ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 6, Issue 1, January 2017

Compression and Encryption approach for Data Security in Mobile Internet of Things

Rafidha Rehiman K A
Research Scholar
Department of Computer Science
Karpagam Academy of Higher Education
Coimbatore.

Dr. S Veni
Associate Professor & Head,
Department of Computer Science
Karpagam Academy of Higher Education
Coimbatore.

***Abstract*—Today's fastest growing mobile communication allows the interconnected objects to communicate with each other in a short period of time and we can see huge explosions in digital transmissions. This involves a lot of security issues and bandwidth utilization problems in the network. Existing protocols and mechanisms are not sufficient for data confidentiality and efficient bandwidth utilization. Hence we propose a combined scheme of compression and encryption for data protection in wireless enabled Internet of Things (IoT) environment. With this, it is to be possible to offer adequate security for data in wireless sensor network with low bandwidth, which is used for reducing the traffic. The methodology incorporates the application of Public Key cryptography in mobile network for enhancing security.**

Keywords—Internet of Things; Securty; Privacy; Compression;

I. INTRODUCTION

Security and Privacy of data is a major consensus for wireless sensor network. Now, message encryption in wireless environment is enabled by WEP RC4 and WPA as a part of IEEE wireless Ethernet standard. An IEEE wireless standard use Advanced Encryption Standard (AES) on the link layer and is operated with specialized hardware to protect the data while in transit, which is totally independent of network protocols. This mechanism does not support host authentication and key management.

However these methods are vulnerable and enough free software tools are available in the cyber world to crack the security measures implemented.[1][2] Moreover it is very difficult to implement algorithms in memory and battery constrained sensor nodes and distribute cryptographic keys between the nodes in a network. Also a standard way of implementing security services for an IoT mobile environment is currently non-existent and the matter requires to be addressed by the research world.

II. RELATED WORKS

With the advancement in technology, everyone trust wireless sensor networks and IoT enabled mobile devices in their day to day activities. So to provide security and enable privacy for mobile data, we require some sort of encryption. At the same time, to protect the bandwidth, means of compression mechanism is also needed.[3]

Over the last few years, various researchers had studied the effectiveness of private key cryptosystems in this area and have written on its various aspects. By encrypting data in mobile environment, there is an increase in the size of the data and it leads to the wastage of bandwidth.

In " A Secure approach for SMS in GSM networks", Neetesh Saxena et al compared different modern block cipher algorithms including DES, 3DES, AES, Blowfish and proposed a combined block cipher encryption and digital signature for securing text against attacks. The work proposes AES as the best candidate but only protect the text while it is in transit.[4]

Johnny Li – Chang Lo also point out the importance of encryption for protecting the data and at the same time found a drawback as this increased the size of the cipher text [5].

Tarek M Mahmoud et al proposed a compressed encryption and compression method for securing short

message service in mobile environment. For securing the text, they used RSA cryptosystem and this also increased the size of the text. [6]

Most of the private data exchange in wireless networks are based on private key cryptosystems and are larger when compared with public key systems when the performance was evaluated on the basis of overhead and computational complexity [7][8].

Most studies in research world combine compression and encryption to improve security and hence, confidentiality of data. We analyzed more recent studies in literature which combined compression and encryption.

Lavisha Sharma and Anuj Gupta used steganography, compression and encryption together on image data to ensure high security in network communication [9]. Alka P Sawlikar et al in "A new approach of Compression and Encryption algorithm" optimized the size of data in network which offered more security to data. This combined scheme offers better performance based on compression ratio, delay and the speed of compression.[10]

In 2014, Swapanil Sonawane presented a scheme of compressed chatting over internet. They studied text messages and images based on compression ratio and observed Huffman encoding and LZW as promising for encoding [11].

In SMS text compression and encryption on android OS, Manoj Patil et al proposed a secure transmission and bandwidth utilization mechanism for SMS messages and implemented this for mobile operating system, Android.[12]. Dr. Nikos Zervas used data compression for low energy IoT connectivity to minimize the energy use for data exchange over wireless network [13].

III. PROPOSED ALGORITHM

Internet of Things has its root in a huge variety of applications and is operated in a heterogeneous environment. Protecting our data, which include our valid credentials, smart card details and everything that needs to be safe and valid is crucial in IoT. Plenty of research works highlight the importance of security and privacy of user data in IoT environment. Users' valuable information is passed through various networks and so today's networks demand reduction in time and space to support resource constrained and connected devices with security.

With this in mind, we designed a secure planning and combining encryption and compression on IoT data, imposing Confidentiality, Integrity, Reliability, Authenticity and Availability. At the same time there exists a need to address the nonfunctional requirements like, light weight solution for constrained devices which should be scalable to the billions of devices that are connected.

A. Data Management in IoT

Everything including physical and mental status of user is locatable using the sensors in IoT. Also IoT share the status of things with the other devices that are connected together and guarantee anywhere, anytime computing and thus need the proper security measures for data protection. IoT devices are distributed in a manner which connects heterogeneous technology like embedded devices and communication links and are thus vulnerable in nature. So it requires strong encryption strategies.

