Journal of Theoretical and Applied Information Technology
15th April 2025. Vol.103. No.7

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

SECURE AND RESILIENT VIDEO BLOCK MANAGEMENT AND PRINCIPLES FOR ZERO TRUST CLOUD NETWORK

[1]K.MUTHULAKSHMI, [2]K.VALARMATHI, [3]J.SATHYAPRIYA, [4]S.PRIYADHARSHINI

[1] Associate Professor, Panimalar Engineering College,Chennai,Tamilnadu,INDIA
[2] Professor, Panimalar Engineering College,Chennai,Tamilnadu,INDIA
[3] Professor, Velammal Engineering College,Chennai,Tamilnadu,INDIA
[4]Asst Professor, Velammal Engineering college,Chennai,Tamilnadu,INDIA
E-mail:[3]dr.sathyapriyaanand@gmail.com,
[4]hai.priyadharshini@gmail.com

ABSTRACT

Cloud computing principles are widely applied to provide reasonable network services to a range of users. In addition to the basic services of cloud networks, security features are highly expected at the user end. Considering these issues as a scope of this article, various existing techniques are identified. The existing solutions on zero trust cloud network target single mode encryption model irrespective of data models. However, the video content delivery systems in cloud platforms need multiple modes of secure data transmissions. According to that, the proposed Secure and Resilient Video Block Management (SRVM) model has been developed to attain both real-time and non-real-time security constraints. On the basis, this proposed model uses switchable block cipher and stream cipher model with respect to video data transmission modes. Similarly, the data blocks collected in the cloud environment are effectively distributed among cloud virtual machines and data is encrypted in a complex manner. This kind of novel idea reduces the chances of data confidentiality breaches and data losses due to attackers. The experiments have been conducted between SRVM, Blockchain based Multimedia Data Security (BMDS), Firefly Optimization and Encryption (FFOE), and Quality of Everything in Edge based Encryption (QMEE) to ensure the testbed performances. In this experiment, the proposed model works 10% to 15% optimally than existing techniques and the details are observed through multiple test cases.

Keywords: *Cloud Computing, Security, Video Data Management, Virtual Machines And Data Confidentiality.*

1. INTRODUCTION

This article explores video data management policies and security principles within various network models, particularly focusing on Zero Trust Cloud Networks (ZTCN). It emphasizes:

Types of computer networks (wired, wireless, centralized, distributed).

Key network performance metrics (delay, bandwidth, jitter, throughput, security).

The role of ZTCN in securing multimedia data (real-time and non-real-time).

Cloud security challenges and ZTCN's "no trust, always verify" approach.

Applications of ZTCN in securing video data streams.

The integration of emerging technologies (AI, IoT, blockchain) for security improvements.

Video data management policies and security principle are crucially expected around various network models. Computer networks vary in the types such as wired networks and wireless networks basically. In the same manner, networks shall be deployed under centralized fashion or distributed fashion. The basic requirements for establishing a good network are denoted with the feature of quality metrics (delay, bandwidth, jitter, throughput and security features). Particularly, reliable communication and secure data management conditions are commonly expected for any type of network. On this expectation, multimedia data (real-time and non-real-time) streams shall be secured through optimal principles. Notably, the deployment of security principles is estimated to provide optimal resource utilization. In this regard, this article analyses the issues in video data

management solutions and security models that can be applied for Zero Trust Cloud Network (ZTCN).

In cloud environment, ZTCN ensures unacceptable trust factors and expected validations, and acknowledgement for all network devices and people. In addition, individual access, information security, location monitoring, internal event monitoring and external event monitoring procedures are enabled under ZTCN perimeter. The process combines analytics basis, cleaning, and logging to verify behaviour and continually monitor for continuous events against vulnerabilities. ZTCN monitors various signs of different actions and invokes threat flag functions against potential threats. ZTCN uses a 'no trust and always verify' concept to improve cloud cyber security and verify cloud network requests. In addition to particular type of data security principles, multimedia data picture data, voice data, real-time video data, non-real-time video data as well as web links and meta data. The enlargement in bandwidth and throughput of recent mobile technology and network technology leads in to huge level of data handling phases under various applications. The data occupied in cloud storages can be related to health care systems, e-commerce systems, online education systems, and other supportive systems.

Safety and security are important concerns for presenting cloud networks services today. As the network channels are being increased in terms of bandwidth and throughput, the amount of data transferred on the channel is getting huge in size. In the same way, the vulnerabilities involved in to the data are increasing all the time. Particularly, video data shall be easily corrupted or dropped due to attacks. In this concern, threats and attacks should be reduced to protect the cloud systems. ZTCN is an optimal idea against many attacks to protect the physical resources and data through identity certification, access control and systematic trust estimation and confidential procedures.

These types of networks work only focuses on security certifications and trust value computation procedures. There are many applications involved in cloud-based audio and video data management platforms. For example, the use of multimedia data in medical healthcare framework allows storage process and exchange of patient data in a worldwide range of format such as photos, letters and voice over the network using smart models. Still maintaining very large and high amount of data information, including each person's findings and image increases human effort and safety risks. Similarly, data dimensions, data originality and data confidentiality are expected to be addressed. management solutions are required with more suitable features. ZTCN can be improved to attain reliable security for Resilient Video Block Management (RVBM) and provides individual access to applications and information. The technical features of ZTCN have been developing over the years, but companies are disinclined to invest in a cloud security approach. Its importance to take security challenges in ways to implement or update the ability of security frameworks that are suitable for both real-time and non-real-time environments. Multimedia data mining and data security principles include text file, audio files, video files and other data resources under cloud data management panels. The discovery of interesting patterns and platforms of multimedia databases that are storing and handling large collection of multimedia objects, huge size of Benefiting from advances in company revolution, artificial intelligence, fifth generation applications, internet of things and block chain technology are expanding the solutions against various network attacks. Particularly, the recent era focuses on the need for system to system and machine to peoples' interactions where big amounts of data information is being shared during the process of information communication devices. As the cost of generic network resources is high, people are moving in to cloud services. The cloud services shall be provides based on infrastructure level, software level and platform level. In addition, the concept of no trust policy is used to improve data security features by removing trust and verifying network request continuously. ZTCN services are enabled to change Virtual Private Network (VPN) and shared solitary access to information and data. The improvements in ZTCN have been spiked over the year. Particularly, the involvement of fifth generation network in cloud platform is used to update the communication quality and develop more volumes of information through very fast networking technology. In particular, there are four types of cloud computing systems such as public cloud models, private cloud models, hybrid cloud models and community cloud models. According to the models of cloud systems, the zero trust policies are enabled to secure the overall network resources. Cloud computing users can avoid capital expenditure on hardware and software by simply paying the provider services under optimal cost. At the same time, the provision of security principles under cloud environment is mandatory for protecting the data.

In this domain, Sarkar et al. [1] executed a comparative study over various articles that are

related to ZTCN. In this study, ZTCN features were insisted to be improved with notable policies such as scope of data access, no trust rule, proofs of work and threat monitoring policies. This work provided the invention of trust value computation policies, zero trust execution over various network architectures, proof of concept solutions and ZTCN models.

