Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 44 No. 5 (2023)

Exploring the Enigmatic Realm of Cloud Computing: Unraveling Security Issues and Pioneering Research Challenges

[1]Syed Imran Patel, [2]Dr. Bajrang Lal

[1]Research Scholar, Department of Computer Science and Engineering, Singhania University, Pacheri Bari, Jhunjhunu, Rajasthan.

[2]Professor, Department of Computer Science and Engineering, Singhania University, Pacheri Bari, Jhunjhunu, Rajasthan

Abstract

The benefits of cloud computing, which include reduced capital expenditures, increased efficiency, scalability, integration, and on-demand access to shared computer resources, are many. Modern data storage solutions sometimes leverage cloud computing to house massive amounts of newline data. It is conceivable that the user is worried about the disclosure of his trade secrets and other sensitive information. It is critical to protect data against malicious attacks in order to make the information system reliable and trustworthy in these situations.

Keywords: *Cloud, computing, Utility, managing, generation.*

Introduction

Cloud computing uses a distributed architecture that integrates server resources into a scalable platform to supply computer resources and services on demand. Cloud service providers (CSPs) offer consumers cloud platforms to use and build their online services in a manner similar to how internet service providers (ISPs) provide customers with high-speed broadband to access the internet. ISPs and CSPs both offer service providers.

Cloud computing, which is quickly constructed and provided without any administrative labor or service provider interaction, enables quick, on-demand network access to a shared pool of programmable computer resources. Businesses use cloud computing and other IT solutions more often since they only have to pay for the services they use. Additionally, companies can easily adjust to the needs of changing markets to stay ahead of their clients.

The concept of "just using the infrastructure without managing it" gave rise to cloud computing, which quickly became an essential tool for businesses. Companies like as Microsoft, Amazon, Google, Yahoo!, and Salesforce.com have lately brought this concept from academia into business. Since the cost of the infrastructure is considerably reduced, this makes it simpler for new entrepreneurs to join the market. Developers might shift their focus from the initial budget to the commercial value as a result. Commercial cloud customers may dynamically rent storage space (virtual space) or processing power (virtual machines) based on their company's need. Thanks to this innovation, consumers may run resource-intensive apps on relatively small and lightweight mobile devices like smartphones, tablets, and laptops.

The three primary elements of cloud computing are platforms, applications, and infrastructure. Each division has a distinct function and offers specialized products and services to businesses worldwide. Web services, utility computing, managed service providers, service commerce, internet integration, and platform as a service are all included in the business application. Because cloud computing integrates so many different technologies, including operating systems, databases, virtualization, scheduling resources, load balancing, concurrency control, and memory management, it presents a number of security risks. Therefore, many of the security issues with these systems and technologies also apply to cloud computing. Secure operations are essential in many aspects of cloud

computing, including the network that links computers and the process of mapping virtual machines to real ones. Encrypting data and establishing guidelines for its sharing are essential for data security.

Literature And Review

Dahiya, Vandna & Dalal, Sandeep. (2018). Major objectives for creating smarter applications are being established by the convergence of Cloud Computing and the Internet of Things. Computing, storage, processing, and other constraints for Internet-connected objects have been transformed as a result. This convergence is fostering innovation in both fields. These days, cloud computing enhances the capabilities of individual "things" by backing up applications. High latency, massive bandwidth needs, dealing with different protocol suites, etc. are just a few of the issues that plague this integration. A new approach, fog computing, has arisen to address these issues. A fog layer is an extra layer that extends cloud services to the network's periphery. The paper explains what fog computing is, how it works, and what features it needs. The paradigm of fog computing has also been characterised by a number of difficulties and potential future developments.

Mushtaq, Muhammad et al., (2017) When it comes to providing clients with on-demand, flexible, and costeffective services over the network, cloud computing shows incredible promise. The organization's capabilities are enhanced in a dynamic way, without the need to invest in new infrastructure, licence software, or educate new employees. The scalability of resources has led to cloud computing's meteoric rise in recent years, making it seem like a rapidly expanding sector of the IT business. When it comes to managing security in the cloud, issues like policy failure or malicious behaviour are a real possibility due to the scalability and dynamic nature of the technology. In this paper, we take a look at the cloud computing architecture's detailed design, which includes models for deployment and services as well as cloud components and security. In addition, the study finds the problems with cloud computing security when data is sent to the cloud and offers a practical way to fix them. Trusted Third Party (TTP) is responsible for establishing cloud computing security standards that are adequate. Public Key Infrastructure (PKI) is a cryptographic solution that works with Single-Sign-On (SSO) and Lightweight Directory Access Protocol (LDAP) to guarantee the authenticity, availability, confidentiality, integrity, and precision of data and communications.

