Controller of Certifying Authorities
Ministry of Electronics & Information Technology
Government of India

G20 भारत 2023 INDIA

IEEE COMPUTER SOCIETY Bangalore Chapter

IAS IEEE INDUSTRY APPLICATIONS SOCIETY Linking Research to Practice Bangalore Chapter

4TH INTERNATIONAL CONFERENCE ON

PUBLIC KEY INFRASTRUCTURE AND ITS APPLICATIONS (PKIA 2023)

SEPTEMBER 8-9TH, 2023

An ECC based Anonymous Authentication Protocol for Internet of Things

Dr.Appala Naidu Tentu,
CR Rao AIMSCS, UoH Campus, Hyderabad
Renuka Cheeturi
IDRBT, Hyderabad

Outline

- Introduction
- IoT Security
- Elliptic Curve Cryptography
- Proposed Authentication Protocol
- Security and comparative analysis
- Conclusion

Introduction

- Advancement of wireless communication and information technologies has resulted in a rapid development of the Internet of Things (IoTs).
- In IoT devices all data is transferred through a network between sensing devices, remote users and up to cloud storages.
- The rapid growth in the number of IoTs devices, the heterogeneity and complexity of networks have made authentication has a challenging task.
- The simple and low cost nature of IoT devices makes them an attractive target for spoofing or impersonation attacks.
- There are malicious attacks also possible such as impersonation, replay, denial of service, and man-in-the-middle attack.

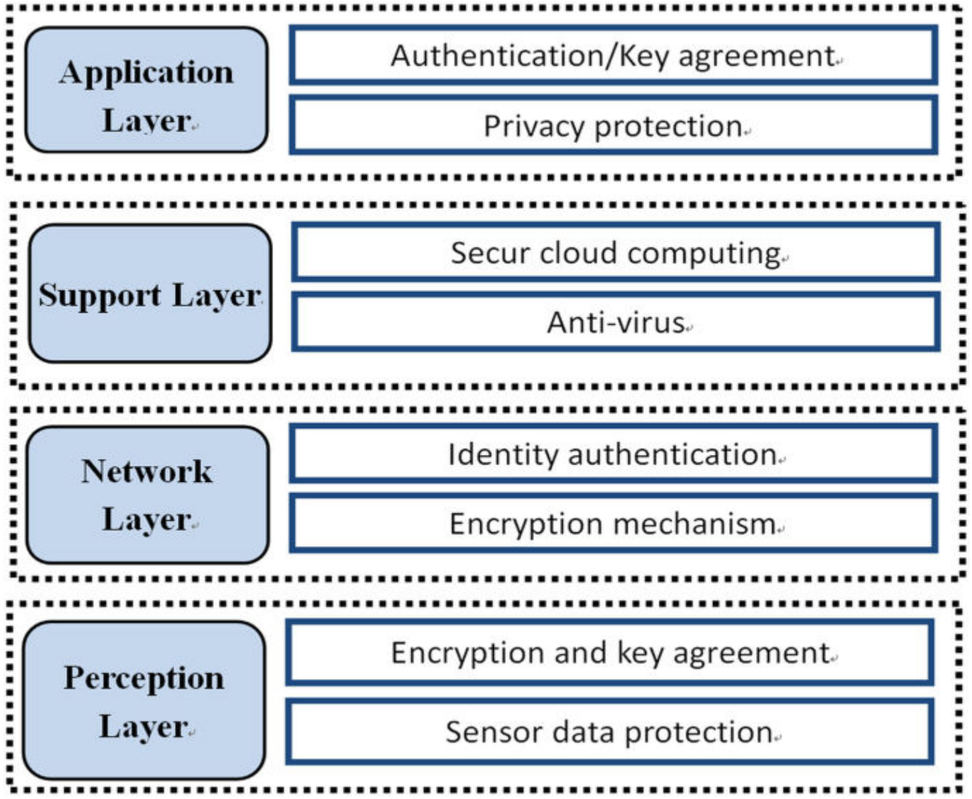
Motivation and contribution

- An efficient, secure, and lightweight remote-user authentication-based solution for an IoT environment is necessary.

