International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-11 Issue-4, March 2022

An Efficient Authentication Scheme Based on Mutual Verification for IoT Devices in Cloud Computing Environment

M. R. Sheeba, G. Suganthi

Abstract*: The Internet of Things (IoT) affords a new paradigm for the expansion of heterogeneous and allotted structures, and it has an increasing number of emerge as a ubiquitous computing carrier platform. IoT has specific sorts of applications, which includes smart home, wearable gadgets, clever linked cars, industries, and clever cities. Therefore, IoT based programs turn out to be the critical elements of our day-to-day lifestyles. However, due to the dearth of adequate computing and garage assets dedicated to the processing and garage of big volumes of the IoT statistics, it tends to undertake a cloud-primarily based structure to address the problems of useful resource constraints. Hence, a series of tough safety issues have arisen in the cloud-based IoT context. So, that during this paper we have proposed a mild weight scheme primarily based on mutual authentication (LWMA–CIoT) to make certain security in IoT based cloud surroundings. This LWMA–CIoT scheme specifically uses identity based encryption to make the scheme as light-weight. The security evaluation shows the effectiveness and significance of the LWMA–CIoT scheme in comparison to the prevailing schemes.

Keywords*: Mutual Authentication, Cloud Computing, IoT Device, Elliptic Curve Cryptography, Hashing.

I. INTRODUCTION

One of the important revolutions in Information and Communication Technology (ICT) is absolutely the IoT [1]. IoT community always desires to have interaction with ambiguous conditions hence ought to face diverse security demanding situations. Users' clever gadgets frequently keep a lot important statistics approximately the person, tool, community and safety parameters, and so forth. Since any consumer-centric utility preserves consumer's identity and credentials, the safety from information leakage will become crucial [2]. For a cozy communique, it is crucial to fulfil the privacy and accept as true with requirements among the IoT tool and the consumer. With the generalization of small embedded sensor gadgets and the commercialization of the IoT, quick- and lengthy-variety wi-fi community technology are being superior hastily, and the demand for deployment of cloud computing (CC) for IoT is growing considerably [3]. CC provides virtualized information era (IT) resources to ensure the workflow preferred by patron at any time and location; it lets in clients to borrow computing assets consisting of software, garage, and servers, as in keeping with their goals without the requirements of complex network and server configurations [4].

CC gives numerous benefits to IoT users through its almost unlimited computing assets, on-demand resource scaling, pay-in keeping with-use pricing scheme, and so forth. Remote CC structures are, basically, as a substitute disbursed in nature, and heterogeneous [5]. In the mobile CC environment, the mobile person authentication scheme need to have a trusted third party, comfy mobile person authentication, mutual authentication have to exist among cell users and cloud servers [6]. The integration of CC and IoT permits a novel version of pervasive and ubiquitous computing. Thus, protection is of extreme situation for such networks, on account that an adversary may interfere into the system to get illegitimate access to the resources if the right authentication mechanisms are not followed [7].

To triumph over the ones disturbing situations, the requirement of remote individual mutual authentication between the IoT network and the client is found out. Mutual authentication guarantees that each the sender and receiver are valid and alternate messages inside the pre-negotiated session [8]. In this issue, one-of-a-type security capabilities ought to be implemented like encryption, authentication, dynamic key control, identity, and biometric-based authentication, and so on. It may be very essential for a far off sensing surroundings to maintain following considerable factors to benefit users self notion [9]. Although the cloud-primarily based totally IoT packages are well addressed and universally time-venerated, but to take advantage of the actual earnings in the ones applications, we need not simplest light-weight authentication protocols but additionally the protocols loose from modern regarded threats. Therefore authentication schemes are a should for any machine [10]. There are several mutual authentication schemes for statistics protection [11]. Kerberos scheme function on the relied on third party whilst Diffie Hellman key alternate (DHKE), that's maximum popular, employs shared mystery key [12]. Apart from this, they need to incur greater overhead for proper key manage as almost all cryptographic algorithms depend upon key. Another solution may be password-primarily based authentication; however, this is susceptible to dictionary attack [14, 13].

Manuscript received on January 31, 2022.
Revised Manuscript received on February 05, 2022.
Manuscript published on March 30, 2022.
* Correspondence Author
M.R.Sheeba*, Registration Number: 17221282162017, Research Scholar, St.Xavier's College, Affiliated to Manonmaniam Sundaranar University, Abishekapatti, Tirunelveli-627012, India. E-mail: sheebasjustus@gmail.com
G.Suganthi, Associate Professor, Women's Christian College, Nagercoil, India. E-mail: dr_suganthi_wcc@yahoo.co.in

Biometric authentication may be a higher option, but it takes longer execution time, and its protection is correlated to time complexity. While considered one of a kind authentication schemes were developed so far through way of the researcher, a appropriate mild-weight, the low-price authentication scheme is but to be determined out, that might address the heterogeneity of records and devices and be resistive to malicious attacks [15]. With the intention to design a secure authentication scheme for IoT based cloud environments the following contributions are made in this research:

- In this, we don't require any key manage element because it does not involve the storage of mystery keys. Simply give up-clients and IoT device node verify every different of their tactics before beginning the conversation.
- This protocol employs elliptic curve cryptography (ECC), it is one of the green algorithms so far. With smaller keys length, they may be appropriate for resource confined stop gadgets. In addition to this, it makes use of a cryptographic hash feature, that is one-way as it hardens the safety with fewer requirements.
- Formal and informal verification grow to be moreover blanketed. Finally, the overall performance of the proposed protocol turn out to be compared with contemporary schemes. The conclusion that can be drawn is that our protocol has a higher exchange-off in phrases of safety and computation overhead than others.

The latter part of this paper has been organized in the following manner: Section 2 opinions preceding research paintings present literature current answers on comparable topics. Section 3 covers the machine fashions and protection goals. Preliminaries, a proposed layout, system with the implementation are defined in Section four. Security validation is obtainable in phase five. The overall performance evaluation is supplied in Section 6. Finally, the segment 7 sums up this paper with conclusions of research.

