JOURNAL OF CYBERSECURITY

Journal of Cybersecurity, 2023, 1–10
https://doi.org/10.1093/cybsec/tyad012
Research paper

Research paper

Realizing credible remote agricultural auditing with trusted video technology

Redowan Mahmud[1,*], Joshua D. Scarsbrook[1], Ryan K. L. Ko[1], Omar Jarkas[1], Josh Hall[2], Stuart Smith[2] and Jonathan Marshall[2]

[1]School of Information Technology and Electrical Engineering, The University of Queensland, St Lucia, QLD 4072, Australia and [2]Bondi Labs—Augmented Intelligence, South Melbourne, VIC 3205, Australia

*Correspondence address. Room 326, 314 New Technologies, Curtin University Campus, Bentley, Western Australia 6102, Australia. E-mail: md.redowan.mahmud@gmail.com

Received 13 July 2022; revised 26 March 2023; accepted 19 May 2023

Abstract

The conventional approaches of auditing agricultural commodities from the production and transportation level to the retailers and consumers often get obstructed by the lack of human resources, delayed response, and high frequency of location updates—resulting in poor quality and safety compliance. Its digital transformation, known as remote auditing, could address these limitations to a greater extent; however, it is still subject to diverse cyberattacks, including tampering with the video streams provided for verification. Since a detailed and concurrent forensic examination of videos during remote auditing significantly increases the computational burden on the network and infrastructure, alternative or complementary solutions should be developed. This paper outlines the technical feasibility of applying digital signatures over live video streams as a way to authenticate the source during remote auditing and thus contributes to limiting the scope of potential cyber threats. It proposes design options for realizing the authentication process with trusted computing technologies at different phases, from signing the videos to transmitting them through unreliable networks. A reference prototype is also developed based on the proposed end-to-end design to quantify the performance of trusted remote agricultural auditing in terms of the frame signing time, attack resistance, and resource overhead.

Key words: remote auditing, smart agriculture, trusted computing, secure key exchange, video attestation

Introduction

Food safety is considered to be one of the major concerns in recent times. According to US Food and Drug Administration (FDA), incidents related to food safety violations increased 33% globally only in 2019–20 [1]. That is why agricultural auditing is now, more than ever, a process to be encouraged. It has already been adopted widely as an independent evidentiary basis to establish trust among different beneficiaries and stakeholders of agri-business. Agricultural auditing can take place at any phase of the value chain and should focus not only on the products but also on the workforce dealing with them [2]. For example, the inspection of plants and livestock for detecting pest attacks and diseases is necessary during production. Similarly, monitoring meat-cutting workers at the processing belts is crucial to verify whether they are following the recommended procedure. Considering such a dimension and the potential impact of agricultural auditing on food safety, it must be continual and accurate.

Conventional agriculture auditing approaches, such as on-site visual inspection, require extensive human resources to manage checklists and regulatory compliance reports across multiple geographically distributed or remote areas, incurring high operational expenditure. This problem further intensifies when the travelling expenses are added [3]. On the other hand, the conversion of manual inspection data to digital and their integration from different sources require additional time that significantly affects the responsiveness of the auditing process. Due to individual preferences, this approach also faces severe performance variation, which is not recommended when food safety is the primary concern [2]. Therefore, the actual cost of auditing the agricultural value chain under conventional settings is substantial. Additionally, there can be uncertain events like the Covid-19 pandemic when the on-site auditing gets halted, resulting in elongation. Because of these reasons, a majority of the farms and government authorities are not willing to support frequent agricultural auditing and thus fail to ensure robust food safety.

A recent advancement in the space of agricultural auditing is the use of information and communication technology that leads to a digital transformation of the conventional approach, known as remote agricultural auditing. It enables online tools and services such as video conferencing, email, and telephone to share and collect the auditing evidence without an auditor being physically present at the site [4]. Additionally, there have been a notable number of research works in the literature that discuss the motivation for promoting such technology from different perspectives. For example, the unification of remote sensing, crop modelling, and economics is considered to be a building block for automated risk assessment in the agricultural domain [5]. Similarly, remote agricultural auditing augmented with artificial intelligence is expected to bring revolution in precision agriculture [6], energy efficient farming [7], and optimized land and water usage [8]. Nevertheless, since remote agricultural auditing saves time and money and provides location-independent data access, its market and necessity are gradually increasing. Several large agricultural farms, including Quality Meat Scotland (QMS) and Scottish Quality Crops (SQC), have already been shifted to remote auditing in 2020. Its global market size is now worth around 1.16 billion, which is also expected to reach 3.03 billion by 2026 [9].

Video streaming is one of the foundation blocks for remote agricultural auditing [10]. However, like other electronic services, it is subject to diverse cyberattacks, including tempering and repudiation. According to a survey conducted by F-Secure (a cybersecurity solution provider), 40% of the respondents indicated such security incidents related to video conferencing while participating in a remote agricultural product showcasing in 2022 [11]. These malicious actions are now more accessible with ready-to-use video editing software and web plugins like Adobe Photoshops that can perform copy-move, splicing, resampling, and deep fake in real-time and create falsified videos [12]. As a result, the volume of cyberattacks against the food and agriculture sector is increasing rapidly, making it the third most vulnerable industry [13]. Nevertheless, the consequences of forged video streams, particularly in remote auditing, could be catastrophic in regard to food safety compliances and affect the consumer–producer trust. Due to these reasons, despite having significant potential, many still consider remote auditing a risky approach.

The cyber-security-related issues of video stream-based remote agricultural auditing can be addressed by inspecting each frame. However, a detailed digital forensic study is required to identify frame-wise manipulation of video streams, which is time-consuming, resource-intensive and can slow down the auditing process [14]. In this case, the verification of origin for the video streams can be a feasible alternative. However, with the torrent of videos provided as the auditing evidence, it is challenging to authenticate the source, especially when they are captured by unlisted devices and transmitted through unreliable communication channels [15]. Due to the lack of origin tracing, any footage tampering in the intervening time also becomes difficult to verify and alert the auditor regarding the discrepancy. Many research works advise extending the concept of cryptographic video authentication to resolve this issue; however, a detailed outline of applying end-to-end digital signatures to verify auditing videos is yet to be studied.

