frontiers | Frontiers in Blockchain

TYPE Review
PUBLISHED 16 April 2024
DOI 10.3389/fbloc.2024.1359130

Integrated cybersecurity for metaverse systems operating with artificial intelligence, blockchains, and cloud computing

Petar Radanliev[1,2]*

[1]Department of Computer Sciences, University of Oxford, Oxford, United Kingdom, [2]School of Management, University of Bath, Bath, United Kingdom

Check for updates

OPEN ACCESS

EDITED BY
Xiaoqi Li,
Hainan University, China

REVIEWED BY
Qasem Abu Al-Haija,
Jordan University of Science and Technology, Jordan
Leijie Fu,
Xi'an Technological University, China

*CORRESPONDENCE
Petar Radanliev,
✉ petar.radanliev@cs.ox.ac.uk

RECEIVED 20 December 2023
ACCEPTED 02 April 2024
PUBLISHED 16 April 2024

CITATION
Radanliev P (2024), Integrated cybersecurity for metaverse systems operating with artificial intelligence, blockchains, and cloud computing.
Front. Blockchain 7:1359130.
doi: 10.3389/fbloc.2024.1359130

In the ever-evolving realm of cybersecurity, the increasing integration of Metaverse systems with cutting-edge technologies such as Artificial Intelligence (AI), Blockchain, and Cloud Computing presents a host of new opportunities alongside significant challenges. This article employs a methodological approach that combines an extensive literature review with focused case study analyses to examine the changing cybersecurity landscape within these intersecting domains. The emphasis is particularly on the Metaverse, exploring its current state of cybersecurity, potential future developments, and the influential roles of AI, blockchain, and cloud technologies. Our thorough investigation assesses a range of cybersecurity standards and frameworks to determine their effectiveness in managing the risks associated with these emerging technologies. Special focus is directed towards the rapidly evolving digital economy of the Metaverse, investigating how AI and blockchain can enhance its cybersecurity infrastructure whilst acknowledging the complexities introduced by cloud computing. The results highlight significant gaps in existing standards and a clear necessity for regulatory advancements, particularly concerning blockchain's capability for self-governance and the early-stage development of the Metaverse. The article underscores the need for proactive regulatory involvement, stressing the importance of cybersecurity experts and policymakers adapting and preparing for the swift advancement of these technologies. Ultimately, this study offers a comprehensive overview of the current scenario, foresees future challenges, and suggests strategic directions for integrated cybersecurity within Metaverse systems utilising AI, blockchain, and cloud computing.

KEYWORDS

artificial intelligence, cybersecurity, cyber assurance, cyber risk, cybersecurity standards, cybersecurity frameworks, cloud security, blockchain security

1 Introduction

Integrating cybersecurity with emergent technologies like Artificial Intelligence (AI), blockchain, cloud computing, and the Metaverse has become a critical study area. This article thoroughly examines the complex interplay between these modern technological domains, shedding light on the evolving landscape of cybersecurity.

The field of cybersecurity, traditionally focused on protecting data within relatively straightforward IT environments, is undergoing a transformative shift. The advent of AI has expanded the horizons of cybersecurity, introducing advanced techniques for threat detection, and enhancing system resilience. AI's capacity for predictive analysis and its adaptive learning algorithms have ushered in a new era where cybersecurity is proactive, capable of identifying potential threats in advance.

Blockchain technology, initially gaining prominence through its association with cryptocurrencies like Bitcoin, has emerged as a vital component in developing robust cybersecurity strategies. Its immutable and transparent characteristics are now being applied across various sectors, ranging from finance to supply chain management, playing a crucial role in safeguarding digital transactions and data.

Cloud computing, with its promise of scalability and efficiency, has reshaped organisational data storage and access methods. This shift, however, brings new cybersecurity challenges to the fore. The centralisation of data in cloud environments has made them attractive targets for cyber threats, necessitating the development of advanced security protocols and innovative risk management strategies.

The Metaverse, a nascent yet rapidly evolving digital Frontier, offers an immersive blend of virtual and augmented realities, heralding a new era of the internet experience. As this technology develops, it introduces many novel cybersecurity concerns, particularly regarding user privacy and data protection in a boundless digital realm.

This article investigates the intricate relationships between these leading-edge technologies and cybersecurity. We explore the current state and future possibilities of cybersecurity in the context of AI, blockchain, cloud computing, and the Metaverse, highlighting both the challenges and opportunities they present.

Employing a methodological approach that includes an extensive literature review complemented by case study analyses, this article aims to provide a comprehensive understanding of cybersecurity's current dynamics and future directions as it intersects with these technological innovations.

As we navigate this era of digital transformation, the article endeavours to contribute a thoughtful and informed perspective to the discussion on cybersecurity amidst the rise of AI, blockchain, cloud computing, and the Metaverse, offering insights beneficial to scholars, industry professionals, and policymakers.

Cybersecurity is just one branch of a larger information security area, and in this article, three separate categories of security are distinguished: 1) cyber security assurance, 2) cyber security risk, and 3) cyber security architecture. Within this structure, there are many emerging concepts and technologies that need to be considered, some of these concepts include Cloud security (Sehgal et al., 2020; Akinrolabu et al., 2019), IT network security (Sun et al., 2019; Henry and Haimes, 2009; Fujita et al., 2015), IoT security (Ahmad and Alsmadi, 2021; Russell and Van Duren, 2016; Roopak et al., 2019; Latvala et al., 2020; Abie and Balasingham, 2012; Crawford and Sherman, 2018; Brass et al., 2018; Altman Vilandrie and Company, 2017; Ayad et al., 2019; Payton, 2018; Jalali et al., 2019), Blockchain security (He et al., 2022; Deshmukh et al., 2022), Web3 security, the Metaverse (Sparkes, 2021; Kim, 2021; Lee et al., 2011; Duan et al., 2021; Park and Kim, 2022; Mozumder et al., 2022; Han et al., 2022; Wang et al., 2022; Mackenzie, 2022; Xi et al., 2022; Akour et al., 2022), along many other emerging areas that are open to cyber-attacks (Lallie et al., 2021).

With the emergence of new technologies, the cyber risk is changing; the threat players are not necessarily the same, the vulnerabilities change, and the risk of exposure needs to be constantly accessed. Some cybersecurity standards, frameworks, and methods are over a decade old. The original version of the NIST framework (Barrett et al., 2017; NIST, 2016; Moreira et al., 2021; NIST, 2023a) is over a decade old, and some of the ISO standards (ISO, 2022) are even older. While special publications and updates are constantly being integrated, with the emergence of such drastic new technologies, such as the Cloud, these frameworks often look like patched approaches, not designed for the current state of play in cyber risk. This article combines the topics of cybersecurity assurance, cyber risk, and cybersecurity architecture, and we expand into cloud security, blockchain security, and the Metaverse. The article also discusses the values and risks of these new technologies.

1.1 Diverse applications of blockchain technology in risk management

In the evolving landscape of digital technology, blockchain technology has significantly expanded its influence beyond its origins with Bitcoin, proving its utility in a wide array of fields, notably in risk management and other pivotal sectors. This discussion offers an insightful exploration of various blockchain applications, demonstrating their versatility and effectiveness in addressing complex challenges.

A prime example of blockchain's transformative role is observed in supply chain management, where it has become a fundamental tool for enhancing transparency and traceability. This is exemplified by the collaboration between IBM and Maersk, which employs blockchain to meticulously track the shipment of goods, ensuring a marked increase in security and efficiency by reducing fraud and augmenting compliance with regulatory standards.

In healthcare, blockchain has brought about transformative changes, especially in managing patient data. By establishing secure and immutable records, blockchain has notably improved data integrity and privacy. A notable application is secure electronic health records systems, which permit medical practitioners and patients alike to access crucial health information seamlessly while upholding the utmost standards of data security and patient privacy.

Moreover, blockchain's utility in the financial sector transcends cryptocurrencies. It has been instrumental in the implementation of smart contracts, which autonomously execute transactions upon the fulfilment of predefined conditions, considerably reducing risks related to non-compliance or fraud. Ripple's utilisation of blockchain to facilitate real-time, cross-border financial transactions exemplifies its potential to revolutionise traditional banking practices.

Blockchain also offers robust solutions in identity verification and management. Estonia's e-Residency program is a case in point, utilising blockchain to offer a secure digital identity for diverse online activities, ensuring a higher level of security and privacy for both business and personal uses.

In the realm of democratic processes, blockchain's application in securing voting systems is noteworthy. By creating transparent and tamper-proof voting mechanisms, blockchain technology paves the way for more reliable and democratic electoral processes, gaining attention as various entities explore blockchain-based voting solutions.

