Столыпинский вестник

Научная статья

Original article

УДК 003.26

APPLICATION OF CRYPTOGRAPHIC TECHNOLOGIES FOR INFORMATION PROTECTION IN CLOUD SERVICES

ПРИМЕНЕНИЕ КРИПТОГРАФИЧЕСКИХ ТЕХНОЛОГИЙ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ В ОБЛАЧНЫХ СЕРВИСАХ

Tiumentsev Denis, spesialist, East Siberian State University of Technology and Management (ESSUTM) (670013, Ulan-Ude, st. Klyuchevskaya, 40v), tel. 8(985) 888-72-55, ORCID: http://orcid.org/0009-0003-5275-3223, tyumencev_dv@rambler.ru

Тюменцев Денис, специалист, Восточно-Сибирский государственный университет технологий и управления (ВСГУТМ) (670013, г. Улан-Удэ, ул. Ключевская, 40в), тел. 8(985) 888-72-55, ORCID: http://orcid.org/0009-0003-5275-3223, tyumencev_dv@rambler.ru

Abstract. The article discusses the application of cryptographic technologies for information protection in cloud services. It explores the fundamentals and principles of cryptography, such as authentication, confidentiality, and integrity. The experiences of leading companies in cloud services, including AWS, Microsoft, Google, and Alibaba, are covered. Advantages and disadvantages of using specific cryptographic technologies are analyzed. The article emphasizes the significance of integrating cryptographic technologies into cloud systems to ensure information security.

Аннотация. В статье рассматривается применение криптографических технологий для защиты информации в облачных сервисах. В нем исследуются основы и принципы криптографии, такие как аутентификация, конфиденциальность и целостность. Освещается опыт ведущих компаний облачных сервисов, включая AWS, Microsoft, Google и Alibaba. Анализируются преимущества и недостатки использования конкретных криптографических технологий. В статье подчеркивается значимость интеграции криптографических технологий в облачные системы для обеспечения информационной безопасности.

Keywords: cryptography, cloud services, information security, authentication, confidentiality, technology integration.

Ключевые слова: криптография, облачные сервисы, информационная безопасность, аутентификация, конфиденциальность, интеграция технологий.

Introduction

The emergence of cloud computing as a network access model has revolutionized the methods of data storage and processing. In the digital era, where data leakage and cyber threats are becoming increasingly common, the protection of confidential information in cloud services (CS) has emerged as a paramount issue. According to a report by Hava (Melbourne, Australia), 98 % of companies worldwide are utilizing CS. It is expected that user spending on cloud storage will grow to $678.8 billion in 2024 [1].

The purpose of this research is to analyze and evaluate the role of cryptographic technologies (CT) in enhancing the security of information in CS.

Main Body

CS are a broad range of services delivered over the internet, providing users with various capabilities like data storage, server access, and software applications. These services enable businesses and individuals to use computing resources hosted by third parties, eliminating the need for local hardware and infrastructure management [2]. The imperative to safeguard information within CS has become increasingly critical in an

era where digital data represents a pivotal asset in both the commercial and personal realms.

According to the IBM Data Breach Report, as of 2023, 45 % of all data breaches are related to cloud environments. A significant number of companies, about 80 %, have experienced at least one CS incident in the past year [3]. This trend underscores the need for robust protective measures. CT encompass a suite of sophisticated methodologies and algorithms designed to secure information by transforming it into an unreadable format for unauthorized users.

Fundamentals of cryptography

The principles of cryptography are based on the mechanism of transforming information to protect it from unauthorized access [4].Confidentiality in cryptography is achieved through encryption, which converts the original readable data (plaintext) into an unreadable format (ciphertext). Integrity is maintained through cryptographic hashing and digital signatures. Hash functions generate a unique digital fingerprint of data, enabling the detection of any changes or tampering. Digital signatures authenticate that a message or document has not been altered since it was signed. Cryptography achieves authentication also through public key infrastructure (PKI). PKI involves the use of digital certificates, which are issued by trusted persons.

In the realm of modern cryptographic algorithms, a distinction is typically drawn between symmetric and asymmetric key algorithms, each catering to specific security needs within digital communications. Symmetric key algorithms, such as the Advanced Encryption Standard (AES), utilize a single key for both encryption and decryption processes. The advantage of AES lies in its simplicity and speed, making it suitable for encrypting large volumes of data. Asymmetric key algorithms, exemplified by RSA (Rivest-Shamir-Adleman) and ECC (Elliptic Curve Cryptography), operate using a pair of keys – a public key for encryption and a private key for decryption. These algorithms are foundational in secure data transmission, especially in scenarios where data needs to be securely shared over untrusted networks, such as the Internet.

Cryptography in CS

According to Statista (Hamburg, Germany), the top cloud security concerns are data loss and leakage (69 %), and data privacy/confidentiality (66 %), followed by accidental exposure of credentials (44 %). In the domain of CS, cryptography is an important component for ensuring data security and privacy [5]. CS providers implement CT to safeguard data at rest, in transit, and during processing. As of 2024, the leaders in the cloud storage market are Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (figure 1).