By leveraging Trusted Computing (TC), this work aims at bridging the gap between the security requirements of remote auditing and the current practices of applying digital signatures in video streams. TC refers to a set of technical solutions for addressing the security problems in digital operations through hardware integration and software enhancement [16]. The proposed design options synthesize TC-enabled digital signatures at different phases of remote auditing, ranging from signing the video frames as soon as they are generated to sharing the cryptographic keys between the end-points and transmitting video frames to the data sink. Thus, it facilitates a trusted video technology that ensures credible agricultural product inspection through robust security, reliability, and integrity. The major contributions of this work are:

- A feasibility study of TC and its limitations restricting the realization of a credible remote agricultural auditing.
- A conceptual integration model of digital signatures, TC and state-of-the-art computing, and networking technologies that ensures reliability and integrity in video signing, key sharing, and stream transmission.
- A end-to-end prototype based on the proposed functional layouts that demonstrates the performance of a remote agricultural auditing system in terms of video frame signing, overhead management, and attack resistance.

The rest of the paper is organized as follows. ‘Related work’ section highlights the literature aiming at remote auditing. ‘Trusted computing and its gaps’ section discusses the basic concepts of TC and its scope of improvements for remote auditing. ‘Devised remote auditing process’ section discusses the phases within a remote auditing process and design options for trusted video technology. ‘Attack Scenarios’ section outlines how the proposed design principles mitigate the effect of potential security threats in remote auditing. The prototype system, along with performance evaluation, is presented in the ‘Performance evaluation’ section. Finally, ‘Conclusion’ section concludes the paper with future directions.

Related work

As discussed earlier, many research initiatives in the literature signify the motivation for enabling remote agricultural auditing. This section explicitly focuses on enlisting its technical aspects and systematically articulates them. Illustratively, video authentication using digital signatures is considered a potential solution to make remote auditing secure and reliable, which has also been consistently evolving. Kang et al. in ref. [17] proposed a low-complexity data origin authentication scheme for video streams by relaxing the necessity of separately managing different secret keys for Keyed-Hash Message Authentication Code (HMAC). Their solution automates and circulates a secret key table prior to initiating communication among the participants and provides support for reconfiguring the secret key table during transmission. Thus, it overcomes the burden of managing keys for multiple senders and receivers. In another work [14], passive object-based wavelet decomposition is discussed for video authentication. It defines a texture descriptor using a forged keyframes localization algorithm to verify whether a legitimate source creates the video. Similarly, in ref. [18], the feasibility of a video authentication solution using the spatio-temporal relationship among the contents is described. It not only verifies the source of videos but also certifies the integrity through a 128-bit message digest of variable length working as the fingerprint of the video.

Additionally, there is a notable number of research works where the integrity of videos is maintained by extending Blockchain. Illustratively, in ref. [19], Qiu et al. highlighted the use of Blockchain to manage public key hash and source identity while facilitating fast authentication for collaborative video data forwarding in driverless vehicular environments. Alternatively, Xu et al. in ref. [20] discussed the potential of Edge computation-based Blockchains to deal with the visual layer attacks such as false frame injection in the video streams. Similarly, in ref. [21], Jamil et al. discussed the adoption of IoT-Blockchains for controlling a greenhouse environment with proven integrity. In another work, Ibrahim et al. [22] proposed a Blockchain framework with a automated data verification and role-based access control method for securing digital services, which is also transferable to remote auditing. Moreover, in ref. [12], Patil et al. illustrated how Blockchain could mitigate the effect of deep fake in video data by listing the granular level details of frames and making them available for cross-verification in real-time. Similarly, in another work [23], Blockchain has been exploited to protect the indexes of video frames generated on-site from tempering. It also enables a decentralized smart contract for the end-points to verify the video frames transmitted through unreliable channels.

There exists some other works in the literature that leverage Blockchain for secure sharing of the cryptographic keys used for video authentication. In ref. [24], Li et al. proposed an application model for video surveillance where the Blockchain has been used to provide the participating bodies, devices, and video streams with publicly accessible and verifiable unique identification numbers. In another work [25], Labbi et al. illustrated the structure of blocks within a chain that can be potentially used to share the public keys for video verification among the end-points with transparency. Similarly, in ref. [26], the use of Blockchain is presented for supporting registration, revocation, and mutual authentication not only between two devices but also between two communication interfaces.

In addition to focusing on video authentication and key sharing, several research works from the literature investigate reliable transitions for video streams through unreliable communication channels. For instance, a video transmission framework is proposed in ref. [27] that can allow communication between two legitimate bodies only by verifying their public-key certificates and private keys. It performs this operation through a specialized controller within the network. In ref. [28], another video conferencing system is outlined that exploits a two-phase routing based on Software-defined Networking (SDN) principles while transmitting high-quality videos between geographically remote end-points. On the other hand, in ref. [29], scalable video coding is adopted to encode data streams at various bitrates so that they can be modified at run-time if the network condition changes due to resource shortage and security threats. Thus, this solution expects to deliver the video frames to the sink with the least possible packet drops, even when transmitted using a less reliable medium.

As Table 1 presents that most of the existing works fail to facilitate video origin verification, cryptographic key sharing integrity, and secure video transmission simultaneously. Moreover, they predominantly depend on cryptographic primitives, which barely exploit the concepts of TC. This work addresses these limitations and paves the way for building a credible remote audit by encapsulating TC-enabled digital signatures with consortium/private Blockchain and a sliced network. The proposed design principles can also be translated to end-to-end prototype using existing networking practices.

Trusted computing and its gaps

TC refers to open standards and specifications that ensure critical data and system protection through secure authentication, strong machine identity, and network integrity [30]. It is patronized worldwide by the Trusted Computing Group[1], a not-for-profit organisation operating since 2003. TC-enabled technologies such as Trusted Platform Module (TPM) and TCG Software Stack (TSS) prevent data, hardware, and other networked resources from being compromised, damaged, or stolen by malicious entities without affecting the privacy preservation rights of respective individuals or businesses. They can also collectively provide the following mechanisms to reduce ownership and operational cost for supporting accredited regulatory compliance.

