International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-11, September 2019

The Implementation Results of Identity-Based Hashing Algorithm for Iot

Rafidha Rehiman K A, S Veni

Abstract—Nonrepudiation in Mobile environment is a major challenge in the area of IoT security. Public-key-based Digital Signature schemes are common and their computational requirements and complexities do not support constrained devices. This paper presents the design and implementation results of light weight nonrepudiation architecture based on public key cryptography and Elliptic Curve addition to reduce the overhead of processing and communication.

Keywords—Nonrepudiation, Digital Signature, IoT Security, ECC cryptosystem, Hashing

I. INTRODUCTION

Internet of Things (IoT) is an important technological advancement, which enables communication between all types of things including living beings. In IoT we can control everything with the help of software including human body parts. IoT changes every aspect of life like Education, Communication, Research and Science, Government function, Business and Human behavior (humanity) [1].The communication language of IoT is a heterogeneous interoperable protocol and many different types of devices communicate with one another. The IoT devices exchange a wide variety of vast information. IoT brings enough challenges, as these devices continuously collect a vast amount of private information. Also, heterogeneous connections are not scalable. Unlike user-operated computing devices smart things with sensors and actuators are not properly controlled when connected to the Internet.The IoT devices sporadically establish connection with other devices and communication entities connected to the network. There is a need in IoT environment to prevent some devices from accessing certain services and restrict the communication.

One major challenge faced by IoT is the problem of securing the network [2], its associated resources and its reliability issues. It has the right in the environment as server to know who are negotiating and accessing the information. Revelation of the sensitive information to unauthorized consumers may lead to security problems in an organization.

The very first step that needs to be taken care of to ensure the integrity and nonrepudiation is hardening the device against the intrusion into the secure perimeter [3]. For the IoT infrastructure, we need to implement the solutions which use minimum resources and communication power. Also, the access control models are a must to prevent policy violation in an Organization.

Traditional public key solutions for nonrepudiation and authentication are computationally complex and are slow, not a benchmarked solution for a constrained environment [4]. With the evolution of Bring Your Own Devices (BYOD) concept, the IoT devices are unavoidable and emerging gadgets in business field. Implementations of cryptographic algorithms for IoT help to ensure security in the environment and the services trustworthy. The common practice in an organization to restrict the access is to validate the users by a shared password. Normally an admin-selected password is shared by all users in the environment. If any user is vulnerable then it will affect the total security. Without proper hashing the scenario will compromise the entire environment. When the algorithms are designed and implemented for IoT, two things need be kept in mind: 1) the algorithms should be cheap in case of resources and 2) it should be capable of offering medium level security. The existing light weight researches provide enough solutions for securing IoT [5][6][7][8]. This work tried to solve the issues related to BYOD to the environment and restrict access to a trusted server.

II.SYSTEM ARCHITECTURE AND COMPONENTS OF AUTHENTICATION SYSTEM

In IoT heterogeneous devices are able to remotely connect to the network on the fly necessitating the requirement of security. Monitoring an organization's security perimeter is crucial for intrusion detection to control unauthorized access [9]. Also, it is not practical for an administrator to scan each individual association request. For implementing security, a virtual environment is created to access the security of the proposed algorithm. For that a network with a Wi-Fi router and change in the default user ID and password of the Access Point needs to be set up.

A. Authentication Server

Authentication server is a high-end workstation connected to the network and authenticates all the devices before connecting to the servers. The authentication server creates a profile of the devices that are permitted in the environment and stored. For creating the profile, the server concatenates the Serial number, product ID and MAC address of the device. When a device is trying to connect with a protected server, Authentication server shares the curve parameter to the device. The pictorial representation of the process is given in figure1. Authentication server is also responsible to verify the signature received from the client device and it allows connectivity with the protected resource server as shown in figure2. Because of automatic connectivity of IoT devices, it is allowed to be part of the networked environment; so access restriction is a must to protect the trusted resources. [10]

Manuscript published on 30 September 2019.
***Correspondence Author(s)**

Rafidha Rehiman K A, department of Computer Science, Karpagam Academy of Higher Education Coimbathore
Dr. S Veni, department of Computer Science Karpagam Academy of Higher Education Coimbathore