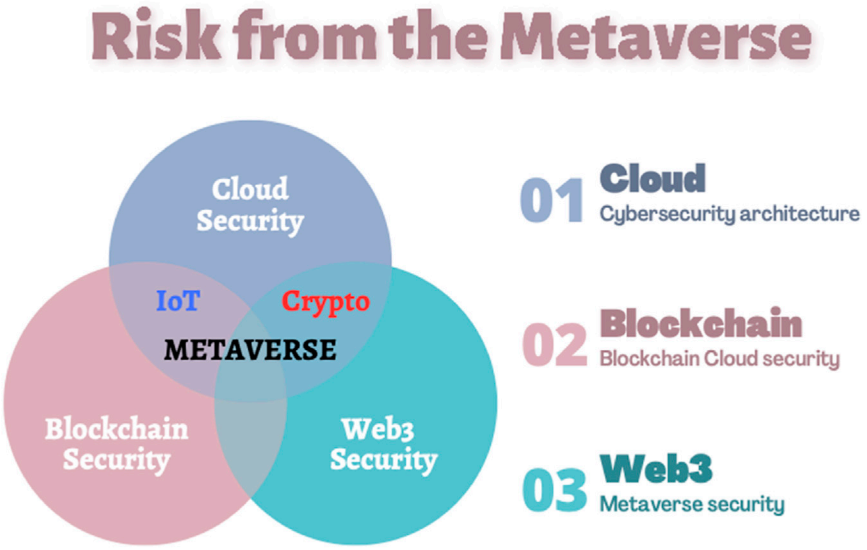

FIGURE 1
The evolving landscape of cybersecurity in the metaverse.

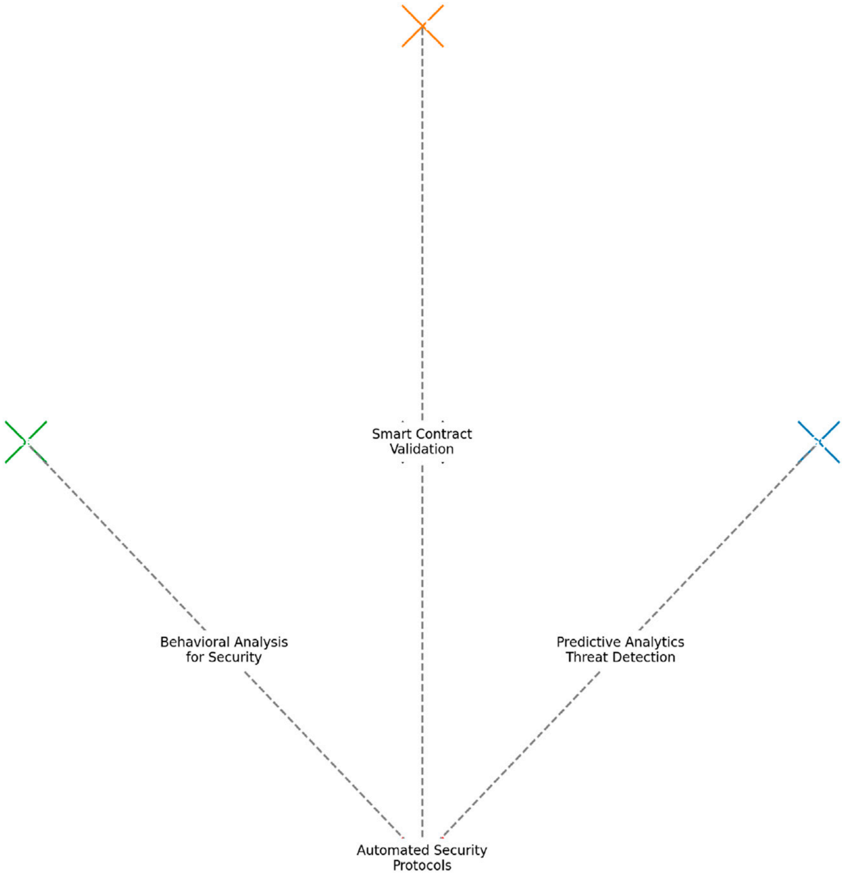
Smart Contract Validation
Behavioral Analysis for Security
Predictive Analytics Threat Detection
Automated Security Protocols

FIGURE 2
Conceptual diagram that visualises the proposed "Integrated Cybersecurity" structure in this article.

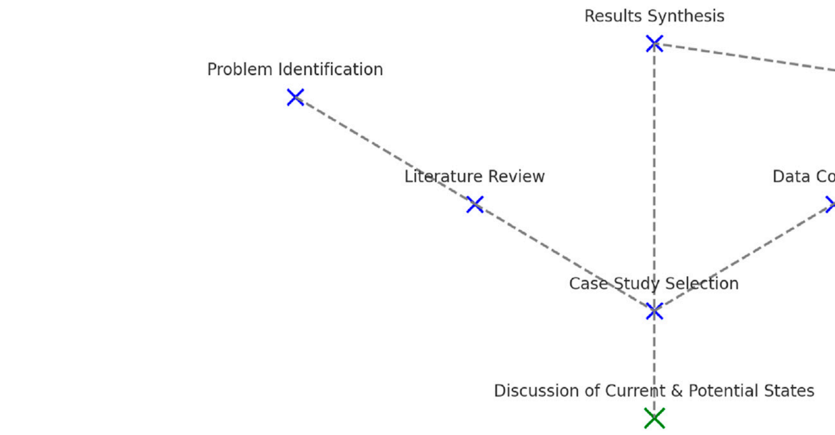

FIGURE 3
Methodological approach and discussion flowchart.

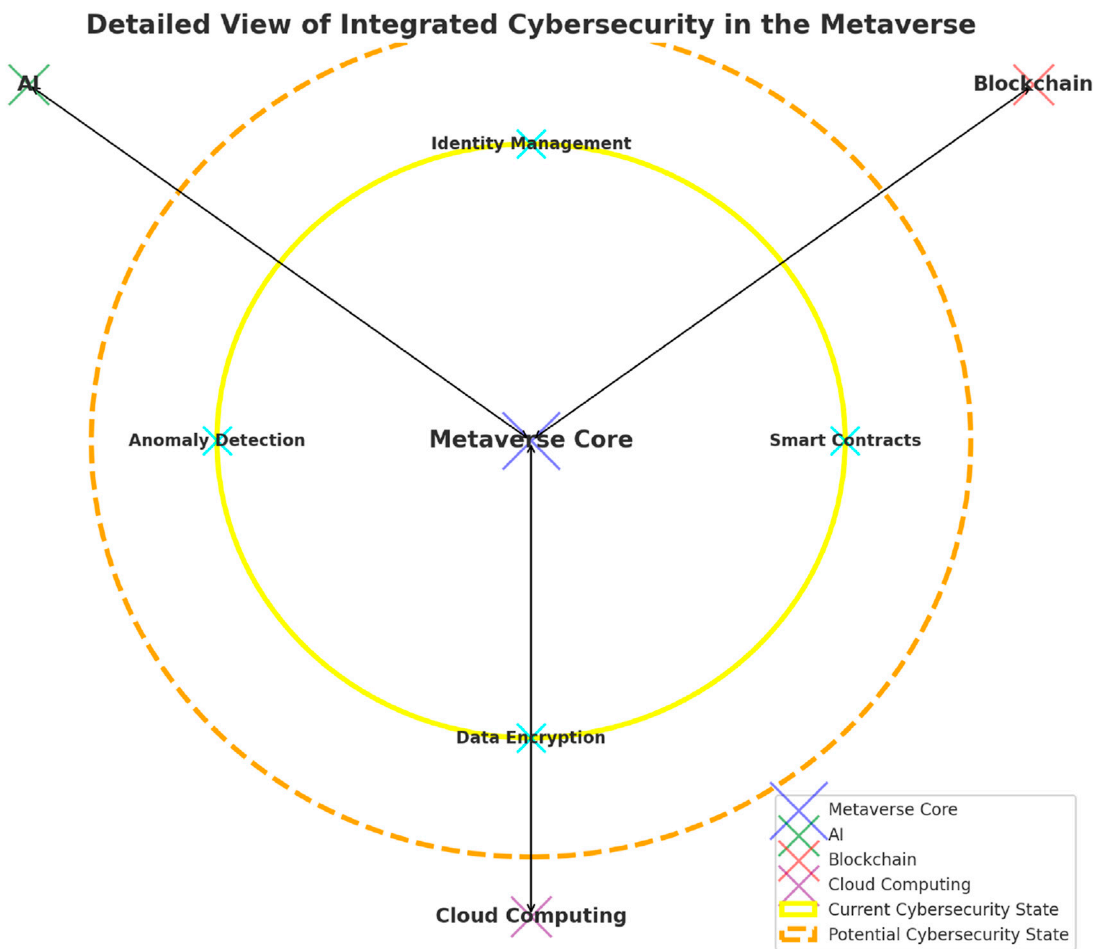

FIGURE 4
Detailed view of the new integrated cybersecurity in the Metaverse with AI, Blockchain, and Cloud Computing.

