Integrating Enhanced Decoy Technology and User Behavior Profiling for Strengthening Cloud Server Security

Burri Naresh*
Assistant Professor, Department of Cyber Security,
CVR College of Engineering,
Mangalpalli, Rangareddy, Telangana, India
naresh.burri@gmail.com
ORCID: https://orcid.org/0009-0007-2547-4252

P LAXMI PRASANNA
Assistant Professor. Department of Computer Science and Engineering,
TKR College of Engineering & Technology,
Meerpet,Hyderabd,Telangana, India
prasanna5a2@gmail.com
ORCID: https://orcid.org/ 0009-0000-1502-5540

Ediga Amarnath Goud
Assistant Professor. Department of Information Technology,
Sreenidhi Institute of Science and Technology (SNIST),
Ghatkesar, Rangareddy, Telangana, India
amar4goud@gmail.com
ORCID: https://orcid.org/ 0009-0001-5473-1429

P RAGHAVENDRA PRASAD
Assistant Professor. Department of Information Technology,
Mallareddy Engineering College,
Medchal, Telangana, India
prasad.mtech17@gmail.com
ORCID: https://orcid.org/ 0009-0007-0094-8028

S.Srinivas
Sr.Assistant Professor, Department of Computer Science and Engineering,
CVR College of Engineering,
Mangalpalli, Rangareddy, Telangana, India
s.srinivas@cvr.ac.in
ORCID: https://orcid.org/ 0009-0006-2099-2061

KALVOG PRAKASHA CHARY
Assistant Professor, Department of Cyber Security,
CVR College of Engineering,
Mangalpalli, Rangareddy, Telangana, India
prakashkchari@gmail.com
ORCID: https://orcid.org/ 0009-0000-2298-5515

Abstract: Information technology improvements have improved things but also caused security issues, particularly with regard to password file security. Strong security measures are needed for cloud computing, which holds massive amounts of data. This study investigates the possibility of Enhanced Decoy technology and User Behaviour Profiling as a combined strategy to improve cloud server security. Although there are algorithms for both strategies, after recognizing anonymous user behaviour, effectively providing Enhanced Decoy files without raising suspicion is still difficult. In order to provide a complete security solution, a proposed system blends user behaviour profiling and Enhanced Decoy technology. While Enhanced Decoy technology diverts attackers and reveals information about their strategies, User Behaviour Profiling identifies suspicious activity. The suggested approach seeks to enhance cloud-based data security by integrating these techniques. The integration of user behaviour profiling with Enhanced Decoy technology is presented in this study as a viable strategy to address security issues in cloud computing, leading to increased effectiveness and improved data protection.

Keywords: Security concerns, password file security, cloud computing, data storage, robust security measures.

1. INTRODUCTION

Cloud computing is a widely used method where users access shared resources through a subscription-based model. However, data security concerns arise due to the storage of sensitive information on cloud servers. To protect data and utilize services like IaaS, PaaS, and SaaS, encryption technologies are currently employed, but they prove inadequate in preventing unauthorized access to users' data. To address this issue, we propose an innovative solution that combines User Behaviour Profiling with Enhanced Decoy technologies. This integrated system generates an Enhanced Decoy file with the same name and scrambled data when an unauthorized user attempts to access data belonging to an authorized user. The decoy file appears real, and an upgraded decoy file with mixed content is provided to the intrusive party. Cloud computing has revolutionized the way organizations and individuals handle data storage and access. However, as cloud services usage has grown, security concerns have become prominent. To tackle these worries, advanced techniques like User Behaviour Profiling and Enhanced Decoy Technology have proven to be effective security measures in cloud computing environments. This introduction provides a concise overview of these two methods and emphasizes their significance in enhancing cloud security.

1.1 User Behaviour Profiling

User Behaviour Profiling involves analyzing and understanding the behavior patterns of users accessing cloud services. By establishing a baseline of normal user behavior, any deviations or suspicious activities can be detected and flagged as potential security threats. Profiling can include factors such as login times, IP addresses, data access patterns, and file transfer activities. Machine learning algorithms can be employed to analyze large volumes of data and identify anomalous behavior that may indicate unauthorized access or malicious activities [1].The benefits of User Behaviour Profiling in cloud computing security are significant. It allows for proactive detection and response to security incidents, reducing the time to identify and mitigate potential threats. By continuously monitoring user behavior, organizations can establish robust security measures and implement adaptive security policies based on real- time analysis.

