Imperial Journal of Interdisciplinary Research (IJIR)
Vol-3, Issue-2, 2017
ISSN: 2454-1362, http://www.onlinejournal.in

Selective Encryption Control Model for Multimedia Big Data with Resource Constraints

Mr. Arshad Inamdar[1] & Prof. Vaidya M. B.[2]
[1]Student, ME Computer, AVCOE, Department Of Computer Engineering, Sangamner[1]
[2]Assistant Professor, AVCOE, Department Of Computer Engineering, Sangamner[2]

***Abstract**: The multimedia big data in multimedia sensing and other IoT (Internet of Things) systems are high-volume, real-time, dynamic and heterogeneous. These characteristics lead to new challenges of data security. When computation and power resources in some IoT nodes are very scarce, these challenges become more serious that complex data security process on multimedia data is restricted by the aforementioned limited resources. Hence, the confidentiality of multimedia big data under resources constraints is investigated in this paper. Firstly, the growth trend of data volume compared with computational resources is discussed, and an analysis model for multimedia data encryption optimization is proposed. Secondly, a general-purpose lightweight speed tunable video encryption scheme is introduced. Thirdly, a series of intelligent selective encryption control models are proposed. Fourthly, the performance of proposed schemes is evaluated by experimental analyses and proves that schemes are effective enough to support real-time encryption of multimedia big data.*

1. Introduction

Nowadays, multimedia is considered as a biggest big data as it dominates the traffic in the internet and mobile phones. Multimedia big data generated by IoT system have some special characteristics, such like high volume, real time, dynamicity, heterogeneity. In addition, other characteristics like individual privacy should also be considered in the big data age. Therefore, excepting the traditional security problems in distributed system, the particular characteristics of the multimedia big data have brought in some new security problems like individual privacy protection, processing of multimedia big data, and etc. Especially, as for large-scale multimedia collaborative work, video conference, intelligent video surveillance system and other multi-stream multimedia sensing system, which are important categories of IoT applications, security of the hundreds of streams with high data volume becomes a new challenge. The nodes in those systems, which process large amounts of media data, might become the bottlenecks. Moreover, as to mobile, unplugged sensing devices, their limited computation and energy resources further restrict the protection of data security, because the computational complexities of encryption and decryption operation are very high. Because of the special characteristics of unplugged devices in IoT, data processing with limited resources has attracted researchers' attention, and there are some researches on it. In the meantime, the impact of limited resources on IoT security has also been considered by scholars. How to achieve data confidentiality under tight resources constraints has become an important topic nowadays. In IETF's draft of "Security Considerations in the IP-based IoT", the "tight resources constraints" is believed to be the first challenge of IoT security. And some other researches pointed out that complex security process should not be used, and energy-efficiency schemes should be considered to achieve a balance between performance and security. Therefore, such system is able to secure the multimedia big data over real time attacks.

Resources Constraints with their Variation Trends in Video Sensing System:
A. Application scenario and its resources constraints
B. The non-convergence of discrepancy between data volume and limited resources
C. The Growth Rate of Data Volume Compared with Computational Resources
D. Intelligent Optimization Model for Data Encoding under Resources Constraints

2. Related Work

L. Atzori and A. Iera define recent improvements in sensor technology and network technology, especially the wireless network technology, the IoT applications are widely deployed [3]. Meanwhile, escalating data volume and the rapid adoption technology inherits its security problems naturally. So the security issues of the big data in IoT become a central concern which may hamper the development of IoT technology, and it has attracted widespread attentions.

T. Heer, O. Garcia present large-scale multimedia collaborative work, video conference, intelligent video surveillance system and other multi-stream multimedia sensing system, which are important categories of IoT applications, security of the hundreds of streams with high data volume becomes a new challenge [4]. The nodes in those systems, which process large amounts of media data, might become the bottlenecks. Moreover, as to mobile, unplugged sensing devices, their limited computation and energy resources further restrict the protection of data security, because the computational complexities of encryption and decryption operation are How to achieve data confidentiality under tight resources constraints has become an important topic nowadays. In IETF's draft of "Security Considerations in the IP-based IoT", the "tight resources constraints" is believed to be the first challenge of IoT security.

