MedCrave
Step into the World of Research
Biometrics & Biostatistics International Journal

Review article
Open Access
CrossMark

Biometric authentication and cybersecurity in the digital age

Abstract

The rapid digitization of society has presented many opportunities and challenges for the protection of sensitive data in several sectors and organizations including banks, health care, education, transport, business organizations, defense and public dealings. Traditional knowledge and possession based authentication systems are no longer sufficient as these are vulnerable to password fatigue, theft, and potentially security breaches. Biometric-based authentication exists to provide a greater level of security, safety and reliability, however, a combination of biometric with one time password (OTP) can provide greater safety and security. Academic literature and trade reports highlighted the biometric authentication utilizes unique human physiological and behavioral identifiers in order to effectively meet security and experience needs of users. Physical biometric includes matching with unique fingerprinting, analysis of facial features, mapping of unique pattern of iris and retina, scanning of vein patterns in the palm and or finger and the measurement of size and shape of fingers and hands. Behavioral biometrics include authentication of a person with his/her voice, the way of walking and heart rate pattern but the behavioral biometrics is neither trustworthy nor reliable in the age of artificial intelligence. The paper reviews the cost ownership, usability, scalability, security, and privacy of various biometric systems. It also situates biometrics within the larger universe of digital risk management and cyber security resilience, whereby biometrics could help mediate risk in online banking and other financial services. In conclusion we find that, while the initial investment is greater in biometric based security, but the continued declining technology costs and scalability has biometrics as an increasingly attractive and sustainable possibility for protecting against digital fraud and counterfeit in an interconnected online world.

Keywords: biometric authentication, cyber security, digital risk management, online banking security, user experience

Volume 14 Issue 2 - 2025

Medhansh Garg,[1] Amar P Garg,[2] Mohd Asif Siddiqui[2]
[1]Department of Computer Engineering, The Grainger College of Engineering, USA
[2]Swami Vivekananda Subharti University, India

Correspondence: Amar P. Garg, Swami Vivekanand Subharti University, Subhartipuram, Meerut, India, Tel +91-9045454762

Received: September 24, 2025 | **Published:** October 30, 2025

Introduction

The introduction of the computer made it possible to convert 0s and 1s to formats machine-readable, formally marking the beginning of digitization in the early 1950s.[1] In 1956, IBM created random-access storage of data in the IBM 305 RAMAC with the IBM 350 disk storage unit that weighed more than a ton and had 5 megabytes of capacity.[2] Although new technology would allow for pulse-code modulation to change analogue signals and conversations into binary counts to create digital audio recording technology at the end of the 1960s, the drive to digital storage and networked computers took time to become main stream. By the mid-1970s, with advancements in personal computers, networking, and other technologies, data began to be digitally stored outside of research institutions and large corporations that had earlier adopted it.[1] Once digital technologies transitioned into consumer technologies in the 1980s, the conversion of text, images, sound, and video content to digital format became widespread and, therefore, a common practice. With the establishment of standardized communication protocols (TCP/IP) in 1983, the framework for modern internet communications was in place.[3]

Computer technology first invaded the territory of foreign airlines, and a few large enterprises in developing countries including India, but only very few organizations. The Government of India wanted to use computer technology as early as 1985, formally endorsing the use of computers to expedite various operations of government machinery and businesses related activities,[4] however, it materialized only at the beginning of the 21st century, to witness transformational growth in digital media players, wireless communication devices, internet technologies and application programs, the rise of e-books, online teaching-learning systems, large quantities of digitized text, were significant contributors to the increasing acceptance of digital technologies. With the commencement of digitization in education during COVID-19, the future of technology-assisted instruction is indivisible from the lives of users in developing and developed countries. In most developing countries, and India in particular, internet-enabled platforms like education, commerce, and healthcare became an essential part of their operations.[5] This transformation has led to widespread automation and digitization in various sectors, including communications, business, banking, healthcare, agriculture, transport, tourism, defense, education, planning, monitoring and prediction of growth under diverse conditions. Artificial intelligence is the product of computer based technology and is the answer to future predicted and unpredicted problems based on collection and analysis of vast data. Digitization is closely tied to emerging technologies like cloud computing, AI, machine learning, and business intelligence, which have significant potential for growth and innovation[6] taken together, these technologies portray the supremacy of the modern digital eon, which encompasses all private and public life across the globe.[7]

The areas in which digitization has improved productivity, efficiency, and communication, while simultaneously lowering operational costs, has expanded what we consider to be normal functions of a business as well as the activities of daily living, by way of improved accuracy and the lifestyle of the common man,[8] and over the years, organisations and individuals have embraced the digitization of methods of operation for conducting and supporting business. Facilities that have used hard copy documents and processes find themselves facing significant digital risks with the increase of

Submit Manuscript | http://medcraveonline.com

©2025 Garg et al. This is an open access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and build upon your work non-commercially.

