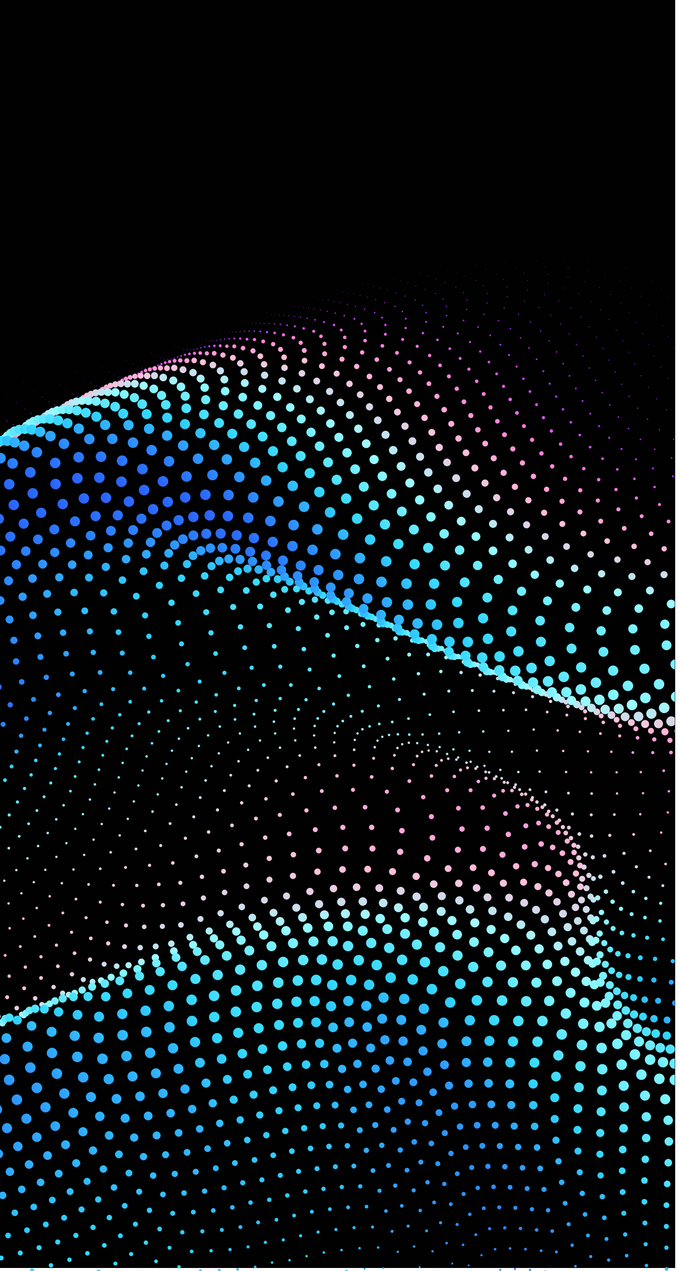
2025 State of Technology Report

bbd
bbdsoftware.com

Digital nervous system | Edge intelligence | Optimising the unseen | The digital battlefield | Your body, your key | Quantum leap



Welcome

The BBD State of Technology Report explores some of the most transformative innovations of our time, offering a deep dive into cybersecurity, quantum computing, edge computing adoption, biometric technology, the intriguing intersection of dark data and sustainability, and the pervasive role of machine learning throughout these domains. With expert commentary woven throughout, this report provides not just an overview of these critical topics but also valuable insights into their implications for the future. For a more in-depth discussion, be sure to check out our companion podcast, **Tech Unboxed**, where we unpack these concepts and their real-world applications.

As you explore these pages, you'll encounter questions that challenge the status quo and spark curiosity. What could widespread adoption of edge computing mean for industries seeking faster, more efficient data processing? Can biometric technology deliver seamless user experiences without compromising privacy? And as organisations grapple with the vast amounts of unstructured dark data they generate, how can this untapped resource be used to drive sustainability initiatives while avoiding ethical pitfalls? These are not just theoretical considerations – they are the pressing issues shaping the technological landscape today.

CONTENTS

01

Digital nervous system:

How IoT is rewiring our world

The Internet of Things (IoT) is a digital revolution brewing beneath the surface of our everyday lives. Imagine a world where your morning coffee starts brewing the moment your alarm goes off, where city streetlights adapt to real-time traffic patterns, and where your health is monitored with precision that would make sci-fi writers blush.

The connected ecosystem: More than just devices

Approaching 2030, we're not just connecting devices; we're crafting a dynamic digital ecosystem that transforms how humans interact with technology.

30bn

The numbers tell a compelling story: we're looking at over 30 billion connected devices globally, powered by lightning-fast 5G networks and increasingly intelligent AI systems.

“Cities are no longer just concrete jungles – they're becoming intelligent organisms. Take Barcelona's innovative smart towers, which aren't just lampposts but urban nerve centres collecting air quality and traffic data, supporting the city’s IoT functionalities as part of the GrowSmarter project, which has expanded connectivity across neighbourhoods,” says Lucky Nkosi, BBD software engineer. “Or consider Oslo's audacious goal of electrifying every vehicle by 2025, with 650 000 LED lights that dynamically adjust to environmental needs.”

Here’s how other innovative countries around the world are pioneering smart technologies, tailored to their specific urban challenges:

Copenhagen, Denmark: Sustainable infrastructure

Copenhagen is on track to achieve carbon neutrality by 2025. The city focuses on integrating smart technologies for traffic management, energy consumption monitoring, and waste management. A centralised platform connects traffic lights and electric vehicle (EV) charging points to optimise the experience for EV drivers.

Amsterdam, Netherlands: Transportation innovations

Amsterdam’s smart city initiatives include sharing traffic data with developers to create mapping applications that integrate with public transport systems. The city also utilises autonomous ‘roboats’ for deliveries via its canals, enhancing urban logistics.

Singapore: Smart Nation Initiative

Singapore’s Smart Nation Initiative leverages technology to address urban challenges, particularly in healthcare for its aging population. This includes digitising healthcare services and developing a comprehensive app for government services and digital identity management.

Dresden, Germany: Thermal storage solutions

As part of the MAtchUp project, Dresden has deployed thermal storage solutions at its Reick Innovation Power Plant to improve district heating efficiency, showcasing how smart technology can enhance energy management in urban settings.

Standing on the brink of a new era defined by unprecedented connectivity, the future of IoT is not just a vision – it's a reality taking shape before our eyes, poised to redefine urban landscapes and enhance our daily lives.

Future trends in IoT

01

Increased device connectivity

By 2025, it is estimated that there will be over 27 billion IoT devices globally. This surge will be particularly evident in urban areas across South Africa, India, the Netherlands, the UK, and Portugal, where smart technologies are being adopted to improve urban management and services.

02

AI integration

The collaboration between AI and IoT – often referred to as AIoT – will revolutionise industries by automating processes and providing real-time insights.

03

Blockchain for security

As IoT devices proliferate, concerns about data privacy and cybersecurity become paramount. The integration of blockchain technology is anticipated to enhance security by providing a decentralised ledger for transactions among connected devices.

04

Edge computing

To manage the vast amounts of data generated by IoT devices, edge computing will become more prevalent, allowing data processing closer to the source rather than relying solely on centralised cloud servers.

05

5G technology

The rollout of 5G networks will enable more reliable connections for devices in both urban and rural settings.

Personal tech: From convenience to empowerment

IoT is expected to significantly impact daily life through enhanced connectivity, convenience and efficiency across various aspects of living – transitioning from a cool gadget ecosystem to a life-enhancement platform:

Enhanced home automation
Imagine fridges that order groceries and thermostats that understand your comfort better than you do. IoT enables smart homes where devices communicate seamlessly. Homeowners can control appliances, lighting, heating and security systems remotely via smartphones or voice commands.

Improved transportation
Smart traffic signals will adapt in real time to traffic conditions, reducing congestion. Vehicle-to-vehicle communication will enhance safety and pave the way for autonomous driving technologies.

Health and fitness monitoring
Wearable devices will become more prevalent – not only tracking steps, but predicting potential health risks – allowing you to monitor your health metrics in real time. These devices track vital signs, physical activity and sleep patterns, providing insights that can lead to healthier lifestyle choices.

