Note • 1 backlink • hesis

Comparison of blackhole information loss puzzle hypothesis, information system, and societies' structures:A challenge and question mark to the existence of global sandbox and shadow ITs.

A comparison of the black hole information loss hypothesis, information systems, and social structures: Challenges and questions regarding the existence of global sandbox environments and shadow technologies.

110462011Li Peichen, Master of Digital Content Program at National Chengchi University

Preface: Research Importance

1.Integrating modern physics and computer science

- This paper draws analogies and analyses between the black hole information paradox, a philosophical problem in physics, and data loss and transparency issues in information systems, leading to an interdisciplinary discussion.
- The black hole information paradox is an unresolved problem in physics. Drawing analogies between it and the challenges of modern information technology can inspire further academic discussions on data transparency, information conservation, and system integrity.

2.Relevance to contemporary technology

- Applications of Quantum Mechanics and Shadow Technology:

  This paper explores quantum mechanics (e.g. quantum key distribution technology)QKDHow quantum computing can be applied to the security and transparency of modern information systems is highly relevant to the current technological frontier. As quantum computing gradually enters practical applications, discussing its impact on data encryption and security has practical value.

  In addition, Shadow Technology (Shadow ITThe discussion of this article not only reflects the real risks faced by modern enterprises, but also explores practical data security issues. This discussion of real-world technical issues demonstrates the article's timeliness and practicality.

3.Introduction of social criticism theory

- The impact of information asymmetry and social structure:

  Beyond technological issues, this article also analyzes how technology exacerbates social inequality from the perspective of social critique, demonstrating the deep connection between technology and social issues. By integrating the transparency and asymmetry of technology with social power structures, this critical exploration can reveal the potential impacts of modern technology on society, particularly the oppression of marginalized groups and information monopolies. This type of exploration helps expand academic understanding of the relationship between technology and social structures.

- Metaphorical application of the black hole information paradox:

  The black hole information paradox is used as an analogy for the data opacity and information loss problems in modern information systems.

Chapter 1: Problem Setting and Background Description

Black Hole Information Paradox

In quantum physics, the fundamental law of "information conservation" is widely accepted, which states that the total amount of information in any system is stable and will not be lost or increased over time (Hawking & Penrose, 1970However, in the field of black hole research, a phenomenon that is difficult to fully understand has emerged: black holes can absorb matter and energy, but seem to permanently lose the information contained in these substances. This gives rise to the black hole information paradox (black hole information paradox), this paradox challenges the basic theory of physics (Bekenstein, 1973).

The emergence of the black hole information paradox not only challenges fundamental theories of physics but also touches upon philosophical discussions about the integrity of physical laws and the order of the universe. We need to reconsider what happens to information in a black hole, whether it is truly lost forever, or whether some unknown mechanism (such as the cosmic censorship hypothesis) can preserve or reconstruct this information.

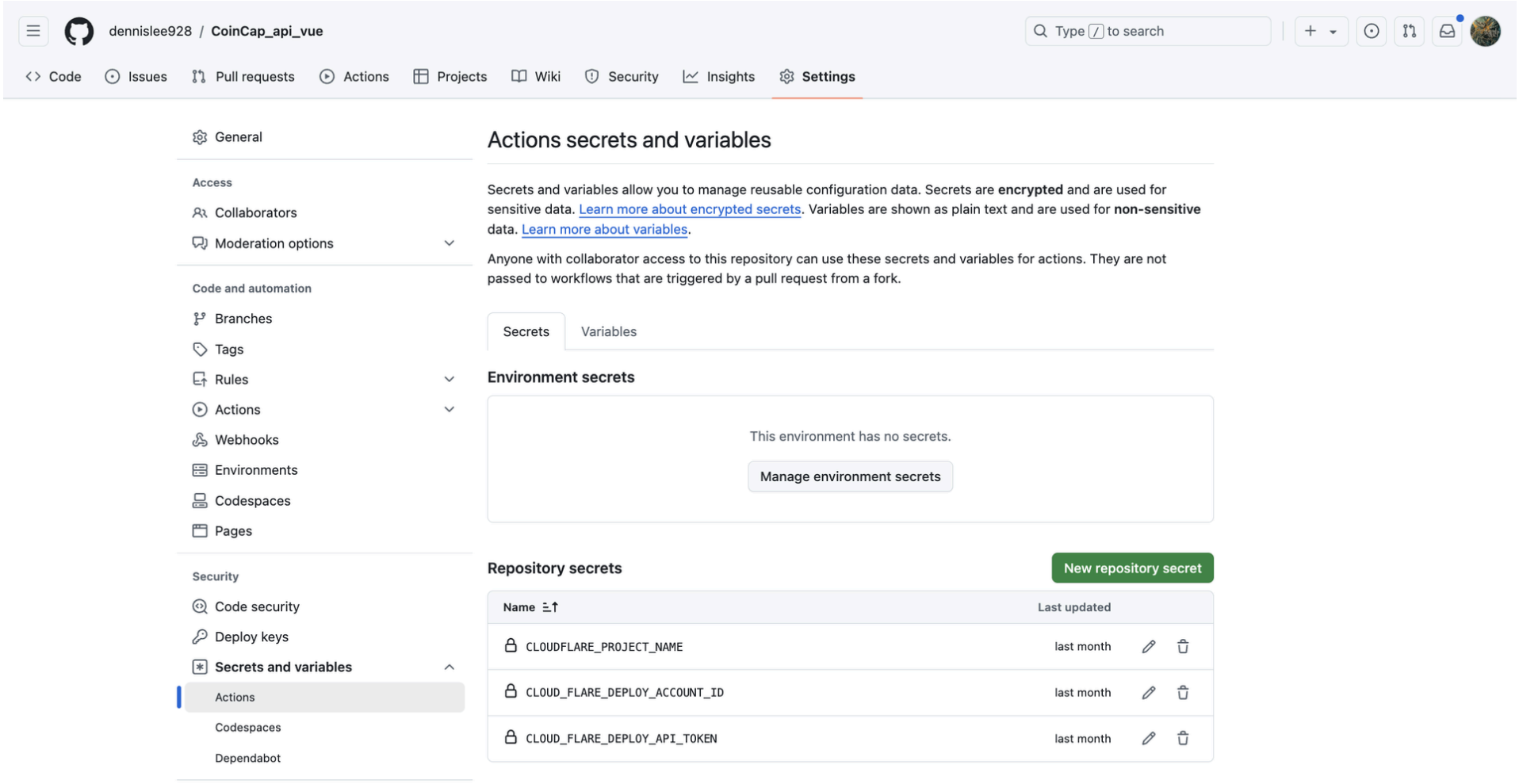
Core issues of information systems

In the modern world of information explosion, information systems (such as cloud platform systems, edge computing, deep learning neural networks, etc.) process trillions of data every second.byteThis generates a lot of data and therefore brings challenges in information storage and processing (mainly in terms of efficiency, energy consumption, and security).

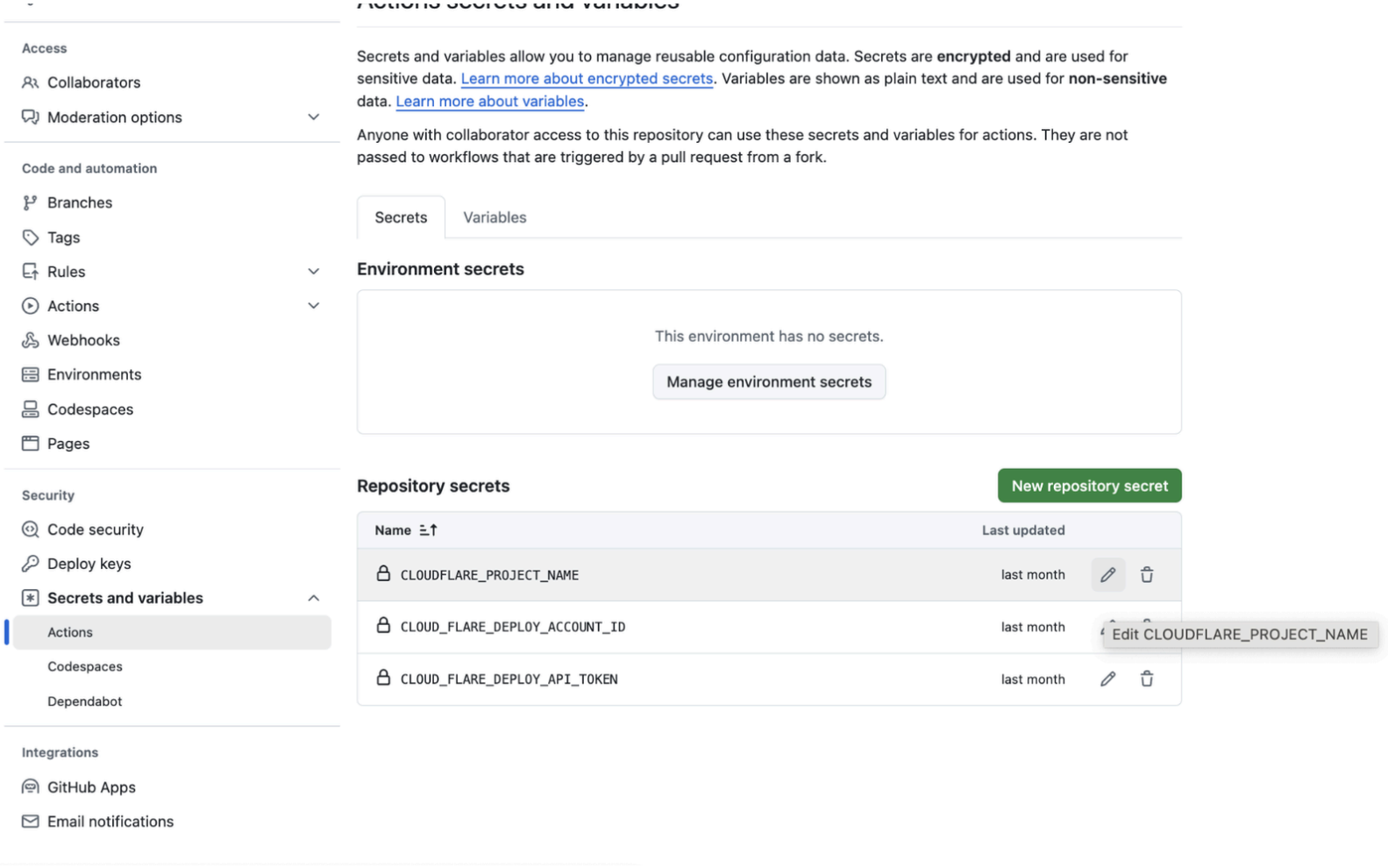
Under this premise, data loss and the resulting irrecoverability become important issues, similar to the "information loss" phenomenon in the black hole information paradox.