Furthermore, blockchain is instrumental in safeguarding intellectual property rights and managing royalties more transparently. Platforms like Ujo Music and Opus employ blockchain to ensure equitable compensation for artists and creators, providing a transparent and immutable record of ownership and earnings distribution.

In the real estate sector, blockchain has streamlined transactions, enhanced transparency, reduced fraud risks, and simplified property ownership verification. This technological advancement significantly transforms property title transfers and transaction recordings, making the real estate market more secure and accessible.

Blockchain's varied applications across diverse sectors underscore its role as a transformative force in the modern digital era. Its impact extends beyond financial transactions, emerging as an asset in risk management and numerous other fields. As blockchain technology continues to evolve, its potential applications are set to broaden, presenting innovative solutions to contemporary challenges.

2 The evolving landscape of cybersecurity in complex virtual systems

This section examines how new technologies and concepts like Cloud security, IT network security, IoT security, Blockchain security, and the Metaverse are reshaping the cyber risk landscape. Figures 1, 2 visualises the evolving landscape of cybersecurity in Cloud Systems, Blockchain Systems, and Web3.

In Figure 1, we can see a diagram showing new and emerging risks from complex virtual systems, and in Figure 2, we can see a diagram outlining the paper's structure. It focuses on "Integrated Cybersecurity" and its connection with four other domains: Cloud Systems, Blockchain Technology, The Metaverse, and Artificial Intelligence.

At the centre of the diagram in Figure 2, you will see "Integrated Cybersecurity" as the main focus. The four other domains are connected to this central theme, highlighting their individual and collective importance in the context of cybersecurity.

The segment on Artificial Intelligence has specific links to the other three domains. These links include short descriptions such as "Predictive Analytics for Threat Detection" in Cloud Systems, "Smart Contract Validation" in Blockchain Technology, and "Behavioral Analysis for Security" in The Metaverse. These descriptions show the roles AI plays in improving cybersecurity in each domain.

This diagram is a visual summary that provides an immediate understanding of the paper's main themes and the crucial role of AI in cybersecurity across different technologies.

2.1 Cybersecurity assurance

Cybersecurity assurance refers to an organisation's trust in its controls to safeguard its data. This process involves security hardening, security testing, and vulnerability management. Security hardening reduces the potential attack surfaces by deactivating unnecessary equipment and updating firewalls. Once the hardening is done, frequent security scans and penetration testing are conducted to identify any remaining vulnerabilities. Finally, vulnerability management addresses vulnerabilities that cannot be resolved promptly. The FAIR Institute's FAIR Method is an important advancement in this field. The Cyber Value at Risk (FAIR, 2017a; Buith, 2016) concept is used in this novel way to measure risk exposure. However, the lack of data strategies to support such methodologies is a barrier.

Cyber risk is a combination of threats, exploits, and vulnerabilities regarding cyber risk management. Adopting the Software Bill of Materials (SBOM) (CISA, 2022; Elias and Hewitt-Jones, 2023; CycloneDX, 2023; Dependency-Track, 2023; Eggers et al., 2022; NIST, 2023b; NTIA, 2023; Carmody et al., 2021) in the United States marks a watershed milestone in this field. Nonetheless, the sheer volume of possible vulnerabilities revealed by SBOMs highlights the critical need for risk management automation. It is important to note that not all vulnerabilities require mitigation. Strategic decisions are taken based on the severity of vulnerabilities, using frameworks such as ISO27001 and the NIST CSF as guides.

The cybersecurity architecture is the final step. This category includes the hardware, software, logical models, and assessment procedures that ensure a system's security. The current recommendations support multi-layered security architectures. The MITRE ATT&CK approach, endorsed by organisations such as the UK's National Cyber Security Centre, is the gold standard in this sector.

2.2 The promise of blockchain in cloud security

Blockchain technology has immense potential but is not a panacea for all security challenges. It is prudent to combine Blockchain's strengths with robust cybersecurity practices. Limitations such as scalability and interoperability, traditionally associated with Blockchain, are gradually being eclipsed as new and innovative Blockchains emerge. Interestingly, the solutions to Cloud security's many challenges may lie in the ongoing developments within Blockchain technology.

Contrary to traditional environments, relational databases in blockchain technologies do not simply scale via load balancers. The intricate balance between reading and writing loads demands a nuanced approach. This approach starts with determining server size, introducing "read replicas", utilising caching, and incorporating queuing systems. Determining server size involves aligning the database servers with the appropriate storage capacity and latency. Introducing the "read replicas" technique diverts the read load from the primary server, enhancing efficiency. Tools like Redis cache can further reduce the load directed at the "read replicas" for utilising caching. Queuing systems such as Kafka can be employed to manage the write load, ensuring seamless database operations. As the Metaverse digital economy navigates unprecedented technological shifts in the new Metaverse, cybersecurity must stay agile, adopting innovative strategies and tools to safeguard our increasingly interconnected world.

2.3 Summary of the paper structure

The study categorises security into three core areas: cybersecurity assurance, cyber risk management, and cybersecurity architecture, framing these within the context of evolving digital technologies.

Due to the complexity of integrating various technological risks into a coherent strategy, the article is structured differently from a traditional format. The structure is described in Figure 3, and is tailored to meet the task requirements, and this is best visualised in a flowchart. The flowchart begins with “Problem Identification” and advances through significant stages such as “Literature Review,” “Case Study Selection,” “Data Collection,” “Data Analysis,” and “Results Synthesis."

Each stage is represented by a blue dot connected by dashed grey lines, indicating the research’s sequential flow and logical progression. The final stage is “Discussion of Current & Potential States,” highlighted in green, signifying the culmination of the research process and its implications for cybersecurity in AI, Blockchain, and Cloud Computing within the Metaverse context.

The layout aims to provide a clear, step-by-step visualisation of the research methodology, leading to a comprehensive discussion of integrated cybersecurity systems’ current state and future potential.

2.4 Emerging solutions that are discussed in the review

In cybersecurity assurance, the paper emphasises organisational confidence in protective controls, highlighting the FAIR Method and Cyber Value at Risk concepts while noting the challenges in data strategy implementation. The cyber risk management section underscores the fluid nature of cyber threats and the critical role of the Software Bill of Materials, advocating for automation in risk management.

The discussion on cybersecurity architecture advocates for a layered defence approach, with the MITRE ATT&CK framework as a key example. This sets the stage for examining the impact of Blockchain in cloud security, where the paper recognises Blockchain’s potential while addressing its limitations, such as scalability.

The study also delves into Virtual Private Cloud (VPC) security, balancing the technical aspects of direct connections and VPNs with disaster recovery strategies. Special focus is given to securing critical infrastructure, particularly in healthcare.

The Metaverse is identified as a significant cybersecurity challenge due to its nascent nature, with concerns around misinformation, asset theft, and data privacy. The paper calls for comprehensive regulations that can address the complexities of this emerging digital realm.

The paper synthesises the intersecting domains of cybersecurity, Blockchain, Cloud, and the Metaverse, anticipating a shift towards more stringent regulations and frameworks. It sets a forward-looking agenda for research and regulatory action in the face of rapidly advancing digital technologies.

3 Differences between cybersecurity assurance, risk, and architecture

Cybersecurity assurance focuses on the trust organisations have in their protective controls, encompassing processes, policies, and standards that ensure data security and compliance with industry benchmarks. Cyber risk management, on the other hand, delves into the evaluation of potential threats, exploits, and vulnerabilities, aiming to discern and mitigate potential threats proactively. Meanwhile, cybersecurity architecture is concerned with the structural design of systems, combining hardware, software, and logical models to create secure environments, bolstered by multiple protective layers and defensive mechanisms to fend off cyber threats. Table 1 summarises the differences between cybersecurity assurance, risk, and architecture.

3.1 Cybersecurity assurance

The term cyber assurance refers to the level of confidence in the controls organisations have in place to control the security and privacy of their information and data security. This includes practices, processes, policies, strategies, standards, and other legally binding mechanisms that are in place to ensure organisations are compliant with the industry standards on cybersecurity. One of the key tasks in cyber assurance is the assurance review of standards-based compliance requirements, e.g., NIST (NIST, 2023c). Other areas of cyber assurance include security hardening, security testing, and vulnerability management.

1. Secure hardening refers to minimising the attack surface, usually by disabling unused systems and installing new versions of firewalls or intrusion detection mechanisms.
2. Security testing refers to identifying the remaining security vulnerabilities in the system after the security hardening stage. This includes regular automated security scans, establishing best practices, and manual security scans for new vulnerabilities (penetration testing).
3. Vulnerability management refers to managing vulnerabilities that remain in the system and cannot be patched at a given time (e.g., delay in patch update from the software developer or the vendor). Systems are not completely secure; this is just how the cyber world operates, but this stage aims to avoid open vulnerabilities that are exploitable, critical, and easy for hackers to use.