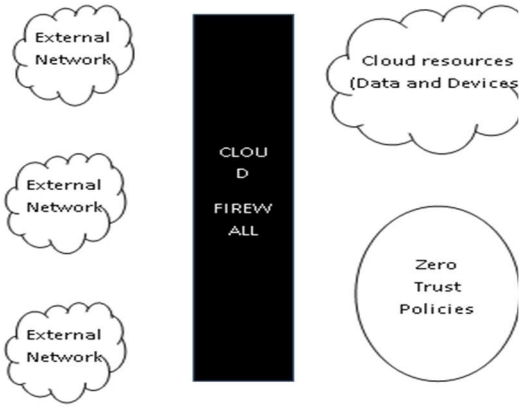

Figure 1. Basic Model for ZTCN

Adahman et a. [2] and Li et al. [3] analysed the possibilities of ZTCN models in future applications. Particularly, the internet of things and hybrid networks have been analysed to enable zero trust policies. These works found the importance of industry systems security and organizational resource security features to ensure the protection state. In these cases, application-based trust models were created to validate the trust factors of each network entity. Similarly, privacy preservation solutions were attained through several recent works [4][5]. In extend, the ZTCN model had been utilized by Saleem et al. [6] to protect multimedia data and digital forensic solutions.

Awan et al. [7] proposed blockchain based zero trust calculation methodologies that were executed through attribute analysis procedures. In this environment, Internet of Things (IoT) entities were identified with heterogeneous range of qualities. In this IoT environment, each device and resource types (data) were classified under multiple classes based on configuration metrics.

This existing scheme provided set of access control mechanisms (zero trust model) to ensure that each attribute specified in transaction were legitimate. Similarly, the identity of each device had been verified through blockchain principles (authentication and integrity). Blockchains are useful technologies in distributed environment to provide hash-based security platforms. On the scope, table et al. [8] proposed multimedia data processing schemes using blockchains for health care applications. Generally, health care data is observed from multiple types of sensors with different data types. Notably, blood pressure data, heart data, muscle movement data and other bio signals can be recorded using IoT policies. This existing scheme collected these medical data from various devices and protected the data using blockchain computation procedures.

Both works were using blockchain principles to protect the data against information threats. At the same time, application of blockchain principles is restricted under distributed network environments. On behalf of centralized cloud networks, the security solution is required to protect real-time and non-real-time multimedia data. Particularly, securing video data streams using improved ZTCN policies.

In general, the video data manipulation subsystem helps the user toad, edit and delete information in the database and query it for valuable response. The software tools within the data handling subsystem are often the primary interface to the user and the database containing the information allows the user to specify its logical information requirements. Through the popularization of home office and hybrid work models, the security of corporate networks needs to be reinvented by not using the user's location as a baseline the zero trust concept. Similarly, most of the existing solutions were enriched with either real-time or non-real-time security principles to protect video data communications. In addition, the establishment of more reliable and secure data encryption solutions are required against data security attacks. These are considered as major problems to be taken.

On the case, the proposed SRVM has been motivated to ensure distributed encryption policies in the ZTCN that can be applied for both real-time and non-real-time video data security solutions. At the same time, the proposed work has been involved to optimize the overall video data encryption procedures in terms of time and memory scales. The contributions of proposed model have been listed below.

- Real-time (Distributed Stream Cipher) and Non-real-time (Distributed Block Cipher) security solutions

- Optimal video data distribution in to VM layers
- Distributed video data management policies and encryption schemes
- Lightweight virtual security procedures
- Dynamic cost computation procedures

Data confidentiality techniques such as block ciphers and stream ciphers can be used to encrypt the data in various applications. The block ciphers such as Data Encryption Standards (DES), Advanced Encryption Standards (AES) and other hash computation techniques are useful for standard data locations. On the other hand, stream ciphers such as RC-4, cipher feedback functions, fish, HC-256 bits and others are useful for ensuring real-time video data security. Anyhow, the usage of these algorithms under inefficient phases leads in to insecure data transmission conditions. In this work, the proposed model uses data sensitive AES for non-real-time video data encryption (VMs) and adaptive RC-4 procedures for ensuring real-time video data security (VM) solutions. Similarly, content aware trust computations and lightweight VM functions are invoked to provide reliable and secure video data management policies in ZTCN.

The implementation of Zero Trust Cloud Networks (ZTCN) faces several challenges. Trust computation complexity arises due to continuous verification, leading to increased computational overhead. Additionally, adoption barriers exist as companies hesitate to invest due to high costs and implementation difficulties. Scalability issues make it challenging to deploy ZTCN across diverse cloud models, and real-time security trade-offs can introduce latency in encrypted video streams. While blockchain enhances security, its effectiveness is limited to distributed environments, requiring alternative solutions for centralized networks.

Based on these contributions, the proposed article has been structured from section 2 with deep literature comparisons. Section 3 has been illustrated for providing the technical details of proposed SRVM and its procedures. Section 4 has experiment testbed details and observed results to ensure the ability of proposed model against existing techniques. Section 5 shows the concluded details and technical improvements can be addressed in future.

2.RELATED WORKS

The related works discussed in this section are mainly focusing to understand the contributions of various technical efforts and limitations. In this regard, the terminologies related to ZTCN, video data management policies, data confidentiality procedures and secure cloud solutions are described. In addition, applications of encryption methods are discussed. Kumar M et al. [10] proposed secure video transmission using firefly optimization and visual cryptography through machine learning (ML) models.

In the workplace, ML is very beneficial to do business and collaboration. The reason why these ML or optimization tools have been so impactful is their ability to learn event behaviours. Over timely tools gather data and insights intrinsic to the user and therefore provide personalized solution for the event interaction of applications. Optimization (firefly) techniques on visual cryptography needs to concentrate on loss of data and recreation of data. In the same manner, results of all stages need to be improved in terms of data flow, costs reduction, and minimized distortions in productivity. The visual cryptography tasks are automated to recognize and deliver the secure data in the right place, to get business profit with productively performing functions. Anyhow, improper placement of generic algorithms increases more time complexity and system overload.

In the same stream, Saraji K et al. [11] developed watermarking functions to protect images and videos. This method was applied for photographer and photojournalist ends. This existing scheme proposed I-watermarking (IWM) by adding a unique text or graphic watermark in the video blocks. This visible water making solution shows owners' creativity and ownership when it was being added to a photo or video. IWM should be the tool for anyone to quickly protect images and videos from piracy issues. IWM is the most popular multi-platform tool for decades that is applied as IWM-Pro and IWM (MAC / windows / android. This method used a variety of visible and invisible digital watermark to link the photo to its creator. Every person who takes photos and videos can apply this solution as an essential for photo journalism, photography, and other social media platforms. Since it allows photographers to maximize the promotion of their photos, while preventing them from losing control and connection as a photo editor. However, this technique is not an efficient procedure against digital vulnerability issues and attacks.

