Jus Corpus Law Journal
Open Access Law Journal – Copyright © 2024 – ISSN 2582-7820
Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

Introducing the Future of Tech Integration: Combine Computing, Blockchain Data, Big Data and the Internet of Things

Anjalika Behera[a]

[a]SOA National Institute of Law, Odisha, India

Received 05 May 2024; *Accepted* 06 June 2024; *Published* 10 June 2024

The future is being shaped by the integration of cutting-edge technologies, and promising advancements across various sectors. This study delves into the potential synergies of combining computing, blockchain, big data, and the Internet of Things (IoT). Through advanced computing, we can process and analyze massive data sets quickly and accurately. Blockchain technology enhances data security and integrity, providing a decentralized framework for transactions and information sharing. Big data analytics offers insights by extracting patterns and trends from vast data repositories, enabling informed decision-making. IoT connects devices, enabling seamless communication and automation across different environments. The convergence of these technologies creates a robust ecosystem where data flows securely and efficiently, leading to innovations in smart cities, healthcare, finance, and supply chain management. This integrated approach optimizes operations and opens up new business models and economic opportunities, driving the next wave of digital transformation. The future of tech integration promises a more connected, intelligent, and secure world. This research paper discusses some new concepts and fields in which cyber-crimes can be expected in the near future and this paper also discusses a few solutions to tackle the upcoming crimes and what type of laws and legislature should be adopted to prevent such.

Keywords*:* *cloud computing, blockchain data, big data, internet of things, laws.*

INTRODUCTION

In the rapidly evolving landscape of technology, four transformative forces are converging to shape the future Cloud Computing, Blockchain Data, Big Data, and the Internet of Things (IoT). Cloud Computing heralds a new era of computational power, where traditional boundaries between hardware and software blur, enabling seamless integration of diverse computing resources. This paradigm shift allows for unprecedented scalability and efficiency, empowering industries to harness immense computational capabilities like never before[1].

Blockchain Data, built on the principles of transparency, security, and decentralization, revolutionizes data management and transactions. By leveraging cryptographic techniques and distributed ledger technology, blockchain ensures immutable and auditable records, fostering trust and integrity in data exchanges across various sectors[2]. Big Data represents the exponential growth of digital information, encompassing vast volumes of structured and unstructured data. Through advanced analytics and machine learning algorithms, organizations can derive valuable insights, uncover hidden patterns, and make data-driven decisions at scale, driving innovation and competitiveness[3].

The Internet of Things (IoT) connects an ever-expanding network of smart devices, sensors, and systems, creating a dynamic ecosystem of interconnected devices. This interconnectedness enables real-time data collection, analysis, and control, empowering industries to optimize processes, enhance efficiency, and deliver personalized experiences[4].

[1] Debranjan Pal, 'Cloud Computing: A Paradigm Shift in IT Infrastructure' (2015) 38(10) CSI Communications <https://www.researchgate.net/publication/271644546_Cloud_Computing_A_Paradigm_Shift_in_IT_Infrastructure> accessed 01 May 2024

[2] Ayodele Johnson, 'The Role of Blockchain in Ensuring Data Integrity' (*Dataflaq*, 13 April 2024) <https://datafloq.com/read/the-role-of-blockchain-in-ensuring-data-integrity/> accessed 01 May 2024

[3] Asad Abbas, 'Leveraging Big Data Analytics to Enhance Machine Learning Algorithms' (2024) Department of Artificial Intelligent University of Agriculture <https://www.researchgate.net/publication/378108443_Leveraging_Big_Data_Analytics_to_Enhance_Machine_Learning_Algorithms> accessed 01 May 2024

[4] Antonio Grasso, 'Connected Human Intelligence Revolutionizing People's Abilities through IoT' (*Medium*, 23 January 2024) <https://antgrasso.medium.com/connected-human-intelligence-revolutionizing-peoples-abilities-through-iot-2ad9e23b8556> accessed 01 May 2024

Together, these four pillars of technology form a synergistic framework, laying the foundation for transformative applications across industries. From revolutionizing supply chains and optimizing healthcare to enhancing urban infrastructure and powering smart cities, the integration of Cloud Computing, Blockchain Data, Big Data, and the Internet of Things promises a future of boundless possibilities and unprecedented innovation.

