EBASKET: ECC Blended Authentication and Session Key Establishment Technique for IoT

Padmashree M G, Arunalatha J S, Venugopal K R

Abstract: ***Security is a prerequisite of each device that provides physical access to anyone and is logically expose to communication network attacks. The Internet of Things (IoT) must assure energy-saving provision due to the unique characteristics of IoT devices that comprise cost-effective, low power, and data delivery capacity. A Key-based Authentication scheme is a need without creating a bottleneck of communication for security in IoT integration. Security solutions viz., Authentication, Access control, and Key management are essential for the protection of communication in IoT applications. Public Key Cryptography (PKC) encapsulates multiple security functionalities and applications in conventional networks. The proposed Elliptic Curve Cryptography (ECC) Blended Authentication and Session Key Establishment Technique (EBASKET), an enhanced HPAKE scheme secures the IoT device interactions using Hash and Public Key Cryptography conjoined with a Stochastic Number. EBASKET authenticates and establishes Session Key for communicating IoT Devices using ECC that enhances the security resisting Key Disclosure, Man-in-The-Middle (MiTM), Relay threats. It incorporates an Elliptic Curve of 256 bits to achieve the 128 bits security level. EBASKET accomplishes Key Establishment utilizes Nonce as the Fragmentary Key after authenticating the intercommunicating Devices. It decreases the overall delay incurred reducing the communication overhead minimizing the quantity and magnitude of the messages exchange for Authentication. A secure Key Establishment for the Session uses a Stochastic, Hashing function, and ECC. The interactions throughout the Predeploying, Authenticating, and Key Establishing process cause a delay. The performance graph depicts that Key Establishment and authenticating the IoT devices using ECC and reducing communicational cost enhance security than Enhanced, Hybrid, and Lightweight Authentication Schemes.***

Keywords: Authentication, Key Establishment, Internet of Things, Key Management, Light-Weight Cryptography Session Key Establishment

Manuscript received on August 27, 2021.
Revised Manuscript received on September 03, 2021.
Manuscript published on September 30, 2021.
* Correspondence Author

M G Padmashree*, Department of Computer Science and Engineering, University Visvesvaraya College of Engineering, Bengaluru, India, Email: padmashree.mg@gmail.com

J S Arunalatha, Department of Computer Science and Engineering, University Visvesvaraya College of Engineering, Bengaluru, India, Email: aruna_veeresh@yahoo.com

K R Venugopal, Vice-Chancellor, Bangalore University, Bengaluru, India, Email: venugopalkr@gmail.com

I. INTRODUCTION

INTERNET of Things (IoT) is an environment of interconnected computing and sensors, machine and virtual devices, things, and participants with explicit identification transmit data robotically *via* the network. IoT aims at connecting living things and nonliving objects. With the integration of industrial equipment, the early design and development of the IoT framework instigate. The IoT vision is to connect the entire universe from technical entities to ordinary objects. The objects vary from Healthcare, Vehicular Smart devices to Energy Savers. The related physical objects include many sensors; these sensors track locality, fluctuation, displacement, and temperature of a particular condition. Through IoT, sensors communicate with each other and the systems and recognize or transmit data directly from the sensors. Machine-to-machine communications and device and network-based intelligence facilitate industries to digitalize specific functions without relying on traditional or cloud-based implementations and solutions. These attributes offer opportunities for gathering a wide range of data but challenges in modeling the proper data communication, data, and privacy protection [1], [2].

Smart devices with the optimized communication cost of the device-to-device information sharing and a self-motivated authentication of encrypted communications enhance the security of the IoT system [3]. Lightweight encryption algorithms improve the security functionality, which depends on the Pre-shared Key set for non-compromised devices. The Authentication and Key management are designed to secure communications in the 6LoWPAN network interface [12]. The embedded system connections and network facilities to carry data between them lead to data protection during transmission. The privacy issue is deteriorating considerably, even with the various proposals [4] by the researchers *viz.*, Combinatorial [5], Batch [6] Key Distribution, RSA based [7], Multiparty [8], [9], User Authentication and Multi-Key Exchange [10]. The information systems and network protection proposals are specifically direct to accomplish data confidentiality, integrity, and availability. The existing security control system does not provide complete protection and efficiency in withstanding the Protocol Attacks.

Motivation: The latest scientific advancements have enabled the development of IoT, consisting of numerous inexpensive, low-energy, and polyfunctional sensor devices that interact through close-range wireless connections [11].

These suit for a broad spectrum of implementations *viz.*, Critical Systems, Risky environmental data aggregation, Military system services. Security solutions *viz.*, Authentication, Access control, and Key management are essential for the protection of communication in IoT applications. Public Key Cryptography (PKC) encapsulates multiple security functionalities and applications in conventional networks *viz.*, PKC initiates shared Keys, validates multi-receiver messaging. However, due to limitations of sensor devices, predominantly the constrained and finite energy, PKC is not widely supported in mobile sensor platforms. The recent advances in implementing ECC on sensor devices have drawbacks in Communication time and Storage Space [12]. EBASKET is a revised and enhanced work of [12].

Contributions: In the Proposed work EBASKET, the key contributions are:

1) Authenticate the IoT devices with finite resources by incorporating ECC for enhancing security.

2) Decrease the overall delay incurred, reducing the communication overhead minimizing the message exchange quantity and magnitude for Authentication.

3) To secure Key Establishment for the Session using a Stochastic, Hashing function, and ECC.

Organization: The paper is organized as follows: Section II summarizes the Related existing Authentication works in an IoT environment, Section III explains the Background Work for Key Establishment. Section IV presents the Proposed ECC Blended Authentication and Session Key Establishment Technique in IoT, and Section V describes the System Model of EBASKET. Section VI explicates the Performance of ECC Blended Authentication and Session Key Establishment; Section VII provides the Conclusions.

II. RELATED WORKS

A Fast Authenticating and communicating Scheme [13] for an IoT multi-device multi-group environment reduce signaling and communication overhead. IoT devices allocate to a fixed Group based on the Attributes using the Anonymous Attribute-based Group Establishment method. It provides Mutual Authentication preserving Identity Privacy with resistance to Protocol attacks. Inter-group multi-cast Group communication uses Group Key. Arockia *et al.*, [14] designed and evaluated the Authentication and Pre-Shared Key Distribution scheme using ten sensor devices and a single Edge Router in a 6LoWPAN. It is resistive to MiTM, Masquerade, Replay Attacks. The keys for each of the four flights generation use the Nonce of Sensors and Border Router with the Session-wise dynamic Key updation. Challa *et al.*, [15] proposed a Signature-derived Authentication Model using a Fuzzy extractor and a Timestamp. Gateway uses a deterministic function with Hamming Distance for Biometric Authentication and SHA-1 and ECC of 160 bits with 3 messages of 2528 bits. The analysis proves the resistance to Privileged Insider, Impersonation, Denial-of-Service (DoS), Replay, and MiTM Attacks.

