International Journal for Research in Engineering Application & Management (IJREAM)
ISSN : 2454-9150 Vol-05, Issue-12, Mar 2020

Secure and Authenticated Key Establishment Scheme for IoT Applications

[1]Gayatri Gunupuru, [2]Sri Vidya Bodda, [3]Lokaika Sai Sravani Dibbidi, [4]Gayatri Penmetsa, [5]Ravi Kiran Avidi

[1]Assistant professor, [2,3,4,5]Student, ANITS, Visakhapatnam, India.

[1]ggayatri.cse@anits.edu.in, [2]99vidya16@gmail.com, [3]saisravani1112@gmail.com, [4]gayatribhannu@gmail.com, [5]ravikiranavidi@gmail.com

Abstract -Internet of Things (IoT) refers to a network comprised of physical objects capable of gathering and sharing electronic information. IoT devices are used vividly in everyday life of people. Using IoT devices has enormously reduced human effort in making things possible. The work done by IoT devices is much richer in accuracy and efficiency compared to work done by humans. Some examples of IoT devices and their contribution to mankind are Smart meters, commercial security systems and smart city technologies that are used to monitor traffic and weather conditions.In this fast moving technological world, where information is considered as the greatest wealth, apart from developing applications, it is highly essential to secure it from threats and attacks.In this paper, methods are proposed to provide security and authenticity to IoT applications.

Keywords- Authentication model, BAN logic, Elliptic curve cryptography, Gateway node, IoT.

I. INTRODUCTION

Security[1] to IoT[2] devices means that the connected devices of the network have to be protected against attacks. Within the network comprising of IoT devices, each device is given an unique identifier and every device has ability to transfer data across the network. The information transfer occurs by connecting the devices to the Internet. When the devices are accessed through Internet, serious vulnerability issues arise. The integration of IoT devices must benefit human in terms of performance and accuracy which can be achieved only when proper security mechanisms are followed. Some of the security mechanisms to be included are authentication and privacy. Authentication[3] is the process of verifying the identity of a person or device. For example, consider an user who signs up for a website and logs in into the website later, the person is said to be authenticated to the website when his/her identity is known. Privacy is the state of being free from attention. In the context of IoT, privacy means that the data shared and received remains inaccessible by unauthenticated users. These security mechanisms are integrated in IoT devices by observing the communication process occurring in the devices for attacks and safeguarding the network

II. AUTHENTICATION MODEL

Every device in the network communicates with other devices by making use of Internet. Therefore, every IoT device must be able to connect to the Internet. This connection of IoT devices with the Internet is possible with the help of gateway nodes[4]. Gateway connects two similar or dissimilar networks using different protocols. IoT device can be programmed by accessing it through GWN. Authentication of IoT device and user is validated through the GWN of the device. An user who wants to make use of the data contained by IoT device must prove his/her identity. Access is granted only after checking mutual authentication. GWN are used to integrate any type of IoT devices like sensors, actuators etc.

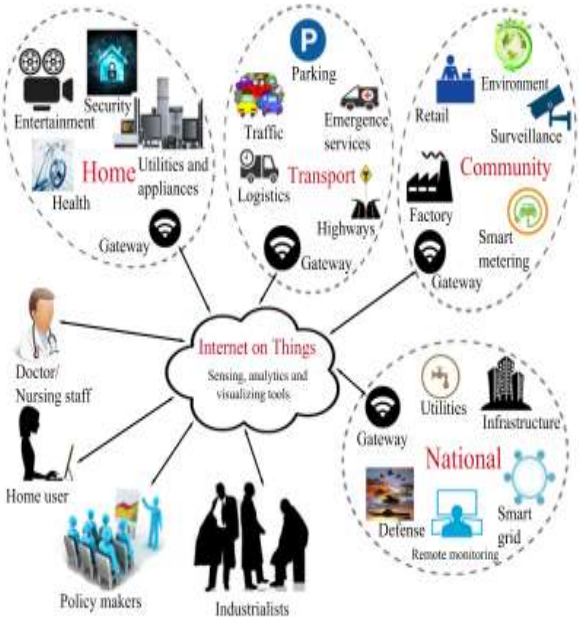

Figure no: 2.1 Authentication model for IoT applications

 DOI : 10.35291/2454-9150.2020.0195

III. MATHEMATICAL PRELIMINARIES

Elliptic curve cryptography[5] is a public key encryption technique based on elliptic curve theory that can be used to create faster,smaller,efficient cryptographic keys. An elliptic curve is a set of points described by the equation

