International Journal of Computing Sciences Research (ISSN print: 2546-0552; ISSN online: 2546-115X)
Vol. 9, pp. 3591-3601
doi: 10.25147/ijcsr.2017.001.1.233
https://stepacademic.net

Concept Paper

A Paradigm Shift in Identity: Conceptualizing Passwordless Authentication using Hashgraph Technology

Christopher Edmund B. Navarro
School of Graduate Studies, AMA Computer University, Philippines
ejnavarro06@gmail.com
(corresponding author)

Jeffrey T. Leonen
School of Graduate Studies, AMA Computer University, Philippines
jtleonen@amaes.edu.ph

Date received: May 20, 2024
Date received in revised form: May 27, 2024; January 29, 2025
Date accepted: February 2, 2025

Recommended citation:

Navarro, C. E., & Leonen, J. T. (2025). A paradigm shift in identity: Conceptualizing passwordless authentication using hashgraph technology. *International Journal of Computing Sciences Research,9,* 3591-3601. https://doi.org/10.25147/ijcsr.2017.001.1.233

Abstract

Purpose – This concept paper uniquely explores the novel application of hashgraph technology in the passwordless authentication realm. Hashgraph algorithm is known for its performance, stability, and security. It achieves the gold standard for security by differentiating itself by focusing on integrating asynchronous Byzantine Fault Tolerance (aBFT) and the gossip protocol for enhanced resilience and scalability. Unlike existing discussions, this study highlights how hashgraph's unique attributes overcome key challenges in digital identity management, providing a paradigm shift from traditional and even next-generation authentication methods.

Method – This study will synthesize current literature and technological advancements in both passwordless authentication and distributed ledger technologies (DLTs).

Conclusion – Hashgraph technology offers a groundbreaking approach to passwordless authentication, effectively addressing the limitations of traditional and next-generation methods. Its features—such as asynchronous Byzantine Fault Tolerance (aBFT), the gossip protocol, and decentralized identifiers (DIDs)—make it highly secure, scalable, and user-friendly. By removing dependency on passwords, this approach enhances both

privacy and resilience against digital attacks. This paradigm shift can lead to more robust and structured digital identity systems, rethinking cybersecurity standards.

Recommendations – To fully realize the potential of hashgraph in passwordless authentication, it is essential to develop a prototype to validate the proposed framework and conduct large-scale testing to assess its scalability and real-world reliability. Developing a seamless integration of this technology with existing authentication systems and ensuring compatibility with current platforms will be critical to driving adoption. Moreover, user awareness campaigns must address potential resistance to change and promote understanding of the potential benefits of this technology.

Research Implications – This study on passwordless authentication using hashgraph technology has significant implications for the future of digital identity management, offering enhanced security and user experience while promoting decentralized identity systems across various sectors. Vital areas for further research include addressing integration challenges, user adoption, data privacy concerns, and the technology's potential in an evolving cybersecurity landscape.

Practical Implications – Hashgraph-based authentication offers significant practical benefits, including enhanced security, reduced operational costs, and an improved user experience with seamless, privacy-centric processes. The properties like low latency and scalability will make it ideal for large-scale applications, potentially reshaping cyber security and digital identity standards for a more secure and user-focused.

Keywords – identity, passwordless authentication, hashgraph algorithm, gossip protocol, asynchronous byzantine tolerance(aBFT), DLTs, digital identity management

INTRODUCTION

What is Identity? On the surface, it is a simple question that often elicits complex answers, as the word "identity" can mean and be used in different ways in different contexts. Identity theories generally agree that the identity of a person comes to hold through their unique values and interpretations of the events in their life can help explain people's behavior, Meltzer et al. (2020). On a personal level, identity often refers to a person's name and other facts about who they are. In the realm of technology, identity is known as digital identity, and it is the user's digital behavior, the online role of a user using online resources - in a nutshell, it is the user's digital version of their human identity.

