IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Study Of Security Threats in Cloud Computing and it's Protection.

Chetan Vijaykumar Dalave[1]

Anushka Alok Lodh[2], Tushar Vijaykumar Dalave[3]

[1, 2]*Dept.Of Computer Engineering Savitribai Phule Pune University, RMD Sinhgad College of Engineering Pune, Maharashtra, India.*

[3]*Dept.Of Information Technology Engineering Savitribai Phule Pune University, of Engineering Pune, Maharashtra, India.*

Abstract: Cloud computing is an emerging discipline in today's generation. From texting someone to streaming any video online, we're generating huge amounts of data. It's important to keep this large amount of information safe and secure, and that's where cloud computing comes in. Cloud computing is a growing model that has attracted a lot of researchers in recent times due to its ability to reduce the costs associated with computing. The key issue with cloud computing is cloud security and proper implementation of the cloud over the network. Cloud computing is the only generation that can secure and maintain interesting records with the help of remote cloud provider hosting. In nowadays world, records are increasing daily. The cloud issuer provides its offerings via the internet and makes use of many internet technologies that get up new security problems. In this paper, we are going to analyse cloud computing, demanding situations in cloud computing, Security threats associated with it and protection of those clouds, with the current protection threats in Cloud computing. The paper additionally discusses lots of open research problems related to the cloud safety.

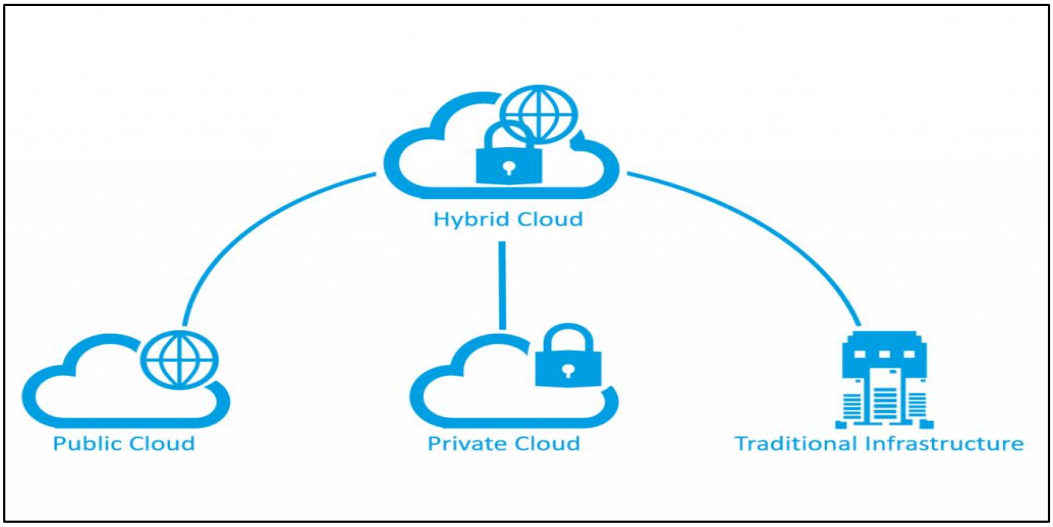
Keywords: **Cloud Computing, Cloud Security threats and Challenges, Protection of cloud.**

I. INTRODUCTION

Everybody is using cloud technology nowadays you don't realize it, for example, if you're using it online. Email sending, watching movies or TV, editing service listening to documents or music and playing and storing games .Cloud computing is behind all these images and other files. The technology that makes it possible basically, a Cloud computing means we're storing and accessing it. Programs and data on the Internet instead of our computers hard drive.

Earlier it was cloud computing but that was all known after cluster and grid computing. Will see about Cluster and grid computing later in this research paper but when cloud providers start selling cloud services to user, then it came the term cloud computing. In the clouds all computing is done using someone else's computing references. These resources are primarily rental services are provided by the cloud service provider. Cloud computing is the biggest business now a today because every little big businesses need space to keep their data with numbers. This is one of the biggest advantages of cloud computing. We do not need to retain our data.

