HHS Public Access

Author manuscript

J Netw Comput Appl. Author manuscript; available in PMC 2022 February 01.

Published in final edited form as:

J Netw Comput Appl. 2021 February 01; 175: . doi:10.1016/j.jnca.2020.102918.

Security and Blockchain Convergence with Internet of Multimedia Things: Current Trends, Research Challenges and Future Directions

Mian Ahmad Jan[a], **Jinjin Cai**[b], **Xiang-Chuan Gao**[c,*], **Fazlullah Khan**[a], **Spyridon Mastorakis**[d], **Muhammad Usman**[e], **Mamoun Alazab**[f], **Paul Watters**[g]

[a]Department of Computer Science, Abdul Wali Khan University Mardan, Pakistan

[b]College of Mechanical & Electric Engineering, Hebei Agricultural University, Baoding, China

[c]School of Information Engineering, Zhengzhou University, China

[d]College of Information Science & Technology, University of Nebraska Omaha, USA

[e]School of Science, Engineering and Information Technology, Federation University, Australia

[f]College of Engineering, IT and Environment, Charles Darwin University, NT, Australia

[g]School of Engineering and Mathematical Sciences, Latrobe University, Australia

Abstract

The Internet of Multimedia Things (IoMT) orchestration enables the integration of systems, software, cloud, and smart sensors into a single platform. The IoMT deals with scalar as well as multimedia data. In these networks, sensor-embedded devices and their data face numerous challenges when it comes to security. In this paper, a comprehensive review of the existing literature for IoMT is presented in the context of security and blockchain. The latest literature on all three aspects of security, i.e., authentication, privacy, and trust is provided to explore the challenges experienced by multimedia data. The convergence of blockchain and IoMT along with multimedia-enabled blockchain platforms are discussed for emerging applications. To highlight the significance of this survey, large-scale commercial projects focused on security and blockchain for multimedia applications are reviewed. The shortcomings of these projects are explored and suggestions for further improvement are provided. Based on the aforementioned discussion, we present our own case study for healthcare industry: a theoretical framework having security and blockchain as key enablers. The case study reflects the importance of security and blockchain in multimedia applications of healthcare sector. Finally, we discuss the convergence of emerging technologies with security, blockchain and IoMT to visualize the future of tomorrow's applications.

[*]Corresponding author iexcgao@zzu.edu.cn (Xiang-Chuan Gao).

Keywords

Internet of Things; Internet of Multimedia Things; Security; Privacy; Trust; Blockchain; Convergence; Emerging Applications

1. Introduction

Internet of Multimedia Things (IoMT) is gaining momentum nowadays due to the advent of multimedia data and interconnectivity of real-world physical devices [1]. Multimedia devices such as, IP-enabled cameras and laptop-controlled drones, enable the firefighters and border patrol agents to conduct numerous operations. These drones can also assist in aerial surveying to maintain infrastructure by examining power lines, and roads or even conducting geologic surveying. The software of these drones are configured to support various communication protocols, e.g. Real-time Transport Protocol (RTP) [2] and Real Time Streaming Protocol (RTSP) [3]. This configuration ensures the retrieval of a drone's video feed in real time. Body cameras [4, 5] are another use case gaining more and more attention nowadays. Body cameras uses RTP to assist law enforcement agencies and first responders in conducting important security operations. These agencies rely upon real-time information to determine what is happening and respond to the situation on time. Robots also generate a huge amount of multimedia data. From underwater submersibles [6], radiation tests [7], healthcare [8] to industrial automation [9], robots are being created for a variety of multimedia applications.

Despite the immense benefits that IoMT brings, the increased interconnectivity among the devices brings a lot of cyber security risks [10]. The increased demand for multimedia and non-multimedia devices and the quest for convenience have left data privacy and security as a second priority. Securing the IoMT devices require the input of consumers, device manufacturers, and government regulatory agencies. There are numerous challenges that need to be resolved for secured communication among the devices. Once a device is manufactured, it is then replicated and mass-produced that exposes all these devices to threats if anyone among them is maliciously manipulated [11]. In an IoMT infrastructure, different manufacturers specialize in manufacturing a specific component and follow different industrial standards [12]. As a result, components used to make a single device might end up having different security standards. This difference in security standards lead to incompatibility or induce vulnerability. Most of these devices use industrial-specific protocols that are not supported by the existing enterprise security tools [13]. As a result, these tools such as firewalls and Intrusion Detection System (IDS) are unable to support the industrial-specific protocols. Due to the interconnection of these devices, compromising their protocol stack makes the whole network vulnerable. Moreover, these devices are not easily patched [14]. They are released in tens of thousands and as consumers rush to purchase them, very few follow-up with the device manufacturers to install software upgrades. Also, most of these devices use device-specific software with low usability making it difficult for users to update the software without an expert [15]. Finally, most of these devices come with default passwords and their manufacturers do not have proper

guidelines for the consumers to change them [16, 17]. On the other hand, the consumers also don't bother to change these passwords that lead to an increased risk to malevolent exposure.

The conventional security approaches, i.e., authentication, privacy and trust, have a pivotal role in mitigating adversarial threats faced by these devices [18, 19]. However, they are not sufficient as the data need to be securely delivered to the right place, at the right time, and in the right format [20]. There are numerous challenges that need to be resolved to fulfill this goal. First, most of the existing IoMT systems rely on non-standardized and incompatible protocols that make the configuration relatively complex [21]. Second, the privacy concerns of these devices are rather complex [22]. Third, there does not exist well-defined standards for the authorization and authentication of these devices [23]. Fourth, the security standards for platform configurations are immature [20]. Lastly, the IoT prototypes mostly rely on centralized communication models, also known as brokered client/server paradigms [21, 18]. The devices are required to connect via the Internet even if they are nearby to each other. The centralized communication models expose the underlying devices to a wide range of malicious threats. Blockchain, a distributed ledger technology, has the ability to overcome most of these challenges [24]. In literature, numerous blockchain frameworks have been proposed for IoMT applications. Due to their distributed nature, these frameworks reduce the operational and deployment overheads. Blockchain is an encrypted and distributed ledger technology for creating real-time records that are resistant to tampering. This technology provides a secured platform for the IoT and IoMT devices by interconnecting them in a reliable fashion, and at the same time, protects them against the adversarial threats that plague the centralized client/server models [25, 26]. The use of smart contracts ensures the privacy of device identity and data integrity. Blockchain supports peer-to-peer communication that reduces latency and communication overhead [25]. Together with conventional security approaches, blockchain technology has the potential to mitigate all adversarial threats faced by the real-world physical devices.

To secure the communication among the devices and also the devices themselves, a significant amount of literature exists. In this paper, we critically analyze the previous literature from reputable sources published in the past five years. Some of these works focused on the conventional security approaches, i.e., authentication [19, 27, 28, 29, 30, 31, 32, 33, 34, 35], privacy [19, 30, 31, 32, 33, 34, 35] and trust management [28, 29, 31, 32, 33, 34, 35, 36, 37, 38], to secure communication among the devices. There are others that cover literature on the use of blockchains and the challenges faced while implementing them in IoT for secured transactions among the devices [35, 39, 40, 41, 42, 43]. Nevertheless, the objective of these studies remains the same, i.e., to cover the latest trends and challenges faced during secured communication among the real-world physical devices. All these studies focus on scalar data only, and also did not cover ongoing large-scale industrial projects. Finally, most of these studies did not discuss any case study for their intended domain of applications. Motivated by research gaps in the existing literature, we present a comprehensive survey of our own. In Table. 1, a comparison of our survey against similar ones is made. The major contributions of our work are as follow.

- A detailed analysis of the conventional security approaches for IoMT is presented. Current trends in authentication, privacy, and trust management are

discussed and numerous research challenges faced by the IoMT are explored. The desirable features of these approaches are also highlighted. Together with blockchain, these features can have a significant impact on the future of IoMT. The emergence of blockchain does not necessarily mean that conventional security approaches are becoming obsolete.

- The convergence of blockchain and IoMT is discussed in view of the unique requirements imposed by multimedia data. This convergence highlights a number of research gaps that need to be explored. The key benefits of this convergence are also discussed that lay a solid foundation for multimedia-enabled blockchain platforms.
- Numerous large-scale industrial and commercial projects for IoMT are discussed that involve security, blockchain, or both as key enablers. These projects highlight the significance of our work from multimedia streaming applications' perspective. The scope, operational mechanism, and the intended applications are discussed, and research challenges are explored.
- A case study within the domain of our survey is presented for health industry. We design a theoretical framework of security and blockchain as the key enablers in Internet of Medical Things [44]. The roles of data confidentiality, privacy, trust, and blockchain are discussed to emphasize the significance of this survey from healthcare perspective.
- Finally, we discuss the convergence of emerging technologies with security, blockchain, and IoMT. We highlight a number of research gaps that need to be explored further. To this end, the future of various IoMT applications are discussed that can benefit from this convergence. We also suggest a number of improvements for applications to benefit from these converging technologies.

The rest of this survey is organized as follow. In Section 2, literature on conventional security approaches and challenges experienced by them while handling IoMT devices and their data is provided. In Section 3, blockchain and its convergence with IoMT is discussed along with key benefits, challenges, and multimedia-enabled blockchain platforms. In Section 4, numerous industrial projects are discussed to highlight the significance of this survey. In Section 5, a case study is presented that demonstrates the importance of security and blockchain in health sector. Section 6 highlights future trends and research directions in IoMT. Finally, the paper is concluded in Section 7.

2. Security in IoMT

Security provisioning is a major challenge faced by the IP-enabled physical devices that render their smart integration with the virtual world. The IoT architectures are supposed to deal with billions of such devices, interacting with each other and with other entities such as human beings and cloud platforms [46, 47]. Such interactions need to be secured for smooth exchange of information and service provisioning [48]. Similar to IoT, the IoMT encompasses a large number of heterogeneous devices, each with its own distinguishing features. The unique features of a device coupled with its heterogeneous nature of operation,

make security provisioning cumbersome and a complicated issue to address in an IoMT infrastructure. Most of the real-world physical devices are connecting with the Internet for the first time. As a result, we do not know how such devices will behave or react in the virtual world of Internet and the physical world of happening events. Integration of IP-enabled multimedia devices with the Internet requires one or more communication models [49]. This requirement will likely add some very ingenious and innovative malicious models. It is of utmost importance that such models should be prevented or at least some mitigating options should be in place to tackle their undesirable effects.

Developing a secured solution in an IoMT context is much more difficult than IoT and conventional Internet. Multimedia devices such as, robots and IP-enabled cameras, impose stringent requirements for the provisioning of data rate, available bandwidth, computational power, storage, QoS prioritization, and data flow management [50]. Besides, the heterogeneity of these devices and their unpredictable nature of multimedia traffic manipulation make things more complicated. It is important to understand the attributes, characteristics, and features of these IP-enabled multimedia devices and their underlying embedded technologies to combat various malicious models. The existing secured solutions for the Internet need to be assessed and adapted in an IoMT environment provided they suit the requirements of these multimedia *things*. However, profiling the secured solutions of Internet may not necessarily comply with IoMT's domain of applications. As a result, their adaptation in an IoMT environment may result in undesirable outcomes [11]. Each protocol of the Internet has its own intended domain of applications and specifications. The modification of a protocol's features may result in deviation from its original use of intend as many Internet-based protocols were designed for traditional computing platforms. The IP-enabled multimedia devices of IoMT were not kept in mind while developing these features. The existing secured solutions for IoT also require significant modifications for their applications to an intended domain of IoMT. At present, there exists very limited security-related literature in the IoMT context. We will analyze the available literature for IoT to determine their feasibility in IoMT domain. Besides, we will also focus on the limited literature available for security provisioning in IoMT to find their shortcomings. For security provisioning, the three key enablers are authentication, privacy and trust, as shown in Fig. 1. We will thoroughly analyze these enablers to determine their feasibility for IP-connected smart multimedia devices. The main objective of this analysis is to find research gaps that need to be filled for efficient utilization of these enablers in IoMT.

2.1. Authentication

Authentication is a key aspect of IoMT security that can easily lead to multiple breaches if approached inappropriately [51]. If our web backend believes that a malicious entity is acting as a legitimate device, then the former can start to do anything that our device has permission to do. It means that malicious entity can access and manipulate the confidential data, e.g. security camera's footage, audio streams, and other scalar information [52]. In Fig. 2, IP-enabled multimedia devices are connected with backend servers via a gateway. These devices provide multiple services to the end users. For example, a connected car provides video services, Voice over IP (VoIP), audio messages, and many other services to the drivers. Authentication allows only the legitimate devices to communicate with each other, their

gateways, and remote servers located at the cloud. This approach ensures that malicious entities are detected to protect the underlying network from various threats. These entities are capable to crash our entire web infrastructure with a single device.

In absence of authentication, an adversary can access the data of legitimate devices and replay to others. Unlike the sensor-embedded legitimate devices of IoMT, the adversary has sufficient computing power and other resources for launching one or more adversarial attacks. For example, an adversary may eavesdrop on the in-transit communication between a connected car and the gateway to intercept the data flows of multimedia streams. Unlike traffic flows, data flows requires seamless connectivity and do not tolerate QoS degradation [53]. Once the data flows are seized, they are replayed to other connected devices in the network. A refrigerator and a wash machine receive the services and features that were intended for a connected car, as shown in Fig. 2. With sufficient available resources, an adversary can launch a wide range of adversarial attacks, e.g. Denial of Service (DoS), Distributed DoS (DDoS), sybil, replay, sinkhole, malware, etc. A robust authentication scheme ensures that an underlying network remains protected from such threats [32].

There are numerous mechanisms for establishing robust authentication among the devices. However, when security is paramount, client-side SSL (Secure Sockets Layer) [54] is highly recommended. SSL is an industry-standard protocol to establish an encrypted and secured connection among the devices that operate over wired and wireless networks. However, it experiences intermittent connectivity, plugin problems, and higher certificate cost. On the other hand, the heterogeneous devices of IoMT operate over Low-power and Lossy Networks (LLNs) [55] and demand seamless connectivity, and low-cost certificates and digital signature for multimedia streaming [56]. In today’s world, smart homes, factories, and vital infrastructures are connected with the Internet. Security has never been more important for scalar and multimedia data generated by these applications. Multi-factor authentication (MFA) [57], of which two-factor authentication (2FA) is the most well-known, is highly resilient to fulfill the demands of these applications. Unlike conventional authentication, MFA focuses on a two-factor approach that makes it more secured and robust. MFA is a way of combining more than one level of security to control access to an underlying network. From a simple SMS code sent to a trusted smartphone to a code generator that creates single-use access codes, MFA is already used in many web applications. For MFA to work in the IoMT, it must be as simple as possible [58]. The tricky aspect of IoMT is that many smart devices do not have a screen or a keypad to enter a password. At the user level, it is vital therefore to consider "what is necessary and what is practical [31]". Security is important, but too much, or the wrong type, is often worse than no security at all.

For secured communication among the real-world smart devices, single-layer and multi-level authentications have widely been studied. In existing literature, both these approaches has been studied mostly in the IoT context. In [59], the authors proposed a single-level lightweight authentication approach for secured communication among the IP-enabled smart devices. The proposed approach is suitable for scalar data, and as such, lacks the support for multimedia streams. It imposes severe limitations on the available resources of smart devices, which is not the case with IoMT due to variable traffic rate and application-specific,

time-varying packet sizes. In [60], a lightweight authentication approach for resource observation in a smart environment was proposed. The identities of interacting clients and the server were validated before establishing an authentication session. The proposed approach lacks any experimental results to verify its feasibility for multimedia streaming applications. Besides, the packet size is limited to only 256 bytes, which is not the case with most of the multimedia data flows. In [61], a bootstrapping protocol was proposed to authenticate the smart connected devices. The proposed protocol is based on mother-duckling relationship and operates in three phases. In the first phase, any new device, known as duckling, interested to join the network sends a POST request to a multicast address associated with neighboring devices. The POST request aims to find a mother device for provisioning of security configurations. In the second phase, when the mother receives the POST request, it imprints a shared secret on the duckling. Once a positive response is received from the duckling, a secured channel for multimedia streaming is established between them. All other configuration information such as default gateway address and network prefix are provided in the third phase. In the proposed protocol, imprinting is usually accomplished by a user-specific action on the duckling, e.g. pushing a button or inserting batteries in duckling. Although, the proposed approach suggests a novel idea for secured transmission of multimedia streams, it lacks sufficient experimental results and detailed operational mechanism of the three phases. It is yet to be determined how good this protocol is for extremely resource-constrained smart devices, i.e., class 0 and class 1 devices [62]. Besides, the communication range between the mother and duckling needs to be investigated as well.