Goundar, Sam. (2012). The term "cloud computing" has recently been popular in the information technology sector and the media at large, but the majority of us still don't understand what it means. The first question that this paper attempts to answer is, "What is cloud computing, and how does it work?" The concept of "the cloud" refers to the integration of previously existing technologies with the Internet in order to do new and exciting things. People that are thinking about using cloud services for their own personal needs will also find this material useful. Free online photo and video sharing services like Flickr, Facebook, and YouTube allow users to upload and share user-generated content. Simple as 1. Sign up 2. Upload 3. Spread the word. Because nothing is ever truly free or easy, some drawback must exist, and people are aware of this. Businesses can find details on cloud computing here! For companies who want to stay ahead of the competition, taking a "flight to the clouds" is a common strategy. Without having to invest in costly IT infrastructure, businesses can access IT services on demand through cloud service providers. The outcome is IT services that are both more agile and cost-effective, and this paper explores the how and why of that. After we cover the benefits of cloud computing, we'll continue on to the cons. Unfortunately, not every interaction we've had online has been a favourable one. Many problems with trust and security exist. The question that many companies and individuals wonder is, "How safe is their data once it's in the cloud?" Your data posted on social networking websites and the data kept by cloud service providers are both subject to taxonomy and ownership analyses. We will conclude this section with some cloud computing anecdotes to back up our cloud computing undertaking. Nowadays, cloud computing is commonplace, not just a passing fad. Cloud computing will not go away any time soon. "Will cloud computing happen?" is an old question. yet, "how are you planning to make use of this technology?"

Kumar, Kiran. (2012). These days, IT firms all around the globe are seeing the increasing trend of cloud computing as a crucial component of their IT networks. The cloud offers several advantages to their company, including increased productivity, decreased costs, and more flexibility. Of paramount importance, though, is the reality that, like other IT innovations, the cloud is not without its share of drawbacks. For reasons of accessibility

and dependability, data stored in the cloud may reside anywhere in the globe; nevertheless, this also runs the risk of letting users' data spiral out of their hands. Without giving any thought to the various concerns raised by the lack of privacy and security in the cloud, numerous IT firms are hastily embracing this new technology. Insight into the cloud and analysis of the many threats to cloud computing are the goals of this lengthy study article. Cloud providers argue that users are more responsible for data security in the cloud, while some cloud users hold this view. By discussing these difficulties and the necessity of maintaining data security in the cloud, this research study bridges the gap between cloud users and providers.

Privacy Enabled Data Preservation Using Secured Data Access Control Privacy-Enabled Data

Preservation for the Secured Data Access in the Cloud

A novel access control strategy based on modified Chebyshev polynomials is proposed by this model. Figure 1 shows the three-tiered strategy that this system is based on. The first-level entity that manages data, keys, and access structure is called a Data Owner (DO). In order to produce the Doc KEY (document key required for decryption) using AHI_AES encryption, the data owner must provide the password DOKEY. The role of the user will be dynamically detected by the cloud server. The CSP's job description includes enforcing the access hierarchy and granting access to data. The third tier contains the Data User (DU). The data is mostly used by the DU. There are authorised and unauthorised users among them, each with their own unique role and set of permissions.

