Video Security in Internet of Things: An Overview

Mina A. Hamoudy, Mahmoud H. Qutqut and Fadi Almasalha

Faculty of Information Technology, Applied Science Private University Amman, 11931 Jordan

Summary
Internet of Things (IoT) became one of the core networking paradigms nowadays. IoT is already interconnected millions of things (e.g., sensors, appliances, video cameras, devices); and expected soon to connect billions of new devices. An important challenge for supporting multimedia applications in the IoT is the security heterogeneity of several of technologies, devices, and protocols. In this paper, we overview the video streaming in the IoT networks; focusing on the security of video in IoT. We present a comprehensive overview of security issues and challenges in video streaming in IoT in order for a better understanding.

Key words:
Internet of Things; Security; Video Streaming; Video Traffic; IoT Video, Video Security.

1. Introduction

The world is witnessing the networking paradigm of Internet of Things (IoT) that is also sometimes called as Internet of Objects. The phrase "Internet of Things" is the methodology of everyday entities such as; industrial machines or tools to general devices – utilizing built-in sensors or any other entities in order to collect all the needed data and also respond to those data through a network [1] . There will 26 billion things connected to the Internet as indicated by IT analyst Gartner [2]. IoT is coming out as one of the most important trends lightening the development of technologies [3]. IoT is an Internet based technical architecture that eases the exchange of goods and many services in wide supply chain networks which also has a strong effect on the privacy and security of the main stakeholders [3].

Basic measurements that ensure the architecture reliance to attacks, access control, data and user authentication need to be established [4]. Privacy includes preventing the publication of personal information as well as the expertise to control what really happens with this information, IoT security seems to be the biggest concern for the stakeholders in order to allow such devices in their daily life routine As IoT is created to be functioning on the Internet, security problems and issues of the Internet will appear in IoT as well. IoT consists of four layers: application layer, support layer, network layer and perceptual layer.

Video streaming becomes very common in IoT networks due to the fact that many of internet connected devices are capable of capturing video content. These video capable devices and applications include surveillance security cameras, smart traffic cameras, transit vehicles, house monitors, etc. Figure 1 shows several applications of video in IoT. As valued data is being captured by these devices, video content in several cases are critical and it is not allowed anyone to access such content [3]. Also, sometimes video needs to be processed in order to extract information from it which adds a significant processing overhead on the IoT devices. Hence, video streaming security is very difficult nowadays to be achieved, due to the critical importance for various multimedia applications in IoT. In addition to that, IoT is by nature created to perform unauthorized user applications and similar end devices for accessing some contents. Moreover, most of the IoT devices run on low profile processors to save some power and memory available on board which leaves the devices with limited capabilities to perform most of the robust security encryption algorithms. Therefore, users and applications are both considered to be vulnerable threats for the security of IoT in general [5].

It is very difficult to fulfill customer privacy needs especially multimedia or video streaming security needs. A wide number of methodologies have been deployed in order to bring off information privacy objectives [4]. Meanwhile, several provocations and challenges will appear in the path of the IoT. Regarding privacy issues, IoT applications that need wide numbers of devices are most likely hard to be deployed due to time limitation, memory, processing, and energy constraints [4].

As we know, multimedia and video streaming security is a challenging problem in heterogeneous communications [3]. Therefore, authentications should take place through deploying methods which could range from user and server authentication to the use of access control certificates. Security and privacy are among the main attributes for IoT applications, in which it faces a lot of challenges.

Nowadays, security is a critical component for many multimedia applications in IoT [3]. Since the IoT is functioned to execute unverified user applications as both users and application can be attached and affected. Meanwhile, users can manipulate with public multimedia data or tire the network to interrupt data or services shared to other users. It is important to adopt a security strategy in

Manuscript received August 5, 2017
Manuscript revised August 20, 2017

order to save secured multimedia applications which are streamed over the IoT system [3].

