IoT and Cloud Integration: A Comprehensive Study of Emerging Issues

Mrs. B. Bala Abirami[1],
[1] Assistant Professor,
Department of Artificial Intelligence and Data Science,
Panimalar Engineering College, Chennai,
bala.bami@gmail.com

Dr. G. Umarani Srikanth[2]
[2] Professor,
Department of Computer Science and Engineering,
Panimalar Engineering College, Chennai,
umaranisrikanth@gmail.com

Abstract —

Everyday items and high-tech networked gadgets may both be linked via the Internet of Things (IoT). Businesses and people alike may benefit from cloud computing services, which enable the storage of data on distant servers and the online access to apps and solutions. In order to make most of the resources that a company has, this is crucial. However, many users can be affected by system outages or cyber-attacks caused by vulnerabilities in the system. Strong security measures must be included in IoT systems to protect sensitive data and prevent system failures caused by cyber-attacks. A number of cyber security laws, standards, and regulations must be followed when dealing with the massive amounts of sensitive data collected by IoT devices. This data includes personal identifying information. Loss of trust from customers, fines, reputational harm, and legal action are all possible outcomes of data breaches involving sensitive personal information.

Keywords— System vulnerability, cyber security, Data Privacy, Cloud Computing, Data Confidentiality, Internet of Things(IoT), Artificial Neural Network(ANN), Blockchain technology.

I Introduction

Cloud computing conveys computing services, such as servers, data storage, databases, networking, data transfer, and more, over the Internet (‘the cloud’). The Internet of Things depicts the embedding of physical objects with sensors, software, and other technologies to connect and exchange information with other devices and systems over the Internet. These devices autonomously collect and share information from diverse sources. Combining these two technologies has brought a new term — Cloud Internet of Things. In simple terms, the Cloud Internet of Things is an IoT infrastructure connected to cloud services. It uses cloud computing services to collect and process information from IoT devices and manage these devices remotely. Since the cloud systems are scalable, it’s possible to process large amounts of data simultaneously.

In the rapidly evolving landscape of IoT security, a multitude of research endeavours have surfaced, each offering distinct insights and proposals to fortify the integrity and resilience of IoT ecosystems. Addressing the fundamental essence of IoT connectivity, studies underscore the significance of efficient wireless communication protocols. At the same time, there is a surge in support of block chain technology to protect sensitive medical records. As IoT deployments burgeon, the ubiquitous utilization of Low Range (LoRa) devices for monitoring applications pervades the discourse, prompting discussions on the necessity for cross-platform compatibility to enhance deployment flexibility. In tandem, proposals advocating for the integration of IoT and block chain technologies endeavour to amplify scalability and streamline transaction processing within IoT networks.

Acknowledging the intricate interplay between security and privacy in IoT ecosystems, studies identify blockchain as a potent solution to mitigate prevalent challenges. Moreover, the burgeoning convergence of 5G and IoT herald a new era of connectivity, underpinning transformative applications in smart cities and precision agriculture. Efforts to foster seamless communication among interconnected IoT devices underscore the need for innovative communication solutions and interoperability protocols. Meanwhile, initiatives to fortify IoT device security through blockchain integration resonate, promising tamper-proof mechanisms for device authentication and data integrity. In tandem, novel encryption algorithms designed to bolster data security in cloud computing environments find traction, offering robust mechanisms for safeguarding sensitive information.

Concurrently, the significance of the Cloud of Things (CoTs) paradigm emerges, offering scalable frameworks for data management and resource optimization. Discussions on advanced machine learning techniques accentuate their pivotal role in combating emerging cyber threats and bolstering IoT security. Augmenting the arsenal of security measures, proposals advocating for AI-driven intrusion detection mechanisms underscore their potential to fortify cloud and network security infrastructures. In essence, the convergence of diverse methodologies and technologies signifies a concerted effort to fortify IoT security, charting a path towards resilient and secure IoT ecosystems [15].