A two-factor authentication (MFA) was proposed for distributed IoT applications in [63]. It operates in two phases: registration and handshaking. In the registration phase, resource-constrained smart devices and end users acquire a certificate from a resource-rich Certificate Authority (CA). Once a cryptographic certificate is acquired, the smart devices are authorized to communicate with each other. The registration phase allows the devices to obtain the certificates. In the second phase, small clusters are formed in the network. Each cluster has a designated cluster head for managing the smart devices within that cluster. If an end user wants to communicate with a smart device in a specific cluster, it first needs to acquire a certificate from its cluster head. During the handshaking phase, the CA issues a certificate to the smart devices. The CA verifies the identity of each device and upon successful verification, a handshaking procedure is initiated. The proposed MFA uses complex cipher suites such as CERT_ECC_160_WITH_AES_128_SHA1. Furthermore, the CA grants a certificate having a 160-bit ECC [64] for key exchange, 128-bit AES [60] for bulk encryption, and SHA1 [65] for message authentication code (MAC). The proposed authentication approach assumes that each device has abundant of resources. Similar to IoT, the IoMT includes class 0 and class 1 devices, as shown in Table 2 [62]. These devices are extremely resource-constrained and have a simple network configuration. Class 0 devices are unable to communicate directly with Internet-enabled devices and mostly rely on gateways and servers for communication purpose. They have less than 10 KB Random Access Memory (RAM) and 100 KB flash memory. On the other hand, class 1 devices can only communicate directly with those devices that host TCP-enabled HTTP protocol. Although, they can run the Constrained Application Protocol (CoAP) [66] and its related

functionalities, they are refrained from communication with HTTP-based web-enabled devices and applications. Irrespective of IoT or IoMT, both classes are unable to support such complex cipher suites and cryptographic algorithms. In case of IoMT, apart from the class type, any designed authentication scheme needs to consider the nature of data as well. Moreover, the bandwidth-consuming and resource-demanding multimedia applications require extremely lightweight authentication schemes.

In IoT, most of the smart applications rely on User Datagram Protocol (UDP) at the transport layer for exchanging messages between a client and the server [67]. The UDP uses Datagram Transport Layer Security (DTLS) as the underlying platform for secured exchange of these messages. DTLS is a two-layered protocol architecture [68] with Record Protocol Payload (RPP) as the upper layer and Record Protocol (RP) as the lower layer. RPP consists of four protocol suites: handshake, alert, ChangeCipherSpec, and data. Handshake is used to initiate a connection between a client and the server, and exchanges security parameters between them. Alert is used for error signaling and closure of a connection. ChangeCipherSpec is a 1-byte long message transmitted between a client and the server for protecting subsequent records on just-negotiated cipher suite. Data suite contains the application layer's data. RP, on the other hand, adds a header to RPP and maintains the security of DTLS messages. In DTLS, handshaking can be classified into three categories [69].

1. No Authentication: Relies on application layer security and safeguards the smart devices against passive eavesdropping. However, it is not robust against active eavesdropping. An attacker can easily manipulate the data in-transit.
2. Server Authentication: Allows a client to authenticate the server using a Pre-Shared Key (PSK), Raw Public Key (RPK), or a certificate. It is effective against man-in-the middle attack.
3. Mutual Authentication: The client and server authenticate each other using a PSK, RPK, or a certificate. It is highly efficient and widely used authentication and encryption scheme in which both parties challenge the integrity and identity of each other.

If the DTLS record is larger in size, then the handshake messages suffer from fragmentation because it will not fit into a 6LoWPAN payload [70]. Each DTLS handshake message has a header of 25 bytes: 12 byte record header and 13 byte DTLS handshake header. At the physical layer of IEEE 802.15.4, there are only 127 bytes available [71]. With the inclusion of MAC layer, UDP, and 6LoWPAN adaptation layer header, only 60-75 bytes are left for DTLS handshake messages. Both 6LoWPAN and DTLS offer fragmentation. The former fragments the IPv6 packets into small data link layer packets. However, such fragmentation may not be an optimal choice for numerous energy-constrained devices. Although DTLS offers fragmentation, it incurs excessive overhead during this process. The IP-enabled devices are resource-starving and would require considerable buffer space to accommodate various fragments. As the messages may arrive out of order, hence considerable buffer space is required in order to accommodate them. This would require enhanced computations on part of each device in reordering these messages at some later stage. The situation gets worse and complicated once messages pertaining to the same flight are sent in parallel [72].

Retransmission of such packets would make the buffer management further complicated and an expensive choice.

2.1.1. Open Research Challenges—There are numerous challenges that needs to be resolved for efficient deployment of DTLS[1] on IP-enabled multimedia devices. These challenges include:

- The IoMT devices come from different manufacturers, hence, interoperability among such devices is a major issue. The IoMT implementations that speak both DTLS 1.2 and DTLS 1.0 are interoperable with those that speak only DTLS 1.0 [68]. Hence, interoperability issue can be resolved with backward compatibility.
- The DTLS sessions are expected to last longer. As a result, the need of renegotiating a new cipher suite is minimal and thus it needs to be avoided. The DTLS handshake is pretty straightforward if performed with PSK. However, the use of RPK makes the process highly complicated and resource-intensive. RPK not only utilizes the public and private keying materials of a certificate but also requires the ephemeral keys [73], which is a burden on the IP-enabled devices of IoMT.
- The DTLS implementation on resource-constrained devices of IoT consumes a considerable amount of code space. This implementation leaves behind very little choice for other functionalities such as 6LoWPAN stack and application layer codes [72]. The implementation of a single PSK of DTLS consumes approximately 16 KB flash and 4 KB RAM. The use of RPKs and certificates will require a considerable amount of these resources. Hence, sufficient and adequate modifications are required in various IoT-supported resource-constrained devices to adapt to IoMT functionalities.
- Similar to IoT [67], most of smart multimedia devices are not capable to support a large chain of cipher suites. Hence, only a few cipher suites need to be embedded in the devices. However, the choice and selection of such cipher suite need to be smart enough in order to provide security for various applications. Ideally, such crypto primitives need to be re-used in order to provide various security features.
- DTLS supports intermittent connectivity among the smart devices. However, the multimedia applications require seamless and interoperable communication without degradation in the QoS.
- For various Voice over IP (VoIP) applications, DTLS-SRTP is widely used [74]. This protocol does not rely on the trustability of the certificates that are used for DTLS. Instead, fingerprints are used to allow users for manually checking if the call is encrypted end-to-end. DTLS-SRTP provides end-to-end encryption, detection of man-in-the-middle attacks. Moreover, there is no longer a need to trust the certification authorities. However, it adds excessive overhead at the

[1]We focus mainly on DTLS 1.2 [68]

beginning of calls that causes significantly higher CPU load. Hence, it is not feasible for those application scenarios that cannot tolerate delays.

- The IoMT devices are expected to operate in a distributed environment with stringent minimum-delay requirements imposed on them. For this purpose, distributed security measures need to be in place to safeguard these devices. The existing authentication approaches are centralized in nature and suffer from scalability and latency issues [75]. For IoMT devices and their underlying applications, delay-sensitive authentication and access control approaches are required. For example, in a safety-critical application, a battery-powered aerial drone may require to perform authentication with multiple command stations in a very short period of time for the exchange of sensitive information [76]. The decentralized nature of blockchain can fulfill the requirements of such applications due to its improved reliability, fault tolerance and unforgeability. These features offer a good solution for authentication challenges. Blockchain enables the integration of smart contracts, which offer a fine-grained access control for time-critical and delay-sensitive IoMT applications.

2.2. Privacy in IoMT

IoMT has the potential to find its application in a diverse range of domains such as smart automation, smart traffic management, smart healthcare, smart surveillance. For all these applications, individuals demand privacy of their personal information related to their habits, behavior, and interaction with other others [77]. In the context of privacy, one thing that is often overlooked with multimedia streaming smart devices is that they usually need to connect to other devices in order to work [78, 79]. So, by proxy, they operate under the same email address, IP address, and phone number. This means that IoMT privacy is still dependent on the privacy of all other devices. So if one has a bad privacy policy or weak privacy settings on his/her smartphone, for example, this new device will suffer from the same data leakage as others. For that reason, it is better to think of these devices as components of a bigger network. A washing machine, connected car, surveillance cameras or television, what if someone could put the data from these devices together? If the IoMT reaches its full potential, one will be surrounded by devices that act as a surveillance network that can constantly monitor and monetize our data [78]. For example, if one have a smart lighting system at his/her house that can be control with a phone, companies could know when the person is at home and when he/she is sleeping.

These fascinating things are surely convenient, but it should be individuals' choice whether to let companies know their personal information or sell it to third parties. There are risks beyond privacy scandals and data breaches. This new flood of multimedia data would give corporations the power to reach even further into our lives. It is becoming apparent that both people and businesses are getting lured into the world of smart connected devices without giving much thought as to what it may do to their privacy. Manufacturers, sensing a business opportunity, are ignoring privacy concerns to focus on how to pair multimedia and scalar data collection with increased convenience and functionality. Since most consumers ignore privacy concerns while purchasing, it is not surprising that companies are neglecting privacy regulations. There is also, of course, the fact that all the data they gather is most likely

another source of revenue. While privacy concerns persist in the IoMT space, there are exceptions. For example, iRobot [80], the company behind the Roomba automatic vacuum cleaner, has a very transparent privacy and data sharing policy. They claim to never sell customer data and share it with third parties, only if the user chooses to do so. Besides, they delete all of the data upon the user request.

The emergence of Intelligent Video Surveillance System (IVSS) [81] has put privacy preservation as the main focus of attention. IVSS extracts the confidential information from CCTV systems, e.g. an individual's location, behavior, traveled paths, etc, as shown in Fig. 4 [81]. The retrieved information is stored at remote backend cloud servers for future use. For secured storage, the extracted information need to be encrypted to prevent it from adversarial threats. However, encryption of video data is not a simple and resilient solution to protect them from malicious threats. Typically, video data are huge in volume and decrypting them back to their original form incur excessive processing overhead [82]. The conventional approaches for privacy preservation of videos store their meta-data as plain-text at the cloud. However, plain-text are easy to access and decrypt. Meta-data alone is sufficient to leak and disclose a considerable amount of original video data, e.g. CCTV video recordings of IVSS [82]. In literature, privacy of video data is achieved via four different approaches: privacy masking, partial privacy, cloud-based privacy, and fog-based privacy. A comparison between these approaches is made in Table 3.

2.2.1. Privacy Masking vs. Partial Privacy—Privacy masking [83, 84] modifies the video contents that prevents leakage of an individual's facial information. To accomplish this task, various mechanisms such as blurring, facial-region removal, and pixilation are used. These mechanisms ensure that original footages are not recovered properly if the videos are intercepted by an adversary. However, with the advent of deep resolution and big data-enabled heterogeneous video streams, privacy masking suffers to recover blurred and pixelated facial regions to their original forms. In applications such as, IP-enabled connected cars, intelligent transportation system (ITS) and industrial automation, privacy masking performs poorly due to stringent requirements of deep resolution and heterogeneity of data.

To overcome the limitations of privacy masking, partial privacy was proposed [85]. This approach aims to perform partial encryption of regions of interest (ROI). The ROI encrypts one or more regions of a video, e.g. face, arm, chest, etc. Encryption restricts the recognition of RIO, and at the same time, enables the recovery of original video provided that the same encryption key is available for decryption. Despite its advantages, partial encryption lacks any explanation about how the meta-data of encrypted RIO is generated and protected. For partial privacy, policies and guidelines need to be in place to decide the modification of video frames or images and also how, when and which portion of the data need to be altered. Denaturing is a set of guidelines that determine the privacy policies [86]. It determines the level of privacy and video analytics based on the value of data. For example, blank videos require perfect privacy but have zero value. On the other hand, video streams with high-critical data require perfect privacy with highest value for video analytics. A balance of privacy level with value of data is a policy issue and varies across different contexts and individual. For example, the IVSS deployed to monitor a large shopping mall may have tens

or hundreds of smart surveillance cameras [85]. These cameras are part of a single integrated system controlled by the mall administration. In this context, mall-wide policies need to be in place for efficient surveillance. The mall administration may implement a default policy to blur faces of each individual. However, universal privacy policy has its own limitation. For example, an individual in the hair salon within the mall may want to keep an eye on his/her children playing with the toys. In this case, face denaturing may not be applicable.

2.2.2. Cloud-based Privacy vs. Fog-based Privacy—Cloud-based privacy [81, 87] relies on SSL protocol [54] for privacy preservation of video footages at the cloud. This approach uses compressed videos, e.g. H.264, H.265, and still images [88]. The recorded videos are compressed at the in-field surveillance cameras and a region-based privacy is applied using an encryption key. These encrypted videos are transmitted to cloud data servers for storage that are subject to normal processing. Only authorized users are capable to fully recover the original videos that were recorded and compressed at the cameras. Both the cloud and cameras use a shared key for encryption/decryption. In [89], a local differential privacy classification (LDP) was proposed for cloud data centers. Initially, Laplace noise is added to the sensitive data generated by IoMT devices. The noise changes the mining pattern of information and it becomes difficult for an adversary to retrieve the original information. The data centers use LDP for data mining of Laplace noise. Cloud-based privacy has its own limitations. Smart IoMT devices incur higher latency and require considerably higher bandwidth due to overhead associated with large-sized videos. Besides, the heterogeneity of smart devices makes privacy preservation a challenging task to accomplish at the data centers.

Fog computing has recently gained popularity by shifting the intelligence and resources from cloud data centers to the network edge [90]. For this purpose, various privacy preserving techniques have been proposed to perform encryption of streaming data generated by smart applications of IoMT. In [91], the authors presented a fog security service (FSS) that enables the fog layer to distribute private keys among the IP-enabled smart devices. The introduction of an extra layer between the perception layer and application layer of IoMT incurs an additional overhead. In [91], a cloud-fog-local video encryption framework was proposed. The fog layer provides the computational resources required for encrypting the videos generated by the underlying applications. For privacy preservation, each video is divided into segments and each segment is considered as an encryption content. In fog-based privacy, the fog layer is privacy enabler for smart multimedia applications of IoMT. However, the limited resources of fog layer is not sufficient for robust privacy preservation of resource-consuming videos, e.g. H. 265 compressed videos with higher pixels and resolution. In this case, the fog layer is unable to preserve the privacy of high data rate live-streaming applications.

2.2.3. Open Research Challenges—IoMT has the potential to provide ubiquitous access to a diverse range of real-world smart devices. An unrestricted access to huge amount of data generated by these devices poses numerous privacy challenges that need to be addressed. Some of the major challenges are:

- Most smart devices fail to encrypt the data that is being transferred, even when they are using the Internet. In case of IoMT, the data streams are either in burst or much larger in size, and it becomes a challenging task for resource-constrained devices to encrypt such data. Various options are available to encrypt such streams, e.g. streams can be encrypted either per-burst or per-packet basis.
- In IoMT, a large number of users and devices rely on weak and simple passwords and authorisations. Many devices accept passwords such as 12345. To protect the data and devices from malicious attacks, it is important to use passwords that are difficult to crack. These passwords need to comply with limitations imposed on the available resources of the devices.
- Most devices are configured to use the default username and password, posing severe privacy threats to confidential data. A more convenient and optimal solution would be hard-code security primitives on these devices.
- Most of the existing solutions have a web/mobile interface for device management. Such an interface is vulnerable to poor session management, cross-site scripting vulnerabilities, and weak default credentials.
- Physical devices in healthcare sector collect atleast one piece of personal information. These devices collect details such as data of birth, user name, etc. Because most of these devices send information across the network without any encryption, severe privacy risk remains at stack. Privacy risk arises when the devices collect and aggregate data fragments that relate to their services. For example, a regular purchase of different food items may reveal the religion or health information of a consumer.
- In most of the IoMT applications, the data is highly private and face numerous privacy-related challenges while being exchanged. For example, in healthcare systems, privacy of data needs to be preserved due to the presence of sensitive information in it. Most of the existing data sharing approaches for healthcare use a centralized architecture that requires a centralized trust management. As a result, it becomes extremely difficult to provide robustness against failure and data exposure [92]. To resolve these issues, the distributed architecture of blockchain can provide efficient and resilient solution by preserving the privacy. Instead of a centralized architecture, the distributed architecture of blockchain provides a secured storage for the data and maintains high level of privacy. However, there are numerous challenges that need to be addressed while using blockchain for privacy preservation. For example, excessive delays in the verification of transactions and cost associated with using blockchain.

2.3. Trust in IoMT

Trust among the communicating smart devices is one of the most important factor for reliable data transmission [38]. Both multimedia and non-multimedia devices often do not take good care of the data they collect from the individuals. Over 90% of data transactions on these devices are not fully encrypted [36]. Apparently, the problem is that many companies have large numbers of consumer-grade devices on their networks.

In addition, many devices are attached to the companies' general networks, and if that network is breached, both multimedia and non-multimedia devices and their data may also be compromised [93]. In some cases, ownership of the data can raise surprisingly serious trust concerns [94]. For example, sleep apps gather highly personal information. These apps have knowledge about when individuals go to sleep, and when they toss and turn. Legal policies and regulations are needed that should decide the trustworthiness of such applications and their manufacturers.

In our smart connected world, Zero Trust is gaining popularity nowadays [95]. Zero Trust requires that security starts with the user, but interestingly, it is not limited to the user identity. Security must focus on, where the threat is most likely to occur. The network-enabled smart devices introduce a massive area of potential compromise for networks and enterprises. As a result, security architects are being forced to re-examine the concept of identity. Essentially, every connected thing has an identity and must be under consideration within the Zero Trust Framework, i.e., users, devices, virtual infrastructure, and cloud assets [76]. Every device is unique and has its own distinguishing features. Truly understanding devices requires much more than simply identifying their IP addresses, manufacturers and model numbers. It is important to gain detailed insight into every device on the network, including its business context and potential for risk. This is where accurate situational awareness makes all the difference. Consider the most common category of IoMT devices: IP-connected cameras [96]. The same camera often performs very different functions. For example, is the camera used for video surveillance or for video conferencing? In financial services, the camera might be used to monitor customers during transactions or built into an Automated Teller Machine (ATM) for scanning cheque deposits. The video feeds from each of these cameras need to share communication paths with different data center applications and cloud services. As such, the concept of device identity and context is foundational for Zero Trust security.

