Journal of Information Systems Engineering and Management
2025, 10(38s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Secure Software Development Lifecycle for Cloud Application

Amitbaha [1]

[1] *Department of Software, National PG College, Lucknow, India. Email: amitabha.engg@yahoo.com*

ARTICLE INFO

Received: 15 Dec 2024

Revised: 18 Feb 2025

Accepted: 26 Feb 2025

ABSTRACT

Cloud Application are Internet based application accessed using web browser or API that is deployed in a cloud environment. They Use Remote servers present in the cloud for storing and processing logics. The paper presents the Life cycle of secure development for cloud. Threat on cloud and challenges are facing in a day to today life. We are living in the era of digital world or we can say on cloud we are started to live, so it is very hard to get know the actual impact on society. Cloud application Vulnerabilities and risk are included in this paper.

Keywords: Cloud, Security, Application.

INTRODUCTION

Cloud Computing is an on-demand delivery of IT Capabilities where IT infrastructure and applications are provided to subscribers as a pay as you go model service over a network. Cloud Computing provides any service at any time that required on metered based on the network. Let go back to 1999, if some request a resource, lets its developer going to need a computer in order to write a web stack for a couple of different requirements. Developer only needs a requirement of a server, how much memory, CPU Cores etc. Developer went to dell.com or hp.com to configure server for the requirement and setup an order then this server will deliver in within 3 weeks or may be 4 weeks. When he got the server, he unboxes and put it on the network (windows NT) and made it ready to the engineer to work on it. All the process will take about 1 Month to start the Woking. Now in 2022, 2023, 2024 onwards a cloud engineer or developer need a resource with number of cores and RAM, check on in boxes and hence apply and prove that self service is available for the developer.

Cloud Computing provides many benefits like Economic, Operational, Staffing and security and many more. In security and types of security everything like multifactor factor authentication to encryption, a quantum algorithm so on as become available in cloud. Following security concerns regarding cloud is available:

- Less Investment in security controls
- Better disaster recovery preparedness
- Efficient, Effective, and swift response to security breaches
- Effective patch management and implementation of security updates
- Ability to dynamically scale defensive resource on demand
- Resource aggregation offers better manageability of security system
- Rigorous internal audits and risk assessment procedures

In present time data security is very horrible. There is huge level of security over the cloud. There is possibility that data is more secure than our premises. Many questions come in mind that file or data on cloud in secure or not. What are you doing to secure your data. Is it encrypted or do you have multifactor authentication. No one can provide 100 % security of data on cloud.

BENEFITS OF CLOUD APPS

There is a lot benefit of clous apps which offers simplified operations. It is scalable. It has a grate reduction in cost for all departments especially in operations. It also has a enhanced data sharing because it all managed, buy, cooperation to the operations. It also has APIs to develop news together and can much easier to develop applications. We also have customized Implementations. So, I can set the service, can use single browser, multiple browser, I can have authentication and can have Multifactor authentication. We can do a lot with it. Different types of benefits for cloud apps are shown in the following Fig1.

