Journal of Informatics
Electrical and Electronics Engineering, 2023,
Vol. 00, Iss. 00, S. No. 000, pp. 0-00
ISSN (Online): 2582-7006

Implementing Cloud Security through AWS for Blood Bank Application

Apoorva Srivastava[1], Syed Wajahat Abbas Rizvi[2], Rashmi Priya[3]

Amity University Uttar Pradesh, India [1,2], GD Goenka University, India[3]
[1]apoorva8.lko@gmail.com, [2]swarizvi@lko.amity.edu, [3]rashmi.priya@gdgu.org

How to cite this paper: A. Srivastava, S. W. A. Rizvi and R. Priya, "Implementing Cloud Security through AWS for Blood Bank Application," *Journal of Informatics Electrical and Electronics Engineering* (*JIEEE*).

https://doi.org/10.54060/jieee.2023.81

Received: 01/04/2023
Accepted: 01/06/2023
Online First: 02/08/2023

Abstract

In today's time the technologies are seeing a huge shift of work from the on-center to over the internet, which means that a huge number of online services is required, these services could be backup and the data recovery should be available over the internet. Cloud computing is the platform over the internet which provide the services of networking, sharing, storing, etc. on the internet. Not only this shift of data is being observed in IT sectors, but also this shift is being observed in the healthcare sector. With the increase in the average age limit of the human beings and new diseases increasing the medical needs. The traditional healthcare is now being replaced by modern and more progressive healthcare. Thus, cloud is providing with several healthcare solutions. However, even after have a lot of benefits of using cloud services it also has some of the risks. The major risk being of the security of the patient's data. This paper analyses the security issues and their possible countermeasures for the same. The security measures presented in the paper are based on patient data in relation to data storing, access and security of data. In the paper I have worked towards the development of the android application of blood bank, the application uses the Android studio as IDE and the AWS Amplify as the cloud service to host and deploy the application over the cloud. In this paper we will also see the benefits of using the cloud computing, its security and also what are the future works that need to be done in the field.

Keywords

Cloud computing, Cloud Security, AWS Amplify, Android Studio.

1. Introduction

Cloud Computing is a distributed architecture which works over the client-server model. The services of the cloud such as storage, security, sharing, networking is given by the cloud service providers (CSP's), all of these cloud service benefactors are just like Internet service providers the difference is that these cloud service providers provide the users a suitable platform to run and use the services to run the function over the internet.

As the population of the world is increasing and also the age of the population, this is leading to a drastic increase in the in-crease diagnosis of chronic diseases like diabetes, respiratory disorders or heart related diseases. These patients usually manage self-management in and out of the hospital, thus the availability of the health care data at all times is important, thus problem could be solved by using cloud health care services. The main aim to provide the cloud platform for the healthcare data is to ensure the availability of the all of the medical data of all the patients at all the possible locations so that all the required health care arrangements can be made accordingly. Maintaining the health care data over the cloud ensures the data security by the cloud security services, not only this but using the cloud services is much more scalable, cost efficient and flexible. The main risk due to which the people want to adopt to the cloud is the data security, the data in the on-center mode may be handled by the third party which rises the main concerns among the users thus the solution of it is given by the cloud security features such as the IAM policies of AWS, where only the authorized personals can get access to the data. The need of this project is to make the blood available at all times so as no person would lose their life due to non-availability of blood, using the cloud also adds an extra layer of security to the application.

The paper has been managed as the following: The second section describes the security that has been provided by the cloud. The third section gives the overview of the data analysis of health data over the cloud. Section four shows all the re-lated works on the cloud security. Section 5 shows the implementation of the blood bank application and the benefits of the security by hosting the same over the cloud The sixth section show the benefits of using the cloud for security purposes, this section is followed by the conclusion.

2. Cloud Security

Security is one of the major concerns when talking about storage of the curtail data. Thus, one of the major concerns for the people transferring statistics to the cloud is mainly the safety of the day. Cloud security is an infrastructure-based security measure which protects the data and ensures the user and customers devices authentication and is the data being accessed is safe.