Personalised consumer experiences
Retailers will leverage IoT to offer personalised shopping experiences through smart shelves and connected devices that track customer preferences and behaviours.

Environmental monitoring:
Real-time monitoring of environmental conditions will enable better management of natural resources. Sensors in agriculture can provide data on soil moisture and crop health while IoT devices monitor pollution levels in urban areas.

The double-edged sword: Challenges and considerations

Nkosi captures the nuanced reality perfectly. “While IoT promises a utopian technological landscape, we're navigating a minefield of privacy, security and ethical challenges. The very interconnectedness that makes IoT so powerful also raises alarms about unauthorised access and the potential misuse of sensitive information. As our devices become more intertwined, the stakes for data security rise dramatically.”

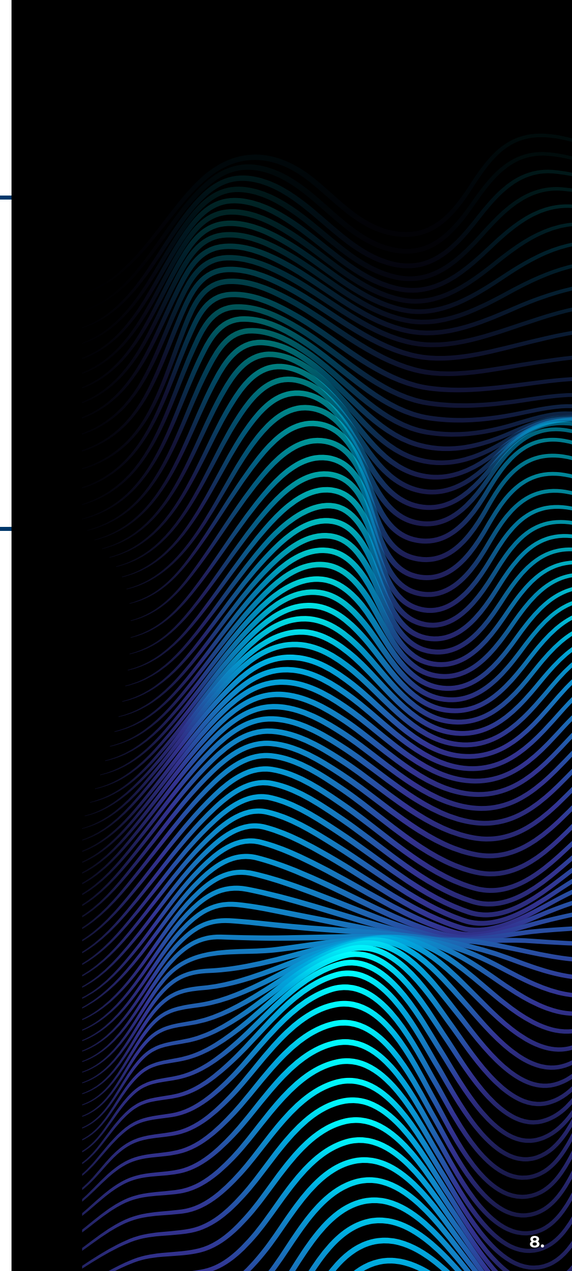
Adding to this complexity are security vulnerabilities. Many IoT devices are built with minimal security measures, making them tempting targets for hackers and cybercriminals. This vulnerability is compounded by the sheer volume of devices flooding the market, leading to interoperability issues. “With countless devices from different manufacturers vying for our attention, ensuring they can communicate effectively is no small feat – standardisation remains a distant goal,” Nkosi says.

IoT systems are heavily reliant on stable internet connectivity. A hiccup in service can render these devices useless, disrupting everything from smart home systems to critical healthcare monitoring solutions. The automation that IoT offers also brings its own set of challenges; while it enhances efficiency, it could lead to job displacement in sectors reliant on routine or manual labour, raising important questions about the future of work.

While IoT holds great potential for sustainability, we must also confront its environmental impact. The production and disposal of millions of connected devices contribute to energy consumption and electronic waste, posing significant challenges for our planet.

Lastly, we cannot overlook the risk of system-wide failures. “A single vulnerability or bug in an IoT system can cascade through interconnected devices, leading to widespread disruptions – especially concerning in critical infrastructure like healthcare and transportation.”

While the journey toward a fully integrated IoT landscape is definitely exciting, it requires careful navigation through these challenges to unlock its full potential responsibly.



The future of IoT isn't just about technological capability – it's about responsible integration. We're not just connecting devices; we're redesigning human experience. As we stand on the brink of this technological renaissance, one thing is clear: IoT isn't just changing how we live, it's redefining what's possible.

References

Cradle Point – What is the relationship between 5G and edge computing | **European Court of Auditors** – Special report smart cities: tangible solutions, but fragmentation challenges their wider adoption | **Forbes** – Internet of Things **Gartner** – Internet of Things: Unlocking true digital business potential | **McKinsey & Company** – The Internet of Things | **Sand Technologies** – What is a smart city? | **Smart Cities World** – Barcelona demonstrates smart tower solution for urban connectivity | **Statista** – Internet of Things (IoT) statistics | **Sustainability Magazine** – Top 10 smart cities leading the way in technology, IoT, and 5G | **Very Technology** – Smart cities and infrastructure

02

$317bn

The global value of edge computing is projected to reach $317 billion by 2026, emphasising its increasing importance across industries.

Edge intelligence:

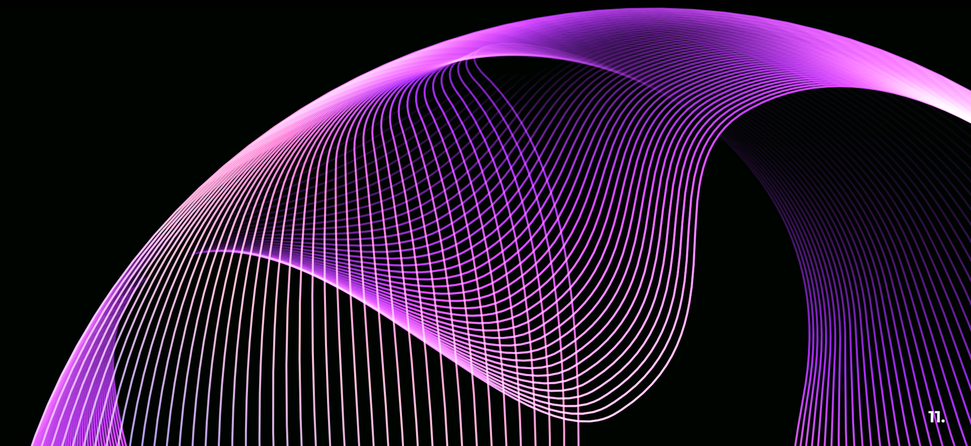
The dynamic duo of machine learning and edge computing

Edge computing represents a significant shift in how data is processed, analysed and utilised across various industries. Unlike traditional cloud computing, which relies on centralised data centres to handle vast amounts of information, edge computing decentralises this process by bringing computation closer to the source of data generation. This approach minimises latency, enhances response times and alleviates bandwidth constraints, making it particularly beneficial for applications that require real-time processing.

At its core, edge computing involves deploying small, low-power devices – often referred to as "edge devices" – strategically positioned near data sources. These devices handle data processing locally and can communicate with each other and the cloud for further analysis when necessary. This hybrid model optimises performance and ensures that critical decisions can be made swiftly without delays associated with transmitting data to distant servers.

"Edge computing is not just a trend; it's the backbone of our future digital infrastructure. It empowers businesses to make faster decisions while ensuring data privacy."

– Tony van der Linden, CIO at BBD.



Current impact of edge computing

The adoption of edge computing is already reshaping various sectors by enhancing operational efficiency and enabling innovative applications. Here are some key areas where edge computing is making a notable impact:

Internet of Things (IoT)

The proliferation of IoT devices has led to an exponential increase in data generation. Edge computing plays a crucial role in managing this data effectively. For instance, in smart cities, traffic lights equipped with edge devices can process real-time data to optimise traffic flow, reducing congestion and improving urban mobility.

Autonomous vehicles

Self-driving cars rely heavily on edge computing to process sensor data instantly. By analysing information from cameras and radar systems on the vehicle itself, these cars can make split-second decisions that enhance safety and efficiency – vital for navigating complex environments.

