ingegneria sismica
International Journal of Earthquake Engineering
Anno XLIII - Num. 2 - 2026

Cloud Computing Technology Empowers Security Management Mechanisms for Enterprise Accounting Systems

Xiaorong Shi[1,*]

[1] School of Economics and Management, Anyang Vocational and Technical College, Anyang, Henan, 455000, China

SUMMARY: *The time of big data and progress in cloud calculation have put forward new requirements to company financial accounting. This research has constructed a cloud-based dispersible financial counting system which uses a service-oriented structure (SOA). Through the introduction of chaos theory, and through its combination with DES and RSA, a chaotic mixed encryption algorithm has been put forward for the building of a safety mechanism. The analysis of safety indicates that the Lena image gives a chi-square value of 255.5 at the 0.05 significance level, which is under the expected value, therefore it proves that the algorithm we put forward has high attack resistance ability. In actual application, the system greatly promotes financial accounting work efficiency for small and medium enterprises, lowers manpower costs, speeds up data processing work, and cuts down mistake occurrences.*

KEYWORDS: *calculation technology in cloud; Encryption arithmetic method; chaos academic theory; enterprises' finance calculation account system Introductory Section*

1 Introduction

The progress of global economy and technology brings challenges and chances, hence it puts forward higher demands for the financial accounting work of enterprises[1]. Business enterprises are the foundation that supports a country's development, hence their accounting work efficiency directly has influence on resource distribution. In the digital time, technologies which include big data, cloud computing and AI give new tools, ideas and modes for accounting work[2, 3]. As a computing innovation of internet age, cloud computing constructs independent virtual environments which integrate computing, storage and information resources, therefore delivers customized, flexible and elastic financial services with high efficiency[5, 6].

Cloud computation can effectively carry out optimization for enterprise financial management, hence promote work efficiency[7]. Nguyen Phu and other researchers discovered that cloud accounting can promote financial management work and solve the problems of security, privacy and compliance[8]. Tsai and other researchers put forward a cloud-based dynamic system for invasion examination, which verifies that it possesses strong capability of safety examination[9]. Through the utilization of mixed-type analysis, Ionescu and other researchers have thus proven that large-scale data and cloud calculation exert positive influences on the production efficiency of business enterprises[10]. Furthermore, the integration of cloud computing can strengthen financial risk management through enhancing calculation ability for high-efficiency risk control[11, 12]. Nagarajan has carried out an evaluation on the security and keeping-secrecy of cloud calculation in bank and financial

*shixiaorong2025@163.com
https://doi.org/10.65102/is2026623
Published: 30 April, 2026

account keeping. This research discovered that cloud-based risk check measures provide bigger expandability and quicker handling velocities, effectively finding possible dangers like data breaking and not-permitted entering[13]. In the age of big data, the wide spread use of cloud calculation and artificial intelligence in all social fields is thus changing enterprise finance management ideas. The usage of cloud computing technique in enterprise finance has promoted the energetic growth of financial informationization[14].

The current paper has developed a cloud - based distributed architecture founded on Service - Oriented Architecture (SOA). This architecture integrates existing platforms and cloud services to achieve unified management, distribution, and oversight of hardware, software, and data resources. As a result, it facilitates real - time sharing and synchronization of financial data.Through an analysis of the Data Encryption Standard (DES) and the Rivest–Shamir–Adleman (RSA) algorithm, this study proposes a chaotic hybrid encryption algorithm (CDR). By incorporating chaos theory, this algorithm aims to ensure data security. It generates chaotic sequences using the Tent mapping to create and optimize encryption keys, and then combines DES and RSA.Experiments conducted on a Hadoop cluster have confirmed that this algorithm offers both security and efficiency. Additionally, a survey involving 400 small and medium - sized enterprises assesses the system's performance in processing financial data and generating reports.

2 Cloud-Based Enterprise Accounting System

2.1 Cloud Computing

2.1.1 Fundamental Characteristics of Cloud Computing

Cloud calculation is a pattern that provides need-based, adjustable computing resources through the Internet by a simple, pay-when-you-use pattern[15]. Providers of service can quickly prepare and put out resources with very little management or mutual interaction. The core natures of cloud computation include:

(1) On-demand type service: Consumers dynamically get calculation resources according to their own needs, thus eliminating direct or indirect mutual interaction with cloud service providing suppliers.

(2) Wide Network Reach: Cloud computation provides service abilities through networks, which supports the accessing from many kinds of clients by means of many kinds of standard network connection ports.

(3) Multi-Tenancy and Resource Sharing: Cloud providers utilize multi-tenant models to serve vast user bases. Resources—including compute, storage, and networking—can be dynamically allocated or reallocated to meet user demands for physical or virtual resources. Users remain unaware of resource location and allocation.

(4) Rapid Elasticity: Cloud computing services can be rapidly provisioned or released. Their available capabilities appear limitless to users, with purchasing unrestricted by time or location.

(5) Service Metricability: Cloud computing utilizes metering capabilities to automatically manage and optimize resource utilization. By monitoring and managing resource usage, it provides greater transparency between service providers and consumers.

2.1.2 Cloud Computing Deployment Models

Cloud computing consists of four distinct deployment models, namely the private cloud, the community cloud, the public cloud, and the hybrid cloud.

(1) Private Cloud

The cloud infrastructure is managed by an enterprise or a third party, primarily located within or outside the enterprise network. Resources are dedicated for internal enterprise use.

(2) Community Cloud

Multiple entities offer the cloud infrastructure, and these entities collaboratively oversee the platform. Cloud computing services are pooled to address shared requirements, including tasks, security prerequisites, policies, and regulatory stipulations.

(3) Public Cloud

Infrastructure is typically provided by large operational organizations or IT companies possessing extensive computing resources. These entities sell computing power on a shared basis to individuals, small businesses, and organizations through a "pay-as-you-go" model.