One of the emerging areas in cybersecurity assurance is the FAIR Method from the FAIR Institute (Factor Analysis of Information Risk) (FAIR, 2017b; Shu et al., 2021; FAIR North Carolina Chapter FAIR Institute, 2023FAIR, 2017c), which promotes the quantification of risk exposure. The FAIR Method uses the Cyber Value at Risk model and Monte Carlo simulations to determine the expected (forecasted) risk in monetary value (FAIR, 2017b). The problem with this approach is that many organisations simply do not have the data strategies to enable them to use this tool. Hence, the problem is not with the methodology design but with the lack of probabilistic data, and this can only be resolved by the organisations themselves or by new standards and regulations on data strategies.

3.2 Cyber risk management

The simplest definition of cyber risk is the sum of threats, exploits, and vulnerabilities, and cyber risk management is an ongoing process of identifying and patching the exploitable

TABLE 1 A summary table of the reviewed standards and emerging frameworks: Tabulated form outline of the standard and frameworks, and the differences between cybersecurity assurance, risk, and architecture.

Aspect	Cybersecurity assurance	Cyber risk management	Cybersecurity architecture
Definition	Trust organisations place in controls to protect their information	The amalgamation of threats, exploits, and vulnerabilities	Hardware, software, logical models, and evaluation mechanisms ensuring system security
Key Components	Security Hardening	Threat Identification	System Layers
	Security Testing	Exploit Detection	Defensive Mechanisms
	Vulnerability Management	Vulnerability Assessment	Evaluation Tools
Tools & Frameworks	FAIR Method (by FAIR Institute)	Software Bill of Materials (SBOM), ISO27001, NIST CSF	MITRE ATT&CK framework
Purpose	Ensure that controls and procedures are effective in protecting data	Assess potential threats and decide on mitigation strategies	Design and implement secure systems with multiple layers of protection
Challenges	Lack of data strategies supporting quantitative methods	Volume of potential vulnerabilities and need for automation	Maintaining robustness against evolving threat vectors

vulnerabilities. The most recent advancement in cyber risk management is the introduction of the Software Bill of Materials (SBOM) (NTIA, 2021), which is a legal requirement now in the United States because of the executive order that has been in effect since August 2022 (Biden, 2023) have been included in the SBOMs exceeds the capacity of cybersecurity teams to review and manage all potential vulnerabilities–considering that CVE contains almost 200,000 different vulnerabilities (MITRE, 2023). Most of the software contains over 100 components on average; this just gives a glimpse of what the problem is. This problem cannot be resolved manually, and we need automation. The more automation we include, the less human control exists in the system. Still, the SBOMs have exposed vulnerabilities in levels that cannot be reviewed by humans alone. This also builds upon the argument that not all vulnerabilities cause concern in most organisations. For example, traditional cyber risk management includes four potential solutions: 1) modification of the likelihood and impact; 2) risk retention; 3) risk avoidance–by not doing some IT activities; and 4) risk outsourcing–insurance. Hence, not all vulnerabilities are patched, and focus is usually placed on the most critical vulnerabilities. To determine which cyber risk (ISO, 2022; NIST, 2016) s are managed by one of the four strategies, cybersecurity practitioners refer to standards and frameworks–e.g., ISO27001 (ISO, 2022), NIST CSF (NIST, 2016), and FAIR Method (FAIR, 2017a).

3.3 Cybersecurity architecture

Cybersecurity architecture contains three parts: 1) hardware and software, 2) logical models keeping the system secure, and 3) evaluation models that quantify the security of the model. NIST recommends a layered approach to cybersecurity architecture and design because that would force adversaries to breach multiple control mechanisms to reach the system. The current state-of-the-art in cybersecurity architecture is the MITRE ATT&CK framework, which is often used to distrust attackers at different stages of the attack. The UK National Cyber Security Centre (NCSC) also recommends the MITRE framework and recommendations on designing systems that can apply security updates as soon as they become available to reduce exposure to vulnerabilities. The final recommendation to discuss in this section is the advice from NIST and NCSC to design systems that are secure by default and secure by design. This reduces the time and effort required to ensure systems are secure. The usual cybersecurity architecture contains five layers (Firewalls, Secure Configuration, User Access Control, Malware Protection, Patch Management). Still, there is a strong push towards more detailed cybersecurity architecture with at least seven layers. The seven layers of cybersecurity contain.

1. Mission-Critical Assets. What data is critical to protect? An example of mission-critical assets in the Healthcare industry is Electronic Medical Record (EMR) software. In the financial sector, its customer’s financial records.
2. Data Security. Security controls that protect the transfer and storage of data–encryption, archiving.
3. Endpoint Security–in the network, cloud, and device.
4. Application Security–security features that control access to an application and the application’s access to your assets.
5. Network Security–security controls; regular updates of security patches; encryption.
6. Perimeter Security–physical and digital security; firewalls.
7. The Human Layer–management controls, phishing simulations, and cyber training for non-technical staff.

In summary, cybersecurity architecture is the system design that protects data, information, and assets from unauthorised access, modification, and destruction. Key elements of cybersecurity architecture include data security, network security, endpoint security, and disaster recovery.

4 Cloud security

The Cloud is simply a virtualised network in a virtualised data centre. The Cloud network is vulnerable to the same types of cyber risk as other networks, including data breaches of Cloud environments that could lead to exposed private, personal, and/or sensitive data. One risk that is specific to Cloud environments is the multi-tenancy issue, where infrastructure and resources are shared with other users, introducing security risks. Insider threats are also an issue, regardless of the access to sensitive data breach being caused accidentally or intentionally. Cloud environments reduce visibility of data and controls applied, in other words, Cloud providers have greater control of the data and infrastructure than the data owner, making it difficult to monitor the security of data and information. Compliance is also a big concern because it is difficult to ensure compliance with data protection regulations, such as the GDPR or HIPAA. Once data and information are in the Cloud, this creates a new attack surface for hackers based in completely different parts of the world–e.g., the Lazaros Group is based in North Korea, but that has not stopped them from hacking Cloud environments in the EU and United States. Many of the Cloud exploits are triggered by incorrect configurations of cloud resources. Hence, Cloud security heavily depends on having experts in Cloud security who can detect and resolve Cloud configuration weaknesses that open vulnerabilities and exploits that can be utilised for cyber-attacks. The final concern with Cloud security is relying on a single provider. This will be one of the leading points of concern in Cloud security in 2024 because many organisations are struggling to understand the technicalities of Cloud environments and tend to rely on one Cloud provider for all critical data and applications, which creates a single point of failure and significantly increases the cyber risk in Cloud environments. The key areas of interest in Cloud security in 2024 will be data storage and information transfer, bringing Cloud security closer to cryptography and, almost undeniably, to Blockchain security.

4.1 New forms of cloud storage

There are three types of Cloud storage, those are.

1. Block storage acts like a virtual hard drive, where data is broken into blocks. It decouples the storage and the computing environment. Block data can be stored anywhere in our environment, and it would feel local, like a local hard drive. Block storage is used when we need a hard drive that will remain across all clouds even after a reboot or instant termination.
2. Object storage is when data is broken into 'objects', and each 'object' contains metadata (or data about the data) and cannot be mounted as a regular drive to be used by a computer. Object storage is designed for data written once and read many times, e.g., in software and distributing photos and videos. When we write to the data, object storage automatically creates a modified version. Hence, it is unsuitable for files we modify frequently because it would create many versions of the same data and fill up the Cloud storage. Object storage is frequently used for software distribution, archival purposes, and big data environments–because we can search for part of the data based on the metadata.
3. File storage is used when multiple offices need to access the same file. The file storage can be local to the system or network file storage (NFS). If we use Windows, we need to use the server message blog protocol.

4.2 Blockchain cloud security

Blockchain technology has the potential to improve Cloud security. Although this technology is still considered in the beta testing stage, the technology has been in existence since 2008, when the first paper on decentralised blockchains 54 was published by a mysterious person or entity called Satoshi Nakamoto. Although Blockchain technology is not used extensively in Cloud security, several potential solutions can be used to enhance Cloud security. Some include.

1. Cryptography is the most obvious solution and the first solution we need to consider enhancing cloud security. Blockchain technology is a database that uses cryptography to secure the validity of stored data records and data in transit. Blockchain technology uses cryptographic techniques to secure transactions, ensure the confidentiality and integrity of data, and secure data and information already stored in the cloud.
2. Decentralisation is another key solution that can be applied in Cloud security. There are already existing decentralised Clouds that will eventually be developed to a level that they could compete with the existing Cloud environments. For example, the decentralised Cloud project called NuNet has the potential to compete with the big Cloud players, and it is based on using the spare storage capacity of millions of users that have too much unused capacity on their personal devices. It is unlikely that this specific project will be the breakthrough in decentralised Cloud environments because the project has not really presented many working solutions that can be used in practice, but the idea is there, and Cloud providers need to start thinking about how the Blockchain technology can help in security their Cloud environments. One key element of decentralisation is that there is no central authority, and cyber risk is reduced in blockchains by eliminating the single point of failure risk, which leads to increased security in that specific Cloud environment.
3. Blockchain-based authentication systems can be used in Cloud environments to improve authentication security by providing a variety of alternative authentication methods, including multi-sign functions, smart contracts, and many other security authentication options available in Blockchain security.
4. Finally, we need to mention that the Blockchain's distributed ledger technology is also an immutable ledger that enables a tamper-proof transaction record that can prevent data breaches by preserving the record's originality, which is also available in open access. Hence, not only is blockchain technology secure, but it is also open access, and yet, nobody has been able to hack the Blockchain. There have been numerous cyber-attacks on crypto bridges, cryptocurrency liquidity pools, and digital wallets, but the blockchain itself has not been hacked yet, not even the less secure Blockchains.