In IoT things are connected and constantly exchange all types of information. IoT uses machine to machine (M2M) computing for data exchange and many factors and technologies are involved in data management. Data Collection and Analysis is a part of core layer of IoT and manages Data Storages, On demand Data Access, and Data Filtering and provide structures to support multiple users and organization. So we require an increase in the level of data protection and security from the devices with sensors and actuators to the data stored platforms.[14][15]

Information collected by the sensor enabled IoT devices are from physical world, which need to describe these observations, associate it to existing concepts and make those available to different applications. The semantic annotations which is performed on the physical descriptions collected is used by the other connected devices. Data acquired and processed according to an application and aggregated is then perceived as reading of a single server.

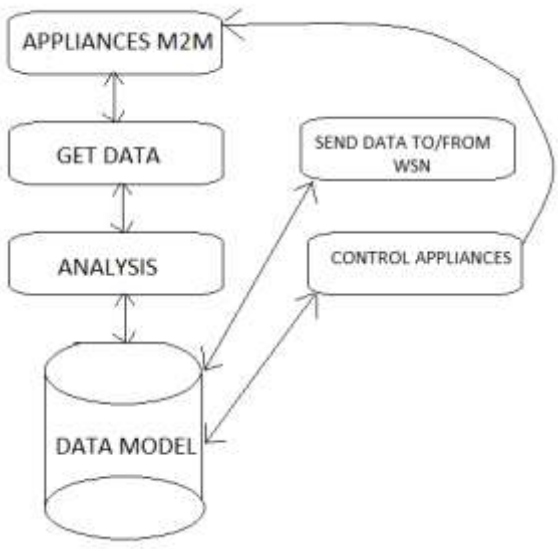

Figure 1 : Data Processing in IoT

For avoiding unauthorized reading, we normally trust on cryptographic encryption schemes. Initially IoT trusts private key systems to establish security. But in IoT , the data is aggregated by a node in wireless sensor network and the aggregating node perform some computations on the data and so there is no direct link between the source of data and the sink. To achieve confidentiality we need to provide a mechanism to aggregate encrypted data or it is required to use some holomorphic encryption mechanisms.

Heterogeneous infrastructures of IoT require an Optimal and Adequate security mechanism. Data Availability in this infrastructure allows intruders to track the profile and location without the subject's consent. While considering heterogeneity and multiplicity, the data model of IoT has to accommodate high rates of sensor data and conduct analysis on it. There are two dominant architectures for data exchange in IoT called decentralized bus based approach and centralized broker based approach.

Today various encryption and authentication technologies are applied to the data to ensure security. One aspect of security to safeguard machine to machine data is by applying encryption over existing Transport Layer and IP Security. Light weight solutions for M2M data protection are available in literature, but we need to identify a secure way to exchange the key and thereby, we are totally dependent on the security of key exchange. Also there is little or no solution in IoT to compress the data to save the bandwidth in today's heavy traffic network.[17][18]

Lossless data compression is a mathematical procedure by which we can reduce the size of data without compromising the quality of content. [19] One of the encoding algorithms in information theory for providing lossless compression is Huffman encoding which generates a compressed sequence on O (nlogn) [16]. Huffman encoding accepts variable length of messages as input and produces small sized code for efficient utilization of storage in repository and bandwidth while in transit [10], enhance the strength of cryptosystem [9].

Majority of standards utilize RSA for ensuring confidentiality and authentication, and bit length of RSA is increased with its increasing processing power [19]. Here we adopt Elliptic Curve Cryptography (ECC) which is smaller in size and computation and offers similar security as RSA, but results in faster computations [9]. A 160 bit ECC key provides similar security as 1024 bit RSA key. ECC is suitable for wireless IoT environment, constrained devices like pagers, cellphones PDAs etc. and reduce the transmission requirements.

B. Algorithms and Block Diagrams

Encryption Algorithm

Step 1: Read the message

Step 2: Convert the message to ASCII equivalent.

Step 3: Convert each ASCII value to 7 bit binary number.

Step 4: Perform multiplication modulo 7 on each binary representation of character with column matrix, successively set different x co –ordinate values.

Step 5: Choose an elliptic curve and generate public key and private key pair.

Step 6: Substitute each x value in the elliptic curve to obtain corresponding y value.

Step 7: Convert the message to cipher text

Step 8: Apply Lossless Huffman encoding operation on the Cipher text

Step 9: Send out the encoded text with public key for decryption.

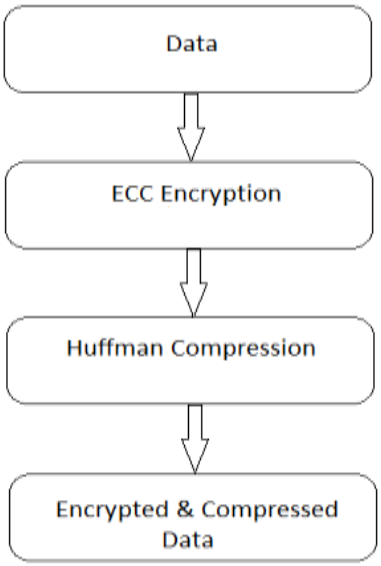

Figure 2 : Sender side procedure

Decryption Algorithm

Step 1: Perform Huffman decoding after receiving the encoded text and public key for decryption

Step 2: Apply ECC Decryption on decoded value with the received public key.

