Navigating Blockchain Challenges: A Comprehensive Exploration of Cybersecurity and Data Privacy in the Digital Era

Mihnea – Vlad NICOLAE
National Institute for Research and Development in Informatics - ICI Bucharest
mihnea.nicolae@ici.ro

Abstract: In this manuscript, we delineate and assess primary obstacles aimed at bridging the knowledge gap among SMEs, corporations, organizations, businesses, governmental entities, and the general public in the adoption, promotion, and utilization of Blockchain technology. The identified challenges primarily revolve around Cybersecurity and Data Privacy. Additional hurdles are expounded upon, with support from relevant literature, addressing the exploration of legal frameworks and data security management systems. This encompasses an examination of the types and variations of valid encryption, data acquisition policies and outcomes according to the General Data Protection Regulations and ISO 27001.

Blockchain, a groundbreaking method characterized by its storage permanence, offers a robust storage strategy. When integrated with a Smart Contract, it empowers users to establish partnerships, share information and provide consent through a legally-grounded system for conducting secure digital business transactions. Ethical and legal challenges vary significantly across different regions worldwide. Building trust and obtaining consent, whether in public or private sectors, for the adoption of defensive data management approaches, directly influences the efficiency of accountability and transparency mechanisms. Hence, it is imperative to invest in and research these areas to facilitate international dialogue encompassing finance, health and market strategies that address societal levels comprehensively. Through the article, we outline a system essential for conducting experiments that involve the detection, capturing, processing and storage of data. This involves the isolation of packet data to inform Cybersecurity levels and privacy-related activities while ensuring transparency is demonstrated in a secure, intelligent and efficient manner.

Keywords: Blockchain, SMEs, Cybersecurity, Data Privacy, Smart Contracts, Encryption.

INTRODUCTION

With the recent emphasis on society's increasing reliance on cloud technologies and the fundamental human need for digital communication and data exchange, Internet of Things devices, including smartphones and various industrial and household appliances, continue to play vital roles in business operations. Social interactions and different types of transactional data, such as those affecting financial markets, drive the rapid advancement of emerging technologies to keep up with supply and demand trends.

https://doi.org/10.54851/v6i1y202409

In domestic environments, the sharing of digital media (like images, videos, documents or music) via messaging services enriches various fields such as information technology, education, health and social sciences. Internet of Things devices facilitate the fast and efficient transfer of data through the Internet of Everything (IoE) via the cloud. In industrial contexts, Smart Sensors, Application Programming Interfaces (APIs), and Internet of Things networks enable remote work across digital boundaries on a global scale.

Instances of potential data sharing or criminal activities, which can lead to severe consequences, impact the confidentiality and safeguards established by governments, businesses and organizations. This scenario often results in legal and ethical disputes with significant financial repercussions, particularly in the case of Denial of Service (DDoS) attacks. Such attacks have the capacity to cause substantial damage and disruptions to entire business data infrastructures, network architectures and services on a large scale.

As society increasingly depends on the exchange and processing of Personal Identifiable Information via the Internet of Things (IoT), trust in reputable institutions, government bodies, broadcast, and digital media outlets becomes a critical concern. When users choose to share personal and sensitive information, such as during online shopping, they should be aware of the nature and intentions of cybercriminal activities and have faith in the criminal justice system. On the other hand, businesses, organizations, government agencies, and academic institutions require the capability to globally validate and authenticate their data to effectively serve societies. The integration of Artificial Intelligence, Big Data and Blockchain plays a significant role in combating cybercrime while enabling legal entities to hold companies, organizations and institutions accountable with the help of new technologies and methodologies. A notable approach in this regard is the utilization of Smart Contracts (SC), which, for example, enhances the legal credibility and value of financial transactions when utilized in drafting and consenting to a legal document or digital certificate. As part of the Blockchain functionality, the Smart Contract undergoes validation, implementation and sharing across a Peer-to-Peer (P2P) network as a Distributed Ledger Technology (DLT), ensuring transparency and accountability visible to all the parties involved.

CYBERSECURITY

When incorporating cybersecurity components, these technical prerequisites aid in efficiently overseeing Internet of Things hardware and software operations, physical interfaces and the formulation of internal policies. Moreover, the ISO 27001 management system endorses data access control, network communication protocols and cryptographic measures (such as password encryption). These elements collectively contribute to establishing a resilient and secure communication methodology, encompassing staff training in cybersecurity, all the while mitigating network communication attacks in the face of potential malicious third-party interventions (Rawindaran, Jayal & Prakash, 2021).

Yet, to effectively leverage and extract value from the abundant volume, diversity, and accuracy of available data, concepts like Big Data, Artificial Intelligence and Machine Learning employ predefined analytical methods and algorithms across extensive amounts of public and private (sensitive data) transmitted with the use of digital networks. This approach significantly heightens the risk of data breaches, viruses and malicious attacks. Simply put, successfully employing these technologies for the lawful acquisition and processing of data from both the public and private sectors, along with implementing practical user measures, can potentially unveil challenges and vulnerabilities, further exposing individuals or groups to cybercriminal activities.

Cybersecurity is defined as „a measure for protecting computer systems, networks, and information from disruption or unauthorized access, use, disclosure, modification or destruction” (Gallaher, Link & Rowe, 2008). Consequently, delving into the comprehension of cybersecurity and its relevance to IoT and smart devices raises additional inquiries that

necessitate analysis within various facets of cyberspace. One potential solution involves consolidating the aforementioned terminologies to underscore the significance of understanding the origins of network intrusion, the methods of detection and the mechanisms for preventing cyber threats. In terms of prevention, the utilization of AI and ML may also potentially contribute to the increasing adoption of this technology for safeguarding and securing data (Zarpelão, Miani & Kawakani, 2017).