In this paper, we overview and describe security issues and challenges in video streaming in IoT in order to give a comprehensive understanding. The rest of this paper is organized as follow; Section 2 provides an overview of the overall security in IoT systems and shows the differences in security issues between IoT and traditional networks. In Section 3, we describe the video streaming in the context of IoT; then shows the challenges in IoT video and categorize video traffic. We overview aspects affect video security in IoT systems in Section 4. Section 5 presents some security elements which can be utilized in IoT video; then we conclude the paper in section 6.

2. Security in IoT

The network and information security must always be protected with special specifications like identification, integrity, and confidentiality as it differs from the internet security. As all IoT security issues are basically application driven, as well as their presented solutions. With plenty of application and security requirements, many security designs can be introduced to overcome the current security features as well as the security of video streaming features [4]. This implies IoT security architecture is created in order not be able to make one framework to take all cases. However, ideas can be borrowed from software engineering in which we can conclude the mutuality across these IoT applications. Then, the abstract security architecture could be created and designed to provide all the needed security solutions to IoT applications. Meanwhile, the architectural security top level offers security adapters with many other applications such as video monitoring and environmental monitoring, in which it can offer application specific algorithms to send/receive data with the top level security algorithms. Therefore, we the differences between different IoT applications can be produced [3].

Security rules and aggregations also state the actual security mechanism requirements that force security rules. In the current common experience, the security rules are either managed by IT departments or maintained with traditional rules. However, most of the time that rules do not meet the requirements of the applications. This implies an unfinished system [6].

Currently, security has a critical importance for various video streaming applications in IoT. On condition that the video IoT is created to the function of unauthorized user applications from different kinds of end users (in which they can access these applications anytime anywhere for different kinds of objectives such as monitoring applications and users) are the main security threats in the IoT system [3].

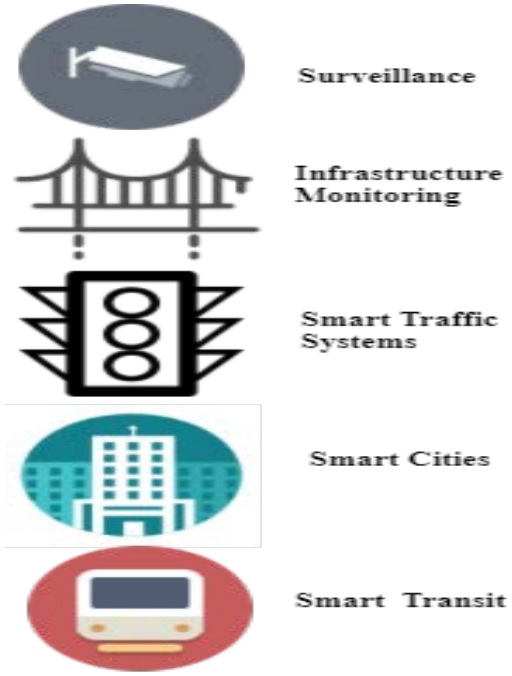

Fig. 1 Applications of using video IoT.

This sums up that the security must be taken into account as a major system level attribute particularly the multimedia security in which must be considered in the architecture design and methods for the IoT solutions [3].

2.1 Security Issues Differences between IoT and Traditional Networks

IoT and classical network security features which may differ in so many methods such as; IoT consist of Radio Frequency Identification (RFID) points and Wireless Sensor Network (WSN) points, in which their resources are restricted, meanwhile, the Internet consist of PC, servers, smart phones in which its resources are plentiful. In the Internet, aggregation of a combination of algorithms can be utilized to increase security with fewer realizations of resource handling like computation power. While in IoT, at so many cases, only lightweight algorithms can be used in order to discover the stability of security and power usage. As mentioned above, the communication between IoT parties is always slow, less secure wireless media, in which could lead to data leakage. On the other hand, most interactions are through fast, more secured wire or wireless connections in the Internet. This implies that even the Mobile Internet, the wireless communications are created on top of composed secure protocols which are almost unfeasible to function for resource restricted IoT parties.

If IoT system control has been lost, it would be a strong security problem. As on the Internet, if the information of one user were not provided by the user himself, attackers will not have the chance to attain that information. With the assistance of the operating system and much more security software, the system's environment is highly secured.

