PAGES:59-66
3/27/24
JOURNAL OF SCIENTIFIC RESEARCH AND TECHNOLOGY(JSRT) VOLUME-2 ISSUE-3 MARCH
Registered under MSME Government of India ISSN: 2583-8660

Cloud Computing And Security Issues In The Cloud

Mr, Anandappa[1], Mrs. Kavita Mudnal[2]

[1]Lecturer, Department of Computer Science and Engineering, Government Polytechnic Raichur, Karnataka, India. anandappa2008@gmail.com
[2]Lecturer, Department of Electronics and Communication, Government Polytechnic Raichur, Karnataka, India. Karnataka, India. kavita.mudnal@gmail.com

ABSTRACT

For future of computing, cloud computing serves as conceptual and infrastructure foundations. There is significant shift in worldwide computer infrastructure toward cloud-based architectures. To take benefit of Cloud Computing, it is vital to deploy it across wide range of industries. However, Security remains primary concern in Cloud Computing environment. There is fresh business paradigm cloud-based technologies because of evolution of cloud services and providers. Because of the widespread use of the internet in many businesses as well as geographically dispersed cloud servers, confidential material of various organizations is typically stored on remote servers and in locations that could potentially be exposed by unwanted parties in cases where those servers are compromised. In the absence of reliable security, cloud computing's flexibility and benefits would be deemed unreliable. Our paper offers a overview of cloud computing ideas and also safety challenges that arise into regards of cloud technology including cloud architecture.

Keywords: Cloud service, computing, computer network, cloud security, security, distributed computing.

1. INTRODUCTION

It's hard to overstate how much recent advances in might computing have impacted both way we compute and how we think about computing resources. Resources in a cloud computing architecture are often located on another party's premises or network and may be accessed by cloud users across a wide area network. Data and other components are sent to a cloud server or infrastructure to process as well as result is delivered after it has been completed. This means that processing occurs remotely. Keeping data on faraway cloud servers may be necessary or at least viable in some circumstances. Following are 3 operationally sensitive situations or eventualities in cloud computing that are of special concern:

- Transfer of sensitive personal information to cloud server
- Data transfer from cloud server to PCs of its users,
- Customers' personal information is stored on cloud-based servers that are external servers that aren’t owned or operated with client.

All three of aforementioned forms of cloud computing is quite vulnerable to security breaches, hence more study and inquiry into cloud computing security is an absolute need. However, the essential premise of cloud computing remains the same — infrastructure or resources stay elsewhere having somebody else's users & ownership 'rent' them for time they utilize infrastructure. There's been number of distinct mixes employed in cloud computing domain. Data saved on external cloud servers may also be included in certain situations. Safe computing techniques have always placed a strong emphasis on security. When it is feasible for any unwelcome party to'sneak' about any personal device through various methods of 'hacking,' the offer of considering a range for accessing somebody's private information via cloud computing ultimately poses additional security problems. Consequently, the reach of cloud computing cannot be eliminated because of its very nature. As a consequence, cloud computing security always has been concern. If you're serious about keeping your cloud computing infrastructure safe and secure, you need to keep an eye out for the latest developments in cloud computing security technology. These four types of clouds are often referred to as

"private," "community," "public," and "hybrid." This article assumes that there is only one form of cloud, public cloud, since this assumption will meet all of requirements for any other sort of cloud. Because of its diverse possibilities, cloud computing is seen as fifth commodity for joining league of current utilities such as electricity, water, gas, & telecommunications instead of simply other service.

The research given in this article is structured to explore and identify methodology towards cloud computing, & security challenges also apprehensions which should be addressed into implementation of a cloud-based computing organization. Within the framework of this study, debate on technical methods and concepts towards cloud computing, including architectural depiction, was already considered. Following that, security risks implicit in cloud computing strategy were highlighted. The investigation of cloud computing's technical and security challenges has resulted in a conclusive revelation of overall elements of cloud computing. Techniques for addressing the security challenges implicit with cloud computing are many, with various aspects and uses that have been left out of purview. A debate on cloud computing validation has taken place, since it serves as comprehensive foundation for embedding authenticity in framework of cloud security.