CLOUD COMPUTING

Cloud computing can be described as providing computer resources over a network connection, such as the Internet. According to the National Institute of Standards and Technology, cloud computing is a model that enables easy and instant access to a shared pool of customizable computing resources, including networks, servers, storage, applications, and services. These resources can be quickly allocated and released with minimal effort from the user or service provider[5]. Upon examination of cloud computing in its current state, it is evident that numerous challenges exist in its governance, management, and categorization. One such issue is that the servers facilitating cloud computing may not be located in the same country as the clients, thus complicating the country's jurisdiction in overseeing and protecting these services.

Cloud computing plays a crucial role in the operations of businesses, service providers, and online transactions. It is relied upon for its on-demand computing services. However, the issue of security in cloud computing is of utmost importance. Any breach in security could result in significant financial losses, potentially reaching crores of rupees. It is worth noting that the value of cloud computing is projected to account for 5% of total investments in India by 2015. Unfortunately, there may be limited legal options available in such cases.

[5] Peter Mell and Timothy Grace, 'The NIST Definition of Cloud Computing, Recommendations of the National Institute of Standards and Technology' (*U.S. Department of Commerce*) <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf> accessed 01 May 2024

SECURITY THREATS IN CLOUD COMPUTING

As outlined by the Cloud Security Alliance, the primary vulnerabilities in cloud computing include:[6]

Data Breaches: These occur when unauthorized parties obtain sensitive and valuable information.

The following can be the solutions opt by the Cloud Security Alliance to tackle the issues:

- **Encryption:** Protect data in transit and at rest.
- **Access Controls:** Use multi-factor authentication (MFA) and role-based access control (RBAC).
- **Regular Audits:** Conduct frequent security audits.

Data Loss: Involves the loss of important data due to malicious activities or physical damage to hosting servers.

The following can be the solutions opt by the Cloud Security Alliance to tackle the issues:

- **Backups:** Regularly back up data to multiple locations.
- **Disaster Recovery Plans:** Maintain comprehensive recovery plans.
- Account or Service Traffic Hijacking is unauthorized access to information gained by exploiting legitimate users' security clearances or credentials.

The following can be the solutions opt by the Cloud Security Alliance to tackle the issues:

- **Strong Authentication:** Implement MFA and strong passwords.
- **Monitoring and Alerts:** Set up activity monitoring and alerts.
- **Insecure Interfaces and Application Programming Interfaces:** Security flaws in the fundamental interface systems can result in a range of security concerns.

[6] 'Cloud Security Alliance Warns Providers of 'The Notorious Nine' Cloud Computing Top Threats in 2013' (*Computer Security Alliance,* 25 February 2023) <https://cloudsecurityalliance.org/press-releases/2013/02/25/ca-warns-providers-of-the-notorious-nine-cloud-computing-top-threats-in-2013> accessed 01 May 2024

The following can be the solutions opt by the Cloud Security Alliance to tackle the issues:

- **Secure Development Practices:** Use secure coding and thorough testing.
- **Regular Updates:** Keep interfaces and APIs patched.
- Denial of Service attacks occur when malicious individuals intentionally disrupt the delivery of cloud services, causing delays or increasing the cost of these services.

The following can be the solutions opt by the Cloud Security Alliance to tackle the issues:

- **Traffic Filtering:** Use firewalls and intrusion prevention systems (IPS).
- **Redundancy and Load Balancing:** Distribute traffic across multiple servers.
- Malicious Insiders pose a threat when system administrators have improper configurations in place, allowing them unauthorized access to sensitive customer data within cloud services.

The following can be the solutions opt by the Cloud Security Alliance to tackle the issues:

- **Strict Access Policies:** Enforce the principle of least privilege.
- **Monitoring and Logging:** Monitor administrative activities.
- **Background Checks:** Conduct thorough employee background checks.
- Abuse of Services involves the misuse of cloud services, such as utilizing computational power to facilitate hacking or distributing pirated software.

The following can be the solutions opt by the Cloud Security Alliance to tackle the issues:

- **Usage Monitoring:** Watch for unusual usage patterns.
- **Rate Limiting:** Control resource consumption rates.
- Insufficient Due Diligence can result in a lack of internal controls and ambiguity in enforcing breach of contract, leaving organizations vulnerable to potential risks.