(4) Hybrid Cloud

A cloud infrastructure composed of two or more clouds (public, private, or community). Specialized technologies or standards integrate them into a unified system for efficient operation. Each component cloud remains independent, while data and applications must maintain portability.

2.1.3 Cloud Computing Service Models

Cloud computing, akin to other computing environments, comprises hardware, application software tiers, and system levels. It mainly presents three service paradigms: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). The correlation among these cloud service models is depicted in Figure 1.

(1) Infrastructure as a Service (IaaS)

IaaS provides cloud users with access to computing, storage, networking, and other resources as services. Users can deploy their required operating systems, storage capacity, and applications using the infrastructure APIs provided by the cloud service provider. Additionally, users can flexibly configure network and security components on demand.

(2) Platform as a Service (PaaS)

PaaS bridges infrastructure and applications, providing programming interfaces and application development capabilities for executable code in internet environments. Users only need to configure their application environment and deploy it to the cloud, without concerning themselves with the underlying cloud infrastructure. PaaS services primarily encompass end-to-end software development, testing, and deployment, along with specialized software development.

(3) Software as a Service (SaaS)

SaaS delivers application services deployed and operated within cloud computing environments. Users access required or customized cloud applications (e.g., web-based email systems) through clients, browsers, mobile devices, or other terminals. They are exempt from managing underlying cloud infrastructure—such as networks, operating systems, and storage—or configuring application development environments.

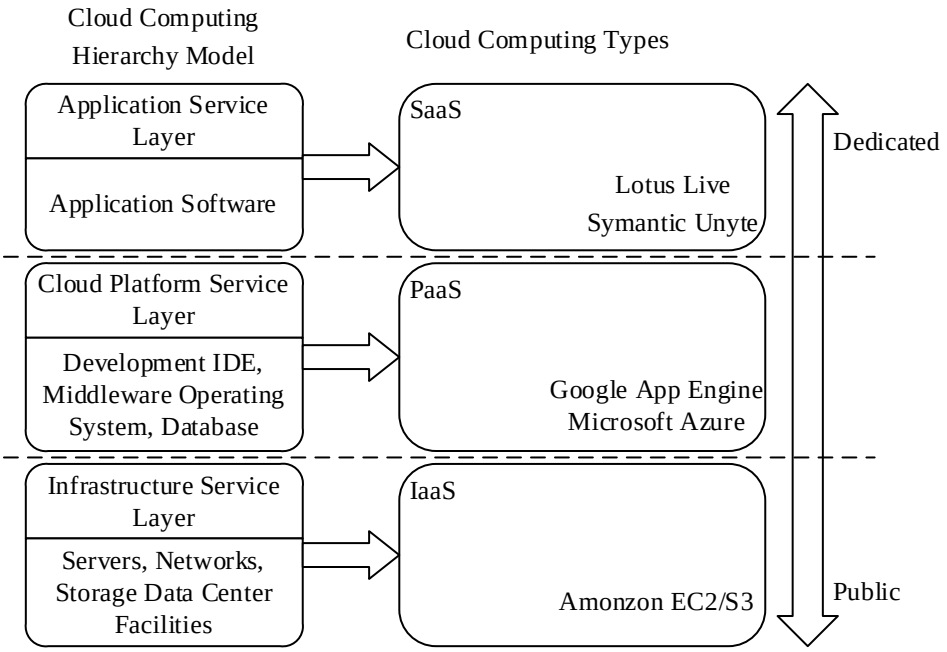


Figure 1: Relationships between cloud service models

2.2 Cloud-Based Enterprise Accounting System Architecture

Based on cloud computing principles and characteristics, this system leverages IT hardware and software resources provided by service providers. Users access resource pools via the internet to obtain required application services. Grounded in a service-oriented architecture, it integrates enterprise financial data resources with services to build a distributed system architecture. This architecture delivers high-speed financial and business processing, cloud-based data access and storage services, and unified communication methods to users.The architecture of the corporate financial accounting system consists of the user level, the software - as - a - service (SaaS) level, the platform - as - a - service (PaaS) level, and the infrastructure - as - a - service (IaaS) level. It combines the existing infrastructure platforms with cloud - based services to attain unified oversight, distribution, implementation, and surveillance of hardware assets, software assets, and data assets. Figure 2 depicts the architecture of the enterprise financial accounting system.