In this survey paper, we present a general overview of IoT architectures, methods / technologies and some common security concerns. The paper comprises the following sections.

1. Existing methods and technologies are discussed in section II.
2. A complete overview of IoT architecture and various technologies are discussed based on the survey of previous papers in section III.
3. Section IV provides analysis of various cloud platforms and technologies with IOT.

II Literature Review

The authors in the paper [1] discussed that IoT is a system that allows physical things to connect to the internet via the use of IP addresses. Because of this innovation, a great many everyday items may now function as smart devices with a wide range of uses. Wireless communication methods that are both energy efficient and provide improved connection are necessary for these devices. In their research, the authors examine the most common IoT communication methods, both long-range and short-range, and they survey the state-of-the-art conventional wireless technologies used by IoT devices. Numerous occurrences of patient privacy breaches highlight the persistent difficulties in protecting healthcare data, as highlighted in this research

[2]. The current state of affairs does not always do a good job of balancing accessibility with privacy concerns. One such solution is blockchain technology. Secure, interoperable, and efficient access to health data is ensured by the suggested solution, Ancile, a blockchain-driven architecture. Security and privacy are both improved by Ancile's use of smart contracts and advanced encryption. The long-standing problems with healthcare data privacy and security are the target of this effort. Ancile is currently in its early stages of development, but it has the potential to greatly enhance EHR administration.

LoRa (Low Range) devices and applications in IoT were surveyed by the authors in the paper [3]. The goal is to evaluate the current state of LoRa devices and the applications that utilize them. Based on the findings, most configurations make use of single-board computers that have LoRa modules installed, which are mostly utilized for monitoring purposes. In order to increase the future use of LoRa technology, the article recommends developing a cross-platform device that can monitor and control. To reduce the load on the global blockchain, the authors [4] proposed integrating IoT with blockchain technology by means of a peer-to-peer network at the local level. This method improves transaction processing speed while reducing the total ledger footprint and block size on global peers. Results from a testbed shows that this method works as advertised, with significant scalability improvements.

The study [5] discussed the privacy and security issues associated with IoT and suggested that blockchain technology provides a possible solution. Data security, scalability, identity, and authentication are some of the major challenges listed. Concerns about data storage and legal ramifications are just two of the obstacles identified by the authors to integrate block chain with IoT. Finally, it suggests directions for further studies. The paper [6] investigates the relationship between 5G and IoT. The advent of 5G networks has propelled the extensive integration of IoT, enabling devices to connect and share data via Internet. This review focuses on the communication technologies that support IoT operations within the 5G infrastructure, emphasizing critical uses such as smart cities and precision agriculture. Nonetheless, the paper also recognizes the hurdles these technologies face, including issues related to privacy, security, and energy consumption. The authors aim for this research to be a useful guide for further studies on communication technologies in 5G-supported IoT environments.

With efficient communication between devices being key to the development of IoT, the objective [7] was to set up a network of linked gadgets. Currently, there is a lack of seamless interaction between Device-to-Device (D2D) communication technologies due to their isolation and the use of different protocols. Finding ways to make these technologies function together at the network layer is the focus of this article, which delves into the challenges of integration. The research work discussed [8] offer a plan to leverage blockchain technology to make IoT devices more secure. Due to their small size and lack of security protections, IoT devices are becoming more vulnerable to assaults as they become more widespread. Blockchain provides an answer by facilitating a distributed ledger system that is safe, unchangeable, and visible.

The authors discussed [9] about enhancing the safety of data stored in the cloud by introducing a new, lightweight encryption mechanism. This method uses the strengths of symmetric and asymmetric cryptography by combining them. Test results showed that this novel technique outperforms state-of-the-art cryptographic algorithms in terms of speed, robustness, and security. In this article [10], focuses on integrating cloud computing with IoT, helps us to overcome obstacles and make the most of what each technology has to offer. The current literature emphasizes the supplementary advantages of this integration, which include increased capacity for processing data in real-time, better management of resources, and increased scalability. Additionally, the studies highlight how cloud platforms provide effective data integration, storage, and analysis, providing a solid groundwork for IoT applications. It also highlights the potential of IoT frameworks powered by the cloud to drive new applications in areas like smart urban development, transportation, healthcare, and more. A number of implementation challenges, such as those involving security, interoperability, and reaction times, have been recognized in the literature. It concludes that these issues need more investigation into order to find creative ways to maximize the complementary nature of Cloud computing and IoT.