Copyright: ©2025 Garg et al.

unauthorised access to sensitive information, such as but not limited to, data cyber security, database breaches, and cyber-hacking against organisations, private and public, that create computer and database vulnerabilities that could impact privacy, security, and safety.[9] Some weak or complicated processes or out dated technologies can potentially result in errant disclosures of data leaks, and system failures; the Microsoft outage of July 2024 was significant and disrupted business and commercial activity across much of the Western world, including India in July of 2024 (BBC News, 2024). As risks associated with business digitisation have grown, the ability to protect the private consumer data of individuals has become ripe for exploitation, much of which becomes more and more commonplace as the frequency and variety of cyber-crimes continue to increase.[10] To that end, from a technical standpoint, in light of the data revolution known as the Fourth Industrial Revolution, digital risk can be defined as the unintended negative business objectives which occur result from digital transformation. To overcome new challenges for organisations and individuals, researchers, innovation experts, technology and digital transformation experts have begun to develop digital risk protection, which, acts as a preventative mitigation to address pre-defined risks through pre-pricing, mitigating and risk monitoring circumstances that ensure business continuity, and user safety.[11]

Different types of digital risks

Cloud technology - Risks impacting systems, processes and people associated with technological incompatibilities, errors and failures. The adoption of cloud computing has contributed to security concerns, including; data loss, account hijacking, and service outages.[12]

Cyber security - Risks related to unauthorized access, malware and data breaches. These risks include both inherent and residual risks that directly threaten sensitive resources.[9]

Data leaks - Accidental exposure of private data that becomes a breach. With the digital ecosystem quickly expanding, maintaining confidentiality of data-in-use, data-in-motion and data-at-rest remains a challenge.[13]

Compliance - Risks resulting from law regulation violations or vendor non-compliance causing vendor accountability through risk mitigation or legal consequence from not adhering to compliance standards. Compliance with standards, such as GDPR and HIPAA, requires vigilance in adhering to policy for data protection.[14]

Process automation - Risks that arise from process automation when changes to old automation are made or new automation becomes introduced. Incompatibility may interrupt service processes and imply new sources of vulnerability.[15]

Resilience - There are risks associated with the availability of business services following a disruption such as; a server failure, ransom ware or natural disaster. To build resilience requires business continuity and disaster recovery.[16]

Data privacy - There are risks related to the protection of private and often sensitive personal/financial information. Privacy breaches can create significant harm for individuals and organizations.[17]

Third-party risk - There are risks associated with your vendors or partners. Risks arising from a third-party ecosystem can include continuance risks, non-compliance, breaches, and the theft of intellectual property.[18]

Workforce talent - There are risks related to being able to fill gaps in digital capability and cyber security knowledge that would allow organizations to be able to achieve their business outcomes in an increasingly digital environment.[19]

Digital risk management strategies

The first principle of digital risk management is to protect the data against cyber-attacks because attacks constitute the largest risks in all digital risk categories. In a perfect world, if organizations put all their digital risk protection efforts, for example, protection against cyber-attacks and risks of data breaches, then subsequently, they could still mitigate other categories of risk including: compliance risk, resilience risk, and third-party risk and likewise.[9] Digital risk protection frameworks are founded on traditional threat intelligence tools and these tools should also be implemented at the same time we build a comprehensive and elaborate threat detection and response system and mitigated risks.[20] Central to this will be threat intelligence. These tools prioritize threat prevention and strategic planning by scanning the entire digital ecosystem for vulnerabilities and managing remediation of risks discovered. These ultimately improve the organization's security posture internally and externally across networks, increasing resilience against cyber-attacks.[21]

Digital risk protection

Digital risk protection (DRP) represents a proactive approach to cyber resilience by detecting threats and mitigating them before they can manifest as significant data breaches (Paterson, 2025). DRP activities emphasize the monitoring and mitigation of risks associated with, but not limited to, data leaks originating from the dark web, corporate brand compromise, account takeovers from imposter accounts, fraud campaigns, reputational risks, and social engineering, or phishing attempts.[22] Digital risk protection emphasizes risk mitigation for any losses that can lead to a cyber-attack whereas threat intel solutions relate to building the cyber resilience of the organization after an attempted breach. For complete protection, DRP strategies should contain the following major components:

Digital foot printing: Continuous monitoring of the security status of exposed assets to identify vulnerabilities.[23]

Remediation workflows: Rapid mitigation protocols for detected threats to minimize potential damage.[9]

Threat exposure mitigation: Strengthening ecosystem resilience to reduce susceptibility to cyber-attacks.[24]

By combining these measures, organizations can effectively reduce risks and safeguard their digital ecosystems against increasingly sophisticated cyber threats.

Management of digital risk

Digital risk management is increasingly recognized as a cyclical process, having gone through a visible phase, insights and remediation phase; each phase builds on the data we have from the previous phase.[9] Visibility is achieved by the process of digital foot printing, which gives organizations an ongoing, near real-time view of exposed assets and any associated vulnerabilities.[24] The visibility data is run through threat intelligence solutions to create actionable insights, providing in-house practitioners with a reliable way to identify risks early on, and take action to prevent or mitigate them. The insights about the digital landscape will inform how remediation strategies are designed and executed, which in turn improves resilience against the evolving nature of cyber-attacks and decreases the potential for a data breach.[25]

Citation: Garg M, Garg AP, Siddiqui MA. Biometric authentication and cybersecurity in the digital age. *Biom Biostat Int J.* 2025;14(2):77–83.
DOI: 10.15406/bbij.2025.14.00437

Copyright: ©2025 Garg et al.