However, an IoT system takes place in a more unsafe environment with restricted resources and fewer network safety guards; lightweight solutions need to be implemented to deal with this unsafe environment [4].

The fast development in the application that utilizes IoT methodologies implies that the privacy and security issues are a top priority. The IoT applications will be strongly deployed and can consist of a huge number of a very sensitive data in which the data developers would not accept these data to be reached by wrong hands [7].

3. Video Streaming over Internet of Things (IoT)

3.1 What is video streaming over Internet of Things?

With the massive dawn of the IoT, there have been several challenges facing this technology, such as visualization which is risky for IoT application as it gives the user the ability to interact with the environment. Along with the development of touch screens that utilize in smart phones and tablets. Video streaming allows the idea of sharing the data between multiple service providers in a very smooth way in which conducting many business opportunities [5].

IoT provides the suitable platform to understand this vision by utilizing body area sensors and IoT backend to have the data to servers shared. For examples, users could use a Smartphone to communicate along with many interfaces such as Bluetooth for interfacing sensors measuring physiological parameters. For the time being, there is much kind of applications that are accessible for Apple iOS, Google Android and Windows Phone operating system that calculates different parameters. However, it is yet to be in the center of the cloud for general users to access the same [8].

Controlling various housing equipment are such as air conditioners, heating machines, washing machines etc., will give the opportunity to have a better home and power control. This will involve end users in IoT development in the same procedure as the Internet development itself. Social media is ready to witness another transmission with a huge number of interconnected parts. An amusing technology will be utilizing Twitter like a methodology where parts of the house can also tweet the readings which can be tracked from any place creating a TweetOT. Although this offers a general framework through utilizing the cloud for accessing information, a new security paradigm could be needed for this issue in order to be fully absorbed and understood unguaranteed access [8].

3.2 Video Streaming Protocols

Streaming multimedia contents over the internet is achieved through multiple protocols; a real-time content uses real time protocols that may eliminate packet delivery process to enhance the delivery latency while others focus on the content delivery more than the real time requirement [9]. Basic network protocols are used at the bottom layers such as TCP and UDP on most IoT devices to enable them emerging seamlessly with existing networks. Higher level protocols are required to enable the full functionality and quality of multimedia streaming [9].

The most used multimedia protocol is RTP (Real Time Protocol), RTP provides end-to-end network transport functionality for the applications that need to transmit real-time data, especially multimedia content. RTP does not support resource reservation or guarantee Quality of Service [10]. The data is monitored through the presence of a Control Protocol (RTCP), which provides basic identification and other controlling features. RTP protocols can be carried over TCP or UDP protocols depending on the application requirements. RTMP and RTSP are built on top of RTP to provide multimedia streaming support which required special network port to work [10].

Recently some vendors started to use HTTP to deliver multimedia contents seamlessly over heterogeneous networks that may disable network protocols required by the RTP. Moreover, Apple HLS (Http Live Streaming), Adobe HDS (Adobe Flash Player) and Microsoft Smooth Streaming is built on top of HTTP to provide multimedia streaming functionalities to network with blocked network ports.

3.3 Challenges of IoT Video Streaming

Traffic management control contributes in an essential role by accomplishing a very high multimedia quality of service (QoS) within a network [5]. Unfortunately, multimedia management algorithms are mainly developed in order to make sure that no delays or distortion might occur while neglecting other security needs. The weak points of these applications can be uncovered by hackers and wrong users, hackers can easily have access to the system to start making bad service attacks. What is more, a hacker can tamper with multimedia shared data or exhaust the network resources to cut the available services to other users. On the other hand, IoT has not launched any specific security methodology to solve the mentioned threats. Thus, it is really necessary to launch a security plan or to save the secured critical

multimedia or video applications streaming in the IoT [5]. Multimedia traffic running over IoT can be divided into three types: communication, computation, and service (discussed in Section 3.3).