- **Memory curtaining**: TC enables hardware-enforced memory isolation to restrict unprivileged access of programs to others' space containing sensitive information such as credentials, certificates, or encryption keys. Even it does not allow operating systems to access the programs' secure memory [30]. This hardware-centred feature of TC also eliminates the necessity to redevelop the existing system software, such as device drivers and kernels, to realize the program-level memory isolation and permits broader compatibility.
- **Remote attestation**: This mechanism of TC resists the malicious alteration within the software by generating a cryptographic certificate at a remote server that attests to the identity of all entities interacting with the software in a digital space [31]. In most cases, this identity is defined as a cryptographic hash, which significantly varies between programs, making them distinguishable. It can also avoid the transmission of sensitive data to a compromised system once determined.
- **Secure input–output**: By supporting secure input and output (i/o) operations, TC restricts the operations of snooping software in a digital system. It facilitates a secure data transfer path from input devices to program and program to output devices so that any intruder cannot get access to perceive how the system has responded to a particular event [30]. It also helps track whether the interaction with the system has been conducted with or without human intervention.
- **Sealed storage**: TC addresses the intractable key storage problem by facilitating sealed storage that restricts the decryption of sensitive information even if they are moved to any different machines other than where encrypted. This feature can also work with memory-curtaining and secure I/O to enforce that the encrypted information can only be read through its creator program and block others attempting to decrypt it.

Despite such innovative features, TC can fall short in providing comprehensive security to the underlying hardware and software systems due to the following reasons.

(1) *Static countermeasures:* TC practices hard trust that fails to maintain robustness in dynamic environments, especially when the interactions among users and digital systems change abruptly. As a result, the availability, reliability, and usability of TC-dependent systems also become a major concern when integrated with state-of-the-art computing and networking solutions.

(2) *Verification of implementations:* The verification of TC-enabled hardware depends on the manufacturer. Consequently, it is not possible for users to check whether the hardware possesses any

[1] https://trustedcomputinggroup.org/

Table 1: A summary of related work and their comparison

Work	Verifies origin	Applies TC	Key integrity	Reliable transfer
Kang et al. [17]	√			
Mizher et al. [14]	√	√		
Sowmya et al. [18]	√	√		
Qiu et al. [19]			√	√
Xu et al. [20]	√		√	
Patil et al. [12]	√			
Nikouei et al. [23]		√	√	
Li et al. [24]	√		√	
Labbi et al. [25]			√	
Tang et al. [26]	√		√	
Xie et al. [27]			√	√
Koryachko et al. [28]	√			√
Clayman et al. [29]	√			√
This work	√	√	√	√

back doors or undocumented features, potentially leaking sensitive information. Even when such defects are detected, users have a very limited option to enable the countermeasures.

(3) *Flawed attestation:* Although TC-facilitated remote attestation resists software on a computer from being altered without the knowledge of the computer's owner, it equally obstructs legitimate modifications due to black-box modelling. As a result, this feature of TC limits the interoperability of digital systems significantly.

(4) *Constrained overriding:* By restricting users' access to security credentials, TC can limit their digital rights. Through explicit isolation of memory, input and output data channels, it also eliminates the control of users to customize the security preferences. Moreover, these overriding constraints affect TC's adaptability, scalability, and performance in digital systems.

Consequently, these gaps in existing TC practices hinder its extension for developing a credible remote auditing process where the end-points are connected through many intermediaries. The rest of the paper discusses how TC can be integrated with state-of-the-art computing and networking concepts such as Blockchain (for ensuring integrity) and SDN (for reliable data transfer) to enable a trusted video technology for remote auditing.

Devised remote auditing process

Remote auditing becomes acceptable to each participating body when the associated process is secure and reliable. Therefore, it is required to outline how different computing and networking entities will interact with each other and how the security principles will be met during such interactions. The following sections devise these aspects in detail.

Remote auditing phases

Figure 1 denotes the information flow of a credible remote auditing process comprising three phases, as discussed below.

- **Signing of video frames:** The credible remote auditing process initiates by configuring the cameras to generate the video frames for product inspection. During this operation, depending on the communication standards (e.g. wired, wireless, or Bluetooth) and residual battery capacity of the cameras, the appropriate frame rate for the video streams is identified. Later, the video frames are made verifiable by signing them live with digital signatures. In this case, to expedite the signing operation and pursue the user-level security preferences, video frames can be organized into clusters, and instead of signing each frame, they are allowed to handle in batches.
- **Secure key exchange:** Only the signing of video frames will not be effective for credible remote auditing if the cryptographic keys used to make the digital signatures are compromised. The security of these keys should not only be ensured during the creation but also while exchanging among the end-points. Therefore, this phase of remote auditing aims at securing the key exchange for verifying the digital signatures on video frames. Its associated tasks include the privacy-preserving binding of public keys with respective entities or bodies, the assurance of integrity while transferring the keys through less reliable intermediate nodes and the initiation of respective countermeasures if necessary.
- **Transmission of video frames:** The performance of remote auditing is subject to the network facilitating the end-to-end transfer of video frames. Therefore, in an industrial environment, sufficient network bandwidth should be allocated to remote auditing services to ensure a predictable latency, which urges it to be real-time. Consequently, it is mandatory to control access to network resources as uncertain events such as packet drops or security attacks are more likely to occur, especially when the bandwidth is shared. This phase deals with such issues by creating secure video transmission channels, where the resources and security policies can be added on-the-fly.

The realization of devised remote auditing process requires a logical chain of digital signatures, working as an adhesive among video frames, TC, Blockchain, and SDN for secure authentication, key integrity, and reliable data transfer. However, while applying such signatures to any digital content: (i) the signing process must be secured, (ii) the access to the private key needs to be controlled, and (iii) the end-points should be notified which cryptographic key to trust proactively. Although TC can address the first two conditions by providing specialized hardware, there is still a chance of backdoor leaking of information and user-level security preferences, especially in the mobile and IoT platforms. Conversely, to meet the third condition, a secure end-to-end channel is required, which is often infeasible to ensure in the agricultural supply chain as the data need to be accessed by the stakeholders through different intermediate nodes while making a remote auditing cycle from consent to completion. Therefore, this work explicitly focuses on a hierarchical cryptographic key manage-