The following can be the solutions opt by the Cloud Security Alliance to tackle the issues:

- **Vendor Assessments:** Evaluate third-party vendors' security.
- **Clear Contracts:** Define security responsibilities and penalties.

- Shared technology vulnerabilities arise when customers use software that, if breached, could compromise the entire cloud-based system.

The following can be the solutions opt by the Cloud Security Alliance to tackle the issues:

- **Isolation Measures:** Use virtualization and containerization.
- **Regular Patching:** Keep software updated with security patches.

INTELLECTUAL PROPERTY AND CLOUD COMPUTING

When data is uploaded and stored on the cloud, there is a chance of generating fresh Intellectual Property. For example, within the PaaS (Platform as a service) service model (it delivers development environment as a service), consumers can develop applications utilizing the libraries and tools offered by the provider, the applications built using PaaS are offered as SaaS and consumed directly from the end users' web browsers. This gives the ability to integrate or consume third-party web services from other service platforms[7]. Without any provision in place, it would pose a challenge to ascertain the individual or entity who would hold the authorship or ownership rights to the patentable or copyrightable work produced on said platform. To resolve this matter, a definitive statement within the contract, such as clause 5 of the Dropbox business agreement, explicitly stating that Dropbox does not possess any intellectual property rights over consumer data, or the assignment of copyright, would aid in establishing ownership over any newly generated work[8].

While serving as a platform for the exchange and storage of vast amounts of data, cloud service providers face the ongoing risk of storing copyrighted material. In such cases, these providers are often shielded by safe harbor provisions. For instance, Section 111[9] in Australia stipulates that recordings made for personal use and intended for later viewing or listening do not infringe the copyright of the original work[10].

[7] Mell (n 5)

[8] 'Business Agreement' (*Dropbox*, 24 April 2024) <https://www.dropbox.com/business_agreement> accessed 01 May 2024

[9] Copyright Act 1968, s 111

[10] *Ibid*

LEGISLATION

Cloud providers in India can be held accountable for hosting illegal data, but this liability is contingent upon proving that the provider was aware of the illicit nature of the data and failed to take appropriate measures to restrict or remove it, despite being informed of the infringement. It is important to note that India is presently not a signatory of the Budapest Convention on Cyber Crime[11]; the principle of location as a connecting factor was overruled by a significant international treaty, resulting in a weakening of our position on the matter from a legal perspective. In India, the Information Technology Act of 2000[12] is the sole legislation governing cloud computing, excluding the provisions of the Indian Contract Act, of 1872[13]. This Act includes four specific provisions addressing breach and misuse of data. Section 43[14] safeguards the owner of the computer, computer system, network, or resource from any unauthorized copying, extraction, database theft, or digital profiling, while Section 65[15] protects cloud service users from tampering with computer source documents. Committing such an offence can result in a fine of up to two lakh rupees and a maximum imprisonment of three years. Section 66[16] of the Act specifically addresses computer hacking and safeguards users against any deliberate tampering or misuse of data on their devices. The consequences are identical to those outlined in Section 65[17]. Furthermore, Section 72[18] stipulates a penalty of one lakh rupees and a prison sentence of up to two years for any violation of confidentiality or unauthorized use of personal information.

Courts have widely interpreted these provisions to encompass most cases involving breaches of security or violations of privacy concerning cloud-based computing. However, the lack of specific laws governing cloud computing and the limited supervisory role of the Telecom

[11] Gowri Menon, 'Regulatory Issues in Cloud Computing: An Indian Perspective' (2013) 2(7) Journal of Engineering, Computers, & Applied Sciences <https://scholar.google.co.in/citations?view_op=view_citation&hl=en&user=_PVD8doAAAAJ&citation_for_view=_PVD8doAAAAJ:u5HHmVD_uO8C> accessed 01 May 2024
[12] Information Technology Act 2000
[13] Indian Contract Act 1872
[14] Information Technology Act 2000, s 43
[15] Information Technology Act 2000, s 65
[16] Information Technology Act 2000, s 66
[17] Information Technology Act 2000, s 65
[18] Information Technology Act 2000, s 72

Regulatory Authority of India (TRAI) leave much to be desired. While there are mentions of penal liabilities for protection, they are wholly inadequate considering the significant economic losses caused by such infringements. Therefore, the current legislative regime is entirely insufficient in addressing the regulation, protection, and supervision of cloud-based services and the potential issues that may arise.

