Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 4, 1016-1022
2025
Publisher: Learning Gate
DOI: 10.55214/25768484.v9i4.6167

Cloud computing security mechanisms random number authentication

Amitabha Yadav[1*]
[1]Department of software, National PG College, Lucknow, India; amitabha.engg@yahoo.com (A.Y.).

Abstract: Cloud computing security is an important aspect that has received extensive research attention because of the increasing use of cloud based services. Field of cloud computing security is continually evolving. Cloud security points towards the group of practices, technologies, rules, and procedures that are kept in place to secure data, applications, and services which are deployed on cloud computing platforms. Cloud computing give permission to organizations and individuals to keep, process, and get data and applications over the internet, but this convenience also initiates new security challenges. Cloud security aims to address the issues and assure the confidentiality, integrity, and availability of cloud services. Cloud security aspects are included in the paper. Boundary level protection framework using honey pot encryption technique is proposed in the paper. How threats are attacking at the boundary level of cloud is discussed. Cloud security framework is proposed in this paper. The author attempts to propose a security mechanism named as Random Number Authentication for the system.

Keywords: *Authentications, Cloud, Data, Security.*

1. Introduction

To enhance cloud security, Businesses should opt for cloud service providers that are both reliable and secure that conduct regular security audits and assessments, and educate their employees about best security practices in the cloud environment. Some key aspects of cloud security include and also shown in the fig 1.:

Data Protection: The security and privacy of data stored in the cloud are paramount. It encompasses the use of encryption methods, access controls, and data loss prevention strategies [1].

Identity and Access Management (IAM): These are the users who has rights to acces cloud services and managing user identities effectively is vital. IAM systems enforce strong authentication, authorization, and multi-factor authentication to prevent unauthorized access [2].

Network Security: Protecting the cloud infrastructure from external threats requires robust Including firewalls, intrusion detection and prevention systems (including vpns), is one way in which network security measures can be implemented [3].

Compliance and Regulatory Requirements: Organizations are required to meet industry-specific regulations and compliance standards [4]. Cloud providers often offer compliance certifications, but the responsibility of maintaining compliance also falls on the cloud users.

Incident Response and Monitoring: Implementing robust monitoring and incident response mechanisms allows early detection and response to security breaches or suspicious activities within the cloud environment [5].

Secure APIs: Application Programming Interfaces (APIs) enable communication and integration between different cloud services. Ensuring the security of APIs is crucial to prevent unauthorized access and data breaches [6].

Data Backups and Recovery: Having a disaster recovery plan in place and regularly backing up data helps ensure business continuity and data availability [7].

Physical Security: Servers and hardware in cloud data centers require physical security

History: Received: 22 January 2025; Revised: 20 March 2025; Accepted: 24 March 2025; Published: 12 April 2025
* Correspondence: amitabha.engg@yahoo.com

measures to prevent unauthorized access and potential physical attacks [8].

Shared Responsibility Model: Users and cloud service providers are both responsible for cloud security [9]. Providers are responsible for securing infrastructure, while users are responsible for securing their applications and data.