The biggest challenge of using smart devices within a home environment which it may have potential benefits for users such as families, members at work or school. Smart phones are also used to control the security of the household which may be explained as using different technologies like a video feed as for motion detection and facial recognition or event to control the lightening of a specific area. Meanwhile, the execution of all the networking protocols that generate video streaming or support multimedia can often result in a few throughput as generally, the protocols oblige the main device to function at an efficiency of approximately 60%. As a result in order to have a very high video streaming quality, it seeks 2400 kbps [7].

Video data needs to be domesticated and visualized using mathematical and computer models because old house techniques are not applicable to unstructured images and video data [11].

The solution for the above-mentioned challenges is to utilize cloud computing model as many IoT applications require a huge data storage space, massive speed broadband to function data, video or audio in which makes cloud computing the perfect and ideal backend to handle large data streams such as video streaming [12].

The major security problem of IoT is related to authentication and data integration. To do the authentication, data exchange between authentication servers and devices need to be done. This problem has not been solved yet. It is most likely for the number of video transmission to cause network congestion. In which it affects the video quality. System breakdown might also happen. If a large event happens at this time, in immeasurable impact might happen due to the shortage of monitoring video result [13].

With referring to the aforementioned challenges, few solutions have been proposed to overcome security vulnerabilities as some privacy enhancing techniques have been introduced to achieve both information and multimedia privacy goals. These Privacy Enhancement Techniques (PET) in which can be described as follows [14] [1]:

• **Virtual Private Networks (VPN);** which are established by private groups or business partners in which only specified authorized users have access to the system as they assure to use the information or multimedia in an appropriate way.
• **Transportation Layer Security (TLS**); based on a confidential and appropriate structure in which improves the confidentiality and security of IoT.

• **DNS Security Extensions (DNSSEC);** uses the public-key crypto system in order to guarantee the authentication of information.

More methods are deployed to enhance the security of multimedia over IoT are peer to peer (P2P) systems in which uses the authentication of users is done by stating shared secrets or using public- key cryptography to maintain that multimedia data cannot be accessed by unauthorized users that would attack or harm the data or network [14].

3.4 Classifications of Multimedia and Video Streaming Traffic in IoT

The attributes of the IoT make it easy to evolve a large number of video traffic. Usually, an IoT is understood through supplying several sensors with robust knowledge of connection, computation, and service capabilities. Multimedia traffic transferring over IoT can be divided into three categories: communication, computation, and service.

3.4.1 Communication Traffic

The phrase “anytime, anywhere, any-media” has been the main objective for the IoT. In this context, the major part of the communication traffic is the Radio Frequency Identification (RFID) system for example that includes plenty of readers and RFID tags. Every tag is specified by a distinct identifier and therefore deployed to different parts. Readers move tag transmission through producing generating a message, which introduces a request for the possible existence of tags in the circumference of the reader. As for a functional IoT, a RFID tag is described as a tiny microchip that is linked to an antenna, and the antenna is then utilized to receive the reader’s message and transmit the tag ID to the reader [5].

Generally, the main goals of designing adequate multimedia video streaming traffic are energy efficiency, scalability, reliability, and robustness [5].

3.4.2 Computation Traffic

Computation traffic can be managed and processed through mobile agents or sink nodes in which mobile agents can access the main nodes for Example: if users demand to access their multimedia data anywhere anytime they could use their mobile applications in order to perform their functions by determining the selected source nodes [5].

3.4.3 Service Traffic

Services traffic consist of two main parts: score and form, the score means how one user is interested in multimedia traffic, while the form is the context attribute of a specific

device. In order to fulfill efficiently operate different kinds of multimedia traffic, data is categorized into three types: preference data, situation data, and capability data [5].

3.5 Security of Video Streaming Storage

IoT interacts with having the data shared and stored in several locations. After storing the data it will be used intelligently in video monitoring and actuation. As the multimedia and video streaming specifically is being developed in which conducting a higher network transmission quality; transmission and storage take a large occupation in space.