CLOUD COMPUTING STANDARDS

Numerous companies in the cloud computing industry provide a wide range of services. The diverse terms and regulations associated with these services can present challenges for users when it comes to switching to different cloud service providers, merging data and applications across providers, or ensuring efficient audit procedures with multiple service providers. The absence of a universal standard in cloud computing not only raises concerns about interoperability but also complicates the process of comparing and assessing cloud services from the outset. These issues related to transitioning between services are commonly classified as:[19]

- **Technical:** The reliability and security concerns linked to cloud services encompass issues such as user authentication, data access authorization policies, and user credential synchronization between enterprises and the cloud[20].
- **Business:** The absence of a standard interface for auditing or assessing the environment can be a challenge in this context.
- **Semantic:** Portability and interoperability of CSPs are crucial aspects. Interoperability involves the ability to exchange information with different entities, while portability refers to the capability to transfer workload and data between providers.

One would assume that transfer and interoperability would be facilitated by setting out one uniform standard. The present scenario suggests otherwise. Instead of collectively creating a single definitive regulation, the top organizations seem to be suggesting their own set of norms.

[19] Rajinder Sandhuand and Inderver Chana, 'Cloud Computing Standardization Initiatives: State of Play' (2013) 2(5) International Journal of Cloud Computing and Services Science <https://ijcloser.iaescore.com/index.php/IJ-CLOSER/article/view/20302/12892> accessed 01 May 2024

[20] Grace A. Lewis, 'The Role of Standards in Cloud Computing Interoperability' (*Carnegie Mellon University*, 01 October 2012) <https://insights.sei.cmu.edu/documents/2235/2012_004_001_28143.pdf> accessed 01 May 2024

There are over 30 standardization initiatives conducted by approximately 20 organizations. These initiatives encompass a wide range of efforts, such as the Institute of Electrical and Electronics Engineers Standards Association's P2301[21] and P2302[22] working groups, which focus on standardization in cloud management and interoperability. Additionally, the National Institute of Standards and Technology has developed the Cloud Computing Standards Roadmap[23], which promotes the adoption of best practices and standards in this field. Various other organizations have also put forth their recommendations for effectively utilizing the organizations involved in cloud computing encompassing The Green Grid, The Cloud Security Alliance, The Distributed Management Task Force, The European Telecommunications Standards Institute, and The Storage Network Industry Association.

Additionally, in October 2014, the International Organization for Standardization (ISO) introduced fresh standards for cloud computing[24]. The collection of guidelines reportedly consists of seven unique cloud services categories, such as Network as a Service (NaaS) and Data Storage as a Service (DSaaS), in contrast to the three categories recognized by NIST (as previously mentioned)[25]. The diverse and intersecting standards appear to be causing additional delays in establishing standardized practices.

BIG DATA

'Big Data' presents enterprises, government organisations, and institutions with a multitude of creative ways to integrate complex, varied data sets[26]. By doing this, they can use a variety of data mining techniques and insights to extract hidden information and fascinating connections.

[21] 'IEEE Guide for Cloud Portability and Interoperability Profiles (CPIP)' (*Institute of Electrical and Electronics Engineers Standards Association,* 13 August 2020) <https://standards.ieee.org/ieee/2301/5077/> accessed 02 May 2024

[22] 'IEEE Standard for Intercloud Interoperability and Federation (SIIF)' (*Institute of Electrical and Electronics Engineers Standards Association,* 08 March 2022) <https://standards.ieee.org/ieee/2302/7056/> accessed 02 May 2024

[23] National Institute of Standards and Technology, *NIST Cloud Computing Standards Roadmap* (CreateSpace Independent Publishing Platform 2013)

[24] International Organization for Standardization, *Information technology — Cloud computing Part 1: Vocabulary* (2nd edn, ISO 2023)

[25] *Ibid*

[26] Marcos D. Assunção et. al., 'Big Data computing and clouds: Trends and future directions' (2014) 79-80 Journal of Parallel and Distributed Computing <https://doi.org/10.1016/j.jpdc.2014.08.003> accessed 02 May 2024

Big data is best understood as a new and revolutionary way to prepare or disclose data in databases; it is 'the nontrivial extraction of the understood, precursor complex and unquestionably essential data from data.' The preparation, management, and archiving of sizable, risky datasets is known as big data analytics. Ten attributes serve as a general definition for big data.