This article [11] delves into the idea of IoT Cloud, often called CloudIoT, which combines IoT with cloud computing. It offers a strategic way to get over the limited resources of IoT devices and encourages their widespread use. But new privacy and security issues arise from this merging. In order to keep data maintained in the cloud reliable, intact, and secret, it is necessary to address these problems, according to the available literature. IoT devices and cloud platforms are vulnerable to data breaches, illegal access, and targeted assaults. The massive collection and storage of private and sensitive data on the cloud also gives rise to privacy concerns. In order to safeguard IoT systems that rely on cloud computing resources, this article takes a close look at the security issues specific to IoT cloud installations, including possible dangers, weaknesses, and ways to fix them. In order to address security concerns with IoT, the paper [12] explored block chain technology. The results have shown that block chain greatly enhances the security of IoT by enhancing its availability, confidentiality, and integrity. To further improve IoT security, the article recommended looking at hybrid models and how to combine block chain with other technologies.

The research [13] presented a system for protecting data stored in the cloud that makes use of Blowfish encryption and MD5 hashing. There are major security holes introduced by cloud computing despite the fact that it provides scalable access to computer resources. The research proposed a hybrid encryption approach that combines Blowfish and MD5 to address these concerns, with the goals of enhancing data security while reducing storage needs. Important for cyber security, the article [14] covered new advances in improving Intrusion Detection Systems (IDS) by integrating deep learning techniques with metaheuristic optimization algorithms. It zeroed in the use of Convolutional Neural Networks (CNNs) for intrusion detection by analyzing complex feature representations in network data. With the introduction of a novel IDS model tailored to IoT environments, CNN-based feature extraction is combined with the Metaheuristic Growth Optimizer (MGO) and the Whale Optimization Algorithm (WOA). In order to overcome the difficulties associated with discrete features in intrusion detection systems, MGO improves the efficacy of intrusion detection and WOA improves the feature selection process.

Data creation has skyrocketed due to the exponential growth of Wireless Sensor Networks (WSNs) and IoT devices [15].

Thus in this literature review, a number of studies have evaluated on current IoT platforms, technologies, and designs in this literature review.

III IoT Architecture and its Technologies

The Internet of Things (IoT) is based on IoT devices, or the "things" in the name. These are physical objects, including sensors and actuators that can communicate with one another and be controlled by an external system, often an IoT platform (a central server). A temperature sensor that is linked to a central server so that the user may view the current temperature is an example of an Internet of Things sensor.

The interaction between users and physical devices is a fundamental concept of Internet of Things (IoT) systems, as demonstrated by these examples. Specifically, sensors provide users information about their surroundings, and users can act on other physical devices based on that information. One other important feature of IoT systems is the ability to create "smart" applications for certain use cases. A variety of activities, including data analysis, prediction, control, and user monitoring and alerting, may be included in these applications. Taking into account the aforementioned instances, the user might set up rules on the IoT platform to automatically turn on or off the ventilation system based on the data that the air quality sensor reports.

IoT architectures can vary significantly based on the specific use case (e.g., smart home, industrial IoT, healthcare, agriculture) and scalability requirements. Designing a robust IoT architecture involves careful consideration of factors like data volume, latency requirements, security concerns, and regulatory compliance.

