

Authentication and authorization models for high-security cloud platforms

Neeraj Kumar Verma [#]

Department of Data Science

Manipal University Jaipur

Jaipur 303007

Rajasthan

India

Nancy Arya ⁺

Department of Computer Science and Engineering

School of Engineering & Sciences

GD Goenka University

Sohna 122103

Haryana

India

Niroj Kumar Pani [§]

Department of Computer Science Engineering and Applications

Indira Gandhi Institute of Technology

Sarang 759146

Odisha

India

Jhum Swain [‡]

Department of Computer Science and Engineering - Data Science

Swami Vivekananda Institute of Technology

Hyderabad 500003

Telangana

India

[#] E-mail: er.neerajkumar@gmail.com

⁺ E-mail: nancy.arya@gdgu.org

[§] E-mail: nirojpani@gmail.com

[‡] E-mail: jhumswain4321@gmail.com

Narendra Babu Tatini [®]
SASI Foundation
Velivenu
East Godavari 534329
Andhra Pradesh
India

Ajit Noonian*
Department of Computer Science and Engineering
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

Abstract

In a technology marked by way of the relentless march of technology and the ever-increasing digitization of our lives, the concept of identity and comfy entry to virtual assets has turned out to be a trouble of paramount significance. E-authentication, or electronic authentication, emerges as the linchpin of this digital age, acting as the gatekeeper to the large panorama of online offerings, touchy records, and digital interactions. E-authentication, or electronic authentication, plays a crucial role in ensuring secure access to cloud computing resources and safeguarding against unauthorized access and potential cyber threats. In a digital age where the availability of data and trustworthy transactions are at the very core of contemporary lifestyles, e-authentication structures serve as vital watchdogs guarding the virtual realm's gates. This summary gives an overview of all aspects of e-authentication, accentuating its significance, types, technology, and important role in ensuring the confidentiality and accessibility of internet-based sources. We will navigate through the history of e-authentication, analyze the many authentication methodologies, investigate the technology that powers it, and consider the more general implications of its use in the contemporary world. This investigation aims to explain the complicated fabric of e-authentication, putting lighter on its evolution and ever-growing importance in today's digitalized world.

Subject Classification: Primary 93A30, Secondary 49K15.

Keywords: Cloud services, E-authentication, Resource provisioning, Computing security, Cloud simulators.

[®] E-mail: tatininarendra@gmail.com

* E-mail: ajit009noonia@gmail.com; (Corresponding Author)
ajit.noonia@jaipur.manipal.edu

1. Introduction

The advent of this paper sets the level for a comprehensive exploration of e-authentication structures, their significance in our contemporary society, and their essential role in ensuring the integrity, confidentiality, and availability of digital belongings [1-2]. E-authentication isn't simply a matter of convenience, however, an essential issue of virtual protection that has far-reaching implications for people, corporations, and governments alike [3-4]. In the following sections, we will embark on a journey through the intricacies of e-authentication. Furthermore, we can recall the regulatory framework that governs e-authentication and the ethical concerns surrounding its use as shown in Figure 1. The research also considers the role of identity management systems in orchestrating e-authentication across diverse cloud services [5-6]. It addresses the integration challenges associated with hybrid and multi-cloud environments, emphasizing the need for standardized protocols and interoperability [7].

2. Related Work

Before the appearance of state-of-the-art digital authentication systems, traditional authentication methods formed the muse of digital get admission to manipulate [8-9]. These strategies were necessitated by the rapid boom of virtual technologies and the increasing want for comfortable entry to laptop systems, networks, and touchy data. Passwords emerged because of the pioneering authentication approach. They have been simple but effective. customers were required to input a mystery