In today’s cybersecurity landscape, digital identity plays a pivotal role in ensuring secure interactions across digital platforms. Central to this is verifying user authenticity and defining their access privileges—a challenge compounded by the vulnerabilities of traditional authentication methods. Understanding that basic assumption that in

cyberspace (a generic name for all online or electronic platforms) we all are attractive targets for attacks by cybercriminals. The intended objects could be our money or data and also range from usernames, passwords, or online presence among others, Sule et al. (2023).

Traditionally, to confirm one's digital identity, user authentication relied heavily on knowledge-based credentials also often referred to as one-factor authentication or "what you know" which requires the user to share a username and password. Then technology exploded and went faster or even beyond the speed of sound – new security vulnerabilities were identified, security breaches were everywhere then three-factor authentication was introduced – "Something you know", "Something you have", and "Something you are". In spite of the good intentions to secure everybody - there are still prevalent limitations such as in SMS OTP(sim-swaps), enhanced password authentication (passwords with texts, numbers, and special characters), and hardware integration issues. To keep up with the cybersecurity landscape, a new security alliance was formed – FIDO (Fast Identity Alliance) – their mission is to promote new authentication standards, and they have confirmed that passwords and other forms of authentication within the context of knowledge-based will always introduce issues such as a hassle to remember, easy to phish, harvest and replay.

Figure 1. Shows the current authentication methods. It displays a wide range of authentication methods starting from traditional Username/Password, Pattern-based, SMS-OTP, Biometrics, Quick Response (QR) codes, Radio Frequency Identification (RFID), and Next-generation authentication.

Figure 1. Current Authentication Methods

Google Cloud's 2023 Threat Horizons Report found that more than 80% of security breaches involved stolen credentials, and credentials issues account for over 60% of compromise factors - - which could be addressed by stronger identity management guardrails in place at the organization level.

Given the security vulnerabilities and limitations of the existing authentication methods, while existing studies explore passwordless authentication using technologies like biometrics, single sign-on (SSO), and public-key cryptography, this concept paper is the first to propose hashgraph technology as a foundational framework for overcoming current limitations. Unlike blockchain or other distributed ledger technologies, hashgraph offers unparalleled efficiency, fairness, and security through its aBFT mechanism and gossip protocol. By examining its unique capabilities, this work aims to set a new direction for discussions in identity verification systems.

LITERATURE REVIEW

Next-generation password authentication methods gained an increase of interest and traction within recent years. In today's digital landscape, increasing security while maintaining user convenience is critical. The first usage of digital passwords at Massachusetts Institute of Technology in the 1960s by then Professor Fernando Corbato for the Compatible Time-Sharing System (CTSS). For the users to use the said machine, several users needed their clear text private access to the terminal, in just a little of 2 years – in 1962, the first password-based data breach was recorded when Allen Scherr launched a cyber attack on MIT computer networks and stealing passwords from their database via a punch card, Wolf, A. (2024). Since then, technology has come a very long way – different hashing algorithms were developed and became popular and used as a tool to secure clear text passwords and that includes features such as one-way, faster computation, deterministic cryptography, avalanche effect, and long impact resistance, Anwar, M. R., et al. (2021).

Almost 4 decades later, the birth of Two-Factor Authentication (2FA) or Multi Password Authentication (MFA) was developed, while the origins of this authentication method are up for debate, most people agree it was invented in the late 1990s by AT&T wherein the patent was granted in 1998. The popularity of smartphones triggered the need to be security-conscious where an increase in digital footprint began to be proportional to an increase in new cybersecurity attacks. 2FA/MFA are not immune to security loopholes such as Sim-swaps, Identity Theft, Fake Apps, and Phishing Attacks.

Markets and Markets (2023) and SPECOPS (2024) highlight that 88% of organizations still use passwords as their primary method of authentication and published a report on 2FA/MFA Market size where it hits 15.2% and expected growth of 34.8% in the next 4 years. However, research found that almost 51% of people still use the same password for their work and personal accounts, Todorov, G. (2023). One of the reasons why users still use or re-use the same password is due to the human nature factor being forgetful. Nari, T.J. (2023) conveys that forgetfulness of being is the biggest threat to humanity.