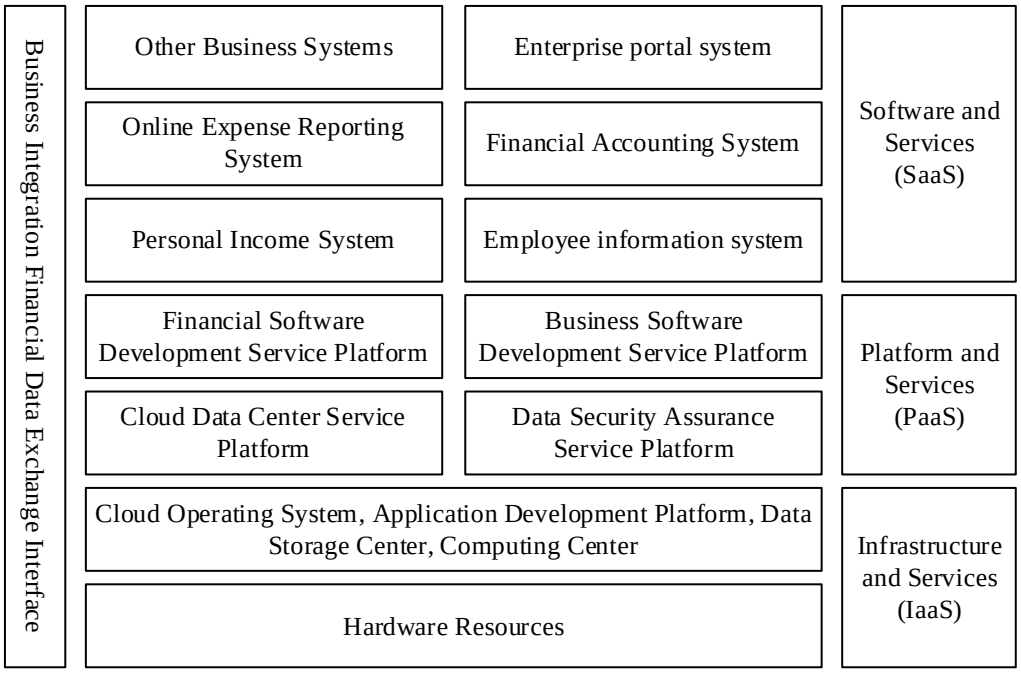


Figure 2: Enterprise accounting system architecture

2.2.1 Infrastructure as a Service (IaaS)

The Infrastructure and Services Layer (IaaS) resides at the foundation of the enterprise financial accounting system architecture, comprising two components: hardware infrastructure and the user service business management platform. The hardware infrastructure integrates hardware resources such as database storage, web application servers, and PC servers.Through using virtualization technology, it puts together storage resources, computing resources, virtual servers, memory resources, network resources, and I/O devices into one unified resource pool. The Consumer Service Business Administration Platform combines cloud operation systems, application exploitation platforms, data depository centers, and calculation centers, dynamically distributing resources according to different consumer demands.

2.2.2 Platform as a Service (PaaS)

The Platform and Service Level (PaaS) acts as the middle layer of the financial accounting system structure. It contains platforms for financial and commercial software development, cloud data center services, and data security guarantee, which forms the basic operation support. This layer can provide basic platform services, it lets users deploy business systems according to their needs, and it gives support to design, development, testing, and hosting work. It promotes the efficiency of development and thus permits the sharing by multiple users.

2.2.3 Software as a Service (SaaS) Layer

The software and services layer can be built on top of IaaS or PaaS, offering high security and scalability while providing highly flexible and reliable support services. It delivers powerful platform application services for enterprise financial accounting systems. By developing new cloud computing applications such as other business systems, online expense reporting systems, personal income systems, financial accounting systems, billing systems, and enterprise portal systems, it delivers more comprehensive and diverse service applications. These include resource cloud, management cloud, analytics cloud, and user cloud services, along with unified

identity authentication and user permission management services, payment settlement services, and more.

Resource Cloud delivers data resource sharing services to employees and business departments through the cloud data service center. The financial demands which are put forward by business departments get handled inside the enterprise accounting system, hence they are given back to operation systems without delay. The financial data which has been generated can be got by management and permitted workers, hence this allows real-time view of finance situations and smooth moving to the next work steps.

The Management Cloud gives out services contain registration management, account management, load management, security management, and service arranging, therefore it guarantees the service platform can offer unified, expandable services toward users.

The Analytic Cloud makes use of data digging and knowledge finding technologies to effectively collect hidden knowledge and moving resources. It on own initiative finds out users' financial demands and information requirements, for the purpose of providing services that have personal characteristics.

The User Cloud can make adaptation for the access devices which are used by both enterprise managers and staff members when they visit the service platform through different terminals.The terminal layer automatically selects access points and provides personalized services tailored to each user.

2.3 System Software Design

2.3.1 Network Information Collection and Security Level Calculation

With the support of hardware equipment, network information is collected. This information gathering is built upon a network information mining engine. The data engine can collect the latest information from various internet websites in the shortest possible time. After classifying and standardizing the format, it promptly publishes the information to individual websites, thereby enhancing timeliness and reducing workload. To ensure standardized data collection and upload, establish network information mapping and collection channels according to the following formula (1).

$$\gamma = \frac{1}{z} \times \sum_{g>1}^{g} z(g) + k \tag{1}$$

In Equation (1), γ represents the network information mapping and collection channel; z denotes the fluctuating value during the information access process; g indicates the network information type; and k signifies the total amount of sampled information. After completing the collection of network information, the data undergoes processing. During this process, the collected information from the internet is first subjected to confidentiality treatment and rapid updates of network operation information. Based on user access requirements, security information is separated. The frequency of remote monitoring is reduced. The security level of network information is calculated based on the network nodes during the sampling process, using the formula shown in Equation (2).

$$\eta = \sqrt{S}\gamma \sum \sum \ln\left[p(a) + p(\phi) \right] \tag{2}$$

In Equation (2), η represents the network information security level; S denotes the amount of information with attack characteristics carried within the network information; p

is the horizontal vector of intrusion signal levels; a indicates the degree of data isolation; and ϕ signifies the density of the data space.

2.3.2 Network Information Security Vulnerability Detection

Building upon the aforementioned content, blockchain technology is introduced to detect network information security vulnerabilities. The detection process leverages blockchain's decentralized nature and block-chain structure to conduct security assessments and vulnerability scans on websites, identifying potential security risks and weaknesses. Within blockchain technology, each data block contains a hash value and timestamp data. This chained kind of structure can guarantee data has very strong ability to resist tampering, hence all data can be collected and checked through Merkle trees, therefore it greatly promotes data completeness and dependability. When we use blockchain technology to carry out network information security leak checking, intelligent contracts can be employed to automatically carry out checking rules, thus allowing overall scanning and evaluation of network stations.

