Multimedia security and privacy protection in the internet of things: research developments and challenges

Wencheng Yang

Security Research Institute,
School of Science,
Edith Cowan University,
Cyber Security Cooperative Research Centre,
WA 6027, Australia
Email: w.yang@ecu.edu.au

Song Wang

School of Engineering and Mathematical Sciences,
La Trobe University,
VIC 3086, Australia
Email: song.wang@latrobe.edu.au

Jiankun Hu*

School of Engineering and Information Technology,
University of New South Wales at the Australian
Defence Force Academy (UNSW@ADFA),
Canberra, ACT 2600, Australia
Email: j.hu@adfa.edu.au
*Corresponding author

Nickson M. Karie

Security Research Institute,
School of Science,
Edith Cowan University,
Cyber Security Cooperative Research Centre,
WA 6027, Australia
Email: n.karie@ecu.edu.au

Abstract: With the rapid growth of the internet of things (IoT), huge amounts of multimedia data are being generated from and/or exchanged through various IoT devices, systems and applications. The security and privacy of multimedia data have, however, emerged as key challenges that have the potential to impact the successful deployment of IoT devices in some data-sensitive applications. In this paper, we conduct a comprehensive survey on multimedia data security and privacy protection in the IoT. First, we classify multimedia data into different types and security levels according to application areas.

Then, we analyse and discuss the existing multimedia data protection schemes in the IoT, including traditional techniques (e.g., cryptography and watermarking) and emerging technologies (e.g., blockchain and federated learning). Based on the detailed analysis on the research development of IoT-related multimedia security and privacy protection, we point out some open challenges and provide future research directions, aiming to advance the study in the relevant fields and assist researchers in gaining a deeper understanding of the state of the art on multimedia data protection in the IoT.

Keywords: security and privacy; internet of things; IoT; multimedia; federated learning; encryption; watermarking; blockchain.

Reference to this paper should be made as follows: Yang, W., Wang, S., Hu, J. and Karie, N.M. (2022) 'Multimedia security and privacy protection in the internet of things: research developments and challenges', *Int. J. Multimedia Intelligence and Security*, Vol. 4, No. 1, pp.20–46.

Biographical notes: Wencheng Yang received his PhD degree from the School of Engineering and Information Technology, University of New South Wales, Canberra, Australia, in 2015. He is a Cyber Security CRC Research Fellow at Edith Cowan University (ECU), Australia. He has authored several papers published in high-ranking journals and conferences, e.g., *IEEE Transactions on Information Forensics and Security* and *Pattern Recognition*. His research interests include biometric security and biometric recognition.

Song Wang received her PhD degree from the Department of Electrical and Electronic Engineering, University of Melbourne, Australia. She is a Senior Lecturer with the Department of Engineering, La Trobe University, Australia. She has published nearly 50 journal papers, many of which appear in high-ranking journals, such as *IEEE Communications Magazine*, *IEEE Transactions on Industrial Informatics*, *IEEE Transactions on Information Forensics and Security* and *Pattern Recognition*. Her research interests include biometric security, blind system identification, and wireless communications.

Jiankun Hu received his PhD in Engineering from the Harbin Institute of Technology, China, in 1993. He is a Full Professor with the School of Engineering and IT, University of New South Wales, Canberra, Australia. His research interests include cyber security including image processing/forensics and machine learning where he has authored many papers in high-quality conferences and journals including *IEEE Transactions on Pattern Analysis and Machine Intelligence* (*PAMI*). He was the recipient of ten Australian Research Council (ARC) Grants and has served at the prestigious Panel of Mathematics, Information and Computing Sciences (MIC), ARC ERA (The Excellence in Research for Australia) Evaluation Committee. He has served as the senior area editor of *IEEE Transactions on Information Forensics and Security*.

Nickson M. Karie received his PhD in Computer Science from the University of Pretoria, South Africa in 2016. He is currently a Cyber Security CRC Research Fellow at Edith Cowan University, Security Research Institute, Perth, Western Australia. He has more than ten years of experience in academic research, teaching and consultancy in different countries including India, Kenya, South Africa, Swaziland, and Australia. His research interests include intrusion detection and prevention, information and computer security architecture, network security and forensics, mobile forensics, and IoT security. He is also actively engaged as a high impact international conference and journal author and reviewer.

1 Introduction

The internet of things (IoT) is rapidly gaining traction in sectors like wireless communication, remote sensing and advanced manufacturing. Karie et al. (2020) noted in their research article, ‘The number of connected IoT devices will rise to 38.6 billion by 2025 and an estimated 50 billion by 2030’. The basic idea of the IoT is to provide us with a variety of things or objects, such as sensors, smart cameras, and smartphones, which can interact and cooperate to perform the tasks of communication, computing and services. Such a network offers a bright future for big data multimedia applications, as the demand for emerging applications such as video on demand (VoD), real-time video surveillance has increased significantly (Zhou and Chao, 2011). With network and multimedia technologies developed for the IoT, multimedia data (e.g., images, audios and videos) are becoming prevalent in industrial environments and social settings. Since the IoT is designed to widely execute unauthenticated user-implemented applications, both applications and users can be a source of security threats to the IoT. Therefore, security is critical for multimedia data in the IoT.

Multimedia data can be generated from a variety of IoT applications, ranging from smart homes to smart transportation; and smart grid to smart cities. In addition, the IoT spans healthcare, surveillance, agriculture and many other industries. No facet of people’s daily lives is left out of the reach of the IoT. This means that multimedia data at stake may be personal, medical, sensitive, or financial. Most multimedia data transferred in open environments (e.g., wireless networks) can be illegally copied and redistributed without much effort, resulting in serious consequences such as privacy leakage and reputational problems (Yongliang et al., 2004). This is why the security and privacy protection of multimedia data play a crucial role in a trustworthy IoT system. If the security of multimedia data is at risk, it can lead to unauthorised access to IoT systems or applications, leakage of highly confidential information, privacy invasion and identity theft. Therefore, multimedia data security in the IoT has been a research focus in recent years and new technologies are constantly developed (Punia et al., 2017).

As multimedia data protection is becoming more and more important in IoT-oriented environments, there is an urgent need to tackle the security and privacy issue. Many IoT devices are subject to constraints such as energy and computing capacity limitations, making them susceptible to attacks. Therefore, implementing effective security and privacy control measures reduces data security threats and risks in the IoT (Karie et al., 2021). However, traditional encryption schemes using static structures, such as Data Encryption Standard (DES), Advanced Encryption Standard (AES) and the algorithm developed by Rivest, Shamir and Adleman (RSA) for text or binary data, need to perform several rounds of computation, incurring huge expenses in execution time and computational overhead, and thus do not seem suitable for multimedia-related IoT applications (Su et al., 2012). Moreover, the situation gets complicated when multimedia data are handled in the IoT, as the algorithms in question should meet strict quality of service (QoS) requirements (Noura et al., 2018).

1.1 Related work

A number of research articles provide overviews specifically on multimedia data security and privacy protection. To begin with, Nahrstedt et al. (2000) introduced several cryptography-based and digital watermarking-based security methods which fulfil the increasing security requirements of multimedia. Tzelepi et al. (2002) indicated that, in addition to cryptography and digital watermarking, the security of multimedia medical data is also dependent on security infrastructures. In their work, an authorisation model for regulating access to multimedia medical data is defined. Moreover, a system architecture for a database management system (DBMS) is proposed to ensure the security of multimedia medical data. Furht and Socek (2003) surveyed multimedia data security in terms of the cryptosystem types (e.g., symmetric cryptosystems vs. asymmetric cryptosystems; and digital rights management (DRM) cryptography vs. communication cryptography), encryption levels, main multimedia data formats (e.g., Moving Picture Experts Group – MPEG and JPEG), and communication encryption approaches (e.g., the naïve approach, scrambling and selective encryption) for video and audio multimedia. Voloshynovskyy et al. (2005) formulated some major security issues related to multimedia data and investigated watermarking-based schemes to address those issues. In addition, the authors presented a unified theoretical framework for analysing different methods of data hiding in a wide variety of implementations.

Su et al. (2012) proposed four evaluation metrics for multimedia data security, namely, time analysis, error robustness, compression ratio and security analysis. The authors subsequently evaluated chaos-based multimedia encryption algorithms using the four metrics. Moravčík et al. (2016) overviewed some common attacks (e.g., eavesdropping and port scanning) and then described how to secure the real-time multimedia signalisation such as asymmetric cryptography and digital signature. Ashour and Dey (2017) gave a brief review on multimedia data hiding techniques (e.g., common procedures of data hiding) and common data hiding applications. The authors also summarised challenges and future data hiding research. Li et al. (2017) put forward security and privacy challenges of crowdsensing multimedia data collected from a variety of applications (e.g., healthcare monitoring, traffic patterns and air quality information retrieval). The authors presented solutions to protecting crowdsensing multimedia data, which include enhancing data reliability and protecting participant privacy and inadvertent data.

Regarding multimedia in the era of the IoT, Alvi et al. (2015) introduced an internet of multimedia things (IoMT) architecture to facilitate multimedia-based services for users. The proposed architecture consists of four stages and technical methods for each stage are reviewed in the work. In addition, challenges and feasibility of the methods for each stage are discussed. Wang et al. (2017a) surveyed the research field of mobile IoT-based multimedia systems. In this review paper, the authors focused on issues such as video traffic prioritisation, mobility management and security. Kumar et al. (2020) conducted a survey on multimedia big data computing for the IoT. Moreover, the authors presented the challenges involved and relevant solutions, of which the benefits and drawbacks are analysed.