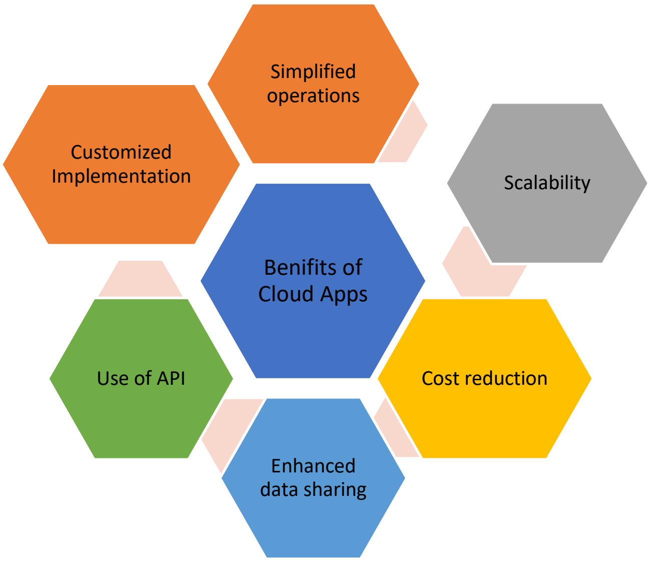


Figure 1. Cloud Apps Benefits

TYPES OF CLOUD APPLICATIONS

In a day today life we all are using different types of cloud applications. You tube, Facebook, disney plus, Netflix man and many more we are using every time from everywhere but as a cloud user you need to know how to secure all these types of apps. Some of the apps like File converting and storing apps, Data retentation and recovery apps, Ecommerce apps, Antivirus apps, Business apps. Image and video making and editing apps, social media apps, educational apps and Entertainment apps and so on as shown in the fig: 2 of categorization of cloud application.

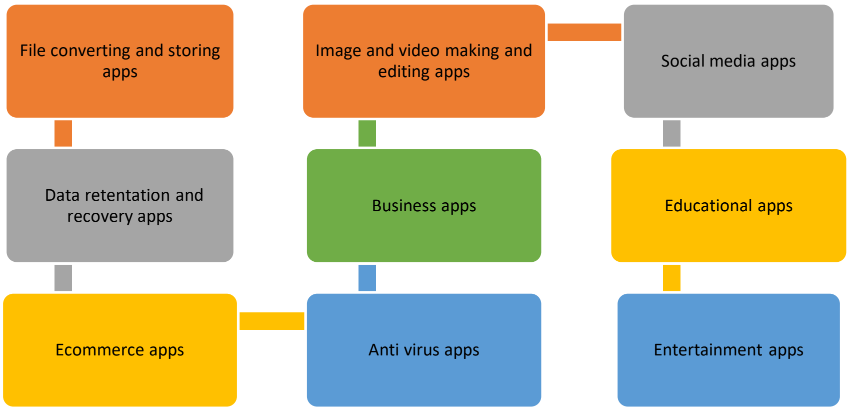

File converting and storing apps
Image and video making and editing apps
Social media apps
Data retentation and recovery apps
Business apps
Educational apps
Ecommerce apps
Anti virus apps
Entertainment apps

Figure 2. Categorization of Cloud Applications

SECURITY BENEFITS OF CLOUD APPLICATIONS

In the development era changes and progress in the processes, pattern and technologies of cloud application development require changes to the existing standard application security. The following are the security benefits:

High baseline security: The third party provides of cloud take the responsibility to provide high baseline security and follow security requirements to meet regulatory and compliance baselines.

Responsiveness: It has nice APIs and allow Automations in very responsive control, can change firewalls, deploy firewalls, can update code very quickly.

Isolated environment: It has a cloud virtual network and its hyper-segregated environment that prevents attacks from using a compromised application to attack control and reduces the attack surface of individual virtual machine.

Independent virtual machine: In this benefit use of microservice architecture enables deploying more smaller virtual machine which helps implement granular security control and reduces the attack surface of individual virtual machines.

Elasticity: Use of auto scale groups or elasticity tool helps dynamic launching of production system based on baseline image. These immutable servers disable remote administration.

DevOps: this is the methodology that focuses on automation of application development and deployment enhances security operations by improving code hardening, change management, and production application security.

Unified management interface and APIs for infrastructure and application services provides full stack visibility and better management.

THREATS IN CLOUD APPLICATION SECURITY

There have been several breaches of security in cloud. One thing that come to mind that if some one deals with security all the time, then there will be more security breaches in cloud. The point is the level of security benefits that we have is the Application Layer. Application layer is the highest layer of the IaaS, PaaS, and SaaS cloud service models.

Application security begins with early design and threat 6220delling to defend attacks against production applications. There are so many security threats to an application and some of the issues are highlighted below:

a. The distributed and complex nature of applications requires fragmented security approaches.

b. The increased attack volumes and the attack vector easily bypass existing security controls.

c. Unmitigated application vulnerabilities are a major risk for production applications

d. No visibility into runtime security events.

There are many different threats and solutions to all these threats. We need to configure each one very carefully as shown in the table 1.