BENEFITS OF BIG DATA PROCESSING

Big data processing provides numerous benefits to businesses, particularly in enhancing decision-making and strategic planning. By utilizing external intelligence gathered from various data sources, companies can make well-informed decisions that take into account a broad spectrum of information. This external intelligence encompasses insights from social media platforms like Facebook and Twitter and data from search engines, which aid organizations in refining their business strategies to better reflect current market trends and customer preferences.

Furthermore, big data enables the swift identification of potential risks associated with products or services. Continuous monitoring and analysis of extensive datasets allow businesses to detect issues early, enabling them to take preventive measures and mitigate risks before they become significant problems. This proactive risk management is crucial in maintaining the integrity and reputation of a brand. In addition to risk management, big data processing significantly improves operational efficiency. By analyzing large volumes of data, businesses can streamline their processes, identify bottlenecks, and uncover opportunities for optimization. This leads to cost savings, increased productivity, and overall better performance.

In summary, the ability to process and analyze large datasets empowers businesses to make data-driven decisions, fine-tune their strategies based on real-time insights, manage risks effectively, and enhance their operational efficiency. These advantages collectively contribute to a more agile, informed, and competitive business environment.

WHY IS BIG DATA IMPORTANT?

1. Cost Savings: Big data helps in providing business intelligence that can reduce costs and improve the efficiency of operations. Processes like quality assurance and testing can involve many complications, particularly in industries like biopharmaceuticals and nanotechnologies.

2. Time Reductions: Real-time in-memory analytics allows businesses to collect information from various sources. Thanks to tools like Hadoop, businesses are now able to analyse data more quickly and make decisions quickly based on their findings.

3. Social Media Listening's: Businesses can perform sentiment analysis using Big Data tools. They can use these to get feedback and learn what people are saying about their business. Businesses can use big data tools to improve their online presence.

LEGAL ISSUES IN BIG DATA

The term 'big data' describes the quick, varied, and thorough gathering of information from many sources. Big data is produced by everything around us. Privacy and legal concerns have also been brought up as a result of the extensive collection and use of user data. This section addresses the range of legal concerns related to big data.

1. Consumer Privacy: The growing ability of powerful computers to store personal data has made large-scale information gatherings, or 'big data,' available for both lawful and illicit purposes. Big data's ability to predict the future has the potential to drastically alter our way of life. However, if you spend a lot of money online, having a lot of information exposes you to security and privacy risks as it could be maliciously misused.

2. Security of Personal Information: Big data's emergence has rapidly expedited societal developments, but there is also growing concern about the causes of data security vulnerabilities. The most knowledgeable individuals take the lead in safeguarding personal data in the big data era. Thus, it emphasises how important personal data security is.

3. Control over Data: Ownership rights over big data offer a major competitive advantage. The owner of the data has authority over it because it is also used and shared. For instance, Twitter gives different businesses that attempt to extract dirty data access to its daily tweets. The data that is obtained from the data analysis must also be owned.

4. Terms of Service Agreement (TOS): Terms of Service A formal understanding defining the responsibilities and limitations related to using a website or other online resource can be called an agreement. The protocols that reduce the possibility of client cases are described in the TOS. There is also a legal obligation in the event that the data examination yields non-out-of-line or inaccurate data.

5. Notice or Consent: Owners of data should be aware of who will use and how their data will be used. Notice also suggests awareness, meaning data owners must be aware of how they are using their information. Before using data, owners should be notified and asked for permission. Organisations should also be open and honest about the purposes and procedures for using data.

6. DNT and DNC: Another area where privacy is compromised is 'Do Not Track (DNT)'. It suggests that using a data owner's information to track them for marketing purposes is not allowed. The collection of personal data, including likes, dislikes, financial, and health information, is prohibited by the Federal Trade Commission (FDC). Tracking or collecting private and sensitive data constitutes a serious privacy violation.