Nauman et al. (2020) provided a comprehensive survey on multimedia IoT. First, available multimedia IoT architectures are summarised. Second, multimedia IoT applications revolutionising human lives are explored. Finally, the limitations and open research issues of multimedia IoT are discovered. Verma et al. (2020) surveyed the IoT multimedia big data computing technologies and architectures in precision agriculture applications. In this study, the authors discussed the challenges from storage to transmission posed by massive amounts of data acquired from IoT devices. The authors also reviewed multimedia data collection, communication and storage technologies in precision agriculture. Nath et al. (2021) shed light on cryptographic and automatic watermarking techniques to meet the security needs of multimedia data in the IoT era. Several types of attacks and the corresponding security measures are detailed in this work. In addition, the authors suggested that cryptographic schemes can be applied to digital watermarking as an additional protection layer to improve system security.

Given that privacy is one of the major concerns over big data, Yu (2016) studied big data privacy and conducted a broad survey on the related privacy research. In this study, big data-oriented privacy is divided into two categories: data clustering and privacy frameworks. Qu et al. (2018b) reported a summary of privacy restrictions and main attacks in the IoT, illustrated by three case studies. The authors also categorised the existing privacy protection schemes into four types, namely clustering-based schemes, differential privacy (DP), encryption and machine learning. Based on their analysis, the authors pinpointed three critical challenges: the lack of a theoretical foundation, the optimisation of the trade-off between privacy and data utility, and the excessive complexity and high scalability of system isomorphism.

Alhirabi et al. (2021) reviewed the development of design notations, models, and languages that can be applied to describing the IoT security and privacy requirements. The authors also discussed possible risk assessment methods and how they can be incorporated in the IoT applications and systems. The authors explained why it is important to integrate privacy in the early stage of system development. Their study shows that while most of the research articles analyse security in some way, they seldom investigate data privacy. In this survey, the authors emphasised the potential challenges and opportunities for proactive design tools that support IoT privacy. Moreover, the authors identified six research challenges related to privacy in IoT systems and their implications for the IoT research community about how to address these challenges.

DP has become one of the privacy protection tactics for IoT applications. Husnoo et al. (2021) presented a thorough and extensive survey on the application and implementation of DP across four areas of IoT applications, namely intelligent transportation systems, healthcare and medical systems, smart grid and industrial internet of things (IIoT). Jiang et al. (2021) provided a comprehensive survey of differentiated privacy opportunities and applications in the IIoT. First, relevant studies on IIoT and privacy protection are reported. Next, the metrics of industrial data privacy are highlighted. Then, the conflict between data utilisation of deep models and individual privacy protection is analysed. Finally, several insightful issues are pointed out and new research directions are suggested.

1.2 Motivation and contributions

Most of the existing survey-style papers inspect the security of multimedia data generally, but few have studied multimedia data security and privacy in the IoT, where there are specific requirements for multimedia data protection. To fill this gap, in this review paper we focus on the security and privacy protection of multimedia data in IoT applications. The contributions of this work are summarised as follows:

1 Very few existing surveys discuss the emergence of new technologies for multimedia data protection in IoT scenarios. In this review paper, in addition to giving an overview of traditional security schemes (e.g., cryptography and watermarking), we investigate emerging technologies for multimedia data protection in the IoT, such as blockchain and federated learning (FL).

2 Implementing security mechanisms may be expensive, which is compounded by the fact that many IoT devices are resource-constrained. It is therefore cost-effective to determine a suitable level of security and privacy for multimedia data protection. In this survey, we classify multimedia data into different categories and security levels based on applications, thus providing an insight into multimedia data protection solutions in conjunction with security requirements.

3 Given the heterogeneity of IoT devices, data types and systems, there is no single data protection technique that is capable of handling all situations. In this work, by reviewing a range of security schemes, we conclude that it is necessary to define a standardised security framework that combines different cryptographic techniques, authentication procedures and defence methods for multimedia data protection in the IoT.

1.3 Paper organisation

The rest of this paper is organised as follows. In Section 2, we review requirements for the security and privacy of multimedia data. In Section 3, we introduce the classification of multimedia data and security levels. In Section 4, we discuss and summarise security and privacy protection schemes for multimedia data in the IoT. In Section 5, we present some open challenges of multimedia security and privacy protection. We conclude the paper and provide future research directions in Section 6.

2 Security and privacy requirements for IoT-oriented multimedia data

Multimedia is a combination of texts, images, audio data, animation and videos (Furht and Socek, 2003). There are some essential security and privacy requirements for multimedia data according to Nahrstedt et al. (2000) and Furht and Socek (2003), as detailed below:

- *Confidentiality:* It means that communication is kept secret and only the wanted communicating parties can access it. It is one of the most desired attributes for IoT scenarios and is also critical for important social and industrial applications. For example, cryptographic systems can keep information confidential from unauthorised entities.
- *Data integrity:* To preserve data integrity in the IoT, communication recipients must be able to verify that received messages are not modified during transmission. Data integrity implies that communication data cannot be tampered with in any manner (Oracevic et al., 2017). If a message is tampered with, it is detectable by all communicating parties. Data tampering can be detected by various means, such as one-way hash functions, message authentication codes, digital signatures and watermarks.
- *Authentication:* Authentication is the procedure of ascertaining if a message is indeed where it claims to come from or what it claims to be. The authentication system should be able to authenticate communicating parties. There are different sorts of entity authentication (e.g., digital signatures and watermarking).

- *Non-repudiation:* Non-repudiation proves that a specific event or action has occurred. For example, an event or action could be the generation, sending or reception of a message. Mechanisms such as message authentication codes or digital signatures can be used for non-repudiation.
- *Privacy:* Privacy is about information protection, ensuring that any individual's private or sensitive information is kept from prying eyes. As privacy is a human right, policy makers, researchers and legal experts should work together to propose appropriate multimedia data mining regulations and techniques so that privacy and proper use of multimedia data can be guaranteed (Aqeel-ur-Rehman et al., 2016).

In addition, the following extra requirements about multimedia data in the IoT can be taken into account:

- *Trade-off between privacy and data utility:* Since IoT users can publish multimedia data in an anonymous manner to prevent privacy leakage leading to data utility degradation, the goal of multimedia data privacy protection in the IoT is to realise an optimal trade-off between privacy and data utility (Qu et al., 2018a).
- *Personalised privacy:* A constant level of privacy is usually applied to all types/categories of multimedia data in the IoT. This is both impractical and resource inefficient. However, this can be resolved by personalised privacy through assigning different privacy levels based on various requirements (Qu et al., 2018a).
- *Privacy measurement:* In general, measurement is the basis of scientific work. So far, the measurement of privacy has not been well-defined, however, the authors believe that privacy measurement should be a requirement for multimedia data in the IoT in the future. Direct measurements are difficult to obtain in some cases, but relative measurements (e.g., Kullback-Leibler distance, correntropy, and Kolmogorov-Smirnov distance) can be an option (Yu, 2016).

3 Multimedia data classification and security and privacy levels

In the IoT, multimedia objects, outfitted with network links interacting with other objects in the absence of human intervention, present great opportunities for improving people's daily lives (Nauman et al., 2020). Since multimedia data contain a wealth of information, some data are normal, non-sensitive and do not need protecting, while other data (e.g., biometric data and healthcare data) are considered sensitive and private and therefore require protection to prevent information leakage or exposure. In this section, we classify multimedia data depending on different categorisations of applications (as shown in Table 1) and specify security levels based on the types of multimedia data. This classification produces less overlapped classes than the classification of Zikria et al. (2020).

Table 1 Classification of multimedia data and corresponding security and privacy level in the IoT

Class	*Data type*	*Security and privacy level*
Class one	Biometric multimedia data	High
Class two	Healthcare multimedia data	High
Class three	Agriculture multimedia data	Low
Class four	Surveillance multimedia data	Medium
Class five	Logistics/transport multimedia data	Low
	Social multimedia data	Medium

3.1 Class one: biometric multimedia data

Biometric multimedia data are collected from an individual's physical or behavioural traits in biometric applications such as face and/or fingerprint recognition (Yang et al., 2018a). While biometrics has innate strengths compared to traditional personal recognition technologies (e.g., passwords), it is vital to ensure the security and integrity of biometric multimedia data. If an individual's biometric data (e.g., face images) are stolen, they cannot be reissued or replaced in the same way as a stolen password or token. To safeguard user privacy, the identifiers of individuals should be de-identified, or biometric multimedia data protection should be reinforced (Ribaric et al., 2016).

- *Example applications:* Given the advantages of high accuracy, robustness to illumination changes and fast implementation of finger vein recognition, Lu et al. (2017) developed an efficient local descriptor for finger vein feature extraction in IoT applications, referred to as histogram of competing orientation and magnitude (HCOM). Two types of local histograms are derived from finger vein images and combined to efficiently and fully represent the competing information. Thilagavathi and Suthendran (2018) designed an innovative method for automatic real-time face recognition from videos captured by IoT devices. Instead of relying on static images, the proposed method uses video-based biometric data, which have more salient information than a single image. The proposed method comprises algorithms such as the Haar cascade classifier and local binary pattern histogram for feature extraction and training. Yang et al. (2019b) presented a lightweight biometric system tailored for resource-constrained IoT devices to save memory usage and computing costs. The proposed algorithm implements block-based logic operations to cut down biometric feature sizes in a simple yet effective way. Experiment results show that the proposed lightweight biometric system achieves high recognition accuracy with a significantly reduced feature size.