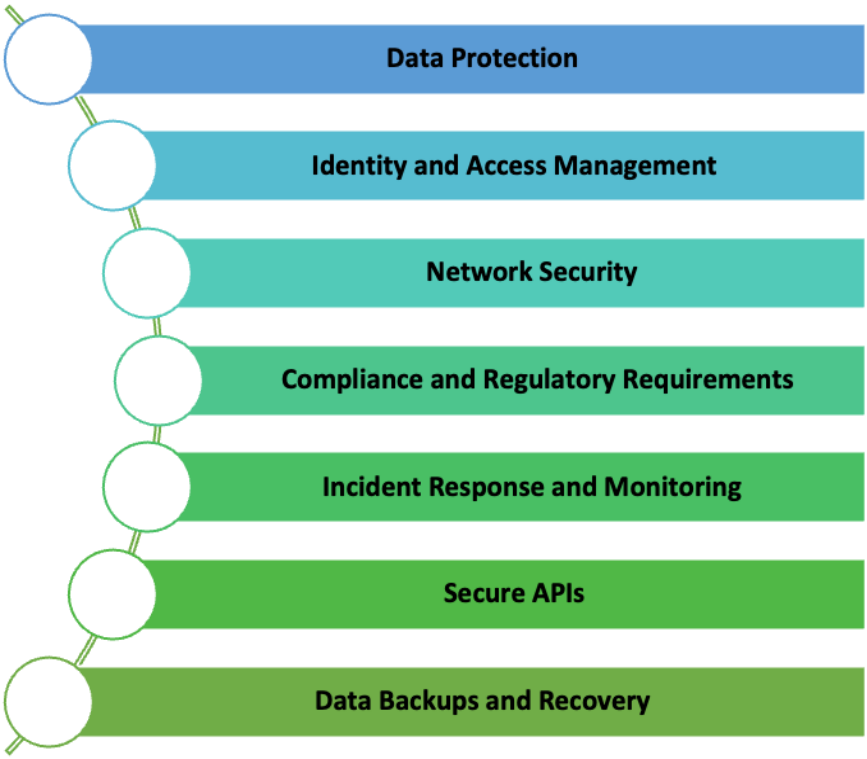

Figure 1.
Some Aspects of Cloud Security.

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 [10, 11]. 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.

2. Boundary Level Protection: Honey Protection

Honeypot encryption is a fast-spreading technique among the security groups. Honeypot act as a computer system on the Internet with intention to attract and trap attackers who are very prone to attack. Attackers are one step a head then developers, to exploit vulnerabilities in IT systems at a very short notice. To get rid from attackers and threats, defender is using Honeypot mechanism to protect the system. Since information technology is an active era for the development and research. Malware and Ransomeware attack on boundary level, We can use honey pots to trap packets that come in from anonymous users attacking the system [12]. In a Ransomeware attack, the malware usually encrypts the data. To find out if there is any encrypted data in the system, a honeypot is set up [13]. The honey pot notifies users via email and SMS if any data is encrypted. If the honey pot detects that the encryption has been initiated by malicious activity, it will sever the system's network connectivity. as shown in Figure 2.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 4: 1016-1022, 2025
DOI: 10.55214/25768484.v9i4.6167