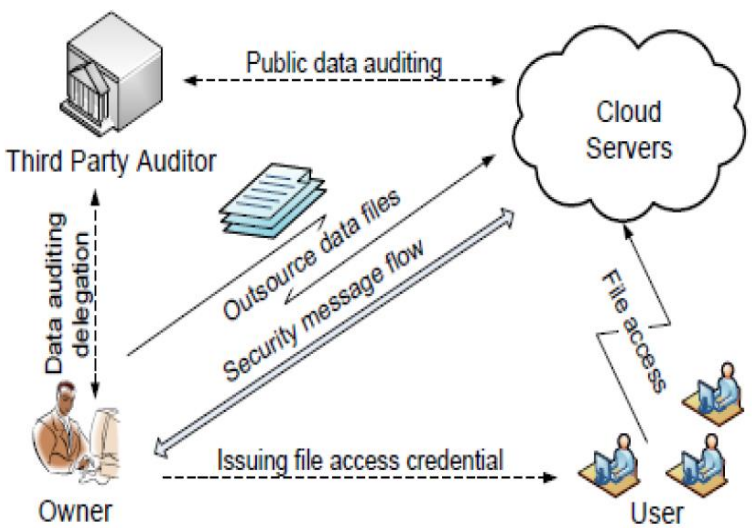

Figure 1. Data Security Architecture of Cloud

2.1. Issues in Cloud Computing Security

The virtual machines (VM) do have nonstop threats. These threats in the VM could be newly introduced if not these could be the risks could be presiding due to its inheritance form the traditional system. [4] The publication by the Burton Group, "At-tacking and Defending Virtual Environments," groups these risk as follows:

- The attacks already existing in the VM are working.
- The hypervisor is risk preservative since the distinct systems must be protected.
- Adding a distinct system to the Virtual Machine increases the threat to it.
- A trusted hypervisor with an untrusted VM is lesser a risk as compared to the trusted VM with an untrusted hyper-visor.

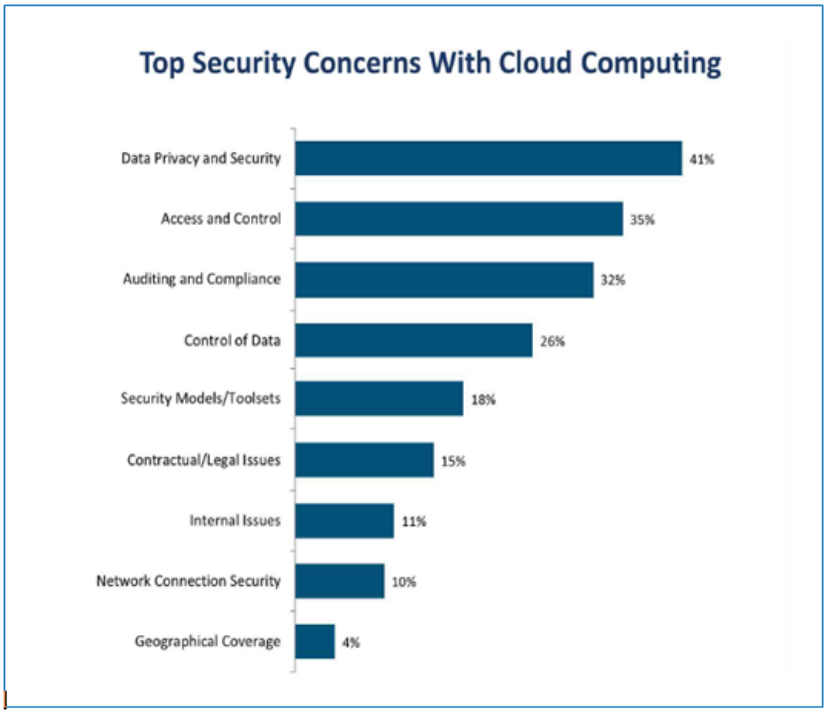

Figure 2. Top Cloud Security Concens[14]

Now keeping the above parameters in mind, we can define the different types of the risks listed as follows can be identified:

- Weak Admittance Control
- Virtual Machines may be Inactive.
- Duties of the virtual machines may be segregated
- Configuration of the virtual machines would be complex

In accordance with the Cloud Security Alliance (CSA), 'The Notorious Nine: Cloud Computing Top Threats in 2013' include: data breaks, data damage, account stealing/ server stealing, apprehensive Application programming interfaces, denial of service (DoS attacks), malevolent person inside the organization, misuse of cloud facilities, deficient due to assiduousness, shared technology vulnerability.