3.2 Class two: healthcare multimedia data

Healthcare multimedia data are readily available from medical professionals, hospitals, patients, insurers and pharmacies, etc. Healthcare data are often fragmented, sensitive and private, and therefore difficult to share between different organisations (Xu et al., 2021).

- *Example applications:* Body sensor network is a major IoT application where various vital bio-signals are captured and managed (BK and Muralidhara, 2015; Muhammad et al., 2017). BK and Muralidhara (2015) proposed an IoT-based smart health monitoring system in which IoT sensors play the role of a catalyst in healthcare applications. In the proposed system, a microcontroller is used as a gateway to interact with various sensors, such as temperature sensors and pulse oximetry sensors. The microcontroller receives sensor data and sends them to the network via Wi-Fi, thus providing real-time monitoring of healthcare data for physicians. Muhammad et al. (2017) discussed the possibility of using IoT-cloud computing to monitor people for speech pathology and proposed a speech pathology detection system. The proposed system uses local binary patterns from a mel-spectrum representation of voice signals, and an extreme learning machine (ELM) classifier to identify pathology.

3.3 Class three: agriculture multimedia data

Collected by IoT sensors, agricultural multimedia data can be used to create an intelligent system, where environmental information (e.g., temperature, CO_2, water level and humidity) along with images can be observed to conduct data analysis. Analysing and interpreting agricultural multimedia data acquired from IoT sensors are instrumental in bringing about production increase and crop quality improvement (Verma et al., 2020).

- *Example applications:* Khattab et al. (2016) developed a customised IoT architecture for precision agriculture applications (e.g., crop monitoring and irrigation control), where IoT sensors collect agricultural data (e.g., air temperature, wind speed, rain gauge, solar radiation and leaf wetness). The proposed three-tier architecture gathers the required data and forwards them to a cloud-based backend, where it is processed and analysed. According to the feedback from data analysis, actions can be sent back to the front-end sensors. Mohanraj et al. (2016) presented an e-agriculture application based on the framework of a knowledge base and a monitoring module. The knowledge base is structured with details of various crops, such as geospatial data and weather forecasts, collected by the monitoring module composed of IoT sensors.

3.4 Class four: surveillance multimedia data

Video streaming is becoming prevalent in IoT-based networks, as many internet-connected devices are capable of capturing videos. Surveillance multimedia data are usually derived from video surveillance applications (e.g., intelligent traffic surveillance and house monitors), where surveillance is for monitoring human activities, such as public safety, incident detection and transport control. In general, video surveillance data are treated as a continuous series of images, which are high-dimensional and unstructured (Yu et al., 2019).

- *Example applications:* Feng et al. (2017) studied security weaknesses in IoT-related video surveillance from the perspective of hardware systems. The authors first developed a proof-of-concept prototype mimicking a video replay attack. They then developed a hardware-based IoT security architecture to address the security issue.

The proposed architecture establishes a trusted execution context and physically separates security-sensitive elements (e.g., the motion detection module) from the remainder of the system. Yu et al. (2019) presented a multilayer ELM-based online prediction scheme for video surveillance applications. In this scheme, temporal and spatial features support a dynamic semantic representation among neighbouring frames. The proposed approach not only identifies multiple objects with varying directions of motion but also effectively recognises fine-tuned semantic features.

3.5 Class five: other types of multimedia data

- *Logistics/transport multimedia data:* IoT applications are diverse (e.g., intelligent transportation systems and self-driving cars). Cars, buses and trains can now be equipped with smart sensors generating massive amounts of multimedia data about road information, traffic congestion, temperature, etc. thereby offering users information to navigate safely (Obaidat et al., 2019).
- *Example applications:* Liu et al. (2017) introduced a new vehicle type classification about images captured by multi-view visual traffic surveillance sensors. The authors combined deep neural networks with balanced sampling. The proposed classification consists of two phases. In the first phase, data augmentation with balanced sampling is employed to alleviate the issue of unbalanced datasets. In the second phase, the parameters learned from the augmented training dataset are used to construct a collection of convolutional neural network models with different architectures to achieve good classification accuracy.
- *Social multimedia data:* With the aid of the IoT, people interact with each other and maintain social relationships more conveniently and intelligently than ever before. We can stay in touch with friends by receiving and posting real-time updates through social media (e.g., Facebook) or APP (e.g., TikTok). The data about individuals and their social relationships generated in the IoT must be protected with appropriate privacy and security technologies (Obaidat et al., 2019).
- *Example applications:* In a social IoT environment, each object can search for a specific service using its relationships. In the work of Hsu and Tung (2020), multimedia IoT devices utilise peer-to-peer (P2P) networks for communication. Peers are represented by multimedia IoT devices with user interactions. As users have their friend lists, social links are categorised into different priorities based on social relationships, such as family, friends and others. The authors presented a strategy for P2P video transmission using weighted fair queues with different queuing priorities. By exploiting the inherent trust in social links, the proposed strategy can decrease the influence of free-riders and provide users with a favourable video sharing and viewing experience on multimedia IoT devices.

3.6 Security and privacy levels of multimedia data

Multimedia data security and privacy are mostly governed by application areas. For this reason, different multimedia data require different levels of security. In this section, we specify three security and privacy levels for multimedia data, namely high-security and privacy, medium-security and privacy and low-security and privacy. The rationale behind arranging multimedia data security and privacy into the three levels is that it can be costly to implement a protection measure, especially considering many IoT devices have limited resources, so it would be more cost-effective to apply high protection to sensitive, private or confidential multimedia data and low or no protection to publicly available information. Selecting a protection mechanism should take into account the security and privacy level of the multimedia data handled by IoT systems or devices. In other words, the security and privacy level of multimedia data is determined by whether they are highly privacy-restricted, privacy-restricted or public.

- *Level 1 – Security and privacy (low):* This is considered the lowest level of security and privacy. Its implementation is cost-effective and uncomplicated. Examples of multimedia data that can be put under this security and privacy category include transport multimedia data and agriculture multimedia data. These data are not necessarily privacy-restricted.
- *Level 2 – Security and privacy (medium):* Level 2 security and privacy improves upon the protection mechanisms of Level 1. Its implementation is more expensive and complex than that of Level 1. Examples of data belonging to Level 2 security and privacy are surveillance multimedia data and social multimedia data.
- *Level 3 – Security and privacy (high):* Level 3 security and privacy means high protection over multimedia data. It is the highest level of security and privacy among the three and thus implementationally more costly and complicated than Levels 1 and 2 security and privacy. For example, security and privacy of human bio-signals are regulated and need to be strictly protected (Zhao et al., 2012; Pandey et al., 2021).

4 IoT-oriented multimedia security and privacy protection schemes

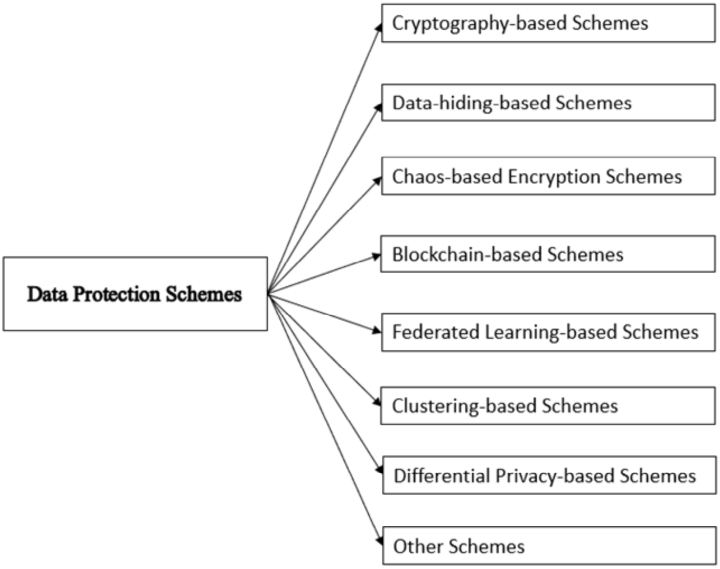
In general, multimedia security and privacy protection schemes are to secure the multimedia content. These schemes are largely based on the cryptography technology to enable communication security and/or privacy protection (Furht and Socek, 2003). There are many methods and techniques specially designed for multimedia security and privacy protection in the IoT as shown in Figure 1. Moreover, a summary about these methods and techniques is provided in Table 2.

4.1 Cryptography-based schemes

Cryptography is a technique for transforming data into an indecipherable format and disseminating it through networked media. It is usually accomplished through a variety of computational functions (Nath et al., 2021).

Xia et al. (2017) proposed a ciphertext-policy attribute-based encryption delegation method that permits the data owner to encrypt the data by specifying an access policy for the attribute, such that only users related to the attribute satisfying the policy can decrypt the data. Moreover, the proposed method is adaptively activated based on the estimate of the decryption overhead for various vehicles. Noura et al. (2018) designed a lightweight cryptographic algorithm based on a single-round dynamic structure containing simple operations and targeting multimedia IoT. In this algorithm, a dynamic key is produced and then utilised to create two robotic replacement tables, a dynamic permutation table and two pseudo-random matrices. This dynamic cryptographic structure reduces the number of rounds to one, while maintaining a high degree of randomness and security. Aljawarneh et al. (2017) developed an efficient GPU encryption system to protect multimedia big data from real-time attacks (e.g., DoS attacks and tampering attacks). The proposed system incorporates the advantages of Feistel encryption and genetic algorithms. In addition, the encryption algorithm developed combines the process of bit scrambling and the replacement of boxes to produce a high avalanche effect. To enable secure multimedia communication in the IoT, Mishra et al. (2018) studied the authentication protocols of Kumari and Om, identifying a number of design defects and proposing a secure mutual authentication protocol with key establishment techniques to abrogate the defects found in the Kumari and Om protocols.