Qui *et al.*, [16] introduced an Enhanced Authentication and Key Establishment Scheme (EAKES) using a hybrid cryptographic approach considering resource constraints on the 6LoWPAN nodes. For a mobile device, a Ticket is generated to achieve rapid authentication during handovers. The complete authentication is processed once the Ticket expires to secure the immobile and mobile devices in IoT. Esfahani *et al.*, [17] presented a Lightweight Authentication Scheme (LAS) that integrates XoR and Hash functionalities in an IoT system where a trusted Router authenticates Sensors. The messages exchanged between the devices do not rely on the Timestamps similar to the Nonce-based Authentication mechanism [18]; therefore, synchronizing the clock of the Server, Router, and Sensor is not mandatory. The Router automatically detects the error when an intruder provides the incorrect device Identity. The Router detects a valid sensor before determining the Key for the Session. When an attacker exploits the Key, an independent new Key generate by the device and the Router using a Hash function and a Nonce of 128 bits, and all the parameters used are 128 bits. Gope *et al.*, [19] developed a Mutual Authentication scheme that allows access to the network only for valid users through a reliable device. Due to the physical safety of the devices set up in the public domain, the hidden credentials are not stored on the Sensors. The security of the system is assured when the Sensor is compromised using Physically Unclonable, Hashing, and Exclusive OR functionalities. The Gateway limitations are excluded in the approach.

Ostad-Sharif *et al.*, [20] recommended an Authentication, Key Establishment scheme for securing the messaging channels with low overheads for communication and computation. AVISPA shows resistance against Masquerade, Replay, and Password Guessing attacks. Wazid *et al.*, [21] proposed an Authentication and Key Distribution method whereby an authorized user accesses data directly from an IoT device using Exclusive OR and Hash with Fuzzy Extractor to validate user Biometry. It ensures protection with low overheads for interaction and computation. The scheme is simulated in NS2 and checked using the tool AVISPA. The direct data access by users in an IoT environment from the IoT devices is a trap door to compromise system security.

Tang *et al.*, [22] employed an Attribute-based Authenticated Key Agreement between the Sensors without the Pre-deployment of Key management overhead in a Body Area Networks. The Controlling Model launches the Sensor Authentication by offloading the authentication overhead from Sensors. A Bilinear Pairings is applied to exchange the Keys *via* the Attribute-based Certificate. The devices are secure with the Decisional Bilinear Diffie-Hellman and Forward Key Secrecy.

ECG signals are the parameters used to reduce the computation, communication cost, and power usage of Devices. Session Keys are generated only for the Sensors that collect unique Attributes.

Eldefrawy *et al.*, [23] presented a resource-constrained IoT device Key Distribution protocol with scaling and robust Key Updates. The protocol is resistant to attacks by Impersonation and Node Capture, providing Future/Past Secrecy. Multiple Hashes are computed using the stored Secret Hash Seed in a resource-constrained IoT device.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication

The security of the system depends on the devices that are not compromised and the new keys extracted without detection. It requires a single message exchange for a resource-constrained IoT system. The security of the protocol is verified using an embedded framework Scyther tool to show the reduced computation and communication costs in a restricted environment.

Xu *et al.*, [24] proposed an Identification and Key Exchange protocol with Hashing and XOR functions guaranteeing forward confidentiality without the use of Asymmetric encryption. It has a low-security risk by maintaining forward confidentiality and significantly reducing the computing costs relative to Asymmetrically encrypted verification. As the opponent quickly captures Sensors, unique non-transmitted parameter embedded Session Keys are introduced on both sides of the authentication in each iteration.

Li *et al.*, [25] designed a Public Key Encryption and the Mutual Authentication scheme to secure IoT devices from Impersonation and MiTM attacks. The Public Keys of the IoT devices, along with Identities, are pre-distributed to achieve Authentication. The computation overhead enhances with the size of the Nonce and the number of passes. It requires 30 passes to achieve a security level of 112 bits with high time complexity. Li *et al.*, [26] simulated an Authentication scheme using a Trusted Gateway that authenticates the User and the Sensor device using preshared keys.

The Authentication scheme of Kumar *et al.*, [27] carried out the Elliptic Curve Encryption and Message Authentication Code (MAC) for the devices in an IoT environment. Hsu *et al.*, [28] proposed Group Authentication and Secret Exchange protocol for Device to Device communication with Public Key using Private Key and Linear encryption technique. Lavanya *et al.*, [29] used Pseudo-Random Functions, Certificateless with Sponge-based Hash functions. The data communication and key updations processes are excluded.

The researchers designed Group-Handover [11], Signature-based [15], [30], Physical Unclonable Function based [31], Pseudonym based [32] and Local Authentication [33] and ECC based [34], [35] Schemes. The Key Agreement schemes [36] for mobile devices [37], [38], and Body Area Network [39], [40] provide efficient performance to incorporate in an IoT environment. The comparison of the related works is in Table I.

III. BACKGROUND WORKS

Hashing validates the IoT devices to ensure that IoT systems implement securely. EAKES [16] uses Hashing to achieve information consistency and data reliability. The Server distributes the Shared Key to every device. The assumptions of computational hardness and Asymmetric Cryptography complicates cracking PKC for an intruder. The LAS [17] uses two discrete 128-bit Shared Keys for Server-Router and Router-Device interactions. The LAS uses Hash and XOR for Key Exchange with Authentication.

Hybrid Secure Authentication and Key Exchange [41] (HSAKE) Scheme address the privacy and modified message issues of the Password-based Authentication and Key Establishment scheme [42]. The Server generates an ECDH public key of 576 bits and the private Key of 832 bits during the initialization phase. A hidden server key of 64 bits with a Server, User, and device identities of 80 bits are used for authentication. HSAKE is resilient to MiTM, Timing, and DoS attacks. The Registration, Password revocation, and Home-Gateway communication are secure with ECDH. The computation and communication cost can further reduce by modifying the Key size.