2. CLOUD COMPUTING INFRASTRUCTURE

The word "cloud computing" refers to a notion that has grown from the terms "distributed computing" and "grid computing." A hybrid of grid & distributed computing, cloud computing has been dubbed the child of both. The simple definition of cloud computing describes characteristics and circumstances in which whole computing may be done by utilizing someone else's network and wherein sovereignty of soft & hardware resources is held by third parties. In common practice, dispersed nature of resources regarded to constitute the 'cloud' by users is fundamentally as in distributed computing form; whilst this is not obvious or required by definition of cloud computing, it is not always evident to users.

In past years, cloud had grown in 2 significant directions: renting infrastructure in the cloud and renting any individual service in cloud. In contrast to first, latter is exclusively concerned with "soft" goods and services offered by cloud service & infrastructure providers. Cloud computing gave rise to slew of new terms to computing diligence, including SaaS (Software as a Service), IaaS (Infrastructure as a Service) & PaaS (Platform as a Service). It's already been mentioned that phrase "cloud computing" and terminology used to describe various combinations of cloud computing are concepts. It's significant to remember that cloud computing is nothing more than specified type of distributed & grid computing that differs in regarding services, architecture, geographic deployment & dispersion. (Hamlen, Kantarcioglu, Khan, & Thuraisingham,2010; Hashizume et.al-2013; & Westphall et.al2011). An operating system serves as platform for software running on top of it, which is what infrastructure refers to when used in the context of computer networks (Lee, 2012; Singh & jangwal, 2012). There is a hierarchical structure to idea of cloud-based services, which is developed from top to bottom with sequence of PaaS, IaaS, & SaaS. At this level of concept, just amount to which an end user may "borrow" infrastructure and software resources is defined; security and computing style, which are of utmost importance, remain untouched. As a consequence, no matter what flavor, hierarchy, or abstraction level cloud computing takes on (Bisong & Rahman, 2011), security must be taken into account. Cloud computing and virtualization go hand in hand, so it's no surprise that virtualization is here to stay. (Ogigau-Neamtiu, 2012; Buyya et al.,2009; Kim, 2009; Hashizume et.al2013; Atayero & Feyisetan, 2011; Mosher,2011; Zissis & Lekkas, 2012) – PaaS & SaaS are 2 examples of cloud services that benefit from virtualization technology, in which single physical infrastructure provides services or platforms to many cloud users at once. As a result, on top of the already-existing cloud computing security problems and challenges, virtualization technology now adds additional security considerations.

Fig-1 depicts typical cloud computing scenario that involves both cloud consumer as well as cloud service provider.

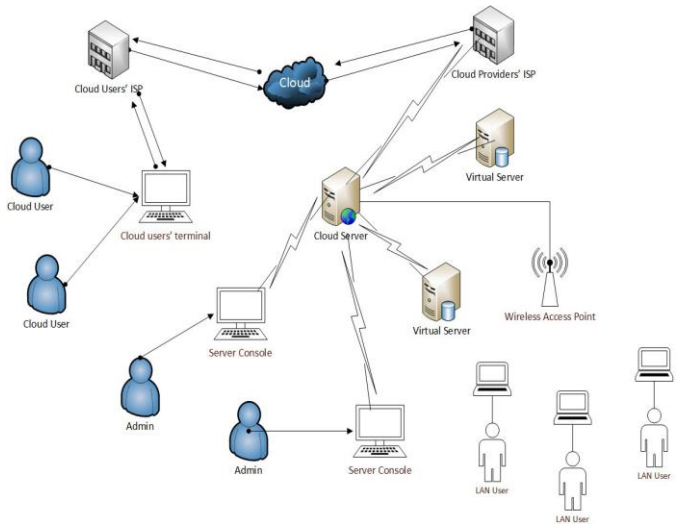

Figure 1: A Typical Cloud Architecture

Figure 1 depicts a simplified cloud computing architecture, omitting some of the more complex aspects of cloud computing (e.g., server replication, redundancy, and geographic dispersion of cloud providers' network) in order to illustrate the arrangement that makes the concept of cloud computing tangible. When seen in conjunction with the description of cloud computing offered previously, network architecture is self-explanatory. Because of their distant locations and methods of remote controlling to cloud servers, administrator consumers who manage cloud servers aren't considered cloud users by cloud service provider's network into scenario, which is an interesting feature of the design. Figure 1's LAN users may or may not be cloud users. Since "cloud computing" is a notion instead of technical terminology, there may be some opportunity for disagreement on the subject. LAN consumers in figure 1 might not have been considered cloud users if cloud computing is defined as servers situated remotely that are accessible over public network (or via cloud). It's important to note that while utilizing cloud services provided by a server, users of local area networks (LANs) are effectively using resources that have been "borrowed" from server and are thus considered cloud users in context of distributed and grid computing, which describe infrastructural approaches to cloud computing.