$y^2 = x^3 + ax + b.$

A group G can be defined such that the elements of the group are points on the elliptic curve and apply the group to generate public - private keys to do encryption.If d is a random integer chosen from {1,2,----n}, where n is the number of elements in the subgroup and G is the base point (beginning and ending point of the sub group), then scalar multiplication can be applied to find H where H is another element of the sub group and obtained as:H=dG. D is used as private key and H as public key.While programming an IoT device using a GWN, it is essential to secure the GWN. To provide the security, public and private keys are generated using elliptic curve cryptography to achieve encryption.SHA(Secure hash algorithm)[6] is used to ensure that data has not been modified. SHA accomplishes this by computing a cryptographic function and any change to a given piece of data will result in a different hash value. As a result, differing hash values are key to determining if the data has been altered. In this project, to ensure that the id's of user and IoT devices in a communication channel remain protected and unaltered a hashing algorithm SHA-1 is used.SHA-1 is a cryptographic hash function which takes an input and produces 160-bit hash value known as a message digest,40 digits long. It works for an input size that is less than 2^{64} bits. In order to overcome vulnerability issues, padding can be done to input string till it reaches a length of 2^{64} bits.

Elliptic curve point addition:

Considering P,Q as two points on elliptic curve, to computer P+Q where P!=Q the possibilities are :

- If P = O (null point), then P + Q = Q.Likewise if Q = O, then P+Q = P.
- Else P = (x_0,y_0) and Q = (x_1,y_1). If $x_0 = x_1$ then P+Q = Q,

Else: $s = (y_0-y_1)/(x_0-x_1)$,

$x_2 = s^2 - x_0 - x_1$

$y_2 = s(x_0 - x_2) - y_0$

$P + Q = (x_2 , y_2)$

Elliptic curve point doubling:

To compute 2P (P + P), the possibilities are :

- If P = O, then 2P = O
- Else P = (x,y) : If y = 0,then 2P = O.

Else: $s = (3x^2 + a) / (2y)$,

$x_2 = s^2 - 2x$

$y_2 = s(x-x_2) - y_1$

$2P = (x_2 , y_2)$

IV. RELATED WORK

- DTLS based Security and Two-Way Authentication :

DTLS[7] is an adaption of the widespread TLS protocol, used to secure HTTPS, for unreliable data-gram transport. All messages sent via DTLS are prepended with a 13 bytes long DTLS record header. This header specifies the content of the message (e.g. application data or handshake data), the version of the protocol employed,as well as a 64-bit sequence number and the record length. The top two bytes of the sequence number are used to specify the epoch of the message which changes once new encryption parameters have been negotiated be-tween client and server.To counter the high energy consumption due to RSA[8] based encryption and public-key infrastructure certificates in ,an elliptic curve cryptography (ECC) based approach is proposed.

- RFID Authentication schemes for Internet of Things (IOT) :

Radio-frequency identification (RFID)[9] is one of the most important technologies used in the IoT as it can store sensitive data, wireless communication with other objects, and identify/ track objects automatically. A RFID tag is composed of a microchip, an antenna, and a dedicated hardware for cryptographic operations. It can store secret data for authentication and communicates with the RFID reader. Usually, the RFID tag's computing capacity and memory storage are very limited. RFID authentication protocols which rely exclusively on the use of Elliptic Curve Cryptography are not secure against the tracking attack.

- BiBa one-time signature and broadcast authentication protocol :

BiBa signature scheme[10], a new signature construction that uses one-way functions without trapdoors. BiBa features a low verification overhead and a relatively small signature size. In comparison to other one-way function based signature schemes, BiBa has smaller signatures and is at least twice as fast to verify (which probably makes it one of the fastest signature scheme to date for verification). On the downside, the BiBa public key is large, and the signature generation overhead is higher than previous schemes based on one-way functions without trapdoors (although it can be trivially parallelized).

- Signature based approach :

While DTLS based approach has higher energy consumption and symmetric approach is prone to denial-of-service attacks, an ideal signature based approach is proposed as it provides faster key generation .In this scheme, immediate authentication is guaranteed and synchronization is not needed. This approach with longer key lengths are used in applications that send messages

 DOI : 10.35291/2454-9150.2020.0195

infrequently.in the cases where rapid communication is needed, keeping the size of key length short is ideal. Making use of signature based approach with ECC as cryptographic encryption technique is the proposed mechanism. Research demonstrates that ECC based public key cryptosystem is suitable for resource-constrained devices. As only 160-bit ECC offers the same level of security as compared to RSA due to its smaller key size.

V. PROPOSED SCHEME

The proposed scheme can be applied in all kinds of IoT applications. A new signature based authenticated key establishment scheme is followed. In IoT, different users communicate with each other and with various smart devices through gateways to ensure secure communication. The mechanism is that a legal user can access the information from a sensing device provided that both mutually authenticate each other after which a secret session will be established for secure communication. The proposed scheme consists of following five phases, 1)System setup phase, 2)Device registration phase, 3)User registration phase 4)Login phase, 5)Session establishment phase.