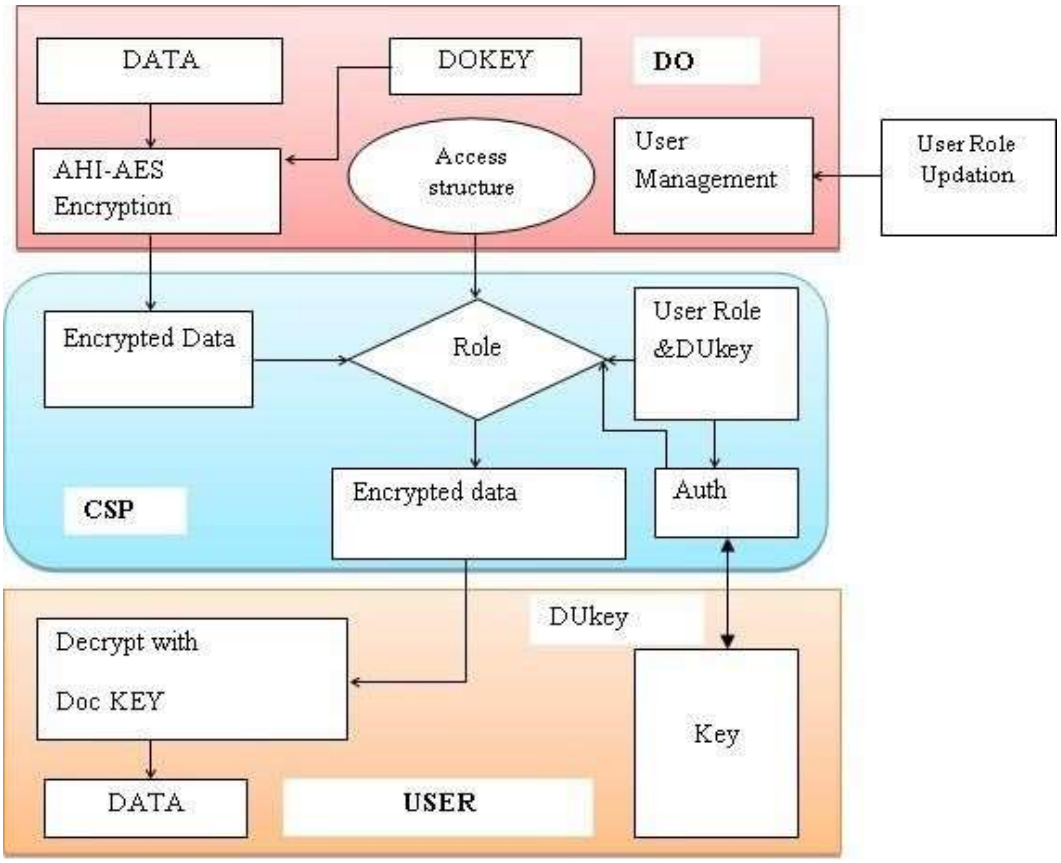

Figure 1: Privacy Enabled Data Preservation Model

Modified Chebyshev polynomial Based Access Control (MCBAC)

During the access control phase, users make data requests to the server, and only users who have been authenticated are given the data they need. To ensure the safe delivery of data to the user and prevent unauthorised access, many layers of authentication and verification are used.

Table 1 provides the whole set of symbols used throughout the authentication and registration processes.

To begin, By EX-ORing the Time encryption technique with the hashing function of the public key Kp and the cloud user Ks's private key, we can potentially obtain Su's session password. Equation represents it.

Table 1: An explanation of the symbols used in the authentication and registration phases

Symbol	Description
K_P	Public key
K_D	Public key of cloud data provider
K_U	Public key of cloud user
K_S	Private key of cloud user
N_U	User name of user
N_S	User name of server
P_U	Password of user
P_S	Password of server
S_U	Session password of user
S_S	Session password of server
T_U	Chebyshev polynomial modulant constant of user
T_S	Chebyshev polynomial modulant constant of server
E (•)	Encryption
h (•)	Hashing function
$\oplus$ $\|\|$	X-OR
	Concatenation
*	Stored value
~ G1 and G2	Received value
	Intermediate messages
+	Computed value

Comparative Methods Of Access Control Of The Mcbac

Here we take a look at some methods that have been developed by different groups and see how they stack up against one another. Using three metrics—detection rate, accuracy, and recall—and Analysing the results of three simulated attacks—a password guessing assault, a brute force attack, and a dictionary attack—we can see how well the suggested access control approach performs. There is a comparison of the MCBAC's performance with the current approaches.

Comparative Analysis of the Access Control of the Proposed Method in the Presence of Password Guessing Attack

Using assessment criteria like accuracy, In the context of a password guessing attack, recall and detection rate are affected by changes in the user count, this section describes the comparative study of the MCBAC's access control with the current approaches.

