Career Point International Journal of Research (CPIJR)
©2022 CPIJR | Volume 3 | Issue 1 | ISSN : 2583-1895

CYBER SECURITY IN IOT-BASED CLOUD COMPUTING

Arshad Hussain

Assistant Professor, School of Computer Applications, Career Point University, Kota, Rajasthan, India,

Abstract: With the flexible architecture that cloud computing offers, data and resources may be distributed across many different places and accessed from a variety of industrial settings. Utilizing, storing, and sharing resources including data, services, and applications for industrial applications have all altered as a result of cloud computing. In the past ten years, companies have quickly shifted to cloud computing in order to benefit from greater performance, lower costs, and more extensive access. Additionally, the internet of things (IoT) has significantly improved when cloud computing was incorporated. However, this quick shift to the cloud brought up a number of security concerns and challenges. Traditional security measures don't immediately apply to cloud-based systems and are occasionally inadequate. Despite the recurring problems with cloud platforms, security issues have been resolved during the past three years. The rapid advancement of deep learning (DL) in artificial intelligence (AI) has resulted in a number of benefits that can be applied to cloud-based industrial security issues. Some of the research's findings are as follows: The cloud-based IoT architecture, services, configurations, and security models that support it are thoroughly examined by us; the in-depth discussion of the four main categories of cloud security concerns in IoT: data, network and service, applications, and people-related security issues; The most recent developments in cloud-based IoT attacks are identified and investigated. We identify, discuss, and evaluate significant security issues and preventative measures in each category; Lastly, we provide a comprehensive analysis of cloud security concerns.

Keywords: cloud computing; IoT security; cybersecurity; cloud configuration; deep learning; machine learning; attacks; attack prevention; platform as a service (PaaS); infrastructure as a service (IaaS); software as a service (SaaS); development as a service (DaaS); forensic as a service (FaaS)

I Introduction

An extensive network that includes a number of IoT-supported applications and devices is known as an IoT-based cloud infrastructure. Real-time processing, operations, underlying infrastructure, and servers and storage make up the infrastructure. Standards and services necessary for securing, managing, and connecting various IoT applications and devices are included in an IoT-based cloud infrastructure. The typical IoT architecture is shown in Figure 1, and the overview of the IoT-based cloud attack model is shown in Figure 2.The cloud has emerged in the past ten years, and its variants are still expanding in the current decade [1,2,3].We see IoT starting to lead the pack among these variations, the web of things

(IoT).In contrast, it is followed by others in recent trends, such as service architectures, distributed cloud environments, data center operations, and management areas [4].The cloud service market is predicted to grow by 25% in 2022, according to a recent Gartner article [5]. Cloud computing is one of the top ten strategic technology trends for 2022.