Healthcare

In the medical field, edge computing enables real-time monitoring of patients through wearable devices. These devices can analyse vital signs locally and alert healthcare providers immediately if any anomalies are detected. This capability not only improves patient outcomes but also enhances the efficiency of healthcare delivery systems.

Manufacturing

The concept of smart factories is becoming a reality thanks to edge computing. By utilising sensors and edge devices, manufacturers can monitor equipment performance in real time, predict maintenance needs, and optimise production processes – leading to reduced downtime and increased productivity.

Entertainment

Edge computing transforms user experiences in gaming and streaming services by reducing latency. Online gaming platforms can utilise edge servers to deliver smoother gameplay experiences by processing game data closer to players' locations.

Machine learning and edge computing adoption

The convergence of machine learning (ML) and edge computing is reshaping the technological landscape, creating a powerful synergy that enhances real-time data processing and decision-making. As organisations increasingly adopt edge computing, machine learning serves as the "golden thread" that weaves through various applications, driving innovation and efficiency across multiple sectors.

Real-time analytics and decision-making

One of the most significant advantages of integrating machine learning with edge computing is the ability to perform real-time analytics at the point of data generation. Traditional cloud-based systems often struggle with latency issues, particularly in applications requiring immediate insights. By processing data locally at the edge, machine learning algorithms can analyse information instantly, enabling rapid decision-making in high-stakes environments.

"Integrating machine learning with edge computing allows raw data to be turned into actionable insights faster than ever before," says van der Linden.

Enhanced efficiency through localised processing

The integration also addresses challenges posed by bandwidth limitations and data privacy concerns. By executing ML models locally, organisations can significantly reduce the amount of data transmitted to central servers, alleviating network congestion while enhancing security by minimising exposure during transmission.

Scalability and cost efficiency

As machine learning models become increasingly complex and data-intensive, edge computing provides a scalable solution that accommodates growing computational demands. The hybrid model allows organisations to leverage both cloud infrastructure for heavy tasks while deploying ML algorithms at the edge for immediate processing needs – optimising resource allocation and reducing operational costs.

Future trends: The rise of edge AI

Looking ahead, the trend towards "Edge AI" – the deployment of artificial intelligence directly on edge devices – is expected to accelerate significantly. According to Gartner, over 55% of all data analysis by deep neural networks will occur at the point of capture in an edge system by 2025. This shift highlights the growing recognition of edge computing as a critical enabler for machine learning applications requiring low-latency processing.

"The future lies in Edge AI – where intelligence meets immediacy at the point of action," says van der Linden.

The integration of machine learning with edge computing represents a transformative shift in how organisations approach data processing and decision-making. By enabling real-time analytics at the edge, this synergy enhances operational efficiency while addressing critical challenges related to latency, bandwidth, and privacy. As industries continue exploring the potential of Edge AI, staying attuned to these developments will be essential for leveraging their benefits fully in an increasingly connected world.

References

Research Gate – Edge computing for autonomous vehicles | **Research Gate** – Toward performance and energy-efficient edge of things | **ACM Digital Library** – ACM transactions on multimedia computing, communications, and applications | **Research Gate** – Service innovation and smart analytics for industry 4.0 and big data environment | **Research Gate** – Internet of Things: Vision, applications and research challenges | **IEEE Xplore** – Edge computing: Vision and challenges | **Forbes** – The rise of edge computing in an increasingly connected world: Five practical applications

03

Optimising the unseen:

Managing dark data for a sustainable future

Dark data – those digital nuggets that organisations collect, store, and often forget – has become a silent yet significant player in our environmental narrative. Imagine a vast ocean of information, where over 55% of this data lies dormant, consuming energy without purpose. This is not just a trivial concern; it's a pressing issue that organisations must confront as they navigate their sustainability journeys.

55%

Dark data is estimated to account for around 55% of the total data stored globally, representing a staggering volume of unused information that organisations often overlook.

6.4M

In 2020 alone, dark data was responsible for approximately 6.4 million tons of CO_2 emissions, equivalent to the carbon footprint of a car traveling around the Earth 575 000 times.

4%

The digital activities associated with dark data contribute to around 4% of global greenhouse gas emissions, surpassing the emissions from the automotive and aviation sectors combined.

175ZB

The rapid growth of global data is projected to reach 175 zettabytes by 2025, with dark data potentially accounting for over half of this total.

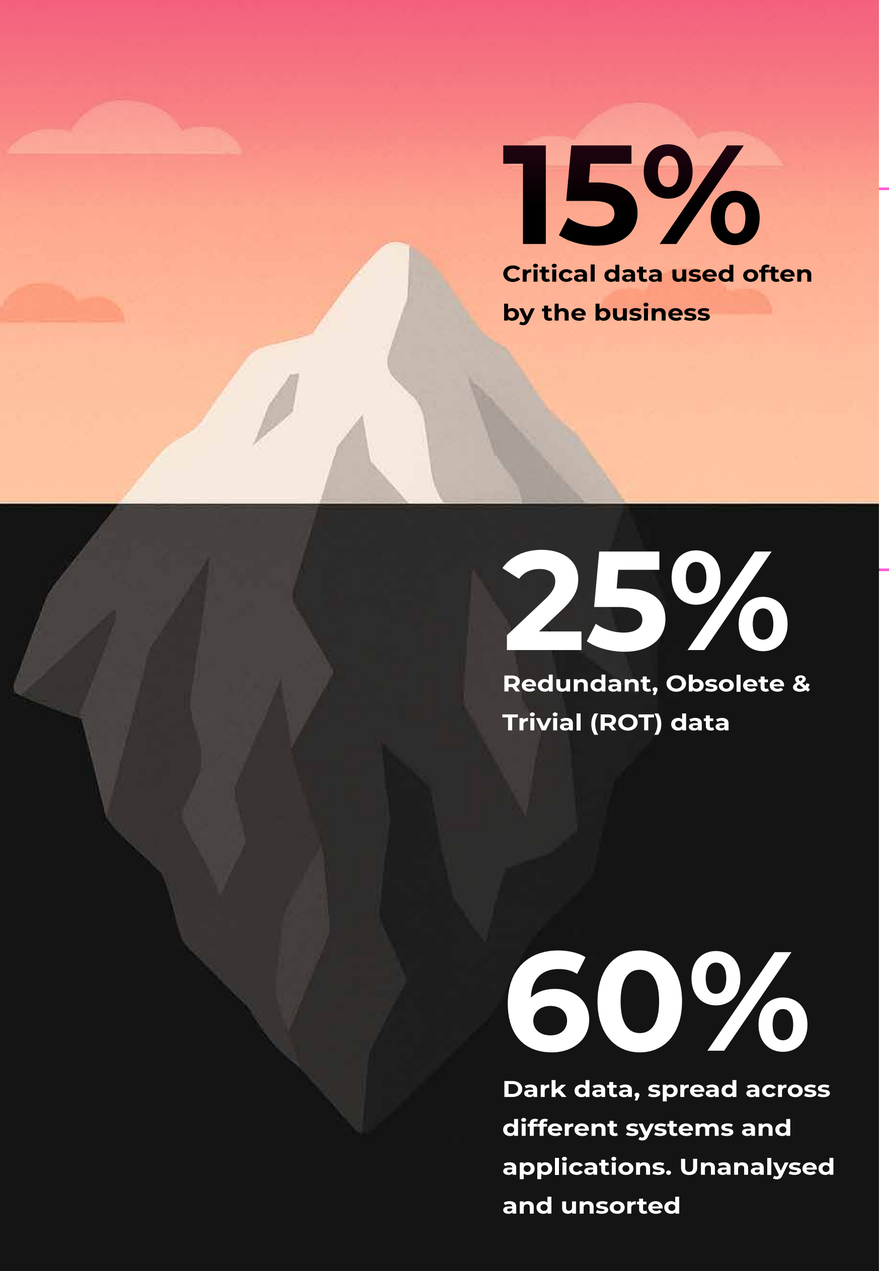
As we move towards a future increasingly reliant on data, the environmental impact of dark data is expected to worsen unless organisations adopt sustainable data management practices. By effectively managing and minimising dark data, organisations can significantly reduce their carbon footprints while also unlocking valuable insights that drive business efficiency.