2.3.3 Establishment of Encryption Mechanisms and Network Information Security Management

After completing the aforementioned design, proceed to establish the network information encryption mechanism. During this process, clearly define the types and targets of network information requiring encryption. Simultaneously, select an appropriate encryption algorithm based on the specific characteristics of the encryption targets. Assuming the plaintext data to be encrypted is denoted as U, the encryption process for U is illustrated in formula (3).

$$V(U) = b \bmod \frac{i}{2} + f(P) \tag{3}$$

In Equation (3), V represents the encryption algorithm; i denotes the modulo function applied to the information; f signifies the state of network data information; and P refers to network information security vulnerability detection (network security assessment). Based on this, generate or select an appropriate encryption key to ensure its security and confidentiality. Encrypt the network information requiring protection using the encryption algorithm and key to produce ciphertext. The ciphertext is transmitted to the recipient, who then decrypts it using the identical cryptographic algorithm and key to recover the original message. This approach achieves encrypted processing of network information during transmission and circulation. To standardize security management after decryption, a database can be established for storing network information.

3 Security Management Mechanism for Corporate Accounting and Financial Systems

3.1 Encryption Algorithms

3.1.1 RSA Encryption Algorithm

In contrast to other encryption algorithms, the RSA algorithm utilizes two separate keys: a public key and a private key. Data encrypted with the public key necessitates the corresponding private key for decryption, whereas data encrypted with the private key demands the public key for decryption [16]. Since encryption and decryption utilize different keys, this algorithm is

commonly referred to as an asymmetric encryption algorithm. At present, the RSA algorithm still is the asymmetric encryption method that most widely uses by people. According to the Euler Theorem, its safety depends on the calculation of large integer power operation, and longer bit lengths can bring higher safety degree. This present paper utilizes the RSA encryption arithmetic to produce starting values for one chaotic system.This algorithm allows the ciphertext to be encrypted using the recipient's known public key. Upon receiving the ciphertext, the recipient decrypts it with their private key to obtain the plaintext. Throughout this process, only the recipient can access the private key information.

The encryption steps are as follows:

Step 1: Randomly select two distinct prime numbers, p and q. Calculate the Euler totient function of $n = p*q$ and n, which is $\varphi(n)$, where $\varphi(n) = (p-1)*(q-1)$.

Step 2: Randomly select an integer e such that $1 < e < \varphi(n)$ and $\gcd(\varphi(n), e) = 1$; compute d from the condition $d \cdot e \equiv 1 \bmod \varphi(n)$. The public key is $P = (e, n)$, and the private key is $S = (d, n)$.

Step 3: Randomly select four large integers m_1, m_2, m_3, m_4. Encrypt them using the public key to obtain ciphertexts $c_i = m_i^e \bmod n$ and $i = 1, 2, 3, 4$. To decrypt, the corresponding private key must be used to generate the plaintexts $m_i = c_i^d \bmod n$ and $i = 1, 2, 3, 4$.

Step 4: Equation (4) computes the initial value of the chaotic system by processing both the encrypted ciphertext and the original plaintext.

$$\begin{cases} x_0 = \sqrt{\log(c_1 + m_1)} \\ y_0 = \sqrt{\log(c_2 + m_2)} \\ z_0 = \sqrt{\log(c_3 + m_3)} \\ w_0 = \sqrt{\log(c_4 + m_4)} \end{cases} \tag{4}$$

3.1.2 Chaotic Cryptographic Algorithms

In chaotic cryptography, the higher the dimension of its chaotic mapping structure, the greater its complexity and randomness. Consequently, the resulting pseudorandom sequences become more unpredictable, and the security of the encryption is better assured. Therefore, to enhance data security, the method employs three three-dimensional nonlinear chaotic systems: the Lorenz chaotic map, the Duffing chaotic map, and the Chens chaotic map.

The state equations for the Lorenz chaotic map are described as follows:

$$\begin{cases} \dfrac{dx}{dt} = p(y - x) \\ \dfrac{dy}{dt} = -xz + rx - y \\ \dfrac{dz}{dt} = xy - ez \end{cases} \tag{5}$$

In the equation, $t1$, p, and r are system parameters. When $t = 8/3$, $p = 10$, and $r = 28$, the system exhibits chaotic behavior.

Duffing chaotic map:

$$\begin{cases} \dfrac{dx}{dt} = y \\ \dfrac{dy}{dt} = -\Delta \cdot y + gx(1-x^2) + f\cos(z) \\ \dfrac{dz}{dt} = \omega \end{cases} \tag{6}$$

Chens Chaotic Mapping:

$$\begin{cases} \dfrac{dx}{dt} = a(y-x) \\ \dfrac{dy}{dt} = (c-a-z)x + cy \\ \dfrac{dz}{dt} = xy - bz \end{cases} \tag{7}$$

When $a = 35$, $b = 3$, and $c = 28$, the system exhibits chaotic behavior.

These three chaotic systems, under the initial conditions $(x0, y0, z0)$, form a three-dimensional chaotic system that simultaneously possesses non-convergence, periodicity, and extreme sensitivity to initial values.

The hybrid chaos of these three chaotic sequences demonstrates excellent performance in autocorrelation, cross-correlation, and distribution uniformity. It enhances security without compromising decryption speed, employs a large number of keys to improve resistance against brute-force attacks, and utilizes linearly correlated parameters across all three chaotic systems, rendering the composite chaotic sequence highly sensitive to initial parameters. A series of experiments demonstrates outstanding performance metrics, including key sensitivity, resistance to clipping attacks, damage tolerance, interference resistance, and execution efficiency.