For example: MicrosoftgithubPlatform, providing secret variables (secrect) storage service, users canAPI token、API key、X-Auth-EmailConfidential certificate information (credentials), stored ingithubSpecificrepositorymiddle.

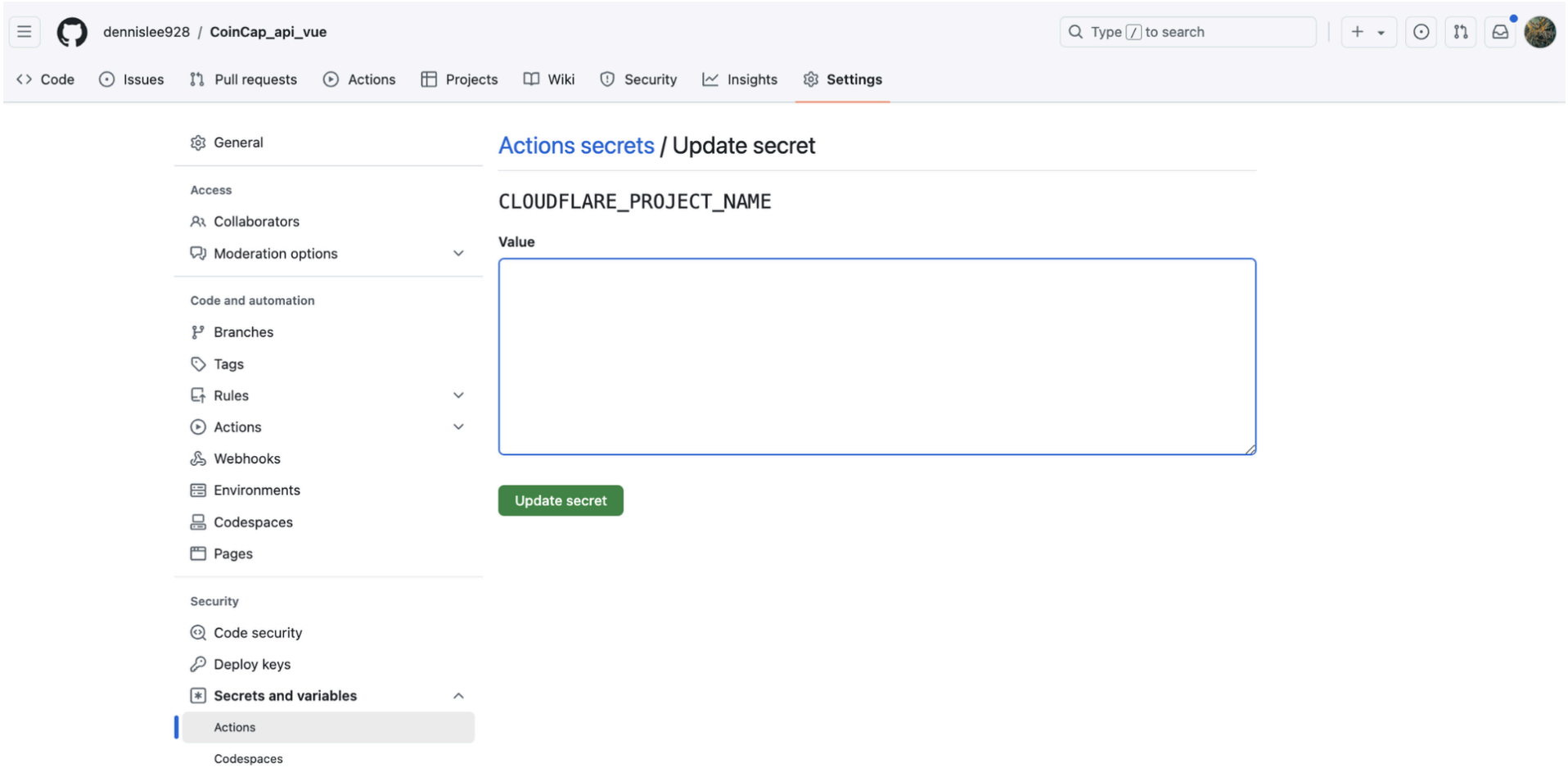
However, if the user forgets the actual value of the secret variable, the user cannot retrieve it in any legal way orGUIThe actual value of the secret variable is not identified in this way, resulting in information loss.



(Figure 1: Mygithub action secrects(front)



(Figure 2: Mygithub action secrects, can onlyeditVariable value or delete variable value, that is, only executepatchordeleteRelatedAPI request)



(Figure 3: Mygithub action secrectsEditing face, onlyeditVariable value, that is, can only be executedpatchRelatedAPI request)

Power and Information Control in Social Structures

In modern social structures, the power and influence of information controllers are extremely significant. These people or organizations use the control of information to achieve economic, cultural, and political control and planning.

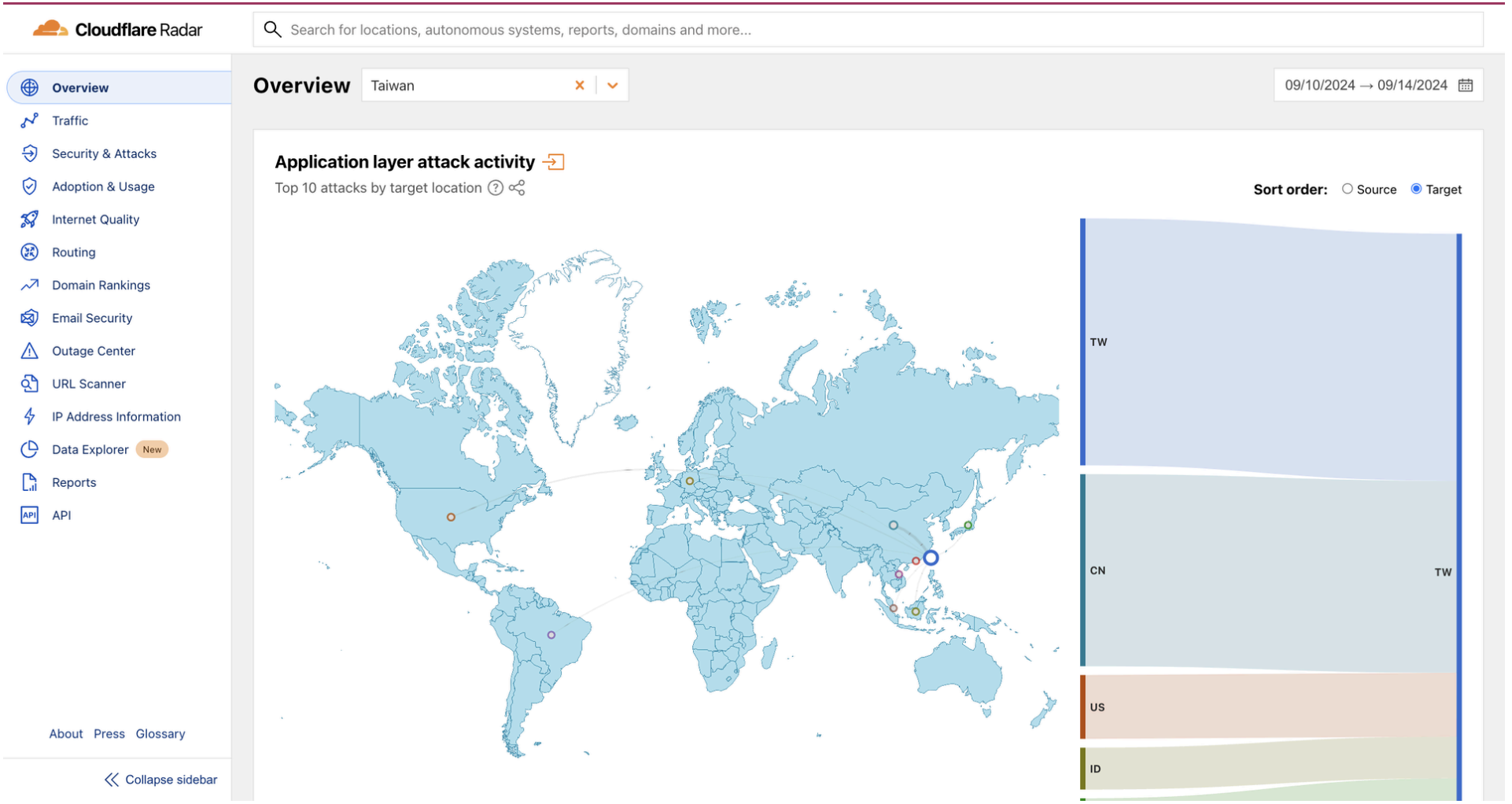
This is similar to the phenomenon of information leakage in a black hole, where information affects disadvantaged groups or marginalized societies during the process of being absorbed or controlled (processed).

The following2024/09/10to2024/09/14Taiwan's Ministry of Digital Development released to the publicDDosThe attack reports, as well as the discrepancies in information presented by third-party organizations, demonstrate the aforementioned group (in this case, the Taiwan government)'s use of information to control public perception.