1) System setup phase

Step1: GWN chooses a non-singular elliptic curve Ep over a prime field. Consider a 163-bit non singular elliptic curve over prime field 2163 i.e., sect163r2[11] .The parameters of the elliptic curve:(m,f(x),a,b,G,n,h) where $f(x)=x^{163}+x^7+x^6+x^3+1$.The elliptic curve equation is:

$y^2+xy=x^3+ax^2+b$.

GWN chooses a base point P, private key d_{GWN} and calculates public key as $Q_{GWN}=d_{GWN}.P$.

Step2 : GWN chooses collision-resistant cryptographic one way hash function I.e., SHA-1.

Step3: User biometrics are scanned using fingerprint scanner and converted to base-64 string for the purpose of calculation of digital signature.

2) Device registration phase

Each device consists of a unique ID and chooses a private key, calculates public key. The ID of the sensing device ex-orred with its private key will be converted to a hash value using SHA-1.

3) User registration phase

During registration phase, every uses will be given a unique ID and a private key, calculates public key. User sends registration request message to GWN.The GWN computes hash value of the message and sends to user.Then the user selects a unique password and imprints biometrics at the sensor.

4) Login phase

User logs in to GWN by imprinting biometrics and entering id, password and chooses a random secret number to generate time stamp, a login message with signature will be calculated. The login message will be sent by user to GWN.

5) Session establishment phase

GWN receives login message from the user, validates the time stamp and performs user signature verification. After successful signature verification, GWN computes authentication request message and sends it to the sensing device. After performing signature verification, a session key and authentication reply message will be generated by the sensing device. When user requires authentication reply message a session key will be generated and shared with the sensing device. thus after sharing session keys, a secure connection is established to achieve secure communication.

Security analysis

The mutual authentication between the user and GWN is checked through timestamp validity of the messages. The validity is proved through session establishment. During mutual authentication, in order to protect the identity of user and the sensing device, the data is converted to hash value. In order to prove that the proposed scheme is secure against attacks, formal and informal security verification is performed using BAN logic[12].

MUTUAL AUTHENTICATION USING BAN LOGIC

To prove that a user and a sensing device mutually authenticate each other through fresh and trustworthy information, the BAN logic is being used. This is achieved by verifying the message's origin, the origin's freshness and trustworthiness. The BAN logic is a set of rules for defining and analyzing information exchange protocols. Specifically, BAN logic helps its users to determine whether exchanged information is trustworthy, secured against eavesdropping.

- $A \mid\equiv X$: A believes the statement X.
- $A \triangleleft X$: A sees X, i.e. A has received a message containing X.
- $A \mid\sim X$: A once said X i.e $A \mid\equiv X$ when A sent it.
- $A \mid\Longrightarrow X$: A has authority or jurisdiction over X.
- $\#(X)$: X is a fresh message.
- $A \overset{K}{\longleftrightarrow} B$: K is shared secret key between A and B.
- X_K: X is encrypted with key K.
- $< X >_Y$: formula X is combined with formula Y.
- $(X)_K$: X is hashed with key K.
- (X, Y): X or Y is one part of formula (X, Y).

Figure no : 6.1 Notations of BAN's postulates

VI. RESULTS

In the system setup phase, based on the type of elliptic curve selected, base points and private keys are obtained. For reducing computational overhead while achieving

 DOI : 10.35291/2454-9150.2020.0195

security,this paper has proposed secure session establishment scheme using sect163r2 elliptic curve with SHA-1 as the hashing algorithm.Once the public and private keys are obtained, the next step is to read user biometrics.The above task is accomplished by making use of a fingerprint scanner that takes the user fingerprint as input and stores the output in the form of Base-64 string.