Benisha et al. [12] proposed video communication quality enhancement using sheep-flock optimizer functions and gained widespread popularity as it

provided a real-time direct transmission. This scheme was aimed to develop the video communication standard of multimedia data with network security enhancement and adaptive resource assignment plans. The important concept of the ability assignment plans was to reach usage of spread ability since video transmission used orthogonal subcarriers and there was a need to convert non flat channels in to flat ones. Particularly, this scheme provided optimality models for reducing communication error rates, data authorization issues and misbehaving attempts. In the same manner, this model increased the ability of wen protocols against attacks.

Anyhow, the application of zero trust assurance and cloud-based implementations were limited under this scheme. Ahamad R et al. [13] proposed unidentified object observation methodologies in Unmanned Aerial Vehicles (UAVs)through video frame analysis procedures.

The automatic detection of faces from UAVs is a difficult task to get more accuracy. On principle component analysis models, fewer Eigen values were used to recognize the faces. The issue of face data recognition and analysis was another complicated issue since inconsistent video/image standards, colouring conditions, and incorporated options of asymmetric occlusion and camouflage. Therefore, super face conversions and system training models were evolved in to video frames /image analysis procedures recognize the presence of any face be foreground/background at different colouring conditions. At the same time, video encryption and decryption solutions were also be expected at any cost in cloud platforms.

On contrast, the development of cloud infrastructures includes Virtual Machines (VM) to manage the functions in a distributed manner. Zhao H et al. [14] proposed VM migration schemes based on overall performance. They were divided in to two main categories based on their usage and any kind of interaction with any real machines or other VMs.VM provides a complete computing platform that supports the functionality of a complete operation system and a functional VM is one designed to process any requests. An important characteristic of a VM is that the software running within it is to validate the utilization of resources and abstractions provided by the cloud services.VM allows the sharing platform in a common physical machine with multiple running operating systems. The software layer in VM called a VM monitor the virtualization platform and allows a computer to share time between multiple single tasking operating systems. This strategy requires implementation of sharing CPU resources between guest operating systems and memory virtualization to share memory on the host. In this regard, performance controlled VM engines shall be created to improve the cloud service utilization factors. Notably, network resource utilization, cloud service demands and user expectations were mapper in the existing techniques.

Encryption is the process of changing information using a process to be unreadable by anyone excepted information called a key. The result of this process encrypted information referred to as cipher text in secret communication. In many contexts, the term encryption also implicitly refers to the reverse process of decryption to make encrypted information readable again through decryption function. Alhayani B Set al. [15] proposed elliptic curve cryptography principles for optimizing video encryption schemes.

It was important to maintain secure money transfer, computerized data transfer and many more through cryptographic engineering and computer security engineering solutions. These techniques have been emerged for enabling secret communication.

In this case, multimedia sensor networks and video-IoT models were utilized to ensure transmission of secure video data blocks. Elliptic curve cryptography is a good method to provide lightweight encryption solution. Anyhow, the data complexity issues were not handled by this existing work properly.

Suresh M et al. [16] proposed Optimized interesting region identification for video steganography using fractional Grey-Wolf optimization with multi-objective cost functions. According to this novel representation, structural similarity index values were measured to initiate video steganography functions. Then the security key frames were subjected to the creation of video sections with the security support of multiple grid lines. Wang Let al. [17] proposed an electronic watermarking and hiding technology using a noisy wave in the form of audio, video or pictures data.

Gupta B et al.[18]proposed This is improving rapidly due to data centralization, increasing security conscious resources etc. but concerns about loss of control over certain sensitive data also persist. Security is as good as or better than legacy systems because providers are able to provide resources to address security issues that many customers cannot afford. Providers can request permission but accessing audit permission themselves can be complicated or impossible. Ownership, control, and access to data can be complicated by cloud providers making it

sometimes difficult to access the benefit of live help with current applications. Under the cloud model providers and third parties. Sustainability comes from improve resources utilization more efficient systems and carbon balance. However, computer and related infrastructure are major energy consumers.

Yin Het al. [19] proposed the general security provisions for pictures cloud systems. This concept uses cloud computing technology to develop the preparing public safety systems. It merges the storage area size of the backend system server execution technology and customizes the working rules of Hadoop principles to build a first normal basic model. Liu JK et al. [20] proposed a framework that permits mobile phone users to safely move, share and search on-time video information. Especially this scheme provided the benefits and advantages of the cloud computing area and platform and fifth generation system technology to reach its targets. Mobile phone customers can move and share their real-time video with their relatives and friends and family members direct the cloud computing while any other candidates. At the same time, video transmission without authorization and improper security features shall be corrupted due to attackers.

Table 1. Literatures and Features

No	Author	Methods	Contributions	Limitations
1	Kumar M et al. [10]	Firefly optimization and visual coding approach.	This method was used to secure multimedia data and converted using watermark in promoted video frame.	Not providing distributed security
2	Swaraja K et al. [11]	A safety concept of optimized and least complication video watermarking approach.	This proposed system increased the bit value within a decent end point by choosing proper non-zero quantity data residuals for fixing the watermark.	Need more recent security models
3	Benisha et al. [12]	Sheep Flock Optimization coding was used to decrease the network error calculation of the HD-RaNN structure by optimizing the heaviness and biases.	This concept aimed to develop the video extraction with high quality of multimedia tools and adaptive resource assignment technique.	Not secure against centralized attacks
4	Teodoro P et al. [13]	UAV based picture extraction and IoT-cloud systems.	This method was used with digital face identification and normal face detection using UAVs.	No data confidentiality
5	Zhao H et al [14]	Effective VM migration schemes against network resource dynamics using ant colony optimization	This work proposed migration functionalities in the cloud VMs to manage resource monitoring processes and event monitoring processes.	Less assumptions in dynamics
6	Alhayani et al. [15]	Optimization on video clips in the network using elliptic curve cryptography (ECC).	This concept used Cohen-Daubechies-Favreau (CDF) approach for evaluating rate of signal changes in video streams and encrypting the edge data.	Easy but less effective in cloud models
7	Suresh M et al. [16]	Optimization procedures for video steganography using Fractional Grey-Wolf identification principles. Compared with multi-things money function.	This work contributed to build segmentation and grid-based video steganography solutions. It was executed through similarity index calculation functions.	Conventional approach

8	Wang L, et al. [17]	Optimized water marking and Discrete Wavelength Transform were used for analysing multi-quality pictures.	Digital technology watermarking, as a worldwide used protect technology has been applied to save many media data copyrights. The watermarking algorithm was applied to achieve invisible and robust watermarking protection from different attacks.	Need to analyse video complexity
9	Gupta BB et al. [18]	Big data computations and security principles were used under mobile cloud platforms.	The special problem identification technique was taken to secure individual's video data in mobile phone and cloud computing with dynamic rules.	Need more application specific efforts
10	Yin H et al.[19]	General security provisions and public safety measurements.	The common safety security platforms for public domain pictures were proposed to help police in the investigation process.	No dual encryption methods
11	Liu JK et al.[20]	Data searching and securing principles on real-time data management systems.	Mobile based real-time video management solutions were proposed with cloud services.	Need flexible confidentiality mode

Liu Z et al. [21] proposed video caching models and multi-edge encryption schemes under Content Delivery Network (CDN). By making the CDN channel effective, this model assured responsive data downloading facilities as fast as possible.