- The different types of cloud are as follows:



1. Public cloud: Public Cloud is the most common and recognizable cloud computing model for its various users and under it services are provided in virtualized environment, and we can call it a standard cloud computing model in which service providers create resources. Such as the application and the store is available to the public.

2. Private cloud: Private cloud means that it is a specific model of cloud computing involves a secure cloud-based environment which specific users can work on. It can happen physically located at the company's onsite data canter. It provides superior security, more control, cost and energy efficiency and more improved reliability.

3. Hybrid cloud: Hybrid Cloud is a private and integrated service. Public so that it can perform different tasks in one go. Organization mostly company and enterprise implement hybrid cloud hosting.

II. LITERATURE SURVEY

Cloud computing activities are mostly those of access to applications, hardware services, platforms, and other services. The main activity, however, is transmitting and receiving data. Cloud computing integrates and interfaces with other applications, services, and applications. The latter is achieved through the use of an application programming interface (API). The service provider must be keen to know all the subscribers who have access to the API data and encrypt any sensitive and confidential data. The encryption process ensures that only the recipient and sender of the data understand the API's encrypted data. It helps maintain the data integrity since those who cannot decrypt the data cannot alter the data stored in the data stores. It also helps keep the sensitive data's confidentiality and make it available only to the known subscribers who are the encrypted data recipients. The commonly used data encryption in cloud computing is Attribute-Based Encryption . This type of encryption helps in solving the issues of secure data storage in cloud computing. It is easily possible to store multiple files through the hierarchical scheme but at the same access level. The hierarchical methods help save the computational cost and the storage space, mainly if the service provider deals with data from prominent institutions and organizations. Cloud computing services can also contain embedded credentials and secrets. Cybercriminals easily crack these secrets. Therefore, the service providers must manage these secrets and credentials, just like the other types of certificates and secrets. Some several procedures and tools can be used in ensuring the protection of the latter. These include passwords, firewalls, the use of packet sniffing tools, rootkit detector, and other tools. The service provider can establish policies and procedures that specify the services' access and how to identify a subscriber, and if they are in the database. The service provider can add on to software that helps the subscribers' authentication, authorization, and accounting managed and verified .This means that they have to prove who they are through the passwords shared with them or an access card and their activities monitored to help in identifying who breached the security of data and the service provider must come up with a way in which specific subscribers are given access to different services depending on their subscription

III. CLOUD COMPUTING ARCHITECTURE

With the help of the internet, we are accessing applications, storage and services that are available in the cloud. Any devices such as laptops, tablets, mobiles, etc. that are connected to internet can access the cloud.

There are cloud service providers who provide to cloud services for customers. Cloud services can be many types depend on user .

IaaS stands for infrastructure as a carrier in this service, most effective provided via hardware and networking cloud carrier. company those sources can be customized consistent with the user call for some agencies that provide IaaS are Amazon internet offerings, IBM, and so on.

PaaS approach platform as a provider in this carrier, the platform Cloud provider is supplied through the issuer which allows the developers to create programs and servers at the internet some of the activities that offer PaaS are Google, home windows, force.com, and so forth.

SaaS stands for Software as a Service. In this service, is an application built on the cloud service provider's platform provided by the provider. The user only has to use the services of some companies that provide SaaS include Facebook, Google, Dropbox etc.

- Cloud computing architecture can be divided in two parts:-

A. Front End:
Front end is the basic meanings we are going through interact with the cloud. One of the front ends is web services communicate with the front end cloud with the help of internet.

B. Back End:
Back end of cloud computing is cloud itself. Backend architecture is the part of cloud computing architecture that powers frontend architecture. It includes the basic components of the system, such as hardware and storage, and is usually located on a server farm in a geographically remote location.