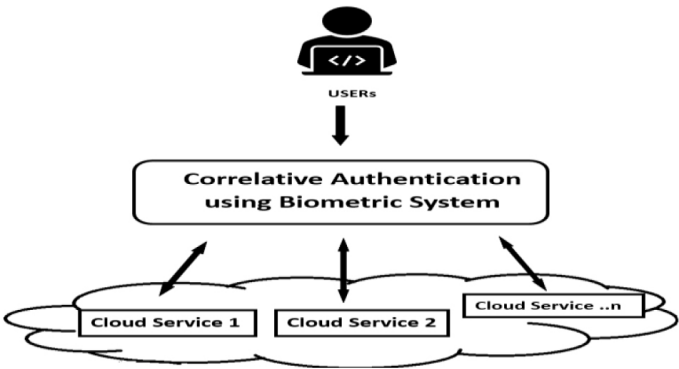


Figure 1
Basic Structure of E Authentication System

string of characters (the password) recognized best to them to advantage get admission to [10-11]. The need for passwords changed into pushed by way of numerous elements like multi-user computer structures, it was critical to characteristic actions and modifications to specific users. Passwords allowed systems to establish person duty [8-10]. As virtual records have become more widespread, defensive touchy statistics from unauthorized get admission to become a paramount problem. Passwords served as the first line of protection. Companies and establishments wanted a manner to govern who may want to get admission to their laptop systems [12-13]. Passwords furnished a mechanism to supply or deny get right of entry to unique people. The appearance of biometric technologies has no longer only more advantageous protection but also advanced person comfort. Governments and economic institutions performed a pivotal role in advancing e-authentication structures [14-15]. The want for relaxed get right of entry to sensitive government offerings, online tax submitting, and comfy financial transactions drove innovation in e-authentication. digital signatures and comfy identification verification methods have become vital additives of e-authorities and online banking [16-17].

3. Challenges in e-authentication detection

The historic adventure of e-authentication systems has been marked by means of widespread improvements, but it has additionally encountered

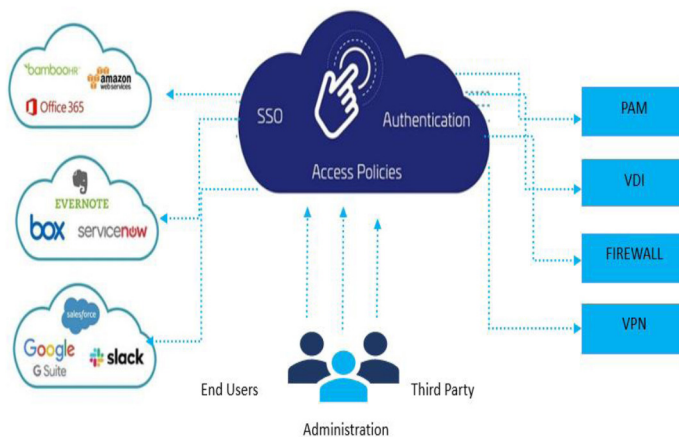


Figure 2

Cloud Security Model Using E-authentication

demanding situations consisting of evolving cybersecurity threats and the want to stability protection with user comfort [18-19]. The future of e-authentication holds promise with rising technologies like blockchain-based identity verification and the continuing integration of biometrics into normal gadgets [20-21]. Understanding this historical context is essential for appreciating the present-day landscape of e-authentication and watching for the revolutionary solutions that will form its future [22-23]. As we delve deeper into the various aspects of e-authentication in the following Figure 2, we can gain a complete angle on its evolution and significance in the digital age [24-25].

4. Proposed Methodology

This improves user experience while ensuring that strong authentication measures are applied at the initial login. Use token-based authentication mechanisms, such as OAuth or OpenID Connect, to manage secure access to cloud services. To authenticate once and gain access to multiple cloud services seamlessly shown in Figure 3. Tokens provide a way to authenticate users without exposing sensitive credentials during communication. Implement identity federation to enable users to use their existing credentials from one trusted identity provider across multiple cloud services. This reduces the need for users to maintain multiple sets of credentials.