In this section, Blockchain technology is not going to resolve all the problems with Cloud security, and organisations still need to ensure they have strong cybersecurity practices in place, including a level-based cybersecurity architecture, to prevent attackers from entering the system if one vulnerability goes unnoticed. There are also inherent limitations to using Blockchain technology in Cloud security, with the most noticeable being the scalability and interoperability problems. However, these are slowly becoming problems of the past because Blockchains - such as AVAX, SOL, MATIC, NEAR, DOT, etc.–are becoming more scalable than existing communication infrastructure. In addition, new Blockchain projects–such as LINK, ATOM, etc.–are focused on interoperability and are designed for cross-chain operations. These changes can shift the value of Blockchain solutions closer to the requirements of Cloud environments. To transfer the focus from Blockchain solutions to Cloud security, we do not have perfect solutions for Cloud relational databases in any case, and the solutions are being developed in Blockchain technologies simultaneously with the new solutions developed in Cloud environments.

4.3 How to scale a relational database

Relational databases cannot be scaled like traditional environments, with a load balancer to front-end multiple servers. The read and write loads need to be considered in a relational database. The first step is to find the correct size for the database servers and then match that with the correct storage and latency. The next step is to add a "**read replica"**, to take the read load from the primary server by pointing to the "read replica", and we can take load from the 'read replicas' by caching, e.g., redis cache. This would reduce the requests for 'read replicas', further offloading the database. A queuing system (e.g., Kafka) can **offload the write-load**. Kafka enables writing to the queue to detect when the server is ready and drain the queue to the database. Hence, in 2024, we typically reduce the write load with a queuing function; we reduce the read load with read replicas and caching. It is also possible to partition the database, but most database architects use a combination of read replicas, caching, and queuing to scale the databases.

4.4 Architectural problems with proprietary databases in a multi-cloud environment

Proprietary databases (e.g., Amazon DynamoDB, Azure Cosmos DB) are not something you want to use because they promote vendor lock-in, and you need to re-code your applications to work on a different vendor, and it is hard to synchronise vendor proprietary things. Most Cloud architectures in 2024 do not use anything proprietary. Instead, open standards are used. For example, Amazon DynamoDB is replaced by MongoDB or Apache Cassandra, which you can run on virtual machines and enable identical environments in the datacentre and multiple Clouds. When hybrid-cloud or multi-cloud are used, proprietary services are avoided because they lock you with the specific Cloud provider. Some risks with proprietary applications are that the cloud provider could raise rates, and getting out of that service and moving to a different cloud provider is difficult. But if you use open standards, you will not have these problems.

5 How to secure a virtual private cloud (VPC)

5.1 When to use a direct connection and when to use a virtual private network (VPN)

With direct connection (e.g., wire), latency is consistent, and you are guaranteed to have the performance of the wire. If your organisation requires guaranteed consistent latency, and guaranteed consistent bandwidth, they need to use a direct connection. VPN is used to create easy connection to multiple sites cheaper than with other options. If all users have Internet access, VPN can create connection on demand, making it easy to connect to multiple remote locations. The issue is that VPN requires Internet bandwidth. VPN is very useful when you need to connect multiple campuses (e.g., 10 campuses) to the Cloud. VPN would enable connections between the Cloud and each remote site. Another option is to set up VPC peering, and each campus can peer with each other. This would present a fully mesh peers where everyone can connect to everyone. The advantage of the fully meshed set up is that if something happens to the central location, the 10 campuses will continue to communicate. The main disadvantage is that the number of peers adds up dramatically (the formula is: N x N-1/2).

5.2 The function of IPSec

IPSec (Internet Protocol Security) performs encryption and provides the ability to authenticate remote end-to-end to prevent a man-in-the-middle attack and ensures the integrity of the data by using a hashing algorithm. IPSec provides the ability to authenticate, determine the message integrity, verify that messages are sent, and provide a non-repudiation environment, in addition to the encryption and the ability to tunnel private IP addresses and private traffic and private routing information over a public network.

IPsec is used to secure network communications by encrypting data. IPsec is applied to secure data transmission between a customer network and the cloud or between cloud environments. The benefits of using IPsec in the cloud include.

1. Encryption: end-to-end encryption of data in transit.
2. Authentication: authentication mechanisms that verify the identity of devices communicating over the network.
3. Integration: can be integrated with firewalls and intrusion detection systems.
4. Compatibility: widely supported and compatible with many networks and devices.

Those are the benefits, but IPsec is complex and needs to be deployed to balance security and performance, because this security solution is not suitable of fully comprehensive for all types of cloud environments.

5.3 Using the cloud for disaster recovery

There are **four options** for using the Cloud for disaster recovery.

Option one is a complete **cold stand-by**, with machine images of the working servers, and data is sent periodically to keep the recovery up to date. The advantage of this option is the low cost, but the disadvantage is that it would take a long time to return to full service in case of a primary failure.

Option two is to keep machine images of the web layer and the application layer, but you also keep a stand-by database that is active and receiving information to be synchronised. This option is still slow, but it is much faster than option one, because the data is always up to date.

Option three is to replicate your working environment but use very small instances in the disaster recovery site and place them in an auto scaling group. This approach might require 10–30 min for the system to auto scale, so it is not the fastest.

Option four is to run a complete hot standby, where the entire working environment is saved in a second location, and the only time it would take is for the DNS to detect that one site is down and re-route the traffic to the other site.

5.4 How to protect critical emergency infrastructure

Emergency infrastructure such as hospitals and ambulances require the most robust environment with a) high availability and b) high security. Since most patients data is digitised, if hospitals cannot access those records, someone will die.

This requires either a hybrid cloud environment, or multi cloud environment, because single cloud can be a single point of failure. Single cloud provider can be down because of 1) a controlled and planned event, 2) a major network event, or 3) a hacking event. Emergency infrastructure requires at least two Cloud providers, and two data centres, and that can only be managed with **vender neutral interoperable services**.

Typical security of emergency infrastructure starts with content delivery network (CDN) for web applications. CDN can eliminate a lot of fake requests from distributed denial of service (DDoS) attacks - and only forward legitimate requests to the web server. Behind CDN, there is usually a strong enterprise grade next-generation firewall. This will not be a Cloud native firewall, because Cloud native firewalls lack interoperability between different Cloud providers. A virtual firewall is usually obtained from the marketplace, e.g., Cisco. Next-generation virtual firewalls have intrusion detection system (IDS) and intrusion protection system (IPS), but emergency infrastructure requires a separate network load balancer, with separate IDS and IPS systems. Behind that, the usual set up includes access control list to keep unwanted traffic out of the subnets. On the Cloud, there is also a security group that acts as a host-based firewall preventing traffic from getting into the servers. Servers are locked with another host-based firewall, with antimalware protection. Unnecessary services are disabled to close ports, and pathing is applied on routine basis to ensure systems are locked down. The next step in the Cloud security is a strong 'Identity and Access Management' (IAM) protocol, to identify who is coming on, what they do and when they leave. Most used protocol is the Microsoft active directory. Additionally, all data in transit and in storage is encrypted, and Machine Learning is used for analysing the VPC flow logs and the security logs, in combination with a data visualisation tool to visualise the log events. This is the typical set-up in 2024 for high availability and high-security Cloud architecture, running the same architecture on two clouds and the data centre on multiple clouds.

5.5 Metaverse security

The Metaverse is often confused with the new renaming of the Facebook platform into Meta, but the reality is that the idea of a Metaverse society is much older than that. The Metaverse has existed for decades without any increase in users to a level that would be considered mass adoption. The term "Metaverse" originated in the 1992 science fiction novel **Snow Crash** (Stephenson, 2003), by the American writer Neal Stephenson. Stephenson used the term to describe a virtual reality-based successor to the internet.

Building upon this idea, the virtual world platform Second Life is often described as the first Metaverse, which went live in 2003, roughly the same time as Facebook or even 1 year earlier. The second version of a working Metaverse is described in the dystopian science fiction called Ready Player One–which presents a VR landscape called "The OASIS". The first novel was released in 2011, with a 2018 film adaptation, and the second novel in 2020. The franchise is based in 2045 when society is gripped by crisis. The Metaverse is presented as the primary escape for people via 'the OASIS' which is accessed with a VR headset and wired gloves.