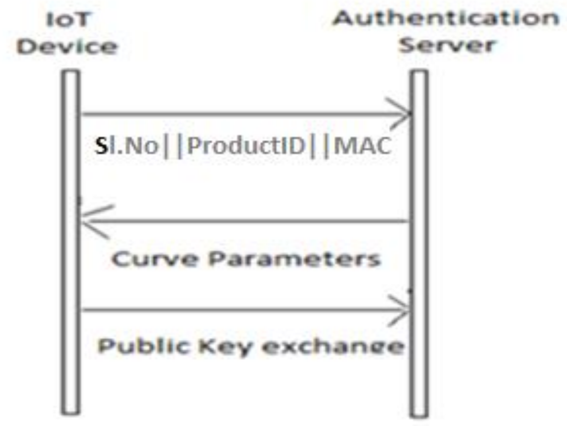


Fig1: Authentication Server

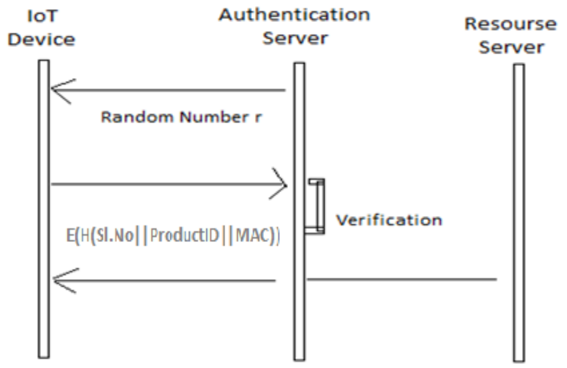


Fig 2: Restricted Access Control

B. End Devices

Mobile devices with sensors and actuators, having the ability to automatically become part of the network, communicate with other entities connected to the network. To become part of the secure architecture the device needs to register with and generate the public key private key pair based on the message from the Authentication Server.

C. Resource Server

The resource server is responsible for all valid data and information, and provides access to the devices connected after authentication message from the Authentication Server.

III. RESULTS AND DISCUSSION

A light weight Elliptic-Curve-addition-based nonrepudiation method is proposed and implemented using python and arduino 1.8.5 IDE. For testing the suitability in IoT, the program uses an ESP board. After compiling, the module is uploaded to board's memory and the board is removed from the system.

For digest preparation and encryption, first the system needs to choose a curve which is able to generate at least 40 points. Here we select the curve with equation Y2=x3+x+6(mod37) for testing the performance of algorithm.

The curve Y2=x3+x+6(mod37) generate 40 points as given in table1. The selection of an arbitrary point R is very crucial for the success of the procedure and as a prime step. Choose an R from the points on the curve to implement dynamic encoding. We can select any point as R, but if the selected R is able to map to different points, calculate 2R, 3R,…… then the point R is treated as a better choice.

Table1: Points corresponding to Y2=x3+x+6(mod37)

(2,4)	(2,33)	(3,6)	(3,31)	(4,0)	(5,5)
(5,32)	(9,2)	(9,35)	(11,4)	(11,33)	(12,9)
(12,28)	(13,12)	(13,25)	(14,10)	(14,27)	(16,14)
(16,23)	(18,11)	(18,26)	(20,16)	(20,21)	(21,1)
(21,36)	(24,4)	(24,33)	(26,12)	(26,25)	(29,2)
(29,35)	(30,10)	(30,27)	(33,7)	(33,30)	(35,12)
(35,25)	(36,2)	(36,35)	infinity		

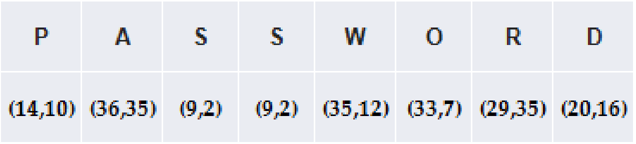
For example, here we select an R value (36, 35) and map it to the first alphabet A in the series, then find 2R,3R etc. The selected R value (36, 35) 2R, 3R….are given below:

2R = (3,6)
3R = (2,33)
4R = (20,16)
5R = (21,36) …… to 26 R for Z
Then, 27R = (12,9) is mapped to 0
28R = (30,27) to 1 ---------

To prepare the hash code, first map all individual characters in the credential to a point on the selected curve by proposed encoding scheme, and divide the points into 8-point blocks. If the last block does not contain eight points apply padding by appending point corresponding to 1 and points mapped for actual length of the message and append zero point if required.

Suppose, as an example first 8 characters are 'PASSWORD' then each character is encoded to a point as shown in table2.