DATA PRIVACY IN THE DIGITAL AGE

The ISO 27001 framework operates in conjunction with the General Data Protection Regulation (GDPR) Regulation (EU) 2016/679 and Data Protection Act 2018 c. 12 (DPA), aiding in the implementation of controls and measures for personal data within the digital boundaries of the UK and the European Union (EU). For the processing of medical data, a compulsory Data Protection Impact Assessment is conducted to identify and assess risks, guided by eight core principles, including the use of lawful and ethical methods for data acquisition, ensuring the security and duration of data storage, promoting fair use and stipulating specific locations and regions for data retention (Wylde et al., 2021).

By integrating these frameworks and management systems, tracking tools like cookies, for instance, may illegitimately leverage the aforementioned AI, ML and algorithmic analysis. Consequently, users may remain unaware of the tracking capabilities embedded within the software, designed for analysis and for marketing purposes. Moreover, the absence of user consent and the necessary ongoing maintenance awareness regarding these cookies, essential for web browsing, could potentially expose business networks to anti-forensic techniques, legal jurisdiction complications, breaches of system hardware and violations of Service Level Agreements (SLAs). These issues can accumulate over time, exacerbating the technical, legal and ethical challenges associated with operating IoT devices in a compliant, safe and secure business environment.

The real problem with cookies is that people don't really seem to fully understant how they really function. Cookies have the capability to retain significant personal data. Similar to any confidential information, it's crucial for users to understand how companies might utilize their cookies. Hence, what precisely do individuals perceive cookies to be employed for? All About Cookies conducted a study in 2023 on 1000 US adults to see how many poeple know about what cookies are and what functions they serve. They have provided a compilation of both genuine and fake ways through which websites utilize cookies to capture people's actual understanding.

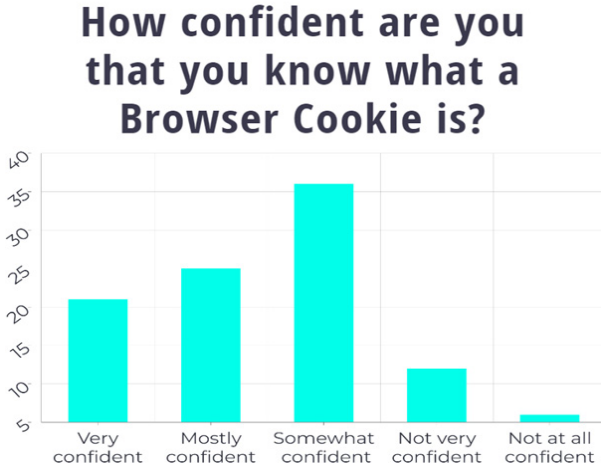

Figure 1. *Knowledge about cookie definition (Source: Josh Koebert, 2024).*

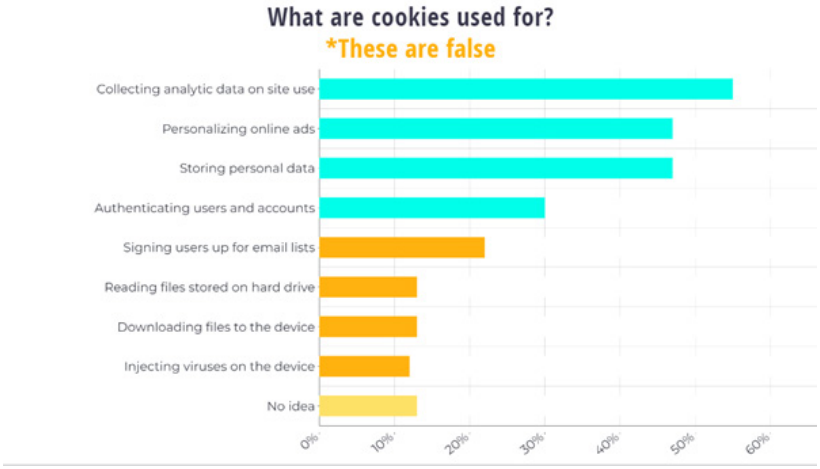

Figure 2. *Knowledge about cookie use (Source: Josh Koebert, 2024).*

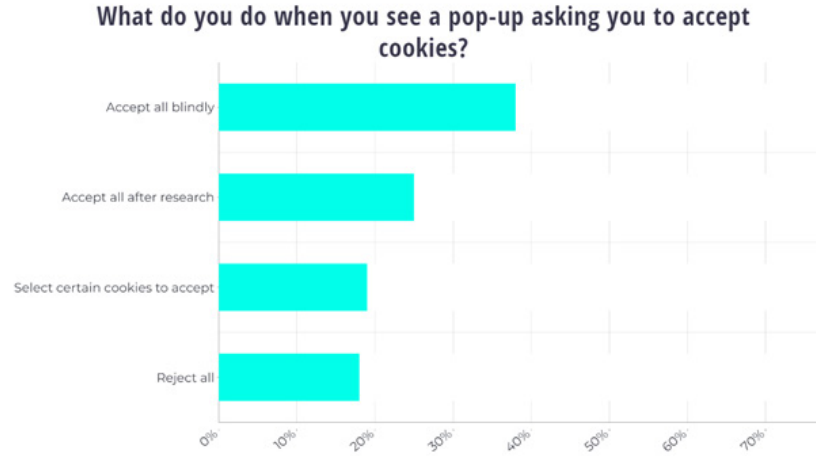

Figure 3. *Behavior regarding cookie acceptance (Source: Josh Koebert, 2024).*

In the context of healthcare services, the implementation of a Smart Contract (SC) policy featuring cryptography as a cybersecurity control method provides transparency, secured agency and accountability to the public, financial markets, business professionals and legal representatives. This ensures the validity and transparency of actions or investigations conducted on behalf of the directorate or client. When applied retrospectively, this approach also instills accountability in maintaining resilience and vigilance in managing cyberspace. It emphasizes the operator's duty of care and consideration regarding confidential data breaches, their sharing, and the consequences of exposing extensive amounts of confidential National Health Service (NHS) patient data, for example (Balasubramanian et al., 2021).