Table 2: Comparative Analysis of Precision in Terms of Password Guessing Attack

Number of Users	Precision in Terms of Password Guessing Attack			
	Existing Schemes			MCBAC
	APHA	MAKU	ECC-MLA	
50	0.674418	0.692307	0.714285	0.81081
60	0.941176	0.957446	0.980769	0.98214
70	0.890909	0.919354	0.935483	0.96491
80	0.567164	0.647058	0.698412	0.75
90	0.647887	0.726027	0.73913	0.77941

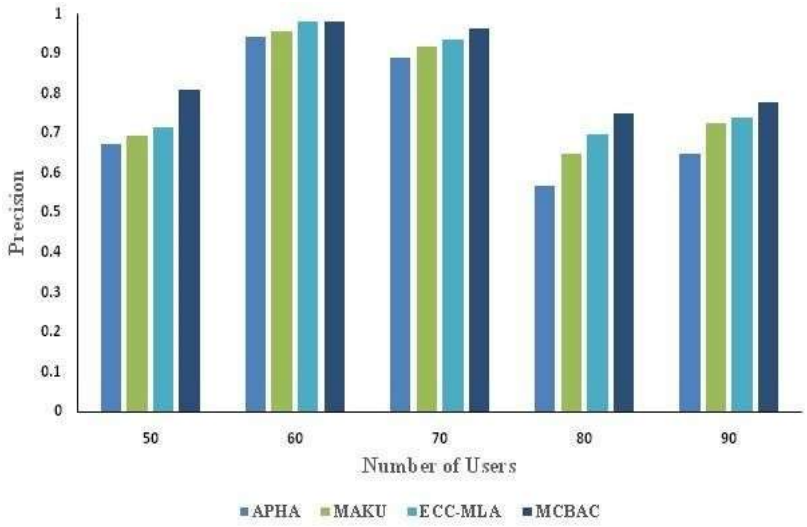

Figure 2: Comparative Analysis of Precision in Terms of Password Guessing Attack

Table 3: Comparative Analysis of Recall in Terms of Password Guessing Attack

Number of Users	Recall in Terms of Password Guessing Attack			
	Existing Schemes			MCBAC
	APHA	MAKU	ECC-MLA	
50	0.75758	0.8182	0.82879	0.82909
60	0.75	0.8	0.85	0.86667
70	0.73134	0.8209	0.85075	0.86567
80	0.77551	0.798	0.82796	0.85184
90	0.77966	0.8644	0.89831	0.89831

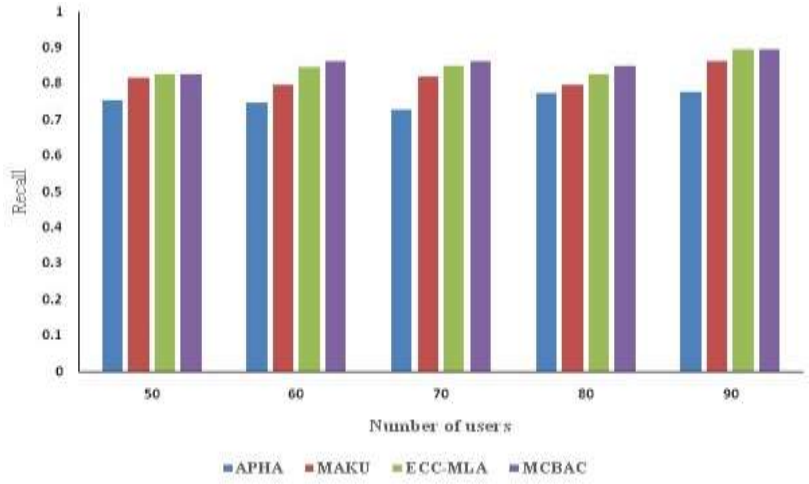

Figure 3: Comparative Analysis of Recall in Terms of Password Guessing Attack

Table 4: Comparative Analysis of Detection Rate in Terms of Password Guessing Attack