Table2: Character mapping



P	A	S	S	W	O	R	D
(14,10)	(36,35)	(9,2)	(9,2)	(35,12)	(33,7)	(29,35)	(20,16)

By using the proposed digest, preparation algorithm based on Elliptic Curve addition converts these 8 characters corresponding to the block to a single point on the curve. A diagrammatic representation of the compression function is given in figure 3, and the characters are converted to a single point as given in table 3

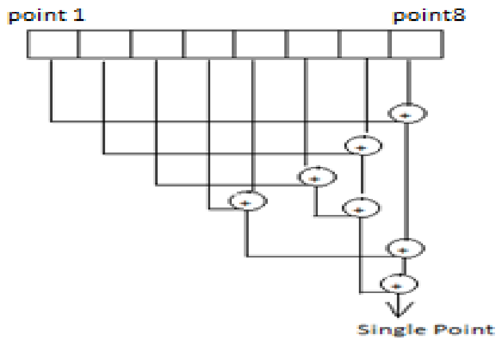
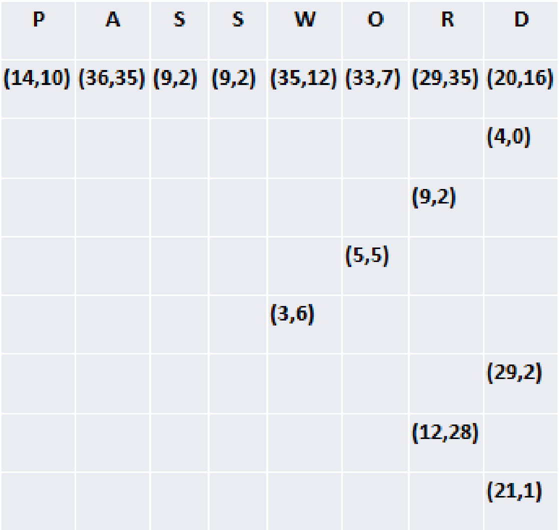


Fig 3 Compression function

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

TABLE3: Character mapping and compression



P	A	S	S	W	O	R	D
(14,10)	(36,35)	(9,2)	(9,2)	(35,12)	(33,7)	(29,35)	(20,16)
							(4,0)
						(9,2)	
					(5,5)		
				(3,6)			
							(29,2)
						(12,28)	
							(21,1)

The proposed digest preparation algorithm converts the first 8 characters to a single point on the curve. Similarly, the process is repeated for all the remaining blocks. The same methodology is repeatedly applied for each point obtained from each block and by using the curve addition before finally obtaining a single point representative for the identity of the device.

After mapping each character to points on an elliptic curve, we utilize two operations supported by the curve arithmetic, Point addition and scalar multiplication. Let P(X1,Y1) and Q (X2,Y2) be any two distinct points on the curve then perform point addition, P + Q = (X3, Y3) is X3 = L2 – X1-X2 (mod P) and Y3 = L(X1-X3) – Y1 (mod p) Where L is Y2-Y1/X2-X1. To calculate 2R i.e. scalar unit 2 is multiplied with point R treated as repeated addition in curve arithmetic, 2R = R + R and 3R = R + R + R.

The point doubled is obtained by the following calculation for a single point P = (X1,Y1) then P + P = 2P = (X3,Y3) is

X3 = L2 – 2X1 (mod P) and Y3 = L(X1-X3) – Y1 (mod p), Where L is 3X12 + a/ 2Y1 (mod p) [11].

Before transmission the point corresponding to R is encrypted by using the public key of the recipient (server), and the compressed point is encrypted by using the private key of the sender who is trying to authenticate with that particular server. After authentication, the server shares the information encrypted using the public key of the recipient to ensure only the intended recipient uses it.

IV. EVALUATION

The computational cost of the proposed system is measured for the time taken for computation. The time taken by the algorithm is compared with two existing ECC and RSA. The results of comparison are given in Table 4 and figure 4 [12].

TABLE4: Result comparison

Algorithm	Time for Algorithm implementation (Sec)
AES without digital Sign	2.718
RSA without digital Sign	2.351
HAN with digital Sign	0.58
Our Scheme with digital Sign	0.379

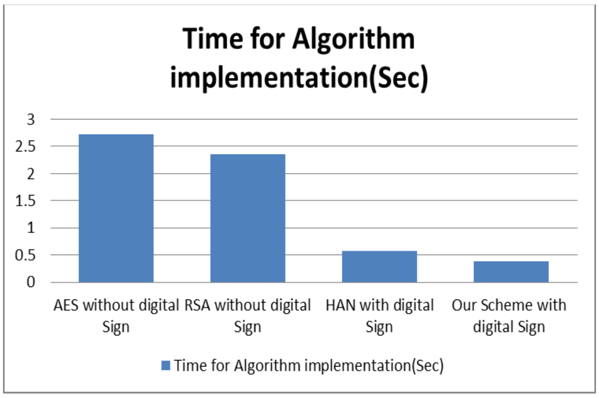


Fig 4 : Comarative matrix

Usually the security implementation of for IoT is tested over a single micro controller and it provides reliable benchmarking as an isolated environment [2].We tested the performance of our algorithm using ESP module. The communication cost is measured based on the size of the digest and compared with existing light weight solution. The results of the analysis are given in Table 5 and figure 5.