II. RELATED WORK

Several researchers have tried to design an efficient authentication scheme to address the security concerns. Some of the very recent solutions carried out to solve these security concerns are outlined in this section. SanazAmanlou et al., [16] Proposed to apply the Elliptic Curve Diffie–Hellman Ephemeral (ECDHE) key change algorithm together with the Pre-Shared Key (PSK) as a mild-weight and relaxed authentication scheme between the fog gateway and IoT tool based totally at the Message Queuing Telemetry Transport (MQTT) publish–subscribe protocol in a dispensed fog computing shape. The ECDHE-PSK authentication scheme makes use of Ephemeral Pre-shared key in place of heavy certificate this is very light-weight and moreover affords Perfect Forward Secrecy (PFS) function to enhance protection in evaluation with the static PSK algorithm. Hakjun Lee et al., [17] stated the security and functional weak spot of the related client authentication schemes utilized in cloud computing and proposed a brand new ECC based totally 3-component authentication scheme to overcome the security shortcomings of current authentication schemes. Badis Hammi et al., [18] prolonged the OTP principle and proposed a completely unique method of OTP generation that is based on ECC and Isogeny an awesome manner to make certain IoT protection. They evaluated the efficacy of our approach with a real implementation and in comparison its overall overall performance with extraordinary tactics specially, Hash Message Authentication Code (HMAC-based) One Time Password (HOTP) and Time-primarily based One Time Password (TOTP). Dipanwita Sadhukhan et al., [19] proposed an ECC-primarily based 3 element far off person authentication scheme that runs inside the clever tool and preserves privacy, and information confidentiality of the communicating character. To assist their claim, a couple of cryptographic attacks are analysed and located that the scheme proposed in [24] isn't vulnerable to attacks. A -trouble primarily based consumer authentication protocol proposed with the useful resource of Kaur and Kumar for smart houses the usage of ECC. Sungjin Yu et al., [20] layout a cozy and mild-weight three-detail based totally privacy-keeping authentication scheme for IoT-enabled clever domestic environments to conquer the security troubles of Kaur and Kumar's protocol. In [25] it is also tested that the scheme proposed via Kaur and Kumar can't face up to safety attacks inclusive of impersonation and session key disclosure attacks, and make sure secure consumer authentication.

III. PRELIMINARIES

It is important to shield the integrity, to keep the privacy, and to hold the confidentiality in addition to availability of resource-restricted cease gadgets. However, there are many protocols, fashions, structure tools, and so on. Proposed to provide safety. Nevertheless, nearly each solution propound up to now isn't completely resilient and lacks in giving whole safety to the device in a few manner or the other. So, that during this paper a simple and light-weight scheme based on mutual authentication (LWMA–CIoT) is proposed for IoT devices inside the cloud surroundings.

A. Security Requirements of LWMA–CIoT

To provide the necessary security, some essential requirements are needed to be provided:

- Data Storage: The quantity of records accrued at the cloud garage is large; because of this it's vital to shield the client facts from being compromised.
- Users Privacy: Allowing only the legitimate person to get right of access to the resources which they'll be prison to get admission to and restricting the evaluation of utilization types of the offerings will gain in restoring privacy.
- Location Privacy: Usually the stop device offload / talk to the nearby node/customer. If any node/purchaser gets compromised with the useful resource of any threat, then it (hacker) gets to understand the area of all the quit devices that have communicated to that node/consumer. Thus it is critical to cozy the individual location.
- Authentication: It is vital to confirm the authenticity of the node/man or woman in advance than starting verbal exchange so that sensitive statistics can be protected from unlawful get right of access to, and most effective the legitimate client is authorized to get admission to the restricted property. Thus, authentication of the communicating events ought to be finished.

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

- Integrity: This feature guarantees that the originality of the message is maintained, and it has, in any circumstances, no longer been modified or altered in the course of entire conversation.
- Confidentiality: This feature is complementary to the authentication process. This technique the valuable records must now not be found out to any entities unless they're criminal to apply it.
- Availability: This characteristic approach that community services ought to be had for valid customers every time they are seeking to access them.
- Non-repudiation: This feature approach it's miles much less tough to discover the starting place of the facts in addition to its authenticity. And the concerned person gained not deny that truth.
- Authorization: This function manner that most effective the valid give up users can forward the generated data.
- Freshness: This characteristic assures that there can be no previous message that is being transmitted through the attacker. It is thereby making sure the freshness of the statistics.
- Forward secrecy: After the consultation gets over or the purchaser exits/moved, no further messages from that individual is entertained or considered.
- Backward secrecy: Whenever any user joins the organization, then it have to be ignorant of formerly transmitted messages.

The demanding situations mentioned above need to be addressed to comfy records integrity, verbal exchange, and storage.

B. Network Model

Let the proposed LWMA–CIoT network model initially had centralized cloud storage (CCS) which is trusted and number of gateway nodes $(g_i N = g_1 N, g_2 N, ...g_n N)$, end users $(U_i = U_1, U_2, ...U_N)$ and end IoT devices $(D_i = D_1, D_2, ...D_N)$ are positioned in the network. The network model of the proposed LWMA–CIoT scheme is shown in fig.1.

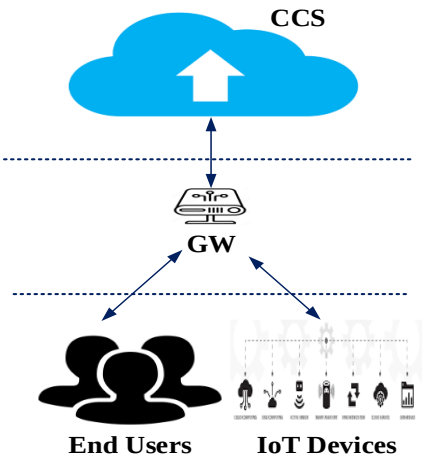

Fig. 1. Network model of LWMA–CIoT scheme

Now the communication will take place between user and gateway, then gateway and cloud, then cloud and IoT device after that end-user and IoT device sequentially. Suppose any user U_i Wants to get admission to the real–time information saved either on CCS, then it need to first verify itself to be a legitimate purchaser over again if the stop-person desires to recognize whether the receiver of the records is a legitimate node or no longer. Thus there is the most want for comfortable mutual authentication due to the fact no man or woman is relied on within the network, and all the communication is finished thru an insecure channel. And if an attacker happens to get the statistics or the get admission to, then it is able to tamper with the statistics. Only after the a hit verification method, verifier will generate the random mystery variety, with a view to be used in developing the private key. So so one can prevent such scenarios, clients and the verifier have to at the equal time authenticate every other. Since no session keys are generated, because of this there may be no need for key control.

C. Threat Model

For the proposed LWMA–CIoT scheme, we've employed a widely appropriate CK-adversary model (Canetti and Krawczyk adversary model). This version assumes that the communique channel isn't always secure, and the two speaking events do not receive as authentic with every special. An eavesdropper ought to intercept the transmitted messages and can either manipulate any part/full message or delete it. This model has the functionality to compromise the credentials and feature manipulate over the session. It is concept that no entity is absolutely trusted, and as a result, they may be compromised. Moreover, an adversary need to bodily seize forestall gadgets and carry out cutting-edge energy assessment attacks to get the credentials or data saved on that device. The statistics received can be introduced to apply to carry out unlawful and unlawful obligations, which encompass impersonation attack, replay attack, or guy-in-the-center attack. The symbols and notations used in this paper is listed in table I.