A. *IoT Workflow*

Cloud IoT is an infrastucture that connects all the essential IoT devices to cloud-based servers, causing in real-time data analytics, data-driven decision-making, optimization, and reducing risk factors. In general, IoT cloud computing implies there is a network of IoT devices that gather data and transmit it to the cloud for further processing, analysis, and storage. This can be broken down into the following steps which is shown in Fig:1

For Example, In Factories the sensors gather some metrics about devices in the factory. We may later foresee this data on the cloud to check for potential malfunctioning of any devices or inconsistencies of any kind. This process can, of course, be fully automated.

In this, “decision making,” “data analysis,” and “data storage” are not firmly ordered. In fact, even “transmission to the cloud” and “data processing” can switch places if one utilizes edge computing, whereby a few information is processed and combined on the level of IoT devices or partially processed and aggregated data to the cloud, which ultimately saves the network bandwidth and decreases latency since the volume of the outgoing data is being decreased.

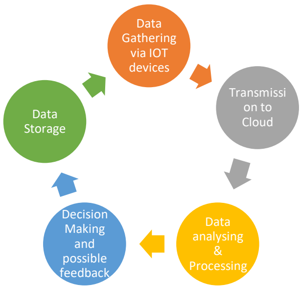
Data Gathering via IOT devices
Transmissi on to Cloud
Data analysing & Processing
Decision Making and possible feedback
Data Storage

Fig: 1 Workflow in IoT Architecture

IoT platforms and devices still don't employ any common standards or technologies as of now. Rather, disparate platforms and devices take into account various standards and technology. As a result, in order to implement an Internet of Things system, users frequently need to research, set up, and combine several architectures and technologies, which can make the process challenging and time-consuming.

In the research literature there has been also many proposed architectures over the past years. One of the simplest is the five-layer model reproduced in Fig. 2, which consists User, proximity, public, cloud and enterprise. Several other more complex multi-layered architectures have been also proposed. Recently, abstract reference architecture was introduced in [10] and shown to map well onto different state-of-the-art IoT platform architectures to avoid the attacks. The reference architecture proposed in [12], and reproduced in Fig. 1, can be extended considering the models defined in the IEEE Standard for an Architectural Framework for the Internet of Things. The result is shown in Fig. 2, where security and management blocks have been added. Such architecture contains ten different parts: Devices/Sensors, Connectivity, Edge Computing, Gateway, Cloud Services, Data Storage, Analytics and Insights, User Interface, Analytics and Insights, User Interface, Security, Integration. These parts are described in Fig.2

B. *IoT Architecture*

IoT (Internet of Things) architecture refers to the structure or framework that supports the interconnection of various IoT devices, sensors, networks, and applications. It involves several layers and components working together to enable the collection, processing, and sharing of data between devices and applications. Here’s a typical IoT architecture breakdown:

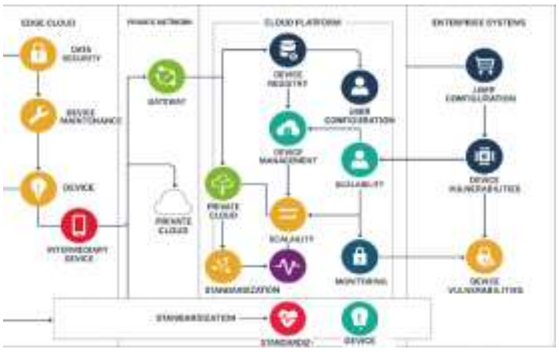

Fig:2 IoT Architecture

These are the various functionalities of the IoT architecture

Edge Cloud: Shows the initial stage where data is collected from IoT devices and highlights the importance of data security and device maintenance. **Private Network:** Depicts the role of gateways in translating protocols and the use of private clouds for secure data transfer.
Cloud Platform: Illustrates the core cloud services, including device registry, user configuration, device management, scalability, and monitoring. **Enterprise Systems:** Represents the final destination of the data, where it is used for business applications, and highlights the ongoing concern of device vulnerabilities. The Fig.2 also shows other components like IoT Gateway, which connects physical devices to the cloud, and API Management, which helps different parts of the cloud communicate securely and efficiently.