Gordin, I. et al. (2021) exemplify that though the most used type of authentication even today is done by using a username and password, and with the emergence of multi-

factor authentication (MFA) that came as the next level of authentication, there are still user resistance to change due to frustration with the additional security feature on top of having to remember their passwords. Passwordless authentication is more convenient because the password now is removed and replaced with "something you have", and it cannot be forgotten.

Parmar, V., et al. (2022) emphasized that Passwordless authentication improves security, increases brand effectiveness, and saves valuable IT resources by eliminating the use of passwords. Single sign-on (SSO), traditional multi-factor authentication (MFA), and similar methodologies have their legacy benefits, but they can all be circumvented through methods such as phishing, keylogging, password spray, or brute force attacks.

CURRENT PASSWORDLESS AUTHENTICATION METHODS

Passwordless authentication methods have emerged as a promising alternative to traditional password-based systems, addressing issues of usability, security, and user frustration. These methods eliminate the need for knowledge-based credentials by leveraging factors such as possession such as tokens, devices, or biometrics. Below, we discuss two prominent approaches—Magic Email Links and Time-based OTPs (TOTPs)—along with their advantages and limitations in the current cybersecurity landscape.

1. MAGIC EMAIL LINKS – Magic Email Links are a simple passwordless authentication mechanism wherein users authenticate themselves by clicking on a unique link sent to their registered email address. This approach replaces passwords with a possession factor like email account access. Below are its advantages and disadvantages:

Figure 2. Email-based passwordless authentication process

One of the main advantages of using email-based passwordless authentication is its fast and simple onboarding process, similar to a "forget-password" workflow. Users do not need to worry about maintaining password storage, avoiding the risk of password-related security breaches. Additionally, there is no dependency on other external hardware making it more convenient for users. However, there are some drawbacks to this method. It is entirely email-dependent, which can lead to unwanted or spam messages. There is also limited visibility for users regarding the authentication process,

and the security of the system is tied to the email account, which could become a vulnerability if the email is compromised.

2. Time-based OTPs (TOTPs) - Time-based One-Time Passwords (TOTPs) rely on a shared secret between the user and the authentication provider, combined with the current timestamp to generate a one-time use coded password. This is often implemented through hardware tokens or mobile authenticator apps. Below are its advantages and disadvantages:

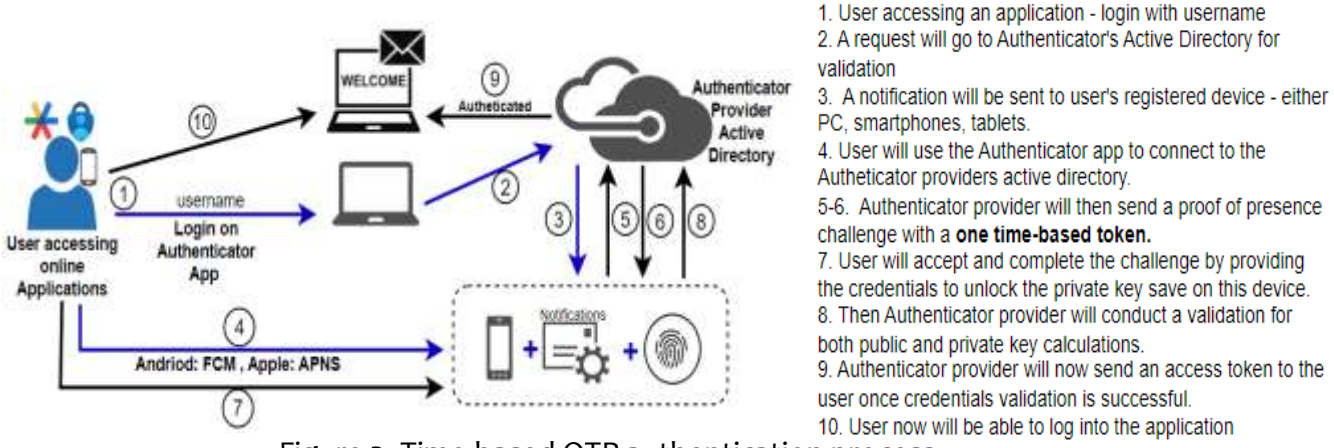

Figure 3. Time-based OTP authentication process

One of the key advantages of time-based OTP (TOTP) authentication is its high level of security, as it is not easily compromised. It is also versatile, allowing users to access multiple applications with ease, and can be used even when the user is offline, adding to its convenience. However, there are some disadvantages associated with this method. It is device-dependent, meaning users need a specific device to generate the OTP. Additionally, it requires some technical know-how to set up and use properly. The authenticator provider can revoke access at any time, and there is little visibility into how the provider manages or stores the keys, which may raise concerns about security and transparency.

THEORETICAL FRAMEWORK

Hashgraph like any other Distributed Ledger Technology (DLT) like Blockchain utilizes a peer-to-peer network, however, Hashgraph is not using a chain or tree of blocks instead using a graph-like structure where all nodes communicate with each other using Gossip Protocol, Baird, et al. (2019). This concept paper was driven by a new form of digital identity based on emerging standards such as Verifiable Credentials and Decentralized Identifiers that can enable a user's digital identity to work everywhere, be more trustworthy, and ensure privacy, Sporny et. Al. (2024). A user-centric identity – seeking to give end users greater control over the sharing of their information.

In this conceptual framework, there are three parties within the chain of trust: **Issuer** - Typically who creates or issues the verifiable credentials to the user or subject. Like Governments, Companies, or Universities. The issuer is the one that can assert the accuracy of data or information about the user or subject. **Subject** - It pertains to the users like students, employees, or people. **Verifier** – It is an accredited service, server, entity, or institution that can verify the authenticity of a verifiable identification or user's digital certificate presented during authentication.

The high-level framework for passwordless authentication using hashgraph technology involves multiple steps and entities working together to establish a seamless and secure authentication process. Below, we outline the key steps involved in this framework, demonstrating how hashgraph's unique properties are utilized to ensure secure digital identity management.