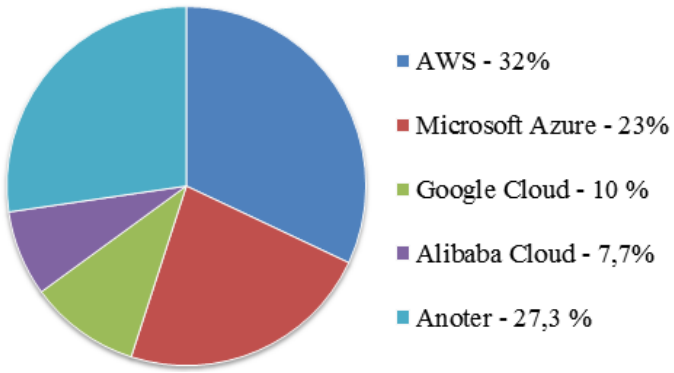

Figure 1 – World leaders in cloud technology market, report by Hava, % [1]

These companies have established themselves as key players, significantly influencing the market dynamics and setting trends in cloud storage solutions globally. For instance, Amazon Web Services (AWS) utilizes server-side encryption to protect data stored in its storage service. This encryption involves automatically encrypting the data as it is written to storage and decrypting it when accessed.

Similarly, Google Cloud Platform offers various encryption options for data at rest, including customer-managed encryption keys, allowing users greater control over their data security.

Another aspect of cryptography in cloud services is the use of TLS/SSL (Transport Layer Security/ Secure Sockets Layer) protocols for data in transit. Microsoft Azure, for instance, employs these protocols to secure data as it moves between Azure services and clients. This ensures that sensitive information remains protected from potential interception during transmission. Additionally, Azure provides Azure Key Vault, a tool to manage cryptographic keys used in its cloud applications and services.

Some providers, such as IBM, are implementing advanced cryptographic methods like homomorphic encryption. This technology allows for computations on encrypted data without the need for decryption. Such innovative methods highlight the evolution of CT in the rapidly developing cloud services market. Table 1 presents the advantages and challenges of applying cryptographic technologies for information protection in cloud services.

Table 1 – Cryptographic technology application in CS.

CT/ Application in CS	**Purpose/Function**	**Benefits**	**Challenges**
Symmetric Encryption (e.g., AES)/ Data Encryption at Rest.	Encrypts stored data on cloud servers to protect it from unauthorized access.	Fast processing, suitable for large data.	Key management and distribution can be complex/
Asymmetric Encryption (e.g., RSA, ECC)/ Secure Data Transmission.	Encrypts data during transmission between client and cloud services to prevent interception.	Strong security.	Slower than symmetric encryption.
Hash Functions (e.g., SHA-256)/ Data Integrity Verification	Ensures that data has not been tampered with during transmission or storage by generating a unique hash value.	Fast computation, non-reversible.	Requires constant updates to ensure security.
Digital Signatures/User Authentication and Non-repudiation	Verifies the identity of the sender and ensures that the message has not been altered.	Authenticates source, verifies integrity	Relies on secure key management and public key infrastructure
Homomorphic Encryption/Secure Data Processing	Allows computation on data in the cloud, generating an encrypted result that matches operations on plaintext.	Preserves privacy of sensitive data.	Computationally intensive.

This detailed table offers an extensive insight into the cryptographic technologies used in cloud services. Each technology plays an important role in ensuring the security and privacy of data in cloud environments, addressing specific security.

Challenges and Limitation. Cryptographic systems possess a complex mechanism for managing access keys. Violating key management protocols can lead to vulnerabilities in the security system. Additionally, the rapidly changing nature of cyber threats demands constant updating and adaptation of cryptographic methods [6]. Adhering to compliance standards and ensuring interoperability across various

platforms create additional levels of complexity. These issues underscore the necessity of continuous research in this area to enhance the effectiveness of CT in CS.

Promising trends and innovations in cryptographic information security technologies in cloud services

The realm of CT in CS is witnessing significant advancements, particularly in the context of quantum cryptography and adaptation to new threats and challenges. Quantum cryptography leverages the principles of quantum mechanics to secure data, offering theoretically unbreakable encryption. This technology is particularly relevant in the era of quantum computing, where traditional cryptographic methods may become vulnerable.

Adaptation to new threats in cloud technologies is another critical area of innovation. With the increasing sophistication of cyber-attacks, cryptographic methods need constant evolution to stay ahead of potential vulnerabilities [7]. This involves developing more advanced encryption algorithms, enhancing key management strategies, and integrating AI for predictive threat analysis. AI and machine learning are increasingly being used to detect and respond to security incidents more swiftly, thereby fortifying cloud security.

Additionally, the integration of cryptographic methods with emerging cloud technologies like edge computing is a developing trend. These technologies present unique security challenges, necessitating specialized cryptographic solutions. For instance, edge computing requires robust encryption and authentication protocols that can operate efficiently in decentralized and often resource-constrained environments. Innovations in lightweight cryptography and multi-party computation are being explored to meet these needs, ensuring secure data processing and storage in diverse cloud environments.