Various methods and techniques were proposed to improve the quality of video data management solutions and encryption possibilities. Anyhow, the existing models were not accurately designed cloud-based video encryption and data management solutions against multiple types of information attacks. Particularly, the special attention is required to improve the quality of cloud-based video data encryption models which is limited now. On the basis, the proposed SRVM has been implemented to provide more reliable and better data security models.

Existing literature on cloud-based video data security often addresses isolated components, lacking an integrated framework that combines dual-mode encryption with computational optimization for scalable, comprehensive protection.

This study aims to enhance video data management and security in cloud environments by leveraging Zero Trust Cloud Networks (ZTCN). The primary focus is on ensuring secure multimedia data transmission using distributed encryption techniques for both real-time and non-real-time video data. The research also explores trust computation policies, block chain integration, and adaptive security frameworks to mitigate threats and attacks in cloud-based video communication and introduces a novel security model that improves video data encryption, trust management, and scalability within ZTCN, addressing critical challenges in cloud-based multimedia security.

Critical Discussion & Key Findings

Strengths: The proposed ZTCN model significantly improves video data security by integrating trust verification, encryption, and blockchain principles. The scalability across hybrid cloud networks is a notable advancement.

Weaknesses: The high computational complexity of continuous trust verification and real-time encryption remains a challenge. Additionally, blockchain's limitations in centralized environments reduce its universal applicability.

Interesting Facts: The adaptive content-aware trust model, machine learning-based threat detection, and dynamic cost computation strategies introduce novel elements to ZTCN-based security frameworks, making this study a valuable contribution to cloud-based multimedia security research.

3. PROPOSED WORK

Research Objectives

To analyze the limitations of existing cloud-based video security models concerning trust verification, computational complexity, and encryption efficiency.

To develop a dual-model encryption framework (SRVM) that integrates block cipher (AES-SHA) for non-real-time data and stream cipher (RC-4-SHA) for real-time video security within a ZTCN framework.

To optimize encryption efficiency using virtual machine (VM)-assisted security mechanisms, reducing computational overhead while maintaining robust security.

To evaluate the performance of SRVM against existing models such as BMDS, FFOE, and QMEE, measuring security, speed, latency, and resource utilization in a cloud.

To propose a scalable and adaptable encryption model for securing video data across healthcare, education, and e-commerce applications, ensuring compliance with evolving cloud security standards.

This proposed is designed to secure video data through ZTCN. In this method, video data are collected and stored as image frames.

Each Image frame has multiple pixel contents of (Red: Green: Blue RGB) intensity values. The encryption system and distributed video block management principles are developed for zero trust cloud network using the details given below. Before the development of proposed security layers, ZTCN model and information model shall be expected to be described. In this concept, virtual machine based distributed security principles are designed to secure the video data. Notably, this proposed SRVM executes both authentication (Secure Hashing-SHA-3) and confidentiality procedures in distributed VMs.

- Data modelling and Distribution Process
- Multi-Level VM configuration
- Distributed and Authenticated AES [Non-Real-Time Video Data]
- Distributed and Authenticated RC4 [Real-Time Video Data]
- Reassembling and Decrypting Video Data in Cloud

VM hypervisor security system with multi-modal encryption scheme is used to provide the secure zero trust cloud services. The internal VM based data security principles are using RGB colour intensity values to store and compute data to cloud environment. After calculating the intensity value, video segment data are stored in the VM server security. At the other end, virtual servers are created for providing protected data server units. This type of innovative and distributed encryption protocol provides a secure way to store RGB video data and encrypt the RGB values for managing sensitive information. RGB colour value extraction and encryption are the efficient solutions to ensure internal data security principles.

In this proposed model, the video data is segmented and distributed in to multiple VMs of cloud environment and decrypted at the centralized cloud collection unit. VM hypervisor supports multiple operating systems without special software and updates for windows, Linux, android and other editions. This environment offers advanced features such as fully authenticated access, zero knowledge encryption, and maximum privacy.

The proposed method provides RGB colours detection with impeccable security features for mobile applications and other computer-based video management platforms. This is the technology useful to store more video data as RGB information in the cloud network. Encryption is a secure way to store any video data as secret RGB information. Block Cipher converts plain text to cipher text by taking its block at a time.

Stream Cipher is a cryptographically technique with secure pseudorandom number generator that is used to encrypt plain text through bit wise operations.

Table 2. Block Cipher and Stream Cipher

Block cipher	Stream cipher
Bits : 64 Bits, 128 Bits, 256 Bits etc.	Bits: 8 Bits to 256 Bits
Confusion and diffusion strategies	Only confusion strategy
AES and DES etc.	CFB and RC4 etc.
Complex and efficient	Easy but task specific
Applied for non-real-time data security	Applied for real-time data security

A generic block cipher that encrypts information in stream of 128 bit using 128,192-, and 256-bit symmetric keys. In this proposed model, AES (256 bits) is used to secure video blocks.

Journal of Theoretical and Applied Information Technology
15th April 2025. Vol.103. No.7

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

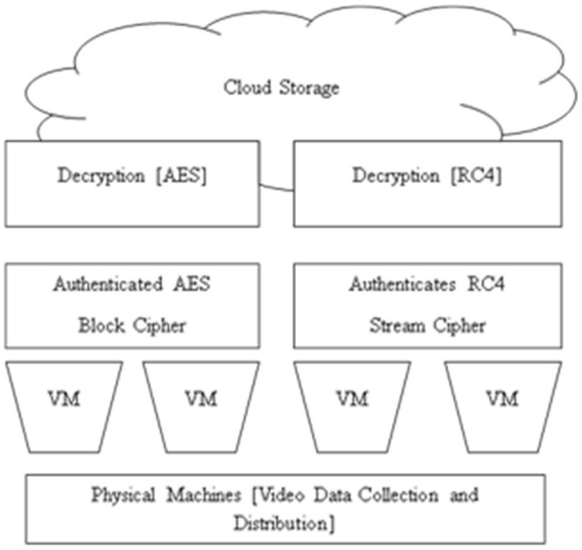

Figure 2. Proposed Srvm Functions

In proposed SRVM, initial phase is designed to create a model of ZTCN. The ZTCN is modelled as given in equation (1)→(3).

$$(t) = n(s(k), c(k), T)\ \forall\ N \quad (1)$$

$$\text{Server units, } s(k) = S(pys, vis).dt \quad (2)$$

$$\text{Client units, } c(k) = S(pyc, vic).dt \quad (3)$$

$T - Zero\ Trust\ model$

$S(pys, vis)$

$- set\ of\ physical\ server\ machines\ and\ virtual\ server\ machines$

$S(pyc, vic)$

$- set\ of\ physical\ client\ machines\ and\ virtual\ client\ machines$

N

$- Total\ number\ of\ nodes\ in\ the\ cloud\ network$

The trust value T is computed for both client units and server units of ZTCN using security procedures A_S and A_C respectively. The details are given in equation (4).