IV Analysing Various Cloud Platform and Technologies

A. AWS

One of the most prominent cloud computing platforms is Amazon Web Services (AWS), which offers more than 200 different services, such as storage, compute, databases, and analytics, among many others, on demand. A pay-as-you-go strategy improves cost efficiency and flexibility by letting firms increase their IT infrastructure dynamically based on their needs. Many businesses are interested in using AWS because of its worldwide network of data centres, which provides vital applications with high availability and fault tolerance. Secure protocols like HTTPS and SFTP encrypt data as it travels via the network, and users may choose between server-side and client-side encryption. Additional levels of traffic limitation are provided by firewalls and Virtual Private Clouds (VPCs), in addition to detailed access restrictions and multi-factor authentication, which assist prevent illegal access. AWS Key Management Service provides secure storage for encryption keys, and compliance certifications and detailed logging ensure accountability.

B. IBM Cloud

IBM Cloud stands out with its comprehensive suite of cloud services, offering both public and private options, and catering to diverse business needs. With a focus on security, it employs AES-256 and Homomorphic Encryption for data confidentiality and Bring Your Own Key (BYOK) for encryption control. Zero Trust principles and continuous AI-powered monitoring mitigate threats, while Identity and Access Management (IAM) ensures least privilege access with adaptive MFA. Through a shared responsibility model, users enhance security via configuration and best practices. Independent security audits attest to their commitment to the highest standards. For IoT integration, IBM Cloud provides secure solutions with encryption, zero-trust architecture, and multi-factor authentication, ensuring data integrity and availability across its global network. Its pay-as-you-go pricing model enables cost optimization, while open standards prevent vendor lock-in.

C. Google platform

Google Cloud Platform (GCP) offers infrastructure, platform, and software cloud computing services. Scalability, security, and a worldwide network make it famous. These capabilities make GCP a flexible and trustworthy option for enterprises wishing to grow and safeguard their digital operations. It supports various programming languages and frameworks, with services like Compute Engine, Big Query, and Kubernetes Engine. GCP prioritizes security through encryption, network security, IAM, private connectivity options, compliance, and advanced threat detection.

D. Microsoft Azure

Since 2010, Microsoft Azure has offered on-demand computing, storage, databases, networking, and analytics. Organizations seeking sophisticated cloud solutions can choose Azure due of its flexibility. It enables businesses to construct, deploy, and oversee applications globally through Microsoft's network of data centers. Azure accommodates various programming languages, tools, and frameworks, providing businesses with a scalable and cost-efficient solution tailored to their needs. In IoT operations, Azure prioritizes data security through a layered approach. It ensures device security through measures like authentication, secure boot, and hardware modules. Data is encrypted both in transit and at rest, with additional protection offered through network segmentation and threat detection tools.

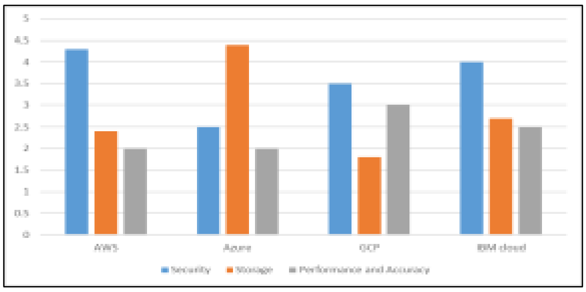

Fig 3: Comparative analysis of security, Storage, Performance and accuracy

Fig 3 compares security, storage, and performance characteristics for AWS, Azure, GCP, and IBM. Effective cloud use requires understanding each platform's features. Identity and Access Management (IAM), encryption, network security, and compliance solutions like AWS Config and AWS Security Hub set AWS apart. AWS Shield protects against DDoS attacks, while AWS WAF improves web application firewalls. Azure storage solutions—Blob Storage for objects, Disk Storage for blocks, and Azure Files for files—are excellent. Azure also provides Azure Archive Storage for long-term backups and Azure Data Lake Storage for large data analytics. Cloud systems perform by meeting user objectives for speed, responsiveness, and efficiency. These characteristics are optimized by each provider to improve user experience and workload management. GCP meets the performance for all the cloud users and it provides global network infrastructure designed for high performance and low latency, with services like Google Compute Engine for compute, Cloud SQL for databases, and Google Cloud CDN for content delivery. GCP also offers services like Google Cloud Load Balancing for distributing traffic.