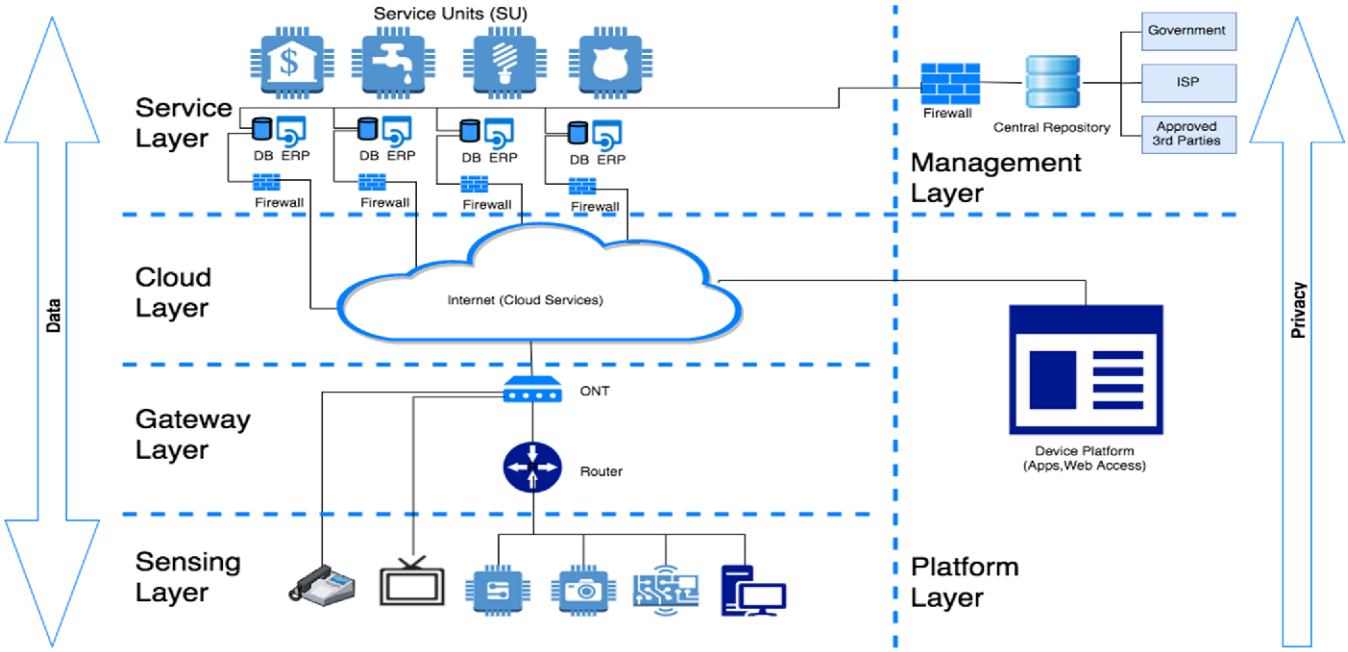

Figure 1. Typical IoT Architecture.

II Literature Review

The National Institute of Standards and Technology (NIST) has identified five essential characteristics of cloud computing [2]. Measured service, resource pooling, rapid expansion, network access, and on-demand self-service are the five of them. To jointly deliver cloud services, four deployment models and three service models are also listed. The primary objective of cloud computing is to offer online computing services like servers, storage, databases, networking, software, analytics, and intelligence. The services that users receive can be tailored to meet their specific requirements. Due to the cloud's quick data storage and access, cost-effectiveness, and flexibility in the workplace, traditional IT services have moved to the cloud. To set up physical on-site data centers, businesses don't have to buy expensive hardware and software with cloud computing. By storing software systems and services on remote servers, cloud technologies automate industries. The majority of industries now follow this trend, which is expanding annually [3].

Numerous industrial applications can take advantage of cloud computing's scalability and regular software and hardware updates [3].In addition, a variety of security solutions and the ability to make effective use of network resources are provided by the cloud. It's clear that cloud computing has a lot of potential thanks to these benefits. In the future, cloud computing and its underlying technologies have the potential to open a wide range of applications, solutions, services, platforms, and more to a wide range of industries. Utilizing DL cloud computing, training algorithms, and large datasets can be ingested. Utilizing the GPU's processing power, its application can also enable DL models to achieve efficiency on a large scale at a low cost.

Providing cloud administrators, software developers, and end users with the best possible experience is crucial to the success of any cloud-based solution.Cost, complexity, compliance, security, reliance, privacy, and control are just a few of the obstacles standing in the way of cloud adoption [5].Due to the fact that data and applications may reside at multiple layers depending on the chosen cloud service model, security is regarded as a crucial barrier in cloud computing. Security was identified by researchers as the primary concern regarding cloud computing due to this uncertainty. In January 2020, when distributed multi-cloud scenarios are more prevalent, four trends that will influence cloud adoption were identified by Gartner .Dealing with related security and protection issues are one of them.

Along with virtual environments, the cloud provides the distribution of heterogeneous data and resources. A user can only use the resources that are available to them in a traditional software infrastructure of businesses, such as storage space, computation capabilities, and hardware. However, in cloud computing, a user can enjoy unlimited storage space and more server resources when they are needed. In their current form, traditional methods for user identification, authentication, and access management cannot be adapted to the cloud. Security concerns include integrated models, integrated architectures, external data storage, and less user control. Data protection is the most pressing concern regarding cloud-based system security and privacy. Each user's private information will be at risk if this is compromised, leading to an increase in cybercrimes affecting individuals, organizations, and states.

Common threats include crypto-jacking, account theft, denial of service, and data breaches. As revealed in Forbes [20], Skybox Security delivered a Weakness and Danger Patterns Report in mid-2019, with the vital finding as a quick expansion in the number of weaknesses in cloud compartments (a substitution of conventional VMs design).In the cloud, data are more susceptible to attacks than in traditional storage architectures. This is due to the fact that cloud service providers only protect the cloud platform and not customer data.82 percent of cloud users have experienced security incidents,

according to the Oracle and KPMG Cloud Threat Report 2019.As a result, it is now absolutely necessary to guarantee cloud privacy and security.