The truth is that software is based on decentralised technologies, and the future version of the internet is likely to be far more immersive than the current Web2 version. Since the emergence of Web1, which was also known as the information highway, society has engaged in a path of technological development, that would result in the current problems in personal and private data security and privacy. It is difficult to see how the next version of the Internet will develop without the security and privacy features that are present in Blockchain technologies. However, many issues remain in terms of the cybersecurity of the Metaverse. Some examples include.

1. Misinformation is one of the key problems with the Metaverse because, with all the privacy-preserving features, it means that one individual can create multiple identities and start information warfare with the use of AI bots. This could result in false and potentially dangerous narratives, causing mistrust and anger.
2. Asset theft is a serious concern, with the rise of cryptocurrencies and digital assets such as Non-fungible tokens (NFTs), we cannot buy virtual goods and even virtual real estate, but these can be stolen by hackers and resold at speed, without any mechanisms to prevent or reverse the transaction.
3. Data privacy in the Metaverse is also a big area of concern because users and creators can build, purchase, or create a digital representation, share personal information, and even develop a brand or image representation in the Metaverse. If this is stolen, users would be subjected to ransomware, or the attacker could simply damage their reputation, making the asset less valuable.

4. Malware is the last issue to discuss, although not the last issue of the Metaverse. Various Metaverse environments can be used for distributing malware and exposing users to security threats. Decentralisation in Blockchain technology refers to preserving the privacy of a centralised entity that would impose controls that are undesired by the community, but centralisation also enables establishing security mechanisms and adapting these mechanisms to new standards. These options will not be operational in a decentralised version of the Internet, hence, the much greater focus would need to be placed on mitigation strategies, such as insurance of digital assets

The most recent standards and frameworks on data and privacy security in the Metaverse are somewhat blurred and almost non-existent. One would think that EU citizens are protected by the EU General Data Protection Regulation (GDPR), but in the Metaverse, a EU or a US, or a UK citizen can enter a virtual environment–e.g., a nightclub, that is developed and hosted by an individual that is based in Japan or China, and the same individual can be a citizen of Canada or India. Privacy of the data collected in the Metaverse is still a topic that needs to be resolved with privacy laws that can be applied across international borders. Since the original design of the decentralised blockchain was aimed at developing a system that cannot be controlled by governments or individual entities, such systems are hard to control and regulate. The EU has developed new regulations called MiCA (MiCA, 2022)which are under development. Still, the UK has not changed regarding regulating Blockchain technologies, cryptocurrencies, and the Metaverse.

6 Discussion

The discussion on integrated cybersecurity for Metaverse systems operating with artificial intelligence, blockchains, and cloud computing begins with a diagram of the study's findings. The diagram provides a more detailed view of integrated cybersecurity in the Metaverse with AI, blockchain, and cloud computing technologies.

As seen in Figure 4, the Metaverse Core is at the centre in blue, labelled "Metaverse Core." The surrounding nodes for AI (green), blockchain (red), and cloud computing (purple) are larger, with bold labels. Bidirectional arrows indicate more dynamic interactions between the Metaverse and each technology. Current (yellow) and potential (orange, dashed) cybersecurity states are shown with thicker circles. Added cyan dots represent specific cybersecurity features: Identity Management, Data Encryption, Anomaly Detection, and Smart Contracts, placed strategically around the Metaverse core. The diagram has an informative legend and titles, enhancing clarity and detail.

To discuss individual sections of the new integrated approach, the discussion expands into the original concepts of cybersecurity assurance, cyber risk management, and cybersecurity architecture.

Cybersecurity assurance is still defined as a process that helps ensure that information systems and assets are secure, protected and resilient to unauthorised access, theft, or damage. Some of the cybersecurity assurance standards include.

- ISO/IEC 27035: Information security incident management
- ISO/IEC 27005: Information security risk management
- ISO/IEC 27037: Information technology - Security techniques - Guidelines for information and communications technology readiness for business continuity
- ISO/IEC 27031: Information technology - Security techniques - Information security for business continuity
- NIST Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity
- CIS Controls: A prioritised set of actions for cyber defence
- Centre for Internet Security (CIS) 20 Critical Security Controls
- The FAIR (Factor Analysis of Information Risk) Institute's Open Risk Management Framework
- SANS Institute's 20 Critical Security Controls for Effective Cyber Defence.

What needs to be emphasised is that the cybersecurity assurance standards are somewhat different than the cyber risk management standards below.

Although there are some developments in **cyber risk management**, the process remains somewhat unchanged from 2023. We still define the process of cyber risk management as the identification, assessment, and prioritisation of risks to information technology systems. The objective of cyber risk management is to reduce the likelihood of a cyber-attack, not to prevent the risk of the event from occurring completely because that could be too costly and not likely to be effective. There are four categories of cyber risk management.

1. Threat assessment refers to identifying potential threats (attacks) from internal and external players.
2. Risk analysis–refers to evaluating the impact and likelihood, then prioritising the risk based on the threats they expose.
3. Mitigation and remediation–refer to implementing countermeasures that reduce the impact; some examples include firewalls, software updates, training for internal employees, etc.
4. Monitoring and review–refers to the continuous checks of the measures' effectiveness, including the entire cyber risk management process.

Some of the standards for cyber risk management include.

- ISO/IEC 27001
- NIST Cybersecurity Framework
- PCI DSS (Payment Card Industry Data Security Standard)
- HIPAA (Health Insurance Portability and Accountability Act)
- SOC 2 (Service Organisation Control)
- CSA STAR (Cloud Security Alliance Security, Trust & Assurance Registry)
- FISMA (Federal Information Security Modernisation Act)
- GDPR (General Data Protection Regulation)
- NYDFS Cybersecurity Regulation
- IEC 62443 (Industrial Control Systems Cybersecurity).

The best cyber risk standard depends on the industry, on the organisation, and on the cyber risk environment. In general, ISO/IEC 27001 is considered as a strong standard for information security management, but in the United States, there is a strong preference for the NIST approach. ENISA has been making attempts to develop a EU based cyber risk standard (ENISA, 2020), and some documents are already available online, but the general feeling is that ENISA is still piggybacking on NIST.

In terms of **cybersecurity architecture**, there are 6 main advancements that we can anticipate in year 2024. Those are.

1. Artificial intelligence and machine learning (AI/ML) is increasingly been adopted and used for threat detection, intrusion prevention and cyber defence in general. AI and ML algorithms can analyse big data to identify patterns and anomalies that indicate a breach, then learn from previous attacks to improve accuracy of the defence mechanisms.
2. Cloud security is on the rise, and given that most organisations would have moved their operations in the cloud by 2025, we can expect most of the security architecture to evolve in the cloud. There has been some serious efforts in developing secure data management in the cloud, and secure cloud environments. Challenges will remain in terms of data privacy, compliance with data regulations, and doubts on the level of protection will remain present in 2024. However, the use of cloud security will increase, and advancements will be in the areas of encryption, multi-factor authentication, and security orchestration of cloud environments.
3. Cryptography will become quantum resistant, and we already have some examples of this (e.g., Algorand), because with the increased developments in quantum computing, we need systems that can resist quantum based cyber attacks. Since quantum computers can crack the existing encryption algorithms, we can expect new cryptography methods to emerge, with expected advancements in the use of post-quantum algorithms - such as: lattice based cryptography, code based cryptography, and hash based cryptography.
4. Zero-trust security is also becoming a prominent aspect of cybersecurity architecture. We need a new security that considers all devices untrusted until proven otherwise. Zero-trust security applies micro-segmentation, multi-factor authentication, and continuous monitoring to ensure the security of networks and data.
5. Internet of Things (IoT) security is also becoming more concerning; with the continuous rise of IoT devices, there is an urgent need to secure such devices and the data collected and transmitted to the cloud. The most recent IoT security includes encryption, secure boot processes, and secure software updates to prevent cyber-attacks.
6. Blockchain security is increasingly used to improve identity management, data privacy, and supply chain management. We can anticipate a big increase in the application of blockchain technologies in cybersecurity architecture, such as banking, finance, healthcare, and government. Blockchain technology enables a secure and transparent way to store and transfer data, and blockchain security includes using smart contracts, secure multi-party computation, and zero-knowledge proofs to ensure the privacy and security of data. We can expect these features to predominate the cybersecurity architecture in 2024.

