ECC based Authentication Approach for Secure Communication in IoT Application

S. Thanga Revathi[1*], A. Gayathri[2], A. Sathya[3] and M. Santhiya[4]

[1*] Assistant Professor, Department of Networking and Communications, School of Computing, SRM Institute of Science and Technology, Chennai, India. thangarevathi84@gmail.com, Orcid: https://orcid.org/0000-0003-1518-006X

[2] Professor, Department of Computer Science and Engineering, Saveetha School of Engineering, SIMATS, Chennai, India. gaybalahari@gmail.com, Orcid: https://orcid.org/ 0000-0002-2533-2357

[3] Associate Professor, Department of Artificial Intelligence and Data Analytics, Sri Ramachandra Faculty of Engineering and Technology, Chennai, India. arunachalam.sathya@gmail.com, Orcid: https://orcid.org/0000-0001-9930-0836

[4] Assistant Professor, Department of Computer Science and Engineering, Rajalakshmi Engineering College, Chennai, India. santhiyamunusamy@gmail.com, Orcid: https://orcid.org/0009-0002-1617-178X

Received: July 22, 2023; Accepted: September 27, 2023; Published: November 30, 2023

Abstract

Internet of Things (IoT) is an advanced applied science in recent years that enables communication among humans and smart components or among Internet-based components. Besides, IoT provides affiliation of physical and virtual elements that are fully controlled by different kinds of hardware, software, and interaction advancements. Though numerous methods of IoT offer many advantages to our day-to-day routine, it also possesses huge security weaknesses. The traditional methods are vulnerable to a huge range of attacks. Hence, establishing safe and effective security alternatives for the IoT environment remains as a main challenge and the major risk in this security solution is to transfer significant information in a secure manner. To address such limitations, an effective authentication approach named CHEK-based authentication methodology is devised for secure communication in IoT. The proposed authentication scheme consists of four steps and the authentication approach is developed by considering various security operations like hashing, encryption, secret key pairs, passwords, and so on. Moreover, the CHEK-based authentication scheme provides promising solution with minimum computational cost of 16.541 and minimum memory usage of 72.3MB.

Keywords: Internet of Things (IoT), Authentication, One Time Password (OTP), Chebyshev Polynomial.

1 Introduction

The IoT is a framework of interconnected components that enables components to interact among each device to communicate data transferring over a network without any manual intervention. Indeed, this

Journal of Internet Services and Information Security (JISIS), volume: 13, number: 4 (November), pp. 88-103. DOI: *10.58346/JISIS.2023.I4.006*

*Corresponding author: Assistant Professor, Department of Networking and Communications, School of Computing, SRM Institute of Science and Technology, Chennai, India.

advanced technology improves the human's daily life by offering better structure for other concepts, namely Internet of Energy (IoE), Internet of Vehicles (IoV), Machine to Machine communication (M2M), and Internet of Sensors (IoS) (Kotenko, I.V., 2017). By integrating IoT with Artificial Intelligence (AI) and deep learning techniques has delivered many opportunities. Nevertheless, the interconnected model of data flow also has many limitations (Chou, W., 2002) (Mandala, J., 2019). Since IoT is a diverse structure, there is no chance to utilize such general alternatives due to the limited elements that are joined to this structure, such as WSN nodes and RFID tags. To address certain limitations, analysts tried to design a lightweight protocol for the IoT model. Among them, authentication and session key agreement protocol has gained more focus and has become a hot research topic among researchers. Though IoT offers many merits to humans in their daily routine, it possesses huge privacy attacks. The ultimate risk in IoT is transferring of crucial information over the network in a secure way (Safkhani, M., 2020) (Mahalle, P.N., 2013) (Shivraj, V.L., 2015) (Chen, Y., 2018). The two prime technologies for IoT security are secret key storage and device authentication. Existing key generation and authentication approaches are mainly dependent on conventional cryptography that offers high-cost secret key storage and high-level complication of cryptographic techniques (Garg, S., 2019) (Miranda, C., 2020) (Pakniat, N., 2020) (Zhang, J., 2021). Most of the techniques depend on a one-factor authentication approach, which is a privacy threat in some scenarios (Anandkumar, M., 2020) (Mahalle, P.N., 2013).