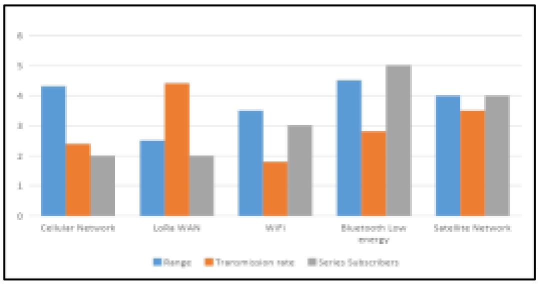

Fig 4: Widely Used Technologies for Sharing Data via IoT Devices

The Fig 4 visualization showcases the estimated market share of various technologies used to transmit data across long distances from IoT devices. Cellular networks, particularly Long Term Evaluation Machine Type Communication (LTE-M) and Narrow Band-Internet of Things (NB-IoT),, reign supreme due to their established infrastructure and reliable connectivity, making them the go-to choice for many IoT applications. Long Range Wide Area Network (LoRaWAN) emerges as a significant player, particularly for deployments requiring long-range communication with low data volume and power consumption. Wi-Fi HaLow finds its niche in situations demanding short-range, high-bandwidth data transfer, while Bluetooth Low Energy (BLE) caters to short-range, low-power device-to-device communication. Finally, satellite networks, despite holding the smallest market share, play an irreplaceable role in bridging the connectivity gap in remote areas where terrestrial networks are unavailable. The choice of technology ultimately hinges on factors like data volume, range requirements, power limitations, and environmental conditions.

IV Conclusion

This survey paper discusses the importance of cloud computing services, the evolving landscape of IoT security, the synergistic advantages of integrating IoT and cloud technologies, common security concerns, and aims to provide a comprehensive overview of security issues specific to IoT Cloud environments. Reliability, integrity, and confidentiality of data in the cloud infrastructure, data security and reduction of storage overhead using a hybrid encryption scheme, security measures implemented by AWS, Google Cloud Platform (GCP), and Microsoft Azure also discussed in this paper there are still a number of difficulties, though, such as the complication and variety of security issues, the demand for big and varied datasets, the need for real-time performance, and cultural issues. Previous proposed works created various outputs and the results are analyzed. It also emphasizes the benefits of integrating cloud platforms with IoT for enhanced scalability and real-time data processing, while also acknowledging challenges such as security, interoperability, and latency issues, with suggestions for future research directions.

REFERENCES

[1] Abdullah Ahmed Bahashwan, Mohammed Anbar, Nibras Abdullah, Tawfik Al-Hadhrami, and Sabri M. Hanshi,"Review on Common IoT Communication Technologies for Both Long-Range Network (LPWAN) and Short-Range Network " Cybersecurity and Privacy in Smart Environments: Current Research Trends and Future Directions, Sensors **2023**, *23*(9), 4430;

[2] Gaby G. Dagher Jordan Mohler, Matea Milojkovic, Praneeth Babu Marella, "Ancile: Privacy-preserving Framework for Access Control and Interoperability of Electronic Health Records Using Blockchain Technology.", February 2018,Sustainable Cities and Society 39(1),DOI:10.1016/j.scs.2018.02.014

[3] Oratile Khutsoane , Bassey Isong, "IoT Devices and Applications based on LoRa/LoRaWAN.", IECON 2017 - 43rd Annual Conference of the IEEE Industrial Electronics Society at South Africa, November 2017, DOI:10.1109/IECON.2017.8217061

[4] S. Biswas, K. Sharif, F. Li, B. Nour and Y. Wang, "A Scalable Blockchain Framework for Secure Transactions in IoT," in IEEE Internet of Things Journal, vol. 6, no. 3, pp. 4650-4659, June 2019, doi: 10.1109/JIOT.2018.2874095.

