International Journal of Pure and Applied Mathematics
Volume 119 No. 12 2018, 13991-13997
ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

ijpam.eu

Evaluating Efficiency of HMAC and Digital Signatures to Enhance Security in IoT

K V V N L Sai Kiran
Dept of Computer Science and Engineering
Amrita School of Engineering, Coimbatore.
Amrita Vishwa Vidyapeetham, India
CB.EN.U4CSE15328@cb.students.amrita.edu

Harini N
Dept of Computer Science and Engineering
Amrita School of Engineering, Coimbatore.
Amrita Vishwa Vidyapeetham, India
n_harini@cb.amrita.edu

Abstract:
It is possible that a few IoT devices may operate continuously unattended which can become the interest of cyber criminals in terms of discovering vulnerabilities in these devices and use them to launch different forms of attacks in the networks. A number of cryptographic primitives are available as per literature to minimize the risk levels but adoption of a scheme need to be based on different factors like convenience, the threat model associated with the environment and the applicability of the scheme with the given constraints on the device. This demands clear experimentation for assessing the suitability of signing and encryption algorithm for IoT. The paper aims at setting up a controlled test bed for experimenting
Various combinations of the cryptographic schemes and identify the best in terms of minimising time related overheads.
Keywords —**IoT, Digital Signature, Encryption, Hash algorithms,MD5,SHA,HMAC,MQT.**

I. INTRODUCTION

The explosion in the growth of Internet technologies has led to the advent of IoT. IoT refers to a virtual platform where billions of entities (People, Devices, Objects etc..) are connected for communication. The challenge associated with IoT is multi-fold like ensuring availability, reliability, privacy etc.It is necessary to provide safeguarded connection between the devices andin the network. Literature specifies technologies including encryption mechanism,signing mechanisms have been widely adopted to improve security and privacy. However,neither of the existing standard measures can be adopted as it is or in its original form in the IoT domain.The reason behind resource constrained environment associated with inthe devices in the platform. This Paper attempts to address the security concerns in this network with the aim of analysing the suitability of standard cryptographic schemes with standard key sizes to secure connections between the participating entities with a scheme particularly suitable for IoT environment. It is expected to have around 50 billion devices by 2020 in this network.
A wide variety protocols for conduct of data transmission like MQTT (Message Queuing Telemetry Transport), Constrained Application Protocol (COAP), Advanced Message Queuing Protocol(AMQP), Hypertext Transfer Protocol (HTTP)are in use. Of these MQTT is considered to be lightweight communication protocol between the entities connected for its property to operate on low bandwidth and high latency data links. A controlled environment using 3 entities namelyPublisher, Subscriber and Broker. It is used to study the performance of cryptographic primitives in the environment. It is worth mentioning that any number of publishers, subscribers can participateand allow entities to communicate with each other. The prime role of the broker entity is to help establishing a communication link to handle data transmissions between subscribers and publishers.

It is reported in literature that IoT platform because of the lack of poor authentication, confidentiality, and minimum security provided by the manufacturer at hardware as well as software level is vulnerable to many forms of attacks like Dos, man in the middle etc... This enables unauthorized access to outsiders to work and take control on the device.The lack of confidentiality service facilitates intruders to sniff payloads and perform data modification attacks. At the hardware level, the device,usually devices are fitted with secure key storage to reduce the chance of attacks. At the software level either the payload or streams are to be encrypted and frequent authentication handshakes are to be performed by the

participating entities. It is important for upcoming standards /schemes to address the shortcomings of prevailing security mechanisms in IoT and offer resistance against common forms of attacks likes Eaves dropping, routing attacks, Distributed Denial of Service.

The rest of the paper isorganised as follows:
Section 2presents undertaken work by the research communities on securing IOT platforms. Section 3 presents the setup of the test bed used to study the impact of the selective integrity and confidentiality procedures in terms of their suitability of implementations in a given environment.As section 4 presents the results of the experimentations and related discussions. Section 5 finally presents the conclusions.
This focus of this paper is to understand the applicating of Hash-based Message Authentication Code(HMAC) and digital signature schemes in the communication in IoT networks.

