d"). An exploit ("e") is a function, which is a code that uses one ("v") or more vulnerabilities ("v1", "v2", ...). My monitor search for exploits through the APIs of the union of {d1, d2, d3}, then reverse engineer the relevant exploit function to get the relevant vulnerabilities. Afterwards, it can apply the vulnerabilities to the APIs to read and - might - even install the fixes. A patch ("p") is a piece of code that fixes a vulnerability.The following pseudo-code sums up the essence of the basic monitor:

```
Relevant_Exploits_Set=Search_Exploits(union{d1,d2,d3})
for each e in Relevant_Exploits_Set
Relevant_Vulnerabilities_Set.Add(Reverse_Engineer(e))
end
Relevant_Fix_Set=Search_Patch(union{d1,d2,d3}, Relevant_Vulnerabilities_Set)
for each p in Relevant_Fix_Set
Install_Patch(p)
end
```

Code 1. : Basic monitor function

Since these are cloud databases, the monitor can access larger vulnerability samples than its local storage. Another advantage of using exploit databases is getting frequent updates because every new exploit potentially adds information about a vulnerability. Machine learning can derive further vulnerabilities from the exploits. The following flowchart Figure(21) illustrates the testing of the basic monitor function based on exploit databases.

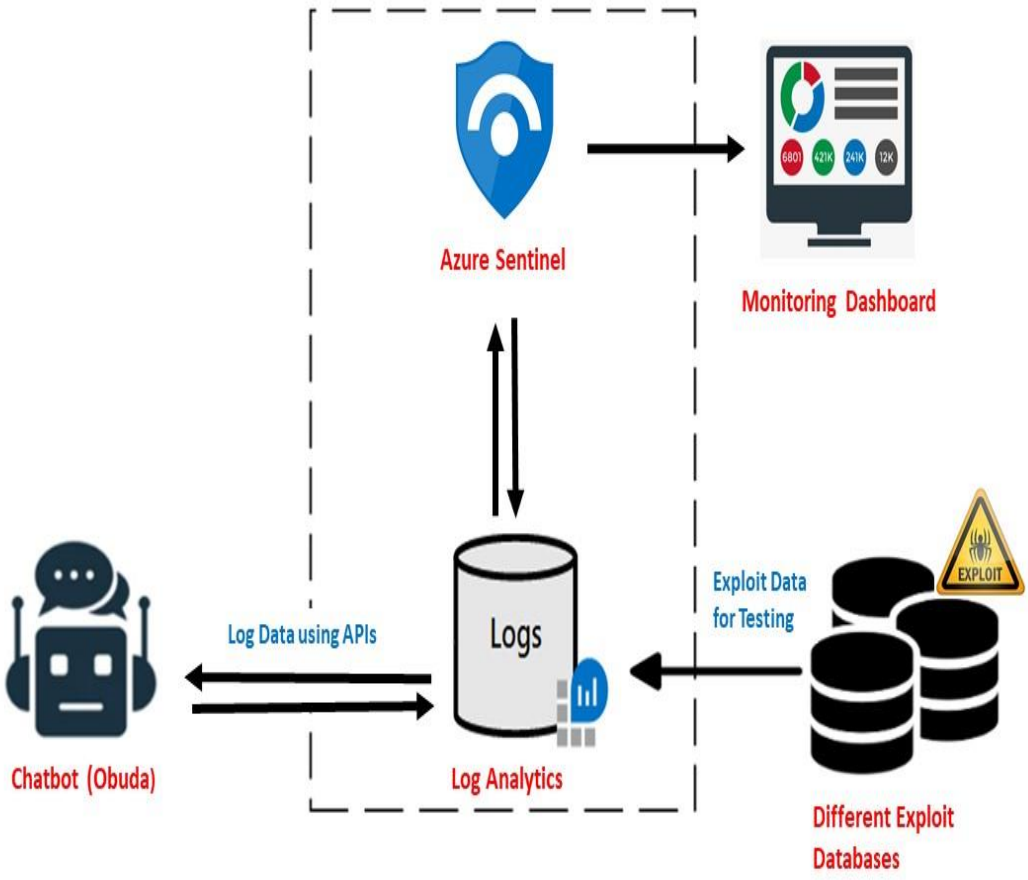


Fig. 20. Prototype of the proactive monitoring system

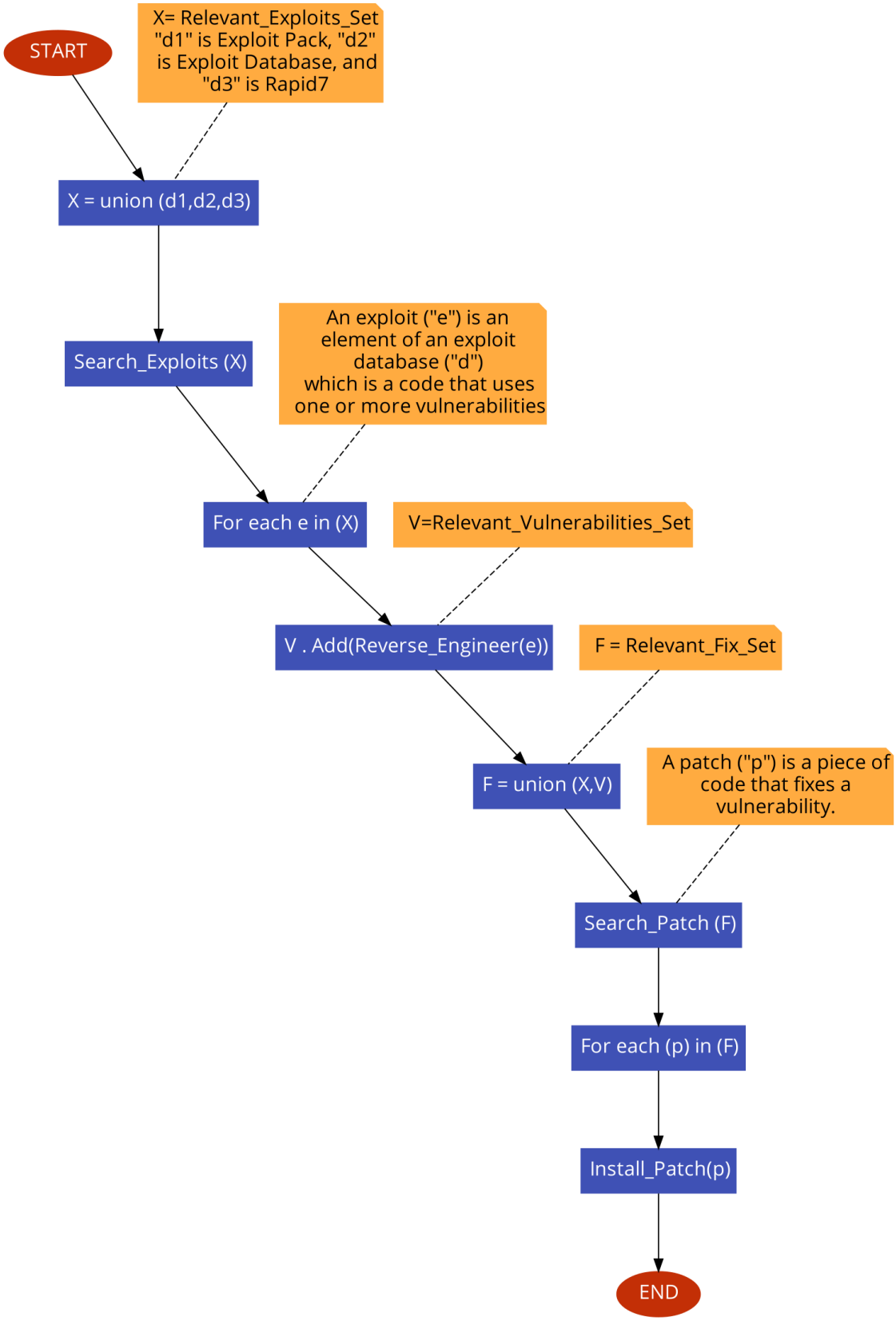


Fig. 21. Flowchart of Basic monitor function

7.5 Result analysis

My proactive monitor collected 219 relevant exploits (mathematical median) during its test runs as shown in Figure (22). 99 test runs have been performed using APIs. The average time to fix the vulnerabilities in these exploits was 500 seconds for high, about the same for medium, and 650 seconds for low severity vulnerabilities. The average time involved the collection and reverse engineering of exploits, the download, and installation of the fixes, and the rescanning of the system components.