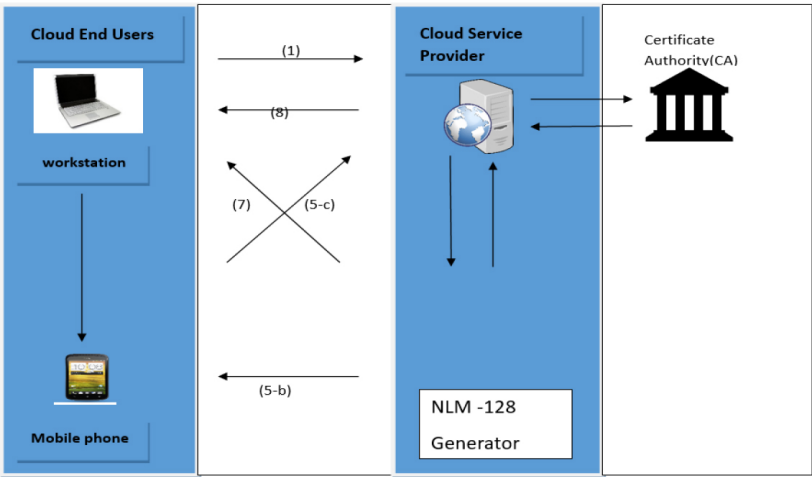


Figure 3
Authentication Framework of E-Authentication

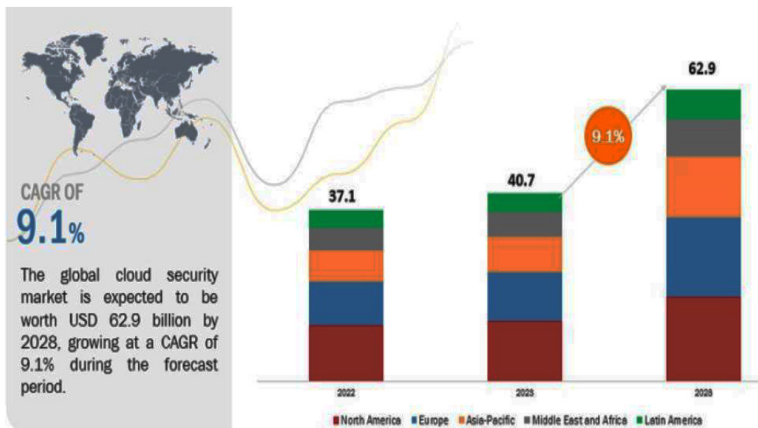


Figure 4

Analysis of Global Cloud Security Market

By adopting a comprehensive approach that combines these strategies, organizations can establish a strong foundation for secure e-authentication in their cloud computing services.

5. Result Analysis

The effective law of digital authentication (e-authentication) is vital to keep accepted as true within digital interactions and shield the rights and privateness of individuals and groups shown in Figure 4.

This chapter explores the regulatory framework surrounding e-authentication, encompassing worldwide, country-wide, and industry-specific regulations shown in Figure 5. Numerous worldwide groups and agreements set up concepts and recommendations for e-authentication on a global scale.

6. User experience and usability

Inside the realm of digital authentication (e-authentication), security is paramount, however, it must in no way come at the cost of user enjoy and value. This bankruptcy explores the vital intersection of consumer level in (UX) and value in e-authentication structures, emphasizing the importance of designing solutions which can be comfy and consumer-friendly.

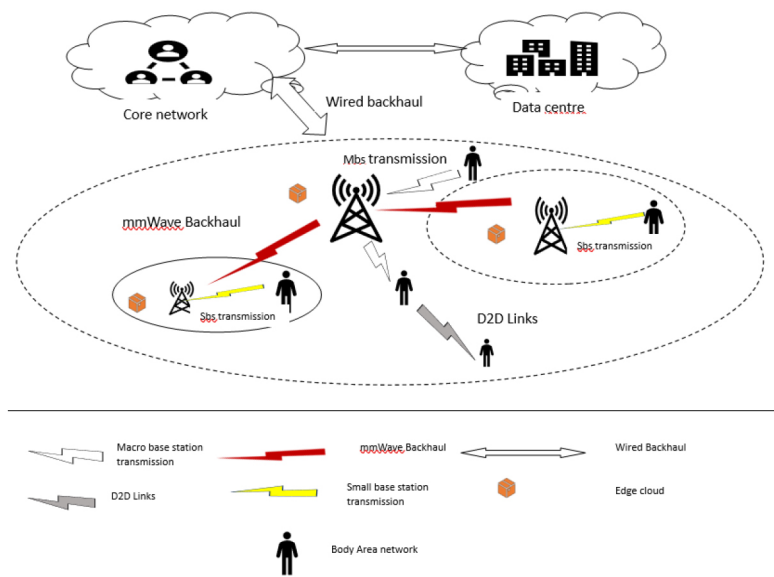


Figure 5
5G E-authentication System

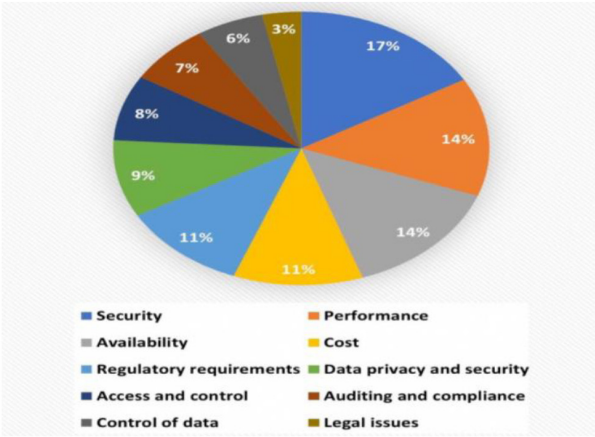


Figure 6
Result Overview of Various Issues Involved in a Cloud Computing System

The consumer level encompasses all components of an individual's interaction with an e-authentication system, which includes how they perceive its ease of use, performance, and ordinary pleasure described in Figure 6.