Table–I: Symbols and Notations Used

Symbols	Descriptions
U_i	End User
D_i	End IoT Device
$g_i N$	Gateway Node
$K_{private}$	private key
K_{public}	public key
α_1	Additive group
α_2	Multiplicative group
$h_1, h_2, .., h_8$	Hash functions
M_1, M_2, M_3	Messages
e	Bilinear mapping
G	Generic point (512 bit prime number)
t	Large prime number (160 bit prime number)
R	Random Number
l	Bit length
Id	Identity

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

Vid	Virtual identity
$Cert, C$	Certificate
ε	Encryption Process
Sk	Secret Key
A_{req}	Authentication request message
η, η_1, η_2	Nonce
TS_1, TS_2, TS_3	Timestamp

IV. THE PROPOSED LWMA–CIoT SCHEME

The proposed LWMA–CIoT scheme is very simple and comprises three phases such as: (i) Registration Phase (ii) Mutual Verification Phase and (iii) Update phase. All the three phases will be performed between user and gateway, then gateway and CCS, then CCS and IoT device after that end-user and IoT device sequentially.

A. Initial Assumptions

Let the CCS takes in the security parameter as input and generates the system parameter. For that it chooses α_1 and α_2 of order t on the elliptic curve with a generator G and e is the bilinear mapping function defined as $\alpha_1 \times \alpha_1 \rightarrow \alpha_2$. CCS selects a random number R_1 as its private key $K_{private}(CCS)$ then computes the corresponding public key $K_{public}(CCS) = R.G$. CCS then chooses cryptographic hash functions: $h_1 : \{0,1\}^* \rightarrow \omega_t^*$ and $h_2 : \{0,1\}^l \rightarrow \omega_t^*$. where l is the bit-length of the plain-texts. Now CCS publishes the message $M_{CCS} = \{\alpha_1, \alpha_2, e, , t, h_1, h_2, G, K_{public}(CCS)\}$.

B. Registration Phase

- **User Registration:** The user U_i will start the registration process by sending the nonce value η and the public key $K_{public}(U_i)$ to the nearby gateway node $g_i N$. i.e The user U_i sends message $M_{Ui \rightarrow g_i N} = \{K_{public}(U_i), \eta\}$ to the gateway node $g_i N$. After completing the registration process the user U_i will generate its virtual id $Vid(U_i)$ with the help of pseudonym function and nonce η through pseudo random number generator (PRNG) and send it to CCS.
- **Gateway Registration:** After receiving the message $M_{Ui \rightarrow g_i N}$ from the user U_i, the gateway node $g_i N$ will send its public key $K_{public}(g_i N)$ and certificate $Cert(g_i N)$ encrypted by the user public key $K_{public}(U_i)$. i.e The gateway node $g_i N$ sends message $M_{g_i N \rightarrow CCS} = \{K_{public}(g_i N), \varepsilon(Cert(g_i N))\}$ to CCS. Where ε is the encryption process.

User Registration

U_i will send $\{K_{public}(U_i), \eta\}$ to $g_i N$.

U_i will generate $Vid(U_i)$.

Gateway Registration

$g_i N$ will encrypt $Cert(g_i N)$ by $K_{public}(U_i)$.

$g_i N$ will send $K_{public}(g_i N)$, $\varepsilon(Cert(g_i N))$ to CCS.

IoT Registration:

D_i will encrypt $Id(D_i)$ by $K_{public}(CCS)$.

CCS will verify $Id(D_i)$.

CCS generate R_2 and send it to D_i.

D_i calculate $h_3 \rightarrow \{R_2 \parallel Id(D_i)\}$.

D_i send h_3 to CCS.

CCS encrypt h_3 by $K_{private}(CCS)$.

Fig. 2. Steps Performed in the Registration Phase

- **IoT Registration:** The IoT device D_i will send its identity $Id(D_i)$ encrypted with the public key of CCS $K_{public}(CCS)$ and sent it through a secure channel. CCS will verify the Identity $Id(D_i)$ received after decryption and generate a random number R_2 and send it to he IoT device D_i. D_i calculate the hash value $h_3 \rightarrow \{R_2 \parallel Id(D_i)\}$, which is basically the concatenation of the generated random number R_2 and Identity $Id(D_i)$ of the IoT device D_i. Now the IoT device D_i send the message $M_{D_i \rightarrow CCS} = \{h_3\}$ to CCS. CCS will encrypt this hash value h_3 with its private key $K_{private}(CCS)$ and send that to through a secure channel while the random number is stored in the database.

The overall steps in the registration process was presented in fig. 2.

C. Mutual Authentication Phase

On getting the authentication request message A_{req}, verification takes place between user to gateway, gateway to cloud, cloud to IoT and IoT to user sequentially.

- **User to Gateway Authentication:** To start the communication between any user U_i and IoT device D_i, an authentication request message A_{req} is generated and broadcasted to the nearby gateway nodes $g_i N$.

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

Before starting the authentication process, the gateway nodes $g_i N$. will calculate the following:

$$R_2' = R_2.G \quad (1)$$

$$Z = h_4(R_2' \| \eta) \quad (2)$$

$$Vid(U_i)' = h_5\{Vid(U_i) \| \eta\} \quad (3)$$

The gateway nodes $g_i N$ will perform hashing of all the above calculated values as $h_6 = h(R_2' \| Z \| Vid(U_i)' \| \eta)$. Now The gateway nodes $g_i N$ send the message $M_1 = \{h_6, R_2', Z, Vid(U_i)', \eta\}$ to CCS.

- **Gateway to CCS Authentication:** On receiving the message M_1, CCS will verify R_2 through its database and confirm that the gateway node $g_i N$ is genuine. After that it will generate another random number R_3 and calculate the secret key Sk as:

$$Sk = \eta' + R_3 \quad (4)$$

$$Sk' = h(\eta' + R_3) \quad (5)$$

$$Sk'' = Sk'.R_3 + K_{public} (\mathrm{mod}\, \eta') \quad (6)$$

Now CCS will perform hashing of the obtained secret key values as $h_7 = h(Sk \| Sk'' \| \eta')$ and send the message $M_2 = \{h_7, Sk', Sk'', \eta'\}$ to the gateway nodes $g_i N$. Then the gateway node $g_i N$ will verify the CCS. For this, the gateway node $g_i N$ will compare the nonce received with the one it has sent. If nothing goes wrong, it will calculate the public key K_{public} and private key $K_{private}$ with the help of the secret key Sk received. CCS will be aware of how the public key K_{public} will be calculated. Thus it will calculate on its own. Thus there is no need to send the public key K_{public} over an insecure channel. At the same time, the private key $K_{private}$ will be secretly derived with the help of a secret key Sk generated. And even the CCS won't have any clue about it. The gateway node $g_i N$ will generate another nonce η_1 and timestamp TS_1. Reminder Public key K_{public} must be calculated utilizing the values available on both sides so that it will be calculated on either side without any hassle. Now the gateway node $g_i N$ will perform the following hash operation.

$$h_8 = h(\eta_1 \,|\, TS_1) \quad (7)$$

Now the gateway node send the message $M_3 = \{h_8, \eta_2, TS_1\}$ to CCS. CCS will calculate the difference in the timestamp and store it in TS_2.