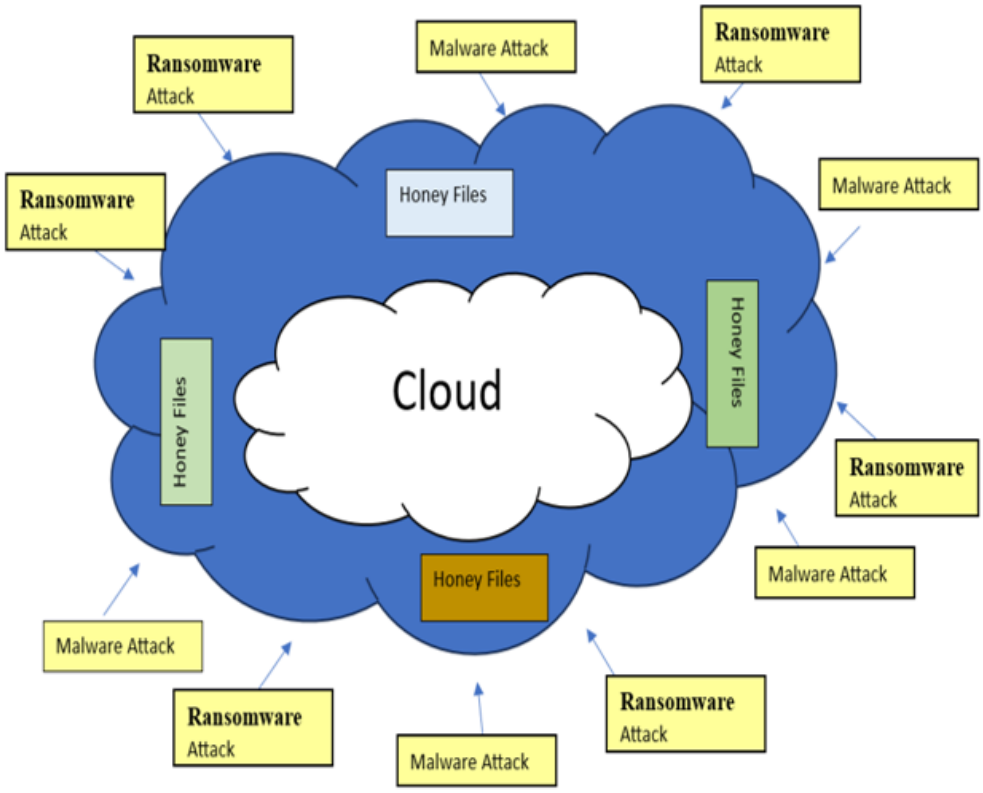

Figure 2.
Attacks at boundary level.

Security services offer built in security integrated with DevOps process to create resilient, agile and scalable solution for security in cloud [14]. Complete security management can be implemented including extra security features or tools as add-ons. Fig 3 is the secure connectivity with the honey pot encryption technique.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 4: 1016-1022, 2025
DOI: 10.55214/25768484.v9i4.6167

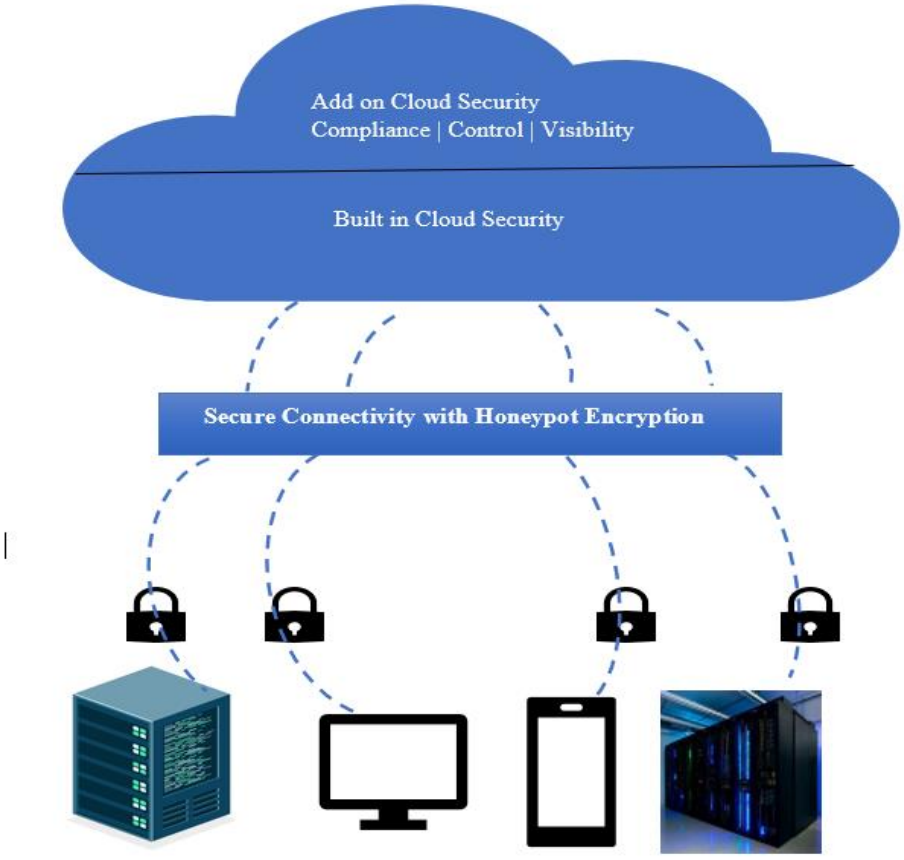

Figure 3.
Connectivity with honey pot.