Table 1. security threats and challenges

Threat/ Challenges	Solution
Incorrect/Appropriate application setup	Logging, network segmentation, audit
Unauthorized access to applications	Access controls, prioritizing initiative, business partnerships
Insecure APIs and Interfaces	Authentication, access control, encryption, activity monitoring

Account Hijacking	Authentication, MFA, restrict the IP addresses allowed to access application in cloud.
Application Vulnerabilities	Web application Firewalls
Bad bots	IP reputation and signature database
Application Layer DDoS Attacks	Application delivery control tools for load balancing
Data breaches	Data recovery plan in place, review the vendor's backup procedures.

SECURITY CHALLENGES IN CLOUD APPLICATION

Cloud application security is prone to change because of shared security model, cloud governance and operations. Increased Application Scope is the management plane security which is of prime importance for cloud security applications. Insecure management plane can expose sensitive data or information. Changing Threat models for Cloud application threat model need to consider the responsibility of cloud provider's shared security model as well as operational and incident plans. Reduced Transparency of Cloud applications are integrated with external services which reduces its transparency.

RESPONSIBILITY ACROSS CLOUD SERVICE MODELS

In cloud computing three most popular deployment models are present including Public Cloud which opens cloud services to the public and the services can be used by anyone. Private Cloud is used by single organization that intends not to share the information with anyone and Hybrid Cloud is a combination of both public and private clouds where private applications/data are places within the orgainzation's networking a private cloud while other services can be placed outside the orgainzation's network in a public cloud. Cloud security application responsibility for various cloud service models is depicted in the table II.:

Table 2. Responsibility for Cloud Service Models

Software as a Service (SaaS)	Cloud provider supplies software applications and hardware for running the application
	Application security is managed by cloud provider
	Example: Google apps, Dropbox, Cisco WebEx, Salesforce etc.
Infrastructure as a Service (IaaS)	Cloud Provider offers infrastructure such as servers, storage, network and virtualization via private or public cloud to manage applications, OS and middleware.
	Application security is the responsibility of the customer or user
	Example: Windows AZURE, AWS Elastic Beanstalk, Heroku, Google App Engine, OpenShift, Apache Stratos.
Platform as a Service (PaaS)	Cloud provider offer a platform for customer to develop, run, and manage applications without having to build and maintain the infrastructure.
	Application security is the responsibility of the customer
	Example: AWS, Microsoft Azure, Google compute engine.

CLOUD APPLICATION VULNERABILITIES AND RISK

Cloud as name suggested applications are kept at some remote area and user is trying to access them. Now a days huge amount of data is handled by the cloud only Pay-as-You-Go model with a minimum finance. But as data is increasing Vulnerabilities and risks on cloud are also getting compromised. Some of the Vulnerabilities and Risk in Cloud are discussed in the given table 2:

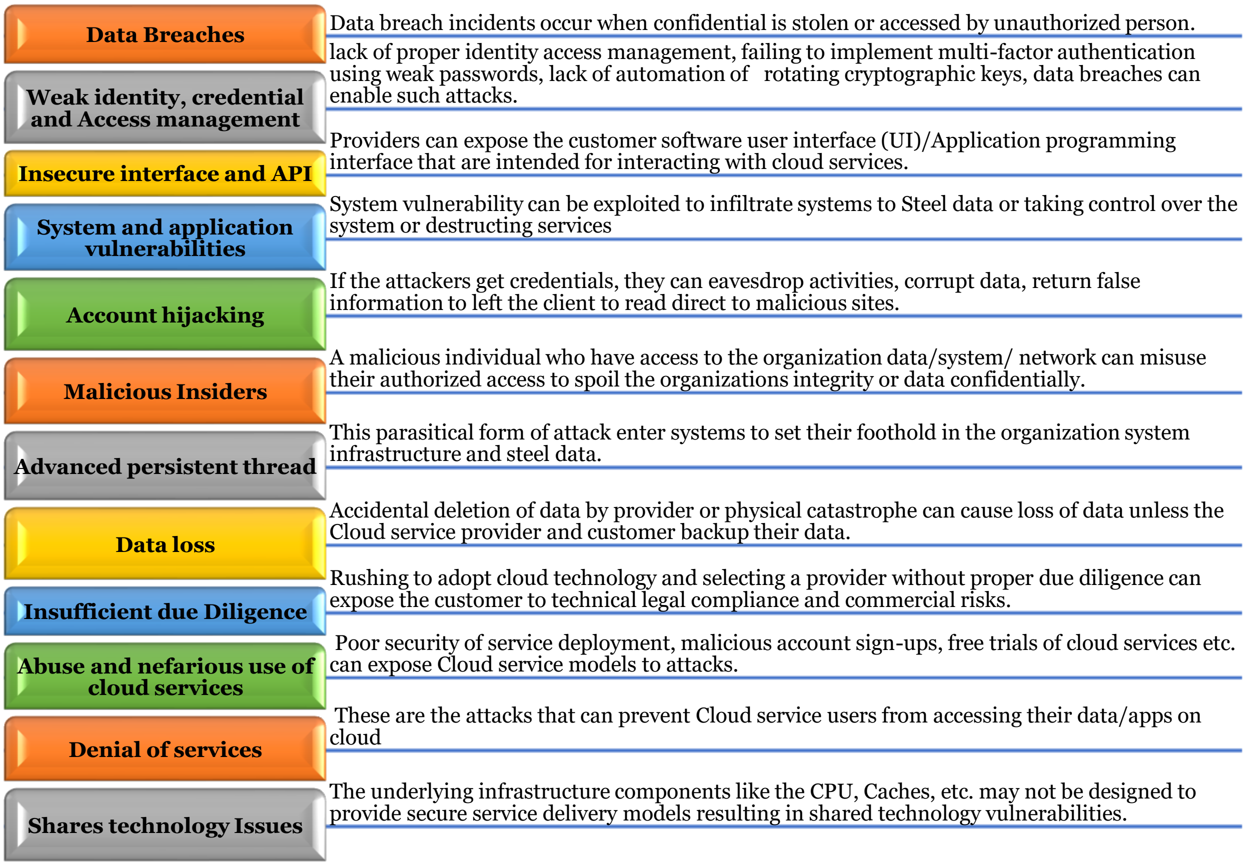
Table 3. Vulnerabilities and Risk in Cloud

Vulnerabilities and Risk	Description
Injection	When untrusted data is sent to an interpreter as part of a command or query, it results in injection flaws, such as SQL, NoSQL, OS and LDAP injection. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
Broken Authentication	Application function related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords keys or sessions token, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.
Sensitive data exposure	Many web applications and APIs do not properly protect sensitive data such as financial, healthcare and Pll. Attacker may steal or modified such weakly protected data to conduct credit card fraud, identity theft or other crime. Sensitive data may be compromised without extra protection such as encryption at rest or in transit and requires special precautions when exchanged with the browser
XML external entities (XEE)	Many older or poorly configured XML processor evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote coat execution, and denial of service attacks
Broken access control	Restriction on what authenticated users are allowed to do our often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data such as access other users' accounts, view sensitive files, modify other users' data, change access rights etc.
Security misconfiguration	Security misconfiguration is the most seen issues. This is commonly a result of insecure default configurations, incomplete or Ad hoc configurations, open cloud storage, misconfigured HTTP headers and verbose error message containing sensitive information. Not only must all operating systems, frameworks, libraries and applications be securely configured, but they must be patched/upgraded in a timely fashion.
Cross-Site Scripting (XSS)	XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping or updates an existing web page with user supplied data using a browser API that can create HTML or JavaScript. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface websites or redirect the users to malicious sites
Insecure deserialization	Insecure deserialization often leads to remove code execution. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attack, injection attacks or privilege escalation attack
Using components with known Vulnerabilities	Components such as libraries firewalls and other software modules run with the same privilege as the application. If a vulnerable component is exploited such as attack can facilitate serious data loss or server takeover. Applications and APIs using