A. Problem Statement

For a given collection of connected IoT devices, to establish a secure authentication and key exchange method, the objectives of the proposed design are:

- To enhance the security by mutually authenticating the communicating resource-constrained IoT devices using ECC.
- To reduce the communication delay while authenticating the IoT Devices by minimizing the number and length of messages.
- To achieve a secure Key Exchange using Stochastic and ECC.

Assumptions:

- During Signing-up, the Generator Point of ECC and the Public Key are shared between Server and network enrolling Devices *via* the Border Router and Router.
- The Physical security of the Devices is attained after the Signing-up process.

IV. PROPOSED EBASKE SYSTEM

The System Architecture shown in Fig. 1 depicts the entities of the Authentication and Session Key Establishment process *viz.*, the resource-constrained Smart Devices (D), Routers (R), Border Routers (B,) and the Authentication Server (A). The Devices interact with each other *via* the Routers and Servers. The Authentication Server possesses the Identities of the Devices.

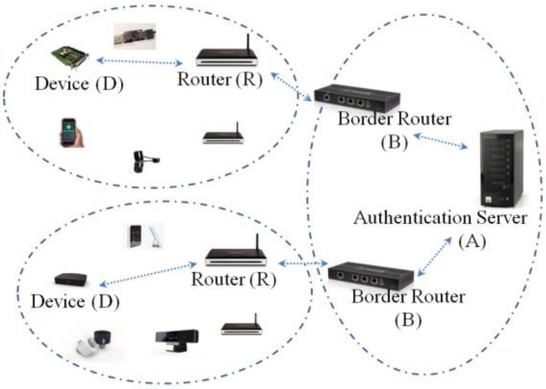

Fig. 1. The Proposed EBASKE System Architecture

V. PROPOSED SYSTEM MODEL (EBASKE)

The System Model describes the Modules of the EBASKE: The Sign-in, Authentication, Key Agreement, and the Session Key Establishment Modules and their interaction to provide security in an IoT Environment as shown in Fig. 2.

Retrieval Number: 100.1/ijitee.K946109101121
DOI: 10.35940/ijitee.K9461.09101121
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication
© Copyright: All rights reserved.

Table II defines the notations used in the Section.

Table-I: Comparison of Recent Related works

Article	Approaches	Advantage	Disadvantage
Esfahani *et al.*, [17]	XoR, Hash; Nonce of 128 bits, trusted Router authenticates Sensors.	No clock synchronizing; Router detects a valid sensor before determining the Key.	The parameters used are 128 bits.
Gope *et al.*, [19]	Physically Unclonable, Exclusive OR, and Hash functions.	Access to the network only for a trusted device; No hidden credentials in Sensors.	Gateway limitations are not considered.
Wazid *et al.*, [21]	Exclusive OR and Hash with Fuzzy Extractor	Low overheads for interaction and computation.	Direct data access by users from the IoT devices is a trap door.
Tang *et al.*, [22]	Bilinear Pairings, Certificates generated from Attributes	Authenticate offloading the authentication overhead; Forward Key Secrecy; ECG signals reduce the computation, communicational cost, and energy requirement of Sensors.	Session Keys generate for Sensors that collect unique Attributes.
Cao *et al.*, [13]	Anonymous Attribute-based Group Establishment	Low signaling and communication overhead with Mutual Authentication, Identity Privacy	Group Session Key for the multi-cast communication between the groups
Arockia *et al.*, [14]	Authentication and Pre-Shared Key Distribution; Sensors and Router Nonce; Session-wise dynamic Key updation	resistive against Impersonation, Replay, and MiTM	simulated for ten sensor devices and a single Edge Router.
Li *et al.*, [25]	The Public Keys, Identities are pre-distributed	The computation cost is in direct relation to Nonce size and amount passes; Secure from Impersonation and MiTM attacks.	30 passes achieve a security level of 112 bits with high time complexity.

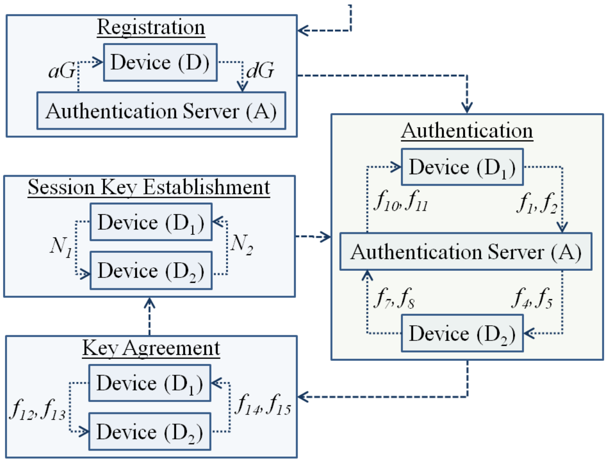

Fig. 2. Block Diagram of EBASKE

Table-II: Table of Notations

Symbol	Definition
dG	Device Public Key
d	Device Private Key
G	Elliptic Curve Generator Point
aG	Public Key
adG	Shared Secret Key
SSKAD	Server-Device Shared Secret Key
D	Device
N	Nonce
f	function
E(y)x	Encrypts *y* using Key *x*
h	hash function
D(y)x	Decrypt *y* using Key *x*

A. Signing-up

Every Device (D) sends the Public Key *dG* to Server *A* as the message *m1* in equation (1), where *d* is the Private Key of Device and *G* is the Elliptic Curve Generator Point. The Public Key *aG* is sent to Device *D* as the message *m2* in equation (2). The Shared Secret Key *adG* is used to Encrypt and Decrypt the messages transfer between the Device and the Authentication Server.

$$m1 = ID_S \,||aG \qquad (1)$$

$$m2 = ID_D||dG \qquad (2)$$

The registration process of the Devices is given in Function 1.

Function 1: *RegisterDevice()*, Signing-up of the Devices

Input: The ECC Generator *G*, The Private Keys *a* and *d* of the Authentication Server *A and* the Device *D*, respectively.
Output: Secret Key SSK_{AD} shared to the Device *D* and the Authentication Server *A*
1: Device *D* computes Public Key, *dG*.
2: The *D* sends $ID_D||dG$ to the Authentication Server *A*.
3: The *A* computes the Public Key *aG*.
4: The *A* transmits $ID_S \,||aG$ to the Device *D*.
5: The *A* derives the Shared Secret Key, $SSK_{AD} = adG$.
6: Device *D* obtains the Shared Secret Key, $SSK_{AD} = daG$.