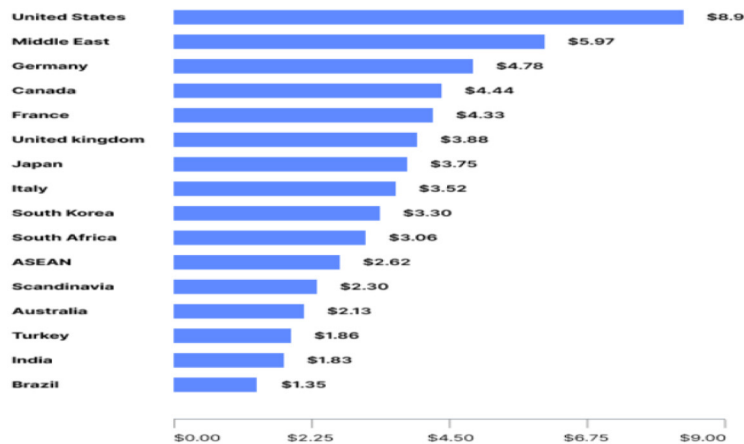


Figure 7
Analysis of Cloud Data Breach

Designing interfaces with the right comparison, scalable fonts, and keyboard navigation for customers with disabilities. Powerful conversation with users is fundamental to a fine e-authentication level explained in Figure 7. Navigating the complicated e-authentication landscape will require a blend of technological advancements, regulatory compliance, and a dedication to supplying relaxed and person-pleasant studies in the digital realm.

7. Conclusion and Future Work

E-authentication serves because it is the gateway to a mess of online services, safeguarding touchy statistics, financial transactions, and personal facts. It concurrently bridges the gap between protection and user experience, placing a sensitive stability that is critical for good-sized adoption. From conventional methods like password-based totally authentication to cutting biometrics and decentralized identity solutions, the area of e-authentication is constantly evolving. As we peer into the future, it’s evident that quantum-safe encryption, AI-pushed authentication, and password-less get entry to will redefine how we verify identities inside the virtual realm. In closing, e-authentication isn’t always a solitary pursuit but a collective undertaking that impacts us all. Its continued evolution holds the promise of a comfortable and user-friendly digital global, in which accept as true within online interactions is

unwavering. As we navigate the intricacies of e-authentication, it's far imperative to remain adaptable, innovative, and devoted to the beliefs of protection, accessibility, and person empowerment. The adventure of e-authentication continues, and its destination holds the capacity for a safer and greater related destiny.

References

- [1] A. K. Singh, A. Nayyar, and A. Garg, "A Secure Elliptic Curve Based Anonymous Authentication and Key Establishment Mechanism for IoT and Cloud," *Multimedia Tools and Applications*, vol. 82, no. 15, pp. 22525–22576 (2023).
- [2] A. Tiwari and R. M. Sharma, "Realm Towards Service Optimization in Fog Computing," in *Research Anthology on Architectures, Frameworks, and Integration Strategies for Distributed and Cloud Computing*, I. Management Association, Ed., pp. 1530–1563 (2021).
- [3] U. Fatima and S. Parveen, "A Review Article on Authentication Protocols in Cloud Computing," *International Journal of Engineering and Management Research*, vol. 13, no. 2, pp. 225–231 (2023).
- [4] D. Dudeja, S. M. Sabharwal, Y. Ganganwar, M. Singhal, N. Goyal, and A. Tiwari, "Sales-Based Models for Resource Management and Scheduling in Artificial Intelligence Systems," *Engineering Proceedings*, vol. 59, no. 1, p. 43 (2023).
- [5] P. K. Srivastava, S. Kumar, A. Tiwari, D. Goyal, and U. Mamodiya, "Internet of Thing Uses in Materialistic Ameliorate Farming Through AI," in *AIP Conference Proceedings*, vol. 2782, no. 1, AIP Publishing (Jun. 2023).
- [6] A. B. Pawar, S. U. Ghumbre, and R. M. Jogdand, "Privacy Preserving Model-Based Authentication and Data Security in Cloud Computing," *International Journal of Pervasive Computing and Communications*, vol. 19, no. 2, pp. 173–190 (2023).
- [7] C. T. Dora Pravina, M. U. Buradkar, M. K. Jamal, A. Tiwari, U. Mamodiya, and D. Goyal, "A Sustainable and Secure Cloud Resource Provisioning System in Industrial Internet of Things (IIoT) Based on Image Encryption," in *Proceedings of the 4th International Conference on Information Management & Machine Intelligence*, pp. 1–5 (Dec. 2022).