II. RELATED WORK

A. Internet of Things(IoT)

Future of the Internet is driven by an omnipresent network of interconnected entities (Devices, People, Object etc.) called Internet of Things and sometimes referred as Internet of Everything(IoE). The prime work of these entities is to gather, transmit and work on the data acquired from other devices or from the environment. The rapid changes in this environment due to more heterogenous device types been added to this network and the very nature of these devices in terms of possession of limited resources and being based on lightweight protocols makes this platform open for cyber criminals to perform different forms of attacks .addressing this issue immediately is difficult due to the complex structure and interaction model that prevails .The security schemes designed for internet cannot be directly applied to this environment which makes the situation more challenging. This brings out a clear need for analysing the existing schemes and validate /understand their usage in IoT.

B. Hash Family (Hashing algorithms)

Hash algorithms are widespread and they are employed in various cryptographic schemes and in security protocols to provide integrity of transmitted data. It offers the receiver a confidence that the received data is not been altered by A sniffer, eaves dropper or by any other means. SHA and MD5 family of algorithms are standard algorithms to assure data integrity.

The input to the Secure Hash Algorithm-1 (SHA-1) produces a 160 bit-fixed length hash value and the output is fixed length hash value which is generally referred toas Message Digest. Secure Hash Algorithm (SHA-2) has two novel hash variants SHA-256 and SHA-512 which compute 32 Bytes and 64 Bytes as Message Digest respectively and SHA-2 has two major components and they are Compression function and Message schedule. Apart, from SHA family MD5 algorithm also provides integrity by resulting a 128-bit hash value. The sender computes the hash value of the message, concatenates them and transmits in the network.The receiver recalculates the hash value from the message and compares it with the hash value present along with the data to ensure integrity. The subsections 1& 2 briefs the procedures involved in SHA1 and MD5.

1) MD 5:

Steps involved in MD5 hashing are as follows

- Affix the padded bits to the message, and is paddedin such a way that it's length is congruent to 448 mod 512 with digit 1 followed by 0 's.
- Affix the actual length of the message to the padded message makes it a chunk of 512 bits.
- Four blocks with size of each block as 32 bits is used to calculate the digest and is initialized with 0x0123456789abcdefedcba9876543210.
- Process the entire message in blocks with the auxiliary functions,$F(X,Y,Z) = (X \wedge Y) \vee (\neg X \wedge Z)$, $G(X,Y,Z) = (X \wedge Z) \vee (Y \wedge \neg Z)$,

$H(X, Y, Z) = X \oplus Y \oplus Z$, $I(X, Y, Z) = Y \oplus (X \vee \neg Z)$

The final message digest iscreated by concatenation of the blocks.

2) SHA 2:

SHA 256 and SHA 512 have a message block of 512 and 1024 bits respectively, which are represented as a sequence of sixteen 32 and 64-bit words respectively, the discrepancy between the two variants is more and steps involved are

- Affix the padded bits to the message and append its length at the end such that it's multiple of its block size.
- Initialization of hash variables is done using with predefined round constants
- The message in chunks of 512 and 1024 bits are taken as initial input and first 16 words are extended to 48 or 64 words.
- Compression utility is applied to compress the hash value obtained using initial working variables.
- Concatenation of the compressed chunk and hash values is performed to obtain Message Digest

C. Digital Signature Schemes

Digital Signature Schemes are used to verify the identity of claimant or a peer who seeks a service. These are generally considered as substitutes forhandwritten signatures in electronic communication possessing a one-to-one mapping between the message and the created signature. Digital Signature algorithms are based on public key cryptography

where each user an expected to hold akey pair (public key&private key)for a process of signing and verifying an electronic document /message. This signing is usually performed with signer's private key and the verification is performedwith corresponding public key Although attacks like existential selective forgeries and total break related to digital signatures are discussed in literature.These could be overcome with the proper choice of domain parameters during key establishment. The strength of RSA and DSA, ECDSA relies on the of prime factorization and discrete log problem (DLP) respectively

1) RSA:
It is highly reliable and safe algorithm and used in vital protocols like Secure Socket Layer(SSL), Pretty Good Privacy(PGP), Secure Shell(SSH). Steps involved in the process:

- *Prime Selection:*

Identify two large primes p and q and form their product(N). p and q are selected as they are in same order.
N=p*q

- *Key Generation:*

Compute φ(N)=(p-1)*(q-1) and select a number 'e' such that GCD(e , φ(N)) = 1 , key pair (e , N) is called public key pair and compute d such that e*d=1 (mod N) from $d = e^{-1} mod\ \varphi(N)$. And d is said to be private key.