Figure 1 Multimedia data protection schemes in the IoT


Data Protection Schemes
Cryptography-based Schemes
Data-hiding-based Schemes
Chaos-based Encryption Schemes
Blockchain-based Schemes
Federated Learning-based Schemes
Clustering-based Schemes
Differential Privacy-based Schemes
Other Schemes

BD et al. (2019) presented a hash-based secure radio-frequency identification (RFID) authentication mechanism for context-aware sensor management systems to decrease the complexity of sensor systems. The presented protocol is based on the hash manipulation of synchronised secret session keys to resist attacks such as replay attacks and man-in-the-middle attacks. Omrani et al. (2019) designed a lightweight cipher specifically for image data, which can be realised on low-resource devices, making it the first attempt to address multimedia security in the context of the IoT. The proposed cipher is built on the so-called 'outer-inner structure', which is tailored to handle the high correlation and redundancy of images and to guarantee the highest level of obfuscation and diffusion characteristics. Ma et al. (2019) proposed lightweight, privacy-preserving data aggregation for mobile multimedia. Most existing data privacy-preserving systems involve a trusted third-party, making it a bottleneck. Yet, in the proposed method there is no trusted third-party and the endpoint computation is lightweight. Moreover, the multimedia data are balanced through creating virtual aggregation zones and the system performance is improved by employing batch verification.

Table 2 A summary of different multimedia protection schemes

Categories	*Schemes*	*Descriptions*	*Requirements covered*	
			Security	*Privacy*
Cryptography-based schemes	Xia et al. (2017)	A ciphertext-policy attribute-based encryption delegation method	Yes	Yes
	Noura et al. (2018)	A lightweight cryptographic algorithm based on a single-round dynamic structure	Yes	Yes
	Aljawarneh et al. (2017)	An efficient GPU encryption system	Yes	Yes
	BD et al. (2019)	A hash-based secure radio-frequency identification (RFID) authentication mechanism	Yes	Yes
	Omrani et al. (2019)	A lightweight cipher specifically for image data	Yes	Yes
	Ma et al. (2019)	A lightweight, privacy-preserving data aggregation scheme for mobile multimedia	Yes	Yes
Data-hiding-based schemes	Hurrah et al. (2019)	A method for copyright protection, data security and content authentication of multimedia images	Yes	Yes
	Rani et al. (2016)	A scheme that integrates steganography and visual cryptography (VC)	Yes	Yes
	Huang et al. (2018)	A scheme that uses vector quantisation (VQ) transformation and least significant bits (LSB) to hide secret data embedded in a cover image	Yes	Yes
	Wu et al. (2021)	A reversible data hiding scheme that can achieve contrast enhancement of magnetic resonance (MR) brain images	Yes	Yes
Chaos-based encryption schemes	Maggo and Chhillar (2013)	A shuffling process together with the Henon chaotic system algorithm for images	Yes	Yes
	Dhall et al. (2014)	A cryptosystem based on chaotic sequence generation for substitution and diffusion	Yes	Yes
	Wang et al. (2017c)	A chaotic system without equilibrium	Yes	Yes
	Mekki et al. (2018)	A secure surveillance scheme for the healthcare application through intelligent integration of the efficient chaotic map	Yes	Yes
	Nie et al. (2020)	Window-based fountain codes to guarantee the multimedia data security of wireless transmission in edge computing	Yes	Yes
Blockchain-based schemes	Vishwa and Hussain (2018)	A decentralised data management scheme using the blockchain technology to manage user data and protect user data privacy	No	Yes
	Li et al. (2021)	A data security module for multimedia blockchains using distributed trusted communication networks and accelerated information search with Bloom filters	Yes	Yes
	Abdur Rahman et al. (2019)	A method that enables multiple parties to safely share multimedia data and conduct financial dealings by hiding the real identities of the participants	Yes	Yes
	Rathee et al. (2020)	A scheme that secures healthcare multimedia data through the blockchain technology	Yes	Yes

Table 2 A summary of different multimedia protection schemes (continued)

Categories	*Schemes*	*Descriptions*	*Requirements covered*	
			Security	*Privacy*
Federated learning-based schemes	Imteaj and Amini (2019)	A scheme that uses FL to leverage sensing platforms for distributed decision-making and learning in IoT networks	Yes	Yes
	Lu et al. (2019)	A scheme that integrates FL in the consensus process of the permission blockchain	Yes	Yes
	Wu et al. (2020)	A scheme that uses personalised FL in intelligent multimedia IoT applications	Yes	Yes
Clustering-based schemes	Liu and Li (2018)	A clustering-based k-anonymity approach to protecting the data privacy of wearable IoT devices and to ensure the usability of the collected data	No	Yes
	Xiong et al. (2018)	A privacy and availability data clustering scheme based on the k-means algorithm and differential privacy	No	Yes
	Guo et al. (2020)	A mutual privacy-preserving k-means scheme based on homomorphic encryption	No	Yes
	Onesimu et al. (2021)	A privacy-preserving data collection scheme for an IoT-based healthcare delivery system	No	Yes
	Tian et al. (2021)	A graph clustering privacy protection method based on structural entropy	Yes	Yes
Differential privacy-based schemes	Xu et al. (2018)	A local differential privacy obfuscation (LDPO) framework for IoT data analysis at the edge without revealing sensitive user data	No	Yes
	Qiao et al. (2019)	A partitioned histogram data publishing algorithm based on the wavelet transform	No	Yes
	Xue et al. (2021)	A privacy-preserving system for classification on IoT devices in an edge computing environment	No	Yes
Cancellable biometric templates	Ratha et al. (2007)	Methods (e.g., Cartesian, polar, and surface folding transformations) to generate multiple cancellable identifiers from fingerprint images	Yes	Yes
	Yang et al. (2019a)	A cancellable iris and steganography-based user authentication system to provide user authentication and secure the original iris data	Yes	Yes
	Kho et al. (2019)	A binary cancellable fingerprint template design based on the partial local structure (PLS) descriptor and permutated randomised non-negative least square	Yes	Yes
Secure multimedia cloud IoT frameworks	Qin et al. (2016)	A high-performing privacy-preserving feature detection system	No	Yes
	Wang et al. (2021)	A privacy-preserving and traitor tracking content-based image retrieval scheme in cloud computing	Yes	Yes
	Yang et al. (2018b)	A data retrieval scheme for multiple users based on the lattice-based mechanism	Yes	Yes

4.2 Data-hiding-based schemes

Data-hiding-based schemes have a unique advantage in that an adversary is not even aware of the existence of a secret, which is a powerful tool for multimedia privacy protection. They are predominately applied in image and video-based applications, such as Nath et al. (2021), Nauman et al. (2020), Huang et al. (2018), Hurrah et al. (2019), and Wu et al. (2021). The main idea of these schemes is to hide a secret in the image/video cover media while maintaining the visual quality of the image/video.

Conventional data-hiding is based on the techniques of Watermarking, steganography and visual cryptography (VC). Watermarking is mainly utilised to recognise the origin of multimedia content, track illegal distribution and deter unauthorised access by inserting unique watermarks into multimedia content (Nauman et al., 2020). Watermarking has been around for many decades and is still the most widely deployed technology in commercial applications due to its maturity. However, most watermarking algorithms have been broken if the multimedia object containing the secret is under examination. Therefore, steganography and/or VC have been introduced. Hurrah et al. (2019) proposed a method for copyright protection, data security and content authentication of multimedia images. Copyright protection is achieved by embedding a robust watermark based on an efficient inter-block coefficient difference algorithm, while authentication of the media content is accomplished through inserting a fragile watermark in the spatial domain. To frustrate the adversary and to ensure that he or she cannot easily access the actual embedded data, the authors combined an encryption algorithm with the Arnold transform to encrypt the data before embedding it. To increase the security and reliability of multimedia data, Rani et al. (2016) integrated steganography and VC. In the proposed method, steganographic images are hidden in VC shares that are nonsensical and cannot be detected by steganalysis tools. VC and steganography play an important role in data security. The proposed method is tested with text and image files and the results demonstrate that there is no degradation in the quality of the recovered information and images compared to the original files. The drawback of such schemes is efficiency, since multiple cover images are needed.

Reversible data hiding is an emerging data-hiding technique that can seamlessly integrate the advantages of watermarking and cryptography according to Huang et al. (2018) and Wu et al. (2021). To convey secret information through an IoT network, Huang et al. (2018) used vector quantisation (VQ) transformation and least significant bits (LSB) to hide secret data embedded in a cover image. The authors designed a technique called two-level coding to remap the VQ-compressed image to the VQ-transformed image, and used the secret data to adapt the new image to be more similar to the original. Most recently, Wu et al. (2021) proposed a reversible data hiding scheme that can achieve contrast enhancement (CE) of magnetic resonance (MR) brain images, while possessing the capability of losslessly recovering the hidden raw medical image with the secret retrieval key embedded in the cover image. This is an interesting result as it can achieve other goals in addition to the conventional objective of data hiding.

4.3 Chaos-based encryption schemes

The main benefit of chaos-based encryption is that chaotic signals are like noise to unauthorised users, ignoring the mechanism by which they are produced. Moreover, the cost of generating chaotic signals is usually low, making it suitable for encrypting large volumes of data (Su et al., 2012). So far, many chaos-based image, audio and/or video encryption methods have been devised.