- Mutual authentication is considered as a key element for successfully accessing various IoT services when it comes to network privacy and security.

- To address this, we propose to design an ECC based anonymous authenticated protocol for internet of things that enables the mutual authentication between users and gateway device.

- The proposed protocol ensures the confidentiality of identity by revealing it exclusively to the server for authentication. No adversary can find the user identity.



IoT Security Architecture

Elliptic curve cryptography-ECC

- The security of ECC is based on the difficulty of the elliptic curve discrete logarithm problem (ECDLP). The ECDLP is to find k for given values of P and Q in the equation Q = kP. Finding the value of k is hard problem.
- ECC based on elliptic curves and requires smaller keys compared to non-elliptic curves cryptography like RSA.
- An elliptic curve E_{Fp}over a finite field $F_p$is defined as the set of all $(x,y) \in F_p$such that $y^2 = x^3 + ax + b$, where $a,b \in F_p$and $4a^3 + 27b^2 \neq 0$, along with a distinguished point at infinity which is denoted by O.

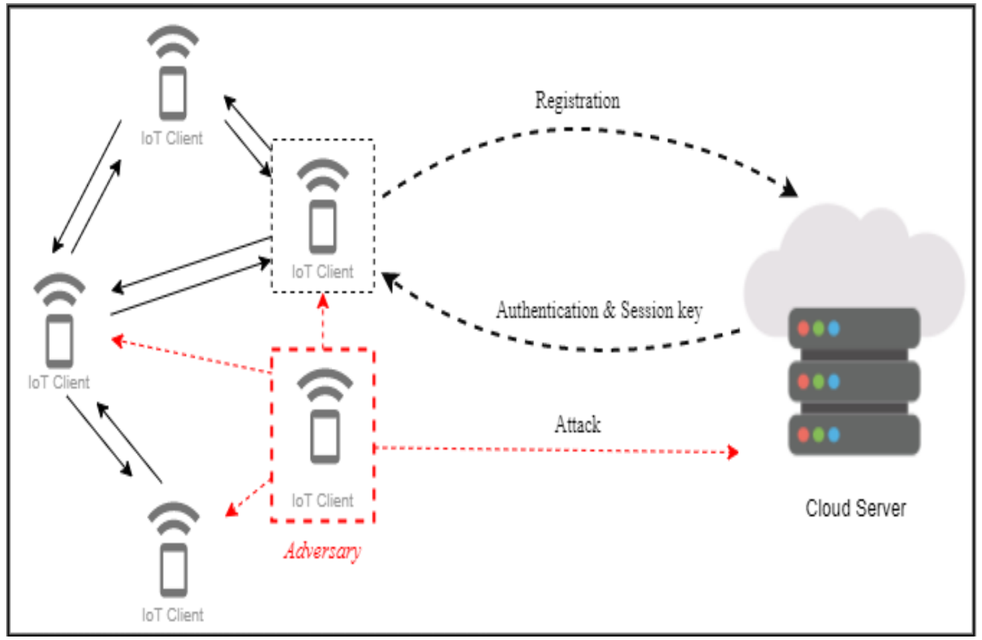
ECC selection criteria

- *Smaller Key Sizes: ECC keys are much shorter than RSA or DSA keys of equivalent strength.*
- *Faster Encryption and Decryption: ECC algorithms are faster than RSA and DSA algorithms.*
- *Lower Power Consumption: it can help to extend battery life on mobile and IoT devices.*
- *Bandwidth Efficiency: Smaller key sizes also mean that less data needs to be transmitted over the network*

Proposed Authentication Protocol

1. System Model

- The IoT environment scenario consists of two communication parties server S and the IoT device D trying to communicate with authentication in the network.
- An Adversary A with defined capabilities(Dolev-Yaos model) in the IoT network having the access of the communication in the network.