Vulnerabilities and Risk	Description
	components with known vulnerability may undermine applications defenses and enable various attacks and impacts.
Insufficient login and monitoring	Insufficient login and monitoring couple with missing and infective integration with incident response allow attackers to further attack system, maintain persistence, pivot to more systems, and tamper or extract or destroy data. Most breach studies shows time to detect a breach is over 200 days, typically detected by external parties rather than internal process or monitoring

CLOUD SPECIFIC RISKS

Following fig 3 demonstrates the risks which are cloud specific:



Data Breaches	Data breach incidents occur when confidential is stolen or accessed by unauthorized person.
Weak identity, credential and Access management	lack of proper identity access management, failing to implement multi-factor authentication using weak passwords, lack of automation of rotating cryptographic keys, data breaches can enable such attacks.
Insecure interface and API	Providers can expose the customer software user interface (UI)/Application programming interface that are intended for interacting with cloud services.
System and application vulnerabilities	System vulnerability can be exploited to infiltrate systems to Steel data or taking control over the system or destructing services
Account hijacking	If the attackers get credentials, they can eavesdrop activities, corrupt data, return false information to left the client to read direct to malicious sites.
Malicious Insiders	A malicious individual who have access to the organization data/system/ network can misuse their authorized access to spoil the organizations integrity or data confidentially.
Advanced persistent thread	This parasitical form of attack enter systems to set their foothold in the organization system infrastructure and steel data.
Data loss	Accidental deletion of data by provider or physical catastrophe can cause loss of data unless the Cloud service provider and customer backup their data.
Insufficient due Diligence	Rushing to adopt cloud technology and selecting a provider without proper due diligence can expose the customer to technical legal compliance and commercial risks.
Abuse and nefarious use of cloud services	Poor security of service deployment, malicious account sign-ups, free trials of cloud services etc. can expose Cloud service models to attacks.
Denial of services	These are the attacks that can prevent Cloud service users from accessing their data/apps on cloud
Shares technology Issues	The underlying infrastructure components like the CPU, Caches, etc. may not be designed to provide secure service delivery models resulting in shared technology vulnerabilities.

Figure 3.

SCOPE OF CLOUD APPLICATION SECURITY

People with different skill sets and roles are required to develop an effectively secure cloud application. SSDLC (Secure Software Development Lifecycle): How cloud applications are secured from design to development. Design and Architecture: Methods to design cloud applications that can enhance their security. DevOps and continuous Integration/Continuous Deployment (CI/CD) is understand the model for the development and deployment of cloud applications which includes security controls to enhance cloud application security.

SECURE DESIGN DEVELOPMENT LIFECYCLE

It describes the steps of security activities to be followed during the development, deployment, and operations phase of cloud applications. Abstraction and automation of cloud computing impact all the phases of SSDLC as shown in Fig 4.

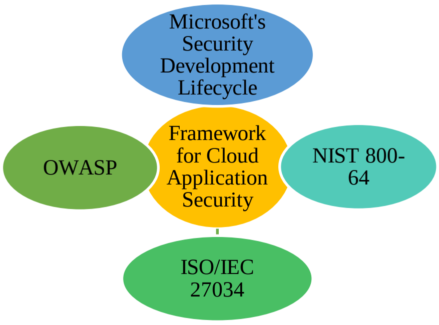

Microsoft's Security Development Lifecycle
OWASP
Framework for Cloud Application Security
NIST 800-64
ISO/IEC 27034

Figure 4. SDDLC for cloud Security

Secure design and Development Standards for training, writing and testing code are required. Secure development Activities for security and testing application while moving them from development to production environment. Secure Operation and Implementing Web application firewalls and vulnerability assessment tools for securing and maintaining applications running in production environment. Involves designing, developing, and testing a high-quality, secured cloud software. Security is built into applications during the entire software/ application development life cycle. Developers need to understand the cloud platform on which the application are executed. The following fig 4 is the Secure software development life cycle stages.