3.2 Chaotic Hybrid Encryption Algorithm Mechanism

3.2.1 Tent Mapping

The Tent mapping, which also is called the Tent map, at present is widely used together with the Logistic map. Compared with the Logistic map, the disordered sequences that are produced by the Tent mapping show lower sensibility for starting conditions and a more even distribution. The present article utilizes the Tent map to act as a chaotic signal generator[17]. Its expression is:

$$x_{n+1} = \begin{cases} 2x_n, & 0 \le x_n < 0.5 \\ 2(1-x_n), & 0.5 \le x_n < 1 \end{cases} \tag{8}$$

3.2.2 Algorithm Principles

The principle of the CDR hybrid algorithm is as follows: First, a random chaotic signal is generated through the Tent mapping. Then, a DES algorithm key is produced via mathematical transformation. This approach leverages the random characteristics of chaotic systems to enhance key security and encryption speed. This key is then used to encrypt plaintext via the

3DES algorithm. Subsequently, the key generated by the chaotic system is encrypted using the RSA algorithm. Both the encrypted key and the ciphertext are transmitted to the recipient. The recipient decrypts the 3DES key using RSA. Since 3DES is a symmetric encryption algorithm, the recipient can decrypt the ciphertext using this key. The algorithm flowchart is illustrated in Figure 3.

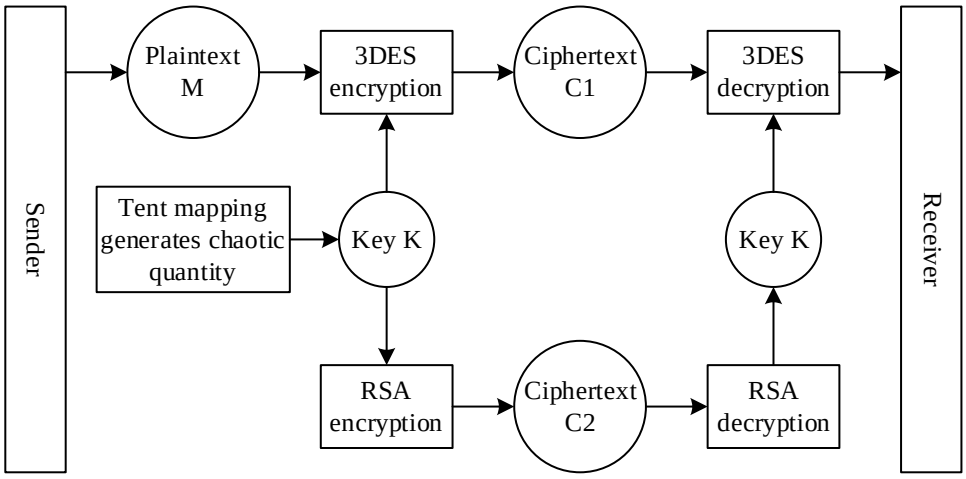


Figure 3: CDR Hybrid algorithm process

3.2.3 Chaotic Key Generation Strategy

The process of generating chaotic keys via the Tent map is as follows:

(1) Randomly generate a number X_0 between 0 and 1. Determine the iteration count based on the DES algorithm's key length.

(2) Substitute X_0 and n into Equation 1 to generate a 64-bit chaotic sequence X using the Tent map.

(3) Rewrite the sequence X according to $X_n = \begin{cases} 0, & 0 \le X_n < 0.5 \\ 1, & 0.5 \le X_n < 1 \end{cases} n = 1, 2, \cdots, 64$ to obtain the integer sequence I.

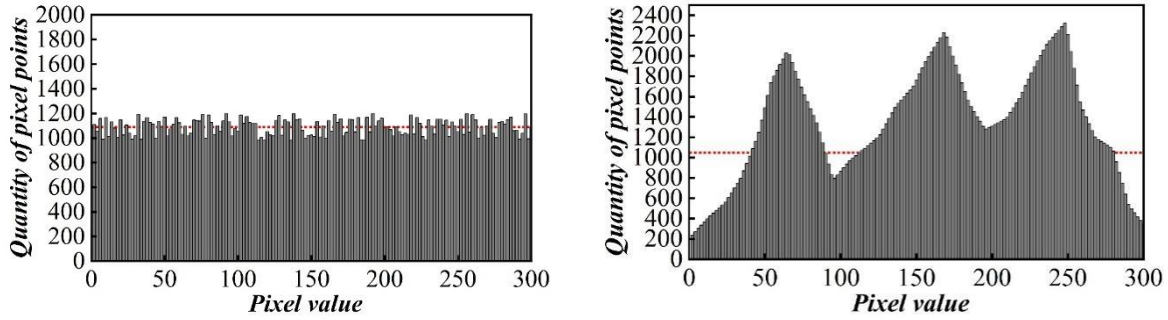
(4) Represent I as the corresponding 64-bit binary form K, which is the DES algorithm key.

3.3 Security Analysis of Corporate Financial Accounting Systems

The histogram of an image reflects the probability distribution of each gray level. To resist statistical attacks, the ideal image histogram distribution must be uniform. To evaluate the uniformity of an image histogram distribution, research employs the chi-square test to assess the difference between the actual histogram and a uniform histogram. A histogram exhibiting a normal distribution shape indicates that the data distribution is relatively uniform with a pronounced central tendency. As shown in Figure 4, (a) and (b) represent the plaintext and ciphertext images, respectively.

Figure (a) exhibits a chi-square distribution with 256 degrees of freedom. At a significance level of 0.05, the histogram distribution of the plaintext image is non-uniform, indicating that attackers could potentially crack the cipher by analyzing the plaintext image's histogram. Figure (b) shows a uniform histogram distribution for the ciphertext image. When encryption is finished through chaotic cryptography and RSA, the image histogram becomes more random

and not regular, thus security is enhanced. Under the 0.05 significance level, the chi-square numerical value of the Lena image is 255.5, it is lower than the expected value, hence this proves that the method can effectively resist attacks that exist in financial accounting systems.