BLOCKCHAIN

Blockchain functions, methods and systems incorporate elements such as Cryptocurrency (e.g., Bitcoin and Ethereum) as substitutes for traditional currencies, off-chain storage, anonymous digital signatures and non-interactive zero-knowledge proofs. When integrated with internal corporate or organizational audits, policy implementations, healthcare provider functions, and security services for legal and domestic activities, these concepts ensure validity, anonymity, and

transparency. This inherently trustless design holds the potential for fair and transparent transactions.

The integration of Blockchain and Smart Contracts serves a dual purpose: as a means of conveying information and as a platform for evaluation, validation, and eventual testing using predefined control protocols. In order to minimize human intervention, an intelligent automated approach is employed to capture network data at predetermined intervals. This combination of technologies not only enhances efficiency but also ensures a reliable and consistent method of data collection, contributing to streamlined operations and increased accuracy in decision-making processes. This can become very useful in the domains of:

- Finance and Banking: Streamlining financial transactions, ensuring secure and transparent record-keeping, and automating contract execution in the banking and financial sectors;
- Healthcare: Securing patient data, managing medical records, and facilitating transparent and auditable transactions among healthcare providers, insurers, and patients;
- Legal and Contractual Agreements: Automating contract execution, ensuring compliance with terms and conditions, and providing a tamper-proof record of legal agreements;
- Supply Chain Management: Enhancing transparency, traceability, and efficiency in supply chain processes, from sourcing raw materials to delivering finished products to consumers and many more.

INTERNET OF THINGS AND MACHINE LEARNING

As Information Technology infrastructure expanded, the broader realm of digital technology experienced growth with an increasing number of devices are being connected to the internet. This interconnectedness allows for unfettered access to data, facilitating the execution of various activities and enabling predictive outcomes. Consequently, to address these developments, diverse mathematical algorithms in Machine Learning (ML), such as Support Vector Machines, Neural Networks and Decision Trees come into play for classification purposes. These algorithms collectively illustrate how data is processed and managed to generate outcomes, fostering predictability crucial for contributing to economic growth as society is progressing. The capabilities of ML extend beyond conquering human pastimes, extending into everyday tasks and events in our daily lives.

Real-life applications of ML are evident in various industries, where it is employed to identify false news, implement spam filters, detect fraudulent or criminal activities online and enhance marketing campaigns. Despite the widespread use of large quantities of private and sensitive data in Cyberspace, which often traverse through digital networks, the existence of cyberspace creates a broader security attack surface, increasing the risk of potential malicious activities. This underscores the significant impact of human factors on the security of IoT (Biju & Mathew, 2020).

The way humans perceive security and privacy in relation to these devices is also a topic for discussion. An example of this is the concept of ‚Cookies' as a tracking tool for online web browsing and the safety measures associated with it. This often becomes a debated subject and the awareness of how it should be used is sometimes overlooked (Cahn et al., 2016). However, recent reports indicate that numerous questions emerge when trying to understand the Internet of Things and the protective measures surrounding it, along with how humans adapt and coexist with Internet of Things. Factors such as anti-forensic methods, Service Level Agreements and jurisdiction exacerbate technical, privacy, security and legal challenges. Furthermore, the coexistence of GDPR and IoT, along with the human elements involved, presents significant challenges in ensuring the safety and security of these devices.

SMALL TO MEDIUM ENTERPRISES

UK Small to Medium Enterprises (SMEs) have consistently grappled with challenges in comprehending cybersecurity, given the escalating threats shown in recent years. The European Commission sets the employment criterion for a minimum cyber-criterion for SMEs as any business with fewer than 250 employees (Cahn et al., 2016). The challenges faced by SMEs are twofold, involving both operational and commercial aspects, as they incorporate Intrusion Detection mechanisms alongside AI and ML techniques to safeguard their data.

In a 2020 study conducted by BullGuard on 3000 small UK and US businesses they found out that "small businesses are over confident and underprepared" as seen in figure 4.



Figure 4. *Results from a study on SME cybersecurity preparedness (Source: Vanessa McGreevy, 2020).*

For SMEs, the implementation of intrusion detection methods has become imperative to ensure the security and integrity of their data, especially with the integration of real-world objects and IoT. Understanding how Machine Learning techniques and Artificial Intelligence can contribute to securing against zero-day attacks and preventing them is crucial. In a study by Rawindaran, Jayal & Prakash (Rawindaran, Jayal & Prakash, 2021), particular attention was given to the SME market. The study presented an experimental scenario comparing intrusion detection and prevention models while examining the perspectives of SMEs. The research explored various approaches to identify ways of detecting and protecting against network intrusions and the operating devices that would facilitate this process.

Additionally, the paper delved into the challenges of safeguarding data and how government policies and procedures could support this endeavor.