Classical examples of use of digital system for public convenience

Electronic recording machine, accounting (ERMA): The economic expansion experienced by the United States in the 1940s and 1950s presented massive increases in the number of individuals with checking accounts. Resulting in great pressure on the back-office's systems involved in the check process, meaning overall banks needed to find a better way of handling their check processing. The invention of the Electronic Recording Machine, Accounting (ERMA) in 1955 began to alleviate the bank's check processing problem and changed the way banks operate forever. The ERMA was invented as a result of work by Stanford Research Institute in conjunction with Bank of America and is credited with automating the check processing, it also introduced magnetic ink character recognition (MICR), which allowed Bank of America to read account numbers with magnetic ink characters which lessened the strain of the work load placed on bankers. At this time Bank of America absorbed the ERMA, now over $200 million it was able to process over 750 million checks annually which was monumental in digitized financial services.[26]

Automatic teller machine (ATM): The first automatic teller machine (ATM) made its debut in 1960, which allowed customers to deposit cash into their bank accounts. In the late 1960s, James Goodfellow developed the personal identification number (PIN) which was used to verify a bank customer accessing an ATM, and increased the security of ATM transactions. As the ATM began to spread, debit cards were also growing in popularity. Debit cards began using magnetic stripes to transmit transaction information, but later EMV technology, using silicon chips, was introduced to provide better verification and reduced fraud.[27]

Pronto system: In 1983, the Pronto System was created by Chemical Bank which allowed customers to manage their own accounts using the telephone, computer, and a television set. This was one of the first types of home banking and within months of offering it, other banks began to think about it and offer solutions as the convenience of the system became clear to consumers.[28] The growth of the Internet in the late 1990s made way for a transition to true online banking. In 1994, Stanford Federal Credit Union became the first financial institution to offer an Internet banking service to its members - account access and transaction capabilities online! The first version of mobile banking came out in the early 2000s and was delivered first by SMS based services, which transitioned to app based versions when smartphones entered gaming finance.[29]

Mobile banking: Mobile banking originated with the utilization of Short Message Service (SMS); customers would receive basic account information and could perform limited transactions. Over time, the enhancement of smartphone technology and mobile applications increased the uptake of mobile banking and further improved customer convenience, access and features. Today, mobile banking has become the most common way for people to view their account details, transfer money, and conduct financial transactions, especially among younger generations who heavily rely on smartphones[30] (Figure 1).

Within the financial services sector, mobile banking is a fundamental service now, especially for the younger generations who are heavily reliant upon their smartphones to manage their finances. In 2021, mobile banking adoption rates reached 95% for Gen Z and 91% for Millennial. There is clear evidence that mobile banking is a convenient and accessible service that offers consumers more than any traditional banking method.[31] It's a red-hot service that allows consumers to perform banking services such as checking their balance, transferring money, and applying for financial services anywhere at any time. In an emerging fast-paced world, consumers are demanding seamless customer experiences, and consumer convenience is driving their decisions. Consumers are satisfied as well with 97% indicating that their digital banking experience has gone well.[31] In addition to the convenience mobile banking offers, it is positioned to strengthen the relationship between customers and banks by providing more personalized interactions and real-time engagement. This level of real-time connection not only helps retain customers, but more importantly creates deeper bank and customer trust and loyalty in an increasingly competitive banking landscape. As more consumers start to use mobile apps as sources of everyday transactions and to help them with financial decision making, mobile banking will remain an important aspect of the modern financial services industry with the vision that it will continue to define banking products and services for generations into the future.[32]

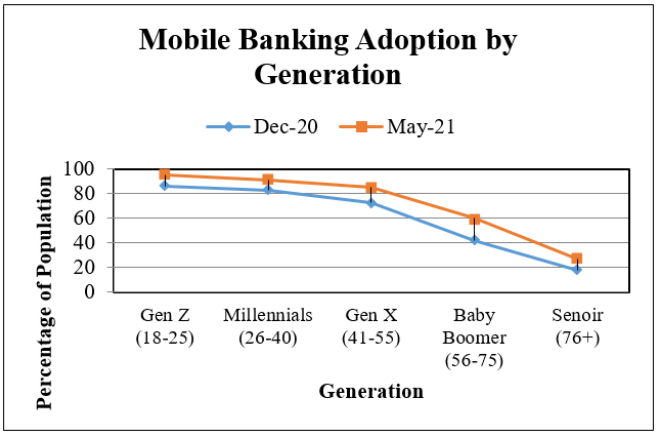

Figure 1 Mobile banking adoption rates across generations (Gen Z, Millennial, Gen X, Baby Boomers, and Seniors) in December 2020 and May 2021, showing increased adoption over time, especially among younger users (Data available on Forbes website).