(a) Plaintext (b) Cryptographic

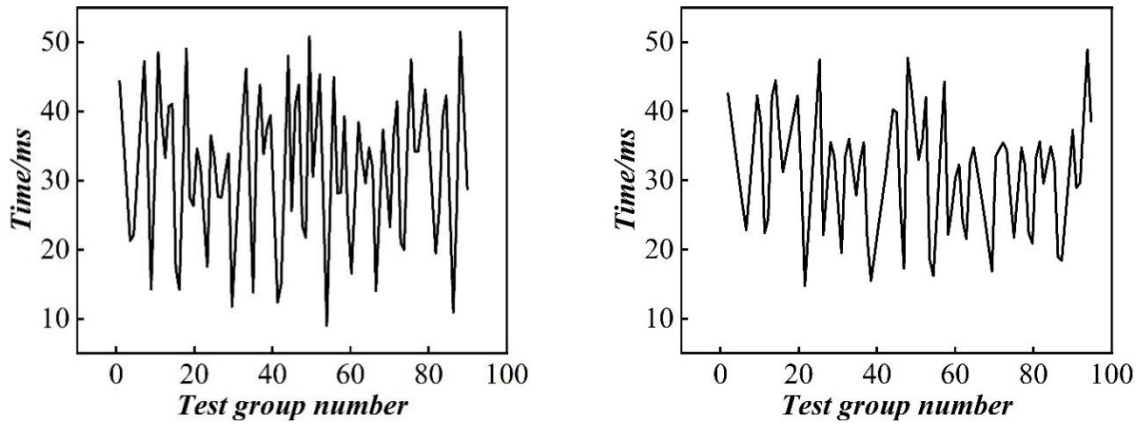
Figure 4: Image histogram

According to this, our study has randomly chosen 1,800 pixels from the original image to be samples, and has carried out analysis on the correlation coefficients of the ciphertext image in three dimensions: horizontal, vertical, and diagonal. In general situation, correlation coefficient values lie between minus one and positive one, and values which are more near zero show higher encryption efficiency. Through the computation of correlation coefficients on horizontal, vertical, and diagonal directions, this study has made comparison of correlation coefficients from different encryption algorithms, which is displayed in Table 1.As demonstrated in Table 1, the proposed chaotic cipher combined with the RSA algorithm transforms the correlation between adjacent pixels in the ciphertext image to zero in all directions. This disruption of correlation renders the statistical characteristics of the ciphertext image more random and irregular, endowing it with strong resistance to statistical analysis.

Table 1: Comparison of correlation coefficients of different encryption algorithms

Channel	Channel 1			Channel 2		
Direction	Level	Vertical	Diagonal	Level	Vertical	Diagonal
Plaintext	0.9411	0.9845	0.9939	0.9981	0.9722	0.9654
CDR algorithm	0.0052	-0.0061	0.0077	-0.0049	0.0058	-0.0075
One-way hash algorithm	0.0258	0.0201	0.0311	0.0178	0.0234	0.0345
International data encryption	-0.0059	-0.0081	-0.0088	-0.0087	-0.0111	-0.0085
Digital signature algorithm	0.0422	0.0818	0.0619	0.0696	0.0555	0.0683
Rijndael encryption algorithm	-0.0286	0.0454	-0.0422	0.0338	-0.0335	0.0555
Safe hash algorithm	0.0088	-0.0078	0.0088	-0.0093	0.0095	-0.0088

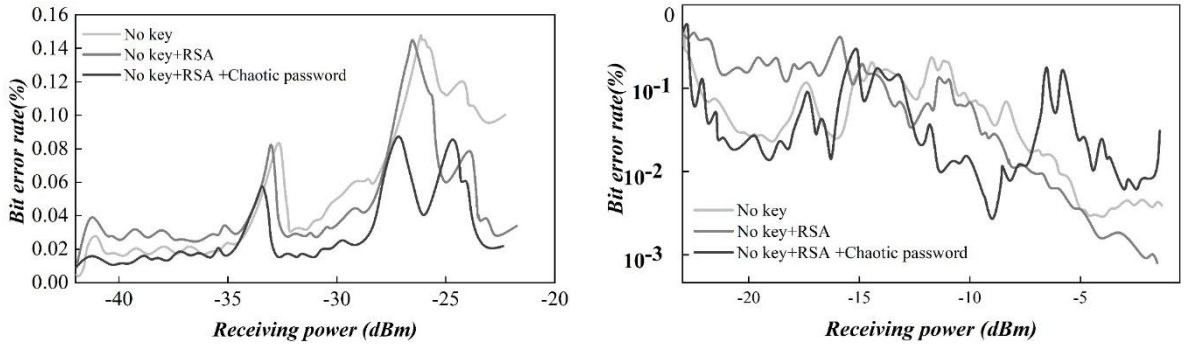
By testing 100 samples using the dataset with N's extreme value of 100 as a parameter, their time-series generation times can be obtained as shown in Figure 5. Experimental results indicate that both sets of hyperchaotic sequences generate within 0.05 seconds, demonstrating that encryption can commence immediately after data acquisition without affecting the continuity of audio and video streams. During simulation, the study decomposed plaintext digital signals into 256 codewords, generated a 25-level chaotic matrix, and then performed an inverse Fourier transform on it.