Besides Zero Trust, another important aspect is Trust management (TM) [36]. It has an important role in our smart connected world for reliable data fusion and mining. TM enhances user privacy and data security by providing context-aware intelligence. It allows the individuals to overcome the perception of risk and uncertainty. It ensures users' acceptance and usability of various services and applications, offered by multimedia and non-multimedia devices. TM has the ability to improve security, privacy, usability, and dependability of the devices and their underlying networks. By combining TM with other management activities such as identity management, power management, resource management, the users can obtain interdisciplinary and cross-domain benefits. In literature, TM has widely been studied to achieve users' confidence and trust on the use of smart devices and their underlying networks. TM can be classified into four classes [97]. In this section, we discuss these four classes and compare them in Table 4.

2.3.1. Recommendation-based—In this technique, trust is evaluated based on prior experience of using trusted entities and their recommendation is taken into account [98, 99]. Assume a large-scale IVSS system in which there are a number of connected cameras. These cameras transmit their data to the cloud data centers via relay devices. The data centers constantly monitor the cameras and relay devices to detect their behavior. Based on

this operational behavior, a trust factor is associated with each camera and relay device. If any adversary sneaks through this network and route data from one or more cameras, the latter can inform the cloud servers about the presence of malicious entity in the network. Besides, the relay nodes also report any irregular behavior or pattern to the data centers. Recommendation-based TM is beneficial for the discovering of misbehaving devices, be they genuine or malicious, for making informed decisions on the selection of routing paths [100]. It helps in the identification of trustworthy recommenders and provide detailed information about recommendation-based trust evaluation and calculation procedures [101]. The existing recommendation-based approaches [98, 99, 100, 101] are highly adaptive and scalable in view of the unique features of smart devices and heterogeneous deployment environments. However, they provide low accuracy and have much lower integrity.

2.3.2. Prediction-based—In this technique, each smart device evaluates the trustworthiness of its peers [102]. This technique is used when a new device joins the network and starts communication with its neighbors. By using prediction-based TM, not only malicious devices are detected but the network security and robustness are also improved [103]. Based on this technique, devices with low trust-level are avoided for communication. The capabilities and interest of devices play a major role in prediction. For example, surveillance cameras monitor a particular region and have the same interest. If one or more cameras is unable to provide accurate view of happening events in the region of interest, the remaining cameras may refrain from communication with it. Moreover, the heterogeneity of applications has a central role in prediction-based TM. As an example, the surveillance cameras are more interested to communicate directly with their peers rather than interacting with smart devices deployed for smart farming. The existing prediction-based approaches [102, 104, 105, 106] have higher scalability and accuracy but they do not guarantee trust evaluation results.

2.3.3. Policy-based—In this technique, a policy is defined for the system or network behavior. Policy works similar to a constraint expressed using natural language or mathematical notation [107]. Policy is a set of rules for trust evaluation. A minimum trust threshold needs to be specified to authorize access and to control the authorization level [108]. This type of TM works well in those environments that require automatic responses based on the network conditions [109]. For example, the relay devices in smart surveillance system can be bounded to justify their presence in the network based on a pre-defined trust-level. If they satisfy the pre-defined condition, they can communicate with the surveillance cameras and cloud data centers. Alternatively, the data centers may only query those relay nodes that have satisfied a pre-defined trust-level for accessing some critical data gathered by the surveillance cameras. The existing policy-based approaches [108, 109, 107, 110] have higher adaptability, accuracy and reliability. However, most of them do not consider the heterogeneity of the devices.

2.3.4. Reputation-based—Reputation is used to build trust or distrust based on the past observations [111]: good or bad. This technique allows each device to rate its peers, helps in feedback collection, and aggregation of collected feedbacks in a distributed or centralized fashion. Based on the aggregate feedbacks, each device generates a reputation score within

the network [112]. This technique improves the confidential level of one device on another, and at the same time, abnormal activities are detected [113]. Due to continuous streaming data in the smart surveillance system of Fig. , a reputation score will significantly impact the performance of the network because trustworthy routes will be dynamically formed for reliable transmission of data. Monitoring the reputation score enables the cloud data centers to extract useful information from the underlying network with much lower latency, reliability and confidence. The existing reputation-based approaches [111, 113, 114, 115] suffer from device heterogeneity and integrity [116].

2.3.5. Open Research Challenges—IoMT faces numerous trust-related issues that need to be resolved to ensure confidence of the users in its products and the operational networks.

- Most of the trust management techniques lack a concern on context-awareness and their results are not personalized. As a result, it becomes difficult to provide intelligent services offered by the smart devices.
- Most of these techniques are designed either for the devices, mobile applications or the backend servers. However, there does not exist a single approach that focus on all these entities. A holistic approach is required that addresses all the entities of an IoMT ecosystem.
- The existing literature lacks a comprehensive and concise Trust Management Framework (TMF) for supporting the confidence of users in the devices and their underlying networks.
- Though, various trust computing platforms have been proposed in literature, they require heavy computation and are complicated for resource-starving smart devices. For these devices, lightweight platforms needs to be designed to combat DoS, DDoS, and other attacks.
- Trustworthy data fusion and mining demand a highly accurate, precise and holistic approach to extract useful features from the gathered data. Not only the data but their origin and intermediaries, i.e., relay devices, need to be trustworthy.

3. Blockchain and IoMT Convergence

Most of the IoMT infrastructures are heavily centralized and suffer from a single point of failure. The centralized nature of IoMT products hinder their widespread adoption because they raise privacy, trust, and security concerns [117]. Moreover, the centralized infrastructure results in higher latency for the end-to-end communication among the multimedia applications generating voluminous traffic, e.g. smart cities, healthcare, industrial automation, etc [118, 42]. To reduce the latency among such applications, these infrastructures rely on content delivery networks (CDNs), network accelerators, and dedicated connections [119]. In recent years, these applications use a completely decentralized infrastructure to record and process multimedia transactions of smart connected devices. The presence of a decentralized and distributed infrastructure enables

these applications to have reduced latency. Blockchain, a distributed ledger technology [39, 40, 41], is a continuously growing list of digital records in packages, also known as blocks. The blocks are linked and secured using cryptography [120], and are stored in a linear chain. Each block in the chain contains data that are cryptographically hashed and time-stamped. Blockchain uses a decentralized network and is seen by many as the technology that will be transforming the future of Internet in times to come. Every major technological company of the world currently acts as a centralized body when it comes to data storage, and payment processing. With the decentralization principle on which the blockchain works, our data will no longer be in the hands of few centralized entities. Thus, reducing the risks of hacking and information theft. The main advantage of blockchain is that the data remains completely secured, authentic, and tamper-proof on these chains. Blockchain technology enables a system of maintaining data that is decentralized, tamper-proof, and trustless. As the success of IoMT depends on its ability to keep the multimedia data flows and scalar traffic secured and confidential, the use of blockchain can transform the IoMT industry to a new horizon [35]. In Fig. 5 [121], we illustrate the use of blockchain for video surveillance in a smart city.

In today's world, a number of innovative blockchain platforms are leading the charge in revolutionizing the world of smart connected devices [122]. IoMT applications such as smart cities, industrial automation, and healthcare generate real-time multimedia streams using surveillance cameras and robots. These cameras and robots are centralized in nature and are prone to various security breaches. However, with the integration of IoMT and blockchain, these devices are becoming decentralized and their smartness is getting enhanced using the advanced facial recognition technology, object detection and real-time video analysis [123]. For example in smart cities, the aim is to create a smart surveillance system using the established computer vision technology. The use of decentralized cameras enables the surveillance system to detect possible threats ahead of crimes being committed and as a result, much more efficient action can be taken [124]. As an example, a face can be blacklisted on the network, in the instance of banned customers. If this face is detected on the video surveillance, the owners will be alerted via push notification to their phones. A typical blockchain-enabled video surveillance for a smart city is shown in Fig. 6.

At present, only minor research work exists on the convergence of blockchain and IoMT to secure data flows of smart devices, i.e., images, audio and video. In [121], a distributed and tamper-proof media transaction framework was proposed to preserve data security. This work concentrated on still images, and lacks any discussion on securing the video streams. In the existing literature, recording the integrity of video streams using blockchain has been focused mainly on individual videos. In [125], the authors recorded videos' integrity from the dashboard of a car for a smartcity surveillance application. These videos are recorded in the event of head-on collision. An android-based system for automatic detection of collision using the built-in accelerometers was used. The videos are cryptographically hashed and their hashes are recording on bitcoin chains using OriginStamp protocol [126]. In [127], an android-based, hashed-enabled blockchain approach was proposed to preserve the integrity of videos in a smart city. Unlike [125], this work considered the integrity of multiple videos of a smart surveillance system. In [128], a novel blockchain-enabled approach was proposed using adaptive block sizes for video streaming in Mobile Edge Computing (MEC). The

authors devised an incentive-based mechanism to facilitate the collaboration among video transcoders, consumers, and content creators. The block sizes were adapted for blockchain-enabled video streams. In blockchain, the size of a block has a significant impact on the performance of video streaming applications. Higher number of transactions can be included on the blocks with larger sizes that enhances the throughput of the chain [129]. However, with an increase in the size of a block, the propagation delay increases that downgrades the performance of a blockchain [130].

3.1. Key Benefits

In this section, we discuss some of the key benefits of integrating blockchain with IoMT. These benefits include:

3.1.1. Cybersecurity—The convergence of blockchain and IoMT provides exceptional defence against cyberattacks [131]. Blockchain treats the messages exchanged among the smart devices as transactions. These transactions are validated by smart contracts. Transactions are recorded in blocks and are arranged in the right sequence and assigned a timestamp, when they are added. The blockchain platforms use cryptographic algorithms that make the consumers' data more secured, private, and prevent any previous records from being altered. The architectural design of a blockchain platform provides a high-level security. If some of the devices are hacked, it will not effect the entire system and its performance. Moreover, the use of machine learning approaches enables the automation of real-time threat detection [132].

3.1.2. Introduces Smart Contracts—Blockchain is designed to serve as a basic layer for IoMT applications that involve transactions and interactions, and smart contracts play a significant role in it [25]. These contracts are carried out automatically without requiring intermediaries to approve or authenticate a transaction when specific conditions are met. These contracts bring secure and autonomous functioning, cheaper and faster transfers, and decreased vulnerability of data security for smart devices. Smart contracts make billing processes easy and comfortable. Thus, complicated payment systems are no longer required. A transaction is executed, tokens are transferred, and these processes are clear and transparent on blockchain. Smart contracts are gaining popularity in various applications such as smart retail, health 4.0, smart city, etc [133, 134, 135].

3.1.3. Decentralization—In contrast to traditional centralized architecture, the use of blockchain platforms improve the fault tolerance of IoMT [122]. A single blockchain runs on thousands of IP-connected smart devices. As a result, a single point of failure does not disable the entire network. Moreover, in a decentralized system, the stored and processed data streams are not controlled by a single device.

3.1.4. Trust—Blockchain enables a trust factor among the transacting parties [76]. The users are no longer required to trust centralized entities for handling their data streams. As a result, malicious third party entities are prevented from accumulating the private data of users. Blockchain enables faster settlements for contracts without the need for trusted intermediaries.

3.1.5. Reduces Cost—Blockchain significantly reduces the connectivity costs among the devices by eliminating the necessity for the infrastructure [122]. Hence, no additional administrative, service maintenance, and setup costs are required.

3.1.6. Transparency—Blockchain is a distributed ledger and each devices of IoMT can share a copy of the transaction [136]. As a result, each device can access the documentation of a transaction and the changes made to it.

3.1.7. Consistency—A clear picture of IoMT and blockchain convergence has transformed the way data is exchanged and maintained [122]. Both these technologies provide a consistency while dealing with the data. Blockchain provides secured methods to transfer information among the smart devices and their participants.

3.2. Open Research Challenges

The convergence of IoMT and blockchain paves the way for a wide range of potential multimedia applications. Despite the aforementioned benefits, this convergence faces numerous challenging issues that need to be addressed. Some of these issues are:

3.2.1. Transcoding—Blockchain-enabled video streaming faces a number of challenges. Among them, video transcoding is a major concern. The original video contents on the blockchain platforms need to be transcoded, i.e., converted into multiple representations in different bitrates, qualities, video codec and resolution, for the heterogeneous devices and users [137]. Video transcoding is a resource-intensive and time-consuming task, and suffers from excessive computational complexity. Another challenging issue is the bitstreams of video contents are significantly higher and are difficult to be incorporated into blocks on any given chain [138]. Thus, there is ample scope for research to protect the video data on the chains.

3.2.2. Security—While the researchers are working toward improving the security guarantees offered by blockchain, there are numerous vulnerabilities in smart contracts and they are exposed to security and privacy attacks [139]. For example, selfish mining, DNS attack, mempool attack, double spending attack and consensus delay. In selfish mining, the miners try to increase their reward by keeping the blocks private. In DNS attack, an attacker broadcast wrong information with its peers whereas, in a mempool attack, the new blocks are flooded with transactions. These blocks are also subject to double spending attack in which two transactions are created from the same unspent transactions. Moreover, recent study have found that blockchain are subject to consensus delay in which the peers are prevented from reading a consensus. Besides, these attacks, there are a number of other attacks faced by the blockchain, e.g. DDoS and theft of wallets. As a result, security is a major concern in blockchain that needs to be explored further.

3.2.3. Read/Write Operations—Securing the links between the blockchain infrastructure and the IoMT applications reading and writing from/to the blockchain is crucial. Protecting a blockchain-based solution is not limited just to the blockchain

architecture, but the whole chain of requests/responses needs to be protected. The protection of whole chain will prevent the risk of man-in-the-middle attack.

3.2.4. Scalability—Most of the existing blockchain platforms are not feasible for the huge amount of data produced by smart devices of IoMT. This huge volume of data will increase significantly because the number of connected devices with the Internet will reach 41.6 billion by 2025[2]. The current state of the existing blockchain platforms does not allow them to deal with the amount of data produced by IoMT devices, without slowing down [140]. In case of scalability, there are numerous other challenges. These include:

- It is unsustainable for large-scale networks to process every multimedia transaction.
- Majority of the “blockchain as a service" architectures are cloud-based.
- There is limited amount of bandwidth available to support the processing of real-time multimedia transactions.
- The traditional techniques for storing data of sensor-embedded smart devices are shaky while dealing with and using DLT, the main driving force behind the blockchain.
- Energy wastage remains a massive hurdle with environmental costs.

3.2.5. Interoperability—All IoMT devices are connected by the Internet, but things get more complicated when we add blockchain. Various blockchain platforms are mostly isolated from each other, and if the interoperability challenge is not addressed, we will end up with smart multimedia devices connected to multiple isolated decentralized networks [141]. It could work fine for particular purposes, but it would not become the Internet of Everything, where all the devices are interconnected and can interact with each other. The convergence of blockchain and IoMT faces a number of interoperability issues. These include:

- Ability to integrate private and public blockchains [142].
- Design of permissioning and data access across multiple “chains•.
- Ability to integrate across multiple open source multimedia platforms.
- Ability to integrate with a wide range of devices, existing data sets, and incumbent systems.
- ability to deal with inherent interoperability challenges faced by smart devices themselves. In absence of a universal standard for communication [56], these devices use incompatible protocol stacks.

3.2.6. Regulation—Designing regulations and compliance into transaction execution is not a simple thing. Enterprise-grade blockchain deployments will face numerous policy and legal questions [143]. Among them, the main question is the lack of a clear monetary

[2] https://www.globaldots.com/blog/41-6-billion-iot-devices-will-be-generating-79-4-zettabytes-of-data-in-2025

regulations and policy associated with cryptocurrencies. Although, certain countries are leaning into - or out of - the blockchain market, the IoMT as well as the IoT space is already foggy with legal uncertainties in data ownership, access, privacy, and far beyond. DLT is not a replacement for governance, it merely introduces new ways to encode rules and process consensus.

3.3. Multimedia-enabled Blockchain Platforms

Live streaming is rapidly increasing in popularity. People tune into live events like political debates and live sports. They join social services to watch streamers entertain and engage with their audience. Yet as it stands today, to actually build an application with live video content, or to broadcast a significant event to a large audience, is still extremely difficult and too expensive. Broadcasters and developers pay the same few centralized companies in order to transcode and distribute their video to all devices and platforms so that it can reach every viewer. Through coordination and economic incentives in a blockchain-based protocol, solutions are possible that can result in a platform being:

- Cheaper to the end user
- More scalable
- More resilient without any single points of failure
- Open, from both development perspective, and from a censorship-free perspective

For multimedia streaming applications, a number of blockchain platforms have been developed. In this section, we discuss some of the most significant ones and compare them in Table. 5.