[5] S. R. Alam, S. Jain and R. Doriya, "Security threats and solutions to IoT using Blockchain: A Review," 2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 2021, pp. 268-273, doi: 10.1109/ICICCS51141.2021.9432325.."

[6] Quy Vu Khanh, Nam Vi Hoai, Linh Dao Manh, Anh Ngoc Le, Gwanggil Jeon, "Wireless Communication Technologies for IoT in 5G: Vision, Applications, and Challenges", Wireless Communications and Mobile Computing, vol. 2022, Article ID 3229294, 12 pages, 2022. https://doi.org/10.1155/2022/3229294

[7] Oladayo Bello, Sherali Zeadally, Mohamad Badra,Network layer inter-operation of Device-to-Device communication technologies in Internet of Things (IoT),Ad Hoc Networks,Volume 57,2017,Pages 52-62,ISSN 1570-8705,https://doi.org/10.1016/j.adhoc.2016.06.010.

[8] Marzan Tasnim Oyshi, Moushumi Zaman Bonny, Zerin Nasrin Tumpa, and Susmita Saha, "IoT Security Issues and Possible Solutions Using Blockchain Technology ." Advances in Distributed Computing and Machine Learning, 2021, Volume 127,ISBN : 978-981-15-4217-6

[9] Sana Belguith, Abderrazak Jemai, Rabah Attia, " Enhancing Data Security in Cloud Computing Using a Lightweight Cryptographic Algorithm." ICAS 2015 :The Eleventh International Conference on Autonomic and Autonomous Systems. 978-1-61208-405-3 , pp 98 to 103

[10] H. F. Atlam, A. Alenezi, A. Alharthi, R. J. Walters and G. B. Wills, "Integration of Cloud Computing with Internet of Things: Challenges and Open Issues," 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Exeter, UK, 2017, pp. 670-675, doi: 10.1109/iThings-GreenCom-CPSCom-SmartData.2017.105.

[11] N. Almolhis, A. M. Alashjaee, S. Duraibi, F. Alqahtani and A. N. Moussa, "The Security Issues in IoT - Cloud: A Review," 2020 16th IEEE International Colloquium on Signal Processing & Its Applications (CSPA), Langkawi, Malaysia, 2020, pp. 191-196, doi: 10.1109/CSPA48992.2020.9068693.

[12] Mohammed Uzair Khan, "Blockchain Technology for the Security of Internet of Things: Challenges, Solutions, and Future Trends. " https://doi.org/10.31224/3060

[13]Shikha Rani, Shanky Rani, " Data Security in Cloud Computing Using Various Encryption Techniques." International Journal of Modern Computer Science (IJMCS), Volume 4, Issue 3, June, 2016, pp.163-166

[14] Abdulaziz Fatani, Abdelghani Dahou, Mohamed Abd Elaziz, Mohammed A. A. Al-qaness, Songfeng Lu, Saad Ali Alfadhli and Shayem Saleh Alresheedi, "Enhancing Intrusion Detection Systems for IoT and Cloud Environments Using a Growth Optimizer Algorithm and Conventional Neural Networks." Cybersecurity and Privacy in Smart Environments: Current Research Trends and Future Directions,Sensors 2023, April 23, 4430.https://doi.org/10.3390/s23094430

[15]Mohammad Aazam, Eui-Nam Huh, Marc St-Hilaire, Chung-Horng Lung , Ioannis Lambadaris , "Cloud of Things: Integration of IoT with Cloud Computing", Studies in Systems, Decision and Control, Springer International Publishing, june 2016,vol.36,pp:77-94