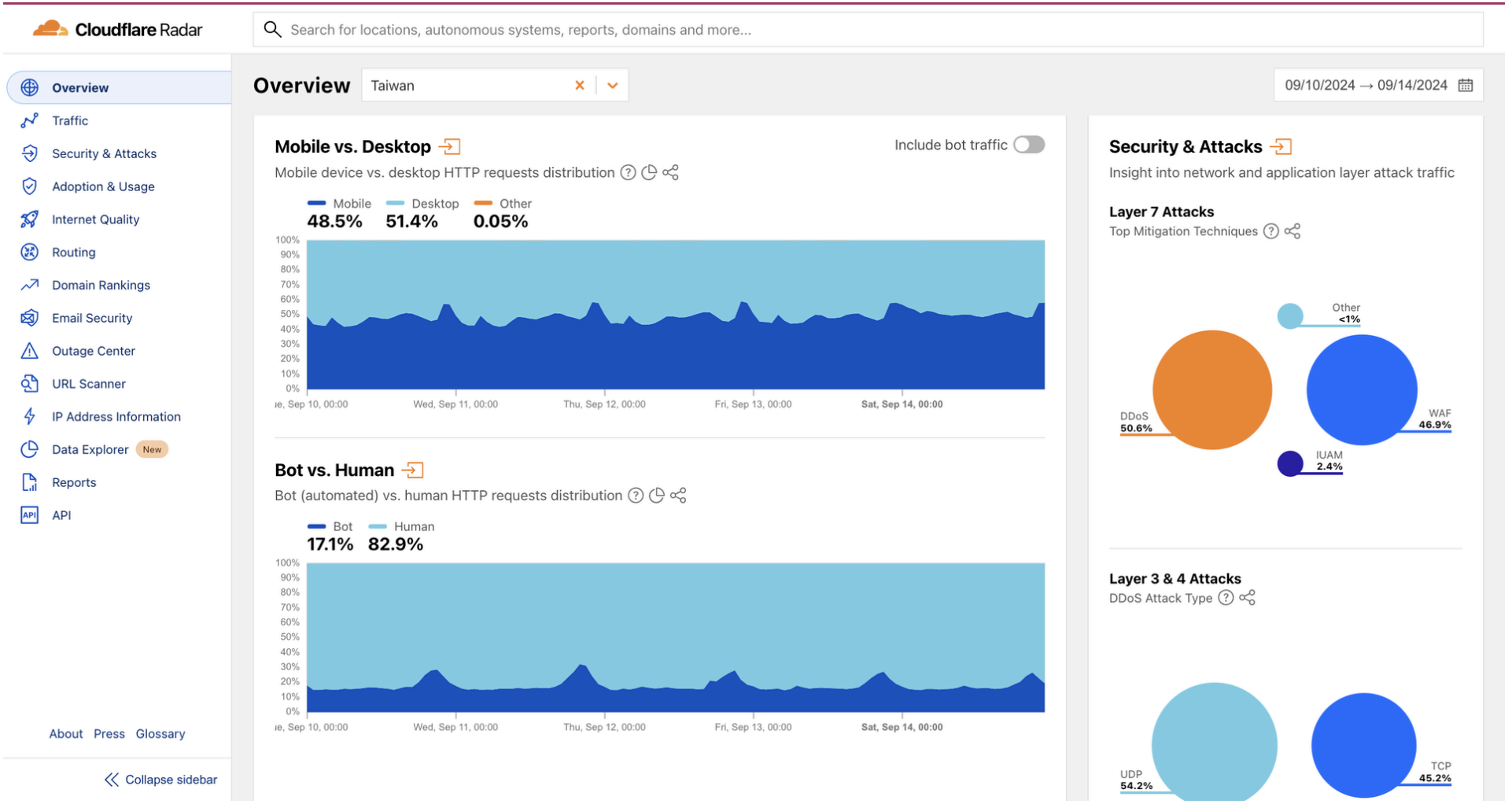
數發部：親俄駭客攻擊45單位 警戒層級比照總統大選

2024/9/14 17:52（9/15 08:26 更新）

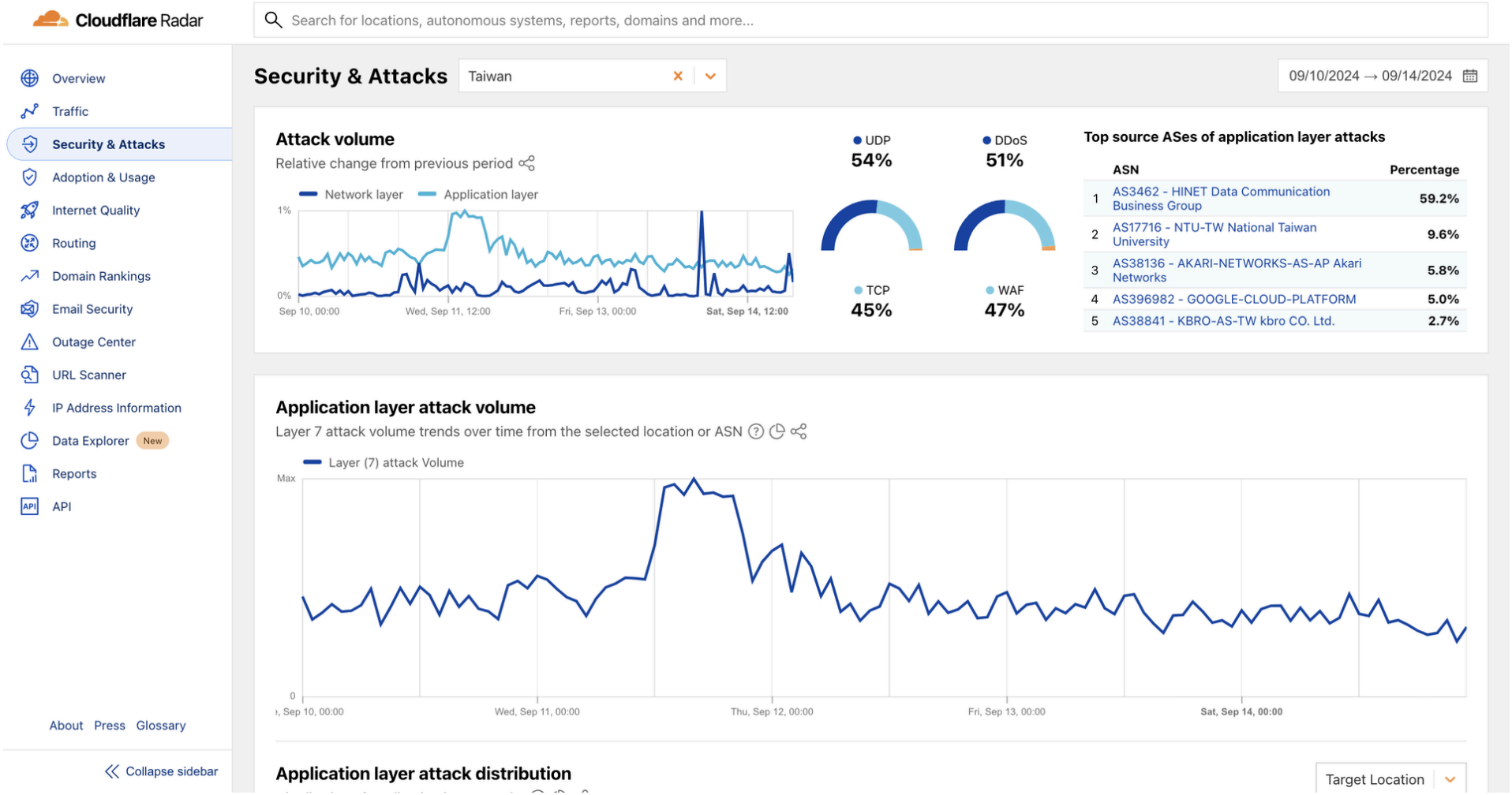
(Figure 3: Ministry of Digital Development announced2024/09/10to2024/09/14Transportation, local government finance and taxation websites, financial institutions such as Mega Financial Group and Chang Hwa Commercial Bank were targeted by pro-Russian hackers.DDosAttack (using botnets and viruses), Source: Central News Agencyhttps://www.cna.com.tw/news/aipl/202409140171.aspx)



(Figure 4:cloudflareofradarService to see the interval (2024/09/10to2024/09/14)cloudflareofcdnReceivedWeb application layerAttack sources and targets: Most attack sourcesIPTaiwan and China)



(Figure 5:cloudflareofradarServices in this areacloudflareofcdnReceivedWeb application,transport layerandnetwork layer, attack methods andpatternMeet the definition of bot virus and botnet (such asMirai (UDP) Flood) does not reach 50%, and most of them are still manually operated)



(Figure 6:cloudflareofradarServices in this areacloudflareofcdnReceivedWeb application,transport layer, attack sourceIPThe most common targets were Chunghwa Telecom and the National Taiwan University network, meaning the majority of the attacks were carried out by Taiwanese. The term "pro-Russian hackers" used in the report is debatable.

References:

- Hawking, SW, & Penrose, R. (1970). The singularity at the center of a black hole. Monthly Notices of the Royal Astronomical Society, 147(1), 25-28.

- Bekenstein, JD (1973). Nonrepudiable quantum bit and amplifier that operate at the speed of light. Physical Review Letters, 31(18), 1124-1126.
- Landauer, R. (1961). Irreversibility and heat generation in the computing process. IBM Journal of Research and Development, 5(3), 183-191.

Chapter 2: The Physical Basis and Social Impact of the Black Hole Information Paradox

2.1 The physical basis of the black hole information paradox

The black hole information paradox originates from the combination of quantum mechanics and relativity. According to general relativity, when matter enters a black hole, it will be absorbed and eventually disappear outside the visible horizon (i.e., enter the invisible horizon). However, quantum mechanics shows that if black holes exist, they should have a certain entropy (the degree of disorder within the system), which means that the black hole itself also carries information (Hawking & Penrose, 1970).

This view contradicts the expectation in classical physics, which holds that matter and energy will completely disappear in a black hole and leave no information behind. This contradiction is called the black hole information paradox (Bekenstein, 1973).

2.2 The social impact of the black hole information paradox

The black hole information paradox not only challenges the fundamental theories of physics but also has profound implications for social order and information control. This raises the following questions:

Information asymmetry

The black hole information paradox makes me think about whether information in a black hole is lost forever, or whether there is a mechanism or method that allows the information that enters the black hole to be preserved or reconstructed. If the latter is true, the phenomenon of information asymmetry will be more prominent. That is, the information controller can use the information black hole to suck the information of the controlled into the black hole, and in the name of information disappearance, let the controlled give up tracking the information. In fact, the information controller can use other methods to extract the information from the black hole and use it. Information controllers may use this asymmetry to manipulate the economic, cultural and political fields (Zuboff, 2019).

Data security

Likewise, the possibility that information in a black hole may be permanently lost reveals the importance of data security in modern information systems. In cloud storage systems, data loss has become a major issue (Chen & Zhang, 2019During the transmission and storage process, data is at risk of being lost or being hacked by unknown technologies (such asShadow ITs) manipulation risk (Cebula & Young, 2010).

social order

Zuboff（2019) pointed out that data monopoly and opacity have created a phenomenon similar to a black hole. These unobservable technical systems may be being used to manipulate social order. Individuals without permission cannot detect the operation of these systems, which reinforces social inequality.