The hidden costs of dark data

Matthew Barnard, BBD executive says, “Contrary to popular belief, digital data isn’t carbon-neutral. The energy required to store this data contributes significantly to global carbon emissions.” In fact, data centres are responsible for about 3% of global emissions – comparable to the aviation sector. “Every outdated spreadsheet or forgotten image on platforms like Google Photos contributes to an unseen carbon footprint. Research indicates that more than half of the digital data generated by businesses is dark data, simply sitting there like an uninvited guest at a party,” he adds.

As we peer into the future, projections suggest that data centre energy usage could balloon to 10% of the global electricity supply by 2030. It would be one thing if all those electrons were generated from wind or solar farms. But in reality, over 60% of the world’s electricity is still produced using fossil fuels.

This trend is sure to accelerate. The challenge isn’t just about managing data; it’s about managing our planet's resources.



Dark data is linked to the real world through the energy it consumes. Even when data is stored without any intention of reuse, it occupies space on servers – vast arrays of computers housed in warehouses that consume significant amounts of electricity.

Energy consumption

Data centres consume approximately 220 terawatt-hours (TWh) of electricity annually, representing around 1.3% of global electricity demand. This energy consumption is expected to rise as the volume of data continues to grow, with projections suggesting that by 2026, data centres could require up to 1 000 TWh.

The storage of dark data clearly makes this problem worse by driving up energy consumption. To put this into perspective, the International Energy Agency (IDC) produced a report back in 2018 that said data worldwide is expected to grow to 175 zettabytes by 2025. The report said: “If a single zettabyte were stored on DVDs, the stack of DVDs would circle the Earth 222 times”.

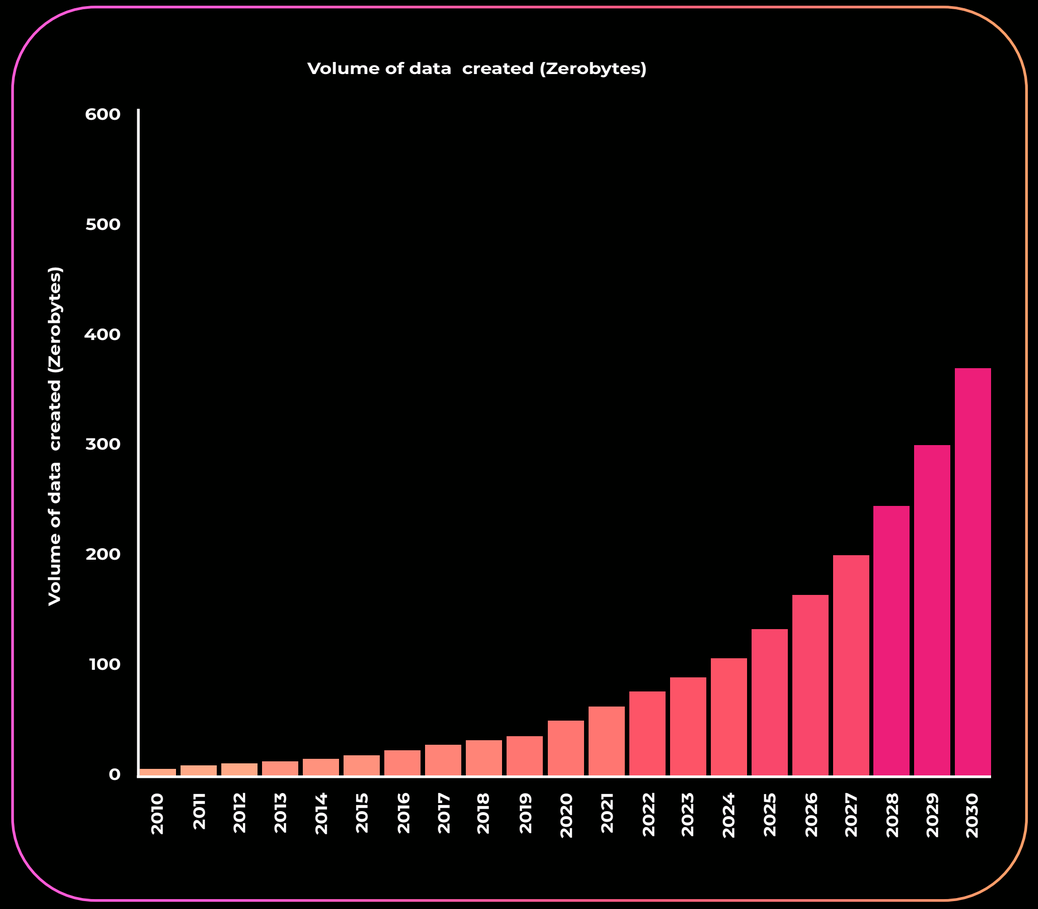
While cloud migration is often hailed as a greener alternative to traditional on-premise solutions, it comes with its own set of challenges, particularly concerning dark data. “Although cloud services can enhance efficiency and potentially lower an organisation’s carbon footprint, they frequently become repositories for an ever-growing volume of dark data,” says BBD’s Liesl Bebb-McKay, BBD Europe Business Development Director. “Without a strategic approach to data management, migrating to the cloud – especially through a straightforward lift-and-shift method – can merely shift the burden of dark data instead of alleviating it. The hidden energy costs tied to dark data are substantial for most organisations.”

While maintaining an effective organisational memory is vital, it raises pressing questions about its environmental impact. As companies strive for net-zero emissions, many are actively seeking innovative ways to reduce their carbon footprints. Traditional guidance has primarily focused on cutting emissions from conventional sources through methods like carbon offsetting – think planting trees to compensate for gasoline use. However, as we grapple with the intensifying climate crisis, it’s crucial to recognise that our digital practices contribute significantly to carbon emissions.

Addressing dark data must be a priority in any comprehensive sustainability strategy, ensuring that our digital endeavours align with a sustainable future. For instance, the Internet of Things (IoT) is projected to generate 1 Zettabyte of data, with an estimated 1% classified as dark data, resulting in approximately 1 million tonnes of CO_2 emissions.

The rise of data volume

This graph illustrates the exponential growth in the volume of data created, copied, and consumed over time, forecasting a continual rise in the amount of data generated. To minimise their digital carbon footprints, organisations must adopt effective data management strategies.



The future of dark data

As we look toward 2030, addressing dark data will be paramount in sustainability strategies. With estimates indicating that up to 75% of all generated data could be classified as dark data in the coming years, organisations must prioritise effective management practices.

“Consider the rise of Smart Cities – an initiative many are excited about. By 2030, cities like Singapore and Barcelona are expected to lead the way with smart infrastructure powered by IoT devices. However, without strategic planning for dark data management, these innovations could inadvertently contribute to environmental degradation,” says Bebb-McKay.

Organisations must prioritise effective management practices to mitigate their environmental impact. Innovative technologies such as artificial intelligence (AI) and machine learning (ML) will play a pivotal role in unlocking the potential value hidden within dark data. By employing advanced analytics tools, organisations can identify unnecessary or redundant information and streamline their data storage practices. This not only reduces energy consumption but also enhances operational efficiency.

Regulatory pressures regarding data privacy and sustainability are likely to intensify. Organisations will need comprehensive frameworks for managing their digital assets responsibly. This includes implementing policies that encourage reducing dark data footprints through regular audits and proactive deletion protocols.

“As more businesses commit to net-zero emissions targets, integrating sustainable practices into cloud migration strategies will be essential. This involves leveraging renewable energy sources for cloud services and optimising workloads to minimise carbon footprints associated with dark data storage,” says Barnard.

Machine learning: The key to unlocking dark data

Enter machine learning (ML), poised to transform how we interact with dark data while promoting sustainable practices. Imagine ML algorithms as skilled detectives sifting through mountains of unstructured datasets, uncovering hidden insights that can drive operational efficiency and reduce waste. **Here's how ML can make a difference:**

Automated data discovery

ML can scan vast datasets across various sources to identify dark data lurking in the shadows. Techniques like pattern recognition and natural language processing allow organisations to find valuable information they didn't even know they had.

Insight generation

Beyond identification, ML can extract actionable insights from dark data. For instance, analysing customer interactions stored as dark data can enhance marketing strategies or inform product development initiatives.

Risk management

With increasing regulatory scrutiny around data privacy, ML helps organisations comply with laws such as GDPR by automatically detecting sensitive information within dark data.