Step 3: Convert points to binary, then to ACII and to corresponding characters.

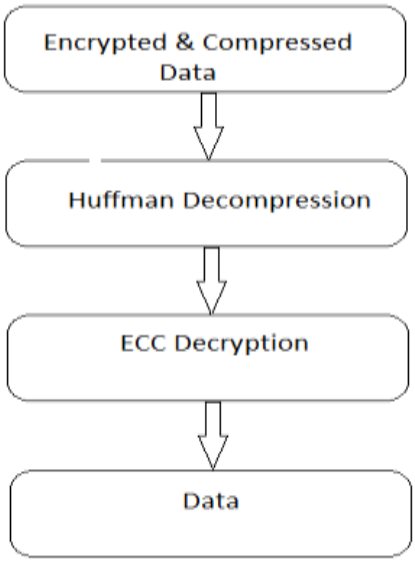

Figure 3 : Receiver side procedure.

IV. CONCLUSION

Compressed encryption scheme on data in an IoT environment reduces the size of the encrypted content. The application of ECC public key system is proposed to ensure confidentiality for data in IoT. ECC helps to reduce computation and offers adequate security. This combined scheme is suitable for wireless devices with constrained resources and can effectively utilize the available bandwidth in the network with high security.

References

[1] Boot strapping Security , Authentication and Data Integrity in IoT, ERICSSON White Paper, 2016.[f]

[2] Rafidha Rehiman KA, Veni S. "Security, privacy and trust for smart mobile devices in internet of things – A literature study. IJARCET. 2015 May; 4(5):1775-9.

[3] Manoj Patil and Vinay Sahu, " A Survey of Compression and Encryption technique for SMS", International Journal of Advancements in Research & Technology, vol 2, issue 5, 2013

[4] Neetesh Saxena et al, "A secure approach for SMS in GSM network", ACM 2012.

[5] Johnny Li Chang Lo, Judith Bishop, JHP Eloff, "SMS security an end to end protocol for secure SMS", Elsevier.

[6] Tarek M Mahmoude et al , "Hybrid Compression Encryption technique for SMS", IJCS.

[7] Anitha Singhhrova, Nupur Prakash, "Performance analysis of mobile security protocols", IJS 2006.

[8] Jung San Lee Ya Fen Chang, Chin Chen Chang, "Secure Authentication protocols for mobile commerce transactions", 2008.

[9] Lavisha Sharma, Anuj Gupta, " Image Encryption using Huffman coding for Steganography, Elliptic Curve Cryptography and DWT for Compression", International Journal of Advance Research, Ideas and Innovations in Technology, Vol 2 , Issue 5, 2016, p.1-10.

[10] Alka P Sawlikar, Dr.Z J Khan, Dr.S G Akojwar, " A new approach of Compression and Encryption algorithm", International Journal of Advanced Research in Computer Science and Software Engineering, Vol 6, Issue4, 2016, p.394-397.

[11] Swapanil Sonawane and Dilip Motwani, "Compressed Chatting over Internet", International Journal of Computer Applications(0975 - 8887), vol 106, No.7, 2014, p.1-5

[12] Manoj Patil et al, "SMS Text Compression an Encryption on Android OS", International Conference on Computer Communication and Informatics(ICCCVI - 2014), IEEE.

[13] Dr.Nikos Zervas , CAST INC, "Data Compression for low energy IoT Connectivity", White paper, 2015.

[14] OvidiuVermesan, Peter Friess, "Internet of Things – From research and Innovations to Market Deployment", River Publishers, 2015

[15] Scott R Peppet, "Regulating the Internet of Things: First step towards managing descrimination, Privacy , Security and Consent, Texas law reviews, 2014.

[16] O. Srinivasa Rao, S.Pallam Setty, " Huffman Compression technique in the context of ECC for enhancing the security and effective utilization of channel bandwidth for images", International Journal of Science and Advanced Technology, Vol I, No 8, 2011, p.13-23.

[17] Sudipta Sahana, Madhusree Majumdar, Shiladitya Bose, Anay Ghoshal, " Security enhancement approach for data transfer using Elliptic Curve Cryptography and Steganography", International Journal of Advanced research in Computer and Communication engineering, Vol.4 Issue 4 , April 2015, p.495-499.

[18] O. Srinivasa Rao, S.Pallam Setty," Comparative study of Arithmetic and Huffman data compression techniques for Koblitz curve cryptography", International Journal of Computer Applications(0975 – 8887), Vol 14- No.5, January 2011, p.45 – 49.

[19] Manoj Patil and Vinay Sahu, " A Survey of Compression and Encryption technique for SMS", International Journal of Advancements in Research & Technology, vol 2, issue 5, 2013