- *Signing:*

Let the message (or message digest) be'm'(where m < N) and compute the sign such that $S = m^d\ mod\ N$and the signature is sent along with the message.

- *Verification:*

The receiver computes $S' = S^e\ mod\ N$and compares it with the message (or message digest) and accept if and only if they are same else the received message is rejected

2)DSA:
It is an ingenious and simplified version of ELGamal Signature scheme based on PKI.

- *Key Generation:*

Choose primes p and q such that q*t =(p-1)where t is an integer i.e q is multiple of (p-1). Select primitive element g such that $g^q\ mod\ p = 1\ mod\ p$ and select a random a such and compute $\beta = g^a\ mod\ p$ and the pair (p, q, g, β) are called public key and (a) is called private key.

- *Signing:*

Select k such that 0< k<q and compute $r = (g^k\ mod\ p) mod\ q$, $S = k^{-1}(m + ar) mod\ q$ and pair (r, S) is sent as signature.

- *Verification:*

On receiving (r, S) ,compute $W = S^{-1}\ mod\ q$ and $U_1 = W * m\ mod\ q$and $U_2 = r * W\ mod\ q$ and
$V = (g^{U_1} * g^{U_1}\ mod\ p) mod\ q$
Then the receiver accepts if and only if V== r

TABLE 1: TABLE OF NOTATIONS- SYSTEM PARAMETERS

Variables	Particulars
p, q	Prime numbers
N	p * q
m	Message
h(m)	Hash of message or Message digest
t	integer
e	Selected Public key in RSA
d	Obtained private key from public key in RSA
S	Signature in RSA
g	Primitive element in Z_p
(p, q, g, β)	Public key in DSA
k	ephemeral key
(r, S)	Signature in DSA
G	Generate element
W,U_1, U_2,V	Signature components and intermediate signature values
a	private key in DSA

III. SUMMARY OF FINDINGS

IOT is Now gaining the focus of research community to secure this emerging domain, one need to deeply analyse the security architectures, features and requirements that are suitable for this environment.
This new emerging platform and the varied properties and entities demand a clear need to inspect the applicability of the existing security schemes in this network. With the aim of understanding the challenges that are present in the existing cryptographic mechanisms in terms of their suitability to protect the sensor data and communicating the entity closed, controlled environment was setup for studying the effect of these primitives.

IV. PROPOSED SYSTEM

Three standard algorithms namely HMAC,DSA,RSA are picked up for experiment with varied key sizes and different IOT devices
Fig (1epicts the procedure that uses keyed hash function(HMAC) using a symmetric key secret for creation of encrypted messages.

Fig 2: depicts the procedure that used by Digital signature (DSS)algorithm uses public key secret to create an authentic message with guarantee of non-forgeability, non-repudiation etc...

Fig 3: depicts the procedure that used by Digital signature (RSA)algorithm uses public key secret to create an authentic message with guarantee of non-forgeability, non-repudiation etc…

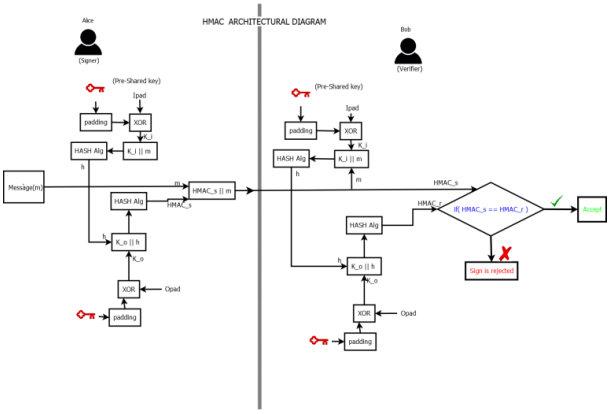
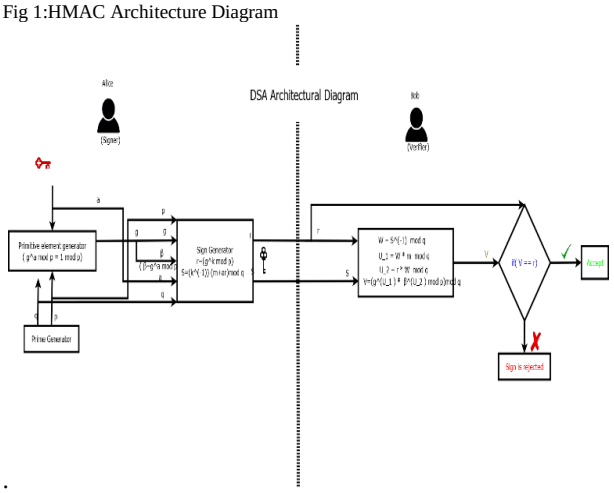


Fig 1:HMAC Architecture Diagram



.