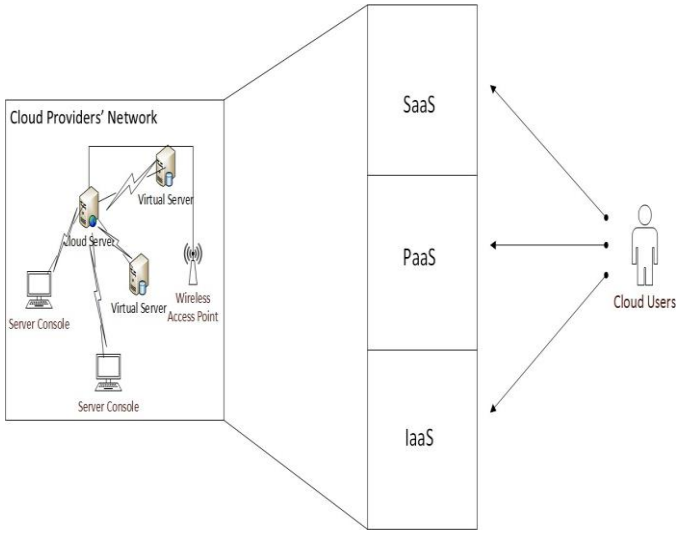

Figure 2: Cloud Service Hierarchy

There are no hidden technical details, arrangements, or administration on cloud service provider's network, as shown in Figure 2. There is no need for a cloud user to be concerned with internal network configuration of cloud service providers, since the service is provided in the form of Saas or PaaS. Whatever causes a disruption, cloud customers will see it as a decrease in service availability or quality, and as a result, the impact and methods for dealing with it are key components of cloud architecture. Security concerns might be motivating element for the disruptions referred to above.

3. AUTHENTICATION IN CLOUD

Because security is so important in every computer environment, it should come as no surprise that cloud is no exception. Identity authentication & management are critical into cloud computing because consumers' sensitive data might be held both at the client's end and on cloud servers (Emam, 2013; Kim & Hong,2012; Yassin, Jin, Susilo, Han & Mu, 2013; Qiang & Zou, Ibrahim, 2012). The cloud's key security challenges include verifying and safeguarding the credentials of qualified users, which might lead to an undiscovered security breach at least for a short time. Figure 3 depicts hypothetical authentication setup for cloud infrastructure.