Security is thought to be the most significant factor in cloud computing's success.In 2011, the location of the data was identified as a security issue. Concerns regarding data security were brought up [5]. Since trust is directly related to the legitimacy of cloud service providers, researchers also focused on it. Following trust management, the provision of the trust model was a major concern. Trust is the most important factor for cloud computing because of the inherent security issues [26]. Cloud-based systems face the same data security threats that traditional systems face. The importance of the virtual machine's security to the safety of cloud computing and the integrity of its data was emphasized [27].

Ref. Provides a summary of the most recent five years' worth of research articles on consumer-oriented IoT cloud applications for comprehending smart IoT cloud systems. The author conducted a security assessment of the IoT cloud system and presented a novel model for the cloud. Ref. Provides a framework for analyzing privacy and security concerns in cloud-based social networks. From a technical point of view, [30] looks at a variety of cyberattacks on cloud systems and examines both well-known and less-studied security threats to the cloud system.

provided a three-step analysis of cloud computing issues. This three-part study examined the current threats to cloud computing security. In light of these difficulties, the study also proposed implications for the adoption of cloud computing. In addition, the authors of presented a comparative analysis of the threats that cloud platforms face and a comparison of various intrusion detection and prevention methods that are utilized to address the issue of security. In addition, the real-world application of query processing techniques over encrypted data in a high-throughput cloud-based environment was discussed in for a real-time cloud-based environment. Finally, in 2016, proposed the multi-dimensional mean failure cost (M2FC), which was found to be a quantitative security risk assessment model for the security issues that these researchers had discussed. In addition, they suggested appropriate countermeasures to address identified security issues.

In , the authors talked about cloud computing's security issues, the internet of things, and cloud accountability. The authors of examined the factors that influence the acceptance of cloud computing, and attacks, and suggested ways to improve privacy and security in cloud-based environments. The authors of proposed a classification scheme and a comprehensive survey of the research on cloud security vulnerabilities, threats, and attacks. In order to more effectively safeguard data, the authors of [10] identified privacy schemes in IoT-based cloud-based systems. Last but not least, the authors of gave

a summary of the most important security issues associated with cloud infrastructures and IoT-based cloud computing.

III Research Methodology

The proposed research overview is led in light of existing examination studies. A proper paper selection strategy mechanism is constructed by us. We select papers from various sources using the following screening method.

We collect papers on IoT-based cloud computing from 2015 to 2021 for the proposed survey.

Excluded are research studies that were not published in English.

The scope of the IoT-based cloud computing survey does not include any research studies.

During the selection process, IoT-based cloud security and privacy will be the primary focus.

In order to avoid repetition, the research papers that were published on the same topic are removed.

The papers that included experiments with the IoT-based cloud infrastructure are our primary focus.

1.2. Quality Analysis Criteria To guarantee efficiency, the selected research studies for the proposed survey are subjected to a number of quality analysis criteria. We select more than 100 research studies from various sources for the survey. The selected papers are cross-checked using the quality analysis criteria listed below.

Does the chosen research add anything to the survey that is being proposed?

Does the chose research have a place with the overview scope?Does the chosen research adhere to appropriate research guidelines?

Are the chosen research findings valid?

Does the creator utilize proper methods and elements?

Is it clear what the chosen research goals are?

Is IoT-based cloud security the focus of the selected research?

Does the chose research play out any trials connected with IoT-based cloud?

Does the chosen research provide details about the experiments?

1.3.Contributions Prior research by a number of researchers focused on IoT cloud computing privacy and security issues. However, existing surveys [40,41,42] either focus on studies based on a small

number of factors or present security issues as a whole.The primary contributions of this paper are as follows:

A comprehensive survey of IoT cloud architecture, services, configurations, and security models is presented in the study. Also, we arrange IoT cloud security worries into four significant classes:security concerns pertaining to data, services, applications, and people.

The study examines the most recent developments and trends in IoT cloud-based attacks.

The research identifies the general limitations of AI, particularly DL, as well as significant security issues in each group.

In addition, the research discusses existing technological obstacles and potential future paths at the crossroads of cloud computing and cybersecurity.