In order to solve this issue, a new concept of multimedia cloud has been proposed to overcome the problem of distributed multimedia processing and space. Therefore, several security schemes for could computing have been proposed. These schemes based on the methodology of data encryption cloud storage by encrypting files in order to authorize a user access storage. The proposed schemes consist of main seven steps: setup, extract, manage role, add a user, revoke a user, encrypt and decrypt [14].

For the moment, the intelligence and control are not the basic components of the original methodology of IoT. Through the large improvement of developed network mechanisms, distributed multi-agent control, and cloud computing, there is a wide transportation with producing the methodology of IoT and autonomous control [15]. Meanwhile, cloud computing has been considered to be the best solution for this problem of video streaming file storage in many research work [14].

4. Factors Touching the IoT video Streaming Security

Many provocations are involved while creating IoT. In this section, important security related provocations are described in brief, as the follow [8] [16]:

Access Control

Access control is indulged with access authentications that are proposed to the parts/devices in IoT environment. In old house database systems, discrete data processing is done, meanwhile in IoT, flowing data processing is done. Two theories are clarified for access control:

1) Data holders (stakeholders, end users), who are involved with send/receive data to objects. Their data should be sent only to authenticated parts.
2) Data collectors (things), which must authenticate users have or hold to be authenticated to the system.

A. Privacy

A data preserving methodology privacy is proposed in IoT.

B. Policy Enforcement

Policy enforcement means that the methodologies used to create the application are systems. Policies are functioning rules which need to be fulfilled for the goal of receiving, security, privacy, and data consistency.

C. Trust

The core idea of trust is held in different ways and with different descriptions. Trust is a critical concept.

D. Mobile Security

Mobile junction or nodes in IoT frequently transport from one cluster to another, in which protocols of cryptography are utilized to provide, authentication, and privacy conservation.

E. Secure Middleware

Numbers of different kinds of middleware layer are also related to impact the consistency and the privacy of devices and data within the exact same information network.

F. Authentication & Confidentiality

Different work implies dissimilar protocols and methodologies to deal with verification and authentication of an end user and confidentiality of its data in the core of IoT.

5. Security Elements Required in the IoT Video

Secure data network needs the accomplishment of mainly three primary security goals. These goals are commonly referred to as the CIA triad and include the following [7]: Confidentiality, Integrity and Authentication. To fulfill the information security needs for multimedia connection, computation, and service in the environment of an IoT, it is important to realize some qualifications that are related to the security strategy and performance and that can be utilized for video streaming security. Some main elements are described below.

5.1 Key Management

Key management is the most difficult part of the cryptographic mechanism of security so that it is very import component to fulfill video and multimedia security such as Lightweight cryptographic algorithm [9].

In the last years, numbers of network-based key management algorithms have been introduced and explained which also could be divided into three parts [5]:

• Non-scalable and scalable schemes. Scalable schemes are also divided into three types: hierarchical key management, centralized flat key management, and distributed flat key management.

5.2 Authentication

Major work authentication and confidentiality related in IoT are as follows: smart business security IoT application protocol, which consolidate cross-platform connections along with encryption, signature, and validation and authentication, as to enhance IoT multimedia video applications growth capabilities and declares the functionality of two-way authentication security scheme as to improve the privacy and security level of multimedia through authenticating the ID of a user through different validation types [14]. User authentication indicates methodologies that range from the utilization of access control and ability certificates to mutual authentication between the server and the end user. We describe these methodologies below.

• Access control: The IoT multimedia server conserves a record of hosts who are either their access is guaranteed to join the service or denied from it. The moment that a user transmits a join request, the server then will check the user's ID in the access control record to decide if the user is registered and permitted or not. It is important to understand that this record needs to be updated as the record may change or be modified dynamically with new authorizations or denials to the multimedia system.
• Ability certificates: the designated certificate authority usually authorizes the certificates. An ability certificate consists of information about the host ID and a set of rules. It is used to authorize the user and give him/her the integrity to access multimedia data.
• Mutual authentication: Users and servers usually authenticate each other through cryptographic methods. In this purpose, the public key scheme can be utilized to authenticate both users and servers to use the video data.