$$T = \begin{cases} pys\ or\ vis\ \in A_S & True \\ pyc\ or\ vic\ \in A_C & True \\ None & False \end{cases} \quad (4)$$

The development of ZTCN and the "no trust" security features lead in to the collection of video segments $V(n1), V(n2) \dots \dots \dots V(nm) \in VD^C$

$$V(n) = fr(r, g, b) \quad (5)$$

$$VD^C = fr\big(V(n1), V(n2) \dots \dots \dots V(nm)\big) \quad (6)$$

As given in equations (4)→(6), the video data are collected and managed as a set of RGB intensity values VD^C . Each video collected in to client machine shall be considered based on the given design to initiate data distribution procedure, P1. Procedure P1 illustrates the video data distribution principles using uniform data distribution model. In this case, each video data block is evaluated for extracting RGB values. As given below, the initial and final RGB intensity values are calculated to find the mean value and variance respectively.

$B(a) = f1(ri, gi, bi): Initial\ data\ block$

$B(b) = fn(ri, gi, bi): final\ data\ block$

Based on application-specific video files, the data collected at each system is classified and flagged in to two categories such as real-time and non-real-time classes. This classification can be executed by activating the flags (0 or 1).

P1: Video Data Block Distribution Model

Input: $\boldsymbol{VD^C}$

Output: $\boldsymbol{VM(Di, Bi) \longrightarrow VM^{Ci}}$

Begin

1: Call uniform VM resource density function

$$\boldsymbol{Population\ Density = n * m}$$

$\boldsymbol{n}$: $\boldsymbol{Number\ of\ clients}$

$\boldsymbol{m}$: $\boldsymbol{Number\ of\ VM\ clients}$

1.2: Call video data distribution function

$$\boldsymbol{VM(Di, Bi)} = \begin{cases} \boldsymbol{B(a) + B(b)} & \boldsymbol{Mean} \\ \boldsymbol{\sqrt{\dfrac{(B(b) - B(a))^2}{VM(ci, i)}}} & \boldsymbol{Variance} \\ \boldsymbol{0} & \boldsymbol{None} \end{cases}$$

2: Get $\boldsymbol{VM(Di, Bi)}$ at each VM, m count

3: Check total $\boldsymbol{VM(Di, Bi)}$ distributions $\in \boldsymbol{VD^C}$

4: Check $\boldsymbol{mode\ flag}$: $\boldsymbol{VM(Di, Bi)}$←[0:1]

Define 0: real-time protocol, 1: non-real-time protocol

5: Call P2 if $\boldsymbol{flag}$: $\boldsymbol{VM(Di, Bi)}$→1

6: Call P3 if $\boldsymbol{flag}$: $\boldsymbol{VM(Di, Bi)}$→0

7. Redo

End

P4: Centralized Video Data Decryption Model

Input: $\boldsymbol{eB\big(VM(Di, Bi)\big)}$: $\boldsymbol{eb(VM\_Bit(Di, Bi))}$

Output: $\boldsymbol{VM(Di, Bi)}$: $\boldsymbol{VM\_Bit(Di, Bi)}$

Begin

1: Invoke data forwarding process in all $\boldsymbol{VM^{Ci}}$

2: Retrieve $\boldsymbol{c(m, i)}$←VM block cipher buffer∀ $\boldsymbol{VM(Di, Bi)}$: $\boldsymbol{VM\_Bit(Di, Bi)}$

3: Call AES (256 Bits) and RC4 (256 Bits) Decryption function

3.1:$\boldsymbol{VM(Di, Bi) = dB(c(m, i)^{Ki}) - V\_Hash(i)}$

3.2:$\boldsymbol{VM\_Bit(Di, Bi) = R_k \oplus c(m, i) - V\_Hash(i)}$

4: Initiate redistribution and defragmentation of

$VM(Di, Bi)$
5: Store the decrypted video data blocks in cloud buffer
6: Redo
End

P2: Distributed VM Centric Block Cipher Model: Non-Real-Time

Input: $VM(Di, Bi)\ at\ VM^{Ci} \in VD^{C}$: $flag: VM(Di, Bi) \rightarrow 1$
Output: $eB(VM(Di, Bi))$
Begin
1: Get all $VM(Di, Bi) \longrightarrow VM^{Ci}$
2:Call content aware AES (256 bits) in all VM^{Ci} : 14 Rounds
2.1: For all, $VM(Di, Bi)$ do encryption
$c(m, i) = eB(VM(Di, Bi))^{Ki} + V\_Hash(i)$
2.2:Set $c(m, i): i = 1, 2, \ldots n$ ($received\ video\ blocks\ in\ VM^{Ci}$)
3: Set local VM block cipher buffer → $c(m, i)$
4: Assign all $c(m, i)$ in to sorted buffer memory
5: Redo and flush memory for each block cipher execution
End

P3: Distributed VM Centric Stream Cipher Model : Real-Time

Input: $VM\_Bit(Di, Bi)\ at\ VM^{Ci} \in VD^{C}$: $flag: VM(Di, Bi) \rightarrow 0$
Output: $eb(VM\_Bit(Di, Bi))$
Begin

1: Get $VM\_Bit(Di, Bi) at\ VM^{Ci}$
2: Call RC4 with random key generation function
2.1: set $l = k = 0$
2.2: Call random key stream production
2.2.1: $l = (l + 1)\%256\ and\ k = (k + r(i))\%256$
2.2.2: swap → $r(i), r(j)$
3: Get random key for encryption phase, R_k
4: Execute, $c(m, i) = R_k \oplus VM_{Bit(Di,Bi)} + V\_Hash(i)$
5: Set local VM block cipher buffer → $c(m, i)$
6: Assign all $c(m, i)$ in to sorted buffer memory
7: Redo and flush memory for each block cipher execution
End

As denoted, stream cipher models are more suitable for real-time security applications than non-real-time applications. On the scope, the VMs configured in each physical machine contain both block cipher tools and stream cipher tools to be initiated. As discussed, the video data transmitted in to cloud environment has to be indicated under either real-time or non-real-time class. The flag shown in procedure 2 and 3 indicates the video traffic model (either guaranteed protocol format or best effort protocol format).

According to flag indications, the proposed model calls either procedure 2 or procedure 3 in VMs. This novel approach supports both types of video encryption techniques in a distributed condition. This solution reduces computation overload and time complexity issues in each VM. To improve the security features of video data transmission in cloud environment, this proposed method uses SHA-3 (256 bits) for authenticating each block of data. Consequently, the production of authenticated secret video data blocks is effectively handled.