3.3.1. Theta—In today's world, content delivery networks (CDNs) suffer from video re-buffering and higher loading times for videos in many parts of the world. The demand of users for 4k, 8k and higher quality streaming create infrastructure bottleneck. The centralized infrastructure means less revenue for content creators and at the same time, users get low quality streams and reward. To reward the users, theta was proposed. It is a decentralized peer-to-peer video delivery blockchain platform that allows the users to earn rewards for sharing their excess bandwidth and resources. Moreover, the content creators also earn with lower streaming costs. Theta provides high quality and smooth video streaming globally and reduce the cost of delivering video streams. Using Theta, video platforms are no longer required to build expensive infrastructure.

3.3.2. Livepeer—Livepeer is a decentralized peer-to-peer technology that allows the nodes to contribute their computation and bandwidth capabilities for streaming live videos [144]. It incentivizes these nodes (users) for contributing their bandwidth and computation toward live video broadcast. Livepeer allows an IoMT device to capture a video and broadcast to a decentralized network, where the nodes encode it into all necessary formats so that it can reach every supported device. All the users that run these nodes are incentivized via fees paid by the broadcaster in Ethereum (ETH). Any user on this network can request to view the video streams and they will be distributed automatically to them in a near real-time.

3.3.3. Moeco—Moeco is a blockchain-powered connectivity platform that integrates various connectivity standards and connects billions of devices across the globe [145]. Moeco helps businesses to adopt the IoT and IoMT technologies. It rolls out new services quickly, effortlessly and cost-efficiently. This platform warrants accurate data delivery and takes over payment and billing processes. It also motivates and rewards users for data transfers.

3.3.4. Waltonchain—Waltonchain provides the hardware and software platform for tracking processes and products in the supply chain application of our smart connected world [146]. It has developed a smart RFID reader-writer that collects, processes and uploads data automatically to the blockchain. The cross-chain technology of Waltonchain tends to achieve data integration, circulation, verification, and storage among blockchains.

3.3.5. IoTeX—IoTeX is a blockchain infrastructure that coordinates autonomous devices and connects them to the physical world [147]. IoTeX leverages a blockchain-in-blockchain architecture with its native IOTX token, launched on the IoTeX Mainnet. IoTeX real-time consensus with instant finality enables efficient cross-chain communication for billions of connected devices. This platform achieves a significantly higher network throughput and reduced transaction cost for multimedia streaming applications.

3.3.6. OriginTrail—OriginTrail is a decentralized blockchain platform for digital supply chains to ensure data integrity [148]. It is a permissionless blockchain that ensures product standard and consumers safety using an incentive protocol. This platform addresses two key factors, i.e., data fragmentation and data centralization, that disrupt data collection and sharing in supply chains. In IoMT, this platform provides interoperability, interconnectivity and data integrity via universal data exchange and immutability.

3.4. Hyperledger Fabric

Hyperledger Fabric is a private blockchain framework that is used for developing blockchain-based applications, networks, etc. Fabric was designed for creating private blockchains that can be used within a single organization or a group of aligned organizations that link to other blockchain implementations. Fabric prioritizes several key features as part of its architecture. These features include:

- Channels: Fabric has the ability of partitioning ledgers into channels that allows the members of a network to create a separate set of transactions, which are not visible to the larger network. This allows for more sensitive data to be segregated from nodes that do not require access.
- Privacy: Fabric requires all nodes within its network to be identified; the prospective members of a Fabric-supported network must join and identify themselves via a Membership Service Provider (MSP), i.e., permissioned membership.
- Scalability: Another distinguishing feature of Fabric for larger enterprises is the immensely scalable network that Fabric provides. Like other implementations, the number of nodes participating in the network can quickly scale; but the

system is capable of still processing large amount of data with a smaller set of resources.

- Modularity: Fabric's architecture is designed to allow separate components to be added and implemented at different times. Many of the components are optional, and can be omitted completely or introduced later without affecting functionality. This feature is intended to give a company sufficient power over "what is and is not" necessary to implement. Some of the components that are considered modular, or "plug-and-play", include the method of achieving consensus, membership services for identification, the ledger self-storage, specific access APIs, and chaincode integration.

3.4.1. Platforms—The famous Fabric platforms are:

- Hyperledger Burrow: A modular client designed to function as permissioned Ethereum smart contract interpreter. Burrow executes smart contract code on an Ethereum Virtual Machine. It is not considered a fix-all, or highly pluggable.
- Hyperledger Sawtooth: This modular platform is designed for creating, and deploying blockchains. It is also a platform for coding applications to interact with the blockchain. It also supports a number of different, pluggable approaches to reaching consensus.

4. Industrial Projects: Security and Blockchain for IoMT

In this section, we will discuss a number of industrial projects that aim to provide seamless and ubiquitous communication in smart multimedia applications of IoMT. In these projects, security and blockchain are the key enablers for confidentiality, access control, privacy, and trust. We will highlight the distinguishing features, supported data, operational mechanisms, and shortcomings of these projects. We will also discuss their intended domains of applications in our smart connected world. A comparison of these projects is made in Table 6. These projects will provide the research community with much needed useful insights of ongoing work in security and blockchain for IoMT applications.

The uBiquitous, secUre inTernet-of-things with Location and contExt-awaReness (BUTLER) is a European Union FP7 project that aims to develop smart and secure applications through context-aware and location-dependent information system [149]. BUTLER is a multi-domain project that covers smart cities, smart healthcare, smart homes, smart transportation and smart shopping. It allows the users to manage their own profiles by restricting the identity sharing over distributed applications. Trustworthy servers are used for trust management at the time of data exchange among these applications. As an example, the users of smart homes need to be authorized by these servers to connect with the users in hospital, and vice-versa. This project provides some promising solutions for the problems faced by the cybersecurity world, the convergence of incoming dynamic data streams from heterogeneous applications still remain at large. The smart devices of these applications support protocol stacks that may not comply with each other. The location and behavior identification and management of a user is a challenging issue yet to be resolved for most of

the security-related frameworks of IoMT and IoT. Moreover, BUTLER lacks the support for blockchain implementation.

Lightweight Scalable Blockchain (LSB) is a joint venture of Data61 and University of New South Wales, Australia for the smart home application of IoMT [150]. The LSB architecture is highly scalable, eliminates the overheads incurred by classic blockchain, and maintains all the security-related features. Unlike classic blockchain, LSB is managed in a centralized fashion to optimize the energy consumption. For authentication, privacy and trust management, an overlay network is created by resource-efficient devices. This network implements a publicly accessible distributed blockchain for ensuring the privacy of exchanged data. A distributed trust approach is adopted to reduce the processing time of block validation. The main features of LSB are: 1) elimination of processing overhead for the miners, 2) separation of data and transactions flow to decrease the service delay, and at the same time, maintains privacy and confidentiality, 3) a gradual decrease in transactions because it requires distributed verification when the nodes increase their trust, and 4) a two-tier blockchain implementation, i.e., a private centralized ledger at the local networks is implemented for managing the local transactions. For the overlay network, a distributed public blockchain is implemented.

IoMT interconnects a large number of information and communication systems. Information security and privacy properties of these systems are difficult for the users to understand. Besides, the users need to be integrated in the trust chain. To achieve these goals, usable Trust in the Internet of Things (uTrustit) was launched [151]. The uTrustit is an EU funded FP7 project for enhancing the user trust perception in an IoT context. uTrustit directly integrates a user in the trust chain to guarantee transparency in the underlying security, privacy and reliability of the communicating smart and intelligent devices. It aims to create a trust-feedback toolkit that provides users with the information required for making an informed decision without any prior knowledge of security. uTrustit enables the system manufacturers and integrators to highlight the underlying security concepts to the users in a clear and logical fashion. Thus, enabling them to make judgment on the trustworthiness of these information and communication systems. Initially, the user requirements are analyzed and security feedbacks are provided accordingly. Also, these feedbacks are analyzed to verify if they are correct or not. This project includes a virtual reality simulator that ensures prompt processing of a user feedback. However, it has no implementation for blockchain.

Smart End-to-end Massive IoT Interoperability, Connectivity and Security (SEMIoTICS) is an EU FP7 project that aims to design a pattern-driven framework for the existing IoMT, IoT and IIoT platforms [152, 153]. It enables and guarantees a secured and dependable actuation and semi-autonomous behavior for applications. SEMIoTICS has a built-in support for cross-layer dynamic adaptation of heterogeneous multimedia streaming devices. For complexity and scalability issues, smart programmable and semantic interoperability techniques are integrated into it. This project aims to develop patterns for the orchestration of these devices and IoT/IoMT/IIoT platforms in those applications that require guaranteed security, privacy, dependability and interoperability (SPDI) Properties. It also aims to develop semantic interoperability for these devices, their underlying networks and cloud platforms. A self-adaptable monitoring technique is designed for supporting

integrated and predictive monitoring of devices at each layer of the protocol stack. To support the adaptation of applications, and end-to-end security, privacy, user control and accountability, core mechanisms are developed for multi-layered embedded intelligence. SEMIoTICS focuses on three major sectors: healthcare, renewable energy and smart sensing. SEMIoTICS lacks the support of trust and blockchain implementation.

Secure Open Federation for Internet Everywhere (SOFIE) is an H2020-EU.2.1.1 project that aims to create novel business platforms for multimedia applications of our smart connected world [154, 155]. Unlike integration, SOFIE aims to use federation for software framework and reference implementation. Using secured open federation powered by SOFIE architecture, platforms are created for various business applications. From a business perspective, anyone will be able to join an open system as there exists no organizational architectural barrier. At technical level, any IoMT platform can be joined virtually to federation as long as it has the support for open interfaces. SOFIE incorporates security at the time of design, i.e., all the required security and privacy features are included to safeguard against cyber-attacks. For this purpose, unforgeable DTLs are used to establish transparency and accountability by providing the users with better control of their multimedia and scalar data. SOFIE maintains data sovereignty in a very systematic and controlled fashion. Data is shared within the limitations imposed by security and privacy policies that are defined by their owners.

Secure and safe Internet of Things (SerIoT) is an EU project that aims to optimize the information security for smart devices and their underlying platforms [156, 157]. This project adopts a cross-layered holistic approach that considers the platforms, devices, SDN routers, honeypots and the operator’s controller. SerIoT offers a secured platform for data communication across the Europe. A unique and portable software-based communication platform has been designed that was tested in individual labs via test-beds. Blockchain is used for data transfer among the communicating devices in a secured, publically verifiable, and trustless manner. SerIoT relies on blockchain for immutable record of the smart devices’ history and to improve the security and privacy of exchanged messages.

A novel Intrusion Detection System (IDS) for smart connected devices was launched by EU FP7 [158]. The IDS framework is part of the broad EBBITS Project and is empowered by IPv6 over Low-power Personal Area Network (6LOWPAN) devices. The framework consists of a monitoring system and an engine for the detection of malicious and adversarial threats. For privacy, a lightweight data protection approach is adopted, whereas, trust management is regulated by trust-empowered servers. The monitoring system of IDS maintains a constant check on any irregular data patterns for security purposes. This framework is feasible only for lightweight multimedia streaming devices. The presence of resource-constrained 6LoWPAN devices and the emergence of bursty and live-streaming data flows may deteriorate its performance. The IDS framework is designed for manufacturing and industrial automation applications.

CLAP is a project of Commonwealth Scientific and Industrial Research Organisation (CSIRO), Australia for exchanging scalar data between low-powered smart connected devices [159]. It ensures secured communication via a public insecure network. CLAP

considers the authentication, privacy and performance issues faced by these devices. It provides untraceability, anonymity, confidentiality, scalability and at the same time, it is modular and scalable. However, CLAP does not account for trust management among the communicating entities. Also, it does not has blockchain features as it relies on a distributed communication pattern.

5. A Case Study: Security and Blockchain for Health Sector

In the Internet of Medical Things [44, 160], security and privacy of patients and their information are challenging aspects that need to be dealt with utmost care. Security is used to protect the exchanged data and underlying smart medical devices from malevolent entities. Novel authentication approaches [161, 162] have been designed to restrict the access to sensitive data. Privacy ensures that only authorized personnel have access to the unaltered medical data, and usage of a patient personal details [163]. Trust, on the other hand, ensures that only verified users are provided the privilege to access the data gathered from trusted entities [109]. In recent years, blockchain has attracted significant attention of the researchers in healthcare sector [164, 165]. Blockchain ensures that the patient data are stored in blocks over a distributed chain and all transactions for data retrieval are verified, accordingly.

In Fig. 7, we have proposed our own model as a use case for the application of authentication, privacy, trust and their convergence with blockchain in healthcare sector. It involves a secured mechanism for data collection and the exchange of Public Health Information (PHI). In the first phase, the public key parameters and health attribute keys are provided to the patient' wearable sensors by the cloud service provider. This phase involves a lightweight authentication between the sensors and service provider to ensure the safety of transmitted security primitives. In the second phase, data, e.g. biomedical images are collected by these sensors and transmitted to a nearby server. Public key encryption can be used here to ensure that the data is exchanged securely, and at the same, its privacy is preserved [162]. In the third phase, the data is securely transmitted from the server to an e-health user, e.g. a physician. During this phase, trust plays an important role. The server communicates with the cloud to verify the trustworthiness of e-Health users. Moreover, the latter also communicates with the cloud to ensure that the communicating server is trustworthy. During this phase, the health service provider verifies the data exchange and also maintains access control. Finally, the encrypted data is stored at the healthcare service provider. For this purpose, blockchain technology can be used [165]. External gateways enable the transmission of data to cloud storage system, which is interconnected to a blockchain-enabled network. The cloud storage hosts multiple applications and is linked to the services required by the patient. The gathered data is stored in a database that can be retrieved by their underlying applications. The blockchain network receives the data verification requests from cloud storage system and the miners generate the receipt for each transaction, accordingly. Smart contracts are generated for each transactions and their identities (IDs) are stored in the blockchain network.

6. Future Trends and Research Directions

In this section, we provide a detailed discussion on future trends and research directions in IoMT. We focus on the convergence of emerging technologies with security, blockchain and IoMT for the realization of exciting applications of the future. We also discuss the challenges that need to be addressed for bringing these applications into reality.

1. The prediction that there will be 50 billion real-world physical devices connected with the Internet by 2025 literally means a plethora of data will be generated that need to be converted into actionable results [166]. In this regard, the role of Artificial Intelligence (AI) cannot be ignored. The AI algorithms will convert this massive data into useful actionable results [167]. Blockchain, on the other hand, achieve the next level of data encryption and security. The convergence of AI with IoMT and blockchain has immense benefits and business opportunities. Most IoMT devices are connected to each other via the public networks that may be hacked. Blockchain resolves the security problem in these environments, creating linear registers which are constantly indexed. These IoMT devices mostly use the centralized client/server communication model. This kind of infrastructure incurs higher maintenance cost, as it uses centralized cloud systems and large server farms with host connectivity equipment. As a counterpoint, there is a peer-to-peer communication model (between equal nodes, without fixed clients or servers) which can provide an effective solution when it comes to reducing costs, but with the associated problem of a lack of security [168]. In this case, blockchain remedies this shortcoming by sharing and verifying the transactions through the nodes forming part of the network, rather than through a single central server. Cryptography can be used to authenticate and identify all other participating nodes and permit them to add transactions to the large blockchain registry. This convergence can realized for a number of applications such as smart cities, smart transportation etc. In future, we will see self-driving cars populating the streets. A proper AI approach can identify the destination and strategize good navigation across a city, a highway and a countryside. In this case, blockchain will help in recording and securing the travel information and allows secure digital payments in fuel stations/workshops/ etc. The IoMT, on the other hand, will enable the car to receive all real-time data on traffic status, weather forecasts, road obstacles, etc.

2. The convergence of Augmented Reality (AR) with IoMT, blockchain and AI is paving the way for Web 3.0. AR requires extensive computational power and the centralized GPUs (Graphics Processing Units) are not capable to fulfill this demand [169]. Blockchain has the ability to enable the distributed GPU computational power. In fact, blockchains dedicated towards AR holographic processing have seen phenomenal growth in recent years [170]. IoMT devices such as, IP-enabled cameras and multimedia sensors, aggregate the real-time data streams from any deployed environment for seamless integration of the virtual and physical worlds. Multimedia sensors such as body-trackers [171] align the self-rendering of a user in AR with virtually enhanced environment

[172]. Next, the depth sensors provide these data for 3D spatial maps. IP-enabled cameras have the ability of absorbing the surface-level meticulous visual input. Moreover, various healthcare sensors gather biometric data of patients such as heart rate, respiration rate and brain activities [173]. Next, the gathered data can be incorporate into our health-related feedbacks in personal recommendation engines and also in our everyday AR interfaces. AI has a crucial role in processing the voluminous data gathered from IoMT devices. Embedded AI algorithms will empower customized AR experiences of our daily lives ranging from personalized dietary plans to artistic virtual overlays [174]. This convergence will revolutionize the experience of using Smart AR Glasses in near future.