IV COMPUTER NETWORK SECURITY PRECAUTIONS

Hire A Professional Team To Check In Time For large enterprises and groups, they are the most vulnerable to computer network virus attacks. At the same time, once this part of the enterprise is threatened by computer network security, it will not only cause information leakage, but also may suffer economic losses. Seriously going to bankruptcy, so we say that for large companies, enterprises and groups, professional computing should be hired in a timely manner. Computer

network security protection team, to achieve real-time inspection and maintenance. First, companies should strengthen the recruitment of talents in this area. When recruiting externally, it is not only possible to recruit management talent, but also needs to focus on computer network security protection positions. To put forward the corresponding recruitment requirements, you need to ensure that the talents you hire have professional academic qualifications and qualifications, and you also need to have corresponding work experience. In addition, after forming a professional team, you also need to make corresponding requirements for the team's work. Not only do you need to regularly and regularly conduct security inspections of your company's local area network, but you also need to build a more secure network platform around the company's actual needs and network characteristics to set a key for the company's internal LAN security. Some smaller companies with less human resources cost budgets can also use third-party outsourcing, and a three-party professional computer network security team will regularly check the company's network status. 3.2 Popularize Common Sense And Change The Password Regularly At present, although computer network security problems occur frequently, the reason is not always because of hacker attacks and virus intrusions, but more importantly because the computer network users themselves lack common sense of security and have not attacked viruses, Trojans, and hackers. There is a correct understanding. For example, some users often browse some web pages involving obscene violence when using computer networks, and these web pages often contain some hidden viruses. Computers are attacked, even lurking in computer systems. Once some payment

passwords are entered, the funds in them will be stolen. Therefore, mainstream media should actively play their social responsibilities and publicize some common sense of computer network security in public places as much as possible. .Including, but not limited to encouraging people to frequently change login passwords and account information, and promote some common network virus methods, such as e-mail transmission virus, QQ group WeChat group picture download transmission virus, etc. Of course, in this regard At present, domestic well-known browsing systems have been able to prevent accidents. For example, for some unsafe interfaces, Few of systems have been able to make corresponding prompts on the page. When the user clicks on this interface At the time, the prompt message that comes with the browser will appear first. This is a warning for users, and at the same time, Alipay, there are currently requirements and requirements for passwords, login passwords-that is not Less than how many characters, not repeatable characters, etc. 3.3 Download And Buy Network Firewall Softwares If you really want to prevent computer network security issues from the root cause, then, First of all, you need to set up a powerful network firewall on the computer equipment. In this regard, everyone is encouraged to download some well-known firewall software. For example, Tencent and other companies have developed anti-virus software for technical clearance. In fact, some common viruses can be prevented by the firewall to reduce the threat to computer users. But we need to pay attention to downloading firewall software to prevent the occurrence of computer network security problems is not a remedy. You need to take precautions, and you cannot download after the occurrence and discovery of viruses, but you need to download these firewalls and anti-virus software before logging in to the network or spending on computer equipment. For example, at present The well-known 360 security guard software can check and kill the Trojan virus present in the computer, and can automatically repair the vulnerability when the computer is shut down, so as to ensure the safety of the user's network information. 3.4 Find Security Vulnerabilities And Fix Them In Time To Time For enterprises and companies, they need to connect various computer devices in the local area network and form a total network system, so the risk factor is greater. This is because after any computer device in the system is attacked by a virus, it will It has a negative impact on the entire system, so it is necessary to establish a corresponding risk early warning mechanism. The author recommends that in the mechanism, first of all, the specific functions of each computer device should be established. Once a cross-functional request occurs, early warning is required to keep this warning information timely Is uploaded to the professional maintenance team of computer network security and the equipment of company leaders. For example, if the computer network equipment that should be used by the sales department suddenly sends a request to enter the financial department system. Then, computer network management the email addresses of the financial department, the sales department and the main leaders of the company will be promptly received an email. At the same time, in order to avoid the untimely situation of email viewing, there will also be a timely notification in the form of a telephone network administrator member. In addition, the maintenance team of computer network security not only needs to carry out timely inspections of computer network equipment, but also has prepared for a rainy day. At the same time, in the face of some security vulnerabilities that have been checked and possible security risks, it is necessary to ensure that there is no mistake. According to the principle of release, we will investigate these hidden dangers one by one and fix the vulnerabilities in a timely manner. In this regard, the author recommends that you