Number of Users	Detection Rate in Terms of Password Guessing Attack			
	Existing Schemes			MCBAC
	APHA	MAKU	ECC-MLA	
50	0.75758	0.8182	0.82879	0.82909
60	0.75	0.8	0.85	0.86667
70	0.73134	0.8209	0.85075	0.86567
80	0.77551	0.798	0.82796	0.85184
90	0.77966	0.8644	0.89831	0.89831

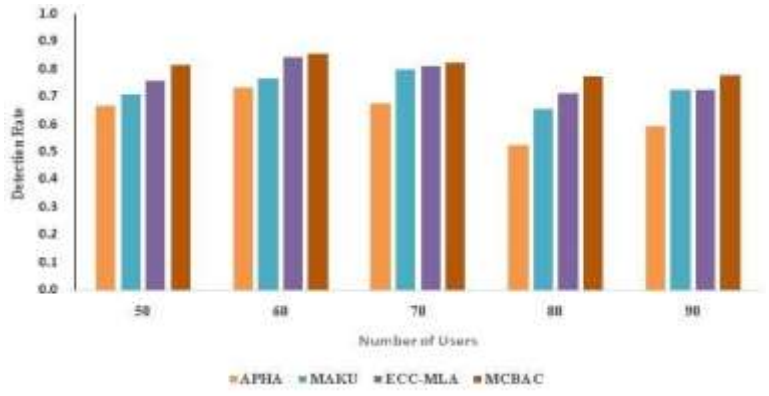

Figure 4: Comparative Analysis of Detection Rate in Terms of Password Guessing Attack

Comparative Analysis of the Proposed Method of Access Control in the Presence of Brute Force Attack

The evaluation criteria, including recall, precision, and detection rate in the context of brute force attack with varying user counts, are described in this section, that were used to compare the MCBAC's access control with current approaches.

Table 5: Comparative Evaluation of Accuracy When Brute Force Attack Is Present

Number of Users	Precision in Terms of Brute Force Attack			
	Existing Schemes			MCBAC
	APHA	MAKU	ECC-MLA	
50	0.692307	0.777778	0.869565	0.87652
60	0.8	0.828889	0.83	0.83103
70	0.666666	0.862068	0.869565	0.89474
80	0.635294	0.866666	0.874117	0.87556
90	0.629629	0.743589	0.875	0.88182

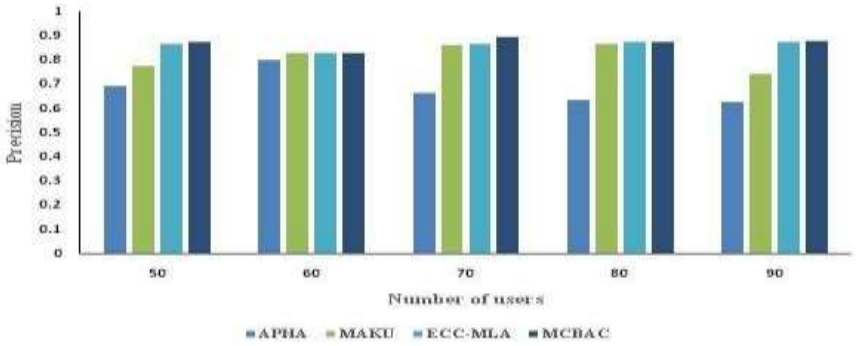

Figure 5: A Comparative Study of Precision When Brute Force Attack Is Present

Table 6: Comparative Evaluation of the Recall When Brute Force Attack Is Present

Number of Users	Recall in Terms of Brute Force Attack			
	Existing Schemes			MCBAC
	APHA	MAKU	ECC-MLA	
50	0.25	0.3889	0.55556	0.61111
60	0.24	0.46	0.68	0.74
70	0.15094	0.3774	0.6717	0.74151
80	0.19444	0.4444	0.65833	0.79722
90	0.28889	0.4222	0.43333	0.7888