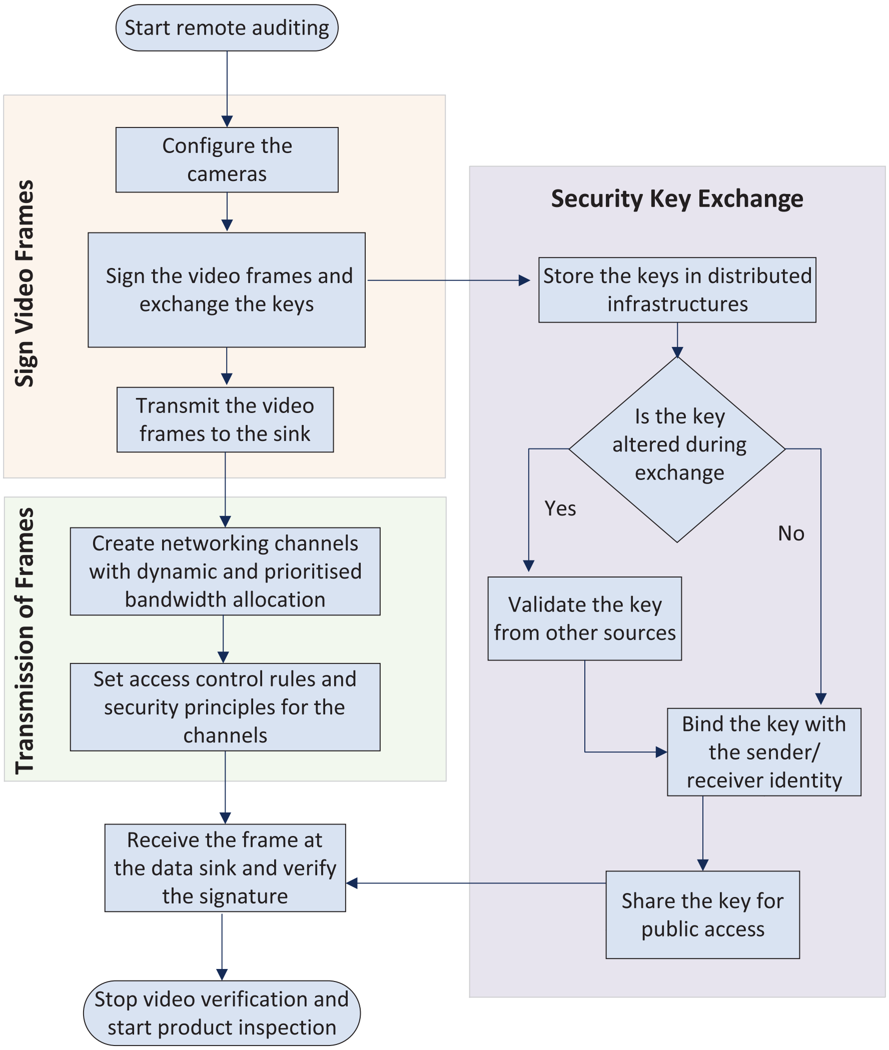
Start remote auditing
Sign Video Frames
Configure the cameras
Sign the video frames and exchange the keys
Transmit the video frames to the sink
Transmission of Frames
Create networking channels with dynamic and prioritised bandwidth allocation
Set access control rules and security principles for the channels
Receive the frame at the data sink and verify the signature
Stop video verification and start product inspection
Security Key Exchange
Store the keys in distributed infrastructures
Is the key altered during exchange
Yes
No
Validate the key from other sources
Bind the key with the sender/ receiver identity
Share the key for public access

Figure 1: Video verification phases in remote auditing.

ment technique to observe the security concerns in remote agricultural auditing.

Proposed hierarchical key management

Figure 2 depicts the proposed hierarchical key management architecture for remote auditing, which spans three different levels. The details are given below.

Device/user level

At this level, the video frame generator resides, which can be an automated camera or a headset operated by the workers of the agricultural production line. These devices are equipped with TC-enabled hardware to create **Kernel-Trusted Video Key** and sign the frames. As this key is stored in compliance with TC specifications, the hardware's kernel protects it from compromises in userspace, providing resistance against unprivileged access even through the host operating system. It also moves the video acquisition out of user mode and into the kernel, restricting the feeding of falsified frames into the transferring queue.

Moreover, at this level, users are also allowed to digitally sign their preferences, such as framing frequency and video-meta data, using the **User-mode Preference Key**. Although this key is stored in the user space, its generation, modification, and access need root privileges. However, once the video frame and user preferences are signed, they are encapsulated in a Data block and forwarded to the Data plane level via an auditing service-provided gateway. The gateway is also supported by the TC concepts so that its authenticity can be easily verifiable. Similarly, the hashes of both Data/User-level keys are transferred to a Blockchain infrastructure exploiting separate private network tunnels with end-to-end encryption to ensure an additional layer of security.

Data plane level

This level consists of networking devices such as gateway routers, switches, and hubs forwarding the data blocks generated at the Device/User level to the receiver. These devices are organized in clusters, and one SDN controller is allocated to each cluster to ensure fine-grained control over the data block transmissions through separate channels. Moreover, the initial recipient of a data block at this level is also responsible for digitally signing it with the **Trusted Video Transmission Key** and referencing the key to the respective SDN controller. Likewise, at the Data/User level, the components of this level will also have TC-enabled hardware to generate and store the keys