- **CCS to IoT Authentication:** Using the private key of CCS, the IoT device D_i will generate a certificate $C = \{a, dc\}$ which cannot be determined by any other. So, the IoT device D_i having this certificate C is assumed to be a genuine one. The certificate value C can be calculated as follows:

$$a = R_2.G \Rightarrow y = \frac{a}{dc} \quad (8)$$

$$x = \frac{nonce\,received}{dc} \Rightarrow \frac{h(\eta_1')}{dc} \quad (9)$$

$$a = x.G + y.K_{public} \quad (10)$$

Sub Eqn (8), (9) in (10) $$a = \frac{h(\eta_1')}{dc} G + \frac{a.((K_{private}.G)}{dc} \quad (11)$$

From Eqn (8) $$R_2.G = \frac{(\eta_1').G}{dc} + \frac{a.((K_{private}.G)}{dc} \quad (12)$$

$$R_2.G = \frac{(\eta_1').G + a.((K_{private}.G)}{dc} \quad (13)$$

$$dc = \frac{(\eta_1').+ a.(K_{private}.)}{R_2} \quad (14)$$

CCS send TS_3 to the end user U_i and grant access for communication between the user U_i and IoT device D_i, if the IoT device D_i is genuine.

- **IoT to User Authentication:** After receiving the access from CCS, the user U_i will verify the IoT device D_i and send its id $Id(U_i)$ encrypted with the public key of IoT device $K_{public}(D_i)$, which it has received in the previous message. The user U_i will keep this virtual id $Vid(U_i)$ for later communications. The user U_i will verify the id of the IoT device $Id(D_i)$. The user U_i will generate the corresponding virtual id $Vid(D_i)$ only if the IoT device D_i is verified and start further communication between the user U_i and the IoT device D_i . Fig. 3 shows the overall steps performed in the authentication process.

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

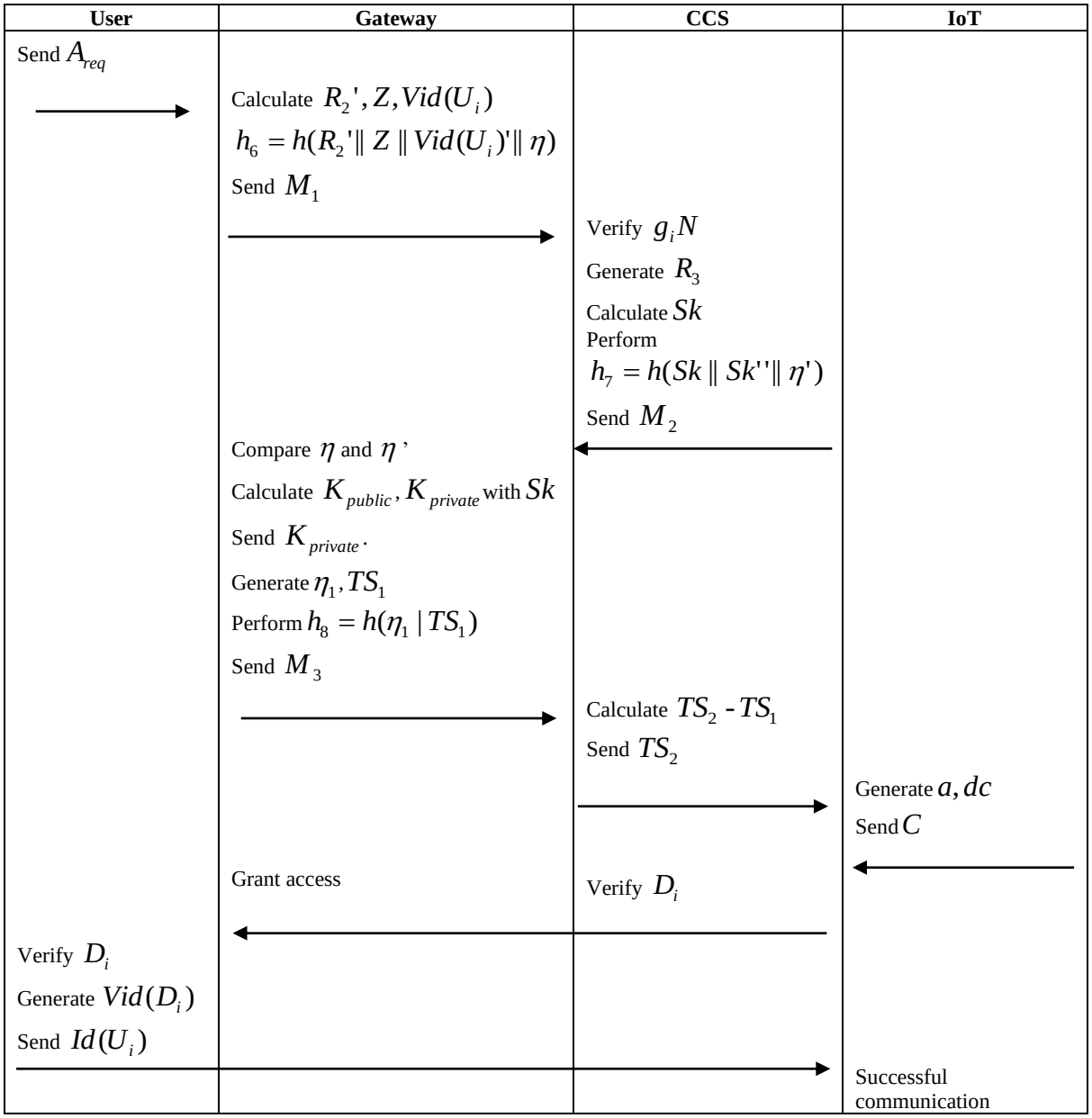

Fig. 3. Steps in the Mutual Authentication Phase.

D. Update phase

In the update phase, the identity Id_i of the user U_i , gateway node $g_i N$ and IoT device D_i ought to be re-registered and thus it tests the antique certificate and virtual identity in the database, and modification is made on the earlier verification manner within the entities.

V. SECURITY ANALYSIS

In this segment, we've got offered the security analysis evidence of LWMA–CIoT scheme. We have completed each formal and casual security evaluation on this section. In addition, we have also analysed the performance of the LWMA–CIoT authentication scheme the use of the simulation effects.

A. Formal Security Analysis

Formal protection evaluation is completed using BAN logic it truly is designed to cryptographic protocols efficiently. It gives interpretation approximately conviction taken by way of the use of the occasions which can be engaged inside the protocols. There are all collectively 4-level in the manner. In the primary stage, the protocol is written and organized in the right steps. This step is known as the idealization of the protocol. In the following step, we want to come to be aware about the set of assumptions and try to explicit them formally. These formal assumptions have to keep if you want to acquire the desires. After that, we need to grow to be aware of the capabilities of the protocol and expressed it formally. Finally, we have to construct proof, with the help of inference policies, to expose that the dreams may be finished thru the usual assumptions.

a. Notations of BAN logic

The following notations are used in the BAN logic.