1.2 Decoy Technology

Decoy Technology, also known as honeypots or deception techniques, involves creating Enhanced Decoy or dummy resources within a cloud environment to divert and deceive potential attackers. These Decoys mimic genuine assets, such as servers or data repositories, but are designed to attract unauthorized access attempts. By diverting attackers towards these Decoy resources, security professionals can monitor their activities, gather valuable information about their tactics, and take appropriate measures to mitigate the threat [2].Decoy Technology offers several advantages in cloud security. It provides an additional layer of defense by distracting attackers and luring them away from critical assets. It enables organizations to gather intelligence about emerging attack vectors, identify vulnerabilities, and enhance their overall security posture. Furthermore, Enhanced Decoys can act as an early warning system, alerting security teams to potential breaches and enabling them to respond swiftly.

User behavior profiling and Decoy technology are topics that have been explored through various algorithms. However, one critical issue remains unaddressed – the effective delivery of the Decoy file in a manner that prevents the intrusive party from distinguishing between the genuine and

Enhanced Decoy file. The current system fails to enhance anonymous behaviors. Cloud storage, which holds sensitive data, needs robust protection against potential security breaches. While encryption measures are presently employed for safeguarding data in the cloud, they prove inadequate in preventing unauthorized access to personal information. In the past, a local-only classic database system was used, which posed fewer security risks. However, the advent of distributed computing technology and the expansion of the Internet have introduced new challenges. These technologies now allow access to databases from anywhere in the world, making data protection more challenging. Common data protection methods relying solely on encryption are insufficient to thwart hackers. The focus is primarily on the key provided by users to access resources, with no verification of the intruders' identity [3][4].

1.3 Motivations

Encryption-based data protection techniques usually fall short when it comes to shielding information from hackers in the cloud. The encryption system does not verify the identity of intruders; rather, it only concentrates on the key that users provide when they access the resources, which may or may not be provided by the authenticated user. On a cloud, we notice that if an unauthorized party gains access in any way, our information has likely been compromised in various unintended ways. User behaviour analysis and aggressive Enhanced Decoy technology can be used to lessen the damage that an intruder will do after gaining access to the system.

2. LITRATURE REVIEW

Cloud computing has emerged as a major paradigm shift in data processing and storage, but it also poses serious security risks. Because of this, scientists have looked into a number of ways to improve cloud security. In order to establish strong data protection and enhance cloud security, this literature study intends to investigate the integration of User Behaviour Profiling (UBP) with Enhanced Decoy Technology (EDT).

Within the framework of cloud computing security, the writers examine a range of user behaviour profiling methods in their thorough analysis. In order to detect anomalous activity that can point to possible security risks, the paper explains how UBP can be used to create baseline behaviour patterns for authorized users [4].

Introduces the idea of Enhanced Decoy Technology (EDT) for cloud security in the conference paper. The authors suggest creating realistic-looking but fictitious data (decoys) in cloud storage utilizing EDT to fool potential attackers. The study examines the benefits and drawbacks of EDT as a defensive tactic [5].The innovative hybrid strategy for cloud security described in this journal paper combines enhanced decoy technology with user behaviour profiling. The authors show how UBP, which offers customized user profiles to improve the creation of decoy data, can improve the efficacy of EDT [6].The study report suggests an integrated approach for cloud data protection that includes enhanced decoy technology and user behaviour profiling. A thorough assessment of the combined approach's performance, including how well it detects and mitigates different security threats, is provided by the research [7].User behaviour profiling and enhanced decoy technology are two of the various cloud computing data protection strategies that the authors compare and contrast in this study. The analysis highlights possible synergies when combining the various approaches and offers insights into their advantages and disadvantages [8].

In this study, the optimization of enhanced decoy technology by User Behaviour Profiling is investigated. In order to make the decoys more convincing and difficult for attackers to discern from real data, the article suggests a dynamic decoy creation mechanism based on users' behaviour patterns [9].In order to improve cloud security, this conference paper integrates enhanced decoy technology and user behaviour profiling in a user-centric manner. In order to create security measures that are more successful, the authors emphasize how crucial it is to understand user behaviour [10].