In given figure shows that, we have many components like management which will look after the maintenance of the cloud, storage which will have all the storage of the cloud, service which will provide the service to the user, application which have all the applications which are present on the cloud, security which will look after the security of the cloud.

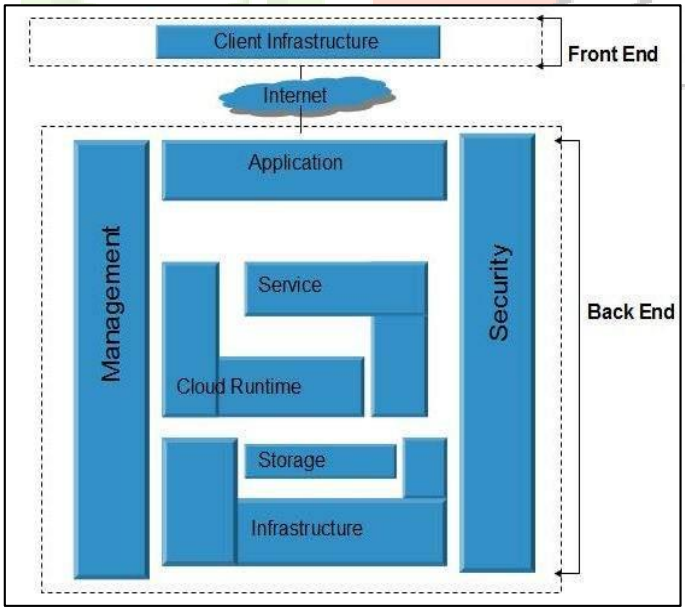


Fig.1: Cloud computing architecture

IV. CHALLENGES IN CLOUD COMPUTING

1. **Security and Privacy:** Security and privacy are the most important missions in cloud computing. It is important to keep interesting and personal data in the cloud secure and confidential. This record is intended for internal use only and is no longer for third party use. The user keeps all kinds of records in the cloud from the least attractive statistics to the most impressive statistics as the user trusts the cloud company and compiles its sensitive statistics on his cloud. Make sure the information on the cloud is comfortable for everyone. Component in this project can be minimized with the help of encrypted file system and statistics loss software program.

2. **Interoperability*:*** Your services must be workable. Interoperability an application that exists on a single platform be able to provide services from other platforms as well as. Suppose you are a service provider and you have created one. The application on Windows and your cloud users are using it an application will be called interoperable when that application Linux will also run on iOS. This challenge can be reduced by using web services because web services run on everyone every platform.

3. **Portability:** Cloud services must be portable means portability can be an application and data running on a cloud platform moved to a new cloud platform whenever needed conflict cloud should be able to transmit data. Another platform and should work in a coordinated manner. Suppose if the person is using a private cloud but now, he wants to go hybrid cloud, so if it could, the cloud would be called portable. So with the least contradiction don't confuse cloud computing with portability. Interoperability means having access to all services from all platforms while portability means .Transfer data and applications from one platform to another second when needed.

4. **Quality Service*:*** Every cloud must provide quality service to its customers. Make sure that whenever the customer requests the service, they there is always a standard service. Quality service is highly involved safe and fastest services. The user is never denied service, whatever the condition. All files must be properly encrypted so that you have sensitive information always safe cloud provider must have all backup plans, even for the worst of natural disasters.

V. SECURITY THREATS IN CLOUD COMPUTING

1. **Data Breach*:*** Data can be leaked in any way even if it is an internal person. Unauthorized access to the data centre or by an outsider of the amount of damage depends on the sensitivity of the data. The data may also include some financial information that may be. Resulting in large losses data from big companies like Microsoft centres are so safe that they need footprints. Fingerprints to enter the premises and also a legit reason for entering server room data centres like Microsoft there are also armed guards so that no one tries to enter room.