- $A \mid\equiv B$: *A believes in message* B
- $A \lhd B$: *message* B *is visible to* A
- $A \mid\sim B$: A *once said* B
- $A \Rightarrow B$: *A controls* B
- $< B > N$: *Message* B *is combined with N*

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

- $A \xleftrightarrow{k} Y$: *A and Y communicate through shared key SK*
- $\{B\}_K$ *: Message* B *is encrypted by N*
- $\#B$ *:* B *is a fresh message*

b. Postulates of BAN logic

Freshness rule: If A believes that B is fresh, then the A believes that the entire formula must be fresh. $A \mid\equiv \#(B) / A \mid\equiv \#(B, N)$.

- Trust Rule: If the principle A believes that believes (B , N), then A and believes (B). $A \mid\equiv (B, N) / A \mid\equiv B$.
- Message meaning Rule: If A believes that K is shared with and sees (B)K , then Y sometimes sent message including $B \,.\, A \mid\equiv A \xleftrightarrow{k} Y, A \lhd \{B\}_K / A \mid\equiv Y \mid\sim B$.
- Jurisdiction Rule: If A believes that has jurisdiction over B and A believes that Y believes B , then A believes B is true. $A \mid\equiv Y \Rightarrow B, A \mid\equiv Y \mid\equiv B / A \mid\equiv B$.
- Nonce verification rule: If A believes B is fresh and A believes that once said, then A believes that Y believes $B \,.\, A \mid\equiv (B, A \mid\equiv Y \mid\sim B / A \mid\equiv Y \equiv B$
- Seeing Rule: If A believes that K is shared with Y and sees B is encrypted under $N''.\, A \mid\equiv A \xleftrightarrow{k} Y, A \rhd \{A\}_K / A \rhd B$

c. Transmitted messages of BAN logic

- $g_i N \rightarrow CCS : M_1 = \{h_6, R_2', Z, Vid(U_i)', \eta\}$
- $CCS \rightarrow g_i N : M_2 = \{h_7, Sk', Sk'', \eta'\}$
- $g_i N \rightarrow CCS : M_3 = \{h_8, \eta_2, TS_1\}$

d. Assumptions of BAN logic

- $A_1 : g_i N \mid\equiv \#(R_2)$
- $A_2 : g_i N \mid\equiv \#(R_3)$
- $A_3 : CCS \mid\equiv \#(R_2)$
- $A_4 : CCS \mid\equiv \#(R_3)$
- $A_5 : CCS \mid\equiv CCS \xleftrightarrow{Sk'} g_i N$
- $A_6 : g_i N \mid\equiv CCS \xleftrightarrow{Sk'} g_i N$
- $A_7 : CCS \mid\equiv CCS \xleftrightarrow{Sk''} g_i N$
- $A_8 : g_i N \mid\equiv CCS \xleftrightarrow{Sk''} g_i N$
- $A_9 : g_i N \mid\equiv CCS \xleftrightarrow{R_2} CCS$
- $A_{10} : CCS \mid\equiv CCS \xleftrightarrow{R_2} g_i N$
- $A_{11} : g_i N \mid\equiv CCS \xleftrightarrow{TS_1} CCS$
- $A_{12} : CCS \mid\equiv CCS \xleftrightarrow{TS_1} g_i N$

e. Security Goals of BAN logic

- **Goal 1:** $g_i N \mid\equiv g_i N \xleftrightarrow{Sk} CCS$
- **Goal 2:** $CCS \mid\equiv g_i N \xleftrightarrow{Sk} CCS$
- **Goal 3:** $g_i N \mid\equiv CCS \mid\equiv g_i N \xleftrightarrow{Sk} CCS$
- **Goal 4:** $CCS \mid\equiv g_i N \mid\equiv g_i N \xleftrightarrow{Sk} CCS$

f. Verification Steps of BAN logic

Applying the seeing rule to M_1,

- **Step 1**: $g_i N \lhd \{h_6, R_2', Z, Vid(U_i)', \eta\}$

Combining the nonce verification rule, A_1 & A_3 to step 1,

- **Step 2**: $g_i N \mid\equiv g_i N \mid\sim \{h_6 \langle R_2', Z, Vid(U_i)', \eta \rangle_{K_{public}}\}$

Using step 2, Jurisdiction rule, A_5 & A_7 we can say $g_i N \mid\equiv \eta$ and $g_i N \mid\equiv \#\eta$

- **Step 3:** $g_i N \mid\equiv g_i N \xleftrightarrow{Sk''} CCS$ [Goal 1 achieved]

On incorporating step 1 with nonce verification rule and assumption A_1, A_6 & A_8, we can write

- **Step 4:** $\dfrac{g_i N \mid\equiv CCS \Rightarrow Sk'', g_i N \mid\equiv CCS \mid\equiv Sk''}{g_i N \mid\equiv Sk''}$ [Goal 2 achieved] [By nonce verification rule, freshness rule and assumption A_1, A_2, A_3 & A_4].

With belief rule we can say $g_i N \mid\equiv CCS \mid\equiv R_3$. And using step 1, step 2 along with freshness rule we can deduce:

- **Step 5:** $\dfrac{g_i N \mid\equiv \#(R_2), g_i N \mid\equiv CCS \mid\sim Sk}{g_i N \mid\equiv CCS \mid\equiv Sk''}$ [Goal 3 achieved]

On applying message meaning rule and A_{10}, we can write

- **Step 6:** $\dfrac{g_i N \mid\equiv CCS \xleftrightarrow{K_{public}} g_i N, g_i N \lhd \{A\}_{K_{public}}}{g_i N \mid\equiv CCS \mid\sim R_2}$ [Goal 4 achieved]

B. Informal Security Analysis

In this section, will analyse the security features of our proposed LWMA–CIoT scheme with respect to earlier mentioned design goals.

- **Confidentiality:** In this authentication scheme, the only virtual identity of the users is used. Secondly, the personal key is not generated with the aid of the usage of any unmarried authority. So no matter the fact that the important authority receives compromised,

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

it gained that be capable of derive customers' personal keys. Apart from that, all transmitted information is typically encrypted over the insecure channel. Even in any case this, an adversary is capable of intercept the transmitted message. It will end up getting the nonce and timestamp, with a purpose to of no want. Hence, the proposed LWMA–CIoT scheme guarantees the confidentiality of records for the duration of the entire conversation.

- **Integrity:** In order you acquire the integrity of the information in communication, it want to be ensured that the data isn't always altered sooner or later of its transmission.

It isn't always that smooth for an adversary to reap the private key with the aid of using compromising the CCS. Since each users, in addition to the verifier thriller keys, are concerned in generating the non-public key. Thus, messages can't be intercepted or tampered. The adversary won't be capable of recognize with whom the communication is going on. Additionally, it will price some thing for performing those operations (tampering) with little or no advantage for the adversary. Hence, the integrity of messages is ensured.