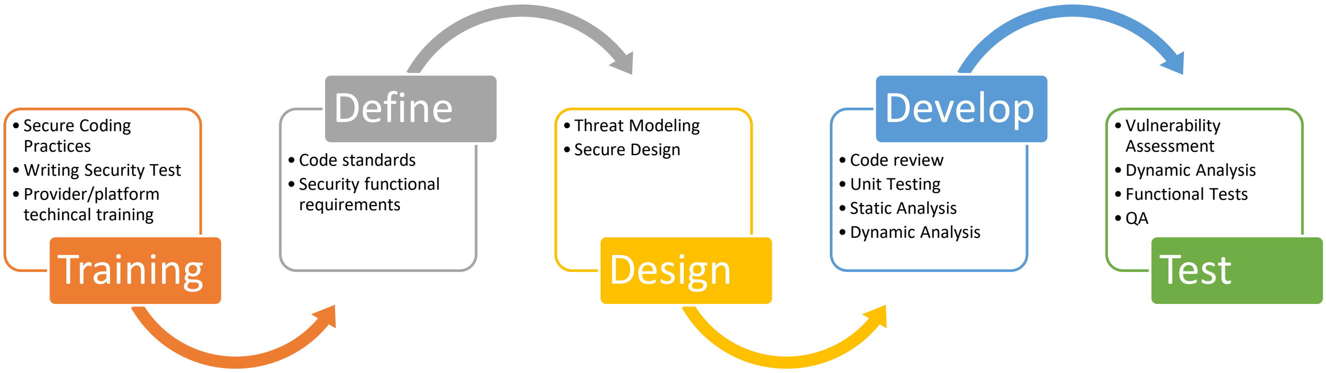


Figure 5. Secure software development life cycle stages

Training is the first phase where the tools, frameworks, the methodologies are used by teams, they all need to be well trained. Define is the second phase where coding standards and functional requirements are defined. This is going to be management/engineering level. Then threat modeling and secure design is done at the design phase. Design phase identify the threats and then design the model against the identified threats. At the develop phase design is going to be developed as functions, code review, unit testing and analysis. As we developing the app, developing functions, sections of the applications we have code review, we look at the various units of the app and test those units. We do statics and dynamic analysis. Static analysis we take executable without running and in dynamic analysis app is executed in a running environment. The last phase is test phase. In this app is going to be tested with includes Vulnerability Assessment, Dynamic Analysis, Functional Tests and QA.

CONCLUSION

The paper presents a brief overview of cloud computing. It is an upcoming technology for sharing resources with the use of Internet. The paper includes the benefits of the cloud technology. Due to the lack of privacy and security is the main obstacle in the broad adaptation of cloud computing. Types of Cloud Applications are explained in the paper. Different types of benefits and threat involved in cloud applications are discussed and covered. The paper demonstrates the Security Challenges in Cloud Application very well. Responsibility across cloud service Models and Cloud application Vulnerabilities and risk are discussed. The paper focuses on Cloud Specific Risks and what are the scopes of application on cloud security. The paper presents the Secure Design Development Lifecycle (SSDLA) along with different types of models and Stages of cloud computing security.

REFRENCES

[1] R. Böhme, M. Brenner, T. Moore, and M. Smith, “High-Speed Fully Homomorphic Encryption Over the Integers,” Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 8438, no. May, 2014, doi: 10.1007/978-3-662-44774-1.

[2] Z. Brakerski and V. Vaikuntanathan, “Fully homomorphic encryption from ring-LWE and security for key dependent messages,” Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 6841 LNCS, pp. 505–524, 2011, doi: 10.1007/978-3-642-22792-9_29.

[3] Ko RKL, Jagadpramana P, Mowbray M, Pearson S, Kirchberg M, Liang Q, Lee BS. TrustCloud: A framework for accountability and trust in cloud computing. IEEE World Congress on Services (SERVICES); 584-588

[4] Seiger R, Groß S, Schill A. SecCSIE: a secure cloud storage integrator for enterprises. IEEE 13th Conference on Commerce and Enterprise Computing (CEC); 252-255.