2. **Data Loss:** The amount of touchy records is increasing day by day on the clouds and these facts ought to wander away in many methods, such as thru herbal calamities like floods, earthquakes, and so forth, accidental deletion, or corruption of data. The cloud now not simplest carries the private data however also carries the statistics of organizations which is a treasured asset for any enterprise this may be decreased by means of retaining lots of backups at information facilities.

3. **Insider Threats:** This is a danger that is very difficult to avoid. This risk includes modifying, deleting, updating or leaking of sensitive data from internal employee. Always a cloud provider makes sure all its employees are trustworthy. This threat can be reduced by checking the background. Employee, giving the employee only the required access and implement automation tools to run all routine tasks.

4. **Data Location:** All cloud data should not be on one location data should be available in different locations with appropriate. Instead, people should not know the data location only high officials.

5. **Account Hijacking*:*** The threat also includes leaking credentials for hijacking. Cloud services and then, they can steal sensitive information, can enter and enter incorrect information. In other people's transactions which may result in legal issues for the user and also to the cloud service provider. The hijacker can access everyone services / information that were previously accessible by authorized user.

6. **Insecure Application Programming Interfaces:** Hackers and application programming interface developers have control over cloud services APIs which user use should not be weak. APIs do monitoring; provisioning and cloud services management may be the result of weak APIs changing application configuration settings, leaking sensitive data, inactive servers, etc. This risk can be reduced by only by accessing Cloud Services APIs with encrypted keys which API will authenticate the user. Encrypted keys must be stored in a secure hardware device.

7. **Multi Tenancy*:***
   - Intervention: Negative situation created by a tenant the other tenant may be adversely affected.
   - Data isolation - because tenant data is on the same server, so it is possible for a tenant to benefit to access to other tenant data.
   - Managing Dangerous Change - Changing the layout one tenant can affect another tenant.

VI. ALGORITHM USED TO PROTECT CLOUD COMPUTING

Computer network security uses network-level administrative controls and technical measures to protect the privacy, integrity, and availability of data in a network environment. Human factors, natural factors, and accidental factors are the biggest threats to network security. Key issues related to data security include data integrity, data availability, data privacy, privacy, data transparency, transparency and data control where data is located. The service provider must ensure that the provider is secure in their infrastructure and the client's data be safe. There are many users of cloud computing like ordinary users, and businesses that have different motives for moving to the cloud. A how to integrate security and performance cloud providers must have.

- Most three common security algorithm used in cloud computing:

i. **AES algorithm:**
   AES is the advanced encryption standard symmertic encryption technique and that was it created by John Daemon and Vincent Rijmen .It is a strong and secure the encryption algorithm uses AES Encrypted sync key or encrypted key Encrypt and decrypt a message; So this it is necessary to use the same secret key for both sender and receiver.