(a) Chaotic sequence 1 generation time (b) Chaotic sequence 2 generation time

Figure 5: Time of timing

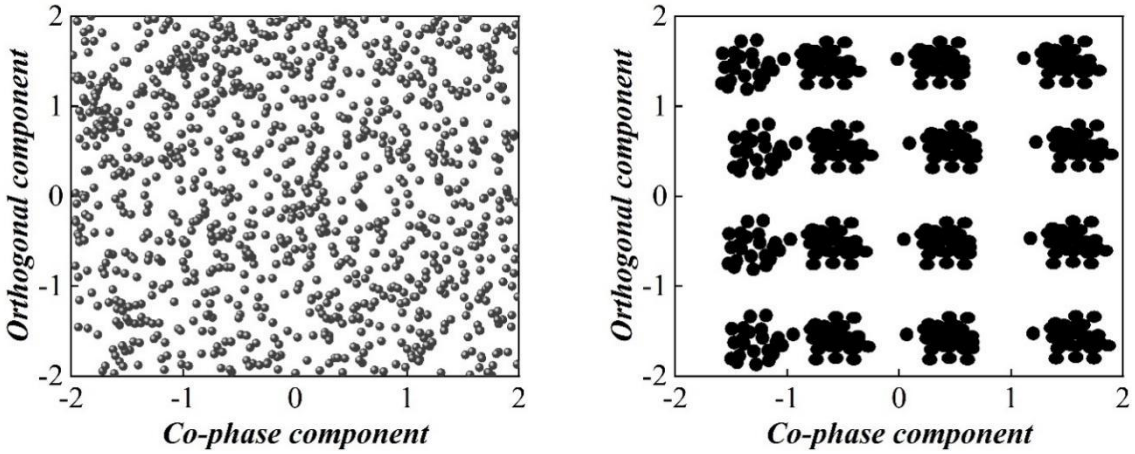
After transmission, the error performance of the modulation signal without key information and the error performance of the received signal are shown in Figure 6. In Figure 6(a), the error characteristics of the modulation signal without key information after transmission are depicted, indicating that the RSA+chaotic cryptography error correction coding has no impact on the encryption function. Figure (b) shows the received signal error rate performance. It is evident that even without stride and initialization information, the error rate of the encoded signal remains close to 1. When incorporating the key, the long non-periodic RSA+chaos encryption algorithm achieves over 11 dB energy gain at a BER of 10^{-2}, demonstrating excellent error correction and dispersion resistance performance.



(a) Non-key receiving signal error performance (b) Reception signal error rate performance

Figure 6: Receiving signal error performance

The constellation diagram for a bit error rate of 1 with successful decryption is shown in Figure 7. In Figure 7, constellation diagrams reflect the modulation scheme and modulation error of the received signal. In Figure (a), with a bit error rate approaching 1, the constellation diagram exhibits significant distortion or offset, indicating a very high number of error bits in the received data. In contrast, Figure (b) shows a correctly decrypted constellation diagram with no noticeable distortion or offset, indicating a very low number of error bits in the received data.



(a) The error rate is close to 1 (b) The sign of the right decryption

Figure 7: The error rate of bits is 1 and the sign that is correctly decrypted

4 Analysis of Security Management Efficiency in Corporate Accounting Systems

4.1 Data Sources and Sample Selection

The data that this research uses come from questionnaire surveys and in-depth interviews. Through the method of stratified random sampling, 400 small and medium-sized enterprises from the whole nation were selected, these enterprises satisfy three standards: they accord with the official definition of small and medium-sized enterprises, they have been established for more than three years, and they have used cloud-based accounting systems for no less than one year. Quota amounts were distributed by each region and each industry for the guarantee of representative property. We altogether have 400 investigation question papers that were given out through online way and on-site way, and we have gotten 375 effective reply materials, the rate of reply is 93.75%.

4.2 Analysis of Enhancing Financial Accounting Efficiency in Small and Medium-Sized Enterprises

4.2.1 Analysis of Enhanced Efficiency in Financial Data Processing

One investigation toward 375 business units discovers that the accounting system very greatly promotes efficiency in daily account keeping, document handling and account checking (see Table 2). This promotion is hence mainly given to automatic data gathering, intellectual identification and handling. This system can extract key information and process transactions in automatic mode, therefore it reduces manual work work and errors that people make. Real-time data synchronization also can make cross-department sharing come true, therefore it eliminates redundant input and information isolated islands. The adoption of this system has the significant positive connection with the processing efficiency of financial data of SMEs.

Table 2: The impact of accounting system on financial data processing efficiency

Index	Pre-system application	Post-system application	Change
Daily time of account	5.5	2.4	56.4%↑
Voucher processing speed	48	81	68.8%↑
Check error rate/%	4.0	0.55	86.3%↓
Data update cycle	3.3	0.4	87.8%↓

4.2.2 Analysis of Enhanced Efficiency in Financial Reporting Generation

The investigation data indicate that this system can make the time which produces financial reports become shorter, and promote the quality of reports (please look at Table 3). Such efficiency promotions come from automatic report making and real-time data renewing. This system uses the templates which are set in advance to extract data, so that it can quickly make financial statements. At the same time, the analysis which is built inside finds unusual situations and carries out difference checks, thus enhancing the accuracy and reliability. Business units also attach importance to its custom making and visual expression, which let reports become more intuitive and therefore give support to decision making. The outcome verifies that there is an obvious positive connection between system usage and report making speed for small and medium-sized enterprises.

Table 3: The impact of the accounting system on the efficiency of the financial report

Report type	Pre-system application/day	Post-system application/day	Lifting amplitude
Monthly report	4	0.8	400%
Quarterly report	8	1	700%
Annual report	12	2	500%
Custom report generation time/h	22	2.5	780%

4.2.3 Analysis of Enhanced Fund Management Efficiency

The results of our investigation show that after enterprises put into use an accounting and financial management system of enterprise, they have appeared obvious promotion in the accuracy of capital forecast, the efficiency of capital use, and the control of capital risk. The influence that enterprise accounting and financial management system exerts on capital management efficiency is displayed in Table 4. These promotion effects mainly come from the system's real-time fund supervision, intelligent prediction, and risk warning functions. This system can make real-time follow-up of capital changes in all company bank accounts, it automatically gathers and studies cash flow rules to give management a complete general picture of the company's financial situation.By making use of big data analysis and machine study, the system gives accurate prediction of capital requirement through past and operation data, which gives support to strategy arrangement. Its intelligent matching carries out optimization for receivables and payables, therefore it boosts capital utilization. The promotion of cash management work differs according to the scale of enterprise and the type of industry, hence retail enterprises and relatively large enterprises can obtain more benefits therefrom. The carrying out of this system has a strong connection with the cash management efficiency of SMEs.