CHALLENGES AND OPPORTUNITIES IN SME CYBERSECURITY

Rawindaran, Jayal & Prakash (Rawindaran, Jayal & Prakash, 2021) conducted a thorough examination of the impact of threat levels from various attacks, including Malware, Ransomware, Phishing and Social Engineering, among others. The comparison was made between an Open-Source device like SNORT (an open source Intrusion Prevention System) and pfSense (an open source firewall) and Commercial Network Intrusion Detection Systems (NIDs) such as Cisco. The study evaluated three different NIDs and compared their features. The findings suggested that while SNORT and pfSense, being open-source, were freely available, their implementation required a certain level of expertise to integrate them into a business model.

The study highlighted the need for businesses and organizations, with the support of government policies and processes, to

collaborate in combating hackers, malicious actors, and their bots while staying proactive and adaptive (Gallaher, Link & Rowe, 2008). The paper delved into various Machine Learning (ML) approaches, such as signature-based models and anomaly-based rules employed by these devices to counteract attacks (Dunham & Melnick, 2008).

Furthermore, the paper underscored the limitation of signature-based models, which could only identify known attacks, whereas anomaly-based systems demonstrated the capability to detect unknown attacks (Kabiri & Ghorbani, 2005). However, despite the potential advantages of anomaly-based NIDs, their maturity posed high operational costs and demanded computing power that was impractical in the SME environment. As anomaly-based NIDs are still in the early stages of development, a more in-depth analysis and future studies are warranted.

Rawindaran's research offered valuable insights for more comprehensive comparisons and relative conclusions, emphasizing the significance of delving further into both empirical and scenario analyses across various dimensions. The study highlighted the evolving nature and contextual intricacies of cybersecurity in today's interconnected world of the internet and cyber connections. Additionally, Machine Learning (ML) techniques have become indispensable to the operations and commercial environment of Small to Medium Enterprises (SMEs) in the UK, delving into success stories from major technology companies like Amazon, Google, and Facebook, which have effectively utilized ML techniques for their cybersecurity measures (Fraley & Cannady, 2017). The research methodology employed structured survey questions directed at a selected sample of respondents, focusing on SMEs' management, technical, and non-technical professionals.

HOW CAN MACHINE LEARNING HELP SMES?

Awareness of Machine Learning and its applications is currently undergoing a learning curve and lacks a definitive definition. The study highlighted the three primary categories of ML: Supervised Learning, Unsupervised Learning, and Reinforcement Learning, along with the algorithms underpinning them (Buczak & Guven, 2016). Instances of Supervised Learning encompassed real-world applications like predictive text in tweets on Twitter, product reviews on platforms such as Amazon and eBay, as well as calculations related to temperature, insurance premiums, pricing, and workforce numbers in relation to a business's revenue.

Examples of Unsupervised Learning included the identification of false news, the implementation of spam filters, the detection of fraudulent or criminal activities online, and the optimization of marketing campaigns. Reinforcement Learning was exemplified by scenarios where algorithms in video games receive rewards for specific actions. Each learning method employed algorithms for calculations and predictions, along with datasets contributing to their development and application structures. The study also quantified examples, demonstrating the impact of ML on SMEs' perceptions and awareness of its applications.

The focus of this study revolved around the incorporation of ML methods and algorithms into SMEs' cybersecurity software packages. Further analysis revealed the existence of algorithms such as Neural Networks, Support Vector Machines, Deep Networks, and Bayesian methods, many of which were intricately embedded within the utilized software.

The first concept of employing an Intrusion, Detection, and Prevention System method, sourced from either a commercial or Open-Source device, to safeguard SME data requires a foundation in the understanding of Machine Learning (ML) and Artificial Intelligence (AI). As hackers become more sophisticated and the prevalence of bots increases, their methods of attack necessitate the reliance on ML and AI technology as protective measures for systems. An IDPS system, utilizing ML, aids in learning about malicious patterns in contrast to valid patterns on the internet. These diverse approaches are crucial for the protection and defense of data. ML, specifically through

anomaly detection, has proven to be more effective in zero-day detection compared to signature-based methods, demonstrating its efficacy in cybersecurity and its adoption within UK SMEs. There exists a substantial gap that could potentially be addressed through greater diversity in the devices used for SMEs, incorporating open-source solutions and leveraging the knowledge of voluntary participants within the community to ensure the future resilience of these devices.

The escalating use of Machine Learning in Intrusion Detection Systems and Intrusion Detection and Prevention Systems within the cybersecurity frameworks of Small and Medium-sized Enterprises (SMEs) has given rise to a novel form of attack known as Adversarial Machine Learning (AML). Anthi et al. (2021) emphasize that the deployment of ML-based IDSs introduces additional attack vectors aimed at compromising the ML algorithms, leading to potential bypasses in these security systems. Such Adversarial Machine Learning attacks pose a significant threat by causing delays in attack detection, potentially resulting in infrastructure damage, financial losses, and even posing risks to human lives. The integration of Industrial Control Systems (ICS) into national infrastructure, such as manufacturing, power grids, water treatment plants, and healthcare, further exacerbates the vulnerability to AML attacks, particularly as ICS becomes more interconnected with the internet.