Enhancing sustainability through data management

The management of dark data has significant implications for sustainability. Here's how ML promotes sustainability:

Efficient data storage

By identifying and eliminating unnecessary or redundant dark data, organisations can reduce their storage requirements, leading to lower energy consumption associated with maintaining large data centres. Machine learning tools can automate the identification of outdated or irrelevant data, facilitating more sustainable practices.

Optimising resource use

Analysing operational data using ML helps organisations identify inefficiencies in their processes. By optimising resource allocation based on insights derived from previously untapped dark data, companies can improve operational efficiency and reduce waste.

Supporting sustainable decision-making

Insights gained from analysing dark data can inform strategic decisions that align with sustainability goals. Understanding supply chain dynamics through previously ignored data may lead to more sustainable sourcing practices or waste reduction initiatives.

Machine learning offers powerful tools for addressing the challenges associated with dark data while promoting sustainable technology practices. By automating processes such as discovery, classification, insight extraction, and compliance management, ML enables organisations to unlock the value hidden within dark data, enhance decision-making processes, ensure regulatory compliance, and contribute to environmental sustainability efforts. As businesses increasingly recognise the importance of effective data management and sustainability, integrating machine learning into their strategies will be essential for future success.

As we approach 2030, addressing dark data should be at the forefront of any comprehensive sustainability strategy. Organisations must recognise their digital practices' environmental impact and take proactive steps to manage their dark data effectively. By leveraging advanced technologies like machine learning, businesses can not only align with sustainability goals but also unlock valuable insights from previously untapped resources. In this era where our reliance on data is only set to increase – projected to reach 175 zettabytes by 2025 – the time for action is now. Let's turn the tide on dark data and pave the way for a sustainable future where every byte counts towards a greener planet.

References

Academy of Social Sciences – Why, where and when dark data affects greenhouse gas emissions | **Dataversity** – Unveiling the power of dark data in strategic decision-making | **Greenoco** – What is the dark data? And what is its carbon impact? – 2023 | **Pivotl** – When dark data turns darker: Data's impact on climate change | **RossumAI** – What is dark data & why does it matter? | **Tech Target** – How to mine dark data with machine learning and AI | **The Week** – What's dark data and why is it bad for the environment? | **ThinkLeaf** – Dark data - Unveiling the mysteries | **Slingshot Simulations** – Dark data – what is it... and should we be scared?

04

The digital battlefield:

Navigating cybersecurity in 2025 and beyond

Cybercrime isn't just a technical problem – it's a US$10.5 trillion annual global industry. The battleground has shifted from physical networks to invisible digital landscapes, where machine learning has become our most sophisticated defence mechanism. Peter Scheffel, BBD executive, describes this new reality vividly: "We're no longer playing defence. We're creating intelligent systems that can predict, prevent, and neutralise threats before they even fully materialise."

$10.5tn

Cybercrime costs are expected to reach US$10.5 trillion annually by 2025.

$562.72bn

The global cybersecurity market is expected to grow from US$193.73 billion in 2024 to US$562.72 billion by 2032.

$200bn

Information security spending is expected to surpass $200 billion in 2024 and more than US$300 billion by 2030.

88%

88% of cybersecurity breaches are caused by human error. The average time to identify a breach is 194 days. The average lifecycle of a breach is 292 days from identification to containment.

Machine learning: The digital immune system

Machine learning isn't just a technology; it's a digital immune system that hunts threats with surgical precision. These intelligent systems don't just detect - they predict, adapt, and neutralise before human analysts can even recognise a potential breach.

Millions of data points are analysed in milliseconds. A suspicious login from an unknown location? Neutralised. An unexpected data transfer? Blocked. A micro-pattern of potentially malicious code? Isolated and eliminated.

Take the 2018 cryptocurrency mining attack that targeted 400 000 users. Microsoft's Windows Defender, powered by machine learning, shut down the crypto miners almost instantly – a feat impossible for human analysts.

The key superpowers of machine learning:

Threat detection
Learning from historical data to recognise attack patterns

Real-time response
Blocking threats faster than you can blink

Predictive analytics
Forecasting cyber threats before they materialise

Machine learning transforms cybersecurity from a reactive discipline to a proactive shield. It's not just about stopping attacks; it's about understanding the enemy's psychology. Imagine an AI that understands user behaviour so intimately that it can detect an insider threat or a compromised account by analysing the subtlest deviations from normal patterns. That's not science fiction – that's machine learning in 2025.

While machine learning is powerful, it's not about replacing humans – it's about augmenting human capabilities. By automating routine tasks, these systems free up security professionals to focus on complex strategic challenges.

As cybercriminals evolve, so do machine learning algorithms. They continuously learn, update, and adapt, ensuring that our digital defences remain one step ahead of potential threats.

IoT and 5G security challenges

The proliferation of internet of Things (IoT) devices and the rollout of 5G networks present significant security challenges. IoT devices often lack robust security features, making them vulnerable entry points for cyberattacks. As these devices connect to larger networks, they can be exploited to gain access to sensitive information or disrupt critical services. The rapid expansion of 5G technology further complicates this issue by increasing the number of connected devices and potential attack vectors. To mitigate these risks, organisations should adopt best practices for IoT security, including implementing strong authentication mechanisms, regularly updating device firmware, and segmenting IoT devices from critical network infrastructure. Additionally, employing threat intelligence solutions can help organisations identify vulnerabilities within their IoT ecosystems and respond proactively to emerging threats.

Mobile device vulnerabilities

With the prevalence of mobile banking and applications, cybercriminals are increasingly targeting mobile platforms to exploit vulnerabilities, leading to a surge in attacks aimed at stealing sensitive financial information and personal data. The convenience of mobile transactions often comes at the cost of security, as many users neglect basic protective measures such as strong passwords and two-factor authentication. To secure mobile devices effectively, organisations should implement comprehensive security strategies that include regular software updates, robust encryption protocols, and user education on safe practices. Additionally, employing mobile device management (MDM) solutions can help organisations monitor and manage device security across their networks, ensuring that sensitive data remains protected against unauthorised access.

Ransomware: The digital extortion economy

Cybercriminals are no longer just targeting individual organisations – they're strategically attacking supply chains, creating cascading effects that can paralyse entire industries. These aren't just attacks; they're precision-engineered digital weapons.

AI-powered attacks

Artificial intelligence has become a double-edged sword. Cybercriminals now use generative AI to craft hyper-personalised phishing emails, create convincing deepfakes, and develop malware that can learn and adapt in real-time.

Quantum computing threats

As quantum computing technology advances, its potential impact on encryption and security protocols becomes a pressing concern. By 2025, organisations must prepare for the reality that current encryption methods may be rendered obsolete by quantum computing capabilities. This necessitates a shift towards quantum-safe cryptography to protect sensitive data against future threats.

Emerging threats require proactive measures from organisations across all sectors. The integration of AI in both attack and defence strategies underscores the need for continuous adaptation in cybersecurity practices. By investing in employee training, adopting advanced technologies for threat detection, and remaining compliant with evolving regulations, organisations can fortify their defences against an increasingly sophisticated array of cyber threats. The future of cybersecurity depends on our ability to anticipate challenges and respond effectively in an ever-changing digital landscape.

References

Bangkok Bank Innohub - 8 Cybersecurity trends to look out for in 2025 | **Built In** - How machine learning in cybersecurity works | **Check Point** - 2025 Cyber security predictions: The rise of AI-driven attacks, quantum threats, and social media exploitation | **Embroker** - Cyberattack statistics 2025 – 2025 | **Fortune Business Insights** – Cybersecurity market analysis – 2032 | **Google Cloud** - Emerging threats: cybersecurity forecast 2025 | **Help Net Security** - Google cloud cybersecurity forecast 2025: ai, geopolitics, and cybercrime take centre stage | **HostPapa** - The most useful tools for AI & machine learning in cybersecurity | **IMB** – Cost of a data breach report 2024 | **NinjaOne** - The role of machine learning in cybersecurity | **Park University** - Cybersecurity trends: protecting business information in 2025 | **SailPoint** - How AI and machine learning are improving cybersecurity | **Sangfor** - Machine learning in cybersecurity: benefits and challenges | **Varonis** - 157 Cybersecurity Statistics and Trends

05

Your body, your key:

Exploring the future of biometric technology

Imagine a world where your body becomes the key to your digital life. Think of it as a digital fingerprint that transcends traditional passwords or ID cards. Instead of wrestling with complex codes, your unique biological traits unlock doors – both physical and virtual. As we step into 2025, the landscape of biometric technology is not just evolving; it's transforming how we interact with our devices, our environments and each other.