At the end, AES decryption and RC-4 decryption functions are called at centralized cloud point. In this proposed model, the authenticated and encrypted video blocks are collected in the centralized cloud point. As the significance to hold the secret data in secure cloud storage, the proposed SRVM introduces cloud centric data recovery (decryption) procedures. On the crucial benefits of this proposed idea, the video data decrypted in cloud storage is delivered to users based on requests and privileges. The details of cloud-centric data decryption functions are illustrated in procedure 4.

The proposed SRVM model significantly enhances the security, encryption efficiency, and computational scalability of cloud-based video data management compared to existing models such as BMDS, FFOE, and QMEE. It is hypothesized that employing a dual-mode encryption approach—utilizing AES-SHA for non-real-time data and RC-4-SHA for real-time data—provides superior data confidentiality and integrity over single-mode encryption techniques.

Comparing to other existing model, the proposed SRVM has been improved with multi-modal confidentiality mechanisms, distributed security models, centralized decryption models and regulated video data distribution models. In this regard, this method performs significantly than other techniques. The experiment details and testbed scenarios are given in section 4.

4. EXPERIMENTS AND RESULTS

Establish a controlled cloud testbed to implement and evaluate the SRVM model's dual-mode encryption and ZTCN authentication against

baseline models using standardized performance metrics for replicable research.

The proposed SRVM functions are developed under zero trust conditions. In this experiment, trust values are calculated at run-time by validating the events raised from various cloud nodes. The implementation setup contains totally 35 VMs that are sparsely distributed among 10 physical machines. On the other side, virtual servers are created (5) at the backend. The proposed SRVM

and the existing techniques such as (E-1: BMDS [8]; E-2: FFOE [10]; E-3: QMEE [21]). The implementation of both proposed and related techniques is executed using cloud simulator (platform) and python (internal security functions). The performance metrics taken to experiment the systems are excessive computation load, encryption and decryption time (milliseconds, ms), decryption time (ms), security complexity factor and total number of successful attacks on video data. In these parameters, encryption and decryption duration are calculated for both block cipher techniques and stream cipher techniques. The existing techniques such as (E-1: BMDS; E-2: FFOE; E-3: QMEE) are providing distributed encryption techniques using various approaches. In this connection, the proposed technique has been designed with dual-encryption modes on video security measures.

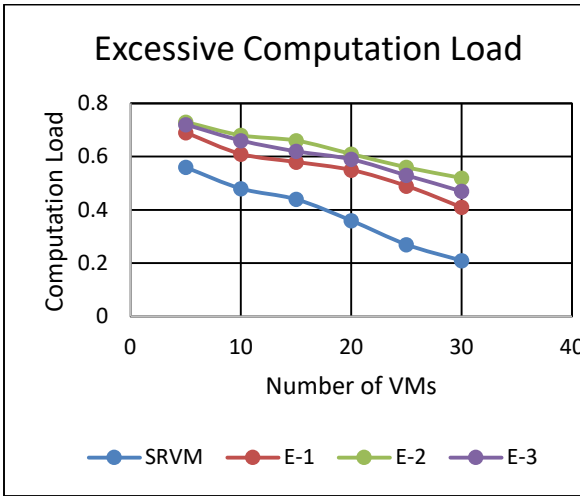

Figure 3. Computation Load

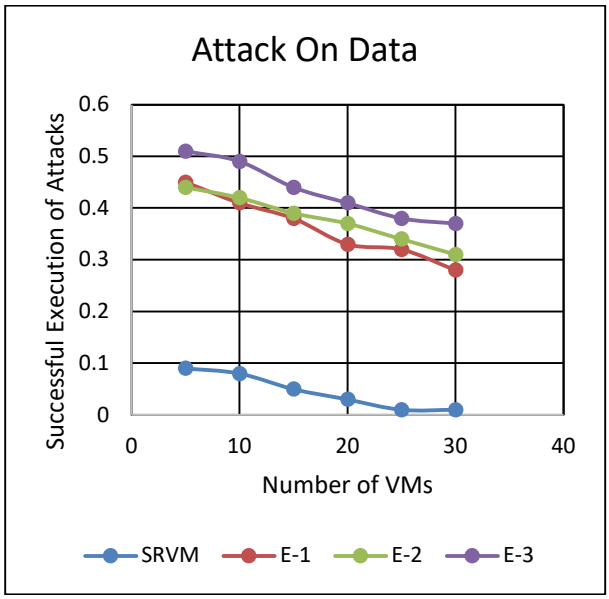

Figure 4. Successful Attacks On Data

Performance evaluation starts with the metrics such as excessive computation load and attack management quality of relevant security systems. Figure 3 illustrates the excessive production of computation load in the systems. In this evaluation, the existing and proposed SRVM are implemented with cloud platforms. However, the proposed SRVM has been provided with distributed trust model function and dual-encryption model. These are suitable for managing even load distribution on both real-time and non-real-time encryption phases [22][23].

At the same time, the BMDS has been designed with distributed authentication solutions to protect video data. Compared to SRVM, BMDS has little more computation overhead as it fails to classify video data modes. In the same case, FFOE has significant hike in additional overhead production during complex video data.

At the same time, the overhead produced by QMEE has the ability to distribute the video data among edge point and reduces the overload compared to FFOE. At the same time, it is not optimal for combining both real-time and non-real-time video data security models [24][25].

Figure 4 shows the positive attempts of attacks to breach the video data confidentiality. In this experiment, data breaching and key extraction attacks are initiated to validate the efficiency of security systems. In this experiment, the proposed

model has minimal attack impact rate than other systems.

As SRVM uses completely distributed VM based encryption (AES, SHA and RC-4) models, the attacks are reduced on data. In addition, the events raised from multiple systems are validated under zero trust scheme. On the other side, BMDS produces optimal stability against attacks as it has strong distributed authentication policies. However, FFOE and QMEE has limited security stability on data confidentiality issues.

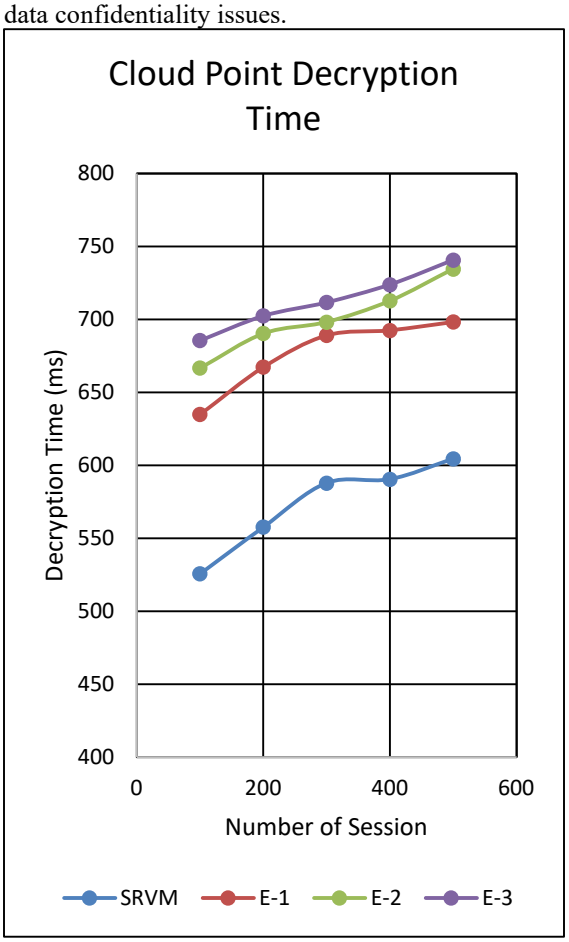

Figure 5. Decryption Time

The time taken to decrypt the video data is an important factor as it is indicated in figure 5. As shown in figure 5, total time taken to decrypt video data is minimal for proposed SRVM than other systems. However, the lack of distributed properties and optimal cloud data collection schemes make the existing techniques weak in terms on decryption time quality. Figure 6 and 7 show the block encryption and stream encryption phases of security models.