Fig 2:DSA ArchitectureDiagram

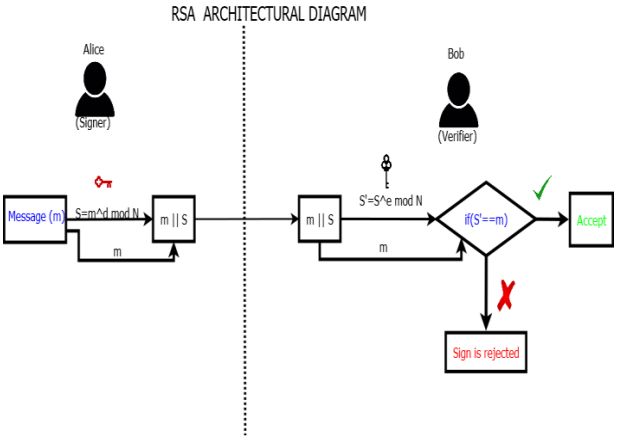


Fig 3:RSA Architecture

A test bed with entities broker, subscriber/publisher was setup, the communicating schemes between entities were monitored using tools like Wire shark. The result of the communication with underlying data transmission protocol as MQTT showed data being transmitted in plain text. An effort was made to understand the stream characteristics and implement the selected algorithms(RSA,DSS)with varies key sizes, parameters. To study theirtime complexities.

V. RESULTS AND DISCUSSION:

A thorough experimentation was carried out with the algorithms named RSA,DSA,HMAC with key sizes 256, 512, 1024 bits the time complexity associated with algorithm is monitored through code constraint and the outcome istabulated in Table2. The message for all the algorithms is the encoded base64 valueof an HD(High Definition) image and key usedwas generated from the default key generating function supported in JAVA. Fig 4-12 present the result obtained with combination of these primitives and the corresponding time complexity observed. Although there is hard and fast rule to choose a combination of these algorithms in our setup (DSA with SHA 256, RSA with SHA256, RSA with SHA 512, HMAC MD5, HMAC with SHA 256,HMAC with SHA 512).