To eliminate redundant data, Maggo and Chhillar (2013) designed a shuffling process implemented on different images. Together with the Henon chaotic system algorithm, the proposed design for lightweight devices requires low computation power and provides high security for multimedia data, especially images. To meet particular resource efficiency demands and to satisfy the inherent properties of redundancy and bulkiness of multimedia in real-time and resource-constrained contexts, Dhall et al. (2014) proposed a cryptosystem based on chaotic sequence generation for substitution and diffusion. Wang et al. (2017c) worked on a chaotic system without equilibrium and its multimedia security applications. In the proposed system, 128 kbit data are encrypted and hidden in the sound file. This work enriches the knowledge of practical applications with systems having no hidden attractors. Mekki et al. (2018) analysed the properties of chaotic systems for multimedia data encryption. The authors developed a secure surveillance scheme for the healthcare application through intelligent integration of the efficient chaotic map to extract data in the monitored scene with a visual sensor in the IoT. Nie et al. (2020) proposed window-based fountain codes to guarantee the multimedia data security of wireless transmission in edge computing. Thanks to the fountain codes, data security for wireless transmission is achieved only when the target receiver accumulates enough coded packets before eavesdroppers. In addition, the authors applied the constellation rotation technology and interfering noise in the wireless signal to disrupt the signal quality of the eavesdropper and augment the packet loss of the eavesdropper.

4.4 Blockchain-based schemes

Due to the growing trend of digital cryptocurrencies like Bitcoin, blockchain emerged as a modern decentralised infrastructure and paradigm for distributed computing. Its principal features consist of de-centralisation, time-series data, collective maintenance and security (Ren et al., 2021).

Vishwa and Hussain (2018) proposed decentralised data management using the blockchain technology to manage users' data and protect user data privacy. The proposed protocol allows users to have complete control over their multimedia files without having to trust a third-party. Li et al. (2021) analysed the privacy protection mechanism of blockchain and safeguarded data privacy to enhance the data query and analysis capability of blockchain. Specifically, the authors built a data security module for multimedia blockchains using distributed trusted communication networks and accelerated information search with Bloom filters. Abdur Rahman et al. (2019) demonstrated the efficacy of blockchain-based secure IoT services, in which IoT devices can be leased from service providers in a secure and privacy-preserving manner. The proposed method enables multiple parties to safely share multimedia data and conduct financial dealings by hiding the real identities of the participants. To protect IoT devices from threats initiated by different kinds of hackers, Rathee et al. (2020) secured healthcare multimedia data through the blockchain technology. The authors constructed a hash for each data stream such that any variation or change in the data or destruction of medicines can be reflected in the whole blockchain network.

4.5 FL-based schemes

FL is a promising solution to user privacy protection by training models on large repositories of decentralised multimedia data in the IoT (Pang et al., 2020).

Imteaj and Amini (2019) employed available sensors built into smartphones to properly collect and broadcast multimedia data for different decision-making purposes in the IoT. The objective of this distributed sensing approach is to utilise token recognition devices to activate distributed end-user devices so that data can be transmitted to the cloud when needed and stored on a cloud server to maintain the appropriate format. To address privacy concerns, the authors use FL to leverage sensing platforms for distributed decision-making and learning in IoT networks. Lu et al. (2019) formulated the issue of data sharing in IoT networks as a machine learning problem and incorporated privacy-preserving FL into it. By sharing the data model instead of revealing the actual data, the privacy of the data is well preserved. Moreover, the authors integrated FL in the consensus process of the permission blockchain so that the computational work for consensus can be applied to FL. To address the problem of heterogeneity in IoT environments, Wu et al. (2020) investigated emerging personalised FL that can mitigate the negative effects of heterogeneity in different aspects. The requirement for fast processing and low latency in intelligent multimedia IoT applications can also be met with the power of edge computing. The authors provided a case study of IoT-based human activity recognition to demonstrate the effectiveness of personalised FL in intelligent multimedia IoT applications (e.g., human activity recognition).

4.6 Clustering-based schemes

According to Yu (2016), data clustering-based schemes were developed from the initial *k*-anonymity method, then the *l*-diversity method and finally the *t*-closeness method. Liu and Li (2018) proposed a clustering-based *k*-anonymity approach to protect the data privacy of wearable IoT devices and to ensure the usability of the collected data. Through *k*-anonymity, data holders can disconnect identities from sensitive data before sharing them, in which case identity information cannot be accurately matched with sensitive data information. In the proposed scheme, the authors first analysed the potential vulnerabilities of existing privacy-preserving approaches to data sharing on wearable devices. Then, the authors proposed to adjust the division of records so that the identities within each equivalent set are indistinguishable, thus protecting privacy. Xiong et al. (2018) developed a privacy and availability data clustering method based on the *k*-means algorithm and DP, which reinforces the initial centroid selection and other point-to-centroid distance calculation methods. In addition, the proposed scheme tries to minimise the outlier effect by detecting outliers in the clustering process. The security analysis shows that the proposed scheme meets the objective of DP and protects against the leakage of private information.

Guo et al. (2020) presented a mutual privacy-preserving *k*-means scheme based on homomorphic encryption that does not reveal either the privacy of the participants or the private data of the cluster centre. The proposed scheme splits each iteration of the *k*-means algorithm into two phases.

- First phase: Find the closest cluster centre for each participant.
- Second phase: Calculate a new centre for each cluster.

In both phases, the cluster centres are kept secret from the participants, and the private information of each participant is not available to the analyst. In addition, the proposed scheme brings in a third-party cloud platform to decrease the communication complexity of homomorphic encryption.

Onesimu et al. (2021) put forward privacy-preserving data collection for an IoT-based healthcare delivery system. The authors used a clustering-based anonymisation model in the proposed scheme to fulfil privacy requirements and safeguard the healthcare IoT from a variety of privacy attacks. On the client-side, an improved clustering-based *k*-anonymity model is employed to anonymise the data produced from IoT nodes. The authors adopted a bottom-up clustering approach to obtain clusters of records based on privacy requirements. Tian et al. (2021) proposed a graph clustering privacy protection method using structural entropy, which integrates data mining with structural information theory. In particular, user privacy information in the social IoT is encrypted via a homomorphic algorithm to produce a graph structure in the ciphertext state. The authors applied a two-dimensional structural information solution algorithm and an entropy reduction principle node module partition algorithm to dividing the ciphertext graph structure into different modules. The internal nodes of the divided modules are further clustered using the *k*-dimensional structural information solution algorithm.

4.7 DP-based schemes

The idea at the core of DP is to add random noise to disturb the data before data release. This addition of random noise can be achieved by a variety of approaches. Xu et al. (2018) proposed a local differential privacy obfuscation (LDPO) framework for IoT data analysis at the edge without revealing sensitive user data. The authors first described the architecture and benefits of the LDPO framework. Then they discussed some technical challenges and presented a preliminary implementation of the LDPO framework. The authors also validated the performance of the proposed framework in terms of the level of privacy protection and data utility with real-world applications and datasets. Qiao et al. (2019) designed a partitioned histogram data publishing algorithm based on the wavelet transform. First, a greedy algorithm-based partitioning method is employed to get a better partition structure. Then, the wavelet transform is utilised to add noise. Finally, a reduced histogram structure is obtained to ensure the authenticity and usefulness of the histogram. The proposed scheme can decrease the complexity of wavelet trees constructed by the wavelet transform and enhance the accuracy of histogram counting queries.

Zia et al. (2020) performed a case study on DP. The authors analysed the impact of the amount of noise on the original data and the relationship between the added noise in the data and the utility of the data. Moreover, the impact of data leakage on privacy violations is discussed. Xue et al. (2021) presented a privacy-preserving system for classification on IoT devices in an edge computing environment. Direct perturbation to the input data in the training set has a dramatic effect on the classification precision, so the proposed system is tailored to perturb the feature extraction component to solve the privacy problem, when machine learning models are discharged from the cloud to the edge nodes. Experimental results on different datasets indicate that the proposed system strikes a good trade-off between privacy preservation and utility.

4.8 Other schemes

- *Cancellable biometric templates:* Biometric authentication has been extensively applied to IoT devices, such as mobile phones and laptops. Normally, for biometric authentication, users' biometric templates are required to be stored on IoT devices, which make them vulnerable to becoming compromised. As people have very limited biometrics (e.g., ten fingers), it is vitally important to protect biometrics templates. Unlike face biometrics where quality face templates can be captured remotely and involuntarily, or even from social media posts, quality fingerprint templates are harder to acquire involuntarily. Plus, with the popularity of fingerprint authentication mechanisms, fingerprint template protection has become a very active research area (Ratha et al., 2007; Yang et al., 2019b; Wang et al., 2017b; Li and Hu, 2014; Kho et al., 2019). Among fingerprint template protection schemes, the cancellable fingerprint is the most popular approach where a transformed fingerprint template instead of the raw template is used. When the stored transformed template is compromised, this technique can revoke it and issue a new transformed template, similar to the mechanism of password revocation.
- *Secure multimedia cloud IoT frameworks:* Cloud IoT is an emerging IoT platform that can manage millions of interconnected global IoT devices and their enormous amounts of generated multimedia data via the cloud. Secure and privacy-preserving retrieval or sharing of these data is a challenging issue. There exist two generic mechanisms for secure searches in the cloud: searchable public key encryption and searchable symmetric encryption (Han et al., 2016). Applications of these security mechanisms to the secure multimedia cloud IoT include searchable encryption of visual features (Datta et al., 2008; Qin et al., 2016; Wang et al., 2021), and lattice assumption-based fuzzy information retrieval (Yang et al., 2018b).