3. The IoMT devices that require low power or produce large volumes of data transmission have until now been difficult and expensive to support [175]. However, with the advent of 5G and Low-Power Wide-Area Network (LPWAN), low-power devices and devices that produce large amounts of data, e.g. IP-enabled cameras, can now be supported [176]. The convergence of these technologies with IoMT applications creates an opportunity for business organizations to provide innovative solutions, enabled with smart automation, immutability, scalability, security, and low-cost transaction capabilities. With billions of devices being supported by 5G and LPWAN connectivity [177], businesses will need these devices to interact and transact with one another in a secure, scalable, cost-efficient and trusted way. Enterprise blockchain [178] provides a proven and robust technological solution to combat the risks of subjective blame, denials of fault or a lack of transparency from IoMT as well as IoT applications. The convergence of 5G and LPWAN with blockchain and IoMT will enable ultra-fast multimedia streaming with extremely low latency for the underlying devices in a highly secured fashion. This convergence will be highly beneficial for a number of applications such as healthcare, industrial automation, smart cities, retail, etc.

4. With the advent of Edge Computing [179], IoT and IoMT applications have seen a phenomenal growth. Edge Computing distributes the computational and storage resources across the network and provides quicker responses to the sensor-embedded devices [180, 181]. IP-enabled cameras and robots generate video feeds that demands fast processing and low-latency responses. Transmission of this data to the cloud will consume higher bandwidth, and at the same time, will incur excessive communication overhead [182]. Combine with 5G and LPWAN, Edge Computing can provide countless opportunities for various IoMT applications. In this convergence, AI has its own role as well. Various Machine learning and data training models can make ultra-fast decisions at the edge for IoMT applications. Blockchain, on the other hand, brings trust in this convergence. The IoMT network needs to be secure, and it needs to be one instance of the truth. It requires a lot of data to make a transaction to take place. Security techniques such as authentication performs the encryption and decryption of data to/from the Edge devices. This convergence

of various technologies will provide countless opportunities for various IoMT applications such as smart cities, industrial automation etc. For example, in a smart city, surveillance cameras constantly monitor various activities [183]. The smart devices require quick feedbacks on their gathered data. Cloud computing has sufficient storage but the response time is relatively slow. Edge computing has the ability to provide fast responses. 5G and LPWAN ensures the delivery of responses in a much faster way. Blockchain will ensure the video feeds of the cameras are transmitted securely by creating transactions. Security, privacy and trust ensures that responses are from only trusted edge servers and the feeds/responses are not disclosed to malevolent entities.

5. Finally, the presence of Software-defined Networking (SDN) [184] cannot be ignored in this convergence. The application of SDN in IoMT-based network enables the SDN controller to get input from front-end application to make decisions for traffic management [185]. Using SDN, a feedback system can be formed within the IoMT devices and the SDN controller. In this system, information of security breaches is passed to the SDN controller, which manages several programmable switches. Any attack is logged by the SDN controller, which clock the attack closer to source and further spread awareness about the attack in the whole network connected by central SDN controller. The SDN controller will acts as a firewall in this case, but at a central location. SDN technology is still not robust enough to prevent an attack on the devices themselves. But SDN can help reduce the impact on the whole network of devices. Since, blockchain is based on the concept of decentralization of data, which means copies of the same data are kept at multiple nodes in the network. With blockchain technology, any transaction of data can be tracked by trusted nodes participating in a network. SDN can be helpful in making an IoMT network secure by blocking cyber-attacks in a short amount of time after detection. Blockchain technology, on the other hand, can enforce privacy for multimedia and non-multimedia devices of IoMT and also capable to maintain trust within the network.

7. Conclusion

The Internet of Multimedia Things (IoMT) is moving from a research vision to concrete manifestations with emerging new applications. It is expected that there will be 41.6 billion smart devices connected to the Internet by 2025 that will generate a plethora of data. The raw multimedia data generated by these devices have some of the stringent requirements in terms of available bandwidth, latency, storage, security provisioning, QoS and Quality of Experience (QoE), among others. In this paper, we surveyed the IoMT applications from security and blockchain perspectives. The latest trends in security primitives, i.e., authentication, privacy and trust were discussed and security-related challenges faced by the multimedia data were highlighted in this context. The shortcomings of these primitives along with distributed storage requirement led to the emergence of blockchain technology. We discussed blockchain and its convergence with IoMT along with multimedia-enabled blockchain platforms. Numerous research challenges along with key benefits of this

convergence were also discussed. The role of security primitives and blockchain have recently been witnessed in a number of large-scale industrial projects. We discussed multiple such projects that highlighted the significance of our work towards the future of multimedia applications. The purpose of this survey would be incomplete had we not discussed its application and feasibility for a real-world scenario. For this purpose, we presented a case study of healthcare sector that relies upon blockchain and security primitives as key enablers for efficient monitoring of a patient. The role of authentication, privacy, trust and blockchain were briefly discussed. The convergence of security and blockchain for multimedia applications has motivated multi-disciplinary research in recent years. We concluded this survey with the discussion on the convergence of emerging technologies with blockchain and security for multimedia applications of tomorrow. In light of this convergence, future trends, research directions, and challenges faced by this convergence were discussed.

Acknowledgements

This work is partially supported by a pilot award from the Center for Research in Human Movement Variability and the NIH (P20GM109090).

Biography

Mian Ahmad Jan is an Assistant Professor at the Department of Computer Science, Abdul Wali Khan University Mardan, Pakistan. He received his PhD in Computer Systems from the Faculty of Engineering and Information Technology (FEIT), at the University of Technology Sydney (UTS) Australia. He had been the recipient of various prestigious scholarships during his PhD studies. He was recipient of International Research Scholarship (IRS) at the University of Technology Sydney Australia and Commonwealth Scientific Industrial Research Organization (CSIRO) scholarships. He has been awarded the best researcher awarded for the year 2014 at the University of Technology Sydney Australia. His research interests are Cluster-based Hierarchical routing protocols in Wireless Sensor Networks, Congestion detection and mitigation, Internet and Web of Things and efficient Intrusion and malicious attack detection in Wireless Sensor Networks. Recently, he has been involved in latest developments in the field of Underwater Sensor Network Localization and Secured Ticketing, Internet of Vehicles security and privacy issues, Software-defined Radio VANET, Vehicular Ad hoc Network, and Big Data Analytics. He has published his research work in top-ranked transactions, magazine and conferences. His research has been published in IEEE Communication Magazine, IEEE Transactions on Mobile Computing, Elsevier Computer Networks, Elsevier Future Generations Computer Systems, Elsevier Information Sciences, Wiley Journal of Concurrency and Computations. Also, he has published in high ranked conferences such as TrustCom, WWIC, HPCC and Future 5V. Recently, he has been chair of various conferences and special sessions such as CCODE-2017, IoT-BC^2. He has been invited to serve as a Technical Program Committee Member for 8 international conferences so far. He has been guest edotor for high-cited and highly ranked international journals, including IEEE Transactions on Dependable and Secure Computing (TDSC), IEEE Transaction on Indutrial Informatics, Elsevier Computer Networks, Springer MONET and Wiley Concurrency and Computation: Practice and Experience.

Jinjin Cai has received PhD degree in Engineering from Hebei Agricultural University, China. She is a lecturer at the College of Mechanical and Electrical Engineering, Hebei Agricultural University. Her research interests include automation and control systems, image and video processing, Internet of tings, and Intelligent Information processing.

Xiang-Chuan Gao received the B.Sc. and M.Eng. degrees from Zhengzhou University, Zhengzhou, China, in 2005 and 2008, respectively, and the Ph.D. degree from the Beijing University of Posts and Telecommunications, Beijing, China, in 2011. His current research interests include IoT, massive MIMO, cooperative communications, and visible light communication.

Fazlullah Khan is working as Assistant Professor at the Department of Computer Science, Abdul Wali Khan University Mardan (AWKUM), Pakistan and as a researcher at Duy Tan University, Vietnam. He has completed his PhD in Computer Systems from AWKUM, Pakistan. He had been the recipient of various prestigious scholarships during his PhD studies and has been awarded the best researcher awarded for the year 2017 at the University. His research interests are Security and Privacy of Wireless Communication Systems, Internet of Things, Machine Learning, Artificial Intelligence. Recently, he has been involved in latest developments in the field of Internet of Vehicles security and privacy issues, Software-defined Networks, Fog Computing and Big Data Analytics. He has published his research work in top-notch journals and conferences. His research has been published in IEEE Communication Magazine, IEEE Transactions on Industrial Informatics, IEEE Access, Elsevier Computer Networks, Elsevier Future Generations Computer Systems, Elsevier Computers and Electrical Engineering, Springer Mobile Networks and Applications, Wiley Journal of Concurrency and Computations. According to Google Scholar, he has an H-Index of 17 and his research articles have received over more than 700 citations since 2015. He has served as the guest editor of IEEE Access Journal, Springer Mobile Networks and Applications, Inderscience Big data Analytics, and Ad Hoc & Sensor Wireless Networks. He has served over 10 conferences in leadership capacities including General Chair, General co-Chair, program co-Chair, track Chair, session Chair, and Technical Program Committee member, including IEEE TrustCom 2017, 2018, EuroCom, GCCE 2019, ITNG 2018, Future5V 2017, CCODE-2017, IoT-BC2 2016. He has been an active reviewer for high-cited and highly ranked international journals, including IEEE Transactions on Dependable and Secure Computing (TDSC), Elsevier Computer Networks, Springer Mobile Networks and Applications and Wiley Concurrency and Computation: Practice and Experience.

Spyridon Mastorakis is assistant Professor in Computer Science at the University of Nebraska, Omaha, USA. I graduated with a Ph.D. in Computer Science from the University of California, Los Angeles in June 2019. I was fortunate enough to work with some great folks at the Internet Research Laboratory and be supervised by Professor Lixia Zhang. I am interested in the broader area of Future Internet and network systems. I have done extensive work in the areas of Information Centric Networking (ICN) and Named Data Networking (NDN). I am also interested in emerging paradigms, such as edge computing. My research intersects with multiple areas of computer science, such as security, artificial intelligence, and big data.

Muhammad Usman is PhD from University of Technology, Sydney. He has joined Federation University in 2019 as a Lecturer in Information Technology. Prior to this, he has worked as a postdoc researcher at Swinburne University of Technology. He has also worked at University of Technology Sydney as a research and teaching assistant. He received his PhD degree from University of Technology Sydney, Australia. His primary research interests are in the areas of cybersecurity (security and privacy), machine learning, QoS, QoE, video processing and streaming, and Internet of Multimedia Things.

Mamoun Alazab is an Associate Professor in the College of Engineering, IT and Environment, IT Discipline. He is acyber security researcher and practitioner with industry and academic experience. His research is multidisciplinary that focuses oncyber security and digital forensics of computer systems including current and emerging issues in the cyber environment like cyber-physical systems and internet of things, by taking into consideration the unique challenges present in these environments, with a focus on cybercrime detection and prevention. Prof. Alazab received his PhD degree in Computer Science and has more than 100 research papers. He presented at many invited keynotes talks and panels, at conferences and venues nationally and internationally (22 events in 2018 alone). He is a Senior Member of the IEEE. He is an editor on multiple editorial boards including Associate Editor of IEEE Access (2017 Impact Factor 3.557), Editor of the Security and Communication Networks Journal (2017 Impact Factor: 0.904) and Book Review Section Editor: Journal of Digital Forensics, Security and Law (JDFSL).

Professor Watters is Australia's leading cybersecurity researcher. He was recently awarded $2.364m from the MBIE Catalyst Strategic - Cyber Security Research by the New Zealand government to develop Artificial Intelligence for Automating Responses to Threats. This collaboration includes Data61, Victoria University of Wellington and the University of Queensland. He has also recently been awarded funding from the Oceania Cyber Security Centre (OCSC) for six projects.

Professor Watters also holds Australian Research Council (Discovery DP160100601) Auto-Internet Warnings to Prevent the Viewing of Minor-Adult Sex Images ($299k) and a grant from the Australian Centre for Combating Child Exploitation (ACCCE) for Automated Internet Warning to Prevent the Uploading of Child Exploitation Material $120k. Professor Watters has previously worked at CSIRO, Macquarie University, the University of Ballarat, and Massey University, and has held honorary positions at University College London and Unitec New Zealand. He has received research funding from the Australian Academy of Technology and Engineering (ATSE), Department of Social Services, Metrix Ltd, Callaghan Innovation, the Motion Picture Association, CASBAA, 21st Century Fox, the Attorney General's Department, Village Roadshow, the Australian Federal Police, IBM, Westpac, Google Inc the National Australia Bank, and End Child Prostituion and Trafficking (ECPAT). Professor Watters leads the Digital Crime and Networking Group at La Trobe.

References

[1]. Alvi SA, Afzal B, Shah GA, Atzori L, Mahmood W, Internet of multimedia things: Vision and challenges, Ad Hoc Networks 33 (2015) 87–111.

[2]. LeCroy C, Vaughan G, Reliable real-time transport protocol, 2006. US Patent 6,996,624.

[3]. Schulzrinne H, Rao A, Lanphier R, Real time streaming protocol (rtsp) (1998).

[4]. Othman NA, Aydin I, A new iot combined body detection of people by using computer vision for security application, in: 2017 9th International Conference on Computational Intelligence and Communication Networks (CICN), IEEE, 2017, pp. 108–112.

[5]. Wu Y, He Y, Shivakumara P, Li Z, Guo H, Lu T, Channel-wise attention model-based fire and rating level detection in video, CAAI Transactions on Intelligence Technology 4 (2019) 117–121.

[6]. Schill F, Bahr A, Martinoli A, Vertex: A new distributed underwater robotic platform for environmental monitoring, in: Distributed Autonomous Robotic Systems, Springer, 2018, pp. 679–693.

[7]. Yang P, Stankevicius D, Marozas V, Deng Z, Liu E, Lukosevicius A, Dong F, Xu L, Min G, Lifelogging data validation model for internet of things enabled personalized healthcare, IEEE Transactions on Systems, Man, and Cybernetics: Systems 48 (2016) 50–64.

[8]. Koceski S, Koceska N, Evaluation of an assistive telepresence robot for elderly healthcare, Journal of medical systems 40 (2016) 121. [PubMed: 27037685]

[9]. Valecce G, Micoli G, Boccadoro P, Petitti A, Colella R, Milella A, Grieco LA, Robotic-aided iot: automated deployment of a 6tisch network using an ugv, IET Wireless Sensor Systems 9 (2019) 438–446.

[10]. Rani S, Ahmed SH, Talwar R, Malhotra J, Song H, Iomt: A reliable cross layer protocol for internet of multimedia things, IEEE Internet of things Journal 4 (2017) 832–839.

[11]. Zhou L, Chao H-C, Multimedia traffic security architecture for the internet of things, IEEE Network 25 (2011) 35–40.

[12]. Noura M, Atiquzzaman M, Gaedke M, Interoperability in internet of things: Taxonomies and open challenges, Mobile Networks and Applications 24 (2019) 796–809.

[13]. Lu Y, Industry 4.0: A survey on technologies, applications and open research issues, Journal of Industrial Information Integration 6 (2017) 1–10.

[14]. Jan MA, Khan F, Alam M, Usman M, A payload-based mutual authentication scheme for internet of things, Future Generation Computer Systems 92 (2019) 1028–1039.

[15]. Taivalsaari A, Mikkonen T, A roadmap to the programmable world: software challenges in the iot era, IEEE Software 34 (2017) 72–80.

[16]. Kambourakis G, Kolias C, Stavrou A, The mirai botnet and the iot zombie armies, in: MILCOM 2017-2017 IEEE Military Communications Conference (MILCOM), IEEE, 2017, pp. 267–272.

[17]. Jan MA, Usman M, He X, Rehman AU, Sams: A seamless and authorized multimedia streaming framework for wmsn-based iomt, IEEE Internet of Things Journal 6 (2018) 1576–1583.

[18]. Al-Fuqaha A, Guizani M, Mohammadi M, Aledhari M, Ayyash M, Internet of things: A survey on enabling technologies, protocols, and applications, IEEE communications surveys & tutorials 17 (2015) 2347–2376.

[19]. Ammar M, Russello G, Crispo B, Internet of things: A survey on the security of iot frameworks, Journal of Information Security and Applications 38 (2018) 8–27.

[20]. Banafa A, Iot and blockchain convergence: benefits and challenges, IEEE Internet of Things 2 (2016) 457–466.

[21]. Sheng Z, Yang S, Yu Y, Vasilakos AV, McCann JA, Leung KK, A survey on the ietf protocol suite for the internet of things: Standards, challenges, and opportunities, IEEE wireless communications 20 (2013) 91–98.

[22]. Ukil A, Bandyopadhyay S, Pal A, Iot-privacy: To be private or not to be private, in: 2014 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), IEEE, 2014, pp. 123–124.

[23]. Kim H, Lee EA, Authentication and authorization for the internet of things, IT Professional 19 (2017) 27–33.

[24]. Liu X, Farahani B, Firouzi F, Distributed ledger technology, in: Intelligent Internet of Things, Springer, 2020, pp. 393–431.

[25]. Reyna A, Martín C, Chen J, Soler E, Díaz M, On blockchain and its integration with iot. challenges and opportunities, Future generation computer systems 88 (2018) 173–190.

[26]. Choudhary T, Virmani C, Juneja D, Convergence of blockchain and iot: An edge over technologies, in: Toward Social Internet of Things (SIoT): Enabling Technologies, Architectures and Applications, Springer, 2020, pp. 299–316.

[27]. Granjal J, Monteiro E, Silva JS, Security for the internet of things: a survey of existing protocols and open research issues, IEEE Communications Surveys & Tutorials 17 (2015) 1294–1312.