One-Time Password (OTP) is an authentication approach in which a latest password is created for individual authentication part and repurpose of such password is impossible. OTP is considered as the highly efficient solution and it has provided better performance (Shivraj, V.L., 2015) (Ahmed, A.A., 2019) particularly in large-scale city infrastructures, like remote control. Nevertheless, some methods employed OTP approaches in IoT (Chen, Y., 2018) (Hammi, M.T., 2018) (Hammi, B., 2020). For effective IoT device authentication, the two key emerging technologies like Physical unclonable functions (PUFs) (Shivraj, V.L., 2015) and voltage over-scaling (VOS (Arafin, M.T., 2017) are developed. VOS is general power reduction advancement and is utilized for appropriate computation (Tawalbeh, L.A., 2020) (Vijayakumar, P., 2017). Hence, VOS-based authentication is highly desirable for resource-constrained IoT applications. On the other hand, VOLTA is very resistant against machine learning (ML) attacks (Zhang, J., 2021) (Jan, M.A., 2019). Nowadays, number of researchers has attempted to introduce a safe authentication scheme depending upon an asymmetric encryption approach. In an example, an infrastructure for an IoT system is constructed with three layers, namely perception, transportation, and application layer. An ECC enabled lightweight mutual authentication protocol is presented for IoT elements to deliver a vulnerable system against IoT vulnerabilities and low communication overhead (Zhang, J., 2021) (Rostampour, S., 2020).

In (Zhang, Y., 2023) authors introduce a method that utilizes public-key based techniques for message authentication. In this approach, the sender creates a digital signature for each message and sends the message along with the signature. (Vijayakumar, P., 2017) By employing the sender's public key, intermediaries along the transmission path, as well as the recipient, can verify the authenticity of the message. Compared to symmetric-key based methods, the management of keys in public-key systems is straightforward and uncomplicated. However, in traditional public key cryptosystems (Tawalbeh, L.A., 2020), a trusted third-party agent is required to generate and distribute public/private key pairs. This simplifies the key management and distribution process. In the context of authenticating messages transmitted within IoT networks, it is also essential to ensure source privacy. For example, in the remote metering system of the smart grid, where meter readings are sent through wireless sensor networks, it is crucial to prevent the identification of the specific household generating power usage statistics through these transmitted messages.

The prime intention of this paper is to establish a secure authentication scheme in IoT. Hence, this research is designed to develop a secure authentication approach in IoT for secure communication. The overall procedure of the proposed approach consists of the following entities, namely IoT device, server and AC. A server is a system that offers utilities, data, or services to other systems, termed as clients. An authentication server is employed to ensure the personal details when a person or another server requires stating who they are to an application. The proposed method contains different steps where the first step is the setup phase, second phase is the registration phase, third phase is the key generation step and fourth step is the authentication. Authentication framework is employed using various security constraints scenarios by considering different security operations, like hashing, encryption, secret key pairs, passwords, and so on.

Proposed CHEK-based authentication: An efficient approach is developed for secure authentication in IoT systems by assuming different security operations, namely hashing, encryption, secret key pairs, and passwords.

The remaining format of the research is arranged as follows: Section 2 explains the existing works regarding secure authentication in IoT system along with its benefits and obstacles that drives the analysts to develop an efficacious approach for secure authentication in IoT. Section 3 elaborates the proposed CHEK-based authentication scheme and results are briefed in section 4. Section 5 concludes the paper.

2 Motivation

This section enumerates the survey of existing techniques corresponding to secure authentication in IoT that provokes the analysts to establish an efficient strategy for safe authentication in IoT system.

Security Weakness in IOT

IoT devices are particularly susceptible to security vulnerabilities primarily due to their lack of inherent security controls, making them susceptible to various threats. This vulnerability is primarily attributed to the constrained nature and limited computational capabilities of these devices. IoT devices typically operate on low power and limited processing capacity, which constrains the functions they can perform, often leaving security controls inadequate. These vulnerabilities in IoT devices can enable cybercriminals to hijack them, potentially launching attacks against critical systems. Some common vulnerabilities include:

- Hardcoded Passwords: The easiest approach for hackers to infiltrate Internet of Things devices is through weak, default, or hardcoded passwords. This can lead to the formation of large-scale botnets and the distribution of malware.
- Insecure Network Services: Sensitive data shared between IoT devices and servers may be compromised by attackers taking advantage of flaws in communication protocols and services. Man-in-the-Middle (MITM) attacks target these vulnerabilities to capture authentication credentials, which can be used for broader attacks. Ensuring secure IoT communication is critical.
- Lack of Security Updates: IoT device attacks can be facilitated by unauthorized software and firmware updates, with the energy and healthcare industries being particularly vulnerable.
- Insufficient Privacy Protection: Numerous Internet of Things devices gather personal information, which needs to be processed and stored securely in order to abide with privacy laws. Failure to implement appropriate controls can compromise user privacy and lead to legal consequences.