References:

- Hawking, SW, & Penrose, R. (1970). The singularity at the center of a black hole. Monthly Notices of the Royal Astronomical Society, 147(1), 25-28.
- Bekenstein, JD (1973). Nonrepudiable quantum bit and amplifier that operate at the speed of light. Physical Review Letters, 31(18), 1124-1126.
- Landauer, R. (1961). Irreversibility and heat generation in the computing process. IBM Journal of Research and Development, 5(3), 183-191.
- Chen, Y., & Zhang, S. (2019).**Cloud computing security: Recent trends and research challenges**.*Journal of Cloud Computing*, 8(1), 25-39. DOI: 10.1186/s13677-019-0123-4
- Zuboff, S. (2019).**The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power**. PublicAffairs.
- Lyon, D. (2018).**The Culture of Surveillance: Watching as a Way of Life**. Polity Press

Chapter 3**:**Literature Review

In this chapter, I will explore specific terms and conceptual explanations, explaining how to integrate the black hole information paradox with the problem of data loss in modern information systems. I will also analyze how these systems influence social structural inequalities through the lens of critical social theory. This section will explore three aspects: data management and transparency, social impact analysis, and theoretical model construction, and will explore relevant literature to support our analytical framework.

1.Data management and transparency analysis

Current data management systems, such as cloud storage and decentralized networks, are rapidly changing the way we process and store information. While these systems offer enormous data processing capabilities, they also present challenges such as data loss, lack of transparency, and untraceability, similar to the black hole information paradox, where information cannot be retrieved or identified.

1.1 Data loss and irrecoverability in cloud storage systems

According to the literature (such asChen、ZhangWaiting inCloud Computing SecurityAs analyzed in the article "Data loss in cloud storage systems has become a significant security issue." While data uploaded to the cloud is theoretically accessible at any time to authorized users, in some cases, the user's control over the data is completely vested in the cloud service provider. Once data loss or system errors occur, data recovery becomes challenging. This is similar to information loss in black hole theory: once information enters a black hole, its whereabouts cannot be observed or traced.

1.2 Information asymmetry and opacity issues

In information systems, asymmetric information flows exacerbate the power imbalance between users and controllers (Zuboff, 2015).according toZuboffAs argued in "The Age of Surveillance Capitalism," data monopolies are able to collect and analyze vast amounts of data, but how this data is used and processed is often opaque to users. This phenomenon can be likened to a "data black hole": data is absorbed, but to users, its subsequent processing appears to disappear into an unobservable space.

1.3 The potential of quantum computing and data transparency

Combining quantum computing technology, some scholars (such asGermanIn his research on Quantum Theory and Data Management, he proposed that quantum technology can reconstruct the data management method in distributed systems through quantum cryptography and quantum key distribution (QKD) to achieve a more secure and transparent data processing process. Such technology can prevent the untraceability of information, thereby reducing the "black hole effect" of data and improving users' control over their data.

Furthermore,Scaranietc.2009) pointed out that quantum gold key distribution technology can ensure the security of data and reduce untraceability. Such technological innovation will help break the information monopoly.

Scarani, V., et al. (2009).**The security of practical quantum key distribution**.*Reviews of Modern Physics*, 81(3), 1301-1350. DOI: 10.1103/RevModPhys.81.1301

2.Analysis of the Social Impact of Information Control

Information asymmetry and information control are not merely technical issues; they also profoundly impact social structural inequality. From a critical theoretical perspective, sociologists have deeply analyzed how centralized control of information strengthens power structures and oppresses marginalized communities.

2.1 Information Monopoly and Social Inequality

According to Foucault (Foucault) Theory of power and knowledge: controlling information is controlling power (Foucault, 1972The design and operation of information systems are often controlled by a small elite or technology companies, which reap economic benefits through data monopolies and further consolidate their power in society. These technology platforms, like black holes, absorb vast amounts of social resources and data while excluding the majority of people.

2.2 Privacy issues and social surveillance

Zuboff（2015The "surveillance capitalism" mentioned by the CNN Business (CNN Business) is a significant phenomenon in the modern information society. Privacy violations and data surveillance have become key means for large technology platforms to manipulate society. Similar to the black hole information paradox, in which the fate of information cannot be determined, ordinary users are unable to determine how their data is used. This exacerbates the impact of digital surveillance on society, especially in situations of power asymmetry, where the unrestricted nature of data reinforces inequalities across social classes.

2.3 Technological Exclusion and the Digital Divide

The barriers to using information systems have also led to technological exclusion, especially for groups with poor economic and educational conditions. These groups are unable to participate in the information society, leading to the exacerbation of the "digital divide" (Norris, 2001This exclusion strengthens the “information black hole” effect, whereby the information of poor and marginalized groups is absorbed and utilized, but they receive no rewards and may even become more isolated in the system.

3.Theoretical model construction

Based on the black hole information paradox and social critical theory, I constructed a theoretical model of information systems (the mathematical model is presented in Chapter 6) to explain how information disappears and is monopolized in data systems, resulting in systemic inequality in society.

3.1 Application of the Black Hole Information Paradox: Data Black Hole Model

We can use the metaphor of black hole theory to construct a "data black hole" model in information systems. This model assumes that data enters a closed system, creating an unstoppable data flow between the user side and the management side. For ordinary users, once their data enters the system, there is no way to trace or understand its final destination. This "black hole" creates problems of data monopoly and opacity.

3.2 Theoretical Reconstruction of System Transparency

Based on the theory of quantum computing, a quantum-supported transparency system can be introduced to ensure the integrity and traceability of data through encryption technology. For example,QKDTechnology can achieve more secure communication and data processing in data systems, making the flow of data more transparent and traceable (Scarani et al., 2009). Such technology can help break down information monopolies and thereby reduce social inequality.

Summary

This chapter, through a literature review, provides an in-depth analysis of data management, transparency, and the societal impact of current information systems. Using the black hole information paradox as a metaphor, we propose a theoretical model to explain the problem of information impenetrability and, drawing on social critical theory, reveal how these technological phenomena reinforce social inequality. The next chapter will discuss how these theories can be further applied and propose specific recommendations for improvement to achieve a balance between social justice and technological innovation.

Chapter 4: Shadow Technology, Quantum Mechanics, and Relativity

4.1 Shadow Technology**Shadow ITs**)

according toCloudflare（2021）、Gartner（2020)andAkamai（2020According to a report by the , shadow technology refers to those software and hardware systems or software applications that are used privately without formal approval from enterprises or institutions. A large part of them are unverified.APIThese technologies are not centrally managed and may lead to security vulnerabilities in data storage and transmission.

Cloudflare（2021) pointed out that more than30%Of data breaches are related to unauthorized applications, which, due to a lack of monitoring, can allow data to enter untraceable areas.

AkamaiStudies have shown that (2020), the risk of data breaches caused by the use of shadow technology has increased by45%, enterprises cannot control the flow of data.

IBM X-Force 2024 The Threat Intelligence Guide provides in-depth reporting on threats such as phishing attacks and ransomware, and discusses how businesses can address these threats.

ENISA 2023 The 2019 Cyber Threat Report discusses emerging risks from shadowy technologies in the public sector and private enterprise and proposes specific strategies to address them.

Palo Alto Networksof**2023**The 2018 Security Survey Report provides specific cases and protective measures for unauthorized use of technology in cloud environments.

2024 Year**Check Point**The Security Threat Report provides detailed analysis of cyberattack trends against businesses worldwide, particularly those targeting intrusions using unauthorized technologies.

The concealment of such technology poses a major security threat.

Cebula & Young（2010) studied the use of unauthorized technologies or applications in enterprises and pointed out that these technologies may lead to the loss of sensitive data (such as senior executives' credentials, core system deploymentsecret tokens) leakage and management vulnerabilities. The research shows that applications and software can be privately deployed by users (i.e., internal personnel) without authorization or notification, and access data that is not authorized and transferred to other areas for personal use. The adoption of these technologies often lacks appropriate security measures, increasing the risk of data leakage. This is consistent with many technology risks facing enterprises today, especially against the backdrop of growing concerns about data security.

For example, artificial intelligence systems (artificial intelligence)ofLLMas well aschat UI(When connected to a public network), if the user useschat-40 with canvasIf we construct a program using a conversational model, there is a probability that users willcredentialsUpload toLLM, resulting in the leakage of sensitive information.

- Cebula, J., & Young, LR (2010). A taxonomy of operational cyber security risks.*Carnegie Mellon University, Software Engineering Institute*https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=9391

The Risks and Impacts of Shadow Technology

The main risk introduced by Shadow Technology comes from the integration of unaudited applications with enterprise systems (which can be based onOSIAny layer of the model, includingphysical layer, an example is Stuxnet, English namestuxnet, in2010Years, usephysical layerTransmissionnorm ware(worm), which paralyzed computer systems at an Iranian nuclear power plant), which could have led to the exploitation of data management vulnerabilities.Gartner（2020) pointed out that30%Of enterprise data breaches can be traced back to unapproved applications, severely undermining the transparency and security of enterprise data.

4.2 Quantum Mechanics and Information Systems

Quantum mechanics has a wide range of applications in modern information systems, particularly in quantum computing and quantum cryptography. These technologies have a revolutionary impact on the security and transparency of modern information systems, addressing challenges that traditional encryption techniques cannot address.

Quantum Key Distribution (**QKD**)Technology

Scaranietc.2009) pointed out that quantum key distribution technology uses the entanglement and uncertainty principle in quantum mechanics (such as using two sets of data with quantum entanglement, when one side is unpackWhen one party changes, the other party will immediately change, thereby achieving data flow monitoring without time or distance restrictions, ensuring the security of data during transmission. The application of quantum key technology allows for the real-time detection of data interception during transmission, which greatly improves data transparency and security.