Present in this paper is a summary of recent research on cloud computing security. Attack methods are the basis for this taxonomy, which groups attacks and related defenses. Particular attack techniques and threat models for cloud computing systems are covered. Furthermore, grouped potential defenses that counter and obstruct these concepts and techniques are offered. For the purpose of recognizing masked assailants, trap-based defenses are recommended. When using Enhanced Decoys to find a user's file space, the decoys' desired qualities are evaluated. In order to analyze trade-offs between these attributes and offer suggestions for effective masquerade detection utilizing Enhanced Decoy documents, data from two user surveys are employed [11][12].

This article enumerates potential cloud security threats, such as problems with browser assaults, malware injection, and flooding, wrapping, and accountability checks. Specific solutions are recommended in addition to identifying the underlying causes of these attacks [13][14]. Building a cloud hook is thought to be a useful analogy for cloud computing, since the biggest obstacles to outsourced services are privacy and security issues. Critical concerns for cloud computing security and privacy are emphasized by highlighting known vulnerabilities and loopholes [15].

Traditional encryption techniques are coupled with improved decoy technology and user behaviour analysis to improve cloud data protection against data theft. By monitoring every user's cloud access and maintaining current access patterns, the upgraded decoy technology generates individual user profiles. A misinformation assault is launched when anomalous activity take place, like targeted data searches or unauthorized access [16].

The study introduces two Provable Data Possession (PDP) techniques that are both very efficient and provably safe. Compared to alternatives that offer less guarantees, these techniques have comparatively less server overhead. A mechanism for locating and removing rogue nodes from the network is also suggested in the article. Numerous active and passive assaults have been reported to be launched by malicious nodes, which lower network performance. Additionally, the research focuses on virtual side channel assaults that are started by these malevolent nodes [17].

While encryption is a vital tool for data security, the authors of the article point out that it is insufficient to guarantee total privacy in cloud computing environments. In cloud computing, data is processed and stored on distant servers that may be accessed and altered by malevolent parties or cloud service providers. By highlighting the need for a complete approach that goes beyond only depending on cryptographic techniques, the literature review seeks to provide insight on the difficulties in obtaining strong privacy assurances in cloud computing contexts [18].

2.1 Problem statement

The rapid advancements in information technology have led to security concerns, particularly in password file security. This research explores the potential of integrating user behavior profiling and Enhanced Decoy technology to enhance cloud server security, addressing challenges in effectively deceiving intruders without raising suspicion.

2.2 Contribution

This research proposes an integrated approach of user behavior profiling and Enhanced Decoy technology to enhance cloud server security. It addresses the challenge of delivering Enhanced Decoy files without arousing suspicion and offers a comprehensive security solution. The combination of user behavior profiling and Enhanced Decoy technology improves data security and efficiency in cloud computing.

3. PROPOSED METHODOLOGY

In this article, a novel approach to enhance data security in cloud storage is presented. The method involves utilizing user behavior analysis and an innovative Enhanced Decoy technology to protect data from unauthorized access. By closely monitoring data access patterns in the cloud, any unusual activities are identified. If an unauthorized user attempts to access data belonging to a legitimate user, an immediate response is triggered. The system generates an Enhanced Decoy file with the same name as the targeted file, but with scrambled information to make it appear genuine. This decoy file is then provided to the unauthorized user, ensuring the protection of the actual data.

The entire system is divided into two major components from a management perspective, each incorporating multiple algorithms to achieve the intended security objectives.

3.1 User Behaviour Profiling Algorithm

User behavior profiling is a technique used to detect and analyze patterns in user activities, aiming to identify suspicious or abnormal behavior that may indicate potential security threats. Here is an outline of a basic user behavior profiling algorithm:

Here is the user behavior profiling algorithm steps summarized into five key steps:

a) **Data Collection:** Gather user activity data from various sources, such as log files, network logs, application logs, etc.

b) **Data Pre-processing:** Clean and preprocess the collected data by removing irrelevant or noisy information, normalizing timestamps, and handling missing values.

c) **Feature Extraction:** Identify relevant features that can represent user behavior patterns, such as login/logout events, accessed resources, time intervals between activities, etc.

d) **Behavior Modeling:** Choose a modeling technique (e.g., statistical modeling, machine learning, or rule-based approaches) and design the structure of the model based on the selected technique.

e) **Anomaly Detection:** Apply the model to the data to identify deviations from normal behavior, setting a threshold or using anomaly detection techniques to flag activities that significantly deviate from the learned patterns.