Conversely, the consequences can be detrimental to both consumers and banks in the absence of proper security in mobile banking. Financial institutions need to maintain trust with their users, and security is crucial to maintaining customers' faith in the platform. A security event can disrupt all of a bank's operations and can mean significant downtime for a bank and its ability to meet its customer needs. Additionally, severity varies by institution - some may not comply with strict regulations and policies, meaning supervisory negative repercussions or penalties. For consumers, though, the effects can be catastrophic: breaches can mean the loss of financial data, unauthorized transactions, or identity theft, causing irreparable damage to one's financial existence.[33]

There are many threats against mobile security from a variety of attackers and they continue to grow in complexity and frequency. Mobile banking applications, specifically, have numerous security obstacles that can threaten financial institutions and end users alike. Common examples of these threats include, but are not limited to:

Phishing attacks – Cybercriminals often use fraudulent messages or emails to trick users into disclosing sensitive information such as login credentials.[34]

Malware – Malicious software, including banking trojans, is designed to steal credentials, intercept communications, or manipulate transactions.[22]

Citation: Garg M, Garg AP, Siddiqui MA. Biometric authentication and cybersecurity in the digital age. *Biom Biostat Int J.* 2025;14(2):77–83.
DOI: 10.15406/bbij.2025.14.00437

Copyright: ©2025 Garg et al.

Man-in-the-middle (MitM) attacks – Attackers intercept communication between a user and the bank's server to steal information or inject malicious commands.[20]

Application vulnerabilities – Weak coding practices, insecure APIs, or lack of encryption can expose mobile banking apps to exploitation.[21]

Online scams – Fraudulent schemes, including fake apps or identity theft, continue to rise as attackers exploit user trust in digital platforms.[33]

These threats highlight the need for robust cyber security measures, including biometric authentication, multi-factor authentication, regular software updates, and user awareness programs to strengthen mobile banking security (Figure 2).

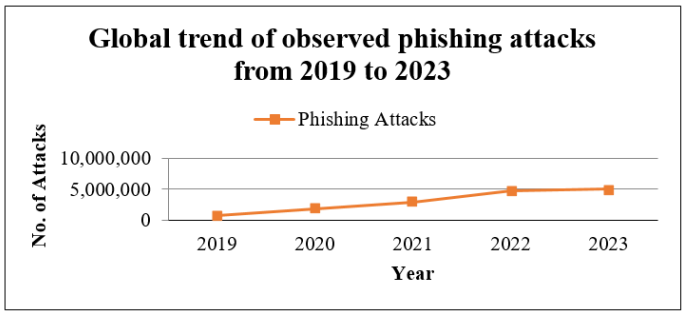

Figure 2 *Global trend of observed phishing attacks from 2019 to 2023 (Data available on APWG/SSL Insights and ControlD website).*

The data highlights a sharp increase in phishing incidents, with attacks rising more than six-fold between 2019 and 2022, and continuing at record levels through 2023.

Current security measures

In the world of increasingly complex online accounts, protecting sensitive or valuable data, and financial information has never been more important; the decision on which authentication methods to use is even more critical with so many choices available. However, examining key considerations for the decision making process, such as implementation costs, user experience, and security, will demonstrate that biometric-based authentication is the best option.[22] Authentication is imperative for protecting sensitive data in a digital form.[9] There are various means of authentication in today's digital world, including knowledge-based, possession-based, and biometric in order to determine the best authentication criteria a determined evaluation is needed.[20] Research shows that biometric authentication provides the greatest security-usability tradeoffs due to the fact that they are based on an individual or organization's unique physical or behavioral traits which are difficult to steal or replicate.[35] In this paper, I argue biometric based authentication is superior in terms of implementation costs, user experience and security. I will examine and present research from not only academic studies but also industry equivalents which include examinations of usability[25] and privacy[23] and the cost of a breach through service.[36] The combined research supports that biometrics are the most appropriate and practical solution to the largest authenticity challenges facing the digital economy today (Figure 3).

To address my research question, first, I identified and defined factors for evaluating authentication methods. The factors included implementation costs, user experience, security, privacy, risk tolerance, and scalability. With these factors established, I then performed a comprehensive investigation of each, looking at each authentication method on the constructed factors. A reputable IEEE source provided information about the cost-effectiveness and implementation of knowledge-based authentication (KBA) describing it as one of the easiest and simplest and cheapest methods of authentication. KBA i.e., passwords and security questions can be implemented, using software without the need for any hardware present on the user-side, with a database to store user data, regular security updates, and an educated user on security practices. With no hardware needs on the user-side and the low cost of implementation, KBA can be used widely across multiple applications.

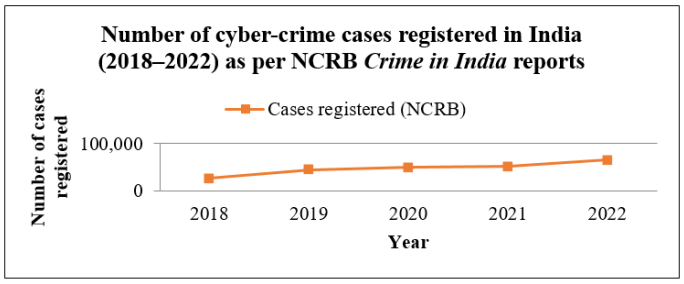

Figure 3 Number of cyber-crime cases registered in India (2018–2022) as per NCRB *Crime in India* reports (Data available on *National Crime Records Bureau (NCRB) website).*