In comparison, the manual collection of the same vulnerabilities took 8 working hours. The manual installation of the patches cost another 8 working hours. So, the AI-supported version was better in order of magnitude. Furthermore, during the manual process, several human errors were detected (forgotten documentation, downloading the wrong version of the patch...)

Fig. 22. Dashboard of proactive monitor

Conclusions

The methodology of the thesis provides an in-depth explanation of how to build an intelligent proactive threat monitoring system for cloud android chatbots. It will become increasingly common for organizations to include chatbots in their operational processes in order to maintain a constant level of customer service. However, it seems that emerging threats against these chatbots require such proactive monitoring systems. Manual threat management is not efficient (see time differences), nor effective (see human errors) anymore. Automated solutions deserve further attention. The prototype developed in this Thesis can be integrated into such a solution. The architecture of the monitoring system in the cloud and steps for making chatbot were explained. There are several advantages to adopting a hybrid cloud approach. Especially if you go with Microsoft Azure and its powerful tool (Azure Sentinel) that can access and analyze data from a variety of sources, a survey chatbot (Obuda bot) was made as digital assistance for collecting log files and sending it to Azure sentinel monitoring system using APIs for integration, as bots can gather information more quickly and provide a more rapid resolution. Finally, these collected data were tested using Exploit databases (Exploit Pack, Exploit Database and Rapid7) to check the existence of vulnerabilities and fix it.

Recommendations

As a solution to protect against threats and vulnerabilities, chatbots can be linked with a blockchain platform in order to provide a variety of security measures and other important functions. Although it is still a relatively young technology, blockchain is fast finding applications beyond cryptocurrencies. Decentralization and data transparency are the two of blockchain's many advantages, and they offer up a whole new world of security options. In order to maintain the integrity of the system, enterprises all around the globe are under growing pressure to strengthen their cybersecurity. Azure provided SQL Database Ledger as shown in Figure (23) below, an attacker or a high-privileged user cannot access data that is protected by Ledger. Included in this group are database admins, systems admins, and cloud admins