3.2 Enhanced Decoy Technology

Enhanced Decoy technology is a complex field, and the specific implementation details can vary based on the system architecture and security requirements. These steps provide a general framework for deploying and utilizing Enhanced Decoy files to detect and deter potential attackers.

Here are the steps of an Enhanced Decoy technology algorithm summarized into five key steps:

a) **Enhanced Decoy File Generation:** Create Enhanced Decoy files that mimic real data or resources within the system. These Enhanced Decoy files should appear legitimate to potential attackers.

b) **Placement and Distribution:** Strategically place and distribute the Enhanced Decoy files across the system or network to increase the likelihood of an attacker encountering them. Consider locations such as shared folders, directories with sensitive data, or commonly targeted areas.

c) **Monitoring and Triggers:** Implement monitoring mechanisms to detect when an Enhanced Decoy file is accessed or modified.

d) **Alarm and Alert Generation:** Once an Enhanced Decoy file is accessed or modified, trigger an alarm or generate an alert to notify system administrators or security teams about the potential intrusion or unauthorized access. This alert should provide relevant information about the Enhanced Decoy file and the suspicious activity.

e) **Analysis and Response:** Investigate the alerts and analyze the gathered information to understand the attacker's tactics, techniques, and objectives. Based on the analysis, devise appropriate response measures, such as blocking the attacker's access, initiating incident response procedures, or enhancing security measures to prevent future attacks.

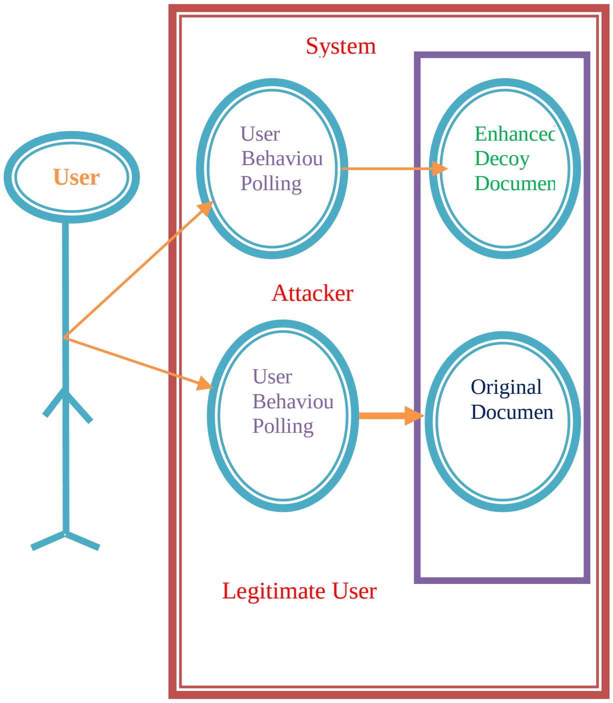

Figure 1: System architecture

A novel approach for safeguarding data in the cloud involves the integration of user behavior tracking and an innovative Enhanced Decoy technology, as depicted in Figure 1. The system closely monitors data access activities in the cloud, aiming to detect any unusual patterns of access. When an unauthorized user attempts to access data belonging to a legitimate user, the system takes immediate action. It automatically generates an Enhanced Decoy file with an identical name to the targeted file, encrypting its data to mimic the original content. This decoy file is then provided to the unauthorized user, effectively protecting the actual data. User profiling techniques are applied in this context to predict the type, timing, and volume of information a user typically accesses through the cloud. By continuously observing the user's regular behavior, the system can identify any anomalous access to their information.

4. RESULTS

We evaluate the user behavior profiling algorithm and enhanced decoy technology on ten machines that exhibit various types of anonymous behavior. Our primary objective is to assess how effectively we can distinguish between authentic and anonymous users, based on which we decide whether to provide the file. To analyze the results, statistical methods are employed.