While the existing literature on security and user experience was substantial, I found two detailed reviews that helped me clarify my thoughts. The first review, from 1Kosmos, evaluated the use of knowledge-based authentication in security and was well-articulated and informative largely because of the background and experience of the author. The second review from Wasfi and Stone[21] entitled Usability and Security of Knowledge-based Authentication Systems provided a useful examination of both KBA's security and usability, including the compromises that exist between the benefits of usability and the risk of vulnerability. Knowledge-based authentication (KBA) is when users are asked personal questions from information only they should know.[20] Balancing security and user experience is important in this type of authentication because security and user satisfaction depend on the number and complexity of the questions asked. For instance, when implementing password creation limits such as character limitations or disallowing reused passwords, security can be increased, but user frustration may increase.[21] The amount of security required will depend entirely on the context of the application; for instance, online banking applications will sacrifice ease-of-use for security, while other applications may prioritize usability.[25] While KBA is easy to use and inexpensive, the downside is forgetfulness. Users typically forget passwords or their answers to security questions, leading to password resets where security and user experience are affected. Other than the slight privacy concerns with KBA—where the passwords could be randomly generated and stored as hashed values so that even if a database leak occurs, the passwords are protected—KBA is a middle-ground risk due to the ability to re-key or periodically reset when a leak does happen. However, this could somewhat increase the protection of passwords in the context of encryption[9] (Figure 4).

While scalability, KBA still has appeal due to its simplicity to implement and typically low hardware requirements. This is very important for application types such as online banking for instance, where there is a need to provide security to a larger and growing amount of users and changes to security practices as a result of how the security landscape evolves. Scalability is accomplished by utilizing software updates and managing the database well, where constant updates may be required to keep up with vulnerabilities and breaches.[20] Possession based authentication has proven itself

Citation: Garg M, Garg AP, Siddiqui MA. Biometric authentication and cybersecurity in the digital age. *Biom Biostat Int J.* 2025;14(2):77–83.
DOI: 10.15406/bbij.2025.14.00437

Copyright: ©2025 Garg et al.

as maybe the most straight forward, cost effective way of securing access to a wide variety of applications and systems. Possession based authentication is unlike knowledge based authentication, where possession based authentication does not depend on information stored in the user's mind but on objects in the user's possession, such as tokens, smart cards or physical security keys.[23] By emphasizing objects, the problems associated with compromised knowledge credentials are clearly reduced. The ease of adopting the possession based authentication method is really just owing to the fact that it simply relies upon hardware; either security tokens or smart cards. According to LumenVox,[37] the protocol method needs an underlying infrastructure including a database and management system to store user credentials and manage security updates. This architecture can improve security by reducing the possibility of accessing accounts through stolen or guessed passwords, thus increasing overall resilience. However, there are still issues when it comes to possession-based protocols. Because users must carry physical authentication pieces, the biggest risk that presents itself comes from the need to rely on users not to lose physical items or have items stolen. For example, losing a debit or credit card could have an immediate and direct detrimental effect such as fraud and account access, representing the risk of the possession-based protocol.[37] However, possession-based protocols represent tangible privacy-related advantages. Research indicates randomized key generation protocols produce a strength in privacy because of the information is not exposed. Thus if the key is lost, there are mechanisms to revoke and replace tokens, or devices, but this is typically a much larger resource cost compared to simply resetting a password.

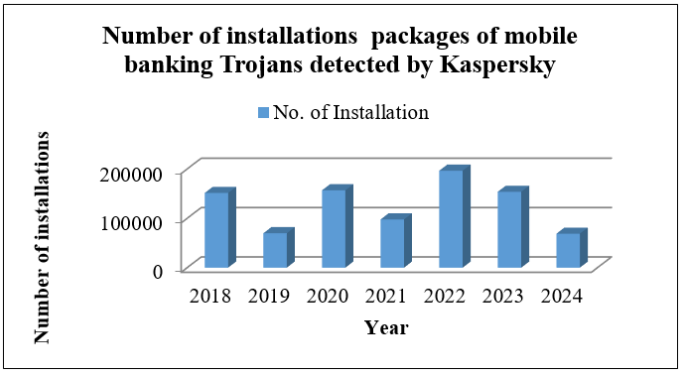

Figure 4 Number of installation packages of mobile banking Trojans detected by Kaspersky, 2018–2024 (based on Kaspersky Security Network [KSN] telemetry).

Login Radius, going into a technical angle, investigates the scalability of possession-based authentication and how organizations can scale their resources associated with this method as they grow. With possession-based authentication, hardware devices or tokens at the user end allows for scalability since only the server needs to create identities and verify tokens. If your organization wants to support a larger amount of users on an application or website then this won't result in additional performance problems. All in all, possession-based authentication is a very practical and relatively secure way of access management. Because it relies on something physical, it enhances security and lowers the risks associated with stolen credentials. Furthermore, while it introduces greater risks (e.g. theft or loss of device), it adds a required countermeasure. The balance between technical scalability, privacy protections, and increased risks (e.g. stolen devices) are examples of the complexity of possession-based authentication as well as its bridging concept between knowledge-based authentication and biometric authentication systems[23,37] (Figure 5).