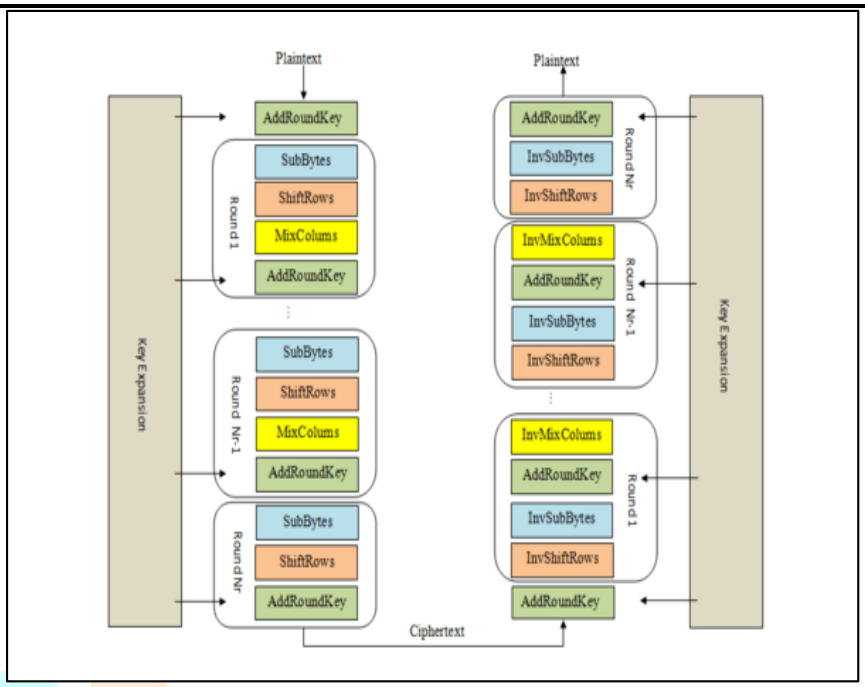


Fig.2: AES Algorithm.

ii. Blowfish algorithm:

Blowfish is an symmetric encryption technique it takes a key size of 32 bits uses 448 bits and the same key for both encryption and decryption. This is ideal it was created to store data developed Bruce Schneier in 1993. That includes 16 round and round consists of one XOR is operation and it has encryption and Key Expansion Techniques.

Blowfish algorithm starts divide plain 64-bit text into two equal blocks the first 32 bits block (L) and the first 32 bits P are subject to bitwise XOR operator. And the result is treated as input cipher function or function count f. This function is used to convert data to a 32 bits block segment with which it is then XOR'ed. The second 32 bits block (R). After placing result of XOR operation, two 32 bits parts (L and R) are exchanged and processed 15 is repeated for repetition.

After the 15th new release, XOR operation with the relaxation of the P array and the cipher feature is calculated. Counting Cipher characteristic is taken into consideration to be the most complex. The part of the set of rules wherein the S-field is used in addition to the powers of the Bluefish set of rules terms of performance, not being patented and certified has made it freely available to be used and numerous additions to edit records the Blowfish set of rules has been further evolved enhance usual performance and make it suitable splendid preferred applications.

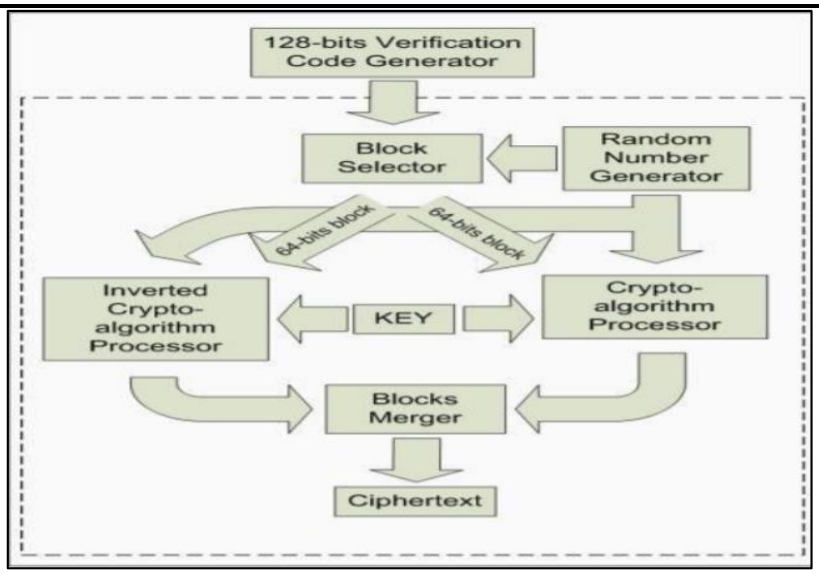


Fig.3: Blowfish Algorithm

iii. RSA algorithm:

RSA Rivest-Shamir-Adleman (RSA) is one Asymmetric encryption techniques and this Created by Ronald Rivest, Adi Shamir and Leonard Adleman in 1977. It uses public key for encryption and private key for decryption, each user has their own encryption and decryption method can be used to encrypt messages without RSA need to exchange secret keys. You can send use an encrypted message and public only. The key to encrypting the message but decrypting it message, you should use a private key.