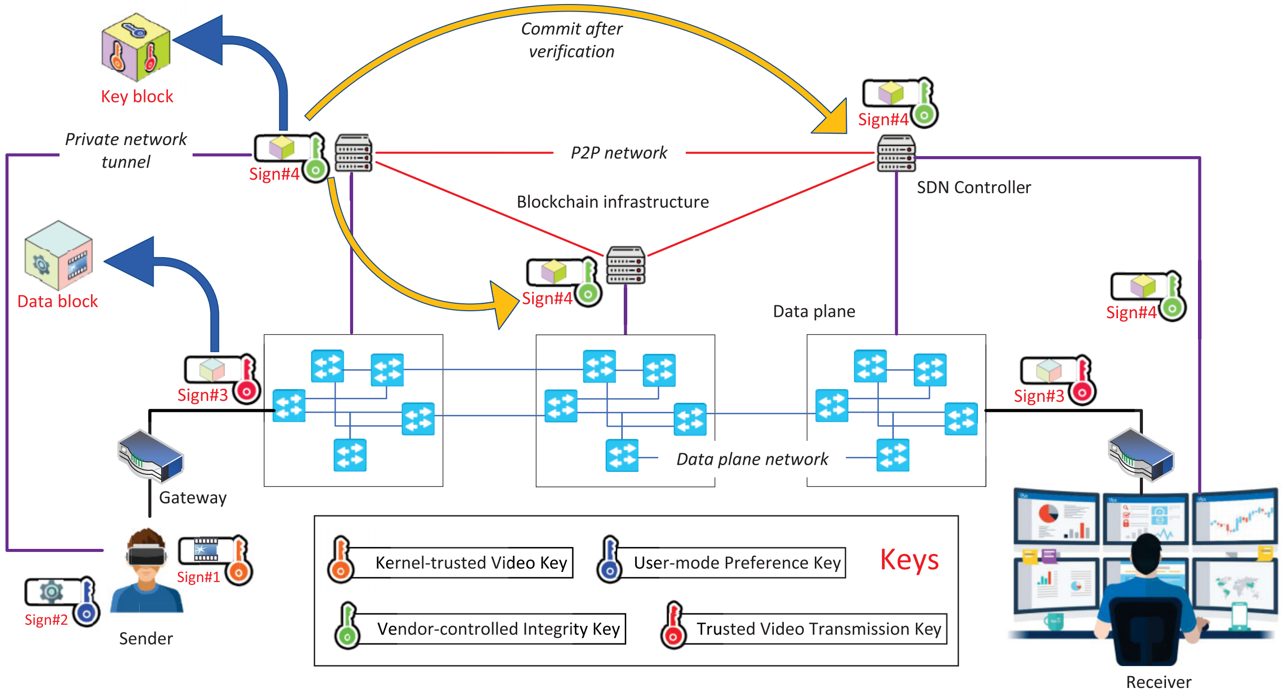

Figure 2: Key management in devised remote auditing process.

so that intruders cannot alter them, even when the data plane is comprehensively shared across multiple applications and services.

Blokchain infrastructure level

At this level, all SDN controllers reside, forming a permissioned Blockchain infrastructure through Peer-to-Peer (P2P) networking to store and share the cryptographic keys with integrity generated at the lower two levels. In this case, the SDN controller having the references of Kernel-Trusted Video, User-mode Preference, and Trusted Video Transmission Key initiates the block mining process. Once the mining is finished, the block comprising all the keys, known as the Key block, is forwarded to other controllers for verification. Such verification confirms that the keys are not altered during the exchange between the controllers. Moreover, the Key blocks are signed with a **Vendor-controlled Integrity Key** so that the corresponding Data block receiver can quickly identify the keys needed to verify the video streams and user preferences for any remote auditing operation.

Nevertheless, this key management architecture can address the existing limitations of TC, as noted in the 'Trusted computing and its gaps' section. For example, its span across multiple communication layers makes the overall architecture scalable to add vendor-specific dynamic security measures. The chain of digital signatures managed by separate entities enables the security of remote auditing even when backdoor leaking happens. Moreover, it not only practices remote attestation transparently but also provides users with overriding control of their preferences. Additionally, the proposed solution resists the use of any symmetric key signatures for remote auditing by enforcing the TPMs to generate asymmetric keys at each level. As Symmetric key signatures rely on a shared key for both signing and verification, it struggles to adapt to any changing security requirements or implement complex security protocols for remote auditing. It also fails to provide non-repudiation, which indicates the ability to prove that a particular video frame or message was sent by a specific sender. Hence, from this perspective as well, the proposed solution is capable of enhancing the credibility of remote agricultural auditing.

Attack scenarios

The implication of the devised remote auditing process and hierarchical key management can be notionally presented by discussing how it deals with diverse attack scenarios. A candidate set of such scenarios are discussed below.

Direct vendor attack

In the agricultural supply chain, the direct vendor attack refers to the alteration of trust in any third-party services playing a vital role in the overall system. By practising this, attackers can quickly get access to the devices generating videos and start tempering them. In most cases, such attacks are triggered by provoking users to install software for the devices from a source other than legitimate. The proposed architecture could resist this attempt by embedding the Kernel-Trusted Video Key to the devices directly through dedicated hardware [31]. However, in this case, the attacker can still alter the user's preferences, which can be a variation of the direct vendor attack. This attempt can be further mitigated by resource integrity checks or internal hosting of information, which is handled in the devised key management architecture through the User-mode Preference Key.

Network spoofing attacks

The current networking infrastructure, especially at the Data plane level, is not secure as it allows unreliable devices to forward data packets on an *ad-hoc* basis when the load for dedicated ones skyrocket. If an adversary gets access to any of such devices, its forwarded data packets can easily be compromised. This security concern further intensifies when the gateway becomes vulnerable and reprogrammed with malicious software. The attackers can also capture service-specific credentials from the gateways and start spoofing attacks from other networking devices [15]. The proposed key management architecture can restrict this attack by signing the data blocks with Trusted Video Transmission Key at the initiation of transmission. Since, in this architecture, the gateway is explicitly arranged by the remote auditing service providers, its trustability can be further verified through the embedded TC hardware. Moreover, the proposed solution does not allow the Device/User level to share the Kernel-Trusted Video and User-mode Preference Key through the gateway. As a result, there will be the least possibility of altering the video authentication process with a compromised gateway.

Key integrity attack

The integrity of public keys and their digital bindings with the actual entity can be ensured by enabling: (i) Key Immutability (implies that keys cannot be modified after it is created and applied); (ii) Key Authenticity (asserts that a legitimate source has generated the keys); and (iii) Access Control (defines that authorized entities can only access and facilitate the sharing of keys). The conventional Public Key Infrastructure (PKI) often fails to meet these aspects as it allows any Certification Authority (CA) to manage the digital identity of an entity if any root CA or intermediaries put it on the trusted list [20]. Hence, when the list is compromised, the whole authentication process collapses. However, the proposed key management architecture addresses this issue by establishing a Blockchain infrastructure with the SDN controllers to which the sender of the video streams and the data plane can directly forward the cryptographic keys.

This Blockchain infrastructure provides the remote auditing process with a P2P network and an immutable database leveraging permissioned consensus to realize group key management for video authentication. It binds each key with the actual identity using a Vendor-controlled Integrity Key, which is verifiable through open-source distributed ledger platforms such as Ethereum. Moreover, it controls access to the keys by explicitly conducting exchanges with trusted Blockchain participant nodes. Thus, the proposed architecture is expected to limit the scope of key integrity attacks to a great extent. Even if such attacks happen, this approach can mitigate the effect by applying the 51% rule of Blockchain technology.

Reverse engineering attack

In this attack, the adversaries obtain a copy of the software or services assisting the remote auditing and reverse engineering it. As a result, they can access any resources used for trusted video authentication and derail their operations. With no interdependency of the keys in signing videos, exchanging the keys, and transmitting the video frames, the mitigation of such an attack becomes even more complex [32]. By applying multiple keys at different hierarchical network levels and supporting cross-verification at each level, the proposed solution resists this attack. For example, the leaking of the Trusted Video Transmission Key cannot provide the adversaries with sufficient information to access or alter the Kernel-Trusted Video Key or User-mode Preference Key used for the verification of the video frames at the receiver end. Similarly, if the User-mode Preference Key is leaked from the Device/User level, the secure video transmission through the data plane will be barely affected.