2.2. Solution for Issues related to the cloud security

Identity and Access Management: IAM is a service of cloud computing that allows limited access to the users. This simply means the users are able to access the cloud services in accordance with their role and hence securing the data and infor-

mation from being lost or used inappropriately. Thus, it can be said IAM allows access to the authorized personals only.

Sustaining the data mutually over traditional platform and Cloud platform: When the data is stored on only either of the traditional platforms or the cloud platforms it has the high chances of data getting lost, being manipulated, or being misused, thus, storing data on both the platforms depending upon the im-portance, usage and security required would be considered as adequate in terms of data and information security.

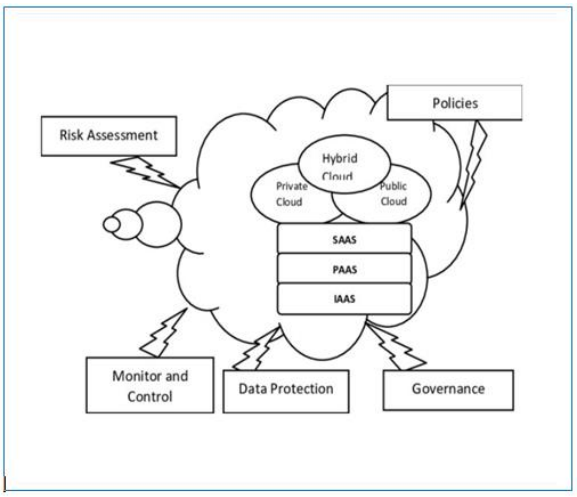

Figure 3. Cloud Security Environment

Security of Data: [6] Data Transmission. It is apparent that the evidence communication is made in the supervision of scattered computing. The data Security broadcasting would be a distinctive delinquent not individually in the surroundings which are not based over the cloud, in all the circumstance in combination to the cloud, for upholding the privacy, expediency and manageableness of the data transmission in the system, cryptographical tactics, for example, IPSec, SSL and VPN, are already prepared to join in the system of the cloud. All of the cloud computing systems provide a level of cryptography station connected along with the data. Data separation. For running limited statistics over the cloud clients, subjects like the visible suppression, containerization, along with education names are regularly utilized to distinct totally exceptional client info (tenure) and preparation of data, in accordance to the axis, subsequent: defense and the security information of the customers. Data distributing. The remainder of the data of the customers in the cloud, such as rounds deprived to the data erase tool which does increase the breaking of the receptive data. The output of which deletion of the data inside the cloud environment is important besides it means will be accomplished. Since the starting, remove the customer's data over the media, for example, rounds in a tremendous cloud data center, once consumers get the possibility to eliminate them, in adding to that, the review must focus at these plates, to approve data on the cloud gets removed. Last but not the least, the distributed support, such as the plates at the particular level, should get reorganized also be reused, so that if there would be a presence of plate in between of this data can't get removed, others will be overwhelmed.

3. Health Data Analysis Over the Cloud Security [15]

Cloud security standards in healthcare

The moral, lawful and methodological provision of the accessible investigation is grounded over the international standards for e-health substructure recognized by the International Organization for Standardization (ISO) and Health Level 7 (HL7)