[5] L. Wei, H. Zhu, Z. Cao, X. Dong, W. Jia, Y. Chen, A.V. Vasilakos, Security and privacy for storage and computation in cloud computing, Inform. Sci. 258 (2014) 371–386.

[6] Q. Liu, G. Wang, J. Wu, Time-based proxy re-encryption scheme for secure data sharing in a cloud environment, Inform. Sci. 258 (2014) 355–370.

[7] Z. Tari, Security and privacy in cloud computing, IEEE Cloud Comput. 1 (1) (2014) 54–57.

[8] Neelima S, Lakshmi Y. A review on distributed cloud intrusion detection system. Int J Adv Technol Eng Res (IJATER) 2013.

[9] Baumann A, Peinado M, Hunt G. (microsoft research) Shielding applications from an untrusted cloud with Haven. ACM Trans Comput Syst August 2015;33(3):26. http://dx.doi.org/10.1145/2799647.Article 8

[10] S. Sridhar, A. Hahn and M. Govindarasu (2012). Cyber–Physical System Security for the Electric Power Grid, Proceedings of the IEEE, 100(1), pp. 210-224.

[11] F. S. Tsai and K. L. Chan (2007). Detecting Cyber Security Threats in Weblogs Using Probabilistic Models, Intelligence and Security Informatics. PAISI, pp. 46-57.

[12] R Zhu, L Liu, H Song et al. (2020). Multi-access edge computing enabled internet of things: advances and novel applications, Neural computing and Applications, pp. 15313–15316.

[13] R. Kondra, S. K. Bharti, S. K. Mishra, ”Honeypotbased intrusion detection system: A performance analysis,”, 3rd Int. Conf. on Computing for Sustainable Global Development (INDIACom), 2016, pp. 2347-2351

[14] Paul Stone Brown Macheso, Angel G Meela, “IoT Based Patient Health Monitoring using ESP8266 and Arduino”, International Journal Of Computer Communication And Informatics, vol.-3, issue- 2, 75-83, 2021

[15] S. A. Ahmad and A. B. Garko, "Hybrid cryptography algorithms in cloud computing: A review," in 2019 15th International Conference on Electronics, Computer and Computation (ICECCO). IEEE, 2019, pp. 1–6.

[16] Y. Yang, S. Tu, R. H. Ali, H. Alasmary, M. Waqas, and M. N. Amjad, "Intrusion detection based on bidirectional long short-term memory with attention mechanism," CMC – Computer Material and Continua, vol. 74, no. 1, pp. 1597–1632, 2022.

[17] I. Ul Hassan, R. H. Ali, Z. Ul Abideen, T. A. Khan, and R. Kouatly, "Significance of machine learning for detection of malicious websites on an unbalanced dataset," Digital, vol. 2, no. 4, pp. 501–519, 2022.

[18] Nawaz Brohi S, Adib Bamiah M, Nawaz Brohi M, Kamran R. Identifying and analyzing security threats to virtualized cloud computing infrastructures, In Proceedings of 2012 international of cloud computing, technologies, applications and management

[19] Kretzschmar, Mario Golling, Sebastian Hanigk, Bassam S. Farroha and Deborah L. Farroha, "Security Management Areas in the Inter-Cloud", published in 2011 IEEE, 4th International Conference on Cloud Computing, Cyber Security Components for Pervasive Enterprise Security Management and the Virtualization Aspects, published in 2010 IEEE , 2010.

[20] P. Sharma, Sandeep K. Sood and Sumeet Kaur, "Security Issues in Cloud Computing", published in Springer-Verlag Berlin Heidelberg , 2011.

[21] J. Surbiryala, Chunlei Li and Chunming Rong, "A Framework for Improving Security in Cloud Computing", the 2nd IEEE International Conference on Cloud Computing and Big Data Analysis, 2017.

[22] A. Verma and S. Kaushal, "Cloud Computing Security Issues and Challenges: A Survey", Proceedings ofAdvances in Computing and Communications.

[23] Daniele Catteddu, Giles Hogben, "Cloud Computing: Benefits, Risks and Recommendations for InformationSecurity", European Network and InformationSecurity Agency (ENISA),