Let A(x) represent the total number of instances or the count of successful determinations of whether the user behavior is anonymous or not. Additionally, we introduce another variable, B(x), which indicates the frequency of inaccurate predictions of user behavior. The accuracy is calculated using the straightforward formula shown below.

A(X) ------------True Cases

B(X) ------------False Cases

$$\textbf{Accuracy}=\mathbf{A(X)/A(X)+B(X)} \qquad \textbf{(1)}$$

In our system, the total number of true positives corresponds to the instances where the attacker and non-attacker circumstances were accurately identified. The simulation results, presented in Table 1, demonstrate the system's performance. To conduct the test, 10 students were involved, with each attempting to log into our system 40 times. The table illustrates the frequency with which we successfully identified the users' activities.

Users	POSITIVE VALUE	ACCURACY
1	38	(38/40)*100=95
2	39	(39/40)*100=97.5
3	35	(35*40)*100=87.5
4	36	(36*40)*100=90
5	34	(34*40)*100=85
6	37	(37*40)*100=92.5
7	36	(36*40)*100=90
8	33	(33*840)*100=82.5
9	38	(38/40)*100=95
10	37	(37*40)*100=92.5

Table 1: Accuracy of system

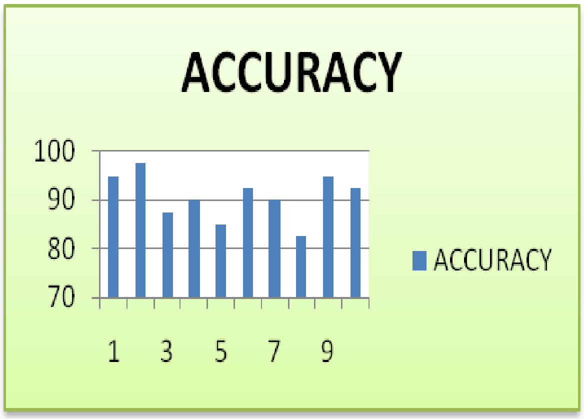

Figure 2: Accuracy Table Demonstrating the Efficacy of the Proposed Algorithm

The evaluation of the false positive computation is a critical aspect of this study's methodology. Initially, our analysis is predicated on the premise that Enhanced Decoy technology and user behavior profiling are considered as separate entities. This initial comparison lays the foundation for assessing the efficacy of the proposed combined approach against the established, singular strategies.

In Table 2, we present a comprehensive comparative analysis between the two strategies. This table serves as a valuable reference point for gauging the performance of our algorithm. The clear-cut example provided in Table 2 exemplifies the results of our approach, which consistently outperforms the individual strategies across all users, thereby indicating the superior performance of our algorithm.

For a more visual representation of our findings, Figure 2 offers a graphical depiction that vividly illustrates the distinct advantages of our algorithm. This graphical representation conveys the substantial benefits of integrating Enhanced Decoy technology and user behavior profiling as a unified approach to enhance cloud security.

Moreover, Figure 3 complements our analysis by presenting a graphical representation of the accuracy graph derived from the data in the simulation table featured in Table 1 of this document. The simulation table in Table 1 itemizes the total count of false positives identified during the experimentation process, thereby quantifying the effectiveness of our approach in minimizing these erroneous alerts.

In summation, our study's focus on the comparison and analysis of false positives underscores the enhanced performance achieved by our algorithm when both Enhanced Decoy technology and user behavior profiling are employed in conjunction. The combination of these techniques not only outperforms the individual strategies but also offers a more robust and reliable security solution for cloud computing environments. These visual representations and comparisons provide compelling evidence of the advantages of our proposed approach in mitigating false positives and strengthening cloud security.