INTERNET OF THINGS

The modern world has benefited greatly from technological advancements, which have improved and eased people's lives. The educational, social, health, and economic spheres, among others, have all seen widespread improvements. Smart gadgets that are always present and have Internet connectivity are referred to as the Internet of Things (IoT). IoT proponents refer to it as 'the first real evolution of the Internet,' suggesting that it has the potential to improve human well-being.[27]

[27] Dave Evans, 'The Internet of Things: How the Next Evolution of the Internet Is Changing Everything' (*Cisco,* 11 April 2011) <https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf> accessed 02 May 2024

THE CONCEPT OF THE INTERNET OF THINGS (IOT)

Three words make up the phrase '**Internet of Things**': Internet, of, and things. Researchers used a variety of scenarios in an attempt to shed light on what the 'IoT' actually is.

When things are referred to as the 'Internet of Things,' they can be understood in two ways: either as a metaphor for the web as it exists today, where objects will connect to one another, use services, generate data, etc., or, more strictly speaking, as an indication that smart things—or proxies, that is, their preventatives on the network—will use an IP protocol stack.[28] 'An emerging global Internet-based information architecture facilitating the exchange of goods and services' is how Rolf and Romana defined the Internet of Things.[29] Adam Thierer defines IoT as 'the point in time when more 'things or objects' are connected to the Internet than people' and acknowledges that the term is interpreted differently by experts and interested stakeholders. IoT is defined as 'a term for when everyday ordinary objects are connected to the Internet' via microchips and sensors.[30]

IOT PROS AND CONS

IoT is expected to have both beneficial and negative effects on modern living, as with previous technology. Positively, proponents of the Internet of Things assert that it is the first genuine evolution of the Internet and that it can improve people's lives in a variety of ways, including employment, entertainment, and education. IoT devices can be extremely helpful in the healthcare industry for controlling chronic illnesses, preventing diseases in other situations, and protecting the elderly. IoT devices that can identify falls or other disturbances can be used to track the activities and general well-being of the elderly and notify family members or emergency personnel in order to improve their quality of life. Other benefits of IoT include

[28] Friedemann Mattern and Christian Floerkemeier, 'From the Internet of Computers to the Internet of Things' (2010) From Active Data Management to Event-Based Systems and More <https://link.springer.com/chapter/10.1007/978-3-642-17226-7_15> accessed 02 May 2024

[29] Rolf H. Weber and Romana Weber, *Internet of Things: Legal Perspectives* (Springer Science & Business Media 2010)

[30] Adam Thierer, 'Privacy and Security Implications of The Internet of Things' (*George Mason University*, 31 May 2013) <https://www.mercatus.org/research/public-interest-comments/privacy-and-security-implications-internet-things> accessed 02 May 2024

safety and security. It is possible to monitor and regulate homes and other structures in order to stop theft and other risky behavior.

The biggest negative aspects of IoT are security and privacy risks. Because of the massive amounts of data generated by sensors, semiconductors, smartphones, and other devices in the Internet of Things, data volumes increase by 50–60% annually[31]. IoT may also lead to issues with employment, particularly for low-skilled employees and primary workers. The majority of everyday tasks will be performed by machines when IoT takes off. Furthermore, it is asserted that reliance on technology is still another issue related to IoT[32]. Another obstacle that can limit the advantages of IoT and hinder its adoption is technical issues.

IOT AND PRIVACY

Several recent studies list the following as ways that IoT may violate people's right to privacy:

- In the IoT era, behavior and consumption patterns—from food to entertainment—may become publicly known.
- IoT devices, such as cameras, sensors, and smart glasses, can identify a person's location and activity at any time.[33]
- In theory, an anonymous dataset can be identified because every individual has a distinct stride or walking style that may eventually allow him to be distinguished from a million other anonymous data points.
- Sensitive information, like exact location, bank account, and health, is directly collected by IoT devices as in traditional Internet;
- Habits, locations, and physical conditions collected over time may allow an entity that does not collect sensitive information to infer it; and
- Decisions about insurance, credit, and employment may be made using IoT data[34].

[31] Samuel Greengard, *The Internet of Things* (MIT Press 2021)
[32] Mattern (n 28)
[33] Samuel (n 31)
[34] Internet of Things, *FTC Staff Report* (2015)

IOT AND THE LEGAL FRAMEWORK

The most crucial step in discussing the legal framework for IoT is deciding which legal model should govern IoT. New data protection rules across the world offer instructions on how to gather, use, and retain data in the digital age. As an illustration, section 5[35] of the Malaysian Personal Data Protection Act (PDPA) 2010 outlines seven guidelines for processing personal data for commercial purposes. Every relevant stakeholder's rights, obligations, and liabilities are covered by the principles[36].