5 Open challenges of multimedia security and privacy protection in the IoT

The emerging IoT-based multimedia applications pose new challenges to multimedia data protection. In this section, we highlight some open challenges of multimedia security and privacy protection in the IoT.

First, it is a non-trivial task to determine what level of security and privacy is appropriate for multimedia data in IoT-related applications. A suitable level of security results in more effective use and protection of multimedia data. The value of the multimedia data to be protected should be carefully weighed against the cost of the protection itself in the decision-making process. If the multimedia data to be protected (e.g., agricultural multimedia data) are not highly valuable or sensitive in the first place, then choosing a relatively low cost and simple encryption scheme is sufficient. On the other hand, if the multimedia data (e.g., biometric or healthcare multimedia data) are private and/or confidential, then a high level of protection must be chosen (Furht and Socek, 2003).

Second, heterogeneity of IoT devices, data types and systems brings challenges to multimedia security in the IoT. Heterogeneity of IoT devices: In the fast-growing IoT, heterogeneous objects, both physical and virtual, are linked to the internet and interact with other entities through unique addressing schemes to provide/request various services (Hamoudy et al., 2017). Heterogeneity of data types: compared to typical data, multimedia data collected, generated and/or transmitted by IoT devices have disparate characteristics due to different types of data (e.g., images, audios and videos), unstructured features, noise and so on (Kumar et al., 2020). Heterogeneity of systems: IoT systems differ in computational capacity, memory storage and communication scope. Since IoT devices can be scattered or inactive, or only a small number of devices may be active to maintain communication with the server, this requires IoT systems to be able to tolerate heterogeneous devices, to be able to generate valid models with low device participation and to be fault-tolerant in the case of scattered or inactive devices in the network (Imteaj and Amini, 2019).

Third, feasibility and computational costs are critical issues for multimedia security and privacy protection in the IoT. While some encryption algorithms offer strong security, their computational costs become higher with an increase of data. Therefore, additional security and privacy requirements pose additional challenges to energy consumption and computing capacity of IoT systems. For IoT devices with limited resources (e.g., memory, processing power and energy) and inadequate cyber security safeguards, lightweight security and privacy solutions are required to handle such cases (Hamoudy et al., 2017).

Fourth, DP is a main privacy preservation technique for IoT multimedia data. The implementation of DP on IoT devices requires expensive computational overhead. It is challenging to develop reliable DP demanding minimal computational overhead in the IoT. Moreover, as the IoT continues to grow, a large amount of multimedia data is being generated on a real-time basis. Therefore, in the application of DP to big multimedia data in the IoT, it is non-trivial to handle high-dimensional multimedia data and conduct optimal calculation of DP composition in big multimedia data analytics (Husnoo et al., 2021).

Fifth, in addition to applying privacy-preserving methods, the lack of transparency and governance over the use of IoT multimedia data is a challenge to protecting user privacy while gaining the benefits of the IoT. It is hard for individuals to be notified that their personal data is being captured. IoT devices in public areas can automatically gather information and users may not be aware that their private information is being collected. Therefore, transparency and governance of IoT devices are needed to protect the privacy of users by securing the way IoT devices collect or use personal information (OVIC, 2021).

6 Conclusions and future research directions

With the explosive increase in IoT devices and the advances of IoT multimedia technologies in today’s world, security and privacy concerns of multimedia data should be treated seriously, particularly in data-sensitive IoT applications. To address these concerns, researchers have proposed a variety of schemes for multimedia data security and privacy protection in the IoT. We have reviewed the research developments in IoT-related multimedia security, especially emerging technologies (e.g., blockchain). We have also classified multimedia data into different types and security levels. Moreover, we have identified key challenges facing multimedia security and privacy protection in the IoT.

Based on the detailed analysis and extensive discussion in this review paper, we recommend the following directions for future research:

- *Application of emerging technologies:* In this work, we go through a number of new technologies, such as blockchain and FL. These emerging technologies bring an increased protection to multimedia data. We suggest that researchers carefully consider the pros and cons of emerging technologies such as artificial intelligence (AI) and fog/edge computing, so that they can be better applied to multimedia data protection in IoT applications. Although AI can provide data security, implementing AI algorithms on resource-limited IoT devices is likely infeasible due to their exhaustive computations causing high energy consumption. Fog/edge computing is better and faster for IoT devices. However, the security aspect of this new technique has not been fully studied.
- *Development of lightweight solutions:* The security of multimedia transmissions over IoT networks has not been adequately examined. IoT devices are usually constrained in terms of computing power and energy consumption. Therefore, to realise secure communication in the IoT requires computationally efficient techniques. Lightweight multimedia data protection solutions can be diverse. For example, Shifa et al. (2016) proposed a lightweight video encryption method, in which video data are not completely encrypted. Different levels of encryption are used to secure multimedia data from attacks to preserve personal privacy and locations.
- *A standardised security framework to handle the heterogeneity of the IoT:* As no single data protection scheme can address all the security issues, a standardised security framework is worth considering, which should combine different encryption techniques, authentication procedures and defence methods to facilitate multimedia data protection in the heterogeneous IoT.
- *Adaptive protection schemes based on the security and privacy level of multimedia data:* Classifying data can improve their use and protection. As far as security and privacy are concerned, data classification is a useful strategy that helps to provide an appropriate and adaptive security and privacy response according to the type and security and privacy level of multimedia data. A very costly attack is frustrating for an adversary, so a simple encryption method may be enough for disseminating MPEG videos. For these applications, DRM or selective encryption is of more interest (Furht and Socek, 2003). The underlying idea of selective encryption is to just encrypt a part of the compressed bitstream. For instance, one could select only the most significant coefficients from the last or middle steps of the compression process and perform encryption on them. Less important coefficients are not encrypted or are lightly scrambled (Furht and Socek, 2003).
- *Trade-off between cost and security/privacy:* In the IoT, the security/privacy of multimedia data is critical but difficult to attain. While, on the one hand, the usual trade-off between high security/privacy and the availability of multimedia data for the IoT is more urgent than ever, on the other hand, security/privacy is considered a costly feature, as many IoT devices have limited resources (e.g., energy and computing power). Therefore, designers of IoT systems need not only means to evaluate possible security/privacy threats and explore solutions, but also methods to assess costs and strike a reasonable balance between cost and security/privacy (Bodei et al., 2019).

Acknowledgements

The work has been supported by the Cyber Security Research Centre Limited whose activities are partially funded by the Australian Government Cooperative Research Centres (CRC) Program. The third author acknowledges the support from ARC Discovery Grants (DP190103660 and DP200103207) and ARC Linkage Grant (LP180100663).

References

Abdur Rahman, M., Loukas, G., Maruf Abdullah, S., Abdu, A., Sadiqur Rahman, S., Hassanain, E. and Arafa, Y. (2019) 'Blockchain and IoT-based secure multimedia retrieval system for a massive crowd: sharing economy perspective', *Proceedings of the 2019 on International Conference on Multimedia Retrieval*, pp.404–407.

Alhirabi, N., Rana, O. and Perera, C. (2021) 'Security and privacy requirements for the internet of things: a survey', *ACM Transactions on Internet of Things*, Vol. 2, No. 1, pp.1–37.

Aljawarneh, S., Yassein, M.B. and Talafha, W.a.A. (2017) 'A resource-efficient encryption algorithm for multimedia big data', *Multimedia Tools and Applications*, Vol. 76, No. 21, pp.22703–22724.

Alvi, S.A., Afzal, B., Shah, G.A., Atzori, L. and Mahmood, W. (2015) 'Internet of multimedia things: vision and challenges', *Ad Hoc Networks*, Vol. 33, pp.87–111.

Aqeel-ur-Rehman, S.U.R., Khan, I.U., Moiz, M. and Hasan, S. (2016) 'Security and privacy issues in IoT', *International Journal of Communication Networks and Information Security (IJCNIS)*, Vol. 8, No. 3, pp.147–157.

Ashour, A.S. and Dey, N. (2017) 'Security of multimedia contents: a brief', *Intelligent Techniques in Signal Processing for Multimedia Security*, pp.3–14, Springer, Cham.

BD, D., Al-Turjman, F. and Mostarda, L. (2019) 'A hash-based RFID authentication mechanism for context-aware management in IoT-based multimedia systems', *Sensors*, Vol. 19, No. 18, p.3821.

BK, B. and Muralidhara, K. (2015) 'Secured smart healthcare monitoring system based on IoT', *International Journal on Recent and Innovation Trends in Computing and Communication*, Vol. 3, No. 7, pp.4958–4961.

Bodei, C., Chessa, S. and Galletta, L. (2019) 'Measuring security in IoT communications', *Theoretical Computer Science*, Vol. 764, pp.100–124.

Datta, R., Joshi, D., Li, J. and Wang, J.Z. (2008) 'Image retrieval: ideas, influences, and trends of the new age', *ACM Computing Surveys (Csur)*, Vol. 40, No. 2, pp.1–60.

Dhall, S., Pal, S.K. and Sharma, K. (2014) 'Cryptographic primitives for multimedia security', *INROADS-An International Journal of Jaipur National University*, Vol. 3, No. 1, S. 2, pp.335–339.

Feng, X., Ye, M., Swaminathan, V. and Wei, S. (2017) 'Towards the security of motion detection-based video surveillance on IoT devices', *Proceedings of the on Thematic Workshops of ACM Multimedia 2017*, pp.228–235.

Furht, B. and Socek, D. (2003) *A Survey of Multimedia Security*, Technical Report.