consortium. ISO 27000 family of standards (ISO 27001 through ISO 27006) addressing general information security, ISO 27799 (Information security management in healthcare using ISO/IEC 27002) and ISO 18308 (Health Informatics requirements for an electronic health record architecture) are identified as main standards in the area of healthcare security. ISO 18308 defines security and privacy issues including communication between systems: authentication as the need of verifying the identity of a person/system that claim to be; authorization as a framework of personal access rights and authorizations role; integrity as the data property to preserve the accuracy and consistency of data regardless of changes made; non-repudiation as the property of data to confirm the integrity and origin of a data item; confidentiality as the data property that indicates the extent to which affected data have not been made available or disclosed to unauthorized individuals, processes or other entities. European Union Agency for Network and Information Security (ENISA) adopts ISO 27001 and ISO 27002 controls for cloud computing offering a security analysis for governmental clouds based on 21 EU countries case studies. Non-profit association Health Level 7 (HL7) developed a series of standards in the area of clinical data communication split into message protocols, conceptual (HL7 RIM), document (HL7 CDA) and application standards (HL7 CCOW) . HL7 Clinical Document Architecture (HL7 CDA) is defined based on exchange XML-Markup document standard for clinical data.

Cloud security requirements in healthcare

Healthcare cloud computing security and privacy risks identified by the authors are authentication and access control, virtualization, mobile access/access via internet, flexibility and changeability of services and service providers. Particularly for public clouds, shared usage of computing resources, outsourced and distributed computing are identified as risks. Cloud Security Alliance has issued the inspection outcome in arrangement of a cloud security coercions to the very top rank in directive of sternness recognizing data fissures, data being lost, accounts being hijacked, and shared technology issues. In a requirements list is build up on a collection of representative research papers used for creation of a security pattern for healthcare hybrid cloud. Authors identify as security requirements for a healthcare electronic system: confidentiality, integrity, availability, non-repudiation, patient privacy, patient consent and authorization. Data transfer from local databases to large data centers involves a series of security challenges in terms of virtualization, accessibility, privacy, confidentiality and loss of data accessed from a third party. Data security in cloud computing analysis with focus on migrating from single cloud to a multi cloud environment done in concluded that data encryption and implementation of secure standards are not sufficient for securing a single cloud. Based on papers results presented above we identify as main requirements for the proposed healthcare hybrid platform in terms of security and privacy the following: availability for assure that data is available when is requested, authentication for person/system identity confirmation, authorization for ensure that data is available only for authorized entities, integrity assures that data is accurate and consistent, confidentiality grant that data is available only for authorized entities and data loss guarantee that data that is stored and processed in the cloud will not be loss.

4. Related Works

A Survey of Cloud Computing Security Challenges, Issues and their Countermeasures (Lokesh B. Bhajantri, Tabassum Mujawar et al. (2019), Cloud computing delivers a resource to accumulate customer's confidential and highly sensitive data over the cloud servers accessible in varied secure platforms. It is very important to realize and also address various security con-cerns present in cloud platform, to keep the user's data private and defend it from any of the illegal access in cloud platform. The most significant characteristic of cloud security is the appropriate authentication, robust encryption method, and preventing the data from the loss. These features should be addressed while occupied by means of all service distribution models along with positioning prototype of cloud. This article explains and discusses about the security problems existing at multiple stages over cloud computing. These cloud security events should be applicable to masses, installed apps along with

the networks. During the application of the security over the statistics, the main future of the framework of the security should contemplate data's storage, in the transfer likewise suggestion for the deletion of the data. The appropriate contact switch framework is required for confirming, the solely effective workers could be accessed by the resources of the cloud. This research article also discusses many problems, provocations and safety needs at every level with the appropriate answers for the mitigation or to dodge them.

Survey on Security Implication for the Downtime of VM in Cloud (Deepika Shekhawat, Dr. Reema Ajmera et al. (2018)) [5] This paper discusses the glitches in the security of the data in cloud environment and their possible resolutions for all the issues related to the security. Other than that, the paper analyzes the finest of the class spreads over the security of the cloud and along with its defense. With the cloud computing procedures along with the valuation of the assembly away grow the stages of the cloud computing for customers along with the statistical deals in the middle of larger number of customers, statistic transmission and volume the harm to the security, the security of the cloud is serious problem to be.

Table 1. Cloud Security Techniques Comparison.