Nevertheless, the aforementioned discussion indicates how the proposed solution renounces the accredited hypotheses of these attacks. However, to formally conduct the security analysis, the operational and administrative procedural components of the proposed solution need evaluation in terms of incident response plans, intrusion detection systems, and governance policies. Considering the nonexistence of any publicly available security analysis platform for remote auditing, such evaluation is tough to arrange. Therefore, this work focuses on evaluating the performance of the proposed solution along with its parametric security analysis on a custom-built experiment environment. Such an approach provides empirical evidence of the security analysis by quantifying the impact of the proposed solution in mitigating a cyberattack, which is often considered as an alternative to formal proof [33].

Performance evaluation

The performance of the proposed credible remote auditing process and the hierarchical key management architecture is evaluated in a real-world environment developed using the FogBus framework [34]. It is a lightweight software solution that integrates end-to-end digital systems incorporating IoT devices, local (e.g. Edge and Fog nodes) and remote (e.g. Cloud-based virtual machines) computing infrastructure. Moreover, its Application Programming Interfaces (APIs) are extensible to implement SDN-enabled data transmission across different communication and computational paradigms. The experimental setup is discussed below.

Experiments on real setup

In the experiment environment, Sony IMX219 image sensors are used as the data source. They are enabled to generate video frames at different frequencies and resolutions using a customised application. A Raspberry PI device is deployed in this environment to act as the service provider gateway for the camera sensors. For further simplicity in imitating the proposed solution, other data plane nodes and SDN controllers are also modelled using Raspberry PIs as they are easy to operate and provided with general-purpose input/output (GPIO) pins for interfacing with third-party hardware. Moreover, to establish a Blockchain within the experiment setup, the Raspberry PIs devices operating as the SDN controllers are positioned with the Hyperledger Fabric development environment. Later, the devices are made interconnected by enabling a Docker Swarm. Finally, the Hyperledger Fabric network is deployed on the swarms through the Docker stack so that the host Raspberry PIs can work as a part of a private Blockchain infrastructure. Nevertheless, Raspberry Pis use Micro SD cards to store the security credentials for digital signatures, which can be an easy target for attackers. Therefore, while setting the Raspberry PIs for experiments, they are interfaced with a TPM chip to make the overall environment compatible with the TC norms. Although the proposed solution is compatible with any available TPM version, the experiments are conducted on TPM 2.0 through OPTIGA TPMs manufactured by Infineon Technologies. Table 2 presents the details of this setup.

However, the specifications detailed here are not rigid for the proposed solution. It can be implemented using alternatives. For example, during experiments, the Asus Thinker board or Orange Pi devices can be used as a service provider gateway, data plane, or SDN controller node, which have built-in TPM 2.0 support. Moreover, in place of Hyperledger Fabric, Ethereum can be adopted to model the Blockchain network. Nevertheless, using these alternatives will not impact the experiment results as our proposed solution is policy-oriented and not dependent on hardware architecture.

Experiment results

While evaluating the efficacy of our proposed remote auditing process: (i) the required time to sign a video frame, (ii) the average key management overhead among the participant nodes, (iii) the average authentication delay, and (iv) the scale of resisting diverse security attacks is considered as the performance metrics. The results are generated by running the experiments in multiple rounds and making

Table 2: Specification of real experimental setup

Duration of experiment : 20 minute				
Gateway configuration: Raspberry PI 3 B+ (Broadcom BCM2837B0)				
Count	RAM	Clock	Uplink	Downlink
1	1 GB	1.4 GHz	2 MBPS	2 MBPS
Data plane configuration: Raspberry PI 3 A+ (Broadcom BCM2837B0)				
Count	RAM	Clock	Uplink	Downlink
9 (in 3 clusters)	1 GB	1.4 GHz	2 MBPS	2 MBPS
Controller plane configuration: Raspberry PI 3 (Broadcom BCM2837)				
Count	RAM	Clock	Uplink	Downlink
3	1 GB	1.4 GHz	2 MBPS	2 MBPS
TPM configuration: OPTIGA SLB 9670 TPM2.0 (Infineon Technologies)				
Count	Interfacing	I/O buffer	Memory	PCRs
13	SPI	1420 Byte	6962 Byte	24)
Frame type ⇒	VGA	HD	FHD	QHD
Attributes ⇓				
Resolution (Pixel)	640 × 480	1280 × 720	1920 × 1088	2560 × 1440
Average size (MB)	0.106	0.230	0.358	0.420
Frequency	10	7	5	3

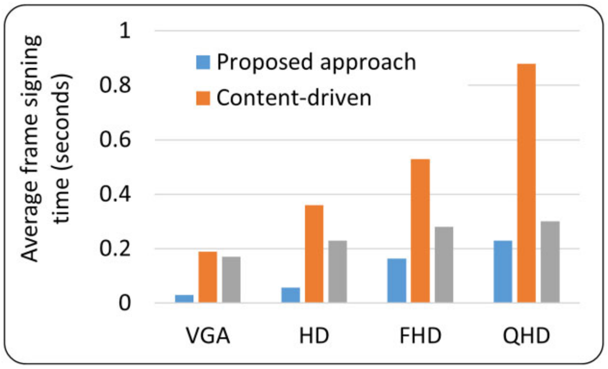

Figure 3: Average frame signing time for different approaches.

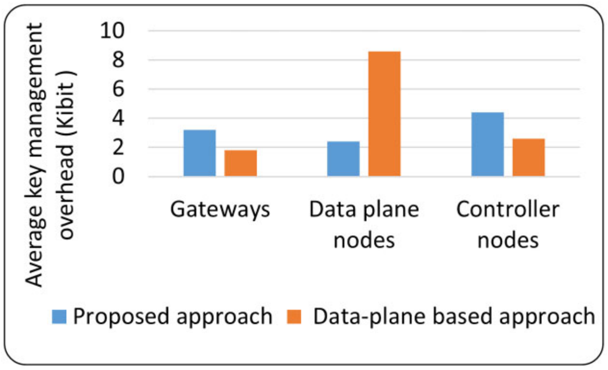

Figure 4: Average key management overhead for different approaches.

an average of the recorded study. Moreover, for each experiment, the performance of the proposed solution is benchmarked with respect to the existing research findings to better illustrate the comparative evaluation. The results are discussed as follows.