Guo, X., Lin, H., Wu, Y. and Peng, M. (2020) 'A new data clustering strategy for enhancing mutual privacy in healthcare IoT systems', *Future Generation Computer Systems*, Vol. 113, pp.407–417.

Hamoudy, M.A., Qutqut, M.H. and Almasalha, F. (2017) 'Video security in Internet of things: an overview', *IJCSNS*, Vol. 17, No. 8, p.199.

Han, F., Qin, J. and Hu, J. (2016) 'Secure searches in the cloud: a survey', *Future Generation Computer Systems*, Vol. 62, pp.66–75.

Hsu, T-H. and Tung, Y-M. (2020) 'A social-aware P2P video transmission strategy for multimedia IoT devices', *IEEE Access*, Vol. 8, pp.95574–95584.

Huang, C-T., Tsai, M-Y., Lin, L-C., Wang, W-J. and Wang, S-J. (2018) 'VQ-based data hiding in IoT networks using two-level encoding with adaptive pixel replacements', *The Journal of Supercomputing*, Vol. 74, No. 9, pp.4295–4314.

Hurrah, N.N., Parah, S.A., Loan, N.A., Sheikh, J.A., Elhoseny, M. and Muhammad, K. (2019) 'Dual watermarking framework for privacy protection and content authentication of multimedia', *Future Generation Computer Systems*, Vol. 94, pp.654–673.

Husnoo, M.A., Anwar, A., Chakrabortty, R.K., Doss, R. and Ryan, M.J. (2021) 'Differential privacy for IoT-enabled critical infrastructure: a comprehensive survey', *IEEE Access*, Vol. 9, pp.153276–153304.

Imteaj, A. and Amini, M.H. (2019) 'Distributed sensing using smart end-user devices: pathway to federated learning for autonomous IoT', *2019 International Conference on Computational Science and Computational Intelligence (CSCI)*, IEEE, pp.1156–1161.

Jiang, B., Li, J., Yue, G. and Song, H. (2021) 'Differential privacy for industrial internet of things: opportunities, applications and challenges', *IEEE Internet of Things Journal*, Vol. 8, No. 13, pp.10430–10451.

Karie, N.M., Sahri, N.M. and Haskell-Dowland, P. (2020) 'IoT threat detection advances, challenges and future directions', *2020 Workshop on Emerging Technologies for Security in IoT (ETSecIoT)*, IEEE, pp.22–29.

Karie, N.M., Sahri, N.M., Yang, W., Valli, C. and Kebande, V.R. (2021) 'A review of security standards and frameworks for IoT-based smart environments', *IEEE Access*, Vol. 9, pp.121975–121995.

Khattab, A., Abdelgawad, A. and Yelmarthi, K. (2016) 'Design and implementation of a cloud-based IoT scheme for precision agriculture', *2016 28th International Conference on Microelectronics (ICM)*, IEEE, pp.201–204.

Kho, J.B., Kim, J., Kim, I-J. and Teoh, A.B. (2019) 'Cancelable fingerprint template design with randomized non-negative least squares', *Pattern Recognition*, Vol. 91, pp.245–260.

Kumar, D., Kumar, P. and Ashok, A. (2020) 'Introduction to multimedia big data computing for IoT', *Multimedia Big Data Computing for IoT Applications*, pp.3–36, Springer, Singapore.

Li, C. and Hu, J. (2014) 'Attacks via record multiplicity on cancelable biometrics templates', *Concurrency and Computation: Practice and Experience*, Vol. 26, No. 8, pp.1593–1605.

Li, D., Liu, W., Deng, L. and Qin, B. (2021) 'Design of multimedia blockchain privacy protection system based on distributed trusted communication', *Transactions on Emerging Telecommunications Technologies*, Vol. 32, No. 2, p.e3938.

Li, Y., Jeong, Y-S., Shin, B-S. and Park, J.H. (2017) 'Crowdsensing multimedia data: security and privacy issues', *IEEE MultiMedia*, Vol. 24, No. 4, pp.58–66.

Liu, F. and Li, T. (2018) 'A clustering-anonymity privacy-preserving method for wearable IoT devices', *Security and Communication Networks*, Vol. 2018, pp.1–8.

Liu, W., Zhang, M., Luo, Z. and Cai, Y. (2017) 'An ensemble deep learning method for vehicle type classification on visual traffic surveillance sensors', *IEEE Access*, Vol. 5, pp.24417–24425.

Lu, Y., Huang, X., Dai, Y., Maharjan, S. and Zhang, Y. (2019) 'Blockchain and federated learning for privacy-preserved data sharing in industrial IoT', *IEEE Transactions on Industrial Informatics*, Vol. 16, No. 6, pp.4177–4186.

Lu, Y., Wu, S., Fang, Z., Xiong, N., Yoon, S. and Park, D.S. (2017) 'Exploring finger vein based personal authentication for secure IoT', *Future Generation Computer Systems*, Vol. 77, pp.149–160.

Ma, S., Zhang, T., Wu, A. and Zhao, X. (2019) 'Lightweight and privacy-preserving data aggregation for mobile multimedia security', *IEEE Access*, Vol. 7, pp.114131–114140.

Maggo, P. and Chhillar, R.S. (2013) 'Lightweight image encryption scheme for multimedia security', *International Journal of Computer Applications*, Vol. 71, No. 13, pp.43–48.

Mekki, N., Hamdi, M., Aguili, T. and Kim, T-h. (2018) 'A real-time chaotic encryption for multimedia data and application to secure surveillance framework for IoT system', *2018 International Conference on Advanced Communication Technologies and Networking (CommNet)*, IEEE, pp.1–10.

Mishra, D., Vijayakumar, P., Sureshkumar, V., Amin, R., Islam, S.H. and Gope, P. (2018) 'Efficient authentication protocol for secure multimedia communications in IoT-enabled wireless sensor networks', *Multimedia Tools and Applications*, Vol. 77, No. 14, pp.18295–18325.

Mohanraj, I., Ashokumar, K. and Naren, J. (2016) 'Field monitoring and automation using IoT in agriculture domain', *Procedia Computer Science*, Vol. 93, pp.931–939.

Moravčík, M., Segeč, P., Hrabovský, J., Papán, J. and Uramová, J. (2016) 'Survey of real-time multimedia security mechanisms', *2016 International Conference on Emerging eLearning Technologies and Applications (ICETA)*, IEEE, pp.233–238.

Muhammad, G., Rahman, S.M.M., Alelaiwi, A. and Alamri, A. (2017) 'Smart health solution integrating IoT and cloud: a case study of voice pathology monitoring', *IEEE Communications Magazine*, Vol. 55, No. 1, pp.69–73.

Nahrstedt, K., Dittmann, J. and Wohlmacher, P. (2000) 'Approaches to multimedia and security', *2000 IEEE International Conference on Multimedia and Expo. ICME2000. Proceedings. Latest Advances in the Fast Changing World of Multimedia*, (Cat. No. 00TH8532), IEEE, pp.1275–1278.

Nath, M.P., Priyadarshini, S.B.B., Ray, M. and Das, D.S. (2021) 'An overview of multimedia technologies in current era of internet of things (IoT)', *Multimedia Technologies in the Internet of Things Environment*, Vol. 2, pp.1–23.

Nauman, A., Qadri, Y.A., Amjad, M., Zikria, Y.B., Afzal, M.K. and Kim, S.W. (2020) 'Multimedia internet of things: a comprehensive survey', *IEEE Access*, Vol. 8, pp.8202–8250.

Nie, H., Jiang, X., Tang, W., Zhang, S. and Dou, W. (2020) 'Data security over wireless transmission for enterprise multimedia security with fountain codes', *Multimedia Tools and Applications*, Vol. 79, No. 15, pp.10781–10803.

Noura, H., Chehab, A., Sleem, L., Noura, M., Couturier, R. and Mansour, M.M. (2018) 'One round cipher algorithm for multimedia IoT devices', *Multimedia Tools and Applications*, Vol. 77, No. 14, pp.18383–18413.

Obaidat, M.S., Rana, S.P., Maitra, T., Giri, D. and Dutta, S. (2019) 'Biometric security and internet of things (IoT)', *Biometric-Based Physical and Cybersecurity Systems*, pp.477–509, Springer, Cham.

Omrani, T., Rhouma, R. and Becheikh, R. (2019) 'LICID: a lightweight image cryptosystem for IoT devices', *Cryptologia*, Vol. 43, No. 4, pp.313–343.

Onesimu, J.A., Karthikeyan, J. and Sei, Y. (2021) 'An efficient clustering-based anonymization scheme for privacy-preserving data collection in IoT based healthcare services', *Peer-to-Peer Networking and Applications*, Vol. 14, No. 3, pp.1629–1649.

Oracevic, A., Dilek, S. and Ozdemir, S. (2017) 'Security in internet of things: a survey', *2017 International Symposium on Networks, Computers and Communications (ISNCC)*, IEEE, pp.1–6.

OVIC (2021) *Internet of Things and Privacy – Issues and Challenges* [online] https://ovic.vic.gov.au/privacy/internet-of-things-and-privacy-issues-and-challenges/ (accessed 30 November 2021).

Pandey, C., Sharma, S. and Matta, P. (2021) 'Privacy techniques for body sensor network in healthcare internet of things (HIoT) – a critical survey', *2021 5th International Conference on Computing Methodologies and Communication (ICCMC)*, IEEE, pp.385–389.

Pang, J., Huang, Y., Xie, Z., Han, Q. and Cai, Z. (2020) 'Realizing the heterogeneity: a self-organized federated learning framework for IoT', *IEEE Internet of Things Journal*, Vol. 8, No. 5, pp.3088–3098.