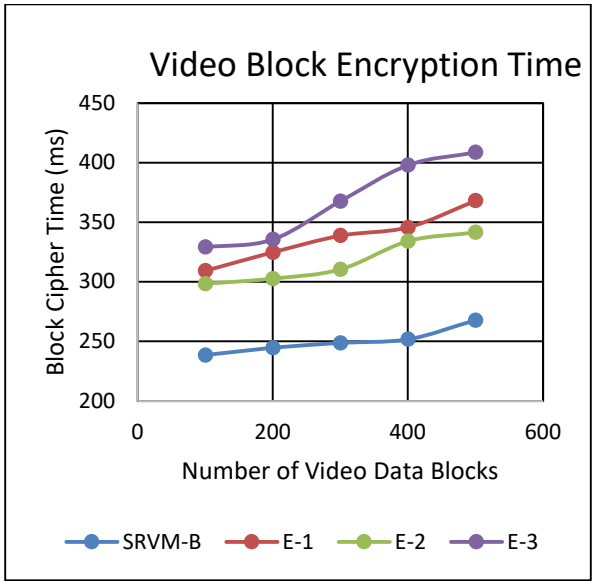

Figure 6. Video Block Encryption

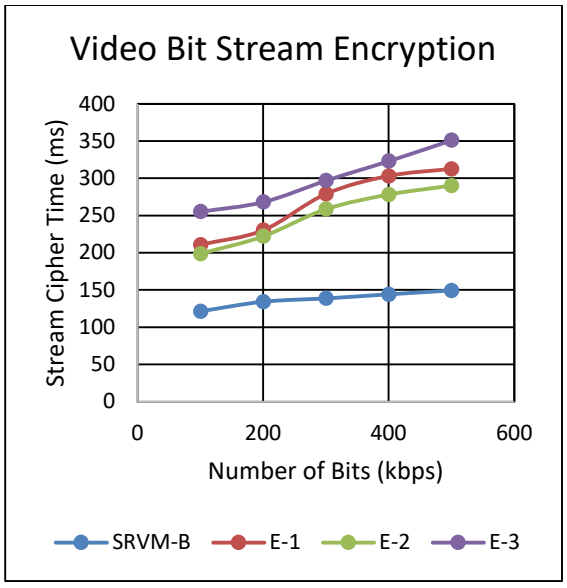

Figure 7. Video Bit Stream Encryption

As the existing models are not enabled with dual-encryption techniques under distributed VMs, the improper data handling effort leads in to maximum time consumption rate. In this experiment, proposed SRVM secures the video data (real-time and non-real-time) contents using AES-SHA and RC-4-SHA fusions respectively. Other techniques are using single mode security schemes such as blockchain and edge-based cryptography models. The experiment has been evaluated for changing

number of blocks and bits over the sessions. The time taken to encrypt both real-time and non-real-time video data shows the optimality and response behaviour of security models.

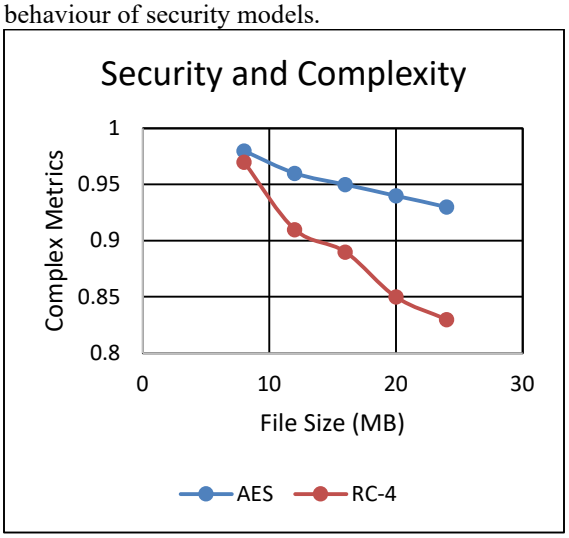

Figure 8. Complexity and Stability

Figure 8 depicts the security-based stability comparison between block cipher and stream cipher techniques (AES and RC-4). As the number of video file size increases from 5 Mega Bytes (MB) to 30 MB, the stability ratio of protection falls gradually. In this experiment, AES has more strong security complexity than RC-4 algorithms. The reason for these observations is that AES has multiple rounds of key generation and complex encryption strategy than bit-wise RC-4 model. At the same time, AES is not a suitable encryption model for time-sensitive (real-time) data transmission that makes delay and it is not acceptable.

On the other hand, the energy consumption rate of proposed SRVM and existing techniques are shown in table 3.

Table 3. Energy Consumption Rate (Joules)

Number of Cloud Blocks	SRVM-B	E-1	E-2	E-3
5	10.56	13.44	2.69	15.62
10	11.67	17.52	4.12	18.91
15	14.67	19.11	5.98	20.26
20	17.94	21.59	9.34	23.58
25	20.13	23.53	1.45	28.47
30	21.41	25.42	3.78	29.47

As given in table 3, the energy consumption rate of SRVM falls between 10.56 J and 21.41 as the video file size increases. Similarly, the existing techniques have more energy consumption rate than the proposed model as they don't have proper video data distribution models, VM based encryption solutions. In addition, the existing techniques are using common solution for both real-time and non-real-time data encryption platforms. In this regard, the proposed model has an advantage to optimize the energy utilization during the execution phases of AES and RC-4 procedures.

5. CONCLUSIONS

The importance of data confidentiality in cloud-based video data management systems is highly recognized at various multimedia applications. In this field, the involvement of both time sensitive and offline video data management models are growing day by day. The existing models were identifying video data encryption techniques under single mode (either block cipher or stream cipher). On the scope, the proposed SRVM had been developed to create distributed dual-model data encryption techniques to secure both real-time and non-real-time data in cloud. In this regard, this proposed model was implemented with VM assisted AE-SHA and RC-4-SHA procedures to enable authenticated security principles in ZTCN. The performance of proposed SRVM was proved against the existing techniques such as BMDS, FFOE and QMEE through notable metrics in cloud testbed. In future, this work has been improved with more accurate and multi-modal security solutions with respect to video qualities.