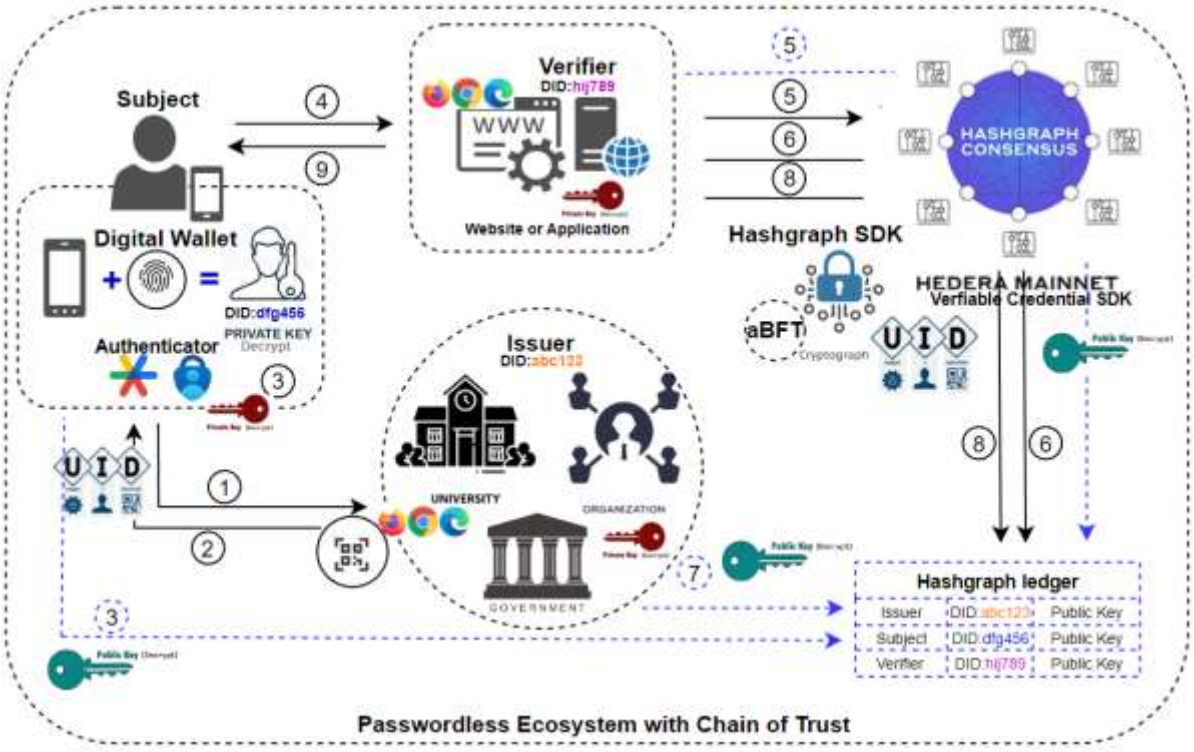

Figure 4. High-level Framework for Passwordless Authentication using Hashgraph

The process of passwordless authentication using hashgraph technology begins with the (1) user retrieving verifiable credentials from a trusted authority, such as a government or university, through their website or system. (2) These credentials can be downloaded via QR code using a supported authenticator app. Once obtained, (3) the credentials are securely stored in the user's digital wallet, which is protected by biometric proof, ensuring that only the user can access their private key. When the user needs to access an application or website, such as submitting school-related information like diplomas or certificates to a company or university, (4) they only need to provide their

name as initial proof of identity, assuming both the company and university are part of the passwordless ecosystem. (5) Hashgraph then generates a unique decentralized identifier (DID) and public key for the user, which is published on the hashgraph ledger for verification. (6) The verifier can then validate the DIDs and associated public keys of both the issuer and the subject on the ledger. (7) Once the issuer confirms the verifiable credentials, a uniquely paired public key is added to the ledger, and both the issuer and verifier agree on the verification process. (8) The verifier cross-checks the ledger, and the hashgraph algorithm confirms the subject's credentials to the web server or application. Finally, (9) the subject gains access to the website or application without the need for a username or password, completing the authentication process seamlessly.

CONCLUSIONS AND RECOMMENDATIONS

This concept paper presents a promising approach to passwordless authentication using hashgraph technology, with the potential to enhance security and user experience significantly. The proposed system offers a robust alternative to traditional methods, addressing current limitations. One of the biggest takeaways from this concept paper is that the user is in control of its information which then unlocks a more trustworthy internet concerning privacy. Future research should focus on developing a prototype, conducting large-scale testing, and exploring integration with existing authentication systems. Overcoming challenges such as scalability, integration with existing systems, and user education need to be addressed to realize the full potential of hashgraph-based authentication.

IMPLICATIONS

The practical implications of hashgraph-based authentication are significant, including enhanced system security, scalability, reliability, and improved user experience through seamless and privacy-centric authentication processes. This innovative solution has the potential to redefine cybersecurity and digital identity standards, paving the way for a more secure and user-focused internet.

ACKNOWLEDGEMENT

We would like to extend our appreciation to the individuals and professional colleagues who have played a significant role throughout the creation of this concept paper.

First and foremost, sincere gratitude to our research adviser, Engr. Jeffrey T. Leonen, for his expert guidance, invaluable insights, and consistent support, which have played a pivotal role in shaping this work.

Finally, I would like to express my deepest gratitude to my family for their unwavering love and support throughout this journey. To my incredible wife, Lorly

Navarro, and my wonderful children, Gaud Tywin and Gabe Julieanne, your constant encouragement, patience, and understanding have been a source of strength and inspiration. I am also profoundly grateful to my mother for her unconditional love, guidance, and belief in me.

FUNDING

The study did not receive funding from any institution, entity, or organization.

DECLARATIONS

Conflict of Interest

I affirm there are no conflicts of interest that could influence the outcomes or objectives of this study. I have no personal or financial connections with any individuals, entities, or institutions that might compromise the impartiality of this research. This commitment ensures the research remains unbiased and credible.