$150.58bn

The global biometrics market is projected to grow significantly, reaching approximately US$150.58 billion by 2030, with a compound annual growth rate (CAGR) of 20.4% from 2023.

The future of biometric authentication includes integrating artificial intelligence to enhance accuracy and enable multi-modal authentication, which uses multiple biometric traits simultaneously.

The booming biometric market

The biometric technology market is on an exhilarating upward trajectory. Valued at around US$47 billion today, it's projected to soar to approximately US$85 billion by 2029, driven by the increasing demand for seamless and secure authentication methods across various sectors such as banking, healthcare and government. This growth represents more than just numbers; it signifies a fundamental shift in how we think about security and identity verification.

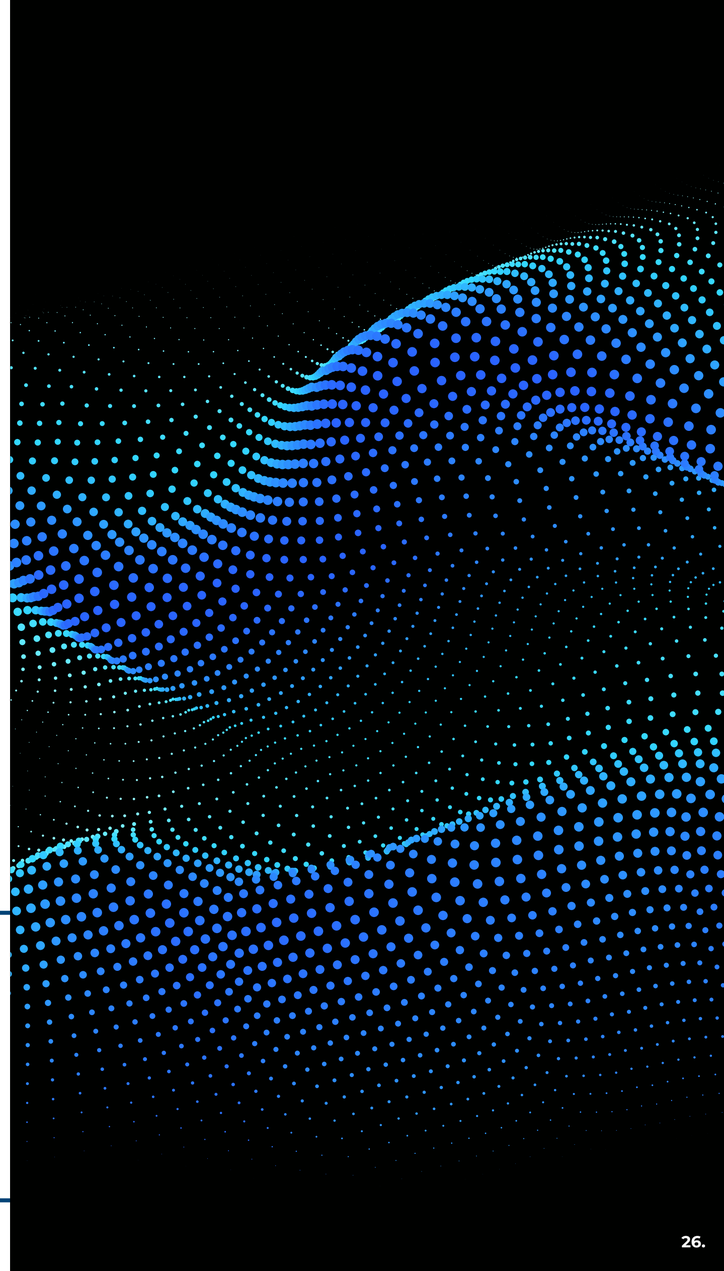
Amazon has released a palm scanning services that allows you to use your phone's camera to scan your hand. This scan can then be used in the future to open retail or banking apps.

Peter Scheffel, BBD's Chief Digital Officer, says, “Why is this so interesting? Current facial recognition implements biometrics on high-end devices. However, scanning a palm with the rear camera can be done by low-end smartphones. This opens secure biometrics up to a much larger audience.”

AI and machine learning: The game changers

At the heart of this transformation are artificial intelligence (AI) and machine learning (ML). These technologies are redefining biometric systems by enhancing their accuracy and responsiveness. Imagine a facial recognition system that can adapt to your changing looks over time, recognising you even if you change your hairstyle or age a few years. This level of sophistication means fewer false positives and negatives, making biometric systems more reliable than ever before.

“AI is revolutionising how technology companies approach biometrics. It allows systems to be created that are not only smarter, but also more intuitive,” Scheffel says. “This technology used to require constant connectivity to large cloud platforms. Now, edge computing means that the models can run offline on handheld devices.”



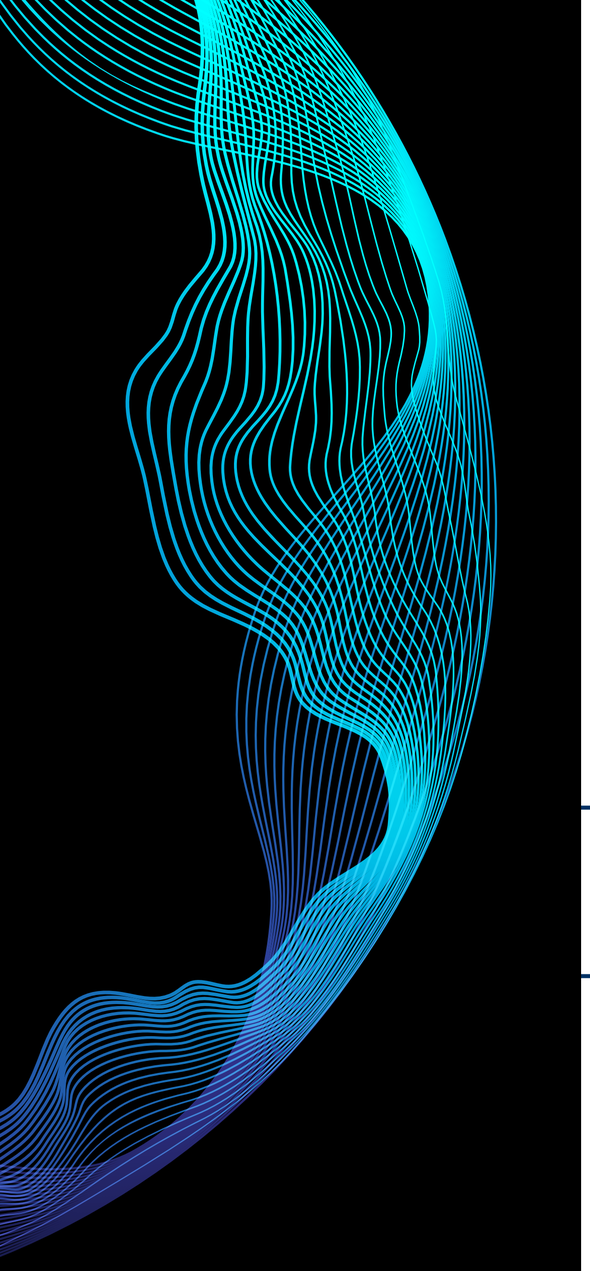
Multimodal biometrics: The future is multi-faceted

Gone are the days when a single biometric factor sufficed. In 2025, we'll see the rise of multimodal biometric systems that combine various identification methods – like fingerprints, facial recognition and voice patterns – to create a fortress of security around our identities. This approach not only enhances security but also adds convenience, making it harder for anyone to spoof or hack into these systems. Additionally, we may soon witness the emergence of next-gen modalities such as odour recognition and heartbeat analysis for secure authentication, further ensuring that only you can gain access. As our homes become smarter, biometrics will also play a crucial role in securing access to everything from smart locks to connected appliances, seamlessly integrating security into our daily lives.