[28]. Yang Y, Wu L, Yin G, Li L, Zhao H, A survey on security and privacy issues in internet-of-things, IEEE Internet of Things Journal 4 (2017) 1250–1258.

[29]. Alaba FA, Othman M, Hashem IAT, Alotaibi F, Internet of things security: A survey, Journal of Network and Computer Applications 88 (2017) 10–28.

[30]. Fernandes E, Rahmati A, Eykholt K, Prakash A, Internet of things security research: A rehash of old ideas or new intellectual challenges?, IEEE Security & Privacy 15 (2017) 79–84.

[31]. Sicari S, Rizzardi A, Grieco LA, Coen-Porisini A, Security, privacy and trust in internet of things: The road ahead, Computer networks 76 (2015) 146–164.

[32]. Hassan WH, et al. , Current research on internet of things (iot) security: A survey, Computer Networks 148 (2019) 283–294.

[33]. Weber RH, Internet of things–new security and privacy challenges, Computer law & security review 26 (2010) 23–30.

[34]. Sha K, Wei W, Yang TA, Wang Z, Shi W, On security challenges and open issues in internet of things, Future Generation Computer Systems 83 (2018) 326–337.

[35]. Khan MA, Salah K, Iot security: Review, blockchain solutions, and open challenges, Future Generation Computer Systems 82 (2018) 395–411.

[36]. Yan Z, Zhang P, Vasilakos AV, A survey on trust management for internet of things, Journal of network and computer applications 42 (2014) 120–134.

[37]. Din IU, Guizani M, Kim B-S, Hassan S, Khan MK, Trust management techniques for the internet of things: A survey, IEEE Access 7 (2018) 29763–29787.

[38]. Altaf A, Abbas H, Iqbal F, Derhab A, Trust models of internet of smart things: A survey, open issues, and future directions, Journal of Network and Computer Applications 137 (2019) 93–111.

[39]. Minoli D, Occhiogrosso B, Blockchain mechanisms for iot security, Internet of Things 1 (2018) 1–13.

[40]. Dai H-N, Zheng Z, Zhang Y, Blockchain for internet of things: A survey, IEEE Internet of Things Journal 6 (2019) 8076–8094.

[41]. Makhdoom I, Abolhasan M, Abbas H, Ni W, Blockchain's adoption in iot: The challenges, and a way forward, Journal of Network and Computer Applications 125 (2019) 251–279.

[42]. Wang X, Zha X, Ni W, Liu RP, Guo YJ, Niu X, Zheng K, Survey on blockchain for internet of things, Computer Communications 136 (2019) 10–29.

[43]. Fernández-Caramés TM, Fraga-Lamas P, A review on the use of blockchain for the internet of things, IEEE Access 6 (2018) 32979–33001.

[44]. Gatouillat A, Badr Y, Massot B, Sejdić E, Internet of medical things: A review of recent contributions dealing with cyber-physical systems in medicine, IEEE internet of things journal 5 (2018) 3810–3822.

[45]. Ferrag MA, Derdour M, Mukherjee M, Derhab A, Maglaras L, Janicke H, Blockchain technologies for the internet of things: Research issues and challenges, IEEE Internet of Things Journal 6 (2018) 2188–2204.

[46]. Díaz M, Martín C, Rubio B, State-of-the-art, challenges, and open issues in the integration of internet of things and cloud computing, Journal of Network and Computer applications 67 (2016) 99–117.

[47]. Li S, Wang G, Yang J, Survey on cloud model based similarity measure of uncertain concepts, CAAI Transactions on Intelligence Technology 4 (2019) 223–230.

[48]. Roman R, Zhou J, Lopez J, On the features and challenges of security and privacy in distributed internet of things, Computer Networks 57 (2013) 2266–2279.

[49]. Roman R, Najera P, Lopez J, Securing the internet of things, Computer 44 (2011) 51–58.

[50]. Al-Turjman F, Radwan A, Data delivery in wireless multimedia sensor networks: Challenging and defying in the iot era, IEEE Wireless Communications 24(2017) 126–131.

[51]. Wu F, Xu L, Kumari S, Li X, Shen J, Choo K-KR, Wazid M, Das AK, An efficient authentication and key agreement scheme for multi-gateway wireless sensor networks in iot deployment, Journal of Network and Computer Applications 89 (2017) 72–85.

[52]. Fernández Bascuñana G, Validation of authentication measures implementation in iot mobile applications, Smart Cities 2 (2019) 163–178.

[53]. Xu J, Ota K, Dong M, Real-time awareness scheduling for multimedia big data oriented in-memory computing, IEEE Internet of Things Journal 5 (2018) 3464–3473.

[54]. Oakes E, Kline J, Cahn A, Funkhouser K, Barford P, A residential client-side perspective on ssl certificates, in: 2019 Network Traffic Measurement and Analysis Conference (TMA), IEEE, 2019, pp. 185–192.

[55]. Kim H-S, Ko J, Culler DE, Paek J, Challenging the ipv6 routing protocol for low-power and lossy networks (rpl): A survey, IEEE Communications Surveys & Tutorials 19 (2017) 2502–2525.

[56]. Noura H, Chehab A, Sleem L, Noura M, Couturier R, Mansour MM, One round cipher algorithm for multimedia iot devices, Multimedia tools and applications 77 (2018) 18383–18413.

[57]. Noura HN, Melki R, Chehab A, Secure and lightweight mutual multi-factor authentication for iot communication systems, in: 2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall), IEEE, 2019, pp. 1–7.

[58]. Ometov A, Petrov V, Bezzateev S, Andreev S, Koucheryavy Y, Gerla M, Challenges of multi-factor authentication for securing advanced iot applications, IEEE Network 33 (2019) 82–88.

[59]. Gope P, Amin R, Islam SH, Kumar N, Bhalla VK, Lightweight and privacy-preserving rfid authentication scheme for distributed iot infrastructure with secure localization services for smart city environment, Future Generation Computer Systems 83 (2018) 629–637.

[60]. Jan MA, Nanda P, He X, Tan Z, Liu RP, A robust authentication scheme for observing resources in the internet of things environment, in: 2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications, IEEE, 2014, pp. 205–211.

[61]. Butun I, Österberg P, Song H, Security of the internet of things: vulnerabilities, attacks and countermeasures, IEEE Communications Surveys & Tutorials (2019).

[62]. Bormann C, Ersue M, Keranen A, Terminology for constrained-node networks, Internet Engineering Task Force (IETF): Fremont, CA, USA (2014) 2070–1721.

[63]. Porambage P, Schmitt C, Kumar P, Gurtov A, Ylianttila M, Two-phase authentication protocol for wireless sensor networks in distributed iot applications, in: 2014 IEEE Wireless Communications and Networking Conference (WCNC), IEEE, 2014, pp. 2728–2733.

[64]. Kapoor V, Abraham VS, Singh R, Elliptic curve cryptography, Ubiquity 2008 (2008) 7.

[65]. Eastlake D 3rd, Jones P, US secure hash algorithm 1 (SHA1), Technical Report, 2001.

[66]. Shelby Z, Hartke K, CB (2014). The Constrained Application Protocol (CoAP), Technical Report, IETF RFC 7552. URI: https://tools.ietf.org/html/rfc7252. Accessed on 04.02, 2018.

[67]. Keoh S, Kumar S, Shelby Z, Profiling of dtls for coap-based iot applications, draft-keoh-dtls-profile-iot-00 (WiP), IETF (2013).

[68]. Rescorla E, Modadugu N, Datagram transport layer security version 1.2 (2012).

[69]. Raza S, Helgason T, Papadimitratos P, Voigt T, Securesense: End-to-end secure communication architecture for the cloud-connected internet of things, Future Generation Computer Systems 77 (2017) 40–51.

[70]. Raza S, Seitz L, Sitenkov D, Selander G, S3k: Scalable security with symmetric keys—dtls key establishment for the internet of things, IEEE Transactions on Automation Science and Engineering 13 (2016) 1270–1280.

[71]. Jan MA, Zhang W, Usman M, Tan Z, Khan F, Luo E, Smartedge: An end-to-end encryption framework for an edge-enabled smart city application, Journal of Network and Computer Applications 137 (2019) 1–10.

[72]. Raza S, Magnússon RM, Tinyike: Lightweight ikev2 for internet of things, IEEE Internet of Things Journal 6 (2018) 856–866.

[73]. Simplicio MA Jr, Silva MV, Alves RC, Shibata TK, Lightweight and escrow-less authenticated key agreement for the internet of things, Computer Communications 98 (2017) 43–51.

[74]. McGrew D, Rescorla E, et al., Datagram transport layer security (dtls) extension to establish keys for the secure real-time transport protocol (srtp) (2010).

[75]. Khalid U, Asim M, Baker T, Hung PC, Tariq MA, Rafferty L, A decentralized lightweight blockchain-based authentication mechanism for iot systems, Cluster Computing (2020) 1–21.

[76]. Hammi MT, Hammi B, Bellot P, Serhrouchni A, Bubbles of trust: A decentralized blockchain-based authentication system for iot, Computers & Security 78 (2018) 126–142.

[77]. Usman M, Jan MA, He X, Chen J, P2dca: A privacy-preserving-based data collection and analysis framework for iomt applications, IEEE Journal on Selected Areas in Communications 37 (2019) 1222–1230.

[78]. Usman M, Jan MA, He X, Chen J, A survey on representation learning efforts in cybersecurity domain, ACM Computing Surveys (CSUR) 52 (2019) 1–28.

[79]. Tingting Y, Junqian W, Lintai W, Yong X, Three-stage network for age estimation, CAAI Transactions on Intelligence Technology 4 (2019) 122–126.

[80]. Cai R, Yang J-M, Lai W, Wang Y, Zhang L, irobot: An intelligent crawler for web forums, in: Proceedings of the 17th international conference on World Wide Web, 2008, pp. 447–456.

[81]. Rodríguez-Silva DA, Adkinson-Orellana L, Gonz'lez-Castano F, Armino-Franco I, Gonz'lez-Martinez D, Video surveillance based on cloud storage, in: 2012 IEEE fifth international conference on Cloud computing, IEEE, 2012, pp. 991–992.

[82]. Kim J, Park N, Kim G, Jin S, Cctv video processing metadata security scheme using character order preserving-transformation in the emerging multimedia, Electronics 8 (2019) 412.

[83]. Dufaux F, Ebrahimi T, A framework for the validation of privacy protection solutions in video surveillance, in: 2010 IEEE International Conference on Multimedia and Expo, IEEE, 2010, pp. 66–71.

[84]. Usman M, Jan MA, Jolfaei A, Xu M, He X, Chen J, Daac: A distributed and anonymous data collection framework based on multi-level edge computing architecture, IEEE Transactions on Industrial Informatics (2019).

[85]. Wang J, Amos B, Das A, Pillai P, Sadeh N, Satyanarayanan M, Enabling live video analytics with a scalable and privacy-aware framework, ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM) 14 (2018) 1–24.

[86]. Wang J, Amos B, Das A, Pillai P, Sadeh N, Satyanarayanan M, A scalable and privacy-aware iot service for live video analytics, in: Proceedings of the 8th ACM on Multimedia Systems Conference, 2017, pp. 38–49.

[87]. Ma X, Yang LT, Xiang Y, Zeng WK, Zou D, Jin H, Fully reversible privacy region protection for cloud video surveillance, IEEE Transactions on Cloud Computing 5 (2015) 510–522.

[88]. Usman M, Jan MA, He X, Cryptography-based secure data storage and sharing using hevc and public clouds, Information Sciences 387 (2017) 90–102.

[89]. Fan W, He J, Guo M, Li P, Han Z, Wang R, Privacy preserving classification on local differential privacy in data centers, Journal of Parallel and Distributed Computing 135 (2020) 70–82.

[90]. Yousefpour A, Fung C, Nguyen T, Kadiyala K, Jalali F, Niakanlahiji A, Kong J, Jue JP, All one needs to know about fog computing and related edge computing paradigms: A complete survey, Journal of Systems Architecture (2019).

[91]. Li H, Gu Z, Deng L, Han Y, Yang C, Tian Z, A fine-grained video encryption service based on the cloud-fog-local architecture for public and private videos, Sensors 19 (2019) 5366.

[92]. Dwivedi AD, Srivastava G, Dhar S, Singh R, A decentralized privacy-preserving healthcare blockchain for iot, Sensors 19 (2019) 326.

[93]. Tewari A, Gupta B, Security, privacy and trust of different layers in internet-of-things (iots) framework, Future generation computer systems (2018).

[94]. Khan F, Rehman AU, Zheng J, Jan MA, Alam M, Mobile crowdsensing: A survey on privacy-preservation, task management, assignment models, and incentives mechanisms, Future Generation Computer Systems 100 (2019) 456–472.

[95]. Samaniego M, Deters R, Zero-trust hierarchical management in iot, in: 2018 IEEE International Congress on Internet of Things (ICIOT), IEEE, 2018, pp. 88–95.

[96]. Alam M, Ferreira J, Mumtaz S, Jan MA, Rebelo R, Fonseca JA, Smart cameras are making our beaches safer: A 5g-envisioned distributed architecture for safe, connected coastal areas, IEEE Vehicular Technology Magazine 12 (2017) 50–59.

[97]. Pourghebleh B, Wakil K, Navimipour NJ, A comprehensive study on the trust management techniques in the internet of things, IEEE Internet of Things Journal 6 (2019) 9326–9337.

[98]. Głowacka J, Krygier J, Amanowicz M, A trust-based situation awareness system for military applications of the internet of things, in: 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT), IEEE, 2015, pp. 490–495.

[99]. Chen R, Bao F, Guo J, Trust-based service management for social internet of things systems, IEEE transactions on dependable and secure computing 13 (2015) 684–696.

[100]. Li J, Bai Y, Zaman N, Leung VC, A decentralized trustworthy context and qos-aware service discovery framework for the internet of things, IEEE Access 5 (2017) 19154–19166.

[101]. Jayasinghe U, Truong NB, Lee GM, Um T-W, Rpr: A trust computation model for social internet of things, in: 2016 Intl IEEE Conferences on Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld), IEEE, 2016, pp. 930–937.

[102]. Abderrahim OB, Elhdhili MH, Saidane L, Tmcoi-siot: A trust management system based on communities of interest for the social internet of things, in: 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC), IEEE, 2017, pp. 747–752.

[103]. Monir MB, AbdelAziz MH, AbdelHamid AA, EI-Horbaty E-SM, Trust management in cloud computing: A survey, in: 2015 IEEE Seventh International Conference on Intelligent Computing and Information Systems (ICICIS), IEEE, 2015, pp. 231–242.

[104]. Jayasinghe U, Otebolaku A, Um T-W, Lee GM, Data centric trust evaluation and prediction framework for iot, in: 2017 ITU Kaleidoscope: Challenges for a Data-Driven Society (ITU K), IEEE, 2017, pp. 1–7.

[105]. Abeysekara P, Dong H, Qin A, Machine learning-driven trust prediction for mec-based iot services, in: 2019 IEEE International Conference on Web Services (ICWS), IEEE, 2019, pp. 188–192.

[106]. Wang Y, Chen R, Cho J-H, Swami A, Lu Y-C, Lu C-T, Tsai JJ, Catrust: Context-aware trust management for service-oriented ad hoc networks, IEEE Transactions on Services Computing 11 (2016) 908–921.

[107]. Qwasmi N, Liscano R, Distributed policy based management for wireless sensor networks to support the internet of things environment, in: Proceedings of 24th Annual International Conference on Computer Science and Software Engineering, 2014, pp. 335–338.

[108]. Li W, Song H, Zeng F, Policy-based secure and trustworthy sensing for internet of things in smart cities, IEEE Internet of Things Journal 5 (2017) 716–723.

[109]. Al-Hamadi H, Chen R, Trust-based decision making for health iot systems, IEEE Internet of Things Journal 4 (2017) 1408–1419.

[110]. Chen JI-Z, Embedding the mrc and sc schemes into trust management algorithm applied to iot security protection, Wireless Personal Communications 99 (2018) 461–477.

[111]. Chen J, Tian Z, Cui X, Yin L, Wang X, Trust architecture and reputation evaluation for internet of things, Journal of Ambient Intelligence and Humanized Computing 10 (2019) 3099–3107.

[112]. Kapoukakis A, Pappas C, Androulidakis G, Papavassiliou S, Design and assessment of a reputation-based trust framework in wireless testbeds utilizing user experience, in: International Conference on Ad-Hoc Networks and Wireless, Springer, 2013, pp. 1–12.

[113]. Hussain Y, Zhiqiu H, Akbar MA, Alsanad A, Alsanad AA-A, Nawaz A, Khan IA, Khan ZU, Context-aware trust and reputation model for fog-based iot, IEEE Access 8 (2020) 31622–31632.

[114]. Debe M, Salah K, Rehman MHU, Svetinovic D, Iot public fog nodes reputation system: A decentralized solution using ethereum blockchain, IEEE Access 7 (2019) 178082–178093.

[115]. Asiri S, Miri A, An iot trust and reputation model based on recommender systems, in: 2016 14th Annual Conference on Privacy, Security and Trust (PST), IEEE, 2016, pp. 561–568.