- Anonymity: To obtain anonymity, inside the proposed LWMA–CIoT scheme, in choice to the actual identities of the talking activities, digital identification is used, that is generated with the aid of pseudonym cryptographic function. An adversary can't obtain the real identities as it's miles calculated by means of taking two halves from Verifier and person. In addition to the digital identification is encrypted with a one-way hash characteristic. Thus, it preserves anonymity property.
- Non-interactivity: The surrender word needs to get confirmed by means of using the node genuinely above it within the hierarchy. There is no need to ship extra messages for getting access to services. Only one message, i.e., the authentication request, is sent, as a result making it non-interactive.
- Traceability: The LWMA–CIoT scheme uses the digital Id, this is the mixture of its actual identification and a random range. This actual identification can be the MAC deal with (IP deal with or something), which modifications due to change inside the community. This way, traceability can be finished.
- Replay attack: In this LWMA–CIoT authentication scheme, we have were given used smooth nonce at the start of the consultation. Even the timestamp is also used to mark the restriction of the session. Hence, the attacker will not be able to repeat the vintage messages for purchasing new access. Therefore, the LWMA–CIoT authentication scheme is relaxed in the direction of the replay attack.
- User impersonation attack: As said above, if an attacker attempts a login attempt by means of sending the digital identity and freshly generated nonce to the Verifier. The Verifier will then flag secure pleasant after the a success validation that the asked customer is legitimate. However, if the attacker tries to impersonate the consumer after verifying the message, the latter part of the communique might be done the use of the individual's non-public key. The attacker has no knowledge approximately this key as each events have been worried in producing the non-public key. So compromising all and sundry party received display screen the secret, and the information obtained from one party is probably nugatory as nicely. Thus, stopping impersonation attacks.
- Man-in-the middle attack: Suppose an eavesdropper intercepts the communique some of the events and in some time try and adjust that intercepted message in such a way that it may get get right of entry to. For doing so, it (eavesdropper) has to deliver its credentials if attempted for login access. In case the eavesdropper favoured to take over the session after the client has been granted access, then additionally he should require the call of the sport personal key of the man or woman to keep on the communique. Likewise, no different messages might be regenerated thru the attacker, which may be used in the procedure of authentication. Hence it proves that the LWMA–CIoT authentication scheme is resilient towards a man-in-the-center attack.
- Privileged-insider attack: The vital authority does no longer keep any statistics about the individual. So, there can be no chance of an insider attack.
- Brute-force attack: In our authentication scheme, no mystery key or password is used. Additionally, all of the communications is secured the use of SHA-2. Leaving no threat for attack to get up. As the brute-pressure attack will only attain fulfilment if enough time is given and with every extra bit of key period, time to perform the attack doubles.

VI. PERFORMANCE ANALYSIS AND COMPARISON

In this segment, we've got offered the performance evaluation of the proposed LWMA–CIoT scheme is achieved in terms of verbal exchange and computation fees. In addition we've also compared the performance of the proposed LWMA–CIoT scheme with a few current strategies.

A. Computation Cost

Computation plays a vital feature in identifying the rate and real-time execution of the protocol. It is crucial to study the overall performance of the LWMA–CIoT scheme the use of computational power. Thus, any authentication scheme's computational rate can be defined due to the fact the sum of all the operations that considerably have an impact on the rate and effect. Because of the regulations of IoT devices, extremely good care has been taken to layout the proposed protocol. To make it light-weight, simple capabilities like hash functions are used, it really is green and fast. In Table II, we've got compared the cryptographic capabilities of the proposed scheme with the current studies papers.

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

Table–II: Comparison in terms of Cryptographic function used

Scheme	Cryptographic Operations Used	Registration Phase	Authentication Phase
[25]	Hashing, Exclusive OR operation	$6T_{hash} + 3T_{XOR}$	$30T_{hash} + 30T_{XOR}$
[26]	Elliptic Curve Multiplication, Hashing	$2T_{hash}$	$9T_{hash} + 6T_{multi}$
[27]	Hashing	$4T_{hash}$	$13T_{hash}$
[28]	Hashing, Elliptic Curve Multiplication	$T_{hash} + T_{multi}$	$12T_{hash} + 5T_{multi}$
[29]	Hashing, Elliptic Curve Multiplication	$7T_{hash} + 2T_{multi}$	$28T_{hash} + 3T_{multi}$
[30]	Hashing, Elliptic Curve Multiplication	$4T_{hash} + T_{multi}$	$13T_{hash} + 3T_{multi}$
[31]	Hashing, Elliptic Curve Multiplication	$6T_{hash} + 2T_{multi}$	$12T_{hash} + 6T_{multi}$
[32]	Hashing, Elliptic Curve Multiplication	$T_{hash} + T_{multi}$	$6T_{hash} + 5T_{multi}$
LWMA–CIoT	Hashing	$3T_{hash}$	$5T_{hash}$

In table II, the compared schemes only use hashing, Elliptic Curve Multiplication operation and exclusive OR as cryptographic functions. A single hashing operation consume 0.063ms as computation time, A single Elliptic Curve Multiplication operation require 15.57ms as computation time and a single Exclusive OR operation require 2.3 ms as computation time. Using these computation time, we can evaluate the total computation cost of each authentication scheme compared in table II. Table III shows the total computation cost of comparison.

Table–III. Computation Cost Comparison

Scheme	Total cryptographic operation	Computation cost (ms)
[25]	$36T_{hash} + 33T_{XOR}$	78.168
[26]	$11T_{hash} + 6T_{multi}$	94.113
[27]	$17T_{hash}$	1.071
[28]	$13T_{hash} + 6T_{multi}$	94.239
[29]	$35T_{hash} + 5T_{multi}$	80.055
[30]	$17T_{hash} + 4T_{multi}$	63.351
[31]	$13T_{hash} + 5T_{multi}$	78.669
[32]	$7T_{hash} + 6T_{multi}$	93.861
LWMA–CIoT	$8T_{hash}$	0.504

The proposed LWMA–CIoT scheme uses only Hashing functions during registration and authentication phase. This requires a computation cost of 0.504ms which is much smaller compared to the computation cost of other compared schemes in table III. This proves the significance of the proposed LWMA–CIoT scheme over existing schemes.

B. Communication Cost

Communication charge is calculated by way of including the complete numbers of messages and size (in bits) communicated to conduct the entire manner of authentication. So a good way to locate the fee of verbal exchange, we need to measure the scale of the messages communicated during the execution (i.e. Registration segment and authentication segment). For calculating the schemes' conversation cost, we've got assumed that the duration of the random quantity, nonce, identification, virtual-identity, and the elliptic curve's protection parameter is one hundred sixty bits. Also, we have assumed the period of the timestamp to be identical to 32 bits. We have used the SHA-2 hash characteristic whose message digest is 256 bits.