The increased reliance on ML in IDSs has become a daily tool for attack detection, making the study of AML crucial. Their research demonstrates how AML targets supervised models by generating adversarial samples and exploiting classification behaviors, using authentic power system datasets to train and test supervised machine learning classifiers. Two prominent AML testing methods, the the Jacobian based Saliency Map Attack and the Fast Gradient Sign Method, illustrate how AML can penetrate systems through ML training models, leading to cyber attacks. Another study by Catak, Catak & Moldsvor (2021) explores the security concerns associated with AML in the context of 6G applications for communicative technology. Focusing on deep learning methods and training in 6G networks, the research identifies Adversarial Machine Learning attacks using Millimeter Wave (mmWave) beam prediction and employs mitigation and prevention methods to enhance 6G security. The paper concludes that introducing faulty results in iterations improves the security and performance of the device, enabling ML algorithms to adapt and enhance predictive capabilities against adversarial attacks.

BALANCING ETHICS AND LEGAL COMPLIANCE: GDPR, DATA PROTECTION IMPACT ASSESSMENTS AND GLOBAL COLLABORATION

In GDPR Recital 4 and the preceding Directive 1995/46/EC Recital 2, a key objective is stated: „the processing of personal data should be designed to serve mankind." In pursuit of this objective, the Data Controller is responsible for ensuring legal compliance and justifying data processing based on necessity (beyond mere convenience) and proportionality. GDPR specifically mandates the performance of a Data Protection Impact Assessment (DPIA) when acquiring high-risk health data, aiming to mitigate risks and assess risk levels to determine whether the data should be processed (Guinchard, 2021). The collaboration between the EU and the United Kingdom in data protection laws underscores principles of cooperation, ethics, transparency, and robust control methods to mitigate breaches of data privacy. However, this also highlights the importance of considering various legal frameworks and the global movement of people, urging governments and businesses to adopt comprehensive data protection strategies.

LEGAL FRAMEWORKS OF DATA PRIVACY

In the collaboration between the EU and United Kingdom, the Data Protection Act 2018 and the General Data Protection Regulations 2016 (GDPR) work in tandem to regulate the utilization of personal data by businesses, organizations, and governments.

Eight fundamental objectives provide guidance for those handling and processing personal data, strictly mandating that data acquisition must be lawful, fair, accurate, and up-to-date. Additionally, the data should not be retained longer than necessary, must be kept safe and secure, and should not be transferred outside the European Economic Area. GDPR, by its design, incorporates principles that align with human rights and includes additional guidelines for data collection and processing, such as defining purposes, data types, and processing duration (Tran & Ngoc, 2020).

In the collaborative effort to curb the transmission of diseases during the ongoing Covid-19 pandemic, the cloud, cellular networks, and IoT devices like smartphones, sensors, and household appliances continue to play crucial roles in various global Tracing-Testing-Tracking initiatives. Diverse approaches are being adopted worldwide to minimize person-to-person transmission (Juneidi, 2020). This highlights that, in response to the pandemic and the imperative to swiftly develop and implement digital solutions, managing data privacy implications becomes increasingly complex, with growing risks to data privacy. Consequently, research on the handling of personal data acquisition has evolved and majorly expanded (Majeed & Lee, 2021).

However, addressing data privacy risks amidst challenging environmental and social conditions requires more than just implementing digital solutions. Challenges related to service delivery, such as consistency, proportionality, and transparency, also increase the likelihood of data privacy breaches. Therefore, in terms of scalability via cloud infrastructure, collaborations between communities, businesses, and governments are necessary to synchronize policy development and implementation with digital solutions.

In a survey conducted in the Republic of Ireland involving over 8000 participants, it was found that 54% would be open to using a contact tracing app. Similarly, a survey in the UK with 2000 participants showed that 55% would be willing to utilize a government-controlled app, with a higher acceptance rate specifically for the National Health Service contact tracing app (Raman et al., 2021). This data highlights a reluctance among 45% of the British population to adopt the app, potentially undermining the government's effectiveness in managing the collection and processing of sensitive medical data.

Conversely, in some countries, citizen consent is implied when data collection is initiated for the public good, granting private entities access to data with government approval. Amnesty International (2020) has highlighted numerous instances of questionable data privacy practices across various countries (Raman et al., 2021). These examples emphasize the diversity in perceptions and attitudes towards data protection, underlining the necessity for a more focused and intensive approach to collaborative research on data privacy. By analyzing various legal and regulatory frameworks, solutions and practices during a pandemic or crisis, valuable insights can be gained to implement robust and scalable outcomes effectively. For example, ensuring robust and transparent data is crucial for the urgent Covid-19 vaccine distribution efforts in each country.

In response to the pandemic, the United Kingdom Government and the NHS X (Digital) contact tracing app, in collaboration with the private sector, faced scrutiny regarding their overall GDPR utility and compliance. The subcontractors and companies representing NHS X are also considered data processors, adding additional pressure for GDPR compliance. Notably, the NHS X app code and Data Protection Impact Assessment were voluntarily submitted to the Information Commissioner's Office, excluding the data store. This potentially indicates a lack of transparency regarding GDPR compliance, health surveillance capabilities, and data storage capacities. For instance, the Joint Committee on Human Rights expressed concerns about the rapid development and deployment of the contact tracing app in March 2020 (Guinchard, 2021).

DATA STORAGE

Precise definitions and effective solutions are imperative for data and storage methods. Currently, there is a need for an integrated and comprehensive understanding of internal organizational personal data storage, a thorough comprehension of regulation across the entire organization, and an auditable trail of essential data processing activities (Tran & Ngoc, 2020). While GDPR compliance has notably improved personal data protection, addressing aspects such as Personally Identifiable Information (PII) sharing via ads and marketing, collection and sharing of location data, child PII sharing, law enforcement data access, and data aggregation, further research is essential to facilitate a user's right to erasure, update, and deletion of data, ensuring complete satisfaction of the GDPR commitments (Zaeem & Barber, 2020).