B. Authentication

The Authentication process involves transferring messages from Devices and the Authentication Server.

Sending Device(D_1): The D_1 generates a Nonce $N_1 = n_1G$ and computes equation (3), equation (4), and equation (5) and Send f$_1$, f$_2$ to *A*.

$$f_0 = ID_1||N_1 \qquad (3)$$

$$f_1 = E(f_0)_{SSKAD1} \qquad (4)$$

$$f_2 = h(f_0) \qquad (5)$$

Authentication Server (A): A obtains f_0 as in equation (6) and if ($f_2 = h(f_0)$) then valid otherwise discard.

$$f_0 = D(f_1)SSK_{AD1} \qquad (6)$$

Then *A* computes f_3, f_4, f_5 as in equation (7), equation (8), equation (9) respectively and send f_4, f_5 to D_2.

$$f3 = ID_A||\, f_0 \qquad (7)$$

$$f_4 = E(ID_{Aj}|\, f_3)_{SSKAD2} \qquad (8)$$

$$f_5 = h(f_3) \qquad (9)$$

Receiving Device(D_2): Computes $N_2 = n_2G$ and obtain f_3

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication

from equation (10) and if ($f_5 = h(f_3)$) then valid otherwise discard.

$$f_3 = D(f_4)_{\text{SSKAD2}} \qquad (10)$$

D_2 computes equation (11), equation (12), and equation (13) to obtain f_6, f_7, and f_8 and Send f_7, f_8 to A.

$$f_6 = ID_2||N_2 \qquad (11)$$

$$f_7 = E(f_6)_{SSKAD2} \qquad (12)$$

$$f_8 = h(f_6) \qquad (13)$$

Authentication Server (A): A extracts f_6 decrypting f_7 as in equation (14) and if ($f_8 = h(f_6)$) then valid otherwise discard.

$$f_6 = D(f_7)_{SSKAD2} \qquad (14)$$

A computes equation (15), equation (16), and equation (17) to obtain f_9, f_{10}, and f_{11} and Send f_{10}, f_{11} to D_1.

$$f_9 = ID_A||\ f_6 \qquad (15)$$

$$f_{10} = E(ID_A||\ f_9)_{SSKAD1} \qquad (16)$$

$$f_{11} = h(f_9) \qquad (17)$$

Sending Device(D1): D_1 obtains f_9 using equation (18) and if ($f_{11} = h(f_9)$) then valid otherwise discard.

$$f_9 = D(f_{10})_{\text{SSKAD1}} \qquad (18)$$

Function 2 provides the steps of the authentication process.

Function 2: *AuthenticateDevices()*, Authentication of the Devices

---

Input: The Two Communicating Devices D1 and D2
Output: The Server Authenticates the Communicating Devices D_1 and D_2

```
The Sending Device D1 generates a Nonce $N_1 = n_1G$
The $D_1$ computes, $f_0$, $f_1$, $f_2$ as given in the equations (3), (4), (5).
The $D_1$ transfers $f_1$, $f_2$ to A.
The Authentication Server A derives $f_0$
if ( $f_2 = h(f_0)$) then
    Valid
else
    Discard
end if
The A computes $f_3$, $f_4$, $f_5$ as in equations (7), (8), (9)
The A sends $f_4$, $f_5$ to $D_2$
The Receiving Device $D_2$ generates s $N_2 = n_2G$
The $D_2$ decrypts $f_4$ using SSKAD$_2$ to obtain the $f_3$
if ( $f_5 = h(f_3)$) then
    Valid
else
    Discard.
end if
The $D_2$ computes $f_6$, $f_7$, $f_8$ using equations (11), (12), (13)
The $D_2$ sends $f_7$, $f_8$ to $A$
The Authentication Server $A$ decrypts $f_7$ using $SSKAD_2$ to obtain $f_6$ as in equation (14)
if ( $f_8 = h(f_6)$) then
    Valid
else
    Discard.
end if
The $A$ computes $f_9$, $f_{10}$, $f_{11}$
The $A$ sends $f_{10}$, $f_{11}$ to $D_1$
The Sending Device $D_1$ Decrypts $f_{10}$ with $SSKAD_1$ to retrieve $f_9$
if ( $f_{11} = h(f_9)$) then
    Valid
else
    Discard.
end if
```

C. Key Agreement

The Key agreement process between the communicating D_1 and D_2 is as follows:

Sending Device(D_1): D_1 computes f_{12} and f_{13} as in equation (19) and equation (20) and Send f_{12}, f_{13} to D_2.

$$f_{12} = ID_1||N_1 \qquad (19)$$

$$f_{13} = h(\ f_{12}) \qquad (20)$$

Receiving Device(D_2): D_2 validates and computes equation (21) and equation (22) and if ($f_{13} = h(\ f_{12})$) and ($f_{13} = h(\ f_3)$) then valid otherwise discard and Send f_{14}, f_{15} to D_2

$$f_{14} = ID_2||N_2 \qquad (21)$$

$$f_{15} = h(\ f_{14}) \qquad (22)$$

Sending Device(D_1): D_1 validates by f_{14}. If ($f_{14} = h(\ f_{15})$) and ($f_{14} = h(\ f_9)$) then valid otherwise discard. Function 3 provides the Key agreement steps.

Function 3: *KeyAgreement()*, Key Agreement between the communicating Devices

---

Input: The Two Communicating Devices D_1 and D_2
Output: The Key exchanges between the communicating Devices

```
The Sending Device $D_1$ generates $f12$, $f_{13}$
The $D_1$ sends $f_{12}$, $f_{13}$ to $D_2$
The Receiving Device $D_2$ validates $D_1$
if ( $f_{13} = h(\ f_{12})$) and ( $f_{13} = h(\ f_3)$) then
    Valid
else
    Discard.
end if
The $D_2$ computes $f_{14}$, $f_{15}$ using equations (21), (22)
The $D_2$ sends $f_{14}$, $f_{15}$ to $D_2$
Sending Device $D_1$ validates $D_2$
if ( $f_{14} = h(\ f_{15})$) and ( $f_{14} = h(\ f_9)$) then
    Valid
else
    Discard.
end if
```

D. Session Key Establishment

Device D_1 derives Session Key n_1N_2 using N_2 from D_2 for the current Session. Similarly, Device D_2 computes n_2N_1 as the Session Key known only by the communicating Devices as in equation (23).

$$SKD_{12} = n_2N_1 = n_1\ N_2 \qquad (23)$$

$$= n_2n_1G = n_1n_2G \qquad (24)$$

The Session Key establishment steps are shown in Function 4.