One potential solution to all these concerns is for one individual country, e.g., the UK, to decide on adopting new Blockchain technologies and developing a new parallel system to the existing national infrastructure. This would enable the UK to be a leader in adoption of a technology that has resulted with a significant profit for individuals that created some of the original crypto projects. It would also enable the UK to be a leading country in testing and developing the Metaverse concept. With the recent collapse of FTX and Alameda research, and the Terra Luna project, we can expect a strong interest in the crypto community from a regulated stablecoin, and a regulated interoperable Blockchain, with digital wallet that is approved and secured by the UK government, in the same way as bank accounts are secured up to a value of £80,000 and investments are secured if stored in a valid organisation. This obviously would come at some risks, but these risks are not different than risks in stock market price fluctuations. If the UK government is responsible for security of the investment, this only covers the event of a bank running out with the money, or bankrupting. The fluctuation of asset prices is not protected with stock market investments, and nobody would expect the UK government to guarantee the price of a crypto asset. The development of a national blockchain, with a national US dollar denominated stablecoin, and a digital wallet, or even a decentralised exchange, would not be a very difficult task. If there are doubts about this, we just need to remember the case of Uniswap and SushiSwap, the two main decentralised crypto exchanges. SushiSwap was simply a copied and pasted code from the Uniswap, and the developed did not even change the name Uniswap, and it worked quite well. SushiSwap is now a major and well-established crypto exchange. It is considered as a stable and secure exchange, much safer than FTX or some of the other centralised exchanges that have bankrupted in the previous year. What prevents governments like the UK from developing national Blockchains? That is difficult to answer, but considering the Ethereum chain has reported collection of $50bn in gas fees in a single month, we can easily see the rationale for a UK national blockchain.

7 Conclusion

As we approach the close of 2024, our exploration into the dynamic interplay of Artificial Intelligence with cybersecurity, particularly in cloud computing, blockchain, and the Metaverse, reveals a landscape teeming with challenges and innovations. Through its methodical investigation, this article has endeavoured to untangle and elucidate this complex web, contributing significantly to our understanding and management of cyber risks in these rapidly evolving domains.

In cybersecurity, AI's transformative impact cannot be overstated. It has not merely enhanced existing protocols but redefined the fabric of security mechanisms. The advent of AI-driven predictive models marks a shift from reactive to proactive cybersecurity strategies, where threats are anticipated and mitigated before they materialise. Such advancements are particularly pertinent as we witness an increasing trend of organisations transitioning to cloud-based operations. AI's role in cloud security extends beyond conventional practices, offering sophisticated solutions to counteract the vulnerabilities intrinsic to single-cloud dependencies and making these systems more resilient against potential cyber threats.

Turning our attention to blockchain technology, we observe a harmonious integration of AI. Here, AI emerges as a shield against contemporary cyber threats and as a visionary force preparing blockchain systems for the future challenges posed by quantum computing. The development of quantum-resistant blockchain technologies, underpinned by AI, is a testament to the foresight and innovation at the heart of this research.

The Metaverse, with its nascent yet burgeoning digital economy, presents a Frontier rife with regulatory and privacy challenges. AI's role within this domain is crucial, forging pathways for ensuring user privacy and data security across a transnational digital landscape. The innovative solutions offered by AI in the Metaverse are indispensable for nurturing safe and secure digital ecosystems.

This article comprehensively explains the nuanced relationships between AI and various cybersecurity domains. It proposes a multi-faceted approach to cybersecurity, where AI acts not only as a tool for enhanced security measures but also as a proactive agent in anticipating and countering emerging cyber risks. As we navigate this digital era, the insights and strategies delineated herein are poised to be pivotal in shaping a secure and resilient cyber future. In doing so, this work not only elevates the discourse within academic circles but also offers practical implications for practitioners and policymakers in cybersecurity.

In 2024, we will likely see a stronger shift toward regulations and standards in many areas of the cyber world that have somehow gotten away in the previous years. With the rise of cloud use, we expect all organisations to shift their IT operations to the cloud by 2025, and this opens a completely new attack surface for hackers. Data privacy regulations will likely increase in terms of Cloud security. However, the most concerning cybersecurity risk from cloud environments remains using a single cloud provider, which seems to be the preferred option for many organisations, even though it creates a single point of failure in their operating systems.

In Blockchain security, we are likely to continue witnessing cyber-attacks on digital wallets, liquidity pools, bridges, crypto exchanges, and many other areas of the cryptocurrency ecosystem. The Blockchain itself remains secure and has not been hacked until the present. Quantum computers are expected to present many cybersecurity challenges for Blockchain technologies, but we already have working solutions for some of these problems. We have existing Blockchains that are already resistant to cyber hacks from quantum computing, and we are likely to see a continuation of this trend in enhanced security. Most Blockchains will resist quantum computing cyber-attacks before we even have working quantum computers that can be used for cyber-attacks. Hence, this area is unlikely to be a cause of major concern in the cybersecurity world.

The Metaverse, on the other hand, remains very challenging to regulate, and cybersecurity is a major concern. Data privacy and security is a major challenge because of cross-border developments. We need new laws and regulations that can be applied across borders, and the current standards and regulations are unlikely to ensure the privacy and security of data in storage and data in transit. Hence, the privacy and security of users and participants remain a concern. With the increased use of Blockchain technologies, the crypto community will likely find solutions for all these concerns, but it will be at the cost of many breaches and security hacks.

Author contributions

PR: Conceptualization, Data curation, Formal Analysis, Funding acquisition, Investigation, Methodology, Project administration, Resources, Software, Supervision, Validation, Visualization, Writing–original draft, Writing–review and editing.

Funding

The author(s) declare that financial support was received for the research, authorship, and/or publication of this article. This work has been supported by the UK EPSRC under grant number EP/S035362/1 and ESRC under grant number ES/V003666/1.

Conflict of interest

The author declares that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

Abie, H., and Balasingham, I. (2012). "Risk-based adaptive security for smart IoT in eHealth," in SeTTIT 2012, Oslo, Norway, September 2012.

Ahmad, R., and Alsmadi, I. (2021). Machine learning approaches to IoT security: a systematic literature review. *Internet Things* 14, 100365. doi:10.1016/j.iot.2021.100365

Akinrolabu, O., Nurse, J. R. C., Martin, A., and New, S. (2019). Cyber risk assessment in cloud provider environments: current models and future needs. *Comput. Secur.* 87, 101600. doi:10.1016/j.cose.2019.101600

Akour, I. A., Al-Maroof, R. S., Alfaisal, R., and Salloum, S. A. (2022). A conceptual framework for determining metaverse adoption in higher institutions of gulf area: an empirical study using hybrid SEM-ANN approach. *Comput. Educ. Artif. Intell.* 3, 100052. doi:10.1016/J.CAEAI.2022.100052

Altman Vilandrie and Company (2017). Are your company's IoT devices secure? Available at: http://www.altvil.com/wp-content/uploads/2017/09/AVCo-IoT-Security-White-Paper-June-2017-vF.pdf (Accessed November 25, 2017).

Ayad, A., Zamani, A., Schmeink, A., and Dartmann, G. (2019). "Design and implementation of a hybrid anomaly detection system for IoT," in 2019 6th International Conference on Internet of Things: Systems, Management and Security, IOTSMS 2019, Granada, Spain, October, 2019, 87–92. doi:10.1109/IOTSMS48152.2019.8939206

Barrett, M., Marron, J., Yan Pillitteri, V., Boyens, J., Witte, G., and Feldman, L. (2017). Draft NISTIR 8170, the cybersecurity framework: implementation guidance for federal agencies. Available at: https://csrc.nist.gov/CSRC/media/Publications/nistir/8170/draft/documents/nistir8170-draft.pdf (Accessed: March 09, 2018).

Biden, J. 2023 Executive order on improving the nation's cybersecurity | the white house. Available at: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/(Accessed: January 02, 2023).

Brass, I., Tanczer, L., Carr, M., Elsden, M., and Blackstock, J. (2018). "Standardising a moving target: the development and evolution of IoT security standards," in Living in the Internet of Things: Cybersecurity of the IoT - 2018, London, March, 2018. doi:10.1049/cp.2018.0024

Buith, J. (2016). Cyber value at risk in The Netherlands. Available at: https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/financial-services/deloitte-nl-fsi-cyber-value-at-risk.pdf (Accessed April 04, 2017).

Carmody, S., Coravos, A., Fahs, G., Hatch, A., Medina, J., Woods, B., et al. (2021). Building resilient medical technology supply chains with a software bill of materials. *npj Digit. Med.* 4 (1), 34–36. doi:10.1038/s41746-021-00403-w

CISA 2022 Software bill of materials. Available at: https://www.cisa.gov/sbom (Accessed December 24, 2022).

Crawford, D., and Sherman, J. (2018). Gaps in United States federal government IoT security and privacy policies. *J. Cyber Policy* 3 (2), 187–200. doi:10.1080/23738871.2018.1514061

CycloneDX 2023 OWASP CycloneDX software bill of materials (SBOM) standard', full-stack bill of materials (BOM) standard. Available at: https://cyclonedx.org/ (Accessed April 19, 2023).

Dependency-Track 2023 Software bill of materials (SBOM) analysis | OWASP. Available at: https://dependencytrack.org/(Accessed: January 03, 2023).