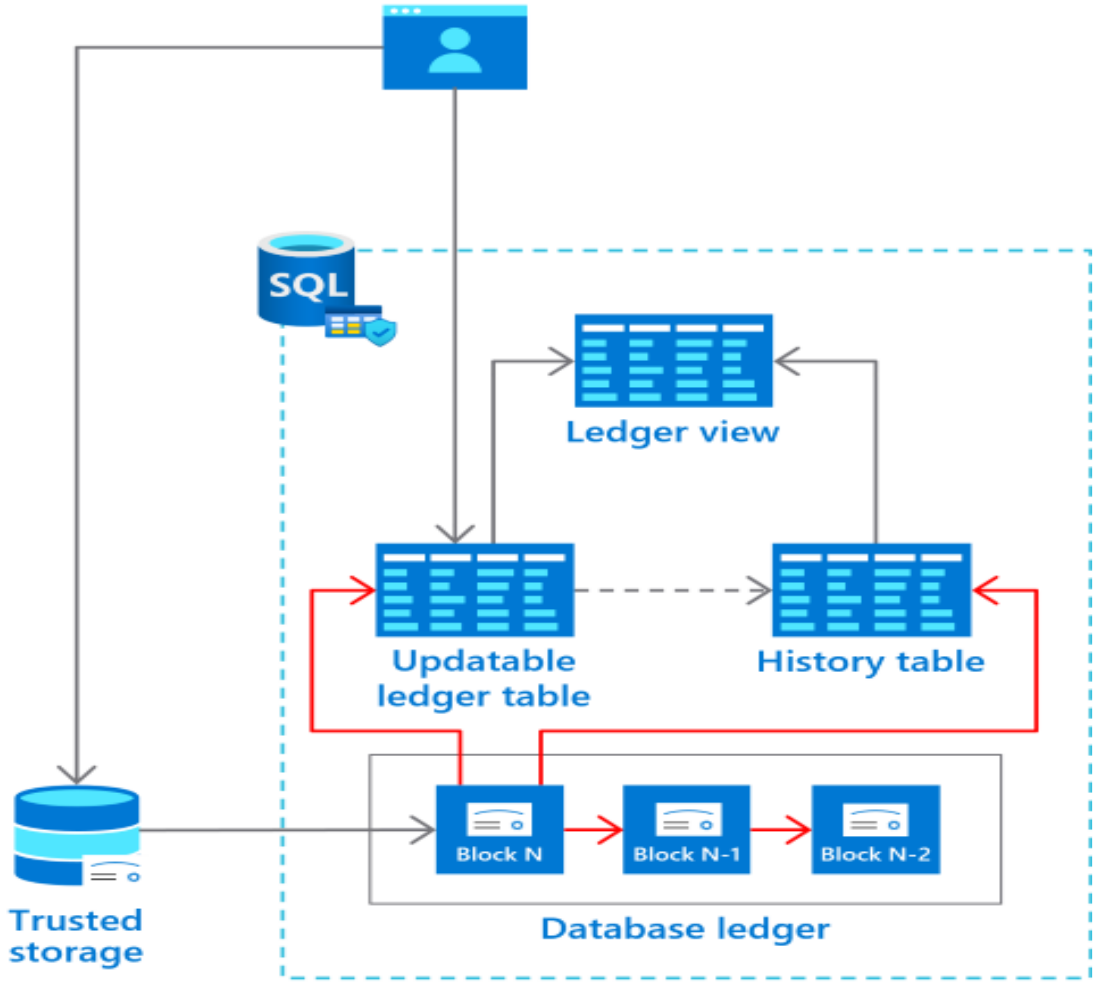


Fig. 23. Azure SQL Database ledger [35]

Upgrade options

There are several upgrade options could be adopting to improve my proactive monitoring system. A chatbot can further enchant the dashboard facilities of traditional exploit databases. Also APIs can enable the building of custom monitors from arbitrary exploit databases as building blocks. Another important options are utilizing modern machine intelligence algorithms that recently have great efforts in solving cybersecurity issues. In many cases, the amount of collected data to be check malicious or not could be massive, therefore, machine intelligence will be treating with these growing problem.

By using supervised ML (Machine Language) for detecting possible future threats by checking malicious data files base on several parameters (structure of data, contents, behavior, etc.) these data are subjects to rules. In other side many data are not subject to rules and pattern recognizing (loose rules) therefore, unsupervised ML will be used for detecting anomalies. Advanced threat detection using unsupervised machine learning can be efficient when paired with data on user accounts, assets, and cyber environment. Therefore, the using of unsupervised ML will my monitoring system proactive and predictive. Figure (24) will illustrate the both types of ML.

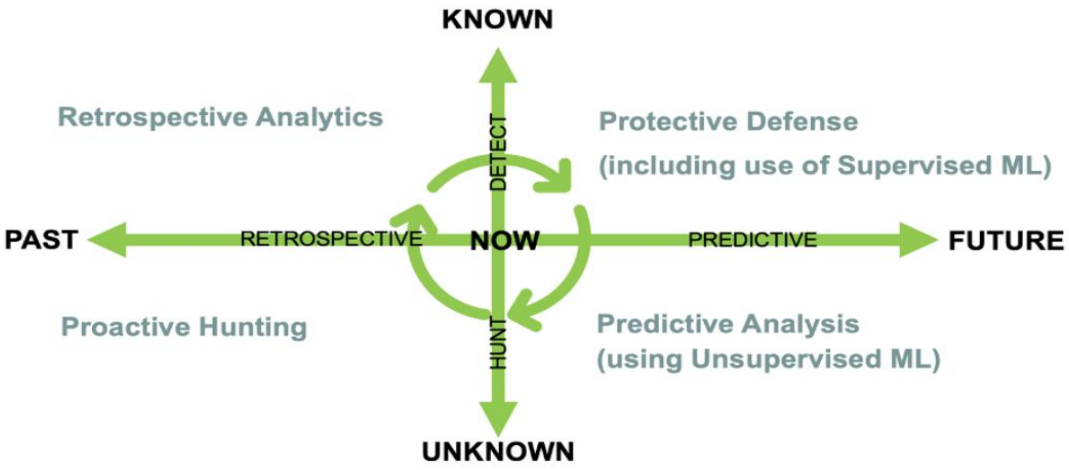


Fig. 24. Supervised and Unsupervised ML functions in time and knowledge axes [36]