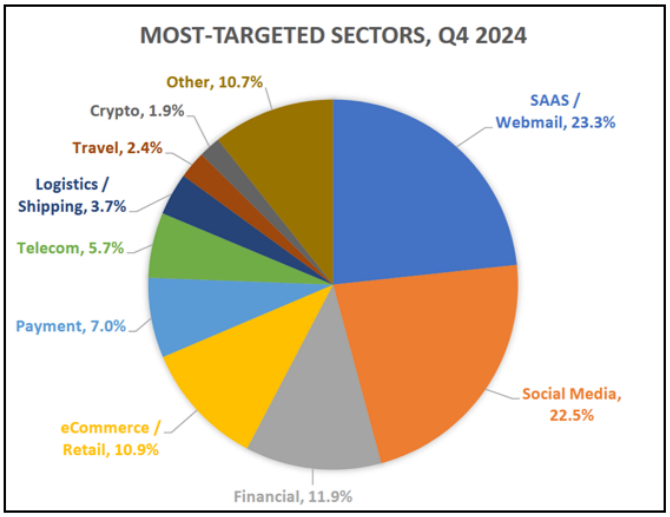

Figure 5 Cyber-attack Trends Q4 2024: SAAS/Webmail and Social Media emerge as the most-targeted sectors (Data available APWG website)

The pie chart in figure 5 shows the sectors that were the most-targeted for cyber-attacks in Q4 2024. The SAAS/Webmail sector (23.3%) and Social Media (22.5%) were the two biggest targets and together accounted for almost half of all incidents. Other impacted sectors included financial services (11.9%), e-Commerce/Retail (10.9%) and Payment systems (7.0%). Finally, Telecom (5.7%), Logistics/Shipping (3.7%), Travel (2.4%), and Crypto (1.9%) were less affected. Finally, 10.7% of attacks specifically targeted other industries, implicating the sheer breadth of cyber threats on a variety of different industries.

Biometric authentication has proven to be an easy-to-use and secure method of access. Biometric authentication has also become more available and widespread, as the cost of implementation goes down with advancing technology. According to Mitek Systems, early applications of biometric authentication included the need for specialized hardware and separate software for collecting and processing biometric data, which led to a higher price of implementation; however, now that technology has advanced and the industry has experienced more economies of scale, the cost has decreased.[38] Keyless Tech describes biometric systems are user focused because they remove the use of passwords or tokens through enabling a user to gain access across multiple devices and service platforms, thus reducing friction while at the same time enhancing experience for the user. From a security perspective, Kaspersky emphasizes that biometric characteristics (e.g. facial structure, fingerprint, etc.) are unique to each individual and provide one of the best forms of defense against impersonation. However, they emphasize that there are attacks that attempt to compromise biometric data that are serious threats; for example, phishing attempts that ask a user to grant camera access on a mobile device or attempts to compromise malware on a computer used to process biometrics. Kaspersky advises that strong encryption and policies around secure storage of biometric data should be implemented to mitigate these outcomes[39] (Table 1).

Citation: Garg M, Garg AP, Siddiqui MA. Biometric authentication and cybersecurity in the digital age. *Biom Biostat Int J.* 2025;14(2):77–83.
DOI: 10.15406/bbij.2025.14.00437

Copyright: ©2025 Garg et al.

Table 1 Global deployment of biometric systems across selected countries, highlighting modalities used, application contexts, and key implementation notes

Country / Region	Modalities used	Deployment Context	Notes / highlights
India	Fingerprint, Iris, Face	Aadhaar (national ID), banking (e-KYC, UPI), airport e-gates	Aadhaar is the **largest biometric ID system worldwide (>1.3B enrolled)**. Fingerprint + iris are primary; face added for verification.
United States	Fingerprint, Iris, Face, DNA	FBI NGI (criminal ID), CBP Biometric Exit/Entry at airports, mobile device unlock	FBI NGI integrates fingerprint & iris; CBP uses face for border checks; consumer biometrics (Face ID, Touch ID) widely adopted.
European Union	Face, Fingerprint	Biometric e-passports, Eurodac (asylum seekers), EES (Entry/Exit System)	EU requires fingerprints + face in passports. Eurodac stores asylum seeker prints. EES (launching) captures fingerprints & facial images for all 3rd-country nationals.
China	Face, Fingerprint, Voice, Gait	National ID, public surveillance (CCTV+FR), border control, banking	Extensive public surveillance with face recognition. Biometric ID used in banking & SIM registration. Reports note rights concerns.
Kenya	Fingerprint, Face, Iris	Huduma Namba (national ID), elections (biometric voter registration)	Biometric registration aims to reduce voter fraud; Huduma Namba project integrates citizen services but raised privacy debates.
United Arab Emirates	Iris, Face, Fingerprint	Border control (IrisScan at airports), banking, e-government	UAE pioneered airport iris scans. Emirates ID integrates multiple biometrics for services.
Japan	Fingerprint, Vein, Face	Border control, ATMs (palm/vein recognition), workplace security	Japan is a leader in palm/vein biometrics for ATMs (Fujitsu/Hitachi tech). Iris/fingerprint also used at airports.