Informed Consent

In this study, we will ensure that all participants provide their informed consent. It is important to us that they fully understand the purpose of the study, the procedures involved, as well as any potential risks and benefits. Participants were given a clear explanation of their rights, and we will emphasize that their participation is entirely voluntary. We are committed to maintaining confidentiality and anonymity throughout the study. Consent forms will be provided and signed before any participation, ensuring that each individual's decision to be involved is made with complete understanding.

Ethics Approval

As a dedicated researcher, I acknowledge the importance of ethical research and commit to conducting this study with utmost integrity. I will strictly follow all relevant guidelines and regulations and ensure the accuracy and authenticity of the information presented in this paper.

REFERENCES

Anwar, M. R. ., Apriani, D. ., & Adianita, I. R. (2021). Hash algorithm in the verification of certificate data integrity and security. *Aptisi Transactions on Technopreneurship, 3*(2), 67–74.

Baird, L., Harmon M., & Madsen, P. (2019). *Hedera: A Public Hashgraph Network & Governing Council, The trust layer of the internet*. https://hedera.com/hh_whitepaper_v2.1-20200815.pdf

Google Threat Horizons, (2023). *Threat Horizons Report*. https://services.google.com/fh/files/blogs/gcat_threathorizons_full_jul2023.pdf

Gordin, I., Graur, A., Vlad, S., Adomnitei, C.I., (2021). Moving forward passwordless authentication: challenges and implementations for the private cloud. In *Proceedings of the 2021 20th RoEduNet Conference: Networking in Education and Research (RoEduNet)*.

Johnson, C., (2024). *Unveiling the Evolution of Multi-Factor Authentication and What's ChangingNext!*. LoginRadius. Retrieved from https://www.researchgate.net/publication/378970415_Unveiling_the_Evolution_of_Multi-Factor_Authentication_and_What's_Changing_Next

Meltzer, B. N., Petras, J. W., & Reynolds, L. T. (2020). *Symbolic interactionism: Genesis, varieties and criticism*. Routledge.

Multi-Factor Authentication Market. (2023). *Markets and Markets*. https://www.marketsandmarkets.com/Market-Reports/multifactor-authentication-market-231220047.html

Nari, T. J., (2023). Forgetfulness of Being as the Biggest Threat to Humanity. *International Journal of Social Science and Human Research, 6*(8), 4920-4928.

Parmar, V., Sanghvi, H., Patel, R., Pandaya, A., (2022). *A comprehensive study on passwordless authentication* (unpublished manuscript). School of Technology, Pandit Deendayal Energy University, Gandhinagar, Gujarat, India.

SPECOPS. (2024). *Breached Password Report 2024.* Outpost24 Company.

Sporny, M., Longley, D., Chadwick, D., Steele, O., (2024). *Verifiable Credentials Data Model v2.0. W3C Candidate Recommendation Draft*. https://www.w3.org/TR/2024/CRD-vc-data-model-2.0-20240513/

Sule, MJ., Zennaro, M., & Thomas, G. (2021). Cybersecurity through the lens of Digital Identity and Data Protection: Issues and Trends. *Technology in Society*, *67*, paper 101734. 10.1016/j.techsoc.2021.101734.

Todorov, G., (2023). *32 Password Statistics 2024. Data Protection and Security*. https://thrivemyway.com/password-statistics/

Turner, A., Centeno, M., Juanillo, K., (2024). *How many smartphones are in the world?*. https://www.bankmycell.com/blog/how-many-phones-are-in-the-world

Wolf, A. (2024). *A Brief History of Cybercrime*. https://arcticwolf.com/resources/blog/decade-of-cybercrime/

Author's Biography

Christopher Edmund Navarro is a Master of Information Technology candidate at AMA Computer University School of Graduate Studies. He holds a Bachelor of Science degree in Electronics and Communications Engineering (2006) from Rizal Technological University, Philippines. He currently works as an Engineering Lead Analyst at Citibank ROHQ NA, Philippines.

Engr. Jeffrey T. Leonen is a distinguished academic and a respected authority in the field of Information Technology. Former Dean of Engineering and the current Research Director of AMA Computer University, Philippines, His leadership, expertise, and mentorship have made him a vital figure in the development of future IT professionals in the Philippines.