These advancements highlight a continuous trajectory towards more secure, efficient, and adaptable cryptographic technologies, crucial for safeguarding the ever-expanding realm of cloud services.

Conclusion

CT in CS are essential in the ever-evolving digital era, safeguarding data against increasing cyber threats. This research underscores the integration of advanced cryptographic methods by leading CS providers like AWS, Microsoft Azure and Google Cloud Platform.

Innovative cryptographic solutions, particularly quantum cryptography and adaptive strategies for new threats, are central to future developments in this field. This study emphasizes the need for continuous evolution in CT to align with the rapid advancements in CS. As the digital landscape transforms, so must the cryptographic strategies, ensuring effective protection and maintaining the integrity of data in cloud infrastructures.

References

1. Cloud market share analysis: decoding industry leaders and trends URL: https://www.hava.io/blog/2024-cloud-market-share-analysis-decoding-industry-leaders-and-trends (date of application: 26.02.2024).
2. Шайхулов Э.А. ANALYSIS OF THE IMPACT OF MANUAL TESTING ON THE ECONOMIC EFFICIENCY OF IT PROJECTS IN THE USA// Proceedings of the XXXII International Multidisciplinary Conference «Prospects and Key Tendencies of Science in Contemporary World». Bubok Publishing S.L., Madrid, Spain. 2023.
3. Cost of a Data Breach Report 2023 URL: https://www.ibm.com/reports/data-breach (date of application: 06.02.2024).
4. Israfilov A. COVID-19 AND ITS CYBERSECURITY IMPLICATIONS: FROM THREAT ESCALATION TO STRATEGIC RESPONSE // Вестник науки №12 (69) том 4. С. 1087 - 1093. 2023 г. ISSN 2712-8849
5. Size of the cloud storage market worldwide from 2022 to 2030 URL: https://www.statista.com/statistics/1322710/global-cloud-storage-market-size/ (date of application: 26.02.2024).
6. Konstantinov D.S. INTEGRATION OF ENERGY-EFFICIENT TECHNOLOGIES IN REFRIGERATION SYSTEMS: REDUCING COST AND

ENVIRONMENTAL IMPACT// Proceedings of the XXXVIII International Multidisciplinary Conference «Innovations and Tendencies of State-of-Art Science». Mijnbestseller Nederland, Rotterdam, Nederland. 2023.

7. L R Abdullina et al (2022) Calculation of the carbon footprint of industrial hybrid solar - wind turbines // IOP Conference Series: Earth and Environmental Science, Volume 981, Russia

Литература

1. Анализ доли рынка облачных технологий: расшифровка лидеров и тенденций отрасли. URL: https://www.hava.io/blog/2024-cloud-market-share-anaанализ-decoding-industry-leaders-and-trends (дата подачи заявки: 26.02.2024).
2. Шайхулов Э.А. АНАЛИЗ ВЛИЯНИЯ РУЧНОГО ТЕСТИРОВАНИЯ НА ЭКОНОМИЧЕСКУЮ ЭФФЕКТИВНОСТЬ ИТ-ПРОЕКТОВ В США // Материалы XXXII Международной мультидисциплинарной конференции «Перспективы и ключевые тенденции науки в современном мире». Bubok Publishing S.L., Мадрид, Испания. 2023.
3. Стоимость Отчета об утечке данных 2023 URL: https://www.ibm.com/reports/data-breach (дата подачи заявки: 06.02.2024).
4. Исрафилов А. COVID-19 И ЕГО ПОСЛЕДСТВИЯ ДЛЯ КИБЕРБЕЗОПАСНОСТИ: ОТ ЭСКАЛАЦИИ УГРОЗЫ К СТРАТЕГИЧЕСКОМУ ОТВЕТСТВУ // Вестник науки №12 (69) том 4. С. 1087 - 1093. 2023 г. ISSN 2712-8849
5. Объем мирового рынка облачных хранилищ с 2022 по 2030 год. URL: https://www.statista.com/statistics/1322710/global-cloud-storage-market-size/ (дата подачи заявки: 26.02.2024).
6. Константинов Д.С. ИНТЕГРАЦИЯ ЭНЕРГОЭФФЕКТИВНЫХ ТЕХНОЛОГИЙ В ХОЛОДИЛЬНЫЕ СИСТЕМЫ: СНИЖЕНИЕ ЗАТРАТ И ЭКОЛОГИЧЕСКОЕ ВОЗДЕЙСТВИЕ//Материалы XXXVIII Международной многопрофильной конференции «Инновации и тенденции современной науки». Mijnbestseller Nederland, Роттердам, Нидерланды. 2023.

7. Л.Р. Абдуллина и др. (2022) Расчет углеродного следа промышленных гибридных солнечно-ветряных турбин // Серия конференций IOP: Науки о Земле и окружающей среде, Том 981, Россия

Для цитирования: Тюменцев Д. Application of cryptographic technologies for information protection in cloud services//*Научный сетевой журнал «Столыпинский вестник» №3/2024.*