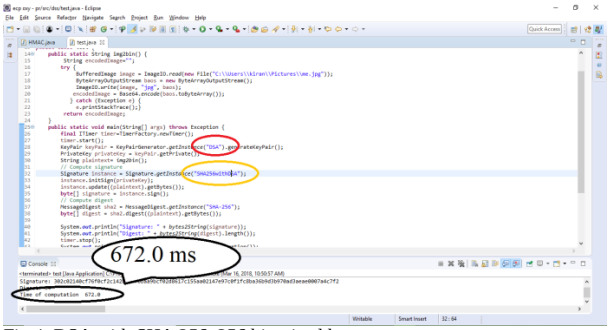


Fig 4: DSA with SHA 256 ,256 bits sized key

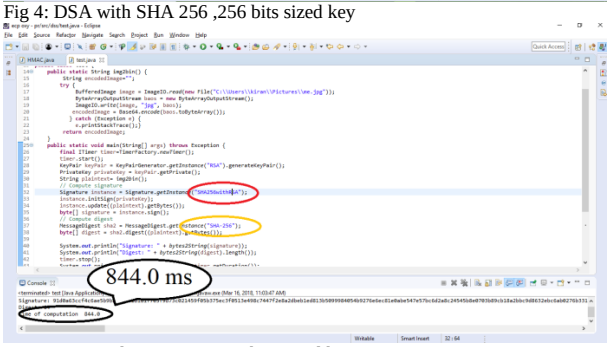


Fig 5: RSA with SHA 256 ,256 bits sized key

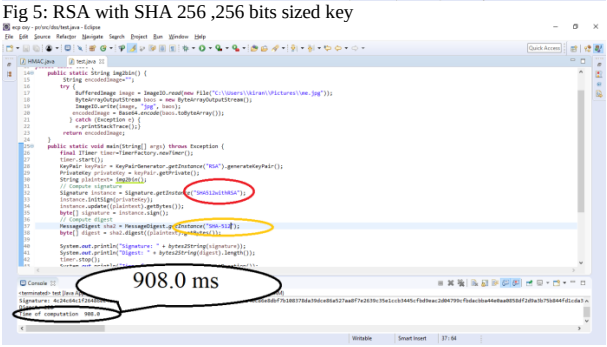


Fig 6: RSA with SHA 512,256 bits sized key

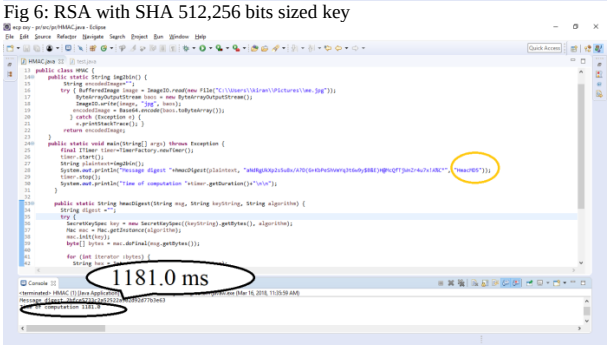


Fig 7: HMAC MD5, 512 bits sized key

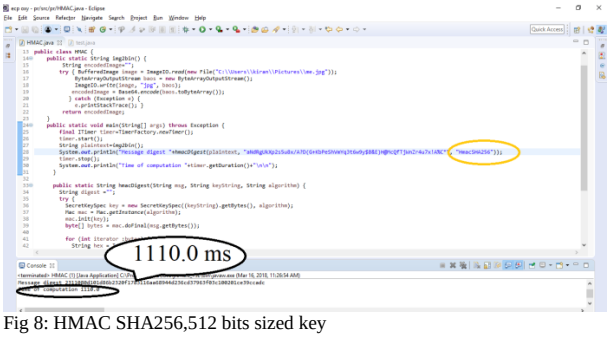


Fig 8: HMAC SHA256,512 bits sized key

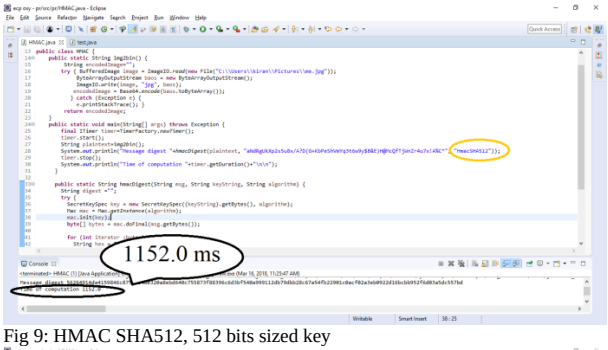


Fig 9: HMAC SHA512, 512 bits sized key

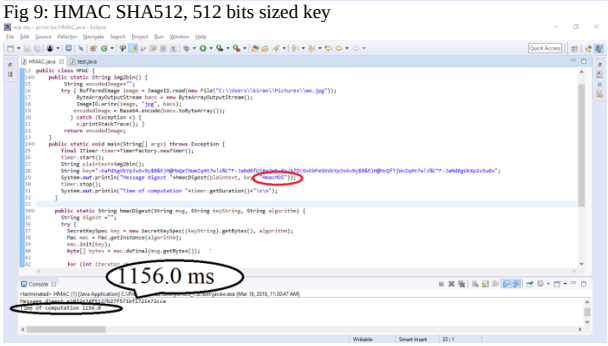


Fig 10: HMAC MD5, 1024 bits sized key

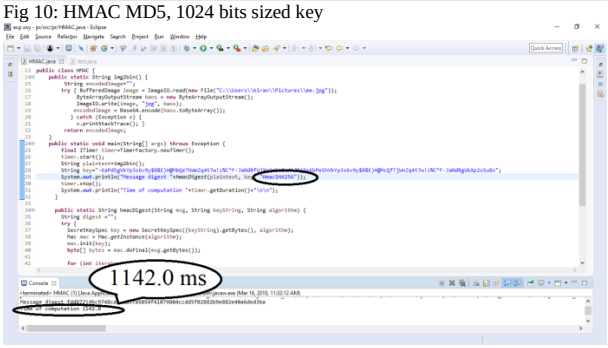


Fig 11 : HMACSHA256, 1024 bits sized key

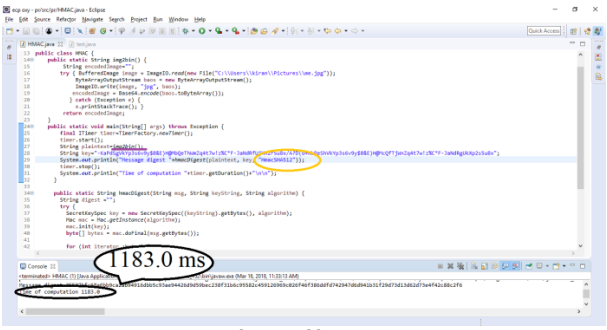


Fig 12: HMAC SHA512,1024 bits sized key

TABLEE 2: PERFORMANCE OF PROPOSED SCHEME IS PROVIDED IN TABLE

Algorithm	Size of key	Time (ms)
* DSA WITH SHA 256	256	672
RSA WITH SHA 256	256	884
RSA WITH SHA 512	256	908
HMAC MD5	512	1181
*HMAC SHA256	512	1110
HMAC SHA 512	512	1152
HMAC MD5	1024	1156
*HMAC SHA256	1024	1142
HMAC SHA 512	1024	1183

CONCLUSION

The experimentation results clearly revealed the suitability (DSA with SHA 256, RSA with SHA256, RSA with SHA 512, HMAC MD5, HMAC with SHA 256, HMAC with SHA 512)to secure the network setup. HMAC are based on symmetric keys and digital signature are based on asymmetric or public key. One has to choose the proper combination of the algorithms to be used. As the future extension to this work the test bench is proposed to be made more complex with addition of more heterogenous devices and the suitability if the chosen algorithms will be studied in detail.

REFERENCES

[1] Dr.N.Harini, Dr T.R Padmanabhan and Dr.C.K.Shyamala , “Cryptography and security”, Wiley India, First Edition, 2011