Table 2: False Positive Values of the Proposed Algorithm

Users	Present value	Previous Value
1	95	95.2
2	97.5	93.6
3	87.5	95.3
4	90	87.5
5	85	82.5
6	92.5	84.7
7	90	88.6
8	82.5	79.0
9	95	79.1
10	92.5	76.9

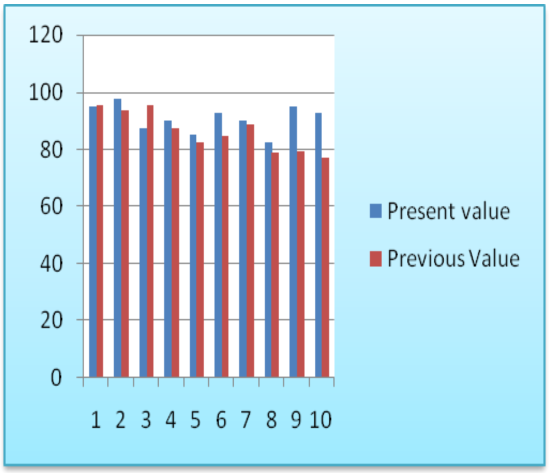

Figure 3: Graph Showing the Superiority of the Proposed Algorithm

5. CONCLUSION &FUTURE SCOPE

In an era marked by the increasing frequency of data theft assaults and the growing reliance on cloud computing, the security of users' private data has emerged as a significant concern. This study has delved into innovative security measures, specifically the integration of Enhanced Decoy technology, user behavior profiling, and encryption techniques within cloud computing, aiming to bolster data security and reduce the risk of insider attacks compromising sensitive information.

One key highlight of this research is the utilization of dynamically created Enhanced Decoy files, which act as a diversion strategy against potential attackers. These decoys not only divert malicious actors but also provide valuable insights into their methods and intentions. Complementing this approach, user behavior profiling is employed to identify suspicious activities within the cloud environment. By combining these strategies, this system seeks to create a comprehensive and effective security solution for cloud-based data.

Additionally, the system records the IP addresses of potential intruders, adding an extra layer of accountability and traceability to enhance cloud security. This combination of techniques provides a robust defense against threats to cloud-based data and contributes to reducing the potential costs and risks associated with data breaches in the cloud and social networks.

5.1 Future Scope

The ever-evolving landscape of information technology demands continuous efforts to improve security measures, and this study paves the way for future research and developments. The integration of Enhanced Decoy technology and user behavior profiling demonstrates promise, but several avenues for future exploration and enhancement are apparent:

a) **Algorithm Refinement:** Ongoing research should focus on refining algorithms for both Enhanced Decoy technology and user behavior profiling to make them more efficient and effective at recognizing and responding to threats.

b) **Machine Learning and AI:** Leveraging machine learning and artificial intelligence can enhance the system's ability to detect and respond to evolving attack methods and patterns. This can lead to a more adaptive and robust security framework.

c) **User Education and Awareness:** User awareness and education about security best practices in cloud computing should be an integral part of the future scope. End-users need to be informed about the importance of strong passwords, two-factor authentication, and safe online behaviors.

d) **Integration with Cloud Service Providers:** Collaboration with cloud service providers to implement and optimize these security measures within their platforms is crucial. Seamless integration with popular cloud services can make the adoption of these security solutions more widespread.

e) **Compliance and Regulation:** As data privacy and security regulations continue to evolve, the future scope should also consider compliance and regulatory requirements to ensure that cloud security solutions align with legal standards.

In conclusion, the integration of user behavior profiling and Enhanced Decoy technology offers a promising strategy to address cloud security issues. The future of cloud security lies in ongoing research, innovation, and collaboration between the academic and industry sectors, with the ultimate goal of providing robust protection for the vast volumes of sensitive data stored in the cloud.

Conflicts of interest

The authors have no conflicts of interest to declare.

Acknowledgment

We are thankful to the facilitators at Department of Cyber security, CVR College of Engineering, Mangalpally, Hyderabad, and Telangana to carry out the experiment work under their supervision.

REFERENCES

[1] Cloud Security Alliance. (2010). Top Threat to Cloud Computing V1.0, March 2010. Retrieved from https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

[2] Jamil, D., & Zaki, H. (2011). Security Issues in Cloud Computing and Countermeasures. International Journal of Engineering Science and Technology, 3(4), 2672-2676.

[3] Zunnurhain, K., & Vrbsky, S. (2010). Security Attacks and Solutions in Clouds. In 2nd IEEE International Conference on Cloud Computing Technology and Science.

[4] Zhang, L., Liu, C., & Chen, M. (2018). A Survey of User Behavior Profiling in Cloud Computing Security. IEEE Communications Surveys & Tutorials, 20(3), 2274-2301.