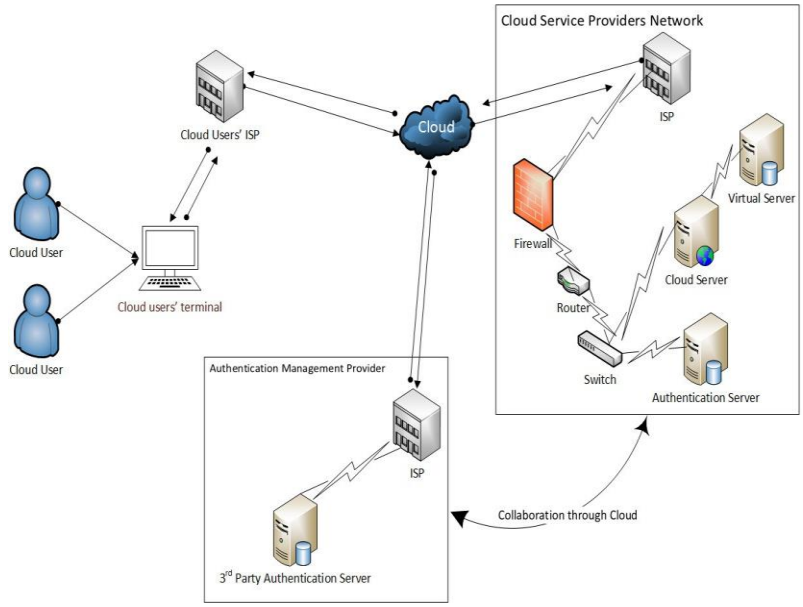

Fig-3:Authentication in the Cloud

Fig3 depicts how cloud users may be authenticated by either cloud service provider or by service provider outsourcing identity managing as well as authenticating services to 3rd party experts. (Miers, Gonzalez, Simplicio, Redigolo, Naslund Pourzandi & Carvalho,2012; Sharma & Mittal, 2013). Cloud service providers are obliged to work together with third-party authentication specialists in latter situation, and this cooperation occurs mostly via cloud throughout authentication process for cloud customers. Due to fact that messages are being exchanged between third-party authenticity board of management as well as cloud service provider, this feature adds both security & performance overheads and risks with cloud context. As previously noted, cloud users are completely unaware of the whole authentication procedure, irrespective presence of 3rd-party authenticity experts. It is assumed that cloud service providers would deploy geographically separated servers, in which case the authentication procedure will be much more difficult in relation to security, core algorithm, and overall performance. Any cloud architecture, no matter how complex, should only introduce third-party authorization and authentication and authorization specialists with one goal in mind, and that is to fortify reliability of confidentiality in concerned area that cloud service provider is also not competent of deploying or offering.

4. SECURITY ISSUES IN CLOUD

It is possible and challenging to use cloud computing concurrently. Cloud computing's route to success is impeded by security concerns, which is seen as a major issue (Ali, Khorshed, & Wasimi,2012). Cloud computing presents a dynamic and wide set of security issues. It's essential that cloud computing data be stored in a secure place (Teneyuca,2011). Location transparency is a major benefit of cloud computing, but it also poses a serious security risk, since it is impossible to enforce local data protection laws without knowing whereas dataset is being stored. Personal data security is main issues for cloud users in cloud computing system (Baker, Joint, & Eccles,2009; King & Raja,2012, Ismail,2011). Cloud service providers' strategic policies are of the utmost importance when it comes to protecting clients' personal or company data (Joint & Baker, 2011). Using cloud services raises issues about security since trust is strongly tied to the legitimacy & legitimacy of cloud service providers (Ryan & Falvy, 2012). The building of trust into cloud computing environment may be key to its success. Providing trust model into cloud computing is vital since this is shared interest area with all stockholders in any particular cloud computing scenario. It is possible that trust in the cloud may be influenced by variety of elements including automated management and human factors, as well as procedures and policies (Martin & Abbadi, 2011). Although cloud computing's security challenges are not directly related to issue of trust, they have significant impact on how people perceive cloud computing. Cloud-based services are vulnerable to same sorts of assaults which affect computer networks and data in transit, including man-in-the-middle attacks, phishing, eavesdropping, sniffing, and other dangers. Attacks like DDoS are a regular but serious threat to cloud computer resources (Dou, Chen & Chen, 2013). The well-known DDoS assault may be an issue for cloud computing, but there is no exception to rule that there is no way to neutralize this. To a larger degree, cloud environment's security will be determined by security of its virtual machines (Mehfuz, Sahoo & Rakhmi 2013; Agarwal & Agarwal, 2011). Safe computing practices include accounting and authentication, as well as encryption, all of which might be seen as posing security risks in the cloud (Ogigau-Neamtiu,2012; Singh & Jangwal,2012; Lee,2012;). Risk and security considerations must be distinguished in this respect. Among the many concerns in cloud-based services that aren't necessarily connected to security, one can be vendor lock-in. On either side, utilizing a certain sort of operating system (for example, open-source vs. proprietary) may bring security threats & issues, which is, indeed, security risk. Other instances of business risks associated with cloud computing include license challenges, service unavailability, and provider business discontinuity, that don't come under technical security concerns. Thus, in the context of cloud computing, a security worry is always some form of risk, however any hazard could not be determined being a security problem arbitrarily. The assignment of tasks amongst parties participating in cloud computing system may result in inconsistencies, which may ultimately lead to a scenario with security risks. The possibility of insider-attack maintains genuine concern for cloud computing, just as it does in every other network environment (Ogigau-Neamtiu, 2012). Most security products or other types of software utilized in a cloud environment may contain security flaws, posing security hazards to cloud infrastructure altogether. 3rd-party APIs, and spammers, pose a danger to cloud environment. (Singh & Jangwal, 2012; Rahman & Bisong 2011;).