"Another example of multimodal biometrics is Microsoft's corporate security solution," says Scheffel. "This system first prompts you to enter your password when logging into an enterprise resource. Upon successful entry, the authentication screen displays a number. You then switch to your phone and launch the Microsoft Authenticator app, which must have been previously linked to your User ID and digital certificates from your organisation. You will be prompted to enter the two-digit number displayed on your screen. For added security, your biometric Face ID must successfully scan before you gain access."

This process exemplifies effective security measures, requiring you to:

1. Remember your password
2. Physically have the previously configured phone with you
3. Read the number and type it on a different device
4. Ensure that the device verifies that the valid user was present when the number was entered



Continuous authentication: Security at every step

Picture this: instead of logging in once when you start using a device, continuous authentication keeps verifying your identity throughout your session. This technology analyses behavioural patterns – how you type, how you navigate – ensuring that only you can access your information.

Scheffel notes, “In some enterprise security applications in China, eye-tracking technology ensures the logged-in user remains present. If you look away, a warning appears, and after a short timer, you're logged out. This approach strengthens security by monitoring user behaviour in real time, offering both protection and a seamless experience without constant interruptions.”

Taking authentication to the next level with behavioural biometrics

As digital fraud becomes rampant and more sophisticated, behavioural biometrics are stepping up to the plate. By leveraging AI and ML, this technology identifies unique and measurable patterns in human behaviour to validate identity and understand intent. For example, you might log into an application or navigate through a website while your system learns from your mouse movements, typing cadence, touch events, and swipe patterns – each action contributing to a unique profile that characterises you as an individual. This profile is continuously updated in real-time, enriched with user-specific information such as IP address, device type, time of access and navigation patterns. The result? A seamless identification process that not only enhances user experience but also significantly boosts fraud detection rates while minimising false rejections.

“Behavioural biometrics is a game changer in fraud prevention. By understanding user behaviour patterns, we can create a more secure environment without sacrificing convenience,” Scheffel says.

Navigating privacy concerns

As we embrace these exciting advancements, we must also address the ethical implications surrounding biometric data collection and usage. With great power comes great responsibility; organisations must prioritise transparency and data protection to earn public trust. “This means implementing robust security measures to safeguard sensitive information while ensuring that users feel comfortable with how their data is handled,” says Scheffel.

As we look ahead to 2025 and beyond, the future of biometric technology is filled with promise and potential. It's not just about enhancing security; it's about creating seamless experiences that make our lives easier while keeping our identities safe. By embracing these advancements with an eye toward ethical considerations, we can ensure that biometrics serve as a powerful tool for good in our increasingly digital world. In this journey toward a more secure future, remember: your body is not just part of who you are; it's becoming the key to unlocking new possibilities in technology and beyond.

References

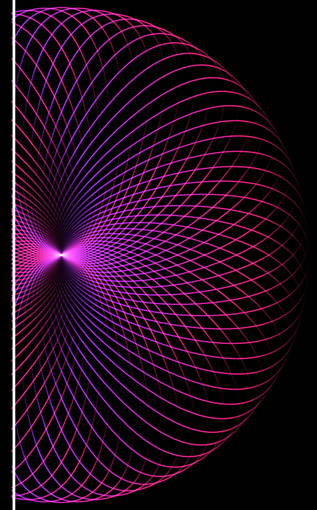
FaceOnLive - Biometric authentication: trends and predictions for 2025 | **First Ignite** - Exploring the latest biometric technology advancements in 2025 | **Forbes Technology Council** - Biometric authentication: Enhancing security without compromising privacy | **Hyperverge** - Future of biometrics: trends, innovations, and challenges ahead | **IT Brief** - The future of authentication: are you embracing biometrics? | **Sigma Technology** - Tech trends 2025: Beyond AI – IT innovations shaping the future | **The Verge** - Amazon's palm-scanning service now lets you sign up from your phone | **Verified Market Reports** - Top 7 trends in next generation biometric

06

Quantum leap:

When machines think in parallel universes

Imagine a world where computers can solve problems in mere minutes that would take traditional computers thousands of years. This is the fascinating realm of quantum computing, where the principles of quantum mechanics are not just theoretical musings, but practical tools that are set to revolutionise technology as we know it.



$106bn

Estimates suggest that the global quantum technology market is projected to reach US$106 billion by 2040.

100M

Google announced it has a quantum computer that is 100 million times faster than any classical computer in its lab.

1M

By 2030, it is estimated there will be a demand for over 1 million skilled professionals in quantum computing-related fields.

100-1000

Quantum computers will reduce power consumption anywhere from 100 up to 1 000 times because quantum computers use quantum tunnelling.

Once a stable quantum computer gets developed, expect that machine learning will exponentially accelerate, even reducing the time to solve a problem from hundreds of thousands of years to mere seconds.

When we talk about quantum computing, it feels like stepping into the pages of a science fiction novel. The reality is that we are on the brink of a technological revolution that challenges our conventional understanding of computing. Currently, the transistors in our computers have reached their physical limits, prompting innovators to explore solutions at the atomic and subatomic levels through quantum computing. Industry leaders are in a fierce race to create and commercialise viable quantum computers. These ground-breaking machines promise to deliver the computational power needed to tackle problems that classical computers simply cannot solve – at least not within a practical timeframe.

At its core, quantum computing leverages quantum bits, or qubits, which differ fundamentally from classical bits that represent either a 0 or a 1. Qubits, often realised through subatomic particles like photons or electrons, can exist in multiple states simultaneously, due to a phenomenon known as superposition. This unique property allows quantum computers to perform complex calculations at speeds unattainable by classical systems. Another principle is entanglement, where qubits become interconnected such that the state of one qubit can depend on the state of another, regardless of distance. This interconnectedness enhances the computational power and efficiency of quantum systems, enabling them to tackle vast amounts of data more effectively than traditional computers. The potential here is staggering tasks that could take classical computers centuries may be completed by a quantum computer in just a few moments.

Quantum computing	Classical computing
Calculates with qubits, which can represent 0 and 1 at the same time.	Calculates with transistors, which can represent either 0 or 1.
Power increases exponentially in proportion to the number of qubits.	Power increases in a 1:1 relationship with the number of transistors.
Quantum computers have high error rates and need to be kept ultracold.	Classical computers have low error rates and can operate at room temp.
Well suited for tasks like optimisation problems, data analysis, and simulations.	Most everyday processing is best handled by classical computers.

Key concepts of quantum computing

Understanding the foundational concepts of quantum computing is crucial for appreciating its potential impact across various sectors.

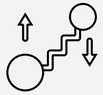
These are the key principles that define how quantum computing operates:

Qubits

The cornerstone of quantum computing, qubits can represent both 0 and 1 simultaneously. This capability enables quantum computers to perform multiple calculations at once, vastly increasing their processing power.

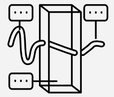
Superposition

Unlike classical bits, which are confined to being either 0 or 1, qubits can hold an undefined value until measured. This state allows quantum computers to explore many possible solutions concurrently, enhancing their ability to tackle complex problems.



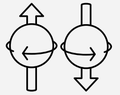
Entanglement

Qubits can become entangled, meaning the state of one qubit is directly related to the state of another, regardless of the distance separating them. This interconnectedness facilitates complex computations that classical systems cannot achieve.



Tunnelling

The cornerstone of quantum computing, qubits can represent both 0 and 1 simultaneously. This capability enables quantum computers to perform multiple calculations at once, vastly increasing their processing power.



Coherence

For a qubit to effectively exhibit superposition and entanglement, it must remain coherent and free from external disturbances. Maintaining coherence is crucial for the successful operation of quantum algorithms.

These foundational concepts define how quantum computers function and highlight their transformative potential across various industries.

How quantum computing will change the world

Quantum computing is poised to revolutionise various sectors by providing unprecedented processing power and addressing complex problems that are intractable for traditional technologies:

Drug discovery could see timelines reduced dramatically

Quantum computers can simulate molecular interactions at an atomic level, dramatically accelerating the drug discovery process. For instance, a study by researchers at the University of California, Berkeley, demonstrated that quantum algorithms could model complex chemical reactions more efficiently than classical methods. This capability allows for rapid identification of effective molecular combinations, significantly reducing development costs and timelines. A quantum computer could potentially identify a viable drug candidate in weeks instead of years, which is a game-changer for the pharmaceutical industry.