Time for signing a video frame

To realize this experiment, a Java-based application program is installed in the gateway that can digitally sign a video frame as soon as it is generated by the camera sensors. The program exploits the TPM on the frame-read datapath and encrypts the frame with the SHA-1 hash function enabled by a 2048-bit RSA asymmetric key pair. Figure 3 shows the average time to sign a video frame of different types through the proposed approach and denotes a comparative study among the Content-driven [18] and watermarking-based [35] video frame signing.

In a Content-driven digital signature, the spatio-temporal relationship between different components within the video frame is transformed into a message digest. The average time in Content-driven frame signing increases drastically with the increment in the video resolution as more temporal dependencies become identifiable. Conversely, in the proposed approach, simple Base64 encoding and decoding are used to parse a video frame for signing, which takes a moderately less amount of time. Moreover, it can deal with the potential security threats of using Base64 by enabling multiple signatures at different communication and computation levels, which is less dependent on solely signing the video frames. However, the watermarking-based digital signature in this experiment performs almost identically for different frame types as it only posts a visual notation on the videos, which does not vary significantly with the changes in frame resolution.

Distribution of key management load

As discussed in the 'Proposed hierarchical key management' section, the proposed remote auditing process manages security keys at different levels of a logical hierarchical architecture. Consequently, it helps in distributing the key management load across gateways, data plane, and control plane, which is reflected in Fig. 4. In this experiment, the gateway and controller plane nodes consume more bits for key management than the data plane as they deal with a group of keys simultaneously. The TPM integrated with each participant node further relaxes the key generation and storage overhead. Moreover, in comparison to the existing data plane-based Blockchain-enabled video transmission framework [27], the proposed solution performs better, as it (i) allows permissioned Blockchain that does not consume additional message bits for setting up the consensus and (ii) focus on securing the key exchange rather than ledgering the data itself.

Attack resistance and authentication delay

During this experiment, three security threat scenarios, such as man-in-the-middle (MITM), replay and node compromising attacks, are intentionally mimicked by making the legitimate communications and nodes vulnerable. The Blockchain-enabled key exchange

Table 3: Attack resistance of different approaches

Attack	Our solution	[17]	[28]
MITM on key integrity	●	❍	●
Replay attack	●	●	❍
Node compromising	●	●	❍

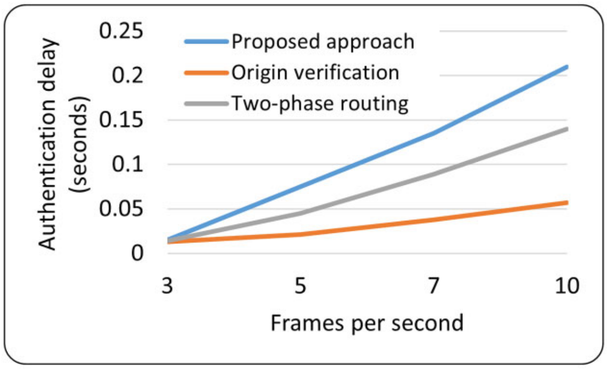

Figure 5: Average authentication delay for different approaches.

approach adopted in the proposed solutions resists the MITM attacker from tampering with the security keys for authentication even when they can tap the communication channel. The encrypted private network tunnel between the camera sensor and controller nodes also provides extra protection in securing the key exchange from MITM attackers.

Furthermore, the proposed solution restricts the impact of node-compromising attacks as it does not allow any nodes from a particular communication level to access the secured information of other levels. Additionally, it distributes the authentication of video frames and user preferences at multiple levels, and their integrity is verifiable at any phase of remote auditing. It also enforces granular and dispersed access control within the data plane that further resists the attackers from forging the identity of any node participating in video frame transmission and thus shrinks the scope of a replay attack.

Table 3 illustrates a comparative study of the proposed solution with existing data origin verification [17] and two-phase video routing [28] approaches. The results show that the data origin authentication fails to ensure security keys' integrity while transferring them through unreliable nodes. Conversely, due to dynamically opening a multitude of web sockets for load balancing, the two-phase video routing approach makes the overall system exposed to replay and node-compromising attacks. However, it maintains the integrity of the security keys by outsourcing the key-exchange operations to Cloud.

As Fig. 5 depicts, our proposed solution increases the average video frame verification delay at the receiver side, although it improves the overall security of the remote auditing process by enabling a hierarchically distributed group key management architecture. However, such a trivial increment in the delay, on the question of credibility, is always possible to waive and could be investigated for further optimization.

Conclusion

Remote auditing in the agricultural domain is gradually replacing conventional on-site practices that need to be more credible and secure, considering recent cyber-attack trends. In this work, we studied how TC-driven concepts and services can be extended for reliable remote auditing. Incorporating Blockchain and SDN with TC, we devised a remote auditing process capable of video-frame authentication and verification. It also supports key management for a chain of digital signatures in a logical hierarchical architecture that can resist diverse security attacks. The results of experiments conducted through an end-to-end prototype system demonstrated that our solution performs significantly better than the existing benchmarks in video frame signing, balancing key management overhead and attack resistance. However, there are still scopes for performance improvement, particularly in optimizing the verification time and overall system responsiveness.

Conflict of interest statement

There have been no conflict interest among the Authors.

Author contributions

Redowan Mahmud (Conceptualization, Investigation, Methodology, Validation, Writing – original draft, Writing – review & editing), Joshua D. Scarsbrook (Data curation, Methodology), Ryan K. L. Ko (Funding acquisition, Project administration, Supervision), Omar Jarkas (Data curation, Validation), Josh Hall (Project administration), Stuart Smith (Project administration), and Jonathan Marshall (Project administration)