Because cloud computing often involves use of public networks and, as a result, exposing the data being sent to outside world, many types of cyber assaults are to be expected. The present modern cloud-based services have been shown to be vulnerable to security gaps that might be malicious activity. Because of the nature of the cloud computing paradigm, both security and privacy are issues that need to be addressed (Bisong & Rahman, 2011). Information security and network security are both at risk because of the way cloud computing is implemented (Qaisar & Khawaja, 2012; Rakhmi, Sahoo & Mehfuz,2013). Third-party relationships, as well as inherent security concerns in infrastructure and virtual machines, might pose a hazard to the cloud environment (Hashizume et al., 2013). Cloud security is constantly complex because of factors such as software faults, social engineering, and human mistakes (Kim, 2009). Detecting intrusions is the most critical part of a network's continuous monitoring. If today's IDSs (Intrusion prevention system) are ineffective, a security compromise in the cloud environment may go unnoticed. (Westphall et.al 2011).

By data, virtual server, including network for operating systems, managing of memory, and concurrency control, there are many ways in which a cloud environment might be harmed by security breaches (Hamlen et al., 2010). Users of the cloud are at risk from database separation and session hijacking. Cloud computing's degree of abstraction and dynamic in scaling provide a concern since they lead to lack of clearly defined

security or infrastructure boundaries. There may be considerable regional variations in privacy and the underlying principle, which might lead to security breaches in cloud services under certain conditions and circumstances (Chen & Zhao, 2012). Cloud servers' security may be breached by many means, including data loss and botnets. In addition, the multi-tenancy model (Ogigau-Neamtiu,2012; & Kuyoro et.al,2011;) must be considered whenever it comes to security. As a single physical server holds multiple customers' data, shared common substrate in regarding physical server or operating system, cloud service providers are likewise concerned about security risks. Data storage security is also intimately tied to the cloud service provider's data centers (Mircea, 2012). Traditional security concerns may be applied to a cloud infrastructure with an additional level of potency, making incessant performance of cloud computing somewhat difficult task. A cloud environment's security challenges come into three broad categories: confidentiality, availability, and integrity. Data and infrastructure are equally vulnerable to threats in cloud environment. (Agarwal & Agarwal 2011).

Data communication & transport methods (eg. satellite communication) must have to be taken in consideration. Large data transfers are expected into cloud setting, and communication technology employed and security risks raised by modified communication technology are now security concerns for cloud computing strategy as a whole. Some communication technology's ability to broadcast is a major problem in this respect (Celesti, Fazio, Villari & Puliafito, 2012). An current concern for cloud computing is that it lacks a robust authentication system that can completely handle the security dangers connected both with virtual and physical resources. As a consequence, grid computing is increasingly being seen as an integral component of cloud computing (Rak & Villano,2013; Casola, Cuomo). Because of the close relationship between virtualized resources and cloud architecture, security concerns about infiltration are of the highest importance. In organisational setting of a cloud computing infrastructure, arbitrary intermittent intrusions must be monitored in order to account for the severity of the likelihood of a virtual machine being hacked (Townsend, Arshad & Xu, 2013). Few reserachers have stated which employing Internet technology isn't really need for cloud computing, however cost effectiveness and internationalization trends would push & drive practically all enterprises to accept Internet and related technologies as the final way towards cloud computing approach.. Cloud-specific security problems are expected, therefore, to be instantly added to the overall Internet security worries. Making cloud services portable is one way to enhance their adaptability. Security risks may arise as a result of cloud services' mobility. Cloud portability makes it possible for cloud customers to migrate between multiple cloud service providers without having to modify the methods they use to perform operations. It's evident that cloud customers have negotiating power, but security risks with cloud mobility must be taken into account. Risks of API-based security breaches are likely to increase as cloud computing becomes more widely used. (Macariu, Petcu, Panica & Craciun,2013).

This shift to mobile computing had made it necessary to integrate mobile computing as well as its related technologies as an integral component of cloud computing. Mobile computing as well as its related technology Due to resource shortages and other mobile computing restrictions, cloud computing has been hindered. Mobile cloud computing's security issues have exacerbated the challenge of massive data processing on mobile end-user devices. To overcome the constraints of mobile cloud computing, researchers have proposed an additional level of cloud known as "mobile cloud" to help in the particular computing and processing on mobile computing devices (Loke, Fernando & Rahayu, 2013). Mobile cloud computing has the same broadcast nature of satellite communication and security concerns as satellite communication since it is wireless. With the inclusion of mobile cloud into the picture, a service provider that already has both a regular cloud and a mobile cloud would have to deal with additional security concerns as well. Incorporating mobile cloud into the scenario would improve performance, but it would also introduce a new security layer concerns for both mobile cloud users and the whole cloud service provider infrastructure itself. There are various levels of extensibility and security risks connected with cloud computing's hierarchical structure, depending on cloud user's needs. It's been suggested by several writers that the very nature of cloud computing makes security concerns an apparent one. As part of the business structure, challenges posed by customers rely on the rules and practices of cloud service providers with whom they do business. Consumers may have security issues while using cloud goods or services if they are unaware of the types and specifics of service or product they are procuring or using in a cloud system; it's also connected to identity and dependability of cloud providers. As a result of this, customers may not capable for recognizing or anticipate all of risks associated into individual cloud transaction that are deal with. (Clarke & Svantesson, 2010).