[116]. Ahmed AIA, Ab Hamid SH, Gani A, Khan MK, et al. , Trust and reputation for internet of things: Fundamentals, taxonomy, and open research challenges, Journal of Network and Computer Applications (2019) 102409.

[117]. Theoleyre F, Pang A-C, Internet of Things and M2M Communications, River Publishers, 2013.

[118]. Chen S, Xu H, Liu D, Hu B, Wang H, A vision of iot: Applications, challenges, and opportunities with china perspective, IEEE Internet of Things journal 1 (2014) 349–359.

[119]. Anjum N, Karamshuk D, Shikh-Bahaei M, Sastry N, Survey on peer-assisted content delivery networks, Computer Networks 116 (2017) 79–95.

[120]. Dinh TTA, Liu R, Zhang M, Chen G, Ooi BC, Wang J, Untangling blockchain: A data processing view of blockchain systems, IEEE Transactions on Knowledge and Data Engineering 30 (2018) 1366–1385.

[121]. Bhowmik D, Feng T, The multimedia blockchain: A distributed and tamper-proof media transaction framework, in: 2017 22nd International Conference on Digital Signal Processing (DSP), IEEE, 2017, pp. 1–5.

[122]. Swan M, Blockchain: Blueprint for a new economy, " O'Reilly Media, Inc.", 2015.

[123]. Conoscenti M, Vetro A, De Martin JC, Blockchain for the internet of things: A systematic literature review, in: 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), IEEE, 2016, pp. 1–6.

[124]. Sharma PK, Park JH, Blockchain based hybrid network architecture for the smart city, Future Generation Computer Systems 86 (2018) 650–655.

[125]. Gipp B, Kosti J, Breitinger C, Securing video integrity using decentralized trusted timestamping on the bitcoin blockchain., in: MCIS, 2016, p. 51.

[126]. Hepp T, Schoenhals A, Gondek C, Gipp B, Originstamp: A blockchain-backed system for decentralized trusted timestamping, it-Information Technology 60 (2018) 273–281.

[127]. Kerr M, Han F, van Schyndel R, A blockchain implementation for the cataloguing of cctv video evidence, in: 2018 15th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS), IEEE, 2018, pp. 1–6.

[128]. Liu M, Yu FR, Teng Y, Leung VC, Song M, Distributed resource allocation in blockchain-based video streaming systems with mobile edge computing, IEEE Transactions on Wireless Communications 18 (2019) 695–708.

[129]. Stone A, An examination of single transaction blocks and their effect on network throughput and block size, Self-published Paper (2015).

[130]. Rizun PR, A transaction fee market exists without a block size limit, Block Size Limit Debate Working Paper (2015).

[131]. Kshetri N, Can blockchain strengthen the internet of things?, IT professional 19 (2017) 68–72.

[132]. Salah K, Rehman MHU, Nizamuddin N, Al-Fuqaha A, Blockchain for ai: review and open research challenges, IEEE Access 7 (2019) 10127–10149.

[133]. Kuo T-T, Kim H-E, Ohno-Machado L, Blockchain distributed ledger technologies for biomedical and health care applications, Journal of the American Medical Informatics Association 24 (2017) 1211–1220. [PubMed: 29016974]

[134]. Hackius N, Petersen M, Blockchain in logistics and supply chain: trick or treat?, in: Proceedings of the Hamburg International Conference of Logistics (HICL), epubli, 2017, pp. 3–18.

[135]. Lee J, Mtibaa A, Mastorakis S, A case for compute reuse in future edge systems: An empirical study, in: 2019 IEEE Globecom Workshops (GC Wkshps), IEEE, 2019, pp. 1–6.

[136]. Dorri A, Steger M, Kanhere SS, Jurdak R, Blockchain: A distributed solution to automotive security and privacy, IEEE Communications Magazine 55 (2017) 119–125.

[137]. He Q, Zhang C, Ma X, Liu J, Fog-based transcoding for crowdsourced video livecast, IEEE Communications Magazine 55 (2017) 28–33.

[138]. Wei L, Cai J, Foh CH, He B, Qos-aware resource allocation for video transcoding in clouds, IEEE Transactions on Circuits and Systems for Video Technology 27 (2016) 49–61.

[139]. Chen H, Pendleton M, Njilla L, Xu S, A survey on ethereum systems security: Vulnerabilities, attacks, and defenses, ACM Computing Surveys (CSUR) 53 (2020) 1–43.

[140]. Novo O, Blockchain meets iot: An architecture for scalable access management in iot, IEEE Internet of Things Journal 5 (2018) 1184–1195.

[141]. Daza V, Di Pietro R, Klimek I, Signorini M, Connect: Contextual name discovery for blockchain-based services in the iot, in: 2017 IEEE International Conference on Communications (ICC), IEEE, 2017, pp. 1–6.

[142]. Yuan R, Xia Y-B, Chen H-B, Zang B-Y, Xie J, Shadoweth: Private smart contract on public blockchain, Journal of Computer Science and Technology 33 (2018) 542–556.

[143]. Crosby M, Pattanayak P, Verma S, Kalyanaraman V, et al. , Blockchain technology: Beyond bitcoin, Applied Innovation 2 (2016) 71.

[144]. Petkanic D, Tang E, Livepeer whitepaper: Protocol and economic incentives for a decentralized live video streaming network, 2017.

[145]. Ferdous MS, Biswas K, Chowdhury MJM, Chowdhury N, Muthukkumarasamy V, Integrated platforms for blockchain enablement, in: Advances in Computers, volume 115, Elsevier, 2019, pp. 41–72.

[146]. Larmuseau A, Shila DM, Private blockchain configurations for improved iot security, in: Blockchain for Distributed Systems Security, John Wiley & Sons, Inc. Hoboken, NJ, USA, 2019, pp. 253–274.

[147]. Fan X, Faster dual-key stealth address for blockchain-based internet of things systems, in: 2018 International Conference on Blockchain (ICBC 2018), ICBC, 2018, pp. 1–12.

[148]. Rakic B, Levak T, Drev Z, Savic S, Veljkovic A, First purpose built protocol for supply chains based on blockchain, OriginTrail, Ljubljana, Slovenia, Tech. Rep 1 (2017).

[149]. Vuppala S, et al. , ubiquitous, secure internet-of-things with location and contex-awareness, BUTLER project D 2 (2018) 1–171.

[150]. Dorri A, Kanhere SS, Jurdak R, Gauravaram P, Lsb: A lightweight scalable blockchain for iot security and anonymity, Journal of Parallel and Distributed Computing 134 (2019) 180–197.

[151]. Hochleitner C, Graf C, Wolkerstorfer P, Tscheligi M, utrustit-usable trust in the internet of things, in: International Conference on Trust, Privacy and Security in Digital Business, Springer, 2012, pp. 220–221.

[152]. Soultatos O, Papoutsakis M, Fysarakis K, Hatzivasilis G, Michalodimitrakis M, Spanoudakis G, Ioannidis S, Pattern-driven security, privacy, dependability and interoperability management of iot environments, in: 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), IEEE, 2019, pp. 1–6.

[153]. Petroulakis NE, Lakka E, Sakic E, Kulkarni V, Fysarakis K, Somarakis I, Serra J, Sanabria-Russo L, Pau D, Falchetto M, et al., Semiotics architectural framework: End-to-end security, connectivity and interoperability for industrial iot, in: 2019 Global IoT Summit (GIoTS), IEEE, 2019, pp. 1–6.

[154]. Siris VA, Dimopoulos D, Fotiou N, Voulgaris S, Polyzos GC, Decentralized authorization in constrained iot environments exploiting interledger mechanisms, Computer Communications 152 (2020) 243–251.

[155]. Kortesniemi Y, Lagutin D, Elo T, Fotiou N, Improving the privacy of iot with decentralised identifiers (dids), Journal of Computer Networks and Communications 2019 (2019).

[156]. Domańska J, Nowak M, Nowak S, Czachórski T, European cybersecurity research and the seriot project, in: International Symposium on Computer and Information Sciences, Springer, 2018, pp. 166–173.

[157]. Domanska J, Gelenbe E, Czachorski T, Drosou A, Tzovaras D, Research and innovation action for the security of the internet of things: The seriot project, in: International ISCIS Security Workshop, Springer, 2018, pp. 101–118.

[158]. Vajda V, Furdík K, Glova J, Sabol T, The ebbits project: An interoperability platform for a real-world populated internet of things domain, in: Proceedings of the International Conference Znalosti (Knowledge), Technical University of Ostrava, Czech Republic, 2011, pp. 317–320.

[159]. Li N, Liu D, Nepal S, Lightweight mutual authentication for iot and its applications, IEEE Transactions on Sustainable Computing 2 (2017) 359–370.

[160]. Al-Janabi S, Al-Shourbaji I, Shojafar M, Shamshirband S, Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications, Egyptian Informatics Journal 18 (2017) 113–122.

[161]. Hamidi H, An approach to develop the smart health using internet of things and authentication based on biometric technology, Future generation computer systems 91 (2019) 434–449.

[162]. Aghili SF, Mala H, Shojafar M, Peris-Lopez P, Laco: Lightweight three-factor authentication, access control and ownership transfer scheme for e-health systems in iot, Future Generation Computer Systems 96 (2019) 410–424.

[163]. Yang Y, Zheng X, Guo W, Liu X, Chang V, Privacy-preserving fusion of iot and big data for e-health, Future Generation Computer Systems 86 (2018) 1437–1455.

[164]. McGhin T, Choo K-KR, Liu CZ, He D, Blockchain in healthcare applications: Research challenges and opportunities, Journal of Network and Computer Applications (2019).

[165]. Xu J, Xue K, Li S, Tian H, Hong J, Hong P, Yu N, Healthchain: A blockchain-based privacy preserving scheme for large-scale health data, IEEE Internet of Things Journal 6 (2019) 8770–8781.

[166]. Bormann C, Castellani AP, Shelby Z, Coap: An application protocol for billions of tiny internet nodes, IEEE Internet Computing 16 (2012) 62–67.

[167]. Singh SK, Rathore S, Park JH, Blockiotintelligence: A blockchain-enabled intelligent iot architecture with artificial intelligence, Future Generation Computer Systems (2019).

[168]. Mastorakis S, Afanasyev A, Yu Y, Zhang L, ntorrent: Peer-to-peer file sharing in named data networking, in: 2017 26th International Conference on Computer Communication and Networks (ICCCN), IEEE, 2017, pp. 1–10.

[169]. Schmalstieg D, Hollerer T, Augmented reality: principles and practice, Addison-Wesley Professional, 2016.

[170]. Fraga-Lamas P, Fernández-Caramés TM, A review on blockchain technologies for an advanced and cyber-resilient automotive industry, IEEE Access 7 (2019) 17578–17598.

[171]. Capece N, Erra U, Romaniello G, A low-cost full body tracking system in virtual reality based on microsoft kinect, in: International Conference on Augmented Reality, Virtual Reality and Computer Graphics, Springer, 2018, pp. 623–635.

[172]. Shannigrahi S, Mastorakis S, Ortega FR, Next-generation networking and edge computing for mixed reality real-time interactive systems, in: 2020 IEEE International Conference on Communications Workshops (ICC Workshops), IEEE, 2020.

[173]. Ahmed G, Islam SU, Shahid M, Akhunzada A, Jabbar S, Khan MK, Riaz M, Han K, Rigorous analysis and evaluation of specific absorption rate (sar) for mobile multimedia healthcare, IEEE Access 6 (2018) 29602–29610.

[174]. Xie H, Wang J, Shao B, Gu J, Li M, Le-hgr: A lightweight and efficient rgb-based online gesture recognition network for embedded ar devices, in: 2019 IEEE International Symposium on Mixed and Augmented Reality Adjunct (ISMAR-Adjunct), IEEE, 2019, pp. 274–279.

[175]. Mekki K, Bajic E, Chaxel F, Meyer F, A comparative study of lpwan technologies for large-scale iot deployment, ICT express 5 (2019) 1–7.

[176]. Schulz P, Matthe M, Klessig H, Simsek M, Fettweis G, Ansari J, Ashraf SA, Almeroth B, Voigt J, Riedel I, et al. , Latency critical iot applications in 5g: Perspective on the design of radio interface and network architecture, IEEE Communications Magazine 55 (2017) 70–78.

[177]. Ullah R, Rehman MAU, Naeem MA, Kim B-S, Mastorakis S, Icn with edge for 5g: Exploiting in-network caching in icn-based edge computing for 5g networks, Future Generation Computer Systems (2020).

[178]. Xie J, Tang H, Huang T, Yu FR, Xie R, Liu J, Liu Y, A survey of blockchain technology applied to smart cities: Research issues and challenges, IEEE Communications Surveys & Tutorials 21 (2019) 2794–2830.

[179]. Shi W, Cao J, Zhang Q, Li Y, Xu L, Edge computing: Vision and challenges, IEEE internet of things journal 3 (2016) 637–646.

[180]. Mastorakis S, Mtibaa A, Lee J, Misra S, Icedge: When edge computing meets information-centric networking, IEEE Internet of Things Journal 7 (2020) 4203–4217.

[181]. Yu W, Liang F, He X, Hatcher WG, Lu C, Lin J, Yang X, A survey on the edge computing for the internet of things, IEEE access 6 (2017) 6900–6919.

[182]. Nour B, Mastorakis S, Mtibaa A, Compute-less networking: Perspectives, challenges, and opportunities, IEEE Network (2020).

[183]. Mastorakis S, Mtibaa A, Towards service discovery and invocation in data-centric edge networks, in: 2019 IEEE 27th International Conference on Network Protocols (ICNP), IEEE, 2019, pp. 1–6.

[184]. Masoudi R, Ghaffari A, Software defined networks: A survey, Journal of Network and computer Applications 67 (2016) 1–25.

[185]. Jararweh Y, Al-Ayyoub M, Benkhelifa E, Vouk M, Rindos A, et al. , Sdiot: a software defined based internet of things framework, Journal of Ambient Intelligence and Humanized Computing 6 (2015) 453–461.