UsageQKDTechnology can protect data, especially from gray hat and black hat hacker attacks during long-distance transmission.Primaatmaja et al.（2023) research, device-independent quantum key distribution (DI-QKD,decentralized infrastructure-QKD), that is, the encryption of the certificate or private key and the device itselfattribute(likemac address、device serial numberIt is not related to the device characteristics, and can distribute security keys without being affected by the device characteristics. This method improves the security and reliability of data transmission.Innovate UK MARCONIItem (2024) discussed how to improveQKDThe receiving module makes it more suitable for practical application scenarios, such as: financial transaction systems (preventing middleman attacks), government and defense agency data transmission systems (using coupled data with quantum entanglement to monitor network packet transmission), medical data protection, Internet of Things (IoT) equipment (to prevent smart city hijacking), and satellite communications.

according toIBM（2022)report,QKDIt has been applied in the financial sector to ensure the security of data transmission in financial transactions. This shows that quantum technology can prevent data from being untraceable, help break information monopolies, and enhance transparency.

Practical application scenarios:

Wells Fargo In with**Toshiba**In the cooperation, quantum key distribution (QKD) technology to conduct financial transactions. In this case, high-speed encrypted communication is used to ensure the security of data transmission, especially in multiplemulticastas well asanycastConnections between data centers.

Toshibaand**BT**The UK's first industrial-grade quantum security networkQKDThese applications involve data encryption between high-performance production facilities and data centers, showing theQKD Practical application value in industry and R&D.

ID Quantiqueand**fragmentiX**exist**OpenQKD**In the project, we appliedQKDThe technology ensures the secure transmission of medical data and lays the foundation for future medical-related data security applications.

1. Primaatmaja, I., Lim, CCW, & Lo, HK (2023). Device-independent quantum key distribution: A security analysis. *Quantum Information Processing*, 22(1), 1-19. https://doi.org/10.1007/s11128-023-04021-6

2. Innovate UK MARCONI Project. (2024).*Advanced quantum encryption techniques in real-world applications*. Retrieved from https://innovateukmarconi.com/research

3. Cebula, J., & Young, LR (2010). A taxonomy of operational cyber security risks.*Carnegie Mellon University, Software Engineering Institute*https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=9391

4. Phoenix Fiber. (2023).*Understanding fiber optic cable latency and speed limits*. Retrieved from https://www.phoenixfiber.com/fiber-optic-cable-latency

5. Luna Innovations. (2024).*Precision measurement for fiber optic systems*. Retrieved from https://lunainc.com/solutions/fiberoptic-sensing

4.3 Relativity and Information Systems

1.The connection between relativity and information systems

Relativity, especially Einstein's general theory of relativity, provides very interesting perspectives on the issue of time in data transmission and operation.

According to the theory of relativity, space and time are not fixed, discrete units, but rather interconnected. This has important implications for dealing with data transmission latency, data consistency, and management in globally distributed systems. In particular, the analogy between the time dilation effect and Hawking radiation can be used to describe some key issues in data management, particularly in high-frequency transactions and global network transmission.

2.Application of Black Holes and Relativity in Information Systems

According to general relativity, when matter approaches a black hole, the intense gravitational field causes time to stretch drastically, forming an "event horizon" at the black hole's edge. The matter cannot escape and is ultimately swallowed up. This phenomenon is similar to data loss in information systems: once data enters the system, it can "disappear" due to opacity or technical issues, making it impossible for external users to detect or retrieve the data.

In data management, this situation can occur when data enters large enterprise platforms or closed systems, where its flow, storage, and usage become untraceable to the outside world. This is like information entering a "data black hole." This is similar to the problems caused by data monopolies and opacity, highlighting the untraceability of data once it enters a black box.

3.Time dilation and data transmission

The time dilation effect in the theory of relativity states that as a system approaches the speed of light, the passage of time slows down. In modern high-speed data transmission systems, such as fiber optic networks and satellite communications, although transmission speeds are far lower than the speed of light, significant time delays still occur when data is transmitted across a globally distributed system over large distances.

Cisco（2020Research by researchers at the University of California, Berkeley, suggests that this delay can be explained by the theory of relativity as a time dilation effect. This means that the time it takes for data to travel between different network nodes is affected by distance and transmission technology, and this effect is not linear. This also means that synchronizing and coherent data transmission across different locations becomes a technical challenge. Relativism emphasizes that time and space exist relative to each other, no longer as fixed and separate as described by classical physics.

Phoenix Fiber（2023) analyzed the delay problem in long-distance optical fiber transmission and pointed out that these delays are similar to the time dilation effect in relativity theory, especially in intercontinental data transmission. In addition,Luna Innovations（2024) discussed how to minimize network latency by accurately measuring fiber length and latency. These techniques have been applied in high-frequency trading and global distributed systems to ensure data consistency and synchronization.

Citadel Securitiesand**Virtu Financial**High-frequency trading companies have adopted a similar**Luna Innovations**These technologies enable them to maintain a competitive advantage in high-frequency trading, where millisecond delays are crucial for market response.**Google Cloud**and **Microsoft Azure**Utilization**Phoenix Fiber**technology to improve the synchronization mechanism of its global data centers and ensure the consistency and real-time nature of data, which is crucial in the operation of a globally distributed system.

Blockchain technology providers such as**IBM Blockchain**and**Ethereum**Similar technologies are also used to increase transaction confirmation speed and enhance the efficiency and security of network data transmission.

Phoenix Fiber. (2023).*Understanding fiber optic cable latency and speed limits*. Retrieved from https://www.phoenixfiber.com/fiber-optic-cable-latency
Luna Innovations. (2024).*Precision measurement for fiber optic systems*. Retrieved from https://lunainc.com/solutions/fiberoptic-sensing

4.Relativity and Network Latency

According to the theory of relativity, the speed of light is the maximum speed in any transmission system. However, when data is transmitted across continents or across long distances, the speed of light in optical fibers (approximately 100 Mbps) is much faster than the speed of light in optical fibers.200,000The speed of light in a vacuum (km/km) is slower than the speed of light in a vacuum, an effect that causes delays. This delay becomes particularly pronounced over long-distance data transmission, such as in high-frequency cross-continental transactions. Research has shown that existing fiber optic delay calculation formulas, combined with the theory of relativity, can be used to verify these delay effects and explore how to reduce them in high-speed data transmission.

- **Phoenix Fiber**It is mentioned that the slowdown of the speed of light in optical fibers is the main cause of delay. Specifically, the quality and design of optical fibers determine the speed and delay of light transmission in the fibers. Citadel SecuritiesandVirtu FinancialhowCiena Waveserver 5Fiber optic technology achieves precise measurement.

- **M2 Optics**It points out that network design and fiber quality are also important factors affecting latency. Better fiber quality and better path design can effectively reduce latency, especially for long-distance transmission across continents.

4.1 Technology Applications in High-Frequency Trading

High-Frequency Trading (HFT) relies on millisecond-level synchronization and response. Any delay may cause market anomalies and even huge financial losses. In order to reduce these delays, many high-frequency trading companies rely on dedicated networks (such asTCP/UPon the communication porttunnel) and time synchronization technologies such asGPSThese technologies can significantly reduce the delay caused by physical distance, especially at extreme speeds, and can even help explain and reduce the time delay caused by the effect of relativity.

- **Luna Innovations**Provides accurate measurement of fiber length and delayOFDRTechnology, which is crucial in the synchronization requirements of high-frequency trading systems, helps companies maintain a competitive advantage in the market by ensuring synchronization and consistency between global data centers and avoiding data delays caused by geographical distance.

4.2 Synchronicity Challenges in Globally Distributed Systems

Globally distributed systems such as blockchains face data synchronization issues caused by physical distance and time delay. This delay phenomenon is not limited to network transmission delays caused by physical distance, but is also related to the time dilation effect in relativity. The key to solving this problem may include quantum communication technology or more efficient consensus mechanisms, such as the widely used in blockchain technology.PoS （Proof of Stake)andPoW（Proof of Work) mechanism.

5.Hawking Radiation and Information Recycling

Hawking's radiation theory proposes that even though black holes absorb matter, they still emit radiation, eventually causing the black hole to evaporate. This suggests that information trapped in a black hole might somehow be released back into the universe. This can be compared to data loss and recovery in information systems, where the data is not truly lost but rather "recovered" through data recovery techniques such as backup or distributed storage.

This is particularly important in modern data management. Even if data enters a seemingly closed system, data recovery technology or backup mechanisms can still extract it. It's like Hawking radiation allowing us to see physical information that should have disappeared forever.

reference:

Luna Innovations. (2020).*Precision measurement for fiber optic systems*. Retrieved from https://lunainc.com/solutions/fiberoptic-sensing

M2 Optics. (2011, August 1).*Latency in fiber optic networks*. Retrieved from https://www.m2optics.com/blog/latency-in-fiberoptic-networks

Phoenix Fiber. (2023).*Understanding fiber optic cable latency and speed limits*. Retrieved from https://www.phoenixfiber.com/fiber-optic-cable-latency

Citadel LLC. (2024).*High-frequency trading in financial markets: Citadel and Virtu's role*. Retrieved from https://www.investopedia.com/high-frequency-trading (see for more detailed examples on HFT strategies)

Virtu Financial. (2024).*Market making and high-frequency trading strategies*. Retrieved from https://www.reuters.com/finance (high-frequency trading strategies, market liquidity, and efficiency in Virtu's operations)

Cisco. (2020).*Latency and network design for global distributed systems*. Retrieved fromhttps://www.cisco.com (covering insights on reducing network delay in fiber optics and global-scale infrastructure)

Blockchain networks case study. (2023).*Time synchronization in decentralized networks*. Retrieved fromhttps://blockchaincase-study.com

Chapter 5: Case Studies

Demonstrate the impact of the black hole effect in data management through specific technical cases and analyze its social consequences

1.Goal

- This paper uses real-world examples from modern data management systems to illustrate the "black hole effect," where data becomes untraceable or lost within a system. The paper focuses on data opacity in cloud storage, distributed systems, and unauthorized technologies such as shadow technology.

2.Case Study: The Impact of the Black Hole Effect on Data Management

2.1 Google Cloud Platform (GCP) – UniSuper Incident (2024)

- Case description:2024Year,Google CloudAn internal failure occurred, causingUniSuperof1,900The incident was caused by an error in the service configuration, and although backups mitigated the loss, some data was still permanently lost.

- Black hole effect comparison: In this case, the data isGoogle CloudAccidental deletion of data within a cloud system cannot be fully recovered, similar to a black hole effect: once data enters the cloud, it cannot be returned to an observable state. This situation emphasizes the risk of data loss in cloud systems.
- Social Consequences: This incident exposed the vulnerability of data management in cloud systems. Once data enters the system, businesses or individual users have limited control over it. Such technical failures could undermine user trust in cloud services and cause significant financial and reputational damage to businesses.