References

1. Woehl R. Cyber security threats to the food industry: consider the cloud. Canada: Global Food Safety Resource, 2021.
2. Sysoieva I, Zagorodniy A, Pylypenko L,. *et al.* Analysis of potential risks of audit of agricultural enterprises. *Agric Resour Econ Int Sci E-J* 2021;7:164–91.
3. Nugraha Y, Martin A. Cybersecurity service level agreements: understanding government data confidentiality requirements. *J Cybersecur* 2022; **8**:tyac004.
4. Hadrović Zekić B. *et al.* Internal auditing in covid-19 environment: is remote auditing a solution? *Paper presented at FINIZ 2021—Are you Ready for the ContinuousNEXT® after Covid-19? Belgrade, Singidunum University, Serbia*, 2021; 3–7.
5. Benami E, Jin Z, Carter MR. *et al.* Uniting remote sensing, crop modelling and economics for agricultural risk management. *Nat Rev Earth Environ* 2021;**2**:140–59.
6. Kabir MS, Islam S, Ali M. *et al.* Environmental sensing and remote communication for smart farming: a review. *Precis Agric* 2022;**4**:82.
7. Snow S, Clerc C, Horrocks N. Energy audits and eco-feedback: exploring the barriers and facilitators of agricultural energy efficiency improvements on Australian farms. *Energy Res Soc Sci* 2021;**80**:102225.
8. Wang M, Wander M, Mueller S,. *et al.* Evaluation of survey and remote sensing data products used to estimate land use change in the United States: evolving issues and emerging opportunities. *Environ Sci Policy* 2022;**129**:68–78.
9. Limited LG. Major farm standards adopt LRQA remote audit technology.. 2020. https://www.lrqa.com/en-au/latest-news/farm-standards-adopt-lr-remote-audit-technology/ (22 December 2022, date last accessed).
10. Snider KL, Shandler R, Zandani S. *et al.* Cyberattacks, cyber threats, and attitudes toward cybersecurity policies. *J Cybersecur* 2021;7:tyab019.
11. F-Secure. A global survey showcasing the digital moments that matter most in 2023. 2023. https://assets.f-secure.com/f-secure/en/consumer/documents/living-secure.pdf (22 February 2023, date last accessed).
12. Patil U, Chouragade P. Deepfake Video Authentication Based on Blockchain. In: *2nd International Conference on Electronics and Sustainable Communication Systems*. IEEE, 2021, 1110–3.

13. Mclean M. Must-know cyber attack statistics and trends. USA: Embroker, 2023.
14. Mizher MA, Ang MC, Abdullah SNHS. *et al.* Passive Object-based Video Authentication Using Stereo Statistical Descriptor on Wavelet Decomposition. In: *International Conference on Information Technology*. IEEE, 2021, 791–8.
15. Alsaedi A, Tari Z, Mahmud R,. *et al.* USMD: UnSupervised Misbehaviour Detection for Multi-Sensor Data. *IEEE Trans Dependable Secure Comput* 2022;**20**:724–39.
16. Anthi E, Williams L, Burnap P. *et al.* A three-tiered intrusion detection system for industrial control systems. *J Cybersecur* 2021;**7**:tyab006.
17. Kang N. Efficient data origin authentication scheme for video streaming transmitted by multiple senders. *NATURAL VOLATILES and ESSENTIAL OILS (NVEO) Journal* 2021;**8**:775–86.
18. Sowmya K, Chennamma H, Rangarajan L. Video authentication using spatio temporal relationship for tampering detection. *J Inf Secur Appl* 2018;**41**:159–69.
19. Qiu W, Yang X, Wei M. *et al.* A Blockchain-based Fast Authentication and Collaborative Video Data Forwarding Scheme for Vehicular Networks. In: *19th International Conference on Embedded and Ubiquitous Computing (EUC)*. IEEE, 2021, 56–63.
20. Xu R, Nagothu D, Chen Y. Decentralized video input authentication as an edge service for smart cities. *IEEE Consum Electron Mag* 2021;**10**: 76–82.
21. Jamil F, Ibrahim M, Ullah I. *et al.* Optimal smart contract for autonomous greenhouse environment based on iot blockchain network in agriculture. *Comput Electron Agric* 2022;**192**:106573.
22. Ibrahim M, Lee Y, Kahng HK. *et al.* Blockchain-based parking sharing service for smart city development. *Comput Electr Eng* 2022;**103**:108267.
23. Nikouei SY, Xu R, Nagothu D. *et al.* Real-Time Index Authentication for Event-Oriented Surveillance Video Query Using Blockchain. In: *2018 IEEE International Smart Cities Conference (ISC2)*. IEEE, 2018, 1–8.
24. Li J, Liu X, Zhao J. *et al.* Application Model of Video Surveillance System Interworking Based on Blockchain. In: *2021 IEEE 4th Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC)*, vol. **4**. IEEE, 2021, 1874–9.
25. Labbi M, Kannouf N, Chahid Y. *et al.* Blockchain-based PKI for Content-Centric Networking. In: *The Proceedings of the Third International Conference on Smart City Applications*. Springer, 2018, 656–67.
26. Tang C, Ma Y, Yu X. Design and implementation of port video terminals security access authentication system using blockchain technology. In: *E3S Web of Conferences*, vol. **253**. EDP Sciences, 2021, 03086.
27. Xie L, Ding Y, Yang H. *et al.* Blockchain-based secure and trustworthy Internet of Things in SDN-enabled 5G-VANETs. *IEEE Access* 2019;**7**:56656–66.
28. Koryachko V, Perepelkin D, Saprykin A. *et al.* Development of Cloud Video Conferencing System Based on Two-Phase Routing Networks. In: *10th Mediterranean Conference on Embedded Computing (MECO)*, IEEE, 2021, 1–4.
29. Clayman S, Tuker M, Arasan H,. *et al.* Managing Video Processing and Delivery Using Big Packet Protocol with SDN Controllers. In: *7th International Conference on Network Softwarization (NetSoft)*. IEEE, 2021, 196–200.
30. Shen Z, Tong Q. The Security of Cloud Computing System Enabled by Trusted Computing Technology. In: *2nd International Conference on Signal Processing Systems*, Vol. **2**, IEEE, 2010, V2–11.
31. Hadan H, Serrano N, Camp LJ. A holistic analysis of web-based public key infrastructure failures: comparing experts' perceptions and real-world incidents. *J Cybersecur* 2021;**7**:tyab025.
32. Yin H, Guo D, Wang K. *et al.* Hyperconnected network: a decentralized trusted computing and networking paradigm. *IEEE Network* 2018;**32**:112–7.
33. Jeffery R, Staples M, Andronick J. *et al.* An empirical research agenda for understanding formal methods productivity. *Inf Softw Technol* 2015;**60**:102–12.
34. Tuli S, Mahmud R, Tuli S. *et al.* Fogbus: a blockchain-based lightweight framework for edge and fog computing. *J Syst Softw* 2019;**154**: 22–36.
35. Ayubi P, Jafari Barani M, Yousefi Valandar M. *et al.* A new chaotic complex map for robust video watermarking. *Artifi Intell Rev* 2021;**54**: 1237–80.