5.3 Watermarking

Basic utilization of watermarks is to identify the origin of a content, to trace illegal copies that are distributed, and also denying unauthorized access to any multimedia content (Health, Monitoring, etc.). In general, attributes and needs for watermarks in video streaming applications are exactly different than other requirements [5]. In order to identify the origin of a video content, it requests the indulgent of an individual watermark into the server content. In order to trace illegal copies, a unique watermark is strongly required depending on the location and ID of the receiver in video applications [5].

5.4 Encryption

Robust encryption is required to secure transmitted data from IoT devices, normally small size data such as key, control commands, push notifications can be fully encrypted within the limited capabilities of IoT devices [8]. Meanwhile, multimedia data inherently contain enormous data transmission [17]. Such data full encryption will overload the processor if it's not capable to handle such complex and heavy process. The trade between processor muscle and the power consumption creates the main challenge of performing full encryption in IoT devices; the more power the more power consumption. This leaves the IoT devices with limited processor power to seek other encryption techniques such as the selective encryption approach [17] [18]. In selective encryption is the amount of data to be encrypted can be minimized to only 5% [17] [19] in most cases using various techniques. The robustness of the later encryption is still facing big questions and is not yet implemented on highly sensitive multimedia stream.

6. Conclusion

In this paper, basic security factors on video streaming over IoT have been presented and explained as it is strongly agreed that the security of video streaming or multimedia over IoT is critical to be fulfilled due to many factors and attributes, so many solutions have been contributed and explained.

Security of video streaming is considered to be a very critical factor as to enable the global spread of IoT methodologies and applications. Users are most likely to adopt with IoT security solutions as a number of security challenges arise. IoT gives the permission to establish a communication between users and devices (things) Anytime, Anywhere, with anything and anyone in multimedia and video streaming. In which it leads to security risks existence while applying IoT, solutions are needed to be conducted in order to overcome the video streaming security issues and deal with the security warnings in such a changing environment of IoT.

The IoT vision gives the opportunity to a lot of users, companies and stakeholders as a global applicability in severing productive specifications such as environment monitoring, home or work, health care, product management security. IoT technologies must cover security and privacy for video streaming in which should take into considerations the architecture design and the solution methodologies. This is predicted to explain the basic requirements for guaranteeing acceptance and reliance by stakeholders and the wide accommodation of the technology security factors. To conclude, privacy and security are considered to play main roles to limit the development of the IoT in which a number of frameworks have been produced to cover privacy and security attributes in designing the system.

Acknowledgments

This research made possible by a financial support from Applied Science Private University in Amman, Jordan to cover the publication fee of this paper.

References

[1] C. Liu and J. Qiu, "Study on a Secure Wireless Data Communication in Internet of Things," International Journal of Computer Science and Network Security (IJCSNS), vol. 15, no. 2, pp. 18-23, 2015.

[2] Gartner, [Online]. Available: http://www.gartner.com/newsroom/id/2636073.

[3] L. Zhou and H. C. Chao, "Multimedia traffic security architecture for the internet of things," IEEE Network, vol. 25, no. 3, pp. 35-40, 2011.

[4] N. Turab, "Internet of Things: A Survey of Existing Architectural Models and their Security Protocols," International Journal of Computer Science and Network Security (IJCSNS), vol. 17, no. 5, 2017.

[5] J. Yang, S. He, Y. Lin and Z. Lv, "Multimedia cloud transmission and storage system based on internet of things," Multimedia Tools and Applications, 2015.

[6] Y. K. Chen, "Challenges and opportunities of internet of things," in 17th Asia and South Pacific Design Automation Conference, Sydney, Australia , Jan 2012.

[7] D. Miorandi, S. Sicari, F. D. Pellegrini and I. Chlamtac, "Internet of things: Vision, applications and research challenges," Ad Hoc Networks, vol. 10, no. 7, pp. 1497 - 1516, 2012.