5. CONCLUSIONS

Cloud computing holds immense potential, however security risks inherent in cloud computing paradigm are proportionally equal to benefits delivered. Cloud computing is a fantastic potential and a profitable choice for both corporations and attackers — both sides may benefit from cloud computing. Immense potential of cloud computing could not be disregarded only for security reasons - continual analysis and development for strong, consistent, and integrated cloud computing security models may be the only road of motivation. Security concerns might have a significant impact on infrastructure. Security is conceived of as a separate layer in cloud computing architecture. Security is a non-negotiable need in the cloud computing environment. Cloud computing is unavoidably becoming the best (and probably the final) method to commercial computing, but security obstacles and other challenges must be addressed for cloud computing to become more feasible. However, cloud computing may enable virtual ownership and accessibility to "super computers" with not being acquiring them physically because of its overall benefits and dynamism, as long as it is implemented inside an integrated and protected infrastructure framework. The term SCC may have been coined as a result of this (Scientific Cloud Computing). A lot of time and effort has been devoted into developing quicker and more secure SCC tools, which will have a significant impact on the speed of investigative work and motivation in a wide range of subjects. When it comes to social ramifications of cloud computing, there are no solid security frameworks in place. Even if no 'hard' security breach occurs, a variety of social inconsistencies may arise, making cloud computing security challenges more complex than just a technological one. Dispersed and dispersed characteristics are to blame. The acquisition of digital evidence is one example of this. The growth of cloud computing may have a substantial impact on digital evidence collecting and storage. For a successful cloud computing infrastructure development and implementation, solid cloud computing security models must be in place. When it comes to ensuring that Service Oriented Architecture can be used safely, the security features and concerns of cloud computing go beyond the infrastructure itself and include everything that's connected to it, including the services that users and cloud service providers utilize. For social and technical reasons, security breaches in the cloud may have huge societal consequences, hence cloud computing security is a sensitive and critical subject. In order to cope with cloud computing's security concerns, it is necessary to examine both technological and epistemological aspects. Rather of focusing only on computer-related issues, cloud computing research is becoming more interdisciplinary to account for its potential influence on both technical and social contexts. The service-oriented architecture & another aspects of cloud computing imply as notion of cloud computing might need to be evaluated in terms of social, commercial, technological, and legal perspectives – all of which would involve security problems in either technological or tactical form. Security flaws in cloud computing may have grave consequences; thus, every kind of cloud computing must address security apprehensions comparable for those of safety-critical systems, no matter what their nature may be. This conclusion is unquestionable.

REFERENCES

[1] Abbadi, I.M. and Martin, A. (2011). Trust in the Cloud. Information Security Technical Report, 16, 108-114. doi:10.1016/j.istr.2011.08.006

[2] Agarwal, A. and Agarwal, A. (2011). The Security Risks Associated with Cloud Computing. International Journal of Computer Applications in Engineering Sciences, 1 (Special Issue on CNS), 257-259.

[3] Arshad, J, Townsend, P. and Xu, J. (2013).A novel intrusion severity analysis approach for Clouds. Future Generation Computer Systems, 29, 416–428. doi:10.1016/j.future.2011.08.009

[4] Atayero, A.A. and Feyisetan, O. (2011). Security Issues in Cloud Computing: The Potentials of Homomorphic Encryption. Journal of Emerging Trends in Computing and Information Sciences, 2(10), 546-552.

[5] Bisong, A. and Rahman, S.S.M. (2011). An Overview of the Security Concerns in Enterprise Cloud Computing. International Journal of Network Security & Its Applications, 3(1), 30-45. doi:10.5121/ijnsa.2011.3103

[6] Buyya, R., Yeo, C.S., Venugopal, S., Broberg, J. and Brandic, I. (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generation Computer Systems, 25, 599–616.