Function 4: *SessionKeyEstablishment()*, Session Key Establishment for Devices to communicate

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication
© Copyright: All rights reserved.

```
----------------------------------------------------------------------
Input: The Two Communicating Devices $D_1$ and $D_2$
Output: Key Establishment for the Devices to communicate
1: The Device $D_1$ derives the Session Key $SKD_{12} = n_1N_2$
2: The $D_1$ acknowledges $D_2$
3: The Device $D_2$ computes $SKD_{12} = n_2N_1$ as the Session Key.
4: The Session Key $SKD_{12} = n_2n_1G = n_1n_2G$ establishment occurs between the $D_1$ and $D_2$
----------------------------------------------------------------------
```

The process of ECC Blended Authentication and Session Key Establishment in IoT is shown in Algorithm 1.

Algorithm 1: EBAS KE, ECC Blended Authentication and Session Key Establishment in IoT

```
----------------------------------------------------------------------
Input: Set of Devices
Output: Session Key Establishment between the two communicating Devices
1: All the Devices Registers to the Server
2: for all Di in Devices do
3:     The Server Registers the Device $D_i$ using RegisterDevice()
4: end for
5: repeat
6:     if $D_i$ Request for $D_j$ then
7:         The Server Authenticates $D_i$,$D_j$ using AuthenticateDevices($D_i$, $D_j$)
8:     end if
9:     if Authentic then
10:        The Sending Device uses KeyAgreement() for the Key Exchange.
11:    end if
12:    The Devices use SessionKeyEstablishment() for Session Key Establishment.
13: until Session Establishment requests from a Device
----------------------------------------------------------------------
```

VI. PERFORMANCE ANALYSIS

The EBASKE effectively Authenticates the communicating IoT Devices. The proposed system simulation uses OpenSSL, ECC, and SHA-512. The performance of the proposed EBASKET is compared with an EAKES [16], HSAKE [41], and LAS [17] in terms of the delay incurred at Router, Border Router, and Server.

Authentication: The new Device Sign-in voluntarily at the Server preceded by distribution and acquiring of the Public Keys. The Secret Key is derivable only using equation (23) and fails to procure from the Public Keys. The Devices authentication uses Hash and ECC functions that enhance the security by resisting Eavesdropping, Key Disclosure, and MiTM Attacks. The EAKES [16] uses a Time-based 160 bits ECC, and the LAS [17] uses XOR operation of 128 bits for Mutual Authentication of the Devices and the Authentication Server. EBASKE incorporates EC256bits to achieve the 128 bits security level.

Session Key Establishment: EBASKE accomplishes Key Establishment, utilizes Nonce as the Fragmentary Key after authenticating the intercommunicating Devices. A secret Stochastic (r, s) and the EC Point (SKH_r, SKH_s) derive the Session Key using equation (23). The EAKES [16] uses an Elliptic Curve of 160 bits. The LAS [17] uses the XOR function of 128 bits to accomplish Key establishment through the Server and the Device. EBASKE derives the Session Key for the interacting devices incorporating EC256bits and a Stochastic Secret.

Delay in Router: The Sender transfers message sequence to Router, the Device in the communication path. Hence, the security evaluation at the Router is significant/essential. Fig. 3 depicts the relativity of communicational delay *via* Router of EBASKE and the EAKES [16], Hybrid Secure Authentication and Key Exchange Scheme (HSAKE), and the LAS [17] schemes. In Router, an aggregate 2.9328s delay in EBASKE, 15.7633s in EAKES, 6.6516s in LAS, and 2.0304s in HSAKE. Thus, EAKES shows 81%, LAS shows 55% more communication overhead due to the use of ECC in the Server authenticating the devices. EBASKE incurs an increase of 30% delay compared to HSAKE with the probability of 90% of Successful Attack.

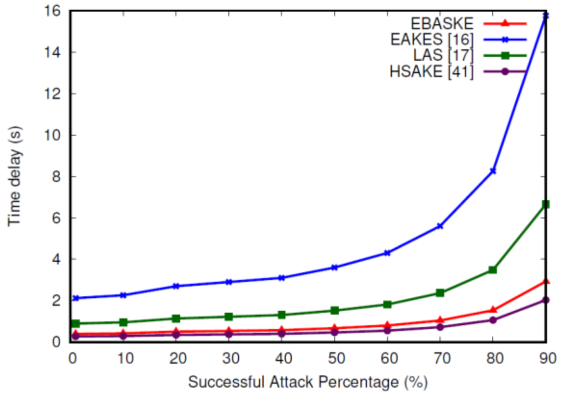

Fig. 3. Delay in Router

Delay at Border Routers: Router forwards the Host messages received to the Border Routers. Fig. 4 depicts the delay caused at the Border Routers of EBASKE with EAKES and LAS for various Successful Attack Percentages. A communication overhead of 14.485s by EBASKE, 15.7633s by EAKES, 17.4042s by LAS, and 1.7293s by HSAKE cause at the Border Routers level. Consequently, EBASKE reduces the communicational cost by 8% at the Border Routers than EAKES and 16% at the Border Routers level than EAKES. Accordingly, the reduction in the message magnitude and quantity during the Server authenticating the device minimizes the communicational cost at the Border Routers. The result shows an 88% increase in delay by EBASKE compared to HSAKE on Successful Attack.

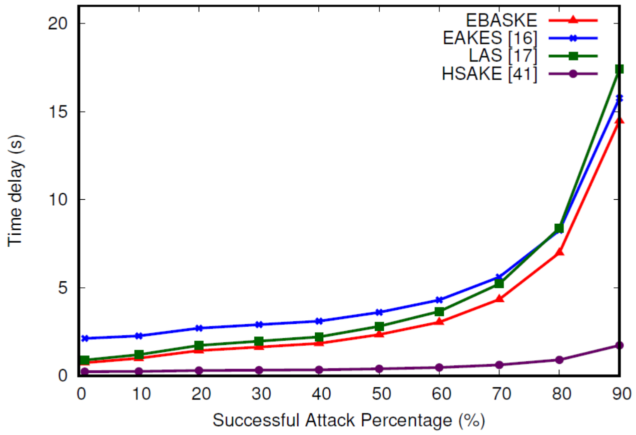

Fig. 4. Delay at Border Routers

Delay in Server: The Server interaction throughout Predeploying, Authenticating, and Key Establishing process cause a delay. EBASKE causes a 0.0973s, the EAKES 0.1883s, LAS 0.288s, and HSAKE 10.9335s delay at the Server as in Fig. 5.