IoT network Scenario

- The server S having enough resources is responsible for allowing genuine device for communication.
- If user wants to communicate with server , it must pass the authentication process.
- The S sends a challenge message to the IoT device , then it authenticated by S and generates a session key once it receives the challenge message. Both S and device D eventually agreed on a shared session key.

Proposed Authentication protocol Construction

The protocol is carried out in three phases:

Registration phase:

- *At the first step of this phase ,a random nonce ns is selected by server(S) as its private key and calculates the curve point G_s as $G_s = n_s G$.*
- *The server selects the random number nd for every device D_i that request to register on server and verifies with $R_d = n_d G$.*
- *The corresponding values R_d,n_d for each device D_i are stored in the database.*
- *Each device stores G_s value in the memory*

Algorithm 2 REGISTRATION

Server (S)	**Device** (D_i)
1: Server generates randomly n_s (Secret Key)	
2: Calculate the curve point $G_s \ni G_s = n_s \times G$	
	3: D_i randomly generates r_i
	4: Compute $ID_i = r_i \times D_i$
	5: Send $\langle ID_i \rangle$ to Server S
6: Choose Random n_d *for each* $D_i \ni 1 \leq d \leq i$	
7: Compute $R_d = n_d \times G$; $1 \leq d \leq i$	
8: Stores $(n_s, G_s, n_d, R_d,)$	
9: Send $\langle G_s, n_d, R_d \rangle$ to each D_i	
	10: Stores (G_s, n_d, R_d)

Construction-Contd...

Login phase:

The authentication phase requires Message exchanges and computations between the device and the server as described in the following steps:

- *To begin the authentication process, the device D_i generates a random number ri and computes its identity as $ID_i = (r_i \oplus D_i)$ sends a request to the server as < Req; ID_i >.*

Algorithm 3 LOGIN

Server (S)	**Device** (D_i)
	1: Send $\langle ID_i \rangle$ to Server S
2: S retrieves respective n_d & R_d	
3: S randomly chooses n_1	
4: Compute $R_1 = n_1 \times G$	
5: Compute $R_1{}' = n_s \times R_1$ $\quad \therefore R_1{}' = n_1 \times n_s \times G$	
6: Send $\langle R_1{}' \rangle$ to D_i	

Construction-Contd...

Authentication phase:

Algorithm 4 AUTHENTICATION

Server (S)	Device (D_i)
	1: D_i randomly generates n_2
	2: Compute $R_2 = n_2 \times G$
	3: Compute $R_3 = n_2 \times R_1{}'$
	4: Compute $R_4 = n_2 \times R_d$
	5: Compute Authentication Parameter $V = H(R_3 + R_4)$
	6: Send $\langle V, R_2 \rangle$ to Server S
7: Compute $V' = H(n_1 \times n_s \times R_2 + n_d \times R_2)$	
8: **if** $V == V'$ **then**	
9: Authentication Successful	
10: S randomly selects n_3	
11: Compute $R_5 = n_3 \times G$	
12: Compute $V_1 = H(n_3 \times R_d)$	
13: Compute $SK = H(R_2 \times n_3 \|\| R_d)$	
14: Send $\langle V_1, R_5 \rangle$ to D_i	
15: **else**	
16: Authentication Failed	
17: **end if**	
	18: Compute $V_1{}' = H(n_d \times R_5)$
	19: **if** $V_1 == V_1{}'$ **then**
	20: Authentication Successful
	21: $SK' = H(R_2 \times n_3 \|\| R_d)$
	22: **else**
	23: Authentication Failed
	24: **end if**

Verification Proof

Server side Verification

$V' = H(n_1 \times n_s \times R_2 + n_d \times R_2)$

$V' = H(n_1 \times n_s \times n_2 \times G + n_d \times n_2 \times G)$

$V' = H(n_2 \times R_1' + n_2 \times R_d) \quad \because R_1' = n_s \times n_1 \times G \quad \because R_d = n_d \times G$