ACCOUNTABILITY

For enhancing government transparency and fostering societal trust, a component of the solution involves robust data privacy and accountability policies. Antal et al. (2021) discuss the effectiveness of Blockchain in ensuring traceability, transparency, vaccine identification, and the secure delivery and storage of vaccines, including mechanisms for self-reporting side effects. The authors propose a Blockchain strategy that leverages the inherent integrity and immutability of Blockchain, particularly in the context of beneficiary registration for vaccination, thereby eliminating the risks of identity impersonation and theft.

An illustrative example from Honduras showcases the launch of ‚Civitas' by a Toronto-based technology, employing user and government-linked IDs on a Blockchain-based network. The Blockchain contains essential data to determine when an individual can purchase medicine, go grocery shopping, and informs government agencies for resource and deployment strategies. Notably, this contact tracing methodology may conflict with the General Data Protection Regulation (GDPR). For instance, the GDPR's right to erasure may pose challenges due to Blockchain immutability and processing speed, potentially inhibiting Blockchain network uptake and scalability.

However, in this scenario, Blockchain could operate within the management and governance confines of Big Data repositories and warehouses, utilizing Smart Contracts to enhance accountability, transparency, and consistency in the appropriate forum.

INTEGRITY OF DATA

Blockchain stands out as one of the most frequently discussed Distributed Ledger Technologies (DLT) designed to ensure data storage and exchange integrity in trust-less and distributed environments. Functioning as a Peer-to-Peer (P2P) decentralized distributed ledger (Zheng et al., 2017), Blockchain facilitates trusted data exchanges among participants in a network, even if they are considered untrusted. Notably, Blockchain systems like Hyperledger Fabric and Ethereum have gained popularity as frameworks for various Blockchain-based software applications. The fundamental features of Blockchain, including immutability and decentralization, are widely acknowledged across sectors like healthcare and finance, offering improvements to their operations. Despite being a relatively recent technology, having emerged just over a decade ago, Blockchain has proven to be revolutionary, with a substantial body of research articles and white papers supporting this assertion.

HOW CAN BLOCKCHAIN HELP CYBERSECURITY?

Addressing how emerging technologies like Blockchain can provide solutions to counteract evolving cybersecurity threats is a crucial inquiry, with significant research interest directed toward exploring how Blockchain can establish the foundations for robust internet security infrastructures (Salman et al., 2019). Numerous articles propose frameworks, prototypes and experimental

beta Blockchain-based solutions designed to address challenges in complex computing systems. Many of these experimental solutions are developed on platforms such as Ethereum and Hyperledger Fabric. Hyperledger Fabric, for instance, is favored for its ease of software development, extensive customizability and interactivity.

Despite Bitcoin's popularity as a Blockchain network, it comes with drawbacks such as latency and substantial resource requirements. Some practical solutions employ innovative techniques to tackle critical cybersecurity issues. However, these solutions often suggest changes to existing system infrastructures that may be challenging to test promptly for efficiency and effectiveness compared to traditional cybersecurity frameworks (Zhang et al., 2019).

INTERNET OF THINGS

In our increasingly interconnected Internet of Things (IoT) landscape, there is a pressing need to enhance cybersecurity. As elucidated in (Pinno, Gregio & De Bona, 2017), the emergence of cyber-attacks exploiting vulnerabilities in IoT devices has raised serious concerns, necessitating appropriate mitigation strategies to address these threats. A captivating area of research revolves around ensuring the integrity of data management and detecting/preventing malware (Kshetri, 2017).

It's important to acknowledge that Blockchain cannot completely eradicate cyber risks; however, it holds the potential to significantly mitigate cyber threats through its core features. While most Information Technology systems are constructed with security frameworks utilizing advanced cryptographic techniques and they often depend on centralized third-party intermediaries like certificate authorities to guarantee the integrity of their data management. Exploiting weaknesses in such centralized relationships, malicious parties can disrupt or penetrate these systems with cyber threats like Distributed Denial of Service attacks, malware, ransomware and so forth.

PROTOCOLS

Blockchain offers a solution to these challenges through its decentralized nature, which eliminates single points of failure and the reliance on third-party intermediaries in IT systems. It ensures the integrity of data storage and exchange through encryption and hash functions (Ali et al., 2016), empowering data owners to fully audit their data within the systems.

A blockchain network, characterized by numerous mutually untrusting nodes, provides greater security compared to networks with few nodes relying on trusted or semi-trusted centralized intermediaries. In a blockchain network, every node maintains a complete copy of the unique record of all transactions, facilitated by the network consensus protocol. The robustness of a blockchain network, in terms of its safety and security, hinges on its decentralization, which, in turn, is governed by its governance and consensus protocols. A comprehensive comparative analysis of Distributed Ledger Technology (DLT) consensus protocols is offered by Shahaab et al. (2019).

GDPR IN BLOCKCHAIN

GDPR and Blockchain Enormous quantities of Personally Identifiable Information (PII) are being illicitly collected, screened, and utilized through cyber-espionage, phishing, spamming, identity theft and malpractice. Blockchain, on the contrary, poses a challenge to GDPR due to its inherent immutability in design and its utility in tracking, storing and distributing data in Distributed Ledger Technology (DLT). This clash is particularly evident in relation to GDPR's „Right to be forgotten", which includes various rights to erasure (Al-Zaben et al., 2018). Here, the authors propose a framework that operates on a separate off-chain mechanism, storing PII and non-PII in distinct locations. While not a perfect fit, this example demonstrates how, by design, a compliant use-case can be enhanced to fulfill parts of GDPR and it emphasizes the importance of designing and regulating network participation to meet GDPR requirements.