3. Cloud Security Framework

Although significant research has been conducted to safeguard the security, privacy, and integrity of cloud data and services, several challenges continue to persist that require attention. A viable strategy for ensuring security and privacy within this emerging computing paradigm involves the utilization of cryptographic techniques [15]. To safeguard the security and privacy of user data, particularly in relation to an untrusted cloud service provider, it is advisable to encrypt the data before uploading and storing it in the cloud [16]. The tool is used to convert Plain test to cipher text. Following fig.4 is a security framework for cloud computing environment.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 4: 1016-1022, 2025
DOI: 10.55214/25768484.v9i4.6167

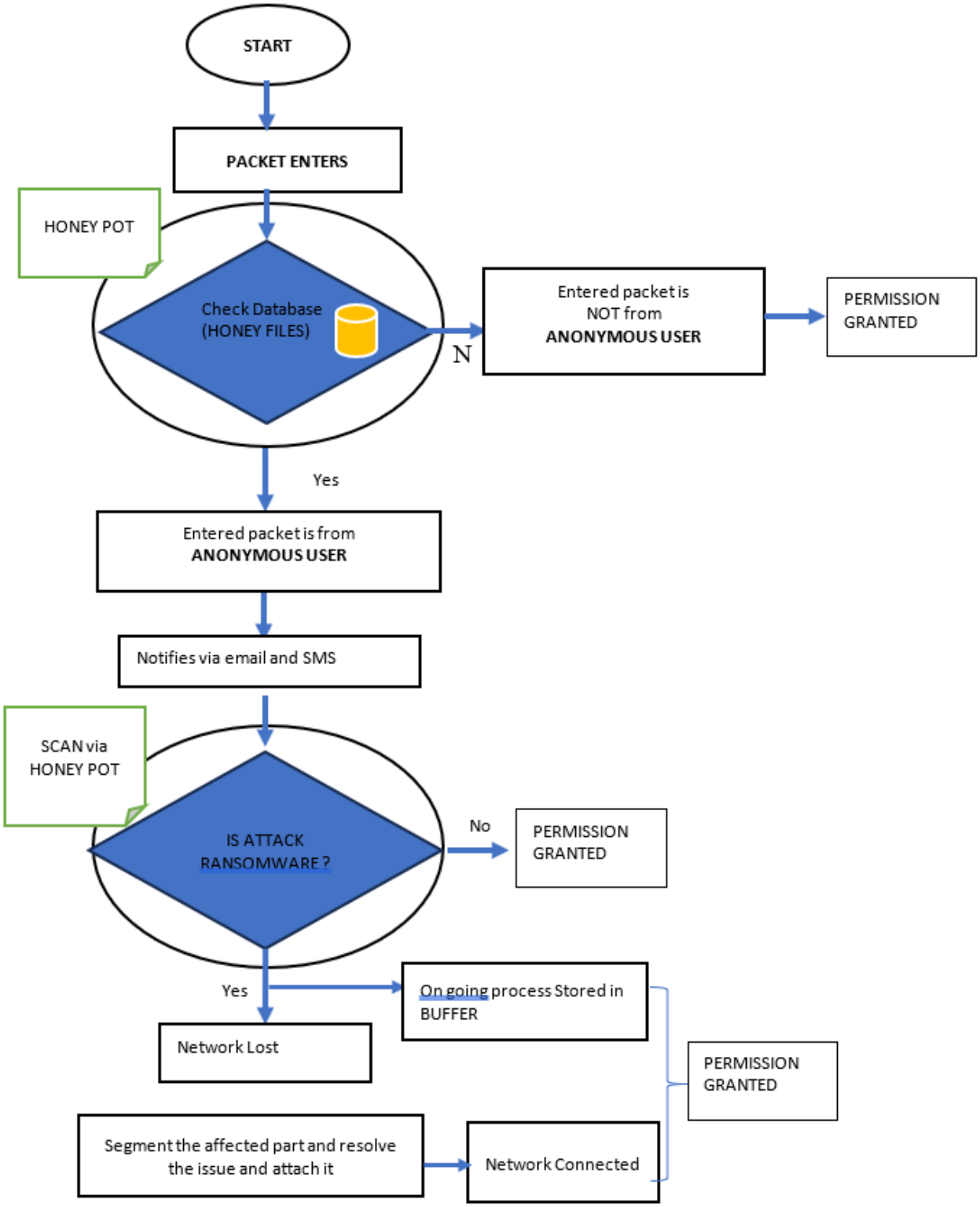

Figure 4.
Framework for cloud Security.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 4: 1016-1022, 2025
DOI: 10.55214/25768484.v9i4.6167