The other important option of enhancement is to using NDR (Network Detection and Response) solutions [37]. NDR uses machine learning and data analytics to identify cyber novel threats on networks. Due to the ease of cyberattacking over networks, cyber attackers are always developing new approaches to bypass networking security systems. Thus, enhanced network security solutions like NDR were required to assist avoid and identify these emerging attacks. For private and public clouds as well as on-premises networks, NDR solution delivers deep network visibility, threat intelligence, and threat hunting capabilities to detect attacks that have passed other security solutions. With NDR, companies can safeguard their data, assets, and workloads against cyber-attacks.

List of Abbreviations

Abbreviation	Definition
1G	1 Generation
2G	2 Generation
3G	3 Generation
4G	4 Generation
5G	5 Generation
AI	Artificial Intelligence
AMQP	Advanced Message Queuing Protocol
API	Application Programing Interface
CDN	Content Delivery Network
CPU	Central Processing Unit
CRUD	Creating, Reading, Updating, and Deleting entries
CSA	Cloud Security Alliance
DdoS	Distributed denial-of-service
DoS	Denial-of-Service
HTTPS	Hypertext Transfer Protocol Secure
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IMS	Internet Motion Sensor
IoRT	Internet of Robot Things
IoT	Internet of Things
IPV4	Internet Protocol Version 4
IT	Information Technology
ITU	International Telecommunication Union
JSON	JavaScript Object Notation
KQL	Kusto Query Language
LAN	Local Area Network
MQTT	Message Queue Telemetry Transport
OS	Operating Systems
OSI	Open Systems Interconnection
PCs	Personal Computers
REST	Representational State Transfer
RFID	Radio-Frequency Identification
ROS	Robot Operating System
SIEM	Security Information and Event Management
SOAR	Security Orchestration Automated Response

Abbreviation	Definition
SQL	Structured Query Language
TCP/IP	Total Control Protocol/Internet Protocol
VM's	Virtual Machines
VNet	Azure Virtual Network
VPN	Virtual Private Network
W-CDMA	Wideband Code Division Multiple Access
Websockets	Web socket
XSS	Cross Site Scripting
YARP	Yet Another Robot Platform
CVE	Common Vulnerabilities and Exposures
ML	Machine Language
NDR	Network Detection and Response

References:

[1] https://kth.diva-portal.org/smash/get/diva2:1479320/FULLTEXT01.pdf. 3/8/2021

[2] Krzysztof Lasota, Piotr Bazydlo, Adam Kozakiewicz. "Mobile platform for threat monitoring in Wireless Sensor Networks", IEEE 3rd World Forum on Internet of Things (WF-IoT), 2016

[3] Gen, H.P.-C.S.A. Controllers, R.: *Hewlett-Packard Enterprise Development LP. Citeseer (2015)*

[4] Aldowah, H. ,Rehman, S., Umar, I. (2019). Security in Internet of Things: Issues, Challenges, and Solutions. 10.1007/978-3-319-99007-1_38.

[5] van Kranenburg and Bassi Communications in Mobile Computing 2012, 1:9 *http://www.comcjournal.com/content/1/1/9*

[6] Joao Paulo de A. Barbosa, Fabio do P. de C. Lima, Leonardo dos S. Coutinho, Joao Paulo R.Rodrigues Leite et al. "ROS, Android and cloud robotics: How to make a powerful low cost robot", 2015 *International Conference on Advanced Robotics (ICAR), 2015*.

[7] Ahmed, H.S., Ali, M.H., Kadhum, L.M., Zolkipli, M.F., and Alsariera, Y.A. (2017). A Review of Challenges and Security Risks of Cloud Computing. *Journal of Telecommunication, Electronic and Computer Engineering, 9*, 87-91.

[8] https://www.cognierblock.com/Blockchain.html. 2/11/2021

[9] https://www.imperva.com/learn/application-security/siem/ 5/11/2021.

[10] Bailey, M., Cooke, E., Jahanian, F., Nazario, J., & Watson, D. (2005, February). The internet motion sensor-a distributed blackhole monitoring system. In *NDSS*.