2.2 Microsoft Azure – Credential Phishing Campaign (2024)

- Case description:2024Year,Microsoft AzureThe platform suffered a phishing attack that compromised hundreds of high-level management accounts. The attackers used credential phishing techniques to gain unauthorized access, exposing a large amount of sensitive data.
- Comparison to the Black Hole Effect: In this case, information was stolen in a phishing attack. For the enterprise, the flow and use of this data cannot be tracked, which is similar to the "information disappearance" in the black hole effect. The stolen information enters an unreachable network, and the enterprise no longer has control over it.
- Social Consequences: This incident highlights the vulnerability of information controlled by the tech elite, and the threat posed by these attacks to power structures. The attack on senior management accounts demonstrates the security challenges facing centers of power and reveals how technological vulnerabilities can exacerbate information asymmetry.

2.3 Amazon Web Services (AWS) – Twitch Data Leak (2021)

- Case description:2021Year, due toAWSSetup error,TwitchEncountered an incident involving128GBThe incident exposed the huge data exposure risks that could result from misconfiguration.
- Black Hole Effect Comparison: This data leak incident reflects that under improper configuration, data is suddenly exposed from "secure" storage. This is similar to the event horizon in a black hole being breached, and the data suddenly becomes available and can be used by the outside world.
- Social Consequences: This incident highlights the configuration challenges in data security and reminds us that even on large cloud platforms, technical vulnerabilities can pose significant risks to personal privacy and corporate secrets, further exacerbating information asymmetry and data opacity.

2.4 Amazon Web Services (AWS) – SeniorAdvisor Breach (2021)

- Case description:2021Year,AWSConfiguration errorS3Storage barrels cause more than300The personal information of Wan Lao people, including their names and email addresses, was exposed.
- Black Hole Effect Comparison: This case shows how data can be inadvertently exposed from a secure environment. Similar to Hawking radiation in black hole theory, data is no longer contained but overflows uncontrollably.

- Social Consequences: This leak, which affected sensitive personal data belonging to the elderly, exposed the vulnerability of vulnerable groups in society to data management. Such incidents exacerbate digital inequality and further highlight the influence of data control and technological elites on ordinary people.

3.Discussion and Analysis: The Relationship between Information Control and Social Inequality

3.1 Critical Analysis: Technical Challenges

- Technical Challenges of the Black Hole Effect: These cases demonstrate the "black hole effect" of information management in cloud platforms and distributed systems. Once data enters these systems, user control and transparency are severely reduced, effectively entering a sandbox environment controlled by organizations and individuals.
- These technical challenges demonstrate that when data enters a highly centralized or centrally controlled environment, it often becomes unreachable and untraceable, exacerbating the power imbalance between data owners and technology operators.
- Data transparency and technological monopoly: Large-scale cloud platforms control data flows and security measures, limiting the control of ordinary users over their data and potentially leading to the emergence of technological monopolies. When a small number of companies control large amounts of data and monopolize data flows, this further weakens user data ownership and transparency.

3.2 Critical analysis at the social level

- Data inequality and social inequity: The data loss and leaks involved in these cases are not merely technical issues; they also reflect social inequalities in data management. Data control is concentrated in the hands of a small number of technology companies, leaving ordinary users with little control over their data. This leads to information power imbalances and exacerbates social inequality.
- Impact on vulnerable groups:SeniorAdvisorThe data breach in 2018 has exposed the vulnerability of vulnerable groups such as the elderly to data breaches. They may not have sufficient technical capabilities to protect their own data, and such breaches further exacerbate their digital marginalization.

3.3 Information Control and Centralization of Power

- Data monopoly by technology companies: These cases show that technology giants' control over data has concentrated information power in the hands of a few companies. This not only affects information transparency, but also changes the distribution of data ownership, forming an "information elite."
- Policy recommendations and improvement measures: In order to reduce this data asymmetry, transparency measures need to be taken at the technical level, such as using blockchain technology for transmission authentication andlogTracking and quantum keys are used for certificate encryption to improve data traceability, and stricter data privacy protection regulations are introduced at the policy level to ensure users' control over their data.

Chapter 6: Black Hole Information System Model Construction

Information system model based on the black hole information paradox

1.1 Model Target

- Objective: To explain how data monopolies and opacity create "data black holes" in information systems. These "data black holes" continuously absorb public information without transparent feedback, ultimately leading to data untraceability and decision-making non-participation, similar to the black hole effect in physics.

1.2 Model elements

1.Data Inflow**(Data Ingestion**: Data enters the big data platform from the user (similar to matter entering a black hole), and the user's data is absorbed into the system, forming data centralization.

2.Data Ingestion**(Data Absorption)**: Once data enters the system, large companies monopolize it, and the data is like entering a black hole, unable to be observed or controlled by the outside world.

3.Data unrecoverability**(Data Invisibility**: Once data enters the system, external users cannot track the data flow, which represents the untraceability in the "data black hole".

4.Non-participation in decision-making**(Decision Exclusion)**: User data is used by companies to make decisions, but ordinary users cannot participate in or influence these decisions, which exacerbates the concentration of power and social inequality.

1.3 Mathematical Model

SettingsD(t)For a momenttThe amount of crowd data, the data absorption rate of the information system is expressed as:

$$\frac{dD(t)}{dt} = \alpha D(t) - \beta R(t) - \delta D(t)^{\epsilon}$$

- αIndicates the rate at which data enters the system.
- R(t)The amount of data returned to the public.

- βIndicates the rate at which data leaves and reaches the correct user end.→0When data is collected, there is almost no data feedback, similar to the situation of a black hole, where all information is absorbed and cannot be returned to the public.

- δIndicates the rate at which data is released (similar to Hawking radiation).
- ϵThe release of the simulated data accelerates nonlinearly with time as an exponential. This variable release process may be nonlinear because the theory of Hawking radiation shows that the release rate increases as the mass of the black hole decreases.
- There is no absolute correlation between α and β, with β being controlled by the information system manager/builder.
- δThis refers to the data flow related to Shadow Technology, that is, the data outflow rate taken away by other information systems.
- Because there are other information systems outside the information system, there is no absolute relationship between α, β, and δ, and only multiples can be used for related calculations.

This model shows that after data enters the system, under extreme conditions (β→0), most of the data cannot be fed back to the public, and only some of the data is released back to users through "Hawking Radiation".

1.4 Adding the firewall hypothesis to quantum entanglement

- Firewall Hypothesis: The firewall is an analogy for a system that prevents data from being completely monopolized. This is technical protection, such as access control or encryption.
- Quantum entanglement: A synchronization effect between data, similar to quantum entanglement, represents the instantaneous transmission or consistency of data between multiple systems, using physical properties to transmit information across systems (such as the left-right spin pairing of coupled up and down quarks).

The model is updated as follows:

$$\frac{dD(t)}{dt} = \alpha D(t) - \beta R(t) - \delta D(t)^{\epsilon} + F(t) + E(t)$$

in:

- F(t)Represents a firewall effect, where data is partially protected or reflected before entering the system.
- F(t)This is a firewall item, indicating that data is protected or reflected before entering the black hole.
- whenF(t)>0When data is encrypted, it will not completely enter the system. This can be compared to a firewall protecting data from entering a "data black hole."

- A firewall can be:

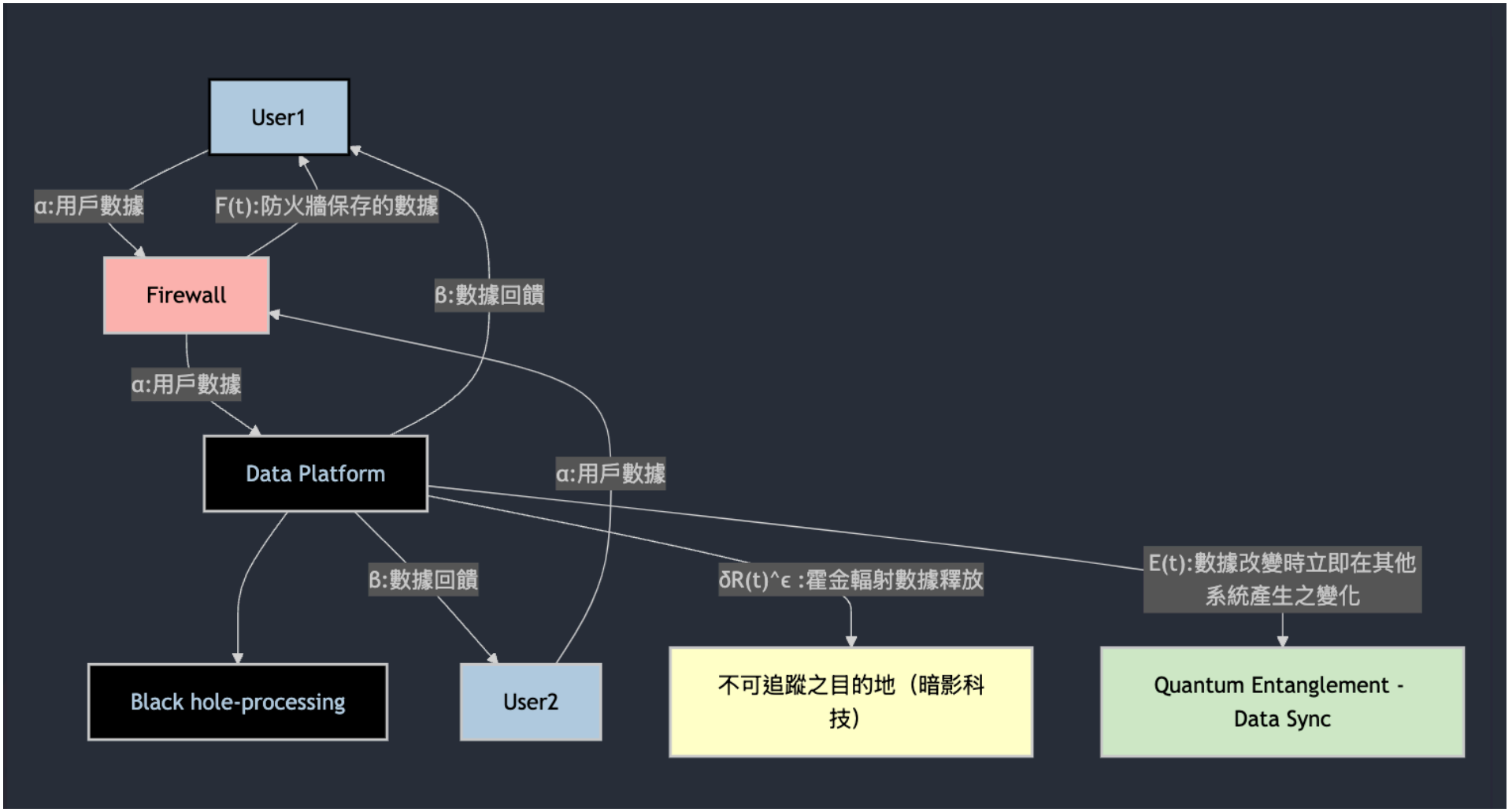
1.Access control system: Only authorized data can enter the deep system, and the rest of the data will be blocked by the "firewall" (i.e.IAM).