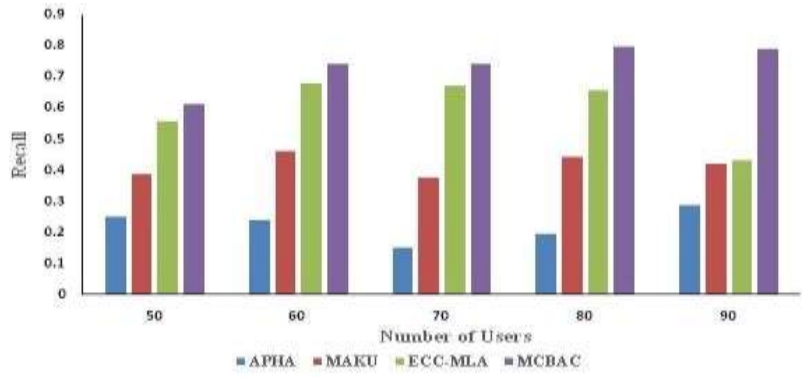

Figure 6: Evaluation of the Recall Comparatively When Brute Force Attack Is Present

Table 7: Comparative Evaluation of Detection Rates When Brute Force Attacks Are Present

Number of Users	Detection Rate in Terms of Brute Force Attack			
	Existing Schemes			MCBAC
	APHA	MAKU	ECC-MLA	
50	0.42593	0.51852	0.6481	0.72222
60	0.35938	0.46875	0.5469	0.70938
70	0.33784	0.51351	0.5676	0.78919
80	0.27381	0.5	0.5	0.73095
90	0.30851	0.43617	0.4468	0.70638

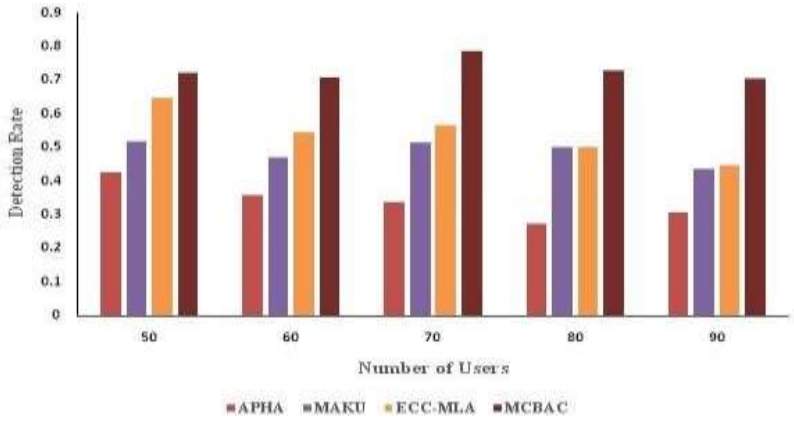

Figure 7: Analyzing Detection Rates Comparatively When Brute Force Attacks Are Present

Comparative Analysis of the Proposed Method of Access Control in the Presence of Dictionary Attack

Here we provide, using evaluation criteria like precision, recall, and detection rate in the context of a dictionary attack and varying user counts, a comparison of the MCBAC's access control with current approaches.

Table 8: Comparative Analysis of the Precision in the Presence of Dictionary Attack

Number of Users	Precision in Terms of Dictionary Attack			
	Existing Schemes			MCBAC
	APHA	MAKU	ECC-MLA	
50	0.6364	0.75	0.830769	0.8375
60	0.5	0.8077	0.815	0.82593
70	0.6	0.7857	0.814815	0.83333
80	0.7	0.8267	0.840952	0.856
90	0.625	0.8125	0.848485	0.85429