Deshmukh, A., Sreenath, N., Tyagi, A. K., and Abhichandan, U. V. E. (2022). "Blockchain enabled cyber security: a comprehensive survey," in 2022 International Conference on Computer Communication and Informatics, ICCCI, Coimbatore, India, January, 2022. doi:10.1109/ICCCI54379.2022.9740843

Duan, H., Li, J., Fan, S., Lin, Z., Wu, X., and Cai, W. (2021). "Metaverse for social good: a university campus prototype," in MM 2021 - Proceedings of the 29th ACM International Conference on Multimedia, Virtual Event, China, October, 2021, 153–161. doi:10.1145/3474085.3479238

Eggers, S. L., Christensen, D., Simon, T. B., Morgan, B. R., and Bauer, E. S. (2022). *Towards software Bill of materials in the nuclear industry*, INL/RPT-22-68847-Rev000. Idaho Falls, ID, United States: Idaho National Laboratory INL. doi:10.2172/1901825

Elias, G., and Hewitt-Jones, J. 2023 Software bills of materials face long road to adoption. Available at: https://www.cyberscoop.com/dhs-sbom-adoption/(Accessed: January 03, 2023).

ENISA (2020). EUCS – cloud services scheme. Available at: https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme.

FAIR 2017a FAIR risk Analytics platform management. Available at: https://www.fairinstitute.org/fair-u (Accessed December 26, 2017).

FAIR 2017b Quantitative information risk management | the FAIR Institute', factor analysis of information risk. Available at: http://www.fairinstitute.org/(Accessed December 26, 2017).

FAIR 2017c What is a cyber value-at-risk model? Available at: http://www.fairinstitute.org/blog/what-is-a-cyber-value-at-risk-model (Accessed December 26, 2017).

FAIR North Carolina Chapter FAIR Institute 2023 Factor analysis of information risk (FAIR) Institute. Available at: https://link.fairinstitute.org/group/8-north-carolina-chapter (Accessed January 12, 2023).

Fujita, T., Kogiso, K., Sawada, K., and Shin, S. (2015). "Security enhancements of networked control systems using RSA public-key cryptosystem," in 2015 10th Asian Control Conference: Emerging Control Techniques for a Sustainable World, ASCC 2015, Kota Kinabalu, Malaysia, May, 2015. doi:10.1109/ASCC.2015.7244402

Han, D. I. D., Bergs, Y., and Moorhouse, N. (2022). Virtual reality consumer experience escapes: preparing for the metaverse. *Virtual Real.* 1, 1443–1458. doi:10.1007/S10055-022-00641-7

He, S., Ficke, E., Pritom, M. M. A., Chen, H., Tang, Q., Chen, Q., et al. (2022). Blockchain-based automated and robust cyber security management. *J. Parallel Distrib. Comput.* 163, 62–82. doi:10.1016/J.JPDC.2022.01.002

Henry, M. H., and Haimes, Y. Y. (2009). A comprehensive network security risk model for process control networks. *Risk Anal.* 29 (2), 223–248. doi:10.1111/j.1539-6924.2008.01151.x

ISO (2022). *ISO/IEC 27001 and related standards Information security management*. Geneva, Switzerland: ISO.

Jalali, M. S., Kaiser, J. P., Siegel, M., and Madnick, S. (2019). The internet of things promises new benefits and risks: a systematic analysis of adoption dynamics of IoT products. *IEEE Secur Priv.* 17 (2), 39–48. doi:10.1109/MSEC.2018.2888780

Kim, J. (2021). Advertising in the metaverse: research agenda. *J. Interact. Advert.* 21 (3), 141–144. doi:10.1080/15252019.2021.2001273

Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., et al. (2021). Cyber security in the age of covid-19: a timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Comput. Secur* 105, 102248. doi:10.1016/j.cose.2021.102248

Latvala, S., Sethi, M., and Aura, T. (2020). Evaluation of out-of-band channels for IoT security. *SN Comput. Sci.* 1 (1), 18–17. doi:10.1007/s42979-019-0018-8

Lee, S. G., Trimi, S., Byun, W. K., and Kang, M. (2011). Innovation and imitation effects in Metaverse service adoption. *Serv. Bus.* 5 (2), 155–172. doi:10.1007/s11628-011-0108-8

Mackenzie, S. (2022). Criminology towards the metaverse: cryptocurrency scams, grey economy and the technosocial. *Br. J. Criminol.* 62, 1537–1552. doi:10.1093/BJC/AZAB118

MiCA (2022). *Proposal for a regulation of the European parliament and of the council on markets in crypto-assets, and amending directive (EU) 2019/1937 (MiCA).*

MITRE 2023 CVE - common vulnerabilities and exposures. Available at: https://cve.mitre.org/(Accessed January 03, 2023).

Moreira, F. R., Silva Filho, D. A.Da, Nze, G. D. A., Sousa Junior, R. T.De, and Nunes, R. R. (2021). Evaluating the performance of NIST's framework cybersecurity controls through a constructivist multicriteria methodology. *IEEE Access* 9, 129605–129618. doi:10.1109/ACCESS.2021.3113178

Mozumder, M. A. I., Sheeraz, M. M., Athar, A., Aich, S., and Kim, H.-C. (2022). "Overview: technology roadmap of the future trend of metaverse based on IoT, blockchain, AI technique, and medical domain metaverse activity," in International Conference on Advanced Communication Technology (ICACT), PyeongChang Kwangwoon_Do, Korea, Republic of, February, 2022, 256–261. doi:10.23919/ICACT53585.2022.9728808

NIST 2023a Cybersecurity framework. Available at: https://www.nist.gov/cyberframework/getting-started.

NIST 2023b AI risk management framework | NIST. Available at: https://www.nist.gov/itl/ai-risk-management-framework (Accessed: April 18, 2023).

NIST 2023c Software security in supply chains: software bill of materials (SBOM) | NIST. Available at: https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/software-security-supply-chains-software-1 (Accessed: April 18, 2023).

Nist, C. (2016). Cybersecurity framework. Available at: https://www.nist.gov/cyberframework.

NTIA (2021). Software bill of materials (SBOM) | national telecommunications and information administration. Available at: https://ntia.gov/page/software-bill-materials (Accessed December 24, 2022).

NTIA 2023 SBOM at a glance', NTIA multistakeholder process on software component transparency | nutria.gov/sbom. Available at: https://tiny.cc/SPDX (Accessed January 02, 2023).

Park, S. M., and Kim, Y. G. (2022). A metaverse: taxonomy, components, applications, and open challenges. *IEEE Access* 10, 4209–4251. doi:10.1109/ACCESS.2021.3140175

Payton, T. (2018). Staying safe in an increasingly interconnected world: IOT and Cybersecurity. *Cyber Security: A Peer-Reviewed Journal* 2 (1), 66–72.

Roopak, M., Yun Tian, G., and Chambers, J. (2019). "Deep learning models for cyber security in IoT networks," in 2019 IEEE 9th Annual Computing and Communication Workshop and Conference, CCWC 2019, Las Vegas, NV, USA, January, 2019, 452–457. doi:10.1109/CCWC.2019.8666588

Russell, B., and Van Duren, D. (2016). Practical internet of things security: a practical, indispensable security guide that will navigate you through the complex realm of securely building and deploying systems in our IoT-connected world. Available at: https://www.packtpub.com/hardware-and-creative/practical-internet-things-security (Accessed: March 06, 2019).

Sehgal, N. K., Bhatt, P. C. P., Acken, J. M., Sehgal, N. K., Bhatt, P. C. P., and Acken, J. M. (2020). "Cloud computing pyramid," in *Cloud computing with security* (Berlin, Germany: Springer International Publishing), 49–59. doi:10.1007/978-3-030-24612-9_3

Shu, Y., Zhang, J., and Yu, H. (2021). Fairness in design: a tool for guidance in ethical artificial intelligence design. *Lect. Notes Comput. Sci. Incl. Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinforma.* 12774 (LNCS), 500–510. doi:10.1007/978-3-030-77626-8_34

Sparkes, M. (2021). What is a metaverse. *New Sci.* 251 (3348), 18. doi:10.1016/S0262-4079(21)01450-0

Stephenson, N., Snow crash: a novel. Spectra, 2003.

Sun, D., Wu, Z., Wang, Y., Lv, Q., and Hu, B., 'Risk prediction for imbalanced data in cyber security: a siamese network-based deep learning classification framework', in Proceedings of the International Joint Conference on Neural Networks, Budapest, Hungary: July. 2019, 2019, pp. 1–8. doi:10.1109/IJCNN.2019.8852030

Wang, F. Y., Qin, R., Wang, X., and Hu, B. (2022). MetaSocieties in metaverse: MetaEconomics and MetaManagement for MetaEnterprises and MetaCities. *IEEE Trans. Comput. Soc. Syst.* 9 (1), 2–7. doi:10.1109/TCSS.2022.3145165

Xi, N., Chen, J., Gama, F., Riar, M., and Hamari, J. (2022). The challenges of entering the metaverse: an experiment on the effect of extended reality on workload. *Inf. Syst. Front.* 1, 659–680. doi:10.1007/S10796-022-10244-X