IDEAL FRAMEWORK

An ideal framework for efficient and secure data management should seamlessly integrate various components to ensure reliability, transparency, and accountability throughout the system. At its core, the Blockchain Layer establishes a foundation of trust and immutability, with Distributed Ledger technology forming a fundamental component to maintain transparent and tamper-proof records. Smart Contracts, working in conjunction with the Distributed Ledger, automate and enforce agreements, enhancing efficiency and reducing the risk of errors.

The framework's Data Security Management System incorporates industry-leading standards such as ISO 27001, along with robust encryption techniques, to safeguard sensitive information against unauthorized access and breaches. Advanced analytics capabilities, including machine learning models, are utilized within the Big Data Analytics component to extract valuable insights from vast datasets, empowering informed decision-making and driving business growth.

Artificial Intelligence, encompassing machine learning models, plays a pivotal role in optimizing processes and enhancing automation across the framework. Visualization tools enable intuitive data exploration and interpretation, while IoT Devices Integration facilitates the seamless collection of real-time data, enriching analytics and enhancing operational efficiency.

Network Security Protocols, encompassing cybersecurity measures, ensure the confidentiality and integrity of data transmission within the framework, addressing concerns related to data security and privacy. Legal and Ethical Compliance are paramount, with features such as GDPR Compliance and consideration of broader legal frameworks ensuring adherence to regulatory requirements and ethical standards.

A transparent and accountable system is maintained through the integration of Decentralized Trust mechanisms and a focus on Data Integrity. Specific modules for data handling incorporate Decentralized Trust to ensure reliability and authenticity, while also prioritizing Data Integrity to uphold the integrity of information throughout its lifecycle.

In summary, an ideal framework for data management should encompass a holistic approach, integrating various technologies and best practices to ensure security, reliability, and compliance. By leveraging Blockchain technology, advanced analytics, IoT integration, and stringent security measures, organizations can build resilient systems capable of meeting the challenges of the digital age while fostering trust and transparency.

CONCLUSION

To establish an effective cybersecurity strategy for SMEs and similar entities, the collaboration between government and private sector financial initiatives is imperative. This collaboration should encompass initiatives for raising awareness and providing training for management, along with ongoing support for staff to seamlessly integrate machine learning (ML) and artificial intelligence (AI) into the workplace. By implementing intrusion detection and prevention policies at various levels, from SMEs to government, the comprehensive benefits and protections of cybersecurity against cybercriminal activities can be sustained and promoted. However, the global interpretation of this concept varies, posing formidable challenges in terms of legal, ethical, and consensual implementation. The extensive collection of personal data across regional divisions to support authorities in resource strategy necessitates a foundation of trust in institutions and technologies for mutual benefit.

Ensuring accountability and transparency demands continuous evaluation of legal frameworks, systems and outcomes, requiring substantial investments from both the public and private sectors. Societal benefits can be substantial through increased public

awareness, enhanced perception, and confidence in the justice system, achieved through transparent and educational measures. Policies addressing mental illness and engaging minority groups can contribute significantly to societal well-being. While the previously proposed framework in research presents a robust and intricate strategy, the evolving landscape poses real-time challenges for SMEs in adopting technology, particularly with Blockchain network latency. The growing trend of digitalization and decentralization leads to diverse communications but concurrently creates a broader attack surface for potential adversaries.

This review paper sheds light on various security challenges arising in digital systems, computational data, and associated trust mechanisms. The diversity of current solutions spans from initial stages in small organizations to state-of-the-art implementations in large-scale enterprises. The dynamic nature of the cyber landscape suggests that further changes are likely, necessitating robust solutions. The paper integrates research insights from various collaborators, aiming to identify challenges and pave the way for designing novel solutions. The ultimate goal is to enhance and establish secure cyber systems that comprehensively address data security concerns.

REFERENCE LIST

Al-Zaben, N, Hassan Onik, M. M., Yang J, Lee N.-Y. & Kim C. S. (2018) General data protection regulation complied blockchain architecture for personally identifiable information management. In: *2018 International Conference on Computing, Electronics & Communications Engineering (iCCECE), 16-17 August 2018, Southend, UK.* IEEE. pp. 77-82

Ali, M., Nelson, J, Shea, R & Freedman M. J. (2016) Blockstack: a global naming and storage system secured by blockchains. In: *Proceedings of the 2016 USENIX Annual Technical Conference (USENIX ATC '16), 22-24 June 2016, Denver, USA.* Berkeley, California, USENIX Association. pp. 181-194.

Antal C, Cioara, T., Antal, M. & Anghel, I. (2021) Blockchain platform for COVID-19 vaccine supply management. *IEEE Open Journal of the Computer Society.* 2, 164-178. doi: 10.1109/OJCS.2021.3067450.

Anthi, E., Williams, L., Rhode, M., Burnap, P. & Wedgbury, A. (2021) Adversarial attacks on machine learning cybersecurity defences in industrial control systems. J*ournal of Information Security and Applications.* 58, 102717. doi: 10.1016/j.jisa.2020.102717.

Balasubramanian, R., Prakash, E., Khan, I. & Platts, J. (2021) Blockchain technology for healthcare. In: T*he 5th Advances in Management and Innovation Conference 2021, AMI 2021, 20-21 May 2021, Cardiff, UK.*

Biju, S. M. & Mathew, A. (2020) Internet of Things (IoT): securing the next frontier in connectivity. In: *International Journal of Scientific Engineering and Science.* 4(5), 18-21, ISSN. 2020.