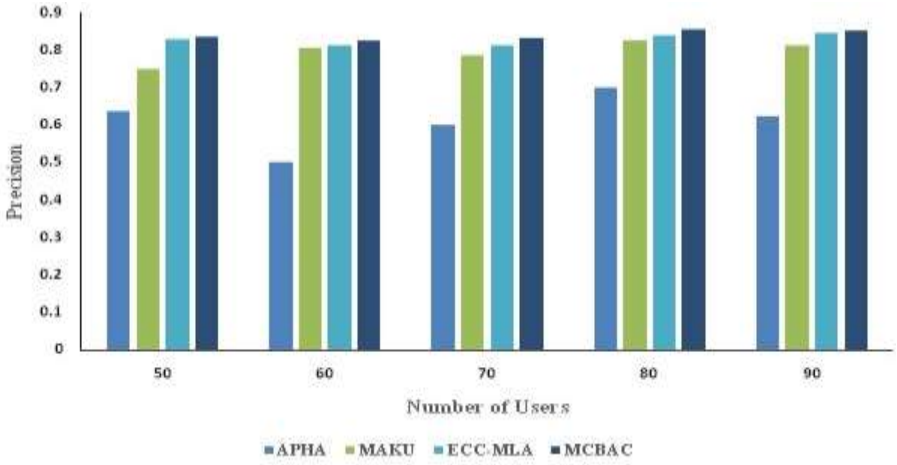

Figure 8: Comparison of the Accuracy When Dictionary Attack Is Present

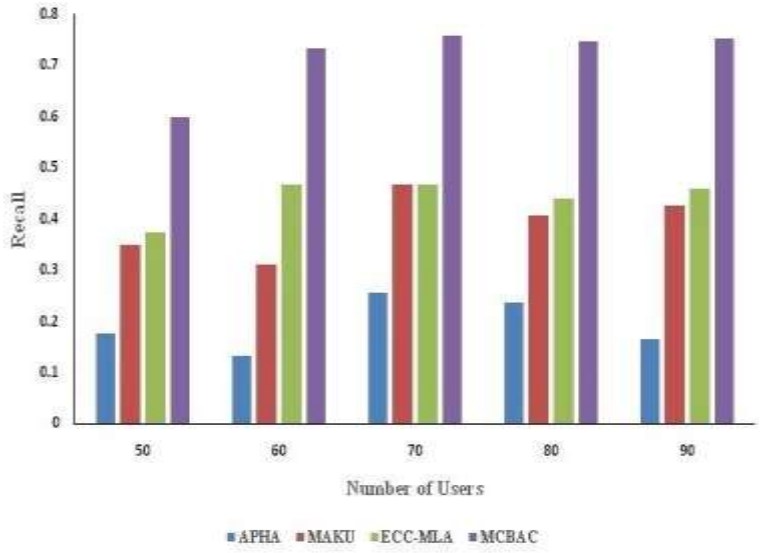

Figure 9: A Comparative Study of Recall When Dictionary Attack Is Present

Table 9: Comparative Analysis of the Recall in the Presence of Dictionary Attack

Number of Users	Recall in Terms of Dictionary Attack			
	Existing Schemes			MCBAC
	APHA	MAKU	ECC-MLA	
50	0.175	0.35	0.375	0.6
60	0.13333	0.3111	0.46667	0.73461
70	0.25532	0.4681	0.46809	0.75957
80	0.23729	0.4068	0.44068	0.74712
90	0.16393	0.4262	0.45902	0.75246

Table 10: Comparative Evaluation of the Detection Rate When Dictionary Attack Is Present

Number of Users	Detection Rate in Terms of Dictionary Attack			
	Existing Schemes			MCBAC
	APHA	MAKU	ECC-MLA	
50	0.31481	0.48148	0.5185	0.66667
60	0.29688	0.48438	0.5469	0.65625
70	0.41892	0.58108	0.5946	0.71622
80	0.39286	0.55952	0.5714	0.67857
90	0.39362	0.56383	0.5957	0.65957

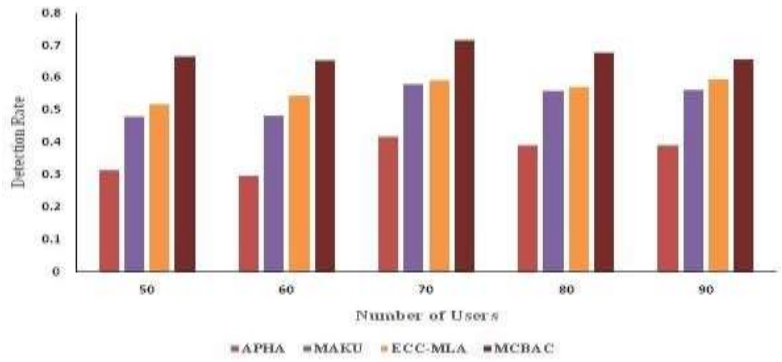

Figure 10: A Comparative Study of Detection Rates When Dictionary Attacks Are Present