EBASKE achieves a reduction in communicational cost by 48% than EAKES, 66% than LAS, and 99% compared to HSAKE at the Server using reduced message size on Successful Attack percentage of 90% as in Fig. 6.

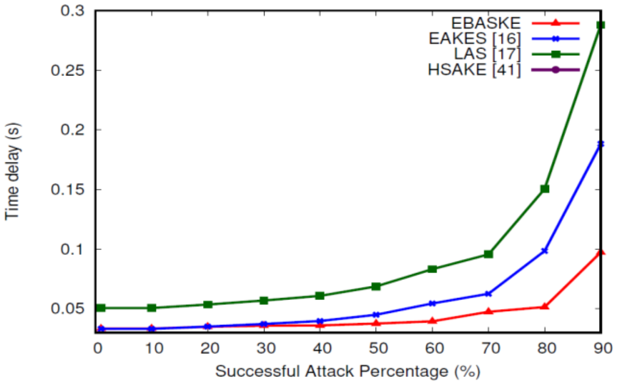

Fig. 5. Delay at Server

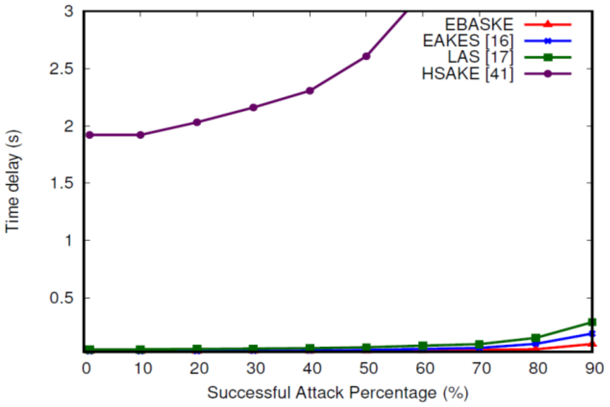

Fig. 6. Delay at Server

Aggregate Delay: Fig. 7 shows a considerable variation in the delays of the EAKES, HSAKE, LAS, and EBASKE. EBASKE incurs an aggregate communication overhead of 17.5151s, EAKES of 31.7149s, LAS of 24.3438s, and HSAKE of 14.6932s. Thus, EBASKE achieves 44% better performance than EAKES, 28% better performance than LAS, and 16% worse performance than HSAKE during security enhancement with the authentication of the communicating devices using reasonable message size.

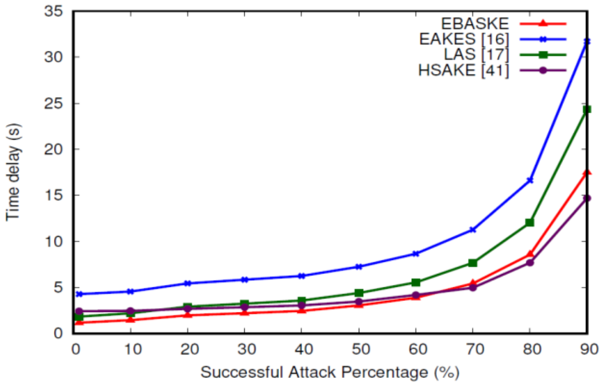

Fig. 7. Total delay

VII. CONCLUSIONS

The security of information is becoming critical with the quick growth of IoT innovations and applications. The solutions *viz.*, Authentication, and Session Key Exchange techniques provide significant security for resource-restricted IoT devices during inter-device communication. An ECC Blended Authentication and Session Key Establishment in IoT (EBASKE) designed secures data by authenticating the resource compelled IoT devices incorporating the ECC and Hash function. A Stochastic and Elliptic Curve Cryptography incorporation in securing Key Establishment accomplishes a delay 44% lower than EAKES. The Communication cost caused by EBASKE is 28% lower than LAS. The message quantity and magnitude transferred during the Authenticating and Key Establishing process decreases Communication overhead. Further, it is important to assess the resilience of EBASKE against various security threats.