Table–IV: Communication Cost comparison

Scheme	Number of bits Used		Total number of messages transmitted	Communication cost (bits)
	Registration Phase	Authentication Phase		
[25]	320	5536	4	5856
[26]	480	1632	4	2112
[27]	640	4320	4	4960
[28]	192	3584	2	3776
[29]	544	2272	3	2816
[30]	448	5632	3	6080
[31]	696	3464	4	4160
[32]	416	2784	3	3200
LWMA–CIoT	416	2784	3	3200

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

Table IV suggests the cost involved when the proposed scheme executes as quickly as. As the network maintain to growth and more quantity of gateway node further to IoT devices is probably delivered and for this reason the rate will increase steadily. From table IV, the conversation charge for [25] is 5856 bits, [27] is 4960 bits, [30] is 6080 bits and proposed LWMA–CIoT scheme is 3200 bits for concluding the scheme as soon as. So, while it occurs to run one thousand instances rate may be 732 Kb, 620 Kb, 760 Kb and four hundred Kb respectively. Difference with appreciate to every scheme is 332 Kb, 220 Kb and 360 Kb respectively which is nearly two instances. So, the proposed LWMA–CIoT scheme can be cost effective.

C. Security Characteristics

The security and functionality features of the proposed LWMA–CIoT scheme and other related schemes are compared in Table V.

Table–V: Security features of the proposed LWMA–CIoT scheme

Security requirements	[21]	[22]	[23]	[24]	LWMA–CIoT
User anonymity	Yes	Yes	No	Yes	Yes
Intractable	Yes	No	No	No	Yes
Forgery Attack	Yes	No	Yes	Yes	Yes
Replay Attack	Yes	Yes	No	Yes	Yes
Impersonation Attack	Yes	No	Yes	Yes	Yes
Mutual Authentication	Yes	Yes	No	Yes	Yes
Man in middle Attack	Yes	Yes	Yes	Yes	Yes
Dictionary Attack	No	Yes	No	No	Yes
Forward Secrecy	Yes	No	Yes	No	Yes
DOS attack	Yes	Yes	Yes	Yes	Yes
Masquerade attack	No	Yes	No	Yes	Yes
Server spoofing attack	Yes	Yes	No	Yes	Yes
login phase verification	No	No	No	No	Yes
Information validation	Yes	No	Yes	No	Yes
Replay protection	No	Yes	No	Yes	Yes

Table V indicates that our protocols offers aided safety functions and is powerful in opposition to a few protection attacks which include impersonation, replay, and many others. Except paper [23] used for contrast has hired Mutual Authentication and is taken into consideration for replay and Man within the Middle Attack. Except for paper [22], all the papers have secured their proposed protocol closer to impersonation attack.

Other than our proposed scheme not one of the paper is resilient in opposition to the Brute-strain attack, Dictionary Attack, and does not have login verification.

D. Simulation Results

We have implemented the proposed scheme in the Windows 10 operating system, with an internal memory of 8.0GB and 4 GHz configuration capability. We use MATLAB software for simulation. The other parameters used for simulation is given in table VI.

Table–VI: Simulation Parameters

Parameters	Description
Routing Protocol	AODV
Radio Range	300 m
Number of gateway nodes	5
Number of users	100
Number of IoT device	50
Simulation time	30 minutes
Communication Range	50m
Data Rate	6 Mbps Packet
Payload	152 bytes

The performance of the proposed LWMA–CIoT scheme is evaluated in terms of end to end delay, throughput and packet delivery ratio (PDR) and presented in table VII.

Table–VII: Simulation Results

Parameters	Values
E2E delay	8.652900e-03
Throughput	25580
Packet Delivery Ratio (PDR)	9.800000e-01

The simulation time is taken as 1800 seconds, which is the actual total time. From table VII, it's far stated that the throughput of the proposed LWMA-CIoT scheme is 25580 bps due to the fact the proposed scheme uses small-sized messages which result in less communication overhead for authentication in comparison to other schemes which growth the significance and throughput of the proposed scheme. Similarly from table VII, the E2ED of LWMA-CIoT is very much less as eight.652900e-03 ms. Which is resulted through the use of small-sized messages for authentication reason.

VII. CONCLUSION

In this paper, we've got provided a completely unique authentication scheme to ensure protection in IoT based totally cloud surroundings. So, that a light-weight, scalable, and espresso-price authentication scheme (LWMA–CIoT) with the aid of using using the standards of Identity-based totally encryption and mutual authentication grow to be proposed. Since this technique neither requires bilinear pairing during encryption nor save any keys or ID's which makes.

it appropriate for useful resource and electricity-constrained devices at an much less luxurious price. Such a scheme is applicable to conditions wherein scalability is demanded. Formal and casual safety analysis changed into accomplished in this paper to show the superioty of the proposed LWMA–CIoT scheme. The analytical outcomes display that the proposed scheme plays on par with the prevailing authentication scheme without compromising the protection level.