2.Encryption technology: Strong encryption is performed before data enters the system to prevent it from entering opaque data systems.

- E(t)It represents the effect of quantum entanglement, where data is instantly synchronized across multiple different information systems.

  That is, if we observe the amount of data absorbed by an information system at a certain moment, the observed amount can be expressed as the amount of data input by users - the amount of data fed back by the system - the amount of data transmitted due to Shadow Technology + the amount of data stored by the firewall mechanism + the amount of data backed up or authenticated by quantum entanglement with other information systems.

1.5 Graph Graphical representation



mermaid markdown code:

```
graph TD;
    A[User1] --α:User Data -->F[Firewall] B[User2] --α:User Data
    -->F[Firewall] F[Firewall] --α:User Data -->C[Data Platform]
    C[Data Platform] --> D[Black hole-processing]
```

```
C[Data Platform] --β:Data Feedback-->A[User1]
C[Data Platform] --β:Data Feedback-->B[User2]
C[Data Platform] --δR(t)^ϵ :Hawking Radiation Data Release -->H[Untraceable Destination (Shadow Technology)]
C[Data Platform] --E(t):Changes to other systems are immediately reflected when data is changed.E[Quantum Entanglement - Data Sync] F[Firewall] --F(t):Data saved by the firewall -->A[User1]
style A fill:#b3cde0,stroke:#000,stroke-width:2px,color:#000 style B fill:#b3cde0,stroke-width:2px,color:#000
style F fill:#fbb4ae,stroke-width:2px,color:#000 style C fill:#000,stroke-width:2px,color:#b3cde0 style D fill:#000,stroke-width:2px,color:#b3cde0 style E fill:#ccebc5,stroke-width:2px,color:#000 style H fill:#ffffcc,stroke-width:2px,color:#000
```

Data simulation and analysis results

Data transmission simulation using quantum encryption technology

In this study, we usedPythonandQuTiPWe conducted data simulations using quantum encryption technology, taking into account multiple variables such as distance, packet size, noise level, environmental factors, and network congestion. These variables can affect data loss rates and provide more specific scenarios to verify the effectiveness of quantum encryption technology under different conditions.

Simulation parameters and scene settings

We designed six different scenarios to simulate data loss:

1.The smaller the packet, the higher the loss rate

2.The shorter the distance, the higher the loss rate

3.The smaller the packet and the shorter the distance, the higher the loss rate.

4.The smaller the packet, the greater the distance, and the higher the loss rate.

5.The larger the packet, the shorter the distance, and the higher the loss rate.

6.The larger the packet, the longer the distance, and the higher the loss rate.

The simulation results show the interaction between packet size, distance, and noise level on the data loss rate, as shown in the figure.

Data loss simulation results

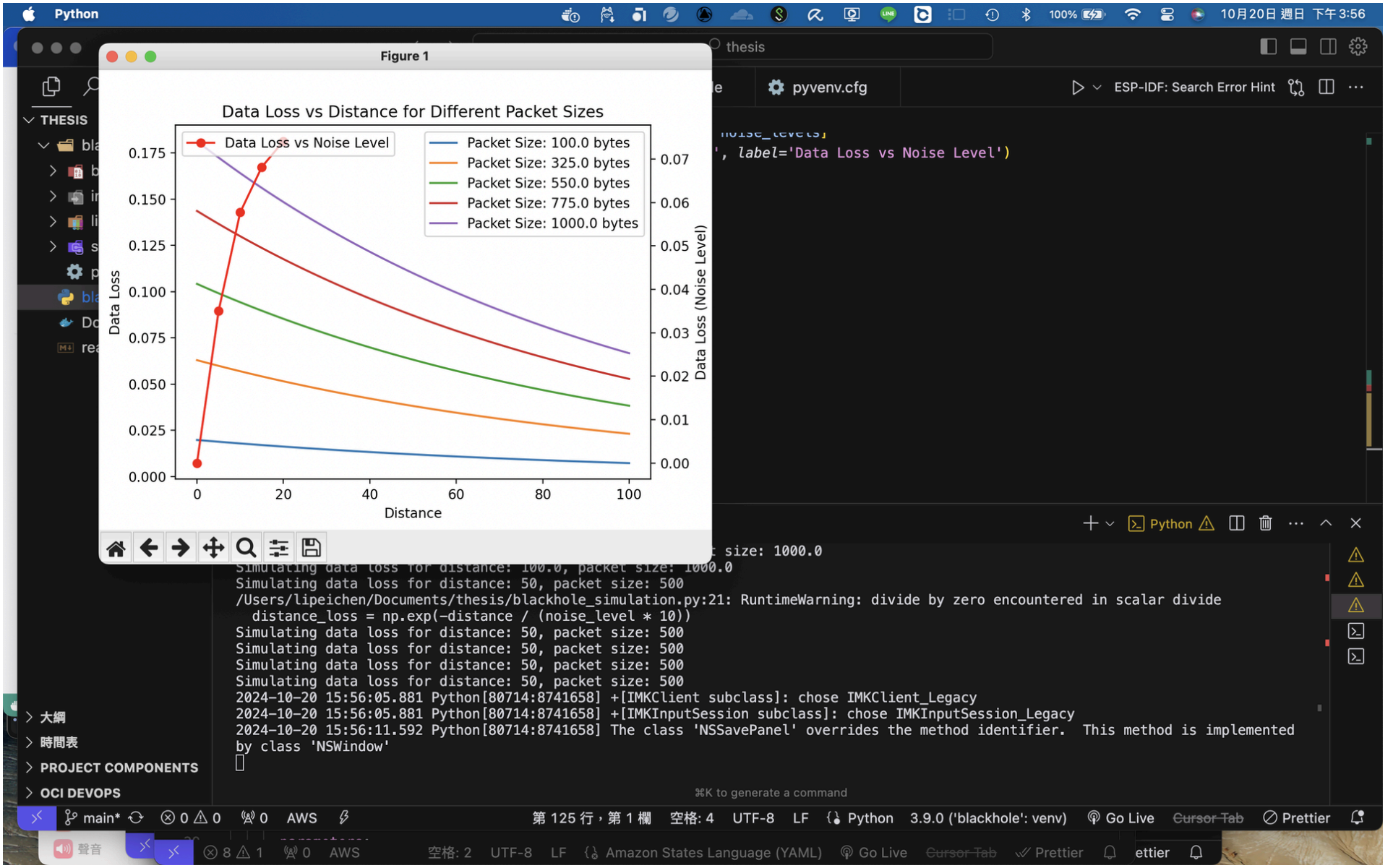
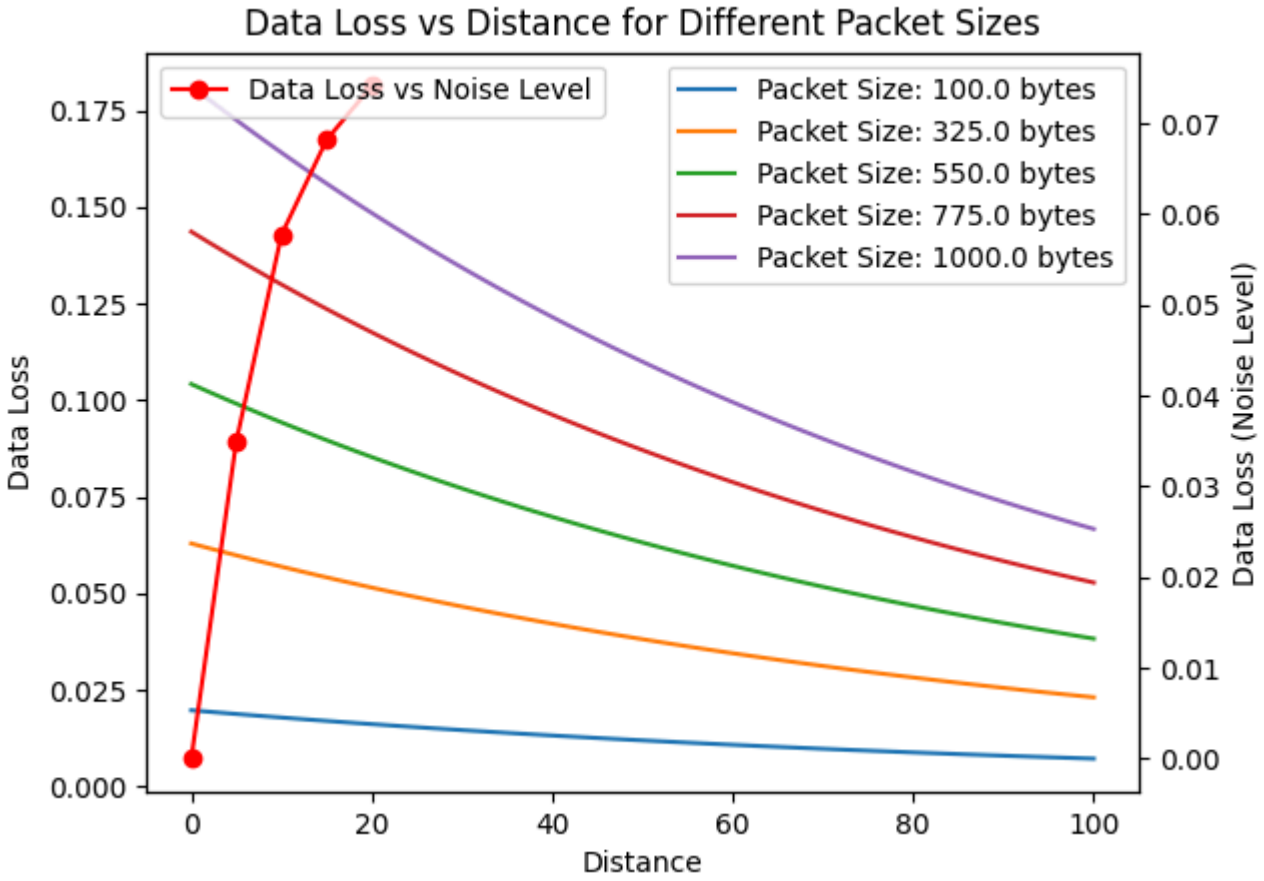