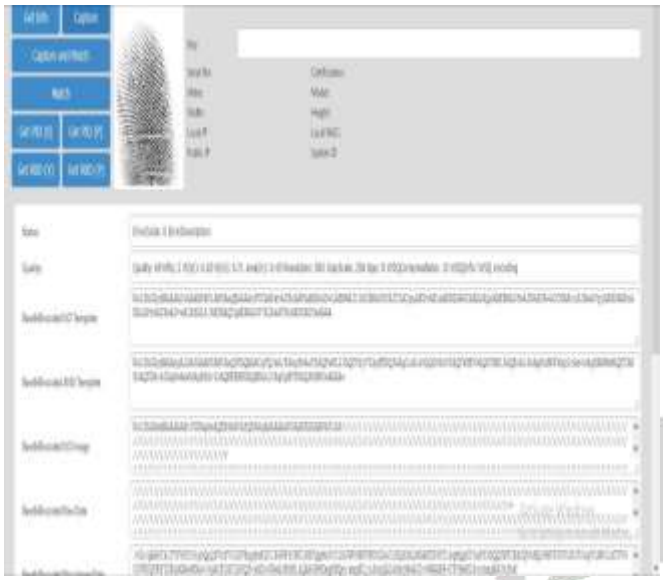

Figure no : 7.1 Conversion of user fingerprint into string

After reading the fingerprints, registering the users and sensing device, the next step taken is calculation and transmission of authentication request and reply messages during the login face. Once the login is successful session keys are generated and secure session establishment is performed.

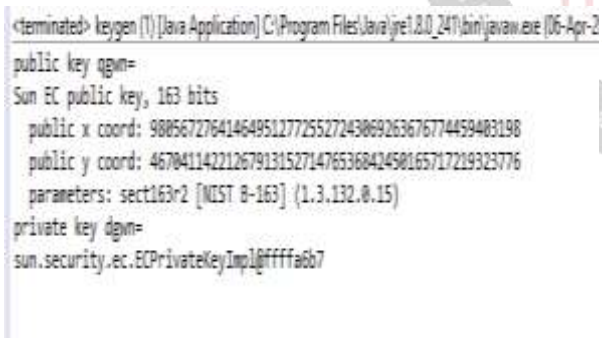

Figure no : 7.2 Key generation using Elliptic curve cryptography

VII. Conclusion

The proposed scheme is implemented using several modules. Each phase is coded separately in order to configure into platforms like Raspberry Pi. By following the above mentioned phases, secure session establishment is performed.These advancements in communication work perfectly in future IoT applications that are developed with more security.The proposed scheme can be enhanced by adding some more phases like password revocation, registration of more umber of users and devices etc.,In order to overcome the security challenges, elliptic curve algorithm is used.In order to check the trustworthyness of the user and preserve the freshness of the message, a widely accepted BAN logic can be used. By considering the functionality and architecture of present IoT devices, the probability of practical implementation of the proposed scheme is greater compared to other available schemes.

References

[1] T. Xu, J. B. Wendt and M. Potkonjak, "Security of IoT systems: Design challenges and opportunities," 2014 IEEE/ACM International Conference on Computer-Aided Design (ICCAD), San Jose, CA, 2014, pp. 417-423.

[2] Mohamad Noor, Mardiana & Hassan, Wan. (2018). Current research on Internet of Things (IoT) security: A survey. Computer Networks. 148. 10.1016/j.comnet.2018.11.025.

[3] Survey of Authentication and Authorization for the InternetofThings-https://www.hindawi.com/journals/scn/2018/4351603/

[4] K. Rajaram and G. Susanth, "Emulation of IoT gateway for connecting sensor nodes in heterogenous networks," 2017 International Conference on Computer, Communication and Signal Processing (ICCCSP), Chennai, 2017, pp. 1-5.

[5] Agrawal, Himja and Prof. P. R. Badadapure. "A Survey Paper On Elliptic Curve Cryptography." (2016).

[6] Sahu, Aradhana & Ghosh, Samarendra. (2017). Review Paper on Secure Hash Algorithm With Its Variants. 10.13140/RG.2.2.13855.05289.

[7] Yassine, Maleh & Ezzati, Abdellah & Belaissaoui, Mustapha. (2016). An enhanced DTLS protocol for Internet of Things applications. 168-173. 10.1109/WINCOM.2016.7777209.

[8] Nisha, Shireen & Farik, Mohammed. (2017). RSA Public Key Cryptography Algorithm – A Review. International Journal of Scientific & Technology Research. 6. 187-191.

[9] R. Want, "An introduction to RFID technology," in IEEE Pervasive Computing, vol. 5, no. 1, pp. 25-33, Jan.-March 2006.

[10] Adrian Perrig. 2001. The BiBa one-time signature and broadcast authentication protocol. In Proceedings of the 8th ACM conference on Computer and Communications Security (CCS '01). Association for Computing Machinery, New York, NY, USA, 28–37. DOI:https://doi.org/10.1145/501983.501988

[11] Sect163r2-https://cryptography.io/en/latest/hazmat/primitives/asymmetric/ec/

 DOI : 10.35291/2454-9150.2020.0195

[12] Sierra, José & Hernandez-Castro, Julio & Alcaide, Almudena & Torres, Joaquín. (2004). Validating the Use of BAN LOGIC.. 851-858.

 DOI : 10.35291/2454-9150.2020.0195