Table 4: The impact of enterprise accounting system on capital management efficiency

Index	Pre-system application	Post-system application	Change
Money forecast accuracy/%	78	98	25.6%↑
Capital turnover rate/ (annual $^{-1}$)	4.1	6.4	56.1%↑
The cost of the money /%	5.4	4.1	24.1%↓
Excess capital detection time/h	50	5	90.0%↓

5 Conclusion

Big data and cloud computing technologies have created more development platforms for corporate financial accounting, providing new information technology tools for financial data mining and analysis. These technologies enable real-time sharing and synchronization of financial data, effectively reducing IT costs and maximizing financial management efficiency. This study introduces cloud computing technology and encryption algorithms, proposing a method that combines chaotic cryptography with asymmetric encryption algorithms to ensure the secure management of corporate financial accounting systems.

The application of RSA combined with chaotic cryptography error correction coding has no impact on the encryption function. Even without step size or initial value information, the error rate of the encoded signal remains close to 1. When incorporating a key, the long non-regular RSA combined with chaotic encryption algorithm achieves an energy gain exceeding 11dB at a BER of 10^{-2}, demonstrating excellent error correction and dispersion resistance performance. The chaotic cryptography has high complexity and high randomness, therefore it can effectively protect the confidentiality and integrity of data. The combination of chaotic cryptology and RSA arithmetic can strengthen the data encrypting work, therefore it can guarantee the safety and completeness in the process of transmission and preservation.

Cloud-based enterprise accounting systems not merely greatly speed up financial data processing and cut mistake rates but also overall promote company financial management via optimized capital distribution. But, when organizations carry out this work, they must solve difficulties which include early-stage input and staff cultivation. Looking to the future, along with the progress in artificial intelligence and big data technologies, intelligent financial systems have good development prospects for being used by small and medium-sized enterprises.

About the Author

Xiaorong Shi, She graduated from Dongbei University of Finance and Economics in 2008, and also he graduated from Zhengzhou University in 2014. Her highest academic degree which she has obtained is a master's degree. She works in Anyang Vocational and Technical College as an accounting teacher. Her research interests include financial accounting, accounting information system and data mining and analysis.

References

[1] Gareeva, G. A., Grigoreva, D. R., & Mahmutov, I. I. (2020). Financial accounting, analysis and features of calculations with personnel. International Journal of Financial Research, 11(5), 221.

[2] Cagle, M. N. (2019). Reflections of digitalization on accounting: the effects of industry 4.0 on financial statements and financial ratios. In Digital Business Strategies in Blockchain Ecosystems: Transformational Design and Future of Global Business (pp. 473-501). Cham: Springer International Publishing.

[3] Zhyvko, Z., Nikolashyn, A., Semenets, I., Karpenko, Y., Zos-Kior, M., Hnatenko, I., ... & Krakhmalova, N. (2022). Secure aspects of digitalization in management accounting and finances of the subject of the national economy in the context of globalization. Journal of Hygienic Engineering & Design, 39.

[4] Kuyoro, S. O., Ibikunle, F., & Awodele, O. (2011). Cloud computing security issues and challenges. International Journal of Computer Networks (IJCN), 3(5), 247-255.

[5] Dimitriu, O., & Matei, M. (2014). A new paradigm for accounting through cloud computing. Procedia economics and finance, 15, 840-846.

[6] Wyslocka, E., & Jelonek, D. (2015). Accounting in the cloud computing. Tojsat, 5(4), 1-11.

[7] Ogiela, L. (2015). Intelligent techniques for secure financial management in cloud computing. Electronic commerce research and applications, 14(6), 456-464.

[8] Nguyen Phu, G., Hoang Thi, T., & Tran Nguyen Bich, H. (2025). The impact of cloud computing technology on cloud accounting adoption and financial management of businesses. Humanities and Social Sciences Communications, 12(1), 1-14.

[9] Tsai, C. L., Lin, U. C., Chang, A. Y., & Chen, C. J. (2010, August). Information security issue of enterprises adopting the application of cloud computing. In The 6th International Conference on Networked Computing and Advanced Information Management (pp. 645-649). IEEE.

[10] Ionescu, L., & Andronie, M. (2021). Big data management and cloud computing: Financial implications in the digital world. In SHS Web of Conferences (Vol. 92, p. 05010). EDP Sciences.

[11] Alali, F. A., & Yeh, C. L. (2012). Cloud computing: Overview and risk analysis. Journal of Information Systems, 26(2), 13-33.

[12] Nutalapati, P. (2024). A Review on Cloud Computing in Finance-Transforming Financial Services in the Digital Age. International Research Journal of Engineering & Applied Sciences| Irjeas. org, 12(3), 35-45.

[13] Nagarajan, H. (2024). Assessing security and confidentiality in cloud computing for banking and financial accounting. International Journal of HRM and Organizational Behavior, 12(3), 389-409.

[14] Ren, S. (2022). Optimization of enterprise financial management and decision-making systems based on big data. Journal of Mathematics, 2022(1), 1708506.

[15] Rahul Vijay & Thankaraja Raja Sree. (2025). Secured trust and reputation management framework for cloud service in cloud computing. Computing,107(9),186-186.

[16] Jing Jiang, Yushu Su, Jingchi Cheng & Tao Shang. (2025). Multi-Link Fragmentation-Aware Deep Reinforcement Learning RSA Algorithm in Elastic Optical Network. Photonics,12(7),634-634.

[17] Wei Zhou, Xianwei Li & Zhenghua Xin. (2025). Image Encryption Algorithm Based on an Improved Tent Map and Dynamic DNA Coding. Entropy,27(8),796-796.