$V' = H(R_3 + R_4) = V$

$\therefore V' = V$

Device side Verification

$V_1' = H(n_d \times R_5)$

$V_1' = H(n_d \times n_3 \times G) \quad \because R_5 = n_3 \times G$

$V_1' = H(n_3 \times R_d) = V_1 \quad \because R_d = n_d \times G$

$\therefore V_1' = V_1$

Session Key Verification

$SK' = H(R_2 \times n_3 \,||\, R_d) = SK$

$\therefore SK' = SK$

Security and Comparative analysis

- *The security level of existing ECC-based authentication protocols are analyzed and Understood that most of the existing protocols are vulnerable to the trace ability attack.*

- *The robustness of the proposed protocol is evaluated based on formal analysis method using widely accepted approaches based on AVISPA tool.*

Scheme	Method	P1	P2	P3	P4	P5
Liao and Hsiao [2]	ECC	X	✓	X	X	X
KS [4]	ECC+Hash	X	X	X	X	X
CWS [7]	ECC+Hash	✓	✓	X	✓	X
KKD [32]	ECC+Hash	X	✓	X	✓	X
WCF [25]	ECC+Hash	X	✓	✓	✓	X
T.M.Butt[23]	ECC+Hash	✓	X	X	X	X
Our method	**ECC+Hash**	✓	✓	✓	✓	✓

P1-MIM attack,P2-Replay attack,P3-Impersonation attack,
P4-Message Integrity attack, P5-Traceability attack.
✓- Resistant, X - Non-resistant.

Conclusion and Future work

- *The ECC based authentication is considered for protocol due to its less memory requirements and computational power, eventually suitable for IoT environment.*

- *We proposed a authentication protocol and the security analysis demonstrates that the proposed protocol is provably secure and meets the requirements for security in an IoT environment.*

- *Our future plan is work on lightweight authenticated key agreement protocol for IoT environments.*

References

1. *Wang, D., Wang, P. (2016). Two birds with one stone: Two-factor authentication with security beyond conventional bound. IEEE transactions on dependable and secure computing, 15(4), 708-722.*
2. *He, D., Zeadally, S., Kumar, N., Wu, W. (2016). Efficient and anonymous mobile user authentication protocol using self-certified public key cryptography for multi-server architectures. IEEE transactions on information forensics and security, 11(9), 2052-2064.*
3. *Challa, S., Wazid, M., Das, A. K., Kumar, N., Reddy, A. G., Yoon, E. J., Yoo, K. Y. (2017). Secure signature-based authenticated key establishment scheme for future IoT applications. Ieee Access, 5, 3028-3043.*
4. *Jia, X., He, D., Li, L., Choo, K. K. R. (2018). Signature-based three factor authenticated key exchange for internet of things applications. Multimedia Tools and Applications, 77, 18355-18382.*
5. *Li, C. T., Lee, C. C., Weng, C. Y., Chen, C. M. (2018). Towards secure authenticating of cache in the reader for RFID-based IoT systems. Peer-to-Peer Networking and Applications, 11, 198-208.*
6. *Fan, K., Gong, Y., Liang, C., Li, H., Yang, Y. (2016). Lightweight and ultralightweight RFID mutual authentication protocol with cache in the reader for IoT in 5G. Security and Communication Networks, 9(16), 3095-3104.*
7. *Wang, K. H., Chen, C. M., Fang, W., Wu, T. Y. (2017). A secure authentication scheme for internet of things. Pervasive and Mobile Computing, 42, 15-26.*
8. *Hankerson, D., Menezes, A. (2021). Elliptic curve cryptography. In Encyclopedia of Cryptography, Security and Privacy (pp. 1-2). Berlin, Heidelberg: Springer Berlin Heidelberg.*

Controller of Certifying Authorities
Ministry of Electronics & Information Technology
Government of India

G20 भारत 2023 INDIA

THANK YOU

भगत संगणन विकास केंद्र
सीडैक CDAC
॥ज्ञानादेव तु कैवल्यम्॥
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING

IEEE COMPUTER SOCIETY
Bangalore Chapter

IAS IEEE INDUSTRY APPLICATIONS SOCIETY
Linking Research to Practice
Bangalore Chapter