- Insecure Data Transfer and Storage: The security of IoT data, whether at rest or in transit, is crucial for maintaining the reliability and integrity of IoT applications. This data often plays a role in automated decision-making processes, making its protection vital.
- Lack of Device Management: A major security concern is managing IoT devices over the course of their lives. Unauthorized gadgets that are incorporated into the Internet of Things ecosystem have the ability to obtain access, monitor business networks, and intercept data. In order to monitor and secure IoT devices, provisioning, operating, updating, and locating and identifying them are critical concerns in device management.

Literature Review

The survey of conventional methods is deliberated as follows: Badis Hammi, *et al.* (Hammi, B., 2020) developed a One Time Password (OTP) authentication scheme, which was an eminent solution for IoT. In order to guarantee IoT security, a scheme of OTP creation based on Elliptic Curve Cryptography (ECC) and Isogeny. Here, a new key was generated to exchange the message between IoT device and server. Unlike synchronous OTP-type method, the developed approach did not depend on a counter or a timestamp. This developed method did not rely on response management. However, the method failed to define an approach for retransmission of lost and non-authenticated messages. Pradeep Sudhakaran, and Malathy C (Sudhakaran, P., 2022) designed an Energy Efficient Distributed Lightweight Authentication and Encryption (EEDLAE) methodology for IoT privacy. Here, the receiver created a token for individual sender and the due time for token was estimated depending upon trust value of sender and sleep duration of user radio was also computed depending upon its remaining energy. Counter with Cipher Block Chaining-Message Authentication Code (CCM) was considered for encryption. The major drawback of this scheme was that it did not handle external attacks. In addition, the designed model did not deliver high security as it utilizes the conventional symmetric encryption and MAC-based authentication. G. Kalyani, and Shilpa Chaudhari (Kalyani, G., 2020) introduced an effective method named Optimal Homomorphic Encryption (OHE) for IoT sensitive information. Initially, sensitive data from IoT were categorized depending upon Deep Learning Neural Network (DNN) architecture. Once the categorization was done, OHE performed sensitive data by processing encryption and decryption mechanisms. In encryption mechanism, optimal key was chosen utilizing Step size Fire Fly (SFF) algorithm. The developed IoT security system achieved high key breaking duration and low computational duration with maximum security. Though the OHE with key authentication model was desirable, the scale count situation was not accomplished and it was very complex process. Masoumeh Safkhani, *et al.* (Safkhani, M., 2020) (Zhou, Y., 2022) an improved protocol named RESEAP was developed to ensure the security of a cryptographic model. The developed RESEAP protocol had better security and also proved its efficiency. However, the developed model cannot have the ability to resist against adversary attacks.

Major Challenges

Some of the major challenges experienced by existing methodologies for secure authentication mechanism in IoT are enlisted as follows:

- The ECC-based authentication scheme developed in (Hammi, B., 2020) is an extended version of OTP scheme was adopted to ensure IoT security and the performance can be improved by considering various kinds of Isogeny. In addition to this, developed scheme failed to resist against Denial of Service (DoS) attacks.

- Though the OHE with key authentication model developed in (Kalyani, G., 2020) was very effective, but under large-scale count circumstance it was a rigorous process. This issue can be addressed by considering multi-cloud design as an efficient strategy that can provide privacy employing Homomorphic techniques.
- RESEAP model designed in (Safkhani, M., 2020) offered better efficiency when compared with ESEAP and it delivered superior results in Real-or-Random (RoR) model. However, the scheme failed to consider various protocols with PUF in order to ensure desired security.

3 Proposed CHEK-based Authentication Approach for Secure IoT Application

This section enumerates the designed CHEK-based authentication scheme for secure IoT application. The ultimate goal of this paper is to establish and develop an efficient authentication approach in IoT for secured communication. Here, the entities involved in this process are IoT device, server, and AC. The IoT device is mainly responsible for gathering the data created by the sensors connected to it and transferred to the server. In many scenarios, IoT also process the data before authenticating to the server. Generally, IoT device communicates with IoT server by means of a wide area network (Shah, T., 2018) (Zhang, Y., 2023). A server is a model that delivers useful utilities, data services, or programs to other system known as clients, whereas an authentication server is employed to verify the personal details of the client. The proposed scheme consists of four steps, such as setup, registration, key generation, and authentication stage. Authentication framework is developed by considering different security factors, such as hashing, encryption, secret key pairs, and passwords. Figure 1 illustrates the schematic view of designed CHEK-based authentication approach.