L. Qiao and K. Nahrstedt [5] present multimedia encoding, the Huffman coding and other coding processes remove the redundant information from the original media data, statistical characteristic of compressed multimedia stream is different from that of text data dramatically. Statistical analysis shows that coded multimedia data have high randomness at the byte level.

J. Li, X. Huang, J. Li, X present processing ability of encryption is highly correlated with the growth of the CPU speed. According to Moore's Law, the performance of computer would double every 18 months, or grows about 60 percent a year. Secondly, the disk densities increase 100 percent per year, which is faster than the increasing of CPU according to the Moore's Law. Moreover, a lot of scholars point out that the image process ability and bandwidth of core network grows even faster than disk capacity. In addition, the computation and encryption capabilities of battery-powered equipments are also constrained by battery capacity, which grows even slower and makes the resource constrained problem trickier

The authors of [7] formulated the network resource allocation problem as a cross-layer decision of transmission strategies across the APP, MAC and PHY layers of a traditional network protocol stack to maximize multimedia quality with rate and delay constraints. In [8], the authors modeled the communication network as a generalized utility maximization problem to provide a systematic optimization method by analysis of layered decomposition, where each layer corresponds to a decomposed sub problem and the interfaces among layers are quantified as functions of the optimization variables coordinating the sub problems. Those efforts are, however, mainly focused on the architectural decisions in networking, not tuning the system parameters for energy-quality-security gain.

The author of [9] presented a quality-driven security design and resource allocation framework for wireless sensor networks with multimedia selective encryption and stream authentication schemes proposed at the application layer and network resource allocation schemes at low layers. In particular, an unequal (partial) error protection-based network resource allocation scheme is proposed by jointly designing selective multimedia encryption and multimedia stream authentication with communication resource allocation. Their cross layer resource management framework for secure multimedia streaming solves a global optimization problem requiring full awareness of the system dynamics while our compositional approach leads to acceptable solution quality at low complexity. Also, the composition can be fully distributed and capable of utilizing different even conflicting local objectives through the generic interface of constraint language.

3. Body of Work

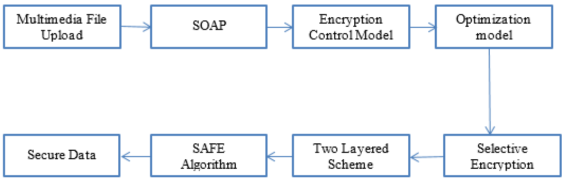

Figure 1. System Flow

When candidate encryption schemes are narrowed to En and E0, based on the weight vi and bandwidth bi of each stream, either encrypt or not for each stream would be determined by the optimization model. After that, as to the bottleneck nodes we concerned, the bandwidths of data will no longer overwhelm their encryption throughputs in most cases. But there are still some problems:

1. When there are several big important streams at a time, the bottlenecks might continue to exist.
2. For those streams not been encrypted, sensitive media information will vulnerable.
3. As to mobile and unplugged devices, limited computation and energy resources still restrict complex security operation. At this time, a better scheme is to select appropriate algorithms with different security levels and different complexities or with tunable security level (e.g. SAFE). Then the streams should been divided into several groups with different levels of value-weight ratios. At last different algorithms would be used to encrypt different groups. However, this scheme is too complex to be calculated automatically.

A compromised scheme is building a layered model with few algorithms and groups. In this subsection two layered scheme is proposed. In this subsection, two layered scheme is proposed, in which three candidate algorithms could be used. The first one is full encryption En; the second one is ESAFE; and third one is unencrypted or some very low encryption rate algorithm (EVLERA), like simple permutation in packet header, whose encryption rate can be ignored. Let CSAFE and CEn be the throughput of En, and ESAFE in the central unit. When, streams with higher value-weight ratio are selected and encrypted by SAFE, and let the other streams encrypted by VLERA. Correspondingly, when full encryption and SAFE are used, all the data should protected by ESAFE firstly. Then the rest resources should be allocated to selected important data by replace ESAFE with traditional encryption algorithm

Selective encryption control model for multistream multimedia system:

1. General Selective Encryption Control Model
2. Simplified single Layer Selective Encryption Control model
3. SAFE based Two Layer Selective Encryption Control model.