In exploring the academic landscape, CiteseerX is a good, comprehensive look at the privacy issues surrounding biometric-based authentication. It analyses such things as the secure collection, storage, and anonymization of biometric data, user awareness and consent, and transparency. Some practices are proposed, such as storing templates or hashes, rather than the biometric itself, to enhance privacy protection.[40] Biometric authentication has a high tolerance for risk, which IEEE points out in its exploration of implementing and scaling. If a biometric template should be breached, it can be replaced or revoked so that the biometric template does not have the same risk profile as traditional authentication elements. Once the infrastructure is in place, it is easy to add new users or grow the user base. The scalability of biometric authentication is critical, especially for applications that evolve with new security needs or increase in their user base. These elements of biometric authentication have been really active: the cost of starting with biometrics, user experience, security, privacy, risk, and scaling. When I looked at FDIC regulations for internet banking, I looked at the requirements of transactions of online banking and considered many aspects of biometric authentication[41] implementation cost, user experience, security, privacy, risk tolerance, and scaling. In the reality of online banking transactions, the key lies in choosing an authentication method that adequately considers all of these factors. Security remains the focus, and compliance with privacy laws is necessary when dealing with sensitive user information. At the same time, a positive experience is needed so that users adopt the system. This consideration also applies to the relative costs of infrastructure and technology needed for secure identification. Balancing these factors involves the cost of the secure transaction process against the types of risk and acceptable tolerance, scalability, and fit in an existing or future overall risk management plan that considers the risks to user data and financial transactions. Knowledge-based authentication may seem easy and economical, but it relies on the use of passwords and security questions that may be forgotten by users. Possession-based authentication uses physical items (such as tokens, or cards) that can be lost, exchanged, or stolen.[42]

Biometric-based authentication presents an attractive opportunity for online banking, balancing secure and user-friendly experiences. With biometric authentication, security is strengthened by physiologically distinct aspects of a person, such as fingerprints or facial features. There may be a higher initial investment, but the costs are decreasing as technology advances. Biometric authentication can be flexible to handle security breaches, as well as scalable to accommodate a growing user base.[43] In online banking, security and user experience are imperative; therefore, biometric-based authentication would be the best option because of its ability to be secure and easy to use while tackling privacy issues. It is a legitimate option because it balances secure user experience with changing online banking environments, making biometric authentication a great option to protect user information and facilitate secure interactions with banking.

Conclusion

In light of the persistence of digital transformation and growing threat of cybercrime, the availability of secure, user-friendly, and scalable authentication solutions is more vital than ever. This paper shows that biometric authentication can provide a more reliable and substantial defense against impersonation, than traditional knowledge and possession-based systems, while also enhancing user convenience by removing dependence on memory and physical objects. While there are criticisms of privacy and cost of implementation, recent innovations in encryption, secure storage, and regulatory frameworks only add to the possibility of overcoming these issues. Biometric authentication, as a stand-alone solution, or as an element of authentication combined with one-time-pass codes or features like fingerprint or retina scan authentication, can provide a higher level of security and trust particularly in high-stakes situations like online banking. This multi-layered approach not only increases security against initial and evolving cyber-attacks, but can also improve customer experience, making biometrically-enhanced solutions and protocols operationally viable and future-ready for risk management practices in a data-driven economy. Biometric authentication with

Citation: Garg M, Garg AP, Siddiqui MA. Biometric authentication and cybersecurity in the digital age. *Biom Biostat Int J.* 2025;14(2):77–83.
DOI: 10.15406/bbij.2025.14.00437

OTP based system provides better and greater cybersecurity and safety in this digital age. The use of mobile based digital technology has become a part of life in this era, but the introduction of artificial intelligence (AI) has posed a great challenge for the use of behavioral biometrics. It, is therefore, suggested that multi-layered biometric authentication coupled with OTP based security may help in digital risk management.

Acknowledgements

None.

Conflicts of interest

The authors declare there are no conflicts of interest.