REFERENCES

1. P. Gope, B. Sikdar, Privacy-Aware Authenticated Key Agreement Scheme for Secure Smart Grid Communication, *IEEE Transactions on Smart Grid*, 10 (4), (2019), 3953–3962.,doi:10.1109/TSG.2018.2844403.
2. S. Khatoon, S. M. M. Rahman, M. Alrubaian, A. Alamri, Privacy-Preserved, Provable Secure, Mutually Authenticated Key Agreement Protocol for Healthcare in a Smart City Environment, *IEEE Access*, 7 (2019), 47962–47971, doi:10.1109/ACCESS.2019.2909556.
3. V. Abreu, A. Santin, A. Xavier, A. Lando, A. Witkovski, R. Ribeiro, M. Stihler, V. Zambenedetti, I. Chueiri, A Smart Meter and Smart House Integrated to an IdM and Key-based Scheme for Providing Integral Security for a Smart Grid ICT, *Mobile Networks and Applications*, 23 (4), (2018), 967–981, doi:10.1007/s11036-017-0960-4.
4. D. Dragomir, L. Gheorghe, S. Costea, A. Radovici, A Survey on Secure Communication Protocols for IoT Systems, *in Proceedings of the International Workshop on Secure Internet of Things (SIoT)* (2016), 47–62. doi:10.1109/SIoT.2016.012.
5. M. B. Paterson, D. R. Stinson, A Unified Approach to Combinatorial Key Predistribution Schemes for Sensor Networks, *Designs, Codes and Cryptography*, 71 (3), (2014), 433–457, doi:10.1007/s10623-012-9749-4.
6. W. Wang, P. Xu, L. T. Yang, One-Pass Anonymous Key Distribution in Batch for Secure Real-Time Mobile Services, *in Proceedings of the IEEE International Conference on Mobile Services (MS)*, (2015), 158–165, doi:10.1109/TSC.2016.2594071.
7. R. Amin, G. P. Biswas, An Improved RSA Based User Authentication and Session Key Agreement Protocol Usable in TMIS, Journal of Medical Systems 39 (8) (2015) 1–14, doi:10.1007/s10916-015-0262-y.
8. G. Ateniese, M. Steiner, G. Tsudik, New Multiparty Authentication Services and Key Agreement Protocols, *IEEE Journal on Selected Areas in Communications*, 18 (4), (2000), 628–639, doi:10.1109/49.839937.
9. S. H. Islam, G. P. Biswas, Design of Two-Party Authenticated Key Agreement Protocol Based on ECC and Self-Certified Public Keys, *Wireless Personal Communications*, 82 (4), (2015), 2727–2750. doi:10.1007/s11277-015-2375-5.
10. K. L. Tsai, Y. L. Huang, F. Y. Leu, I. You, TTP Based High-Efficient Multi-Key Exchange Protocol, *IEEE Access* 4 (2016), 6261–6271. doi:10.1109/ACCESS.2016.2613442.
11. J. Cao, H. Li, G2RHA: Group-to-Route Handover Authentication Scheme for Mobile Relays in LTE-A High-Speed Rail Networks, *IEEE Transactions on Vehicular Technology*, 66 (11), (2017), 9689–9701. doi:10.1109/TVT.2017.2750219.
12. M. G. Padmashree, J. S. Arunalatha, K. R. Venugopal, HPAKE: Hybrid Precocious Authentication and Key Establishment in IoT, *in Proceedings of the IEEE Fifty Third International Carnahan Conference on Security Technology (ICCST)* (2019), 129– 134. doi:10.1109/CCST.2019.8888423.
13. J. Cao, P. Yu, M. Ma, W. Gao, Fast Authentication and Data Transfer Scheme for Massive NB-IoT Devices in 3GPP 5G Network, *IEEE Journal on Internet of Things*, 6 (2), (2018), 1561–1575. doi:10.1109/JIOT.2018.2846803.
14. A. G. R. Arockia Baskaran, P. Nanda, S. Nepal, S. He, Testbed Evaluation of Lightweight Authentication Protocol (LAUP) for 6LoWPAN Wireless Sensor Networks, *Concurrency Computation: Practice and Experience*, (2018), 1–12. doi:10.1002/cpe.4868.