4. Proposed Algorithm

Algorithm: Continuous data stream oriented encoding scheme:

```
Procedure SAFE1
Begin:      //process the data by packet
Repeat
1. Use FE to encrypt the current first packet (as Packeti) in buffer
2. For j:=1 to l do let the following l packet's CipherPckt i+j= Pckt i+j-1□Pckt i+j.
Until get the last packet in buffer
End Procedure
```

Algorithm: Packet oriented encoding scheme:

```
Procedure SAFE2
Begin:      //process the data by packet
Repeat
1. Use FE to encrypt the current first packet as Packeti  in buffer.
2. For j:=1 to l do let the next l packet's CipherPckt i+j=Pckt i□Pckt i+j..
Until get the last packet
End Procedure
```

5. Conclusion

Our propose technique provides data security using data encryption in Multimedia Big Data in cloud environment. For maintaining the security of multimedia big data in multimedia sensing and other Internet of Things, our system is work. In this paper, first analyse the various resource constraints in multimedia sensing system, and it is found that which problems of resources constraints will be arrive. After that for data encryption for under resources constraints an optimization model is proposed. Then, to reduce the computation overload on weak nodes and to achieve a balance between performance and security, a general-purpose lightweight speed adjustable video encryption scheme is defined. Our system present a series of selective encryption control models, in which the improved model is built based on SAFE encryption scheme. Finally, our system shows an experimental analyses that the performances of the presented schemes are effective enough to support real-time applications.

6. Acknowledgement

I express my sincere thanks to my project guide Prof. M. B. Vaidya who always being with presence & constant, constructive criticism to made this paper. I would also like to thank all the staff of Computer Department for their valuable guidance, suggestion and support through the paper work, who has given co-operation for the project with personal attention. Above all I express our deepest gratitude to all of them for their kind-hearted support which helped us a lot during paper work. At the last I thankful to my friends, colleagues for the inspirational help provided to me through a paper work.

7. References

[1]. Minyoung Kim, Mark-Oliver Stehr, Ashish Gehani, and Carolyn Talcott, “Ensuring Security and Availability through Model-based Cross-Layer Adaptation”, SRI International mkim, 2016.

[2]. S. Mohapatra, N. Dutt, A. Nicolau, and N. Venkatasubramanian, “DYNAMO: A cross-layer framework for end-to-end QoS and energy optimization in mobile handheld devices,” IEEE Journal on Selected Areas in Communications, vol. 25, no. 4, pp. 722–737, 2007.

[3]. L. Atzori and A. Iera, "The internet of things: A survey. Computer Networks",2010, 54(15), pp. 2787-2805.

[4]. T. Heer, O. Garcia-Morchon, R. Hummen, S.L. Keoh, S.S. Kumar and K. Wehrle, ”Security Challenges in the IP-based Internet of Things,” Wireless Personal Communications, 2011. 61(3), pp. 527-542.

[5]. L. Qiao and K. Nahrstedt, ”A new algorithm for MPEG video encryption,” In Proceeding of the First International Conference on Imaging Science, Systems and Technology (CISST"97). Las Vegas:. Nevada, July 1997.

[6]. J. Li, X. Huang, J. Li, X. Chen and Y. Xiang, ”Securely Outsourcing Attribute-based Encryption with Checkability,” in Proc. IEEE Transactions on Parallel and Distributed Systems, 2013.

[7]. M. V. D. Schaar and S. Shankar, “Cross-layer wireless multimedia transmission: challenges, principles, and new paradigms,” IEEE Wireless Communications, vol. 12, pp. 50–58, 2005.

[8]. M. Chiang, S. H. Low, A. R. Calderbank, and J. C. Doyle, “Layering as optimization decomposition: a mathematical theory of network architectures,” in Proceedings of the IEEE, vol. 95, no. 1, Jan. 2007, pp. 255–312.

[9]. W. Wang, “Quality-driven cross layer design for multimedia security over resource constrained wireless sensor networks,” University of Nebraska, Lincoln, Dept. of Computer and Electronics Engineering, Ph.D. Dissertation, 2009.

[10]. H. Ning and H. Liu, “Cyber-Physical-Social Based Security Architecture for Future Internet of Things,” Advanced in Internet of Things, 2012.

[11]. Q. Jing, A.V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: perspectives and challenges," Wireless Networks, 2014.