Cryptographic systems will need a complete overhaul

As quantum computers advance, traditional encryption methods may become obsolete due to their ability to break current algorithms like RSA – an encryption scheme invented by MIT researchers Ron Rivest, Adi Shamir, and Leonard Adleman in the 1970s (hence the name “RSA”) – and Elliptic curve cryptography (ECC), introduced in 1985 by Victor Miller and Neal Koblitz who both independently developed the idea of using elliptic curves as the basis of a group for the discrete logarithm problem. A notable example is the work done by researchers at MIT, who have shown that quantum computers can factor large integers exponentially faster than classical computers using a quantum factoring algorithm created by MIT professor, Peter Shor, in 1994. This necessitates a shift towards quantum-resistant cryptography, prompting the development of new security protocols to safeguard sensitive information.

Optimisation problems in logistics could be solved with ease

Industries such as logistics and finance stand to benefit immensely from enhanced optimisation capabilities offered by quantum computing. For example, Volkswagen has been exploring how quantum algorithms can optimise traffic flow in urban areas. By simulating various traffic scenarios and routes in real-time, they aim to reduce congestion and improve efficiency. Similarly, financial institutions like JPMorgan Chase are investigating quantum computing for portfolio optimisation and risk assessment, allowing for better decision-making processes.

Climate modelling could lead to breakthroughs in understanding our planet

Quantum computers can analyse complex climate data more efficiently than classical systems. A study published in Nature demonstrated that quantum algorithms could simulate climate models with higher accuracy and speed than traditional methods. By improving our understanding of environmental dynamics, these advancements can aid in climate change mitigation efforts and lead to more effective policies.

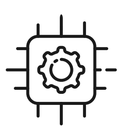
Financial optimisation

Enhanced modelling for risk assessment and investment strategies will be possible through quantum computing. For example, Goldman Sachs has been exploring how quantum algorithms can improve option pricing models and risk management strategies. By providing more accurate predictions in financial markets, firms can make better-informed decisions regarding investments and asset management.

The intersection of machine learning and quantum computing

The convergence of quantum computing and machine learning presents exciting possibilities for data processing and analysis. The synergy arises from quantum computing's ability to handle vast amounts.
Several algorithms have been developed specifically for machine learning tasks:

Quantum Support Vector Machines (QSVM)
Enhances traditional support vector machines by utilising quantum properties for improved classification performance.



Quantum Principal Component Analysis (QPCA)
Allows for efficient dimensionality reduction by identifying principal components more rapidly than classical methods.

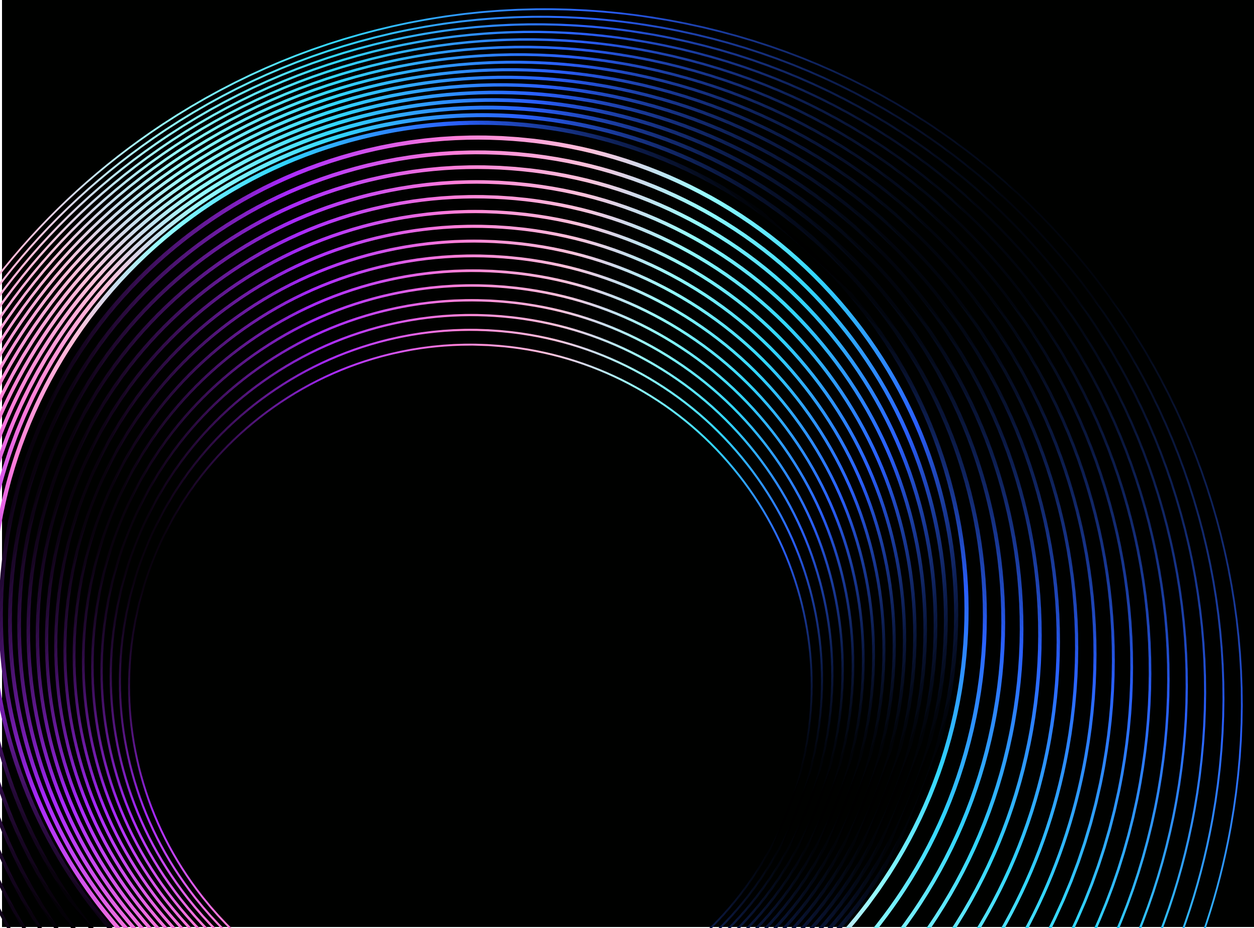
These algorithms demonstrate how quantum computing can significantly outperform classical approaches in specific scenarios.

As we stand on the brink of this technological revolution, it's clear that quantum computing holds immense promise for reshaping our world. By harnessing its unique capabilities, we can solve problems once deemed impossible – ushering in an era where computation transcends our current limitations and opens doors to innovations we have yet to imagine.

References

ABC Science - Quantum computers explained: How quantum computing works | **Biforesight** - Quantum market growth is not just a leap of faith | **Business Insider** - 9 facts about quantum computing that will melt your mind **CBInsights** - Quantum computing vs. classical computing in one graphic | **FourWeekMBA** – Quantum computing explained | **Goldman Sachs** – Engineering quantum algorithms | **Google Blog** – When can quantum annealing win? **IBM Quantum** – Quantum computing | **McKinsey & Company** – Quantum technology monitor | **MIT News** – Toward a code-breaking quantum computer | **Research Gate** – Quantum machine learning in climate change and sustainability: a short review | **Volkswagen Group** – Volkswagen optimizes traffic flow with quantum computers | **World Economic Forum** – How quantum computing is changing drug development at the molecular level

Thank you



As we bring the BBD State of Technology Report to a close, it's clear that the technologies explored here are shaping the future in profound ways. With machine learning serving as a golden thread throughout these innovations, these advancements drive progress and present new challenges and opportunities for businesses and society alike. The insights shared in this report highlight the importance of understanding and embracing these technologies to remain competitive and sustainable in an ever-changing world.

To continue the conversation, we encourage you to tune into our **Tech Unboxed** podcast, where we take a deeper dive into the topics covered in this report. Through engaging discussions with our experts, the episode unpacks key trends, real-world applications and the future possibilities of these transformative technologies. Whether you're looking to gain fresh perspectives or practical insights, Tech Unboxed is your companion for navigating the exciting world of innovation. Let's keep exploring what's next, together.

bbd
bbdsoftware.com