Data users must take reasonable precautions to safeguard personal information against all forms of security threats or breaches, as mandated by the Security Principle as outlined in Section 9 of the PDPA 2010[37].

Section 6 of the General Principle[38] requires data users to get consent from data subjects before processing their personal data. The legitimacy of IoT users legally presents a challenge, nevertheless, as consumers occasionally may be unaware that their gadgets are gathering personal data about them[39]. Privacy in the digital sphere can be protected with the same technology that threatens it.

One more important concern is that products and gadgets that are networked in an Internet of Things environment may not always originate from or be situated in a single country. Actually, spanning national borders and legal boundaries, servers and providers are from many nations. The legislative framework on the protection of personal data will face yet another compliance difficulty as a result. Within the Malaysian context, for instance, the transboundary transfer of personal data to non-Malaysia nations that do not offer an equivalent level of security is restricted by section 129 of the PDPA 2010[40]. Numerous significant data protection regimes worldwide contain similar rules. Thus, ensuring that all parties involved have guarantees on the

[35] Personal Data Protection Act 2010, s 5

[36] Sonny Zulhuda et.al., 'Big Data, Cloud and Bring Your Own Device: How the Data Protection Law Addresses the Impact of "Datafication"' (2015) 21(10) Journal of Computational and Theoretical Nanoscience <http://dx.doi.org/10.1166/asl.2015.6493> accessed 03 May 2024

[37] Personal Data Protection Act 2010, s 9

[38] Personal Data Protection Act 2010, s 6

[39] Data Protection Working Party (2014), art 29

[40] Personal Data Protection Act 2010

data protection rules in place—whether by legal or contractual force—will be another difficulty for data consumers and service providers to manage when handling data across borders. It is asserted that this region presents additional challenges for Malaysia and numerous other nations seeking to adopt IoT with ease.

BLOCKCHAIN TECHNOLOGY

Blockchain technology is a decentralized digital ledger that records transactions across multiple computers in a way that is transparent, secure, and tamper-resistant. Each block in the chain contains a cryptographic hash of the previous block, linking them together, hence the name 'blockchain'. Blockchain is a method of recording information that makes it impossible or difficult for the system to be changed, hacked, or manipulated. A blockchain is a distributed ledger that duplicates and distributes transactions across the network of computers participating in the blockchain.[41]

It records, stores and verifies data using decentralized techniques to eliminate the need for third parties, like banks or governments. Every transaction is recorded, and then stored in a block on the blockchain. Each block is encrypted for protection and chained to the preceding block — hence, 'blockchain' — establishing a code-based chronological order.[42]

ELEMENTS OF BLOCKCHAIN TECHNOLOGY

Decentralisation: Blockchain operates on a distributed network of nodes, eliminating the need for a central authority. This decentralisation enhances security and prevents single points of failure.

Immutable Ledger: Each block in a blockchain contains a cryptographic hash of the previous block, creating a chain of blocks. Once data is recorded on the blockchain, it cannot be altered or deleted, ensuring the integrity of the data.

[41] Ravikiran A S, 'What is blockchain technology? How does blockchain work' (*Simplilearn,* 18 October 2023) <https://www.simplilearn.com/tutorials/blockchain-tutorial/blockchain-technology> accessed 03 May 2024

[42] Brook Becher, 'Blockchain: What is it, how it works, why it matters' (*Bulletin,* 29 March 2024) <https://builtin.com/blockchain> accessed 03 May 2024

Cryptographic Hash Functions: Blockchain uses cryptographic hash functions to secure data within each block. These functions convert input data into a fixed-size string of characters, making it extremely difficult to tamper with the data without being detected.

Permissioned vs Permissionless: Blockchain networks can be either permissioned (private) or permissionless (public). Permissioned blockchains restrict access to approved participants, while permissionless blockchains allow anyone to participate in the network.