4. Cloud Security Mechanisms

Despite the fact that concerns regarding cloud security have consistently been identified as one of the primary obstacles to the adoption of cloud technology, the specific security issues unique to cloud computing remain ambiguous [17]. There is two defence mechanism to protect cloud from being compromise password policy and Random Number Authentication.

Password Policy: A robust password significantly enhances the security of your accounts. Therefore, it is essential to establish a comprehensive password policy that includes various options [18]. Firstly, you may implement a minimum password length requirement and specify the inclusion of certain character types. For instance, you might mandate the use of uppercase letters, lowercase letters, numbers, and special characters such as question marks. Additionally, you can decide whether to permit users to change their own passwords or enforce a policy that requires users to update their passwords periodically, such as every 90 days. Lastly, it is advisable to prevent password reuse, ensuring that users do not revert to previous passwords when making changes. Overall, a well-defined password policy is instrumental in safeguarding accounts against brute force attacks.

Random Number Authentication (RNA): The second defence mechanism is Random Number Authentication or RNA. If users have access to account, They have the potential to perform numerous tasks, particularly if they hold administrative roles, as they are able to modify configurations, remove resources, and undertake various other actions.. So, there is basic requirement to protect at least Root Account of cloud users [19]. It can be possible with RNA devices either virtually or physically as shown in fig5.

RNA employs a combination of a user-known password and a personal security device. This dual approach significantly enhances security compared to relying solely on a password policy.

Figure 5.
Cloud Security random number authentication.

The advantage of RNA lies in its ability to safeguard accounts even in the event of a password being lost due to theft or hacking. This is because a hacker would also need to obtain the physical device of the individual, such as a phone or other devices, in order to compromise the account [20]. Algorithm is used to generated the random number on a single device it can be once mobile or any third-party device to authenticate the right person.

5. Conclusion

Cloud security concerns have persistently been identified as one of the primary obstacles to the adoption of cloud technology; however, the specific security issues unique to cloud computing remain ambiguous. To address this matter, the author seeks to identify cloud security challenges by analyzing different definitions of cloud computing and a reference architecture. Attacks at boundary level of cloud is the main focused in the paper. The paper presents a Connectivity with honey pot technique to secure the clouds system. The paper proposed a Framework for cloud security to secure cloud using honeypot encryption technique. The paper proposed a Cloud Security random number

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 4: 1016-1022, 2025
DOI: 10.55214/25768484.v9i4.6167

authentication.

Transparency:

The author confirms that the manuscript is an honest, accurate, and transparent account of the study; that no vital features of the study have been omitted; and that any discrepancies from the study as planned have been explained. This study followed all ethical practices during writing.

Copyright:

References

[1] M. Jensen, J. Schwenk, N. Gruschka, and L. Iacono, "On technical security issues in cloud computing," in *Proceedings of the 2009 IEEE international conference on cloud computing (CLOUD '09). Washington, DC, USA: IEEE Comput Soc; 2009. p. 109–16 http://dxdoiorg/101109/CLOUD200960*, 2009.

[2] A. Joseph, G. Jaspher, and W. Kethrine, "Security of real time cloud service providers: A survey," presented at the In: Electronics and Communication Systems (ICECS). 2014 International Conference on, Coimbatore, 2014.

[3] A. Bhardwaj and S. Som, "Study of different cryptographic technique and challenges in future," presented at the 1st Int. Conf. Innov. Challenges Cyber Secur. ICICCS 2016, no. Icicccs, pp. 208–212, 2016. https://doi.org/10.1109/ICICCS.2016.7542353, 2016.