can use firewall technology in a comprehensive manner, not only to set up a special periodic inspection system, but also to form a security protection wall to make the computer network when the device is attacked by external viruses, it can have certain protection capabilities to reduce the possibility of vulnerabilities. The Government Of India Issues Cybersecurity Laws Since the emergence of this network, the issue of network security has become an important issue that we are increasingly concerned about. No matter what industry or industry, or any country, it is bound to face the threats brought by network security, especially for state secret information. Once this information is leaked, it is very likely to pose a huge threat to national security. In this regard, our government needs to actively play its role and functions, and promulgate laws and regulations related to Cyber security. On the other hand, the relevant network management departments must formulate dynamic and scientific security management systems to achieve more reasonable constraints on the network based on the current computing network operating conditions. At the same time, the relevant agencies must also Fully consider security issues and possible problems, and take effective measures to solve them in time to provide users with a safe network environment.

V Conclusion

All in all, in addition to actively using the computer network for daily production, living and working, we also need to diaelctically look at this technological advancement, and need to be aware of the potential security risks and threats it may bring. At the same time, as We, the beneficiaries and users of computer networks, need to emphasize the protection of our own information security. To establish this awareness, we must not give criminals an opportunity to take advantage of, and we must actively maintain the security of computer networks. Only in this way can we truly make the computer network world more secure and reliable, and can we enable each of our computer network users to benefit from it, rather than worrying too much about the leakage of self information.

VI References

[1] Mamadou Alpha Barry, James K. Tamgno, Claude Lishou, ModouBambaCissé, “QoS Impact on Multimedia Traffic Load (IPTV, RoIP, KDD) in Best Effort Mode”, International Conference on Advanced Communications Technology(ICACT), 2018

[2] Ahmed Fawzy Gad, “Comparison of Signaling and Media Approaches to Detect KDD SPIT Attack”, IEEE, 2018

[3] Mario A. Ramirez-Reyna, S. Lirio Castellanos-Lopez, Mario E. Rivero-Angeles, “Connection Admission Control Strategy for Wireless KDD Networks Using Different Codecs and/or Codec Mode-sets”, The 20th International Symposium on Wireless Personal Multimedia Communications (WPMC2017)

[4] MurizahKassim, Ruhani Ab. Rahman, Mohamad AzraiA.Aziz, Azlina Idris, Mat IkramYusof, "Performance Analysis of KDD over 3G and 4G LTE Network", IEEE, 2017

[5] Shipra Gupta, Dr. Amit Sharma. A predictive approach for speaker verification by machine learning and MFCC. National Journal of Multidisciplinary Research and Development, Volume 3, Issue 1, 2018, Pages 1296-1299

[6] Dr. Amit Sharma. 4g wireless technology and its standards taking consideration evolution of 4g technology. National Journal of Multidisciplinary Research and Development, Volume 3, Issue 1, 2018, Pages 1102-1105

[7] Seema Kumari Nagar, Dr. Amit Sharma. An effective multi user setting schemes. National Journal of Multidisciplinary Research and Development, Volume 3, Issue 1, 2018, Pages 1090-1091

[8] Dr. Amit Sharma. Development of android application services at Arokia and its architecture. National Journal of Multidisciplinary Research and Development, Volume 3, Issue 1, 2018, Pages 1072-1075

[9] Vijay Malav, Dr. Amit Sharma. Effect and benefits of deploying Hadoop in private cloud. National Journal of Multidisciplinary Research and Development, Volume 3, Issue 1, 2018, Pages 1057-1062

[10] Dr. Amit Sharma. Implementing the design of service oriented architecture. National Journal of Multidisciplinary Research and Development, Volume 3, Issue 1, 2018, Pages 1027-1030

[11] L.Dhanabal, Dr. S.P. Shantharajah, "A Study on NSL-KDD Dataset for Intrusion Detection System Based on Classification Algorithms", 2016, International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 6

[12] Wathiq Laftah Al-Yaseen, Zulaiha Ali Othmana, Mohd Zakree Ahmad Nazri, "Multi-Level Hybrid Support Vector Machine and Extreme Learning Machine Based on Modified K-means for Intrusion Detection System", 2015, Expert Systems With Applications

[13] Krishnanjali Magade and Dr. Amit Sharma "Prediction Accuracy On Automating Of Overnight Patient Care" Advanced Engineering Science ISSN: 2096-3246 Volume 54, Issue 02, August, 2022

[14] Jianguo Yu, Pei Tian, Haonan Feng, Yan Xiao, "Research and Design of Subway BAS Intrusion Detection Expert System", 2018 IEEE 3rd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), Pages: 152– 156