Author	Work Accomplished	Result
Padhy et al. [8]	Defines cloud computing, its security problems and models	As of the complexity of the cloud it is quite tricky to achieve endwise security
Chaoqun et al. [9]	Converse hi-tech methods for security of the data in cloud.	Many problems are needed to be solved in data prevention of cloud.
Yu et al.	Presents threats to cloud environment.	Protects applications of cloud computing for health
Sengupta et al.	Cloud security holistic views	A broader view of the cloud emergency view concerns
Anandaraj et al.	Big data security inside the cloud	Offer leading challenges in cloud services.

5. Application of Cloud and its security benefits

5.1. Blood Bank with AWS Amplify

The application was built using the Android Studio and AWS Amplify Console. The backend was developed in the MySQL and PHP. The application helps the recipient t to find the apt donor for the recipient. The application was developed on the Android Studio which is a very good IDE and the reason for choosing android studio as the IDE is, it provides faster coding, fast emu-lator, Solid testing and feature rich environment. The Android Studio gives user- authentication- gated cryptographical key that needs the storage of the cryptographic key along with the facility providers which is also handler appraisers. The strategies along with the sensors for fingerprint, supervisors are able to register more single or additional fingerprints and utilize these fingerprints so as to solve the devices along with completing many different jobs.

AWS Amplify: AWS Amplify is the service that is provided by the AWS that aids in building an extensible full stack mobile and web applications. By using AWS amplify the apps are easy to start, they are very scalable, and the development of the application is very highly scalable. The applications on AWS amplify can be built for both Android, iSO, along with web, React. UI Components. GraphQL & REST APIs. AWS Amplify is also open source.

Videos with the shared responsibility model where the protection inside cloud are managed with the help of the AWS and the security of the cloud is managed by the user thus keeping the data of the blood bank application user much more secure. The AWS Amplify provides with the following security services [10]:

- Identity and Access Management for Amplify
- Data protection in Amplify.
- Security event logging and monitoring in Amplify.
- Compliance variation in Amplify.
- Infrastructure security in Amplify.

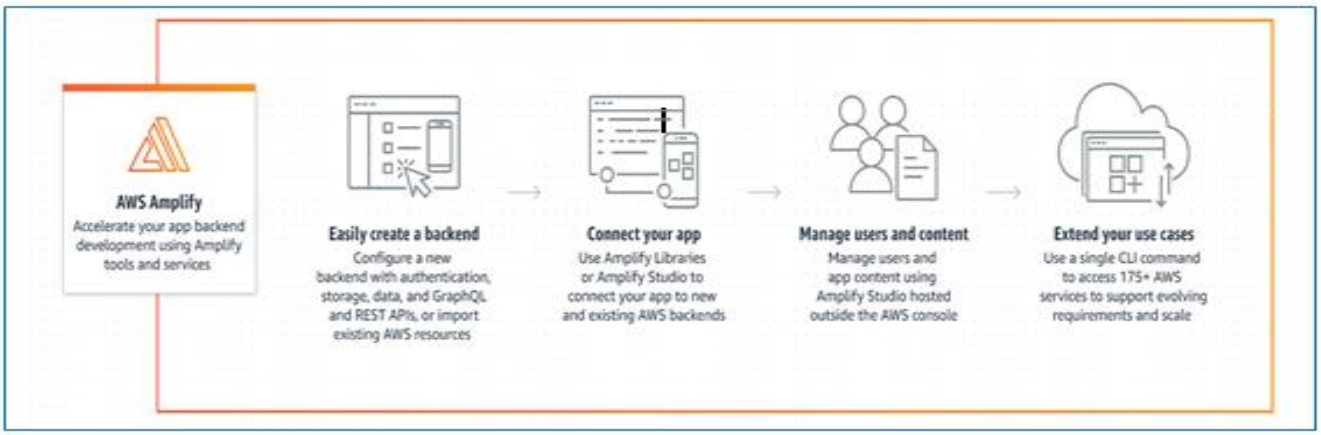

Figure 3. Creating Backend using AWS Amplify

While making the application following steps to be followed in order to develop and deploy the applications with all the tools used:

Create an Application Over the Android: The App was developed from android studio IDE, data and the entries of the application was collected in the database using the mySQL and PHP.