Figure 1
Data Loss vs Distance for Different Packet Sizes
Data Loss vs Noise Level
Packet Size: 100.0 bytes
Packet Size: 325.0 bytes
Packet Size: 550.0 bytes
Packet Size: 775.0 bytes
Packet Size: 1000.0 bytes
Data Loss
Data Loss (Noise Level)
Distance
0.175
0.150
0.125
0.100
0.075
0.050
0.025
0.000
0.07
0.06
0.05
0.04
0.03
0.02
0.01
0.00
0
20
40
60
80
100
thesis
pyvenv.cfg
ESP-IDF: Search Error Hint
', label='Data Loss vs Noise Level')
Python
size: 1000.0
Simulating data loss for distance: 50, packet size: 500
/Users/lipeichen/Documents/thesis/blackhole_simulation.py:21: RuntimeWarning: divide by zero encountered in scalar divide
distance_loss = np.exp(-distance / (noise_level * 10))
Simulating data loss for distance: 50, packet size: 500
Simulating data loss for distance: 50, packet size: 500
Simulating data loss for distance: 50, packet size: 500
Simulating data loss for distance: 50, packet size: 500
2024-10-20 15:56:05.881 Python[80714:8741658] +[IMKClient subclass]: chose IMKClient_Legacy
2024-10-20 15:56:05.881 Python[80714:8741658] +[IMKInputSession subclass]: chose IMKInputSession_Legacy
2024-10-20 15:56:11.592 Python[80714:8741658] The class 'NSSavePanel' overrides the method identifier. This method is implemented by class 'NSWindow'
THESIS
大綱
時間表
PROJECT COMPONENTS
OCI DEVOPS
⌘K to generate a command
main*
AWS
第 125 行，第 1 欄
空格: 4
UTF-8
LF
Python
3.9.0 ('blackhole': venv)
Go Live
Cursor Tab
Prettier
空格: 2
Amazon States Language (YAML)
10月20日 週日 下午 3:56



The right-hand parameter area displays data loss for packets of different sizes at different distances. We can see that the data loss rate increases significantly with increasing packet size and distance. This indicates that data integrity is more susceptible to damage when transmission distances are longer or packets are larger.

The parameter area on the left shows the impact of noise level on data loss. As the noise level increases, the data loss rate also increases significantly. This verifies that physical interference and noise significantly affect data transmission quality, especially in high-noise environments, where data loss rates become extremely high.

code:

Python

```
#1importQuTiPTo simulate quantum
entanglement fromqutipimport*
importnumpyasnp
importmatplotlib.pyplotasplt

#  Initialize "a" quantum entanglement: (2,x)of2Representation2A complex set of data, namely (x,0)⊗(x,1)of0,1Indicates the coupling pairwiseness (i.e. set toaThe data is1rulesbThe data is0,vice versa) bell_state=(tensor(basis(2,0),basis(2,1))+tensor(basis(2,1),basis(2,0))).unit()

#  Print to confirm (measure)
quantum state print("Initial Bell
state:") print(bell_state)


defsimulate_data_loss(distance,noise_level,packet_size,environment_factor=1.0,congestion_factor=1.0):
    """
    Simulate data loss rate, taking into account distance, noise (physical layer effects: such as cable material, resistance,empinterference, voltage stability, etc.) and the impact of packet size. """

    print(f"Simulating data loss for distance:{distance}, packet size:{packet_size}")

    #  Assuming distance has little effect
    distance_loss=np.exp(-distance/(noise_level*10))

    #  Assuming packet size has little effect
    packet_loss=1-np.exp(-packet_size/5000)

    #  Impact of environmental factors
    environment_loss=environment_factor

    #  Impact of network congestion
    congestion_loss=congestion_factor
```

```
    # The total loss rate takes into account the impact of all factors
    total_loss=distance_loss*packet_loss*environment_loss*congestion_loss returntotal_loss


# Scenario1: The smaller the packet, the higher the loss rate
defsimulate_data_loss_small_packet(distance,noise_level,packet_size,environment_factor=1.0, congestion_factor=1.0):

    packet_loss=np.exp(-packet_size/5000)
    # The rest of the function is the same as the original one.
    # . . .

# Scenario2: The shorter the distance, the higher the loss rate
defsimulate_data_loss_short_distance(distance,noise_level,packet_size,environment_factor=1.0, congestion_factor=1.0):

    distance_loss=1-np.exp(-1/(distance+1))
    # The rest of the function is the same as the original one.
    # . . .

# Scenario3: The smaller the packet and the shorter the distance, the higher the loss rate
defsimulate_data_loss_small_packet_short_distance(distance,noise_level,packet_size,environment_factor=1.0, congestion_factor=1.0):

    # The smaller the packet, the shorter the distance, and the higher the loss rate.
    packet_loss=np.exp(-packet_size/5000) distance_loss=1-np.exp
    (-1/(distance+1)) noise_loss=np.exp(-noise_level/10)

    total_loss=packet_loss*distance_loss*noise_loss*environment_factor*congestion_factor returntotal_loss


# Scenario4: The smaller the packet, the greater the distance, and the higher the loss rate
defsimulate_data_loss_small_packet_long_distance(distance,noise_level,packet_size,environment_factor=1.0, congestion_factor=1.0):
```

```
    # The smaller the packet, the greater the distance, and the higher the loss rate.
    packet_loss=np.exp(-packet_size/5000) distance_loss=
    np.exp(-distance/100) noise_loss=np.exp(-noise_level/
    10)
    total_loss=packet_loss*distance_loss*noise_loss*environment_factor*congestion_factor returntotal_loss


# Scenario5: The larger the packet, the shorter the distance, and the higher the loss rate
defsimulate_data_loss_large_packet_short_distance(distance,noise_level,packet_size,environment_factor=1.0, congestion_factor=1.0):

    # The larger the packet, the shorter the distance, and the higher the loss rate.
    packet_loss=1-np.exp(-packet_size/5000) distance_loss=1-np.
    exp(-1/(distance+1)) noise_loss=np.exp(-noise_level/10)

    total_loss=packet_loss*distance_loss*noise_loss*environment_factor*congestion_factor returntotal_loss




# Scenario6: The larger the packet, the longer the distance, and the higher the loss rate (original assumption)
defsimulate_data_loss_large_packet_long_distance(distance,noise_level,packet_size,environment_factor=1.0, congestion_factor=1.0):

    # This scenario is the same as the original function
    returnsimulate_data_loss(distance,noise_level,packet_size,environment_factor,congestion_factor)

# Simulate data loss at different distances and packet sizes
print("Starting data loss simulation...") distances=np.
linspace(0,100,50) packet_sizes=np.linspace(100,1000,
5)                                          # Packets of different sizes

# Set differentnoise_levelvalue
noise_levels=np.linspace(0,20,5)#For example, from0arrive20, divided into5Different values
```

```
# Create a graph and subgraph
fig,ax1=plt.subplots()

# Drawing Differentlypacket_sizeData loss
curve under forpacket_sizeinpacket_sizes:
    losses=[simulate_data_loss(d,10,packet_size)fordindistances] ax1.plot(distances,losses,label=
    f'Packet Size:{packet_size}bytes')

# Set the label and title of the first subplot
ax1.set_xlabel('Distance') ax1.
set_ylabel('Data Loss')
ax1.set_title('Data Loss vs Distance for Different Packet Sizes') ax1.legend(loc='upper
right')

# Create a second subgraph sharexaxis
ax2=ax1.twinx()

# Drawing Differentlynoise_levelData loss curve under
losses=[simulate_data_loss(50,nl,500)fornlinnoise_levels]
ax2.plot(noise_levels,losses,marker='o',color='r',label='Data Loss vs Noise Level')

# Set the label of the second subimage
ax2.set_ylabel('Data Loss (Noise Level)') ax2.legend(loc
='upper left')

# Display graphics
plt.show()
```

Githubas well as**docker image**Link:

https://github.com/dennislee928/thesis

Chapter 7

7.1 Future research directions

- Development of quantum computing technology and its practical applications and data transparency: Explore quantum encryption technology (such as quantum key distributionQKDAnd how quantum entanglement and post-quantum cryptography (such as physical encryption) can improve data transparency and prevent data from being absorbed without restrictions by monopolies.
- These technologies may address the data black hole effect by ensuring data transparency and feedback through a greater number of data tracking and protection technologies.
- Applying blockchain technology to data decentralization: A deeper exploration of how blockchain technology can improve the availability of data through decentralization and avoid quantum computing technology to achieve quantum hegemony (quantum advantage) brute force attack on blockchain applications (brute-force attack).
- Data management can be distributed to multiple nodes of different units or organizations (node), reduce monopoly phenomena, and thus prevent, stop, and mitigate the risks of data leakage, misuse, and dissipation.

- Data Rights Laws and Policies Research: Further research is needed on how to regulate data monopolies through policy and protect individual data ownership. Privacy protection laws and data feedback mechanisms should be strengthened to safeguard the public's rights in data management. Technical shortcomings should also be addressed through changes to the education system and regulations.

2.2 Practical Suggestions

- Technical aspects:
    - Use quantum computers for quantum-level encryption to enhance the transparency and traceability of data management systems.
    - Use smart contract technology to ensure the transparency of data flow.
    - Build a national-level private cloud system and infrastructure (including a reliable power source) and set upload balancing、total shut down backup plan、rollup planwait.
- Policy level:
    - For blockchain management,AI Governance, quantum computing management and other emerging fields, and establish special laws in the fields of education, commerce, and administration.

- Promote the "data user right to know" law to protect users' right to know the flow and use of their data and prevent the occurrence of information black hole effect.