The proposed SRVM model introduces a novel dual-model encryption approach, combining block cipher (AES-SHA) for non-real-time data and stream cipher (RC-4-SHA) for real-time data, ensuring comprehensive security across different video data types. By leveraging virtual machines (VMs), the model optimizes encryption efficiency, minimizing computational overhead while maintaining high security standards. Comparative performance evaluations demonstrate that SRVM outperforms existing models such as BMDS, FFOE, and QMEE in terms of security, speed, and resource utilization within a cloud testbed environment. Additionally, the integration of Zero Trust Cloud Network (ZTCN) principles enhances trust verification and identity authentication, mitigating risks associated with unauthorized access. This advancement significantly improves security in multimedia cloud applications, making it an ideal

solution for healthcare, online education, and e-commerce video services. Furthermore, the lightweight encryption techniques employed in SRVM enhance cloud resource efficiency, optimizing video storage and transmission processes. Looking ahead, future improvements may focus on AI-driven adaptive encryption and multi-modal security solutions, further refining data protection mechanisms based on video content sensitivity and quality requirements.

REFERENCES

[1]. Sarkar S, Choudhary G, Shandilya SK, Hussain A, Kim H. Security of zero trust networks in cloud computing: A comparative review. Sustainability. 2022 Sep 7;14(18):11213.

[2]. Adahman Z, Malik AW, Anwar Z. An analysis of zero-trust architecture and its cost-effectiveness for organizational security. Computers & Security. 2022 Nov 1; 122:102911.

[3]. Li S, Iqbal M, Saxena N. Future industry internet of things with zero-trust security. Information Systems Frontiers. 2022 Mar 10:1-4.

[4]. García-Teodoro P, Camacho J, Macie-Fernández G, Gómez-Hernández JA, López-Marín VJ. A novel zero-trust network access control scheme based on the security profile of devices and users. Computer Networks. 2022 Jul 20; 212:109068.

[5]. Tang F, Ma C, Cheng K. Privacy-preserving authentication scheme based on zero trust architecture. Digital Communications and Networks. 2023 Feb 4.

[6]. Saleem M, Warsi MR, Islam S. Secure information processing for multimedia forensics using zero-trust security model for large scale data analytics in SaaS cloud computing environment. Journal of Information Security and Applications. 2023 Feb 1; 72:103389.

[7]. Awan SM, Azad MA, Arshad J, Waheed U, Sharif T. A Blockchain-Inspired Attribute-Based Zero-Trust Access Control Model for IoT. Information. 2023 Feb 16;14(2):129.

[8]. Taloba AI, Elhadad A, Rayan A, Abd El-Aziz RM, Salem M, Alzahrani AA, Alharithi FS, Park C. A blockchain-based hybrid platform for multimedia data processing in IoT-Healthcare. Alexandria Engineering Journal. 2023 Feb 15; 65:263-74.

[9]. Lee D, Park N. Blockchain based privacy preserving multimedia intelligent video surveillance using secure Merkle tree. Multimedia Tools and Applications. 2021 Nov; 80:34517-34.

[10]. Kumar M, Aggarwal J, Rani A, Stephan T, Shankar A, Mirjalili S. Secure video communication using firefly optimization and visual cryptography. Artificial Intelligence Review. 2022 Apr 1:1-21.

[11]. Swaraja K, Madhaveelatha Y, Reddy VS. A secure method of optimized low complexity video watermarking. ARPN J. Eng. Appl. Sci. 2015 Mar;10(4):1822-7.

[12]. Benisha RB. An efficient Sheep Flock Optimization-based hybrid deep RaNN for secure and enhanced video transmission quality. Neural Computing and Applications. 2023 Jan 6:1-6.

[13]. Ahamad R, Mishra KN. Hybrid approach for suspicious object surveillance using video clips and UAV images in cloud-IoT-based computing environment. Cluster Computing. 2023 Feb 17:1-25.

[14]. Zhao H, Feng N, Li J, Zhang G, Wang J, Wang Q, Wan B. VM Performance-aware Virtual Machine Migration Method Based on Ant Colony Optimization in Cloud Environment. Journal of Parallel and Distributed Computing. 2023 Feb 15.

[15]. Alhayani BS, Hamid N, AL mukhtar FH, Alkawak OA, Mahajan HB, Kwekha-Rashid AS, İlhan H, Marhoon HA, Mohammed HJ, Chaloob IZ, Al-Hayat A. Optimized video internet of things using elliptic curve cryptography-based encryption and decryption. Computers and Electrical Engineering. 2022 Jul 1; 101:108022.

[16]. Suresh M, Sam IS. Optimized interesting region identification for video steganography using Fractional Grey Wolf Optimization along with multi-objective cost function. Journal of King Saud University-Computer and Information Sciences. 2022 Jun 1;34(6):3489-96.

[17]. Wang L, Ji H. A Watermarking Optimization Method Based on Matrix Decomposition and DWT for Multi-Size Images. Electronics. 2022 Jun 28;11(13):2027.

[18]. Gupta BB, Yamaguchi S, Agrawal DP. Advances in security and privacy of multimedia big data in mobile and cloud computing. Multimedia Tools and Applications. 2018 Apr; 77:9203-8.

[19]. Yin H. Public security video image detection system construction platform in cloud computing environment. Computational

Intelligence and Neuroscience. 2022 Feb 10;2022.

[20]. Liu JK, Au MH, Susilo W, Liang K, Lu R, Srinivasan B. Secure sharing and searching for real-time video data in mobile cloud. IEEE Network. 2015 Mar 24;29(2):46-50.

[21]. Liu Z, Qiao B, Fang K. Joint optimization strategy for QoE-aware encrypted video caching and content distributing in multi-edge collaborative computing environment. Journal of Cloud Computing. 2020 Dec; 9:1-5.

[22]. Dinh HT, Lee C, Niyato D, Wang P. A survey of mobile cloud computing: architecture, applications, and approaches. Wireless communications and mobile computing. 2013 Dec 25;13(18):1587-611.

[23]. Tanga O, Akinradewo O, Aigbavboa C, Thwala D. Usage of Cloud Storage for Data Management in the Built Environment. In Advances in Artificial Intelligence, Software and Systems Engineering: Proceedings of the AHFE 2021 Virtual Conferences on Human Factors in Software and Systems Engineering, Artificial Intelligence and Social Computing, and Energy, July 25-29, 2021, USA 2021 (pp. 465-471). Springer International Publishing.

[24]. Thamrin A, Xu H. Cloud-Based Blockchains for Secure and Reliable Big Data Storage Service in Healthcare Systems. In2021 IEEE International Conference on Service-Oriented System Engineering (SOSE) 2021 Aug 23 (pp. 91-99). IEEE.

[25]. Suresh P, Keerthika P, Sathyamurthy V, Logeswaran K, Sentamilselvan K, Sangeetha M, Sagana C. Cloud-based big data analysis tools and techniques towards sustainable smart city services. In Decision support systems and industrial IoT in smart grid, factories, and cities 2021 (pp. 63-90). IGI Global.