Initialize AWS Amplify: The first step to add the AWS Amplify service to the Application is to install the same. The amplify is distributed in the form of Apache Maven packages. The following code will be added to the Gradle Script, build.gradle(Module:Blood_Bank.app) and sync the Gradle.

```
android {
    compileOptions {
        // Support for Java 8 features
        coreLibraryDesugaringEnabled true
        sourceCompatibility JavaVersion.VERSION_1_8
        targetCompatibility JavaVersion.VERSION_1_8
    }
}

dependencies {
    // Amplify core dependency
    implementation 'com.amplifyframework:core:2.6.0'

    // Support for Java 8 features
    coreLibraryDesugaring 'com.android.tools:desugar_jdk_libs:1.1.5'
}
```

Figure 4. Gradle Script for adding required AWS Amplify Resources

As the Gradle build is synced you will see BUILD SUCCESSFUL. After that, to start provisioning resources in the backend, change directories to your project directory and run amplify into it. Next, we configure the AndroidManifest.xml as follows:

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    package="com.example.MyAmplifyApp">

    <!-- Add the android:name attribute to the application node -->
    <application
        android:name=".MyAmplifyApp"
        ...
    </application>
</manifest>
```

Figure 5. Android Manifest

Next, build and run the application. In logcat, you'll see a log line indicating success:
com.example.MyAmplifyApp I/MyAmplifyApp: Initialized Amplify

- the Verification
- the API and the Record
- the Storage

By following steps mentioned above steps we can simply develop an application and deploy it over the AWS Cloud.

5.2. Drawbacks of using AWS Amplify

Using AWS Amplify for application development process is well opiniated but There are still some scenarios where you shouldn't use Amplify: Non-AWS or multi-cloud projects: AWS Amplify can only target the AWS cloud platform. Non-fullstack projects: if you creating pure front-end or back-end projects, Amplify might not be the most effective choice.

6. Application of Cloud and its security benefits

One major issue is the risk of data being unavailable to be accessed by the different group of same organization causing silos of data, as data may be spread between numerous stages and sites. This would cause difficulty to hold up and study incident data, leading to probable slits in the safety and the risk management of the data. A lot of the security team's struggle to date has remained fixated on cloud safety and detection, as it is demonstrated by the extensive acceptance of Cloud Security Posture Management (CSPM) and Cloud Workload Protection Platforms (CWPP). Nevertheless, whenever it comes to examination and answers, there has been a huge gap. Once anything corrupt is recognized, establishments often don't have the skills and capabilities to rapidly comprehend the true possibility and main reason of the incident. As cloud defense and detec-

tion skills are becoming commoditized, many more establishments will go ahead to develop their post-discovery competences in the cloud, also including the forensics and the incident response.

7. Conclusion

In this paper we have tried to see how cloud security and cloud elements does have helped the developers with the application development. [11] The paper also discusses the benefits of using clouds, its security features and how it can be helpful for the business to shift to the cloud infrastructure. This paper proves this the cloud provides a way so as to store the sensitive data of the users in the protected environment. The significant characteristics of cloud security embrace appropriate authentication, robust encryption methods and the deterrence of data being lost. The paper puts a highlight on various of the security concerns present in the various cloud environments. The paper discourses numerous problems, challenges and security necessities for each and every level among the applicable answers to alleviate or sidestep them.

Acknowledgement