Buczak, A. L., Guven, E. (2016) A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials.* 18(2), 1153-1176. doi: 10.1109/COMST.2015.2494502.

Cahn, A., Alfeld, S., Barford, P & Muthukrishnan, S. (2016) An empirical study of web cookies. In: *Proceedings of the 25th international conference on world wide web, WWW '16, 11-15 April, 2016, Montréal, Canada*. Republic and Canton of Geneva, International World Wide Web Conferences Steering Committee. pp. 891-901.

Catak, E., Catak, F. O. & Moldsvor, A. (2021) Adversarial machine learning security problems for 6G: mmWave beam prediction use-case. In: *2021 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), 24-28 May 2021, Bucharest, Romania.* IEEE. pp. 1-6.

Dunham, K. & Melnick, J. (2008) *Malicious bots: an inside look into the cyber-criminal underground of the Internet.* Boston, Auerbach Publications.

Fraley J. B. & Cannady, J. (2017) The promise of machine learning in cybersecurity. In: *SoutheastCon 2017, 30 March - 2 April 2017, Concord, USA.* IEEE. pp. 1-6.

Gallaher, M. P., Link, A. N. & Rowe B. R. (2008) *Cyber security: economic strategies and public policy alternatives.* Cheltenham, Edward Elgar Publishing.

European Parliament, Council of Europe (2016) *General Data Protection Regulation (GDPR).*

Guinchard, A. (2021) Our digital footprint under Covid-19: should we fear the UK digital contact tracing app?. *International Review of Law, Computers & Technology.* 35(1), 84-97. doi: 10.1080/13600869.2020.1794569.

Josh Koebert (2024) AllAboutCookies.org [Accessed Jan 24 2024].

Juneidi S. J. (2020) Covid-19 tracing contacts apps: technical and privacy issues. *International Journal of Advances in Soft Computing and its Applications.* 12(3), 25-44.

Kabiri, P. & Ghorbani, A. A. (2005) Research on intrusion detection and response: a survey. *International Journal of Network Security.* 1(2), 84-102. doi: 10.6633/IJNS.200509.1(2).05.

Kshetri, N. (2017) Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommunications Policy.* 41(10), 1027-1038. doi: 10.1016/j.telpol.2017.09.003.

Majeed A. & Lee, S. (2021)Towards privacy paradigm shift due to the pandemic: a brief perspective. *Inventions.* 6(2), 24. doi: 10.3390/inventions6020024.

Pinno, O. J. A., Gregio, A. R. A. & De Bona, L. C. E. (2017) ControlChain: blockchain as a central enabler for access control authorizations in the IoT. In: *GLOBECOM 2017 - 2017 IEEE Global Communications Conference, 4-8 December 2017, Singapore.* IEEE. pp. 1-6.

Raman, R., Achuthan, K., Vinuesa, R. & Nedungadi, P. (2021) COVIDTAS COVID-19 tracing app scale-an evaluation framework. *Sustainability.* 13(5), 2912. doi: 10.3390/su13052912.

Rawindran, N., Jayal, A. & Prakash, E. (2021) Artificial intelligence and machine learning within the context of cyber security used in the UK SME Sector. In: *The 5th Advances in Management and Innovation Conference 2021, AMI 2021, 20-21 May 2021, Cardiff, UK.*

Longitudinal Study. *Brain, Behavior, and Immunity.* 94, 41-50. doi: 10.1016/j.bbi.2021.03.008.

Salman, T., Zolanvari, M., Erbad, A., Jain, R. & Samaka, M. (2019) Security services using blockchains: a state of the art survey. *IEEE Communications Surveys & Tutorials.* 21(1), 858-880. doi: 10.1109/COMST.2018.2863956.

Shahaab, A., Lidgey, B., Hewage, C. & Khan, I. (2019) Applicability and appropriateness of distributed ledgers consensus protocols in public and private sectors: a systematic review. *IEEE Access.* 7, 43622-43636. doi: 10.1109/ACCESS.2019.2904181.

Tran J, Ngoc C. (2020) *GDPR handbook for record of processing activities.* Case: the color club A/S.

Vanessa McGreevy (2020) ResponseSource.com [Accessed 9 Mar 2020].

Wylde, V., Prakash, E., Hewage, C. & Platts, I. (2021) Covid-19 Crisis: Is our Personal Data Likely to be Breached? In: *The 5th Advances in Management and Innovation Conference 2021, AMI 2021, 20-21 May 2021, Cardiff, UK.*

Zaeem, R. N. & Barber, S. K. (2020) The effect of the GDPR on privacy policies: recent progress and future promise. *ACM Transactions on Management Information Systems.* 12(1), 1-20. doi: 10.1145/3389685.

Zarpelão, B. B., Miani, R. S., Kawakani, C. T. & de Alvarenga, S. C. (2017) A survey of intrusion detection in Internet of Things. *Journal of Network and Computer Applications.* 84, 25-37. doi: 10.1016/j.jnca.2017.02.009.

Zhang, R., Xue, R. & Liu, L. (2019) Security and privacy on blockchain. *ACM Computing Surveys.* 52(3), 1-34. doi: 10.1145/3316481.

Zheng, Z., Xie, S., Dai, H., Chen, X & Wang, H. (2017) An overview of blockchain technology: architecture, consensus, and future trends. In: *2017 IEEE International Congress on Big Data (BigData Congress), 25-30 June 2017, Honolulu, USA.* IEEE. pp. 557-564.



This is an open access article distributed under the terms and conditions of the Creative Commons Attribution-NonCommercial 4.0 International License.