[2] J.-Y. Lee, W.-C. Lin, Y.-H. Huang, A lightweight authentication protocol for internet of things, in: 2014 International Symposium on Next-Generation Electronics, ISNE 2014, Kwei-Shan, 2014

[3] An Overview of Privacy and Security Issues in the Internet of Things, Carlo Maria Medaglia- Springer Link Journal 2013

[4] Digital Signature Standard (DSS), FIPS PUB 186-3, 2009. [6] RSA Cryptography Standard, PKCS #1 v2.1, 2002.

[5] Cryptography and Network Security Principles and practices, William Stallings, Pearson Education, Fifth Edition.

[6] Digital Signature Standard(DSS),FIPS PUBS 186-3,Information Technology Laboratory, National Institute of Standards and Technology, Gathers burg, MD 20899-890,FIPS (1996)

[7] M. Palattella et al., "Standardized protocol stack for the Internet of (Important) things", *IEEE Commun. Surveys Tuts.*, vol. 15, no. 3, pp. 1389-1406, 2013

[8] C. Bormann, A. Castellani, Z. Shelby, "CoAP: An application protocol for billions of tiny Internet nodes", *IEEE Internet Comput.*, vol. 1, no. 2, pp. 62-67, Mar./Apr. 2012.

[9] AhtoBuldas, Peeter Laud, HelgerLipmaa, and Jan Villemson. Time-stamping with Binary Linking Schemes. In Hugo Krawczyk, editor, Advances on Cryptology — CRYPTO ’98, volume 1462 of Lecture Notes in Computer Science, pages 486–501, Santa Barbara, USA, August 1998. Springer-Verlag.

[10] Peter W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In IEEE Symposium on Foundations of Computer Science, pages 124–134, 1994.

[11] MQTT V3.1 ProtocolSpecification. http://public.dhe.ibm.com/software/dw/webservices/ws-mqtt/mqtt-v3r1.html

[12] On Functionality Extension of the Digital Signature Standards by Minh H. Nguyen, Duy N. HOi, Dung H. Luu, Alexander A. Moldovyan, and Nikolay A. Moldovyan, 2011 International Conference on Advanced Technologies for Communications (ATC2011).