I want to convey my profound and genuine gratefulness towards my guide Prof. (Dr.) Syed Wajahat Abbas Rizvi, for providing the opportunity so as to carry out the exploring, providing and researching valuable direction during working over this re-search. His vision, vitality and serenity has encouraged me, he has inspired and trained me with the methodologies to carry out the research and helping me to show this research work as evidently as possible. It has been a huge pride and honor to work and study underneath his supervision. I am tremendously thankful for all his help and guidance throughout the research.

References

[1]. H. Y. Kang, J. Y. Lee, and S.-Y. Noh, “A case study of cloud computing service models for the general computing environment in a university,” Int. J. Cloud Appl. Comput., vol. 12, no. 1, pp. 1–17, 2022.

[2]. M. Maliyaem, N. M. Tuan, D. Lockhart, and S. Muenthong, “A study of using machine learning in predicting COVID-19 cases,” Cloud Computing and Data Science, pp. 54–61, 2022.

[3]. Cloud computing market size, growth,” Fortunebusinessinsights.com. [Online]. Available: https://www.fortunebusinessinsights.com/cloud-computing-market-102697. [Accessed: 06-Jun-2022].

[4]. D. Ottenheimer and M. Wallace, Securing the virtual environment: How to defend the enterprise against attack, 1st ed. John Wiley & Sons, 2012.

[5]. D. Shekhawat and R. Ajmera, “Survey on Security Implication for the Downtime of VM in Cloud,” in Second World Conference on Smart Trends in Systems, Security and Sustainability, 2018.

[6]. L. B. Bhajantri and T. Mujawar, “A Survey of Cloud Computing Security Challenges, Issues and their Countermeasures,” in Third International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2019.

[7]. Y. Sun, J. Zhang, Y. Xiong, and G. Zhu, “Data Security and Privacy in Cloud Computing,” International Journal of Dis-tributed Sensor Networks, vol. 10, no. 7, 2014.

[8]. K. Hashizume, D. G. Rosado, E. Fernández-Medina, and E. B. Fernandez, “An analysis of security issues for cloud computing,” J. Internet Serv. Appl., vol. 4, no. 1, p. 5, 2013.

[9]. M. Rabi Prasad Padhy and S. C. Ranjan Patra, “Cloud Computing: Security Issues and Research Chal-lenges”,” International Journal of Computer Science and Information Technology & Security, vol. 1, no. 2, pp. 136–146, 2011.

[10]. L. Ronaldo and R. D. Krutz, “Cloud Security A Comprehensive Guide to Secure Cloud Computing”,” Wiley India, pp. 147–148, 2010.

[11]. S. W. A. Rizvi and R. A. Khan, “Improving Software Requirements through Formal Methods,” International Journal of Information and Computation Technology, vol. 3, no. 11, pp. 1217–1223, 2013.

[12]. H. Parveen, A. Syed Wajahat, and P. Shukla, “Disease Risk Level Prediction using Ensemble Classifiers: An Algorithmic Analysis,” in IEEE Xplore INSPEC Accession Number: 21662591, 12th International Conference on Cloud Computing, 2022, pp. 585–590.

[13]. Amazon.com. [Online]. Available: https://docs.aws.amazon.com/amplify/latest/userguide/security.html. [Accessed: 06-Jun-2022].

[14]. R. Charanya , M. Aramudhan , K. Mohan, S. Nithya, ”Levels of Security Issues in Cloud Computing,” *In International Journal of Engineering and Technology (IJET)* ,vol. 5, no. 2, pp. 1912-1920, 2013.

[15]. P. R. Kumar, P. H. Raj, and P. Jelciana, “Exploring data security issues and solutions in cloud computing,” Procedia Comput. Sci., vol. 125, pp. 691–697, 2018.

[16]. Y. S. Lee, N. Bruce, T. Non, E. Alasaarela, and H. Lee, “Hybrid cloud service based healthcare solutions,” in 2015 IEEE 29th International Conference on Advanced Information Networking and Applications Workshops, 2015.

[17]. R. Marcu and D. Popescu, “Security solution for healthcare hybrid cloud platform,” in 2014 18th International Conference on System Theory, Control and Computing (ICSTCC), 2014.

[18]. M. R. Lyu, Handbook of Software Reliability Engineering. Los Alamitos, California: IEEE Computer Society Press, 1996.

[19]. Ritu, K. Solanki, A. Dhankhar, and S. Dalal, “An analysis of software reliability estimation using fuzzy logic function with cocomo ii model,” Int. J. Comput. Sci. Eng., vol. 7, no. 6, pp. 623–626, 2019.

[20]. R. A. Khan, K. Mustafa, and S. I. Ahson, Operation Profile-a key Factor for Reliability Estimation. University Press, 2004.