REFERENCES

1. M. S. Farash, M. Turkanovic, S. Kumari, and M. Holbl. 2016. An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the internet of things environment. Ad Hoc Netw. 36 (2016), 152.
2. Anwar Ghani, Khwaja Mansoor, Shahid Mehmood, Shehzad Ashraf Chaudhry, Arif Ur Rahman, and Malik Najmus Saqib. 2019. Security and Key Management in IoT based wireless sensor networks: an authentication protocol using symmetric key. Int. J. Commun. Syst. 32 (2019), 16.
3. [Rajesh Gupta, Sudeep Tanwar, Sudhanshu Tyagi, and Neeraj Kumar. 2019. Tactile internet and its applications in 5G era: A comprehensive review. Int. J. Commun. Syst. 32 (2019), 14.
4. Rajesh Gupta, Sudeep Tanwar, Sudhanshu Tyagi, and Neeraj Kumar. 2020. Machine learning models for secure data analytics: a taxonomy and threat model. Comput. Commun. 153 (2020), 406–440.
5. R. Amin, N. Kumar, G. Biswas, R. Iqbal, and V. Chang, "A light weight authentication protocol for iot-enabled devices in distributed cloud computing environment," Future Generation Computer Systems, Vol. 78, pp. 1005–1019, 2018.
6. U. Satapathy, B. K. Mohanta, D. Jena, and S. Sobhanayak, ''An ECC based lightweight authentication protocol for mobile phone in smart home,'' in Proc. IEEE 13th Int. Conf. Ind. Inf. Syst. (ICIIS), Rupnagar, India, Dec. 2018, pp. 1–6.
7. L. Zhou, X. Li, K.-H. Yeh, C. Su, and W. Chiu, "Lightweight iot-based authentication scheme in cloud computing circumstance," Future Generation Computer Systems, Vol. 91, pp. 244–251, 2019.
8. R. Amin, S. Kunal, A. Saha, D. Das, and A. Alamri, "Cfsec: password based secure communication protocol in cloudfog environment," J. Parallel. Distrib. Comput., Vol. 140, pp. 52–62, 2020.
9. M. Wazid, A. K. Das, V. Bhat, and A. V. Vasilakos, "Lamciot: lightweight authentication mechanism in cloud-based iot environment," Journal of Network and Computer Applications, Vol. 150, pp. 102496, 2020.
10. P. Soni, A. K. Pal, and H. SK Islam, ''An improved three-factor authentication scheme for patient monitoring using WSN in remote healthcare system,'' Comput. Methods Programs Biomed., vol. 182, Dec. 2019, Art. no. 105054.
11. Y. Dodis, L. Reyzin, and A. Smith, ''Fuzzy extractors: How to generate strong keys from biometrics and other noisy data,'' in Proc. Int. Conf. Theory Appl. Cryptograph. Tech., Interlaken, Switzerland, 2004, pp. 523–540.
12. D. Wang, H. Cheng, P. Wang, X. Huang, and G. Jian, ''Zipf's law in passwords,'' IEEE Trans. Inf. Forensics Security, vol. 12, no. 11, pp. 2776–2791, Nov. 2017.
13. S. J. Yu, J. Y. Lee, K. K. Lee, K. S. Park, and Y. H. Park, ''Secure authentication protocol for wireless sensor networks in vehicular communications,'' Sensors, vol. 18, no. 10, pp. 3191–3214, 2017.
14. K. Park, Y. Park, A. K. Das, S. Yu, J. Lee, and Y. Park, ''A dynamic privacypreserving key management protocol for V2G in social Internet of Things,'' IEEE Access, vol. 7, pp. 76812–76832, 2019.
15. Run-Fa Liao, Hong Wen, Jinsong Wu, Fei Pan, Aidong Xu, Huanhuan Song, Feiyi Xie, Yixin Jiang, and Minggui Cao. Security enhancement for mobile edge computing through physical layer authentication. IEEE Access, 7:116390–116401, 2019.
16. Singh, Sunakshi, and Vijay Kumar Chaurasiya. "Mutual authentication scheme of IoT devices in fog computing environment." Cluster Computing 24, no. 3 (2021): 1643-1657.
17. Lee, Hakjun, Dongwoo Kang, Youngsook Lee, and Dongho Won. "Secure three-factor anonymous user authentication scheme for cloud computing environment." Wireless Communications and Mobile Computing 2021 (2021).
18. B. Hammi, A. Fayad, R. Khatoun, S. Zeadally and Y. Begriche, "A Lightweight ECC-Based Authentication Scheme for Internet of Things (IoT)," in *IEEE Systems Journal*, vol. 14, no. 3, pp. 3440-3450, Sept. 2020, doi: 10.1109/JSYST.2020.2970167.
19. Sadhukhan, Dipanwita, Sangram Ray, G. P. Biswas, Muhammad Khurram Khan, and Mou Dasgupta. "A lightweight remote user authentication scheme for IoT communication using elliptic curve cryptography." The Journal of Supercomputing 77, no. 2 (2021): 1114-1151.
20. Yu, Sungjin, Namsu Jho, and Youngho Park. "Lightweight Three-Factor-Based Privacy-Preserving Authentication Scheme for IoT-Enabled Smart Homes." IEEE Access 9 (2021): 126186-126197.
21. Ibrahim, M.H.: Octopus: an edge-fog mutual authentication scheme. IJ Netw. Secur. 18(6), 1089–1101 (2016).
22. Amor, A.B., Abid, M., Meddeb, A.: A privacy-preserving authentication scheme in an edge-fog environment. In: 2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA), pp. 1225–1231. IEEE (2017).
23. Arij, B. E. N., Mohamed, A. B. I. D., and MEDDEB, A.: CASK: conditional authentication and session key establishment in fogassisted social IoT network. In: 2019 15th International Wireless Communications and Mobile Computing Conference (IWCMC), pp. 114–119. IEEE (2019).
24. Pardeshi, M.S., Yuan, S.M.: SMAP fog/edge: a secure mutual authentication protocol for fog/edge. IEEE Access 7, 101327–101335 (2019).
25. Zhou, L., Li, X., Yeh, K.H., Su, C., Chiu, W.: Lightweight IoTbased authentication scheme in cloud computing circumstance. Future Gener. Comput. Syst. 91, 244–251 (2019) .
26. Yeh, H.L., Chen, T.H., Liu, P.C., Kim, T.H., Wei, H.W.: A secured authentication protocol for wireless sensor networks using elliptic curves cryptography. Sensors 11(5), 4767–4779 (2011) .
27. Shi, W., Gong, P.: A new user authentication protocol for wireless sensor networks using elliptic curves cryptography. Int. J. Distrib. Sens. Netw. 9(4), 730831 (2013) .
28. Xu, X., Zhu, P., Wen, Q., Jin, Z., Zhang, H., He, L.: A secure and efficient authentication and key agreement scheme based on ECC for telecare medicine information systems. J. Med. Syst. 38(1), 9994 (2014) .
29. Wazid, M., Das, A.K., Kumar, N., Vasilakos, A.V.: Design of secure key management and user authentication scheme for fog computing services. Future Gener. Comput. Syst. 91, 475–492 (2019)
30. Dhillon, P.K., Kalra, S.: A secure multi-factor ECC based authentication scheme for Cloud-IoT based healthcare services. J. Ambient Intell. Smart Environ. 11(2), 149–164 (2019)
31. Li, H., Li, F., Song, C., Yan, Y.: Towards smart card based mutual authentication schemes in cloud computing. KSII Trans. Internet Inform. Syst. 9(7), 2719–2735 (2015).
32. Singh, Sunakshi, and Vijay Kumar Chaurasiya. "Mutual authentication scheme of IoT devices in fog computing environment." Cluster Computing 24, no. 3 (2021): 1643-1657.

AUTHORS PROFILE

M.R.Sheeba obtained her Bachelor's degree in Computer Science from St.Mary's College, Tuticorin. Then she obtained her Master's degree in Computer Applications from V.V. Vannaiaperumal College, Virudhunagar. She has also obtained Masters Degree in Computer Science and Engineering from Rajalakshmi Engineering College, Chennai. Currently, she is doing her research in St.Xavier's College, Palayamkottai. Her research interests are Grid Computing, Cloud Computing, Internet of Things. email: sheebajustus@gmail.com.

Dr. G.Suganthi received M.Sc degree from Madurai Kamaraj University and M.Phil from Mother Teresa University. She obtained her Ph.D. degree from the Manonmaniaum Sundaranar University, Tirunelveli. She is working as Associate Professor in the Department of Computer Science, Womens Christian College, Nagercoil. She is Guiding Ph.D. Scholars. She has presented 25 papers in National and International conferences and published 16 papers in International Journals. She has authored 5 books. She received awards namely Shiksha Rattan Pureskar in October 2012 at New Delhi and Best Citizen Award by International publishing house, New Delhi in February 2013.She has also received Best Researcher and Innovative Researcher in Image Processing Award for her excellent Research Activities. Her area of specialization Parallel Processing, Image Processing, Internet Security. email: dr_suganthi_wcc@yahoo.co.in

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