RELATED LEGAL ISSUES

Some of the most common legal challenges of blockchain technology are:

Privacy Issues: The fight around blockchain privacy and the legality of this doesn't seem to settle down anytime soon. Lawmakers are trying their best to prevent crime by removing the tools that can assist fraudsters in moving money from one place to another without being caught. While the cryptocurrency companies are pointing out that every individual has the right to privacy. The cryptocurrency community makes a fair point, but unfortunately, this also works in the favor of money launderers and other criminals.[43]

Regulatory Compliance: Governments around the world are grappling with how to regulate blockchain and cryptocurrencies. Issues include taxation, anti-money laundering (AML) laws, and securities regulations.

Smart Contracts: While smart contracts offer efficiency, they also raise legal questions about their enforceability, liability, and interpretation under existing contract law.

Intellectual Property: Ownership and protection of intellectual property rights related to blockchain technology, such as patents, copyrights, and trademarks, are significant concerns.

Jurisdictional Challenges: Determining the jurisdiction for legal disputes involving blockchain transactions conducted across borders is complex and may require international cooperation.

[43] Ahlawat & Associates, 'Top 15 Legal Issues to look out for your Blockchain Start-up' (*Lexology*) <https://www.lexology.com/library/detail.aspx?g=e2ccba98-930b-454d-8687-f402db0296f5> accessed 03 May 2024

Consumer Protection: As blockchain applications become more mainstream, ensuring consumer protection, including fraud prevention and dispute resolution, becomes essential.

Token Regulation: The classification of tokens (e.g., utility tokens, security tokens) and their treatment under securities laws is a key legal issue in blockchain ecosystems.

CONCEPT OF BLOCKCHAIN TECHNOLOGY IN INDIA AND OTHER COUNTRIES

The Government of India has been taking a keen interest in blockchain technology and its application to the public domain, as is evident from the release of the 'National Strategy on Blockchain' by MeitY in December 2021, which elucidated its vision to adopt blockchain in various sectors like healthcare, agriculture, finance, voting and e-governance, while laying the groundwork for establishing a 'National Blockchain Framework,' under which it will work towards building a national-level infrastructure for blockchain. The government is currently in the process of deploying blockchain technology for land registration, issuing digital certificates and customs duty payment. Organizations like the Telecom Regulatory Authority of India (TRAI) and the Securities and Exchange Board of India (SEBI) are also playing an active role in the adoption of blockchain in their respective sectors.[44]

OTHER COUNTRIES

Some countries like the US, Switzerland, and Singapore have developed clearer regulatory frameworks for blockchain and cryptocurrencies, providing more certainty for businesses and investors. Several governments have been proactive in promoting blockchain technology through initiatives such as funding research and development, establishing regulatory sandboxes, and integrating blockchain into public services.

In countries like the US, Switzerland, and Singapore, industries have been more aggressive in adopting blockchain technology. Financial institutions, technology companies, and supply

[44] Prateek Tripathi, 'The growing role of blockchain and Indian governance' (*Observer Research Foundation*, 27 November 2023) <https://www.orfonline.org/expert-speak/the-growing-role-of-blockchain-in-indian-governance#> accessed 03 May 2024

chain networks have actively implemented blockchain solutions to improve efficiency, transparency, and security.

CONCLUSION

A comprehensive conclusion for the convergence of computing, blockchain data, big data, and the Internet of Things (IoT) reveals a transformative landscape poised to reshape industries, societies, and economies. This synergy capitalizes on the strengths of each component to foster innovation, efficiency, and transparency across various domains.

Combining computing power with blockchain technology ensures secure, decentralized, and immutable data storage and transactions. This fusion enhances trust and reliability in data management, facilitating seamless transactions and fostering new business models. Big data analytics leverages vast volumes of structured and unstructured data generated by IoT devices, enriching decision-making processes with actionable insights. The integration of blockchain ensures data integrity and privacy, enhancing the value derived from big data analytics while preserving individual rights.

The IoT ecosystem thrives on interconnected devices that collect, exchange, and analyze data in real time. By incorporating blockchain technology, IoT networks can achieve enhanced security, interoperability, and trust among disparate devices and platforms. Together, these technologies pave the way for a future where digital ecosystems are interconnected, secure, and transparent. From supply chain optimization and smart cities to healthcare and finance, the convergence of computing, blockchain data, big data, and IoT holds the promise of driving unprecedented innovation, efficiency, and sustainability across industries and society as a whole.