Table 11: Comparative Analysis of the Access Control Phase Methods

Attacks	Metrics	Methods			
		APHA	MAKU	ECC-MLA	MCBAC
Password guessingattack	Precision	0.6909	0.6194	0.8355	0.8649
	Recall	0.7797	0.8644	0.8983	0.8983
	Detection rate	0.7344	0.7656	0.8438	0.8563
Brute force attack	Precision	0.6667	0.8621	0.8696	0.8947
	Recall	0.1944	0.4444	0.6583	0.7972
	Detection rate	0.3378	0.5135	0.5676	0.7892
Dictionary attack	Precision	0.625	0.8125	0.8485	0.8543
	Recall	0.2553	0.4681	0.4681	0.7596
	Detection rate	0.4189	0.5811	0.5946	0.7162

Conclusion

Every facet of social life and network systems is in a perpetual state of flux due to the exponential development of communication technologies. An example of how the ease of use of the internet has attracted many users is the fact that patients may get instantaneous medical advice via the system. They need to know which users have permission to access which types of data, so they implement fine-grained data access control when they publish data on cloud servers for sharing. For this reason, data owners should make use of the cloud's surplus resources to implement the access controls efficiently and affordably.

To top it all off, they have a greater responsibility to protect the privacy of the data stored on cloud servers. Confidentiality, hierarchical access control, forward security, data availability, and strong user and data authentication are all met by the privacy-enabled data preservation for the secured data access control system.

References

[1] Goundar, Sam. (2012). Cloud Computing: Understanding the Technology before Getting "Clouded". 10.1007/978-3-642-28798-5_30.

[2] Mushtaq, Muhammad & Akram, Urooj & Khan, Irfan & Khan, Sundas & Shahzad, Asim & Ulah, Arif. (2017). Cloud Computing Environment and Security Challenges: A Review.

[3] Dahiya, Vandna & Dalal, Sandeep. (2018). Fog Computing: A Review on Integration of Cloud Computing and Internet of Things. 10.1109/SCEECS.2018.8546860.

[4] Kumar, Kiran. (2012). Security Issues in Cloud Computing Technology, Attributes and concerns towards it.

[5] B. Prabadevi and N. Jeyanthi, "Distributed denial of service attacks and its effects on cloud environment- a survey," The 2014 International Symposium on Networks, Computers and Communications, 2014.

[6] B. Alouffi, M. Hasnain, A. Alharbi, W. Alosaimi, H. Alyami, and M. Ayaz, "A systematic literature review on cloud computing security: threats and mitigation strategies," IEEE Access, vol. 9, pp. 57 792– 57 807, 2021.

[7] P. Akello, N. L. Beebe, and K.-K. R. Choo, "A literature survey of security issues in cloud, fog, and edge it infrastructure," Electronic Commerce Research, pp. 1–35, 2022.

[8] M. Humayun, M. Niazi, N. Jhanjhi, M. Alshayeb, and S. Mahmood, "Cyber security threats and vulnerabilities: a systematic mapping study," Arabian Journal for Science and Engineering, vol. 45, pp. 3171–3189, 2020.

[9] R. Shaikh and M. Sasikumar, "Security issues in cloud computing: A survey," International Journal of Computer Applications, vol. 44, no. 19, pp. 4–10, 2012.

[10] N. Kumar and J. K. Samriya, "Security issues in cloud computing: A survey."

[11] Patel, N. Shah, D. Ramoliya, and A. Nayak, "A detailed review of cloud security: issues, threats & attacks," in 2020 4th International conference on electronics, communication and aerospace technology (ICECA). IEEE, 2020, pp. 758–764.

[12] H. Tabrizchi and M. Kuchaki Rafsanjani, "A survey on security challenges in cloud computing: issues, threats, and solutions," The journal of supercomputing, vol. 76, no. 12, pp. 9493–9532, 2020.

[13] Sharma, U. K. Singh, K. Upreti, and D. S. Yadav, "An investigation of security risk & taxonomy of cloud computing environment," in 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC). IEEE, 2021, pp. 1056–1063.

[14] R. M. Jabir, S. I. R. Khanji, L. A. Ahmad, O. Alfandi, and H. Said, "Analysis of cloud computing attacks and countermeasures," in 2016 18th international conference on advanced communication technology (ICACT). IEEE, 2016, pp. 117–123.