References

1. Ceruzzi PE. Computing: A Concise History. MIT Press; 2012.
2. Campbell-Kelly M, Aspray WF, Yost JR, Tinn H, Díaz GC. Computer: A History of the Information Machine. Routledge; 2023.
3. Leiner BM, Cerf VG, Clark DD, et al. A brief history of the Internet. *ACM SIGCOMM Comput Commun Rev.* 2009;39(5):22–31.
4. Rajaraman V. History of computing in India: 1955-2010. *IEEE Ann Hist Comput.* 2015;37(1):24–35.
5. Dhawan S. Online learning: A panacea in the time of COVID-19 crisis. *J Educ Technol Syst.* 2020;49(1):5–22.
6. Mariani M, Borghi M. Industry 4.0: A bibliometric review of its managerial intellectual structure and potential evolution in the service industries. *Technol Forecast Soc Change.* 2019;149:119752.
7. Klaus S. The Fourth Industrial Revolution. World Economic Forum; 2016.
8. Brynjolfsson E, McAfee A. The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies. WW Norton & Company; 2014.
9. Sutton D. Cyber Security: A Practitioner's Guide. BCS Publishing; 2017.
10. Symantec. *Internet Security Threat Report.* Symantec Corporation; 2023.
11. PwC. Managing Digital Risk: Creating Resilient Business Ecosystems. PricewaterhouseCoopers; 2023.
12. Hashizume K, Rosado DG, Fernández-Medina E, et al. An analysis of security issues for cloud computing. *J Internet Serv Appl.* 2013;4(1):5.
13. Kshetri N. Big data's impact on privacy, security and consumer welfare. *Telecomm Policy.* 2014;38(11):1134–1145.
14. Goddard M. The EU General Data Protection Regulation (GDPR): European regulation that has a global impact. *Int J Mark Res.* 2017;59(6):703–705.
15. Rashid A, Danezis G, Chivers H, et al. Scoping the cyber security body of knowledge. *IEEE Secur Privacy.* 2018;16(3):96–102.
16. Bhamra R, Dani S, Burnard K. Resilience: the concept, a literature review and future directions. *Int J Prod Res.* 2011;49(18):5375–5393.
17. Cavoukian A. Privacy by design: origins, meaning, and prospects for assuring privacy and trust in the information era. In: Privacy Protection Measures and Technologies in Business Organizations: Aspects and Standards. IGI Global; 2012:170–208.
18. Rasner G. Third-party risk and threat hunting. *ISSA J.* 2020;18(9).
19. Abed AR. Knowledge economy and the future of human jobs. *World Econ Finance Bull.* 2022;10:65–72.
20. Shah SW, Kanhere SS. Recent trends in user authentication—a survey. *IEEE Access.* 2019;7:112505–112519.
21. Wasfi H, Stone R. Usability and security of knowledge-based authentication systems: a state-of-the-art review. *Int J Adv Comput Sci Appl.* 2023;14(5).
22. Kaspersky. What Is Biometrics? How Is It Used in Security? Kaspersky Resource Center; 2023.
23. Erlich Z, Zviran M. Authentication methods for computer systems security. In: *Encyclopedia of Information Science and Technology.* 2nd ed. IGI Global; 2009:288–293.
24. Patterson L. Investigating New Zealanders' Attitudes, Behaviours and Intentions Toward Cyber Security, Privacy, Authentication and Artificial Intelligence (AI) [doctoral dissertation]. Te Herenga Waka—Victoria University of Wellington; 2025.
25. Katsini C, Belk M, Fidas C, et al. Security and usability in knowledge-based user authentication: a review. In: *Proceedings of the 20th Pan-Hellenic Conference on Informatics.* 2016:1–6.
26. McKenney JL, Fisher AW. Manufacturing the ERMA banking system: lessons from history. *IEEE Ann Hist Comput.* 2002;15(4):7–26.
27. Goodfellow J. Automated Teller Machine and Personal Identification Number (PIN) System. US Patent 3,637,994. US Patent and Trademark Office; 2006.
28. Pikkarainen T, Pikkarainen K, Karjaluoto H, et al. Consumer acceptance of online banking: an extension of the technology acceptance model. *Internet Res.* 2004;14(3):224–235.
29. Shaikh AA, Karjaluoto H. Mobile banking adoption: a literature review. *Telemat Inform.* 2015;32(1):129–142.
30. Jun M, Palacios S. Examining the key dimensions of mobile banking service quality: an exploratory study. *Int J Bank Mark.* 2016;34(3):307–326.
31. Deloitte. 2022 Global Digital Banking Survey. Deloitte Insights; 2022.
32. Nocera G. Fintech Revolution and Traditional Banks: What Factors Influence Members of Generation Z to Place Their Trust in Fintech Companies, Specifically Neobanks, Over Traditional Banks as Banking and Financial Service Providers? [Master's thesis]. 2022.
33. Aite-Novarica Group. *The Consumer Impact of Financial Fraud.* Aite-Novarica; 2021.
34. Gupta BB, Arachchilage NA, Psannis KE. Defending against phishing attacks: taxonomy of methods, current issues and future directions. *Telecommun Syst.* 2018;67(2):247–267.
35. Prabhakar S, Pankanti S, Jain AK. Biometric recognition: security and privacy concerns. *IEEE Secur Privacy.* 2003;1(2):33–42.
36. Soni R. What is a token? What are its pros and cons? *LoginRadius Blog.* Published July 29, 2021.
37. LumenVox. About Possession-Based Authentication. LumenVox Speech Understood; 2023.
38. Mitek Systems. Understanding Biometric Identity Verification: Enhancing Security in the Digital Age. Mitek Blog; 2025.
39. Kaspersky. Phishing Evolves with AI and Stealth: Kaspersky Highlights Biometric and Signature Risks. Kaspersky Press Release; 2025.
40. Melzi P, Rathgeb C, Tolosana R, et al. An overview of privacy-enhancing technologies in biometric recognition. *ACM Comput Surv.* 2024;56(12):1–28.
41. Rane S, Wang Y, Draper SC, et al. Secure biometrics: concepts, authentication architectures, and challenges. *IEEE Signal Process Mag.* 2013;30(5):51–64.
42. Rathgeb C, Uhl A. A survey on biometric cryptosystems and cancelable biometrics. *EURASIP J Inf Secur.* 2011;2011(3).
43. Pope JA, Bartmann D. Securing online transactions with biometric methods. *Int J Electron Mark Retail.* 2010;3(2):132–144.