[7] Casola, V., Cuomo, A., Rak, M. and Villano, U. (2013). The CloudGrid approach: Security analysis and

performance evaluation. Future Generation Computer Systems, 29, 387–401. doi:10.1016/j.future.2011.08.008

[8] Celesti, A., Fazio, M., Villari, M. and Puliafito, A. (2012). Virtual machine provisioning through satellite communications in federated Cloud environments. Future Generation Computer Systems, 28, 85–93. doi:10.1016/j.future.2011.05.021

[9] Che, J. Duan, Y, Zhang, T. and Fan, J. ().Study on the security models and strategies of cloud computing. Procedia Engineering, 23, 586 – 593. doi:10.1016/j.proeng.2011.11.2551

[10] Chen, D. and Zhao, H. (2012). Data Security and Privacy Protection Issues in Cloud Computing. International Conference on Computer Science and Electronics Engineering, 647-651. doi: 10.1109/ICCSEE.2012.193

[11] Dou, W., Chen, Q. and Chen, J. (2013). A confidence-based filtering method for DDoS attack defense in cloud environment. Future Generation Computer Systems, 29, 1838–1850. doi:10.1016/j.future.2012.12.011

[12] Dukaric, R. and Juric, M.B. (2013). Towards a unified taxonomy and architecture of cloud frameworks. Future Generation Computer Systems, 29, 1196–1210. doi:10.1016/j.future.2012.09.006

[13] Emam, A.H.M. (2013). Additional Authentication and Authorization using Registered Email-ID for Cloud Computing. International Journal of Soft Computing and Engineering, 3(2), 110-113.

[14] Fernando, N., Loke, S.W. and Rahayu, W. (2013). Mobile cloud computing: A survey. Future Generation Computer Systems, 29, 84–106. doi:10.1016/j.future.2012.05.02

[15] Priyanka Kulkarni, & Dr. Swaroopa Shastri. (2024). Rice Leaf Diseases Detection Using Machine Learning. Journal of Scientific Research and Technology, 2(1), 17–22. https://doi.org/10.61808/jsrt81

[16] Shilpa Patil. (2023). Security for Electronic Health Record Based on Attribute using Block-Chain Technology. Journal of Scientific Research and Technology, 1(6), 145–155. https://doi.org/10.5281/zenodo.8330325

[17] Mohammed Maaz, Md Akif Ahmed, Md Maqsood, & Dr Shridevi Soma. (2023). Development Of Service Deployment Models In Private Cloud. Journal of Scientific Research and Technology, 1(9), 1–12. https://doi.org/10.61808/jsrt74

[18] Antariksh Sharma, Prof. Vibhakar Mansotra, & Kuljeet Singh. (2023). Detection of Mirai Botnet Attacks on IoT devices Using Deep Learning. Journal of Scientific Research and Technology, 1(6), 174–187.

[19] Dr. Megha Rani Raigonda, & Shweta. (2024). Signature Verification System Using SSIM In Image Processing. Journal of Scientific Research and Technology, 2(1), 5–11. https://doi.org/10.61808/jsrt79

[20] Shri Udayshankar B, Veeraj R Singh, Sampras P, & Aryan Dhage. (2023). Fake Job Post Prediction Using Data Mining. Journal of Scientific Research and Technology, 1(2), 39–47.

[21] Gaurav Prajapati, Avinash, Lav Kumar, & Smt. Rekha S Patil. (2023). Road Accident Prediction Using Machine Learning. Journal of Scientific Research and Technology, 1(2), 48–59.

[22] Dr. Rekha Patil, Vidya Kumar Katrabad, Mahantappa, & Sunil Kumar. (2023). Image Classification Using CNN Model Based on Deep Learning. Journal of Scientific Research and Technology, 1(2), 60–71.

[23] Ambresh Bhadrashetty, & Surekha Patil. (2024). Movie Success and Rating Prediction Using Data Mining. Journal of Scientific Research and Technology, 2(1), 1–4. https://doi.org/10.61808/jsrt78

[24] Dr. Megha Rani Raigonda, & Shweta. (2024). Signature Verification System Using SSIM In Image Processing. Journal of Scientific Research and Technology, 2(1), 5–11. https://doi.org/10.61808/jsrt79