- [8] A. H. Gamlo, "A Trust-based Elastic and Dynamic Authentication Solution for Multi-Cloud Computing," Ph.D. dissertation, University of Manchester (2023).
- [9] V. V. Rohinidevi, P. K. Srivastava, N. Dubey, S. Tiwari, and A. Tiwari, "A Taxonomy Towards Fog Computing Resource Allocation," in 2022 2nd International Conference on Innovative Sustainable Computational Technologies (CISCT), pp. 1–5, IEEE (Dec. 2022).
- [10] D. Sudarsa and A. P. Sivakumar, "An effective and Secured Authentication and Sharing of Data with Dynamic Groups in Cloud," *Data & Knowledge Engineering*, vol. 145, p. 102125 (2023).
- [11] N. K. Singh, A. Jain, S. Arya, W. E. G. Gonzales, J. E. A. Flores, and A. Tiwari, "Attack Detection Taxonomy System in Cloud Services," in 2022 2nd International Conference on Innovative Sustainable Computational Technologies (CISCT), pp. 1–5, IEEE (Dec. 2022).
- [12] G. A. Qadir and B. K. Hussan, "An Authentication and Access Control Model for Healthcare based Cloud Services," *Journal of Engineering*, vol. 29, no. 3, pp. 15–26 (2023).
- [13] A. Tiwari and R. Garg, "ACCOS: A Hybrid Anomaly-Aware Cloud Computing Formulation-Based Ontology Services in Clouds," in ISIC, pp. 341–346 (2021).
- [14] S. Radha and S. Jeyalakshmi, "Deterministic Hash and Linear Congruential BlowFish Extreme Learning for User Authentication in Cloud Computing," *SN Computer Science*, vol. 4, no. 6, p. 796 (2023).
- [15] A. Tiwari, M. Mahrishi, and S. Fatehpuria, "A Broking Structure Originated on Service Accommodative using MROSP Algorithm," unpublished (2014).
- [16] A. Kumar Sharma, A. Tiwari, B. Bohra, and S. Khan, "A Vision towards Optimization of Ontological Datacenters Computing World," *International Journal of Information Systems & Management Science*, vol. 1, no. 2 (2018).
- [17] A. Tiwari and R. M. Sharma, "A Skywatch on the Challenging Gradual Progression of Scheduling in Cloud Computing," in Applications of Computing, Automation and Wireless Systems in Electrical Engineering: Proceedings of MARC 2018, pp. 531–541, Springer Singapore (2019).
- [18] Y. V. Rangaiah, A. K. Sharma, T. Bhargavi, M. Chopra, C. Mahapatra, and A. Tiwari, "A Taxonomy towards Blockchain based Multimedia

- content Security,” in 2022 2nd International Conference on Innovative Sustainable Computational Technologies (CISCT), pp. 1–4, IEEE (Dec. 2022).
- [19] A. Tiwari and R. M. Sharma, “Realm Towards Service Optimization in Fog Computing,” *International Journal of Fog Computing (IJFC)*, vol. 2, no. 2, pp. 13–43 (2019).
- [20] M. K. Sah, V. Kumar, and A. Tiwari, “Security and Concurrency Control in Distributed Database System,” *International Journal of Scientific Research and Management*, vol. 2, no. 12, pp. 1839–1845 (2017).
- [21] A. Tiwari and R. Garg, “Eagle Techniques in Cloud Computational Formulation,” *International Journal of Innovative Technology and Exploring Engineering*, vol. 8, no. 1, pp. 422–429 (2019).
- [22] A. Tiwari, S. Kumar, N. Baishwar, S. K. Vishwakarma, and P. Singh, “Efficient Cloud Orchestration Services in Computing,” in *Proceedings of 3rd International Conference on Machine Learning, Advances in Computing, Renewable Energy and Communication: MARC 2021*, pp. 739–746, Springer Nature Singapore (Sep. 2022).
- [23] R. Manikandan, R. K. Maurya, T. Rasheed, S. C. Bose, J. L. Arias-González, U. Mamodiya, and A. Tiwari, “Adaptive Cloud Orchestration Resource Selection using Rough Set Theory,” *Journal of Interdisciplinary Mathematics*, vol. 26, pp. 311–320 (2023).
- [24] A. Tiwari and R. M. Sharma, “Rendering Form Ontology Methodology for IoT Services in Cloud Computing,” *International Journal of Advanced Studies of Scientific Research*, vol. 3, no. 11 (2018).
- [25] B. Mallikarjuna, A. Noonina, G. Berar, L. Rani, K. N. Tripathi, and S. Sebastian, “Comparing the Roles of Cryptography and Blockchain Technology in Relation to Internet of Things,” *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 27, no. 7, pp. 1015–1025 (2024).

Received November, 2024