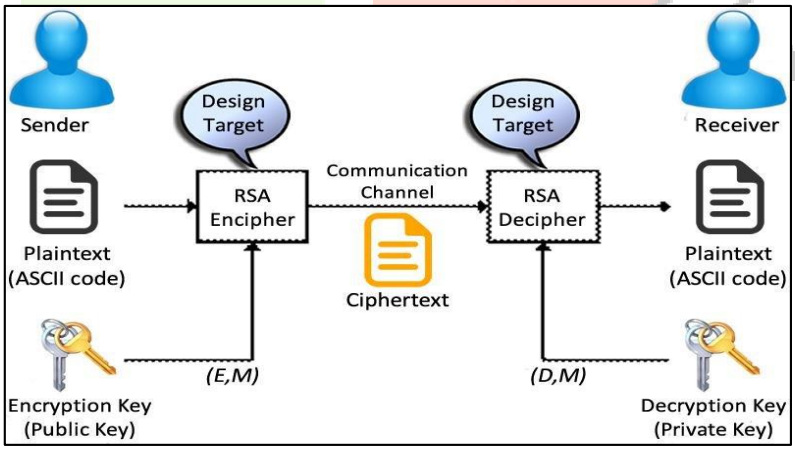


Fig.4: RSA algorithm

Comparison of algorithm:

Table show the advantage of Blowfish over AES and RSA Algorithms in the memory used, the advantages of Blowfish on the entropy values and AES gives the highest value of avalanche effect respectively.

Algorithm	Memory used (KB)	Average entropy per byte of the encryption	Percentage of the avalanche effect
AES	12.7	3.84024	85%
Blowfish	8.93	3.93891	60%
RSA	30.5	3.0958	30%

VII. CONCLUSION

This paper concludes that there's an urgent need for securing the facts present in the cloud. Cloud provider may give their nice in securing and preserving these records; however, nevertheless, there are numerous protection threats in cloud computing that are mentioned in this paper. It also concludes that there's a large responsibility on the cloud carrier to ease this fact. It can be concluded that if the security problems are resolved then the future will be the solutions by cloud for small as well as big firms.

VIII. REFERENCES

[1] B. Nassif, M. A. Talib, Q. Nasir, H. Albadani and F. M. Dakalbab, "Machine Learning for Cloud Security: A Systematic Review," in IEEE Access, vol. 9, pp. 20717-20735, 2021, doi: 10.1109/ACCESS.2021.3054129.

[2] Avijit Mondal, Radha Tamal Goswami, Enhanced Honeypot cryptographic scheme and privacy preservation for an effective prediction in cloud security, Microprocessors and Microsystems, Volume 81, 2021, 103719, ISSN 0141-9331,

[3] C. Esposito, A. De Santis, G. Tortora, H. Chang and K. -K. R. Choo, "Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?," in IEEE Cloud Computing, vol. 5, no. 1, pp. 31-37, Jan./Feb. 2018, doi: 10.1109/MCC.2018.011791712.

[4] Shadi A. Aljawarneh, Ali Alawneh, Reem Jaradat, Cloud security engineering: Early stages of SDLC, Future Generation Computer Systems, Volume 74, 2017, Pages 385-392, ISSN 0167-739X,

[5] J. Aikat et al., "Rethinking Security in the Era of Cloud Computing," in IEEE Security & Privacy, vol. 15, no. 3, pp. 60-69, 2017, doi: 10.1109/MSP.2017.80.

[6] Ashish Singh, Kakali Chatterjee, Cloud security issues and challenges: A survey, Journal of Network and Computer Applications, Volume 79, 2017, Pages 88-115, ISSN 1084-8045,

[7] X. Li, Q. Wang, X. Lan, X. Chen, N. Zhang and D. Chen, "Enhancing Cloud-Based IoT Security Through Trustworthy Cloud Service: An Integration of Security and Reputation Approach," in IEEE Access, vol. 7, pp. 9368-9383, 2019, doi: 10.1109/ACCESS.2018.2890432.