15. S. Challa, M. Wazid, A. K. Das, N. Kumar, A. Goutham Reddy, E. J. Yoon, K. Y. Yoo, Secure Signature-Based Authenticated Key Establishment Scheme for Future IoT Applications, *IEEE Access*, 5 (2017), 3028–3043. doi:10.1109/ACCESS.2017.2676119.
16. Y. Qiu, M. Ma, A Mutual Authentication and Key Establishment Scheme for M2M Communication in 6LoWPAN Networks, *IEEE Transactions on Industrial Informatics*, 12 (6), (2016) 2074–2085. doi:10.1109/TII.2016.2604681.
17. A. Esfahani, G. Mantas, R. Matischek, F. B. Saghezchi, J. Rodriguez, A. Bicaku, S. Maksuti, M. G. Tauber, C. Schmittner, J. Bastos, A Lightweight Authentication Mechanism for M2M Communications in Industrial IoT Environment, *IEEE Journal on Internet of Things*, 6 (1), (2019), 288–296. doi:10.1109/JIOT.2017.2737630.
18. H. Khemissa, D. Tandjaoui, S. Bouzefrane, An Ultra-Lightweight Authentication Scheme for Heterogeneous Wireless Sensor Networks in the Context of Internet of Things, *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 10566LNCS(2017), 49–62. doi:10.1007/978-3-319-67807-8 4.
19. P. Gope, A. K. Das, N. Kumar, Y. Cheng, Lightweight and Physically Secure Anonymous Mutual Authentication Protocol for Real-Time Data Access in Industrial Wireless Sensor Networks, *IEEE Transactions on Industrial Informatics*, 15 (9), (2019), 4957–4968. doi:10.1109/tii.2019.2895030.
20. A. Ostad-Sharif, D. Abbasinezhad-Mood, M. Nikooghadam, A Robust and Efficient ECC-based Mutual Authentication and Session Key Generation Scheme for Healthcare Applications, *Journal of Medical Systems*, 43 (1). doi:10.1007/s10916-018-1120-5.
21. M. Wazid, A. K. Das, N. Kumar, A. V. Vasilakos, J. J. P. C. Rodrigues, Design and Analysis of Secure Lightweight Remote User Authentication and Key Agreement Scheme in Internet of Drones Deployment, *IEEE Journal on Internet of Things*, 6 (2), (2019), 3572–3584. doi:10.1109/JIOT.2018.2888821.
22. W. Tang, K. Zhang, J. Ren, Y. Zhang, X. Shen, Flexible and Efficient Authenticated Key Agreement Scheme for BANs Based on Physiological Features, *IEEE Transactions on Mobile Computing*, 18 (4), (2019), 845–856. doi:10.1109/TMC.2018.2848644.
23. M. H. Eldefrawy, N. Pereira, M. Gidlund, Key Distribution Protocol for Industrial Internet of Things Without Implicit Certificates, *IEEE Journal on Internet of Things*, 6 (1), (2019), 906–917. doi:10.1109/JIOT.2018.2865212.
24. Z. Xu, C. Xu, W. Liang, J. Xu, H. Chen, A Lightweight Mutual Authentication and Key Agreement Scheme for Medical Internet of Things, *IEEE Access*, 7 (2019), 53922–53931. doi:10.1109/ACCESS.2019.2912870.
25. N. Li, D. Liu, S. Nepal, Lightweight Mutual Authentication for IoT and Its Applications, *IEEE Transactions on Sustainable Computing*, 2 (4), (2017), 359–370. doi:10.1109/tsusc.2017.2716953.
26. X. Li, J. Peng, M. S. Obaidat, F. Wu, M. K. Khan, C. Chen, A Secure Three-Factor User Authentication Protocol with Forward Secrecy for Wireless Medical Sensor Network Systems, *IEEE Systems Journal*, 14 (1), (2020), 39–50. doi:10.1109/jsyst.2019.2899580.
27. P. Kumar, A. Gurtov, M. Sain, A. Martin, P. H. Ha, Lightweight Authentication and Key Agreement for Smart Metering in Smart Energy Networks, *IEEE Transactions on Smart Grid*, 10 (4), (2019), 4349–4359. doi:10.1109/TSG.2018.2857558.
28. R. H. Hsu, J. Lee, T. Q. Quek, J. C. Chen, GRAAD: Group Anonymous and Accountable D2D Communication in Mobile Networks, *IEEE Transactions on Information Forensics and Security*, 13 (2), (2018), 449–464. doi:10.1109/TIFS.2017.2756567.
29. M. Lavanya, V. Natarajan, Lightweight Key Agreement Protocol for IoT based on IKEv2, *Computers and Electrical Engineering*, 64 (2017), 580–594. doi:10.1016/j.compeleceng.2017.06.032.
30. M. G. Padmashree, S. Khanum, J. S. Arunalatha, K. R. Venugopal, SIRLC: Secure Information Retrieval using Lightweight Cryptography in HIoT, *in Proceedings of the IEEE Region 10 Conference (TENCON)* ,(2019), 269–273. doi:10.1109/TENCON.2019.8929266.
31. J. R. Wallrabenstein, Practical and Secure IoT Device Authentication Using Physical Unclonable Functions, *in Proceedings of the Fourth IEEE International Conference on Future Internet of Things and Cloud (FiCloud)*, 2016 (2016), 99–106. doi:10.1109/FiCloud.2016.22.
32. V. Odelu, A. K. Das, A. Goswami, SEAP: Secure and Efficient Authentication Protocol for NFC Applications using Pseudonyms, *IEEE Transactions on Consumer Electronics*, 62 (1), (2016), 30–38. doi:10.1109/TCE.2016.7448560.
33. Y. H. Lin, J. J. Huang, C. I. Fan, W. T. Chen, Local Authentication and Access Control Scheme in M2M Communications with Computation Offloading, *IEEE Journal on Internet of Things*, 5 (4), (2018), 3209–3219. doi:10.1109/JIOT.2018.2837163.
34. X. Li, J. Peng, J. Niu, F. Wu, J. Liao, K. K. R. Choo, A Robust and Energy Efficient Authentication Protocol for Industrial Internet of Things, *IEEE Journal on Internet of Things*, 5 (3), (2018), 1606–1615. doi:10.1109/JIOT.2017.2787800.
35. S. Sciancalepore, G. Piro, G. Boggia, G. Bianchi, Public Key Authentication and Key Agreement in IoT Devices with Minimal Airtime Consumption, *IEEE Embedded Systems Letters*, 9 (1), (2017), 1–4. doi:10.1109/LES.2016.2630729.
36. M. G. Padmashree, S. Khanum, J. S. Arunalatha, K. R. Venugopal, ETPAC: ECC based Trauma Plight Access Control for Healthcare Internet of Things, *Springer International Journal of Information Technology*, 13 (4), (2021), 1481–1494. doi:10.1007/s41870-021-00691-1.
37. P. Xie, J. Feng, Z. Cao, J. Wang, GeneWave: Fast Authentication and Key Agreement on Commodity Mobile Devices, *IEEE/ACM Transactions on Networking*, 26 (4), (2018), 1688–1700. doi:10.1109/TNET.2018.2848262.
38. L. Wu, J. Wang, K. K. R. Choo, D. He, Secure Key Agreement and Key Protection for Mobile Device User Authentication, *IEEE Transactions on Information Forensics and Security*, 14 (2), (2018), 319–330. doi:10.1109/TIFS.2018.2850299.
39. D. He, S. Zeadally, N. Kumar, J. H. Lee, Anonymous Authentication for Wireless Body Area Networks with Provable Security, *IEEE Systems Journal*, 11 (4), (2017), 2590–2601. doi:10.1109/JSYST.2016.2544805.
40. M. A. Iqbal, M. Bayoumi, A Novel Authentication and Key Agreement Protocol for Internet of Things Based Resource-Constrained Body Area Sensors, *in Proceedings of the Fourth International Conference on Future Internet of Things and Cloud Workshops, (W-FiCloud)*, (2016) 315–320doi:10.1109/W-FiCloud.2016.70.
41. U. Coruh, O. Bayat, Hybrid Secure Authentication and Key Exchange Scheme for M2M Home Networks, *Security and Communication Networks*, 2018 (2018), 1–25. doi:10.1155/2018/6563089.
42. X. Sun, S. Men, C. Zhao, Z. Zhou, A security Authentication Scheme in Machine-to-Machine Home Network Service, *Security and Communication Networks*, 8 (16), (2015), 2678–2686. doi:10.1002/sec.551.

AUTHORS PROFILE

M. G. Padmashree received the B.E. Degree in Computer Science & Engineering from JNNCE, Shivamogga, Kuvempu University, Karnataka, India, in 1998 and the M.Tech. Degree in Computer Science & Engineering from RVCE, Visvesvaraya Technological University, Karnataka, in 2011. She is currently pursuing a Ph.D. degree in Computer Science and Engineering at Bangalore University, Bengaluru, India. She was working in Engineering Colleges with 17 years of teaching experience. She has published 6 articles in refereed International Journals and Conferences. Her research interest includes Scheduling, Operating Systems, Cryptography, Security in IoT.

J S Arunalatha is a Professor in the Department of Computer Science and Engineering at University Visvesvaraya College of Engineering, Bangalore University, Bangalore, India. She obtained her Bachelor of Engineering in Computer Science and Engineering from PES College of Engineering, Mandya, Mysore University. She received her Master's degree in Computer Science and Engineering from Bangalore University. She pursued her Ph.D. program in the area of Biometrics. She has published 17 articles in refereed International Journals and conferences; Her research interest is in Biometrics, Image Processing, IoT, Big Data Analytics, and Web Mining.

K R Venugopal is currently the Vice-Chancellor of Bangalore University, Bangalore. He obtained his Bachelor of Engineering from University Visvesvaraya College of Engineering. He received his Masters degree in Computer Science and Automation from Indian Institute of Science Bangalore. He was awarded Ph.D. in Economics from Bangalore University and Ph.D. in Computer Science from Indian Institute of Technology, Madras.

He has a distinguished academic career and has degrees in Electronics, Economics, Law, Business Finance, Public Relations, Communications, Industrial Relations, Computer Science, and Journalism. He has authored and edited 77 books and has over 980 research papers to his credit. His research interests include Computer Networks, Wireless Sensor Networks, Parallel and Distributed Systems, Digital Signal Processing, Data Mining, IoT, and Cloud Computing. He received IEEE Fellow and ACM Distinguished Educator award from USA for his outstanding contributions to Computer Science and Engineering.