[4] D. K. Sharma, N. C. Singh, D. A. Noola, A. N. Doss, and J. Sivakumar, "A review on various cryptographic techniques & algorithms," *Materials Today: Proceedings*, vol. 51, pp. 104-109, 2022. https://doi.org/10.13140/RG.2.1.1031.5601

[5] S. Shevchenko, H. M. bin Abu Bakar, and J. Wong, "Taiwan heist: Lazarus tools and ransomware," *Bae Systems Threat Assessment (Baesystemsai Blog Spot Co Nz/2017/10/Taiwan-Heist-Lazarus-Tools Html)*, 2017.

[6] H. Yang, Q. He, Z. Liu, and Q. Zhang, "Malicious encryption traffic detection based on NLP," *Security and Communication Networks 2021;2021*, 2021.

[7] R. Verma and A. K. Sharma, "Cryptography: Avalanche effect of AES and RSA," *International Journal of Scientific and Research Publications*, vol. 10, no. 4, pp. 119-122, 2020.

[8] X. Zhou and X. Tang, "Research and implementation of RSA algorithm for encryption and decryption," in *Proc. of the 6th International Forum on Strategic Technology, Harbin, Heilongjiang, 2011, pp. 1118-1121*, 2011.

[9] M. Omar, "Cloud computing security: Abuse and nefarious use of cloud computing," IGI Global, 2015, pp. 30-38.

[10] S. K. Kondra, S. K. Bharti, Mishra, and K. S. Babu, "Honeypotbased intrusion detection system: A performance analysis," presented at the 3rd International Conference on Computing for Sustainable Global Development (INDIACom), 2016, pp. 2347-2351, 2016.

[11] J. Surbiryala, L. Chunlei, and R. Chunming, "A framework for improving security in cloud computing," presented at the The 2nd IEEE International Conference on Cloud Computing and Big Data Analysis, 2017.

[12] L. Wei *et al.*, "Security and privacy for storage and computation in cloud computing," *Information Sciences*, vol. 258, pp. 371-386, 2014.

[13] D. Zhe, W. Qinghong, S. Naizheng, and Z. Yuhan, "Study on data security policy based on cloud storage," in *Proc. IEEE IEEE 3rd Int. Conf. Big Data Secur. Cloud (BigDataSecurity) Int. Conf. High Perform. Smart Comput., (HPSC) IEEE Int. Conf. Intell. Data Secur. (IDS), Beijing, China, May 2017, pp. 145–149*, 2017.

[14] D. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in *Proc. IEEE SP, Berkeley, CA, USA, May 2000, pp. 44–55*, 2000.

[15] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber–physical system security for the electric power grid," in *Proceedings of the IEEE, 100(1), pp. 210-224*, 2012.

[16] P. Gayatri, M. Venunath, V. Subhashini, and U. Syed, "Securities and threats of cloud computing and solutions," in *Proceedings of the Second International Conference on Inventive Systems and Control (ICISC 2018)*, 2018.

[17] F. S. Tsai and K. L. Chan, "Detecting cyber security threats in weblogs using probabilistic models," presented at the In Pacific-Asia Workshop on Intelligence and Security Informatics (pp. 46-57). Berlin, Heidelberg: Springer Berlin Heidelberg, 2007.

[18] J. A. Gómez-Hernández, L. Álvarez-González, and P. García-Teodoro, "R-Locker: Thwarting ransomware action through a honeyfile-based approach," *Computers & Security*, vol. 73, pp. 389-398, 2018.

[19] Fediushyn, V. Ruzhentsev, I. Fedorov, and K. Moskvin, "Honeypot data storage and analysis software to prevent intrusions," presented at the 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC ST), 2021, pp. 169-173, https://doi.org/10.1109/PICST54195.2021.9772139, 2021.

[20] V. R. Pancholi and B. P. Patel, "Enhancement of cloud computing security with secure data storage using AES," *International Journal for Innovative Research in Science and Technology*, vol. 2, no. 9, pp. 18-21, 2016.