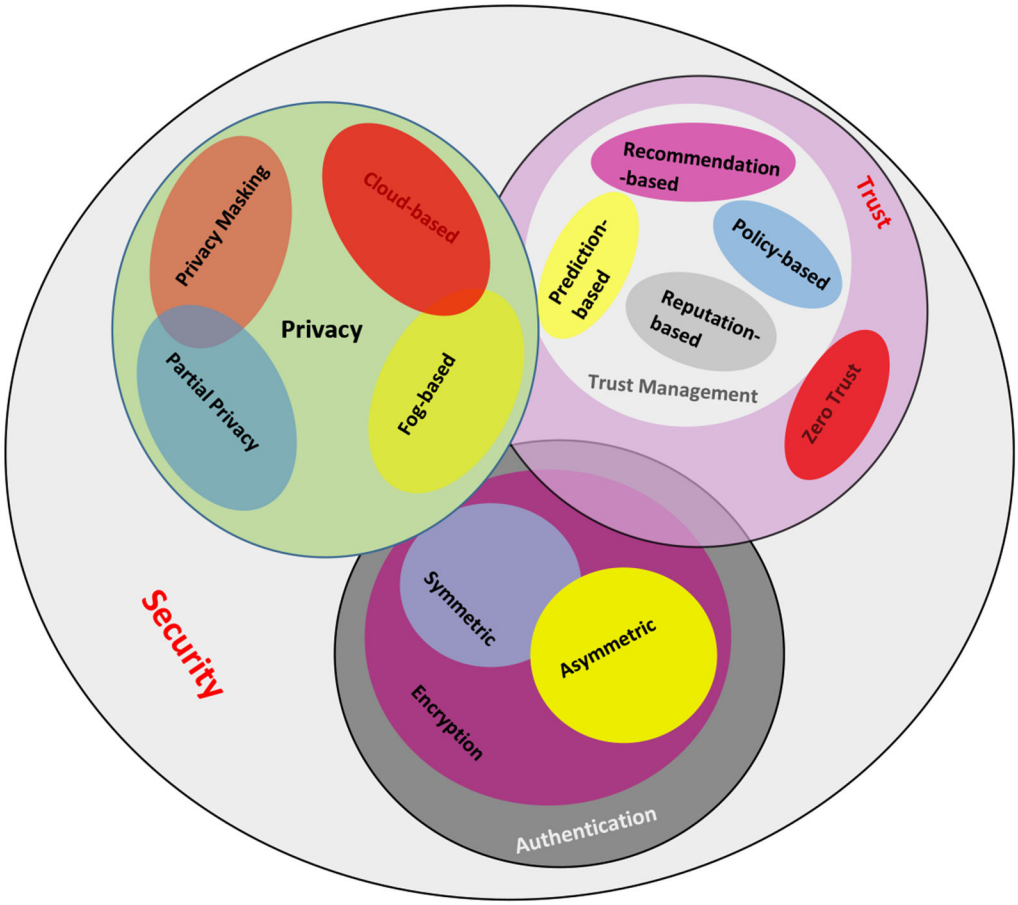

Figure 1:
Internet of Multimedia Things Security

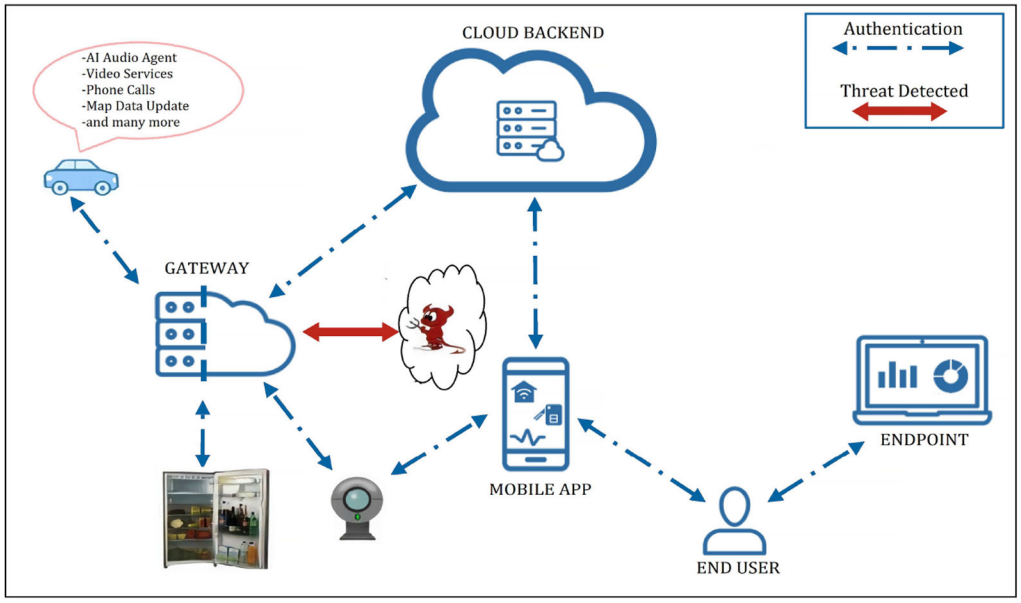

Figure 2:
IoMT Authentication

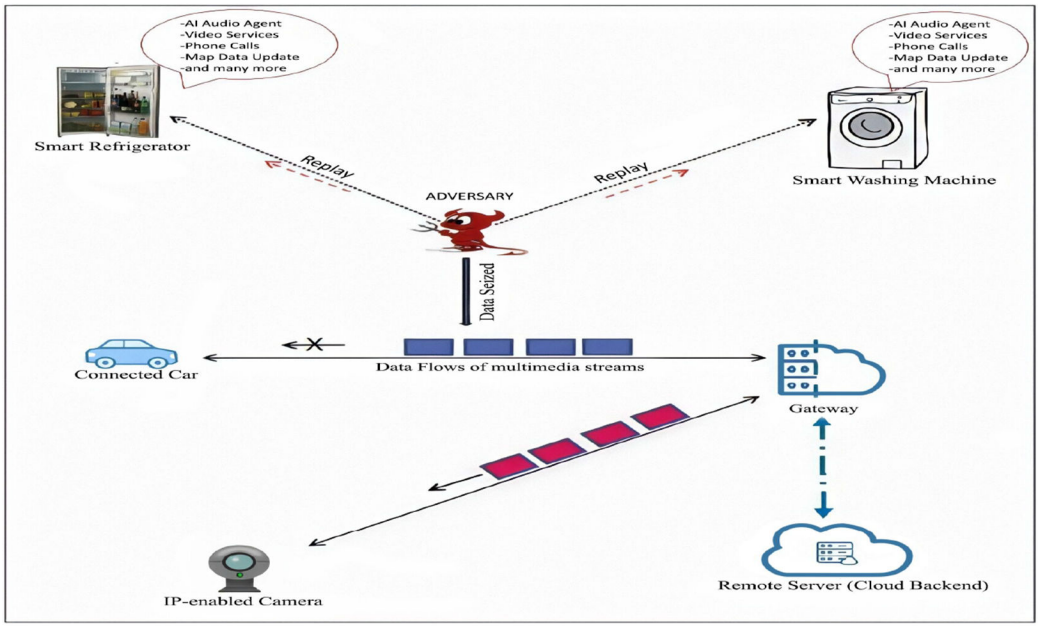

Figure 3:
Replay Attack in IoMT

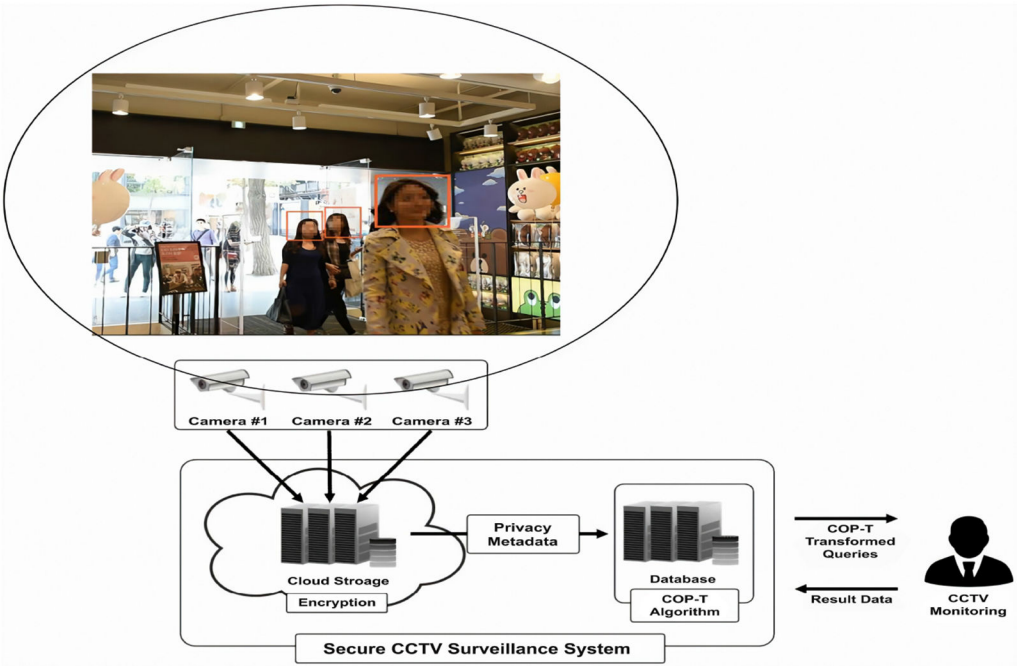

Figure 4:
Privacy preservation in Intelligent Video Surveillance System

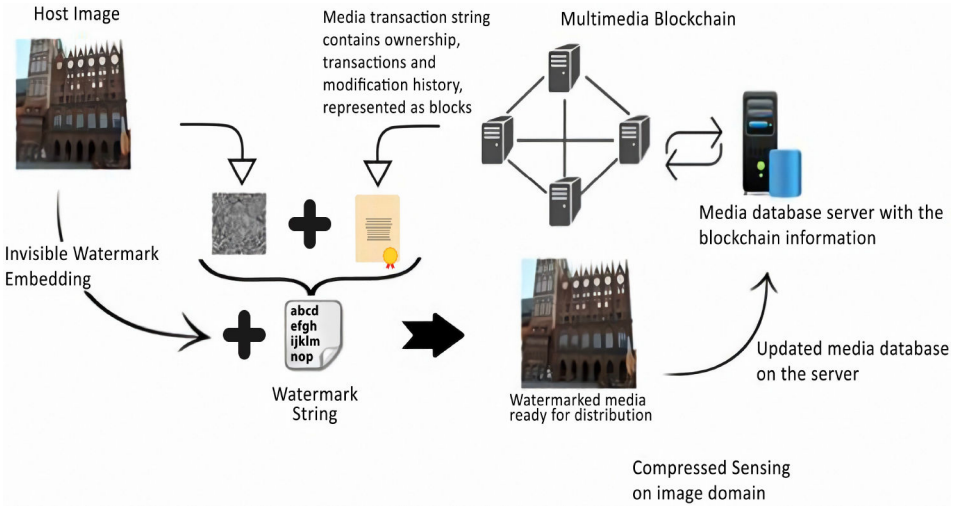

Figure 5:
Blockchain for Multimedia streaming Applications

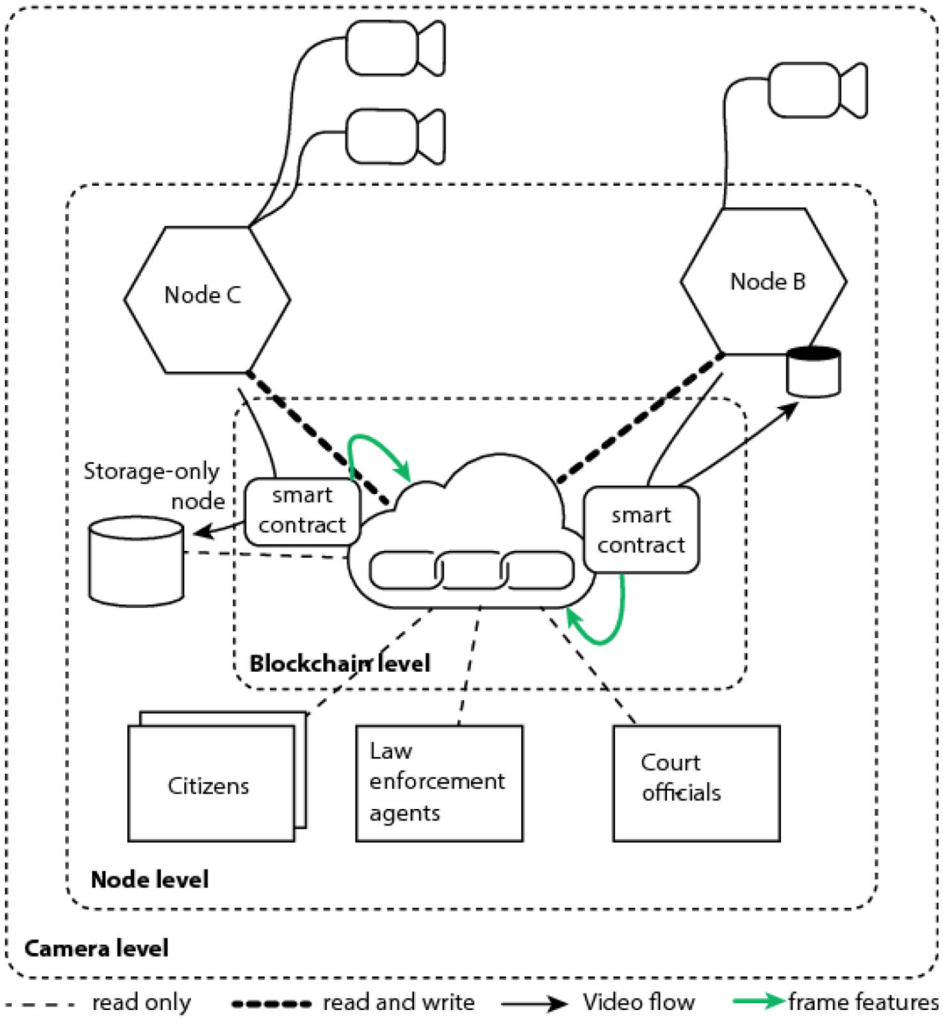

Figure 6:
Blockchain-enabled Video Surveillance in a Smart City

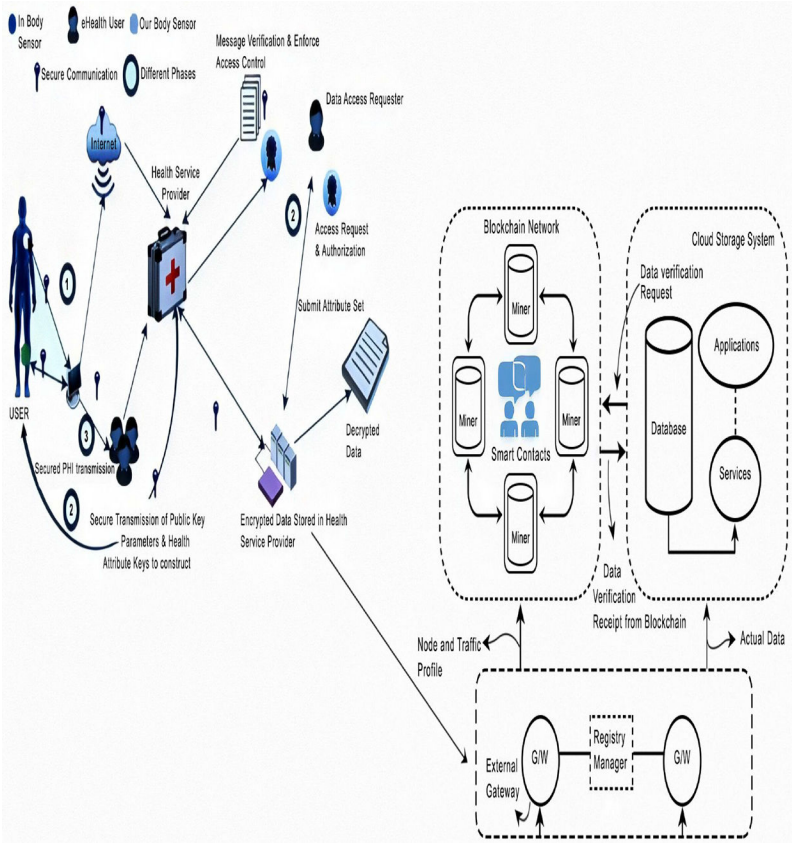

Figure 7:
Security and Blockchain for Healthcare

Table 1:

Comparison with Existing Surveys

Survey	Security			Blockchain	On-going Commercial Projects	Case Studies
	Authentication	Privacy	Trust			
[36]	x	x	✓	x	x	x
[37]	x	x	✓	x	x	x
[38]	x	x	✓	x	x	x
[27]	✓	x	x	x	x	x
[28]	✓	x	✓	x	x	x
[29]	✓	x	✓	x	x	x
[19]	✓	✓	x	x	x	x
[30]	✓	✓	x	x	x	x
[31]	✓	✓	✓	x	x	x
[32]	✓	✓	✓	x	x	x
[33]	✓	✓	✓	x	x	x
[34]	✓	✓	✓	x	x	✓
[35]	✓	✓	✓	✓	x	x
[39]	x	x	x	✓	x	✓
[40]	x	x	x	✓	x	✓
[41]	x	x	x	✓	x	✓
[42]	x	x	x	✓	x	✓
[43]	✓	✓	x	✓	x	✓
[45]	✓	✓	x	✓	x	✓
Our Work	✓	✓	✓	✓	✓	✓

Table 2:

Smart IP-enabled Devices: Type of Classes

Class	RAM (KB)	Flash (KB)	Limitations
0	« 10	« 100	Unable to communicate with Internet-enabled devices
1	≈ 10	≈ 100	Unable to communicate with HTTP-based web-enabled applications
2	≈ 50	≈250	Unable to support high data rate live-streaming applications

Table 3:

Privacy preservation Techniques for Smart IP-connected Devices of IoMT

Techniques	Operational Mechanism	Type of Data	Limitations
Privacy Masking	Blurring, pixelation, facial-region removal	Facial	Unable to deal with deep resolution and big data-enabled heterogeneous video streams.
Partial Privacy	Denaturing	selected regions of interest (RIO)	No precise explanation for meta-data generation and protection.
Cloud-based Privacy	Local differential privacy (LDP)	H.264, H.265 and Images	Demands higher bandwidth and incurs excessive latency
Fog-based Privacy	Fog layer encryption	H.264 and Images	Unable to support high data rate live-streaming applications

Table 4:

Trust Management in IoMT

Techniques	Pros	Cons	Attacks Addressed
Recommendation-based [98, 99, 100, 101]	adaptive, scalablity	Accuracy, Integrity	collusion, sybil, self-promoting attacks
Prediction-based [102, 104, 105, 106]	scalable, accurate	does not guarantee trust evaluation results	malicious behavior
Policy-based [107, 108, 109, 110]	adaptability, accuracy, reliability	device heterogeneity	collusion, malicious behavior
Reputation-based [111, 113, 114, 115]	reliability, confidence	device heterogeneity, integrity	malicious behavior, self-promoting attacks

Table 5:

Blockchain-enabled IoMT Platforms

Platforms	Type	Speed	Token	Energy	Consensus
Theta	Public	1000+ TPS	Theta MainNet 2.0	Low	multi-Level BFT
Livepeer	Public	-	LPT	Low	Depends on Eth
Moeco	Public	Depends on Eth	MOE	High	Depends on Eth
Waltonchain	Public and Private	100 TPS	WTC	Low	WPoC
IoTeX	Private	200 TPS	VITA	Low	Roll-DPoS
OriginTrail	Public	Eth+ODN	TRAC	Moderate	PoW

Table 6:

Industrial Projects: Security and Blockchain for IoMT

Project	Operational Mechanism	Security			Blockchain
		Authentication	Privacy	Trust	
BUTLER [149]	Context-aware system	✓	✓	✓	x
LSB [150]	Distributed Ledger	✓	✓	✓	✓
uTrustit [151]	Trust-feedback Toolkit	✓	x	✓	x
SEMIoTICS [152, 153]	Self-adaptation	✓	✓	x	x
SOFIE [154, 155]	Federation-centric	✓	✓	x	✓
SerIoT [156, 157]	Cross-layer Holistic	✓	✓	x	✓
IDS [158]	Search Engine	✓	✓	✓	x
CLAP [159]	Rate Regulation	✓	✓	x	x