[8] Al-Issa, Y., Ottom, M. A., & Tamrawi, A. (2019). eHealth Cloud Security Challenges: A Survey. Journal of Healthcare Engineering, 2019, 1–15. doi:10.1155/2019/7516035

[9] Radu Sion and Yinqian Zhang. 2020. CCSW'20: 2020 Cloud Computing Security Workshop. Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security. Association for Computing Machinery, New York, NY, USA, 2133–2134. DOI:https://doi.org/10.1145/3372297.3416242

[10] D. Gonzales, J. M. Kaplan, E. Saltzman, Z. Winkelman and D. Woods, "Cloud-Trust—a Security Assessment Model for Infrastructure as a Service (IaaS) Clouds," in IEEE Transactions on Cloud Computing, vol. 5, no. 3, pp. 523-536, 1 July-Sept. 2017, doi: 10.1109/TCC.2015.2415794.

[11] J. Luna, A. Taha, R. Trapero and N. Suri, "Quantitative Reasoning about Cloud Security Using Service Level Agreements," in IEEE Transactions on Cloud Computing, vol. 5, no. 3, pp. 457-471, 1 July-Sept. 2017, doi: 10.1109/TCC.2015.2469659.

[12] R. Herardian, "The Soft Underbelly of Cloud Security," in IEEE Security & Privacy, vol. 17, no. 3, pp. 90-93, May-June 2019, doi: 10.1109/MSEC.2019.2904112.

[13] Rakesh Kumar, Rinkaj Goyal, On cloud security requirements, threats, vulnerabilities and countermeasures: A survey, Computer Science Review, Volume 33, 2019, Pages 1-48, ISSN 1574-0137,

[14] Talal Halabi, Martine Bellaiche, A broker-based framework for standardization and management of Cloud Security-SLAs, Computers & Security, Volume 75, 2018, Pages 59-71, ISSN 0167-4048,

[15] Vijayakumar, V., Priyan, M.K., Ushadevi, G. *et al.* E-Health Cloud Security Using Timing Enabled Proxy Re-Encryption. *Mobile Netw Appl* **24,** 1034–1045 (2019).

[16] P. S. Negi, A. Garg and R. Lal, "Intrusion Detection and Prevention using Honeypot Network for Cloud Security," 2020 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence), 2020, pp. 129-132, doi: 10.1109/Confluence47617.2020.9057961.

[17] M. Alruwaythi and K. E. Nygard, "Fuzzy Logic Approach Based on User behavior Trust in Cloud Security," 2019 IEEE International Conference on Electro Information Technology (EIT), 2019, pp. 1-6, doi: 10.1109/EIT.2019.8834173.

[18] Agnieszka Jakóbik, Stackelberg game modeling of cloud security defending strategy in the case of information leaks and corruption, Simulation Modelling Practice and Theory, Volume 103, 2020,102071, ISSN 1569-190X.

[19] Abirami, P., Bhanu, S.V. Enhancing cloud security using crypto-deep neural network for privacy preservation in trusted environment. Soft Comput 24, 18927–18936 (2020).

[20] Nagarajan Susila, Anand Sruthi, Sakthivel Usha, C hapter Ten - Impact of cloud security in digital twin, Editor(s): Pethuru Raj, Preetha Evangeline, Advances in Computers, Elsevier, Volume 117, Issue 1, 2020, Pages 247-263, ISSN0065-2458, ISBN 9780128187562.

[21] J. Aikat et al., "Rethinking Security in the Era of Cloud Computing," in IEEE Security & Privacy, vol. 15, no. 3, pp. 60-69, 2017, doi: 10.1109/MSP.2017.80.