Punia, A., Gupta, D. and Jaiswal, S. (2017) 'A perspective on available security techniques in IoT', *2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, IEEE, pp.1553–1559.

Qiao, Y., Liu, Z., Lv, H., Li, M., Huang, Z., Li, Z. and Liu, W. (2019) 'An effective data privacy protection algorithm based on differential privacy in edge computing', *IEEE Access*, Vol. 7, pp.136203–136213.

Qin, Z., Yan, J., Ren, K., Chen, C.W. and Wang, C. (2016) 'SecSIFT: secure image SIFT feature extraction in cloud computing', *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM)*, Vol. 12, No. 4s, pp.1–24.

Qu, Y., Yu, S., Gao, L., Zhou, W. and Peng, S. (2018a) 'A hybrid privacy protection scheme in cyber-physical social networks', *IEEE Transactions on Computational Social Systems*, Vol. 5, No. 3, pp.773–784.

Qu, Y., Yu, S., Zhou, W., Peng, S., Wang, G. and Xiao, K. (2018b) 'Privacy of things: emerging challenges and opportunities in wireless internet of things', *IEEE Wireless Communications*, Vol. 25, No. 6, pp.91–97.

Rani, M.M.S., Mary, G.G. and Euphrasia, K.R. (2016) 'Multilevel multimedia security by integrating visual cryptography and steganography techniques', *Computational Intelligence, Cyber Security and Computational Models*, pp.403–412, Springer, Singapore.

Ratha, N.K., Chikkerur, S., Connell, J.H. and Bolle, R.M. (2007) 'Generating cancelable fingerprint templates', *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol. 29, No. 4, pp.561–572.

Rathee, G., Sharma, A., Saini, H., Kumar, R. and Iqbal, R. (2020) 'A hybrid framework for multimedia data processing in IoT-healthcare using blockchain technology', *Multimedia Tools and Applications*, Vol. 79, No. 15, pp.9711–9733.

Ren, Y., Zhu, F., Zhu, K., Sharma, P.K. and Wang, J. (2021) 'Blockchain-based trust establishment mechanism in the internet of multimedia things', *Multimedia Tools and Applications*, Vol. 80, No. 20, pp.30653–30676.

Ribaric, S., Ariyaeeinia, A. and Pavesic, N. (2016) 'De-identification for privacy protection in multimedia content: a survey', *Signal Processing: Image Communication*, Vol. 47, pp.131–151.

Shifa, A., Asghar, M.N. and Fleury, M. (2016) 'Multimedia security perspectives in IoT', *2016 Sixth International Conference on Innovative Computing Technology (INTECH)*, IEEE, pp.550–555.

Su, Z., Zhang, G. and Jiang, J. (2012) 'Multimedia security: a survey of chaos-based encryption technology', Karydis, I. (Ed.): *Mutimedia: A Multidisiplinary Approach to Complex Issues*, InTech, pp.99–124.

Thilagavathi, B. and Suthendran, K. (2018) 'Boosting based implementation of biometric authentication in IoT', *Journal of Cyber Security and Mobility*, pp.131–144–131–144.

Tian, Y., Zhang, Z., Xiong, J., Chen, L., Ma, J. and Peng, C. (2021) 'Achieving graph clustering privacy preservation based on structure entropy in social IoT', *IEEE Internet of Things Journal*, Vol. 8, pp.1–17.

Tzelepi, S., Pangalos, G. and Nikolacopoulou, G. (2002) 'Security of medical multimedia', *Medical Informatics and the Internet in Medicine*, Vol. 27, No. 3, pp.169–184.

Verma, S., Bhatia, A., Chug, A. and Singh, A.P. (2020) 'Recent advancements in multimedia big data computing for IoT applications in precision agriculture: opportunities, issues, and challenges', *Multimedia Big Data Computing for IoT Applications*, pp.391–416, Springer, Singapore.

Vishwa, A. and Hussain, F.K. (2018) 'A blockchain based approach for multimedia privacy protection and provenance', *2018 IEEE Symposium Series on Computational Intelligence (SSCI)*, IEEE, pp.1941–1945.

Voloshynovskyy, S., Koval, O., Deguillaume, F. and Pun, T. (2005) 'Multimedia security: open problems and solutions', in *Proceedings of NATO-Advanced Study Institute: Security through Science Program 2005*.

Wang, Q., Zhao, Y., Wang, W., Minoli, D., Sohraby, K., Zhu, H. and Occhiogrosso, B. (2017a) 'Multimedia IoT systems and applications', *2017 Global Internet of Things Summit (GIoTS)*, IEEE, pp.1–6.

Wang, S., Yang, W. and Hu, J. (2017b) 'Design of alignment-free cancelable fingerprint templates with zoned minutia pairs', *Pattern Recognition*, Vol. 66, pp.295–301.

Wang, X., Akgul, A., Kacar, S. and Pham, V-T. (2017c) 'Multimedia security application of a ten-term chaotic system without equilibrium', *Complexity*, pp.1–10.

Wang, Z., Qin, J., Xiang, X. and Tan, Y. (2021) 'A privacy-preserving and traitor tracking content-based image retrieval scheme in cloud computing', *Multimedia Systems*, Vol. 27, pp.1–13.

Wu, H-T., Zheng, K., Huang, Q. and Hu, J. (2021) 'Contrast enhancement of multiple tissues in MR brain images with reversibility', *IEEE Signal Processing Letters*, Vol. 28, pp.160–164.

Wu, Q., He, K. and Chen, X. (2020) 'Personalized federated learning for intelligent IoT applications: a cloud-edge based framework', *IEEE Open Journal of the Computer Society*, Vol. 1, pp.35–44.

Xia, Y., Chen, W., Liu, X., Zhang, L., Li, X. and Xiang, Y. (2017) 'Adaptive multimedia data forwarding for privacy preservation in vehicular ad-hoc networks', *IEEE Transactions on Intelligent Transportation Systems*, Vol. 18, No. 10, pp.2629–2641.

Xiong, J., Ren, J., Chen, L., Yao, Z., Lin, M., Wu, D. and Niu, B. (2018) 'Enhancing privacy and availability for data clustering in intelligent electrical service of IoT', *IEEE Internet of Things Journal*, Vol. 6, No. 2, pp.1530–1540.

Xu, C., Ren, J., Zhang, D. and Zhang, Y. (2018) 'Distilling at the edge: a local differential privacy obfuscation framework for IoT data analytics', *IEEE Communications Magazine*, Vol. 56, No. 8, pp.20–25.

Xu, J., Glicksberg, B.S., Su, C., Walker, P., Bian, J. and Wang, F. (2021) 'Federated learning for healthcare informatics', *Journal of Healthcare Informatics Research*, Vol. 5, No. 1, pp.1–19.

Xue, W., Shen, Y., Luo, C., Xu, W., Hu, W. and Seneviratne, A. (2021) 'A differential privacy-based classification system for edge computing in IoT', *Computer Communications*, Vol. 182, pp.117–128.

Yang, W., Wang, S., Zheng, G., Chaudhry, J. and Valli, C. (2018a) 'ECB4CI: an enhanced cancelable biometric system for securing critical infrastructures', *The Journal of Supercomputing*, Vol. 74, No. 10, pp.4893–4909.

Yang, Y., Zheng, X., Chang, V., Ye, S. and Tang, C. (2018b) 'Lattice assumption based fuzzy information retrieval scheme support multi-user for secure multimedia cloud', *Multimedia Tools and Applications*, Vol. 77, No. 8, pp.9927–9941.

Yang, W., Wang, S., Hu, J., Ibrahim, A., Zheng, G., Macedo, M., Johnstone, M. and Valli, C. (2019a) 'A cancelable iris- and steganography-based user authentication system for the internet of things', *Sensors*, Vol. 19, No. 13, p.2985.

Yang, W., Wang, S., Zheng, G., Yang, J. and Valli, C. (2019b) 'A privacy-preserving lightweight biometric system for internet-of-things security', *IEEE Communications Magazine*, Vol. 57, No. 3, pp.84–89.

Yongliang, L., Gao, W. and Liu, S. (2004) 'Multimedia security in the distributed environment', *APCC/MDMC'04. The 2004 Joint Conference of the 10th Asia-Pacific Conference on Communications and the 5th International Symposium on Multi-Dimensional Mobile Communications Proceeding*, IEEE, pp.639–642.

Yu, H., Wang, J. and Sun, X. (2019) 'Surveillance video online prediction using multilayer ELM with object principal trajectory', *Signal, Image and Video Processing*, Vol. 13, No. 6, pp.1243–1251.

Yu, S. (2016) 'Big privacy: challenges and opportunities of privacy study in the age of big data', *IEEE Access*, Vol. 4, pp.2751–2763.

Zhao, H., Qin, J. and Hu, J. (2012) 'An energy efficient key management scheme for body sensor networks', *IEEE Transactions on Parallel and Distributed Systems*, Vol. 24, No. 11, pp.2202–2210.

Zhou, L. and Chao, H-C. (2011) 'Multimedia traffic security architecture for the internet of things', *IEEE Network*, Vol. 25, No. 3, pp.35–40.

Zia, M.T., Khan, M.A. and El-Sayed, H. (2020) 'Application of differential privacy approach in healthcare data – a case study', *2020 14th International Conference on Innovations in Information Technology (IIT)*, IEEE, pp.35–39.

Zikria, Y.B., Afzal, M.K. and Kim, S.W. (2020) 'Internet of Multimedia Things (IoMT): opportunities, challenges and solutions', *Sensors*, Vol. 20, No. 8, pp.1–8.