TABLE 5: Result analysis

Light Weight Scheme	Digest Size (Bits)
PRESENT -80	64
PHOTON - 80/20/16	80
PHOTON - 128	128
PHOTON - 160	160
PHOTON - 224	224
PHOTON - 256	256
U-QUARK	128
D-QUARK	160
T-QUARK	224
SPONGENT-88	88
SPONGENT-128	128
SPONGENT-160	160
SPONGENT-224	224
SPONGENT-256	256
ARMADILLO	48
OUR DIGEST	48

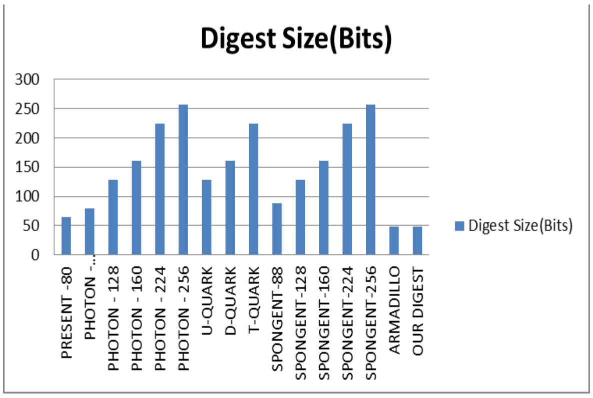


Fig 5: Digest size comparison.

V. SECURITY ANALYSIS

The proposed digest preparation method mapped variable sized input to a single point on the curve by mapping and point addition and offered collision resistance. It is computationally difficult to exactly reproduce that input characters from single decrypted point of the curve. Thus, the system offers pre-image resistance and a suitable procedure for digest preparation. The proposed method reduces computation and cost overhead, so suitable in IoT environment to utilize available resources.

VI. CONCLUSION

This research presents the implementation results of digital signature scheme used to authenticate and restrict the intrusion of IoT device into a security perimeter. The algorithm was implemented using python and arduino 1.8.5 IDE. The algorithm implementation was tested for constrained devices using an ESP board. The implementation offered a moderate level of security within a time limit. The algorithm used less memory and was easy to implement in an IoT device. The results show that reducing the size reduces the overall computation time and gives greater throughput for constrained devices.

REFERENCES

1. Zeinab Kamal et al , “Internet of Things Applications, Challenges and Related future technologies”, worldscientificnews.com.
2. Geovandro C C et al , “Performance Evaluation of Cryptographic algorithms over IOT platforms and Operating Systems”, Hindawi, Security and Communicatiohn Networks,2017.
3. A new approach to IoT security – 5 key requirements to securing IOT communications, 2009-2015 PubNub, Inc.
4. Mohsen Toorani, Ali A Beheshti, “LPKI – A Lightweight Public Key infrastructure for the mobile environment”, IEEE ICCS08, pp162-166, 2018.
5. Mahajan, P, Sachdeva, A. “A study of Encryption algorithms AES, DES and RSA for security”. Glob. J. Comput.Sci. Technol. 2013.
6. Agrawal, M, Mishra, P. “A comparative survey on symmetric key encryption techniques”. International Journal of Computer. Science and Engineering. 2012..
7. Thambiraja, E. Ramesh, G. Umarani, R. “A survey on various most common encryption techniques”. International Journal of Advanced. Research in Computer Science andSoftware Engineering. 2012.
8. Eisenbarth et al ,”A survey of lightweight-cryptography implementations”, . IEEE 2007.
9. Sudip Maitra, Kumar Yelamarathi, “Rapidly Deployable IoT Architecture with Data Security: Implementation and Experimental Evaluation” , Sensors , MDPI , 2019.
10. K Sambasiva Rao, M Kameswara Rao, “A Lightweight Digital Signature Generation mechanism for authentication of IOT Devices”, International Journal of Recent Technology and Engineering, ISSN 2277-3878, vol-7, issue -6, 2019.
11. Rafidha Rehiman K A, Veni S, “Secure Method for Short Message Encoding And Encryption Using Elliptic Curve For IOT Mobile Devices”, International Journal of Pure and Applied Mathematics, Volume 119 No. 12, 2018.
12. Amirhossein Safi, “Improving the security of Internet of Things Using Encryption Algorithm”, International Scholarly and Scientific Research and Innovation 11(5) , 558 – 561, 2017.

AUTHORS PROFILE

Rafidha Rehiman K A is working as Assistant Professor in the Department of Comuter Applications CUSAT. Currently doing Phd in Karpagam Academy of Higher Education. Research area is IoT and its Security.

Dr.S.Veni is working as Professor in the department of Computer Science in Karpagam Academy of Higher Education. She has completed her Doctoral degree from Bharathiar university. She has published 47 research articles and has attended various national and international conferences. Her research area includes networks and data mining.