[11] Yu, W., Xu, G., Chen, Z., & Moulema, P. (2013, October). A cloud computing based architecture for cyber security situation awareness. In *2013 iEEE conference on communications and network security (cNS)* (pp. 488-492). IEEE.

[12] Chen, Z., Zhang, H., Hatcher, W. G., Nguyen, J., & Yu, W. (2016, June). A streaming-based network monitoring and threat detection system. In *2016 IEEE 14th International Conference on Software Engineering Research, Management and Applications (SERA)* (pp. 31-37). IEEE.

[13] Luigi Coppolino, Salvatore D'Antonio, Giovanni Mazzeo, Luigi Romano, Cloud security: Emerging threats and current solutions, *Computers & Electrical Engineering, Volume* 59, 2017, Pages 126-140, ISSN 0045-7906

[14] Giampaolo Fiorentino; Carmelita Occhipinti; Antonello Corsi; Evandro Moro; John Davies; Alistair Duke, "Blockchain: Enabling Trust on the Internet of Things," in *The Internet of Things: From Data to Insight* , Wiley, 2020, pp.141-157, doi: 10.1002/9781119545293.ch11.

[15] Dutta, S., Joyce, G., & Brewer, J. (2017, July). Utilizing chatbots to increase the efficacy of information security practitioners. In *International Conference on Applied Human Factors and Ergonomics* (pp. 237-243). Springer, Cham.

[16] Tyson Brooks, Jerry Robinson, Lee McKnight. "Conceptualizing a Secure Wireless Cloud",International Journal of Cloud Computing and Services Science (IJ-CLOSER), 2012.

[17] Lal, N., Tiwari, S. M., Khare, D., & Saxena, M. (2021). Prospects for Handling 5G Network Security: Challenges, Recommendations and Future Directions. In *Journal of Physics: Conference Series* (Vol. 1714, No. 1, p. 012052). IOP Publishing.

[18] Gupt, Krishn & Singh, Vinay. (2016). Evolution of Modern Communication Systems. 5. 10.17148/IJARCCE.2016.5606.

[19] McWhorter, Rochell , Delello, Julie. (2016). Green Technologies Enabling Virtual Learning Environments. International Journal of Information Communication Technologies and Human Development. 8. 38-55. 10.4018/IJICTHD.2016100104.

[20] Hajjaj, Sami and Sahari, Ksm. (2017). Establishing remote networks for ROS applications via Port Forwarding: A detailed tutorial. International Journal of Advanced Robotic Systems. 14. 172988141770335. 10.1177/1729881417703355.

[21] https://docs.microsoft.com/bs-cyrl-ba/azure/iot-hub/about-iot-hub.21/11/2021

[22] https://docs.microsoft.com/hu-hu/azure/iot-hub/virtual-network-support.24/11/2021

[23] https://docs.microsoft.com/en-us/azure/sentinel/overview.27/11/2021

[24] https://www.microsoftpressstore.com/articles/article.aspx?p=2999392.3/12/2021

[25] https://onlinelibrary.wiley.com/doi/10.1002/cpe.6426. 24/1/2022

[26] https://www.ibm.com/cloud/learn/rest-apis. 26/1/2022

[27] https://docs.microsoft.com/en-us/azure/sentinel/connect-common-event-format.27/1/2022

[28] https://phpenthusiast.com/blog/what-is-rest-api. 29/1/2022

[29] https://docs.microsoft.com/en-us/rest/api/securityinsights/incidents. 29/1/2022

[30] https://dev.landbot.io/docs/?content=apis.4/2/2022

[31] https://www.avast.com/c-exploits#topic- 20/2/2022

[32] https://exploitpack.com. 20/2/2022

[33] www.offensivesecurity.com 20/2/2022

[34] https://www.rapid7.com 20/2/2022

[35] https://docs.microsoft.com/en-us/azure/azure-sql/database/ledger-overview 10/03/2022

[36] https://fidelissecurity.com/threatgeek/network-security/using-machine-learning-for-threat-detection/ 27/2/2022.

[37] https://www.checkpoint.com/cyber-hub/cloud-security/what-is-network-detection-and-response-ndr/27/2/2022