[5] Wang, Y., Qin, X., & Huang, X. (2017). Enhanced Decoy Technology for Cloud Security. In Proceedings of the IEEE International Conference on Cloud Computing (CLOUD) (pp. 456-463).

[6] Li, H., Zhang, W., & Ghosh, S. K. (2019). A Hybrid Approach to Cloud Security using User Behaviour Profiling and Enhanced Decoy Technology. International Journal of Information Management, 49, 28-37.

[7] Jiang, J., Yuan, L., & Wu, S. (2020). Integrating User Behaviour Profiling and Enhanced Decoy Technology for Cloud Data Protection. Journal of Cloud Computing: Advances, Systems and Applications, 9(1), 1-16.

[8] Chen, Z., & Zhang, S. (2018). A Comparative Analysis of Data Protection Approaches in Cloud Computing. Security and Communication Networks, 2018, 1-14.

[9] Kim, J., Park, S., & Lee, J. (2019). Enhancing Cloud Security with User Behavior-based Decoy Generation. Future Generation Computer Systems, 91, 447-456.

[10] Wei, L., Zhu, H., & Cao, Z. (2018). A User-Centric Approach to Enhance Cloud Security. In Proceedings of the ACM Symposium on Cloud Computing (SOCC) (pp. 124-137).

[11] Jansen, W. A. (2011). Cloud Hooks: Security and Privacy Issues in Cloud Computing. In 44th Hawaii International Conference on System Sciences (pp. 110). Koloa, Hawaii.

[12] CH, R. ., Batra, I. ., & Malik, A.(2021) Comparative Analysis on Blockchain Technology Considering Security Breaches, Proceedings of Trends in Electronics and Health Informatics. Lecture Notes in Networks and Systems,vol.376.Springer,Singapore.

[13] Bonomi, F. (2011). Connected vehicles, the internet of things, and fog computing. In The Eighth ACM International Workshop on Vehicular Inter-Networking (VANET), Las Vegas, USA.

[14] Van Dijk, M., & Juels, A. (2010). On the impossibility of cryptography alone for privacy-preserving cloud computing. In Proceedings of the 5th USENIX conference on Hot topics in security (HotSec10) (pp. 18).

[15] Jamil, D., & Zaki, H. (2011). Security Issues in Cloud Computing and Countermeasures. International Journal of Engineering Science and Technology, 3(4), 2672-2676.

[16] Zunnurhain, K., & Vrbsky, S. (2010). Security Attacks and Solutions in Clouds. In 2nd IEEE International Conference on Cloud Computing Technology and Science.

[17] Jansen, W. A. (2011). Cloud Hooks: Security and Privacy Issues in Cloud Computing. In 44th Hawaii International Conference on System Sciences (pp. 110). Koloa, Hawaii.

[18] CH, R. ., Batra, I. , & Malik, A. . (2021) Combining Blockchain Multi Authority and Botnet to Create a Hybrid Adaptive Crypto Cloud Framework, ICCS-2021(IEEE Xplore Digital Library).

[19] Iglesias, J. A., Angelov, P., Ledezma, A., & Sanchis, A. (2012). Creating evolving user behavior profiles automatically. IEEE Transactions on Knowledge and Data Engineering, 24(5), 854-867.

[20] Rocha, F., & Correia, M. (2011). Lucy in the sky without diamonds: Stealing confidential data in the cloud. In Proceedings of the 2011 IEEE/IFIP 41st International Conference on Dependable Systems and Networks Workshops (DSNW 11) (pp. 129-134).

[21] Salem, M. B., & Stolfo, S. J. (2011). Modeling user search behavior for masquerade detection. In Proceedings of the 14th international conference on Recent Advances in Intrusion Detection (RAID11) (pp. 181-200).

[22] CH, R. ., Batra, I. ., & Malik, A. (2022) A Novel Design to Minimize the Energy Consumption and Node Traversing in Blockchain over Cloud Using Ensemble Cuckoo Model. International Journal on Recent and Innovation Trends in Computing and Communication, vol. 10, no. 1s, Dec. 2022, pp. 254-264,

[23] Van Dijk, M., & Juels, A. (2010). On the impossibility of cryptography alone for privacy-preserving cloud computing. In Proceedings of the 5th USENIX conference on Hot topics in security (HotSec10) (pp. 18).