[8] R. Fisher and G. Hancke, "DTLS for Lightweight Secure Data Streaming in the Internet of Things," in Ninth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, Guangdong, China, 2014.

[9] S. Alvi, B. Afzal, G. Shah, L. Atzori and W. Mahmood, "Internet of multimedia things: Vision and challenges," Ad Hoc Networks, vol. 33, pp. 87 - 111, 2015.

[10] Network Sorcery, "Real Time Transport Protocol (RTP)," [Online]. Available: http://www.networksorcery.com/enp/protocol/rtp.htm.

[11] C. Aggarwal, N. Ashish and A. Sheth, "The Internet of Things: A Survey from the Data-Centric Perspective," in Managing and Mining Sensor Data, Boston, MA, Springer US, 2013, pp. 383-428.

[12] I. Lee and K. Lee, "The Internet of Things (IoT): Applications, investments, and challenges for enterprise," Business Horizons, vol. 58, no. 4, pp. 431-440, 2015.

[13] J. Gubbi, R. Buyya, S. Marusic and M. Palaniswam, "Internet of Things (IoT): A vision, architectural elements, and future directions," Future Generation Computer System, vol. 29, no. 7, pp. 1645-1660, 2013.

[14] A. Balte, A. Kashid and B. Pati, "Security Issues in Internet of Things (IoT): A Survey," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 5, no. 4, pp. 450-455, 2015.

[15] Z. Qin, G. Denker, C. Giannelli, P. Bellavista and N. Venkatasubramanian, "A Software Defined Networking architecture for the Internet-of-Things," in IEEE Network Operations and Management Symposium (NOMS), Krakow, Poland, Jun 2014.

[16] F. Bao and I. Chen, "Trust Management for the internet of Things and its Application to Service composition," in IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM), San Francisco, CA, USA, 2012.

[17] F. Almasalha, R. Hasimoto-Beltran and A. Khokhar, "Partial Encryption of Entropy-Coded Video Compression Using Coupled Chaotic Maps," Entropy, vol. 16, no. 10, pp. 5575-5600, 2014.

[18] A. Khokha, F. Almasalha and N. A. and, "Secure Multimedia Transmission over RTP," in Tenth IEEE International Symposium on Multimedia, Berkeley, CA, USA, 2008.

[19] S. Khanvilkar and A. Khokhar, "Efficient transmission of MP3 streams over VPNs," in IEEE Global Telecommunications Conference (GLOBECOM), San Francisco, CA, 2006.

[20] H. Y. Yang, K. H. Lee and S. H. Lee, "Method and apparatus for partially encrypting speech packets". USA Patent US20090041231 A1, February 2009.

Mina A. Hamoudy is an MSc student at the Faculty of Information Technology at Applied Science Private University in Amman, Jordan. Mina received her BSc degree in computer science from Applied Science Private University in 2015.

Mahmoud H. Qutqut is an Assistant Professor at the Faculty of Information Technology at Applied Science Private University in Amman, Jordan; since October 2014. He received his Ph.D. degree from the School of Computing at Queen's University in Canada 2014, under the supervision of Prof. Hossam Hassanein. He received his MSc degree in Telecom Systems from DePaul University at Chicago, Illinois in 2007 and BSc degree in computer systems from Applied Science University in 2015. He has served as a TPC co-chair and a technical program committee member for several IEEE international conferences. His research interests include mobile heterogeneous small cells networks, Internet of Things (IoTs) enabling technologies, and smart cities enabling services.

Fadi Almasalha is an Associate Professor at the Faculty of Information Technology at Applied Science Private University in Amman, Jordan; received his M.S. in computer Science from New York Institute of Technology, in 2005 and Ph.D. in Computer Science from University of Illinois at Chicago, in 2011. In fall of 2011, he joined the Department of Computer Science at the Applied Science University. Dr. Fadi Almasalha received his Associate rank on 2016, during his appointment as the head of computer science department. Dr. Fadi has published more than 10 technical papers, journals and book chapters in refereed conferences and journals in the areas of multimedia systems, data mining, and cryptography.