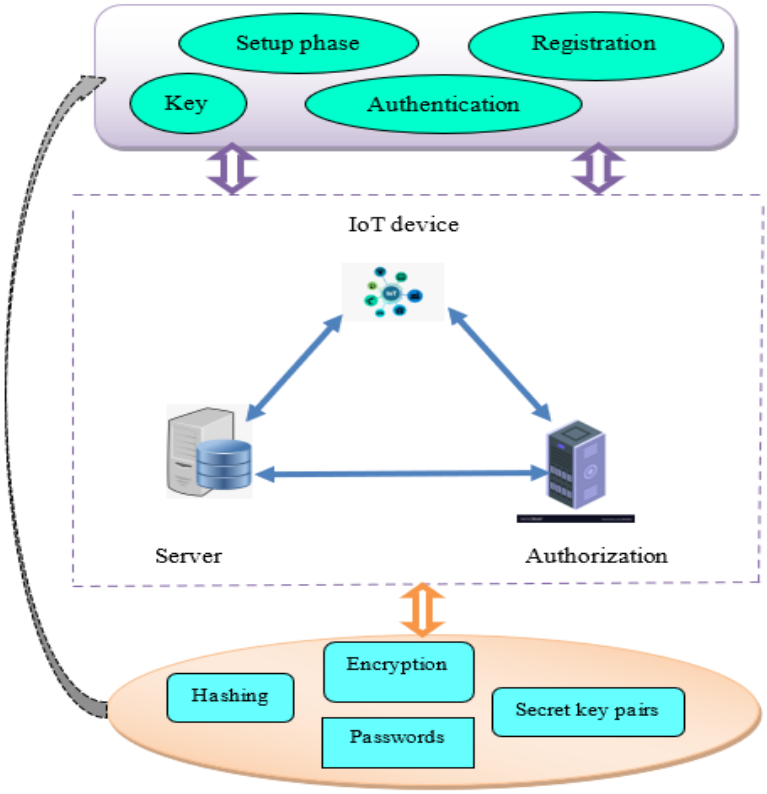


Figure 1: Schematic View of Devised CHEK-based Authentication Approach

The symbols and descriptors used in this proposed method are illustrated under Table 1.

Table 1: Symbols and Descriptions of Proposed CHEK-based Authentication Approach

SL. No	Symbols	Descriptions
1	E_{id}	Device id
2	E_{pwd}	Device password
3	J_{id}	Server id
4	J_{pwd}	Server password
5	u, v	Random number
6	m_1, m_2	Message
7	V_1	Verification message
8	H	Hashing
9	X	Encryption
10	p	Security parameter
11	C	Chebyshev polynomial
12	OTP	One Time Password
13	M_k	Master key
14	S_k	Sever key
15	P_k	Authorization public key
16	G_k	Authorization private key
17	$\oplus$	Mod operator
18	Y_k	Secret key pair
19	Q_1	Authentication request

Setup Stage

The first stage of devised CHEK-based authentication scheme is setup phase, which is performed at the AC. This phase is mainly used to initialize the system security parameter in the network. The AC generates a random number u and v that lies in the range of [0, 2] along with this a security parameter p is generated by AC.

Registration Phase

The second phase is registration phase and entities involved in this phase are IoT device, server, and AC. Registration is the process of collecting user's confidential data and before accessing data services in IoT, user must register his/her own credentials to server and every user registers his/her personal credentials to server through a secure channel. Thus, device is registered at the server. Initially, server id J_{id} and server password J_{pwd} is generated at the server and it is then stored at AC as J_{id}^* and J_{pwd}^*. Thereafter, a server key is created using below expression,

$$S_k = H\left(J_{id}^* \| u \| p\right) \quad (1)$$

Here, the server key is created by concatenating stored id of server J_{id}^* with random number u and security parameter p. Thereafter, hashing operation is performed to the concatenated result, thereby generating a server key. Once the server key is created, it is stored in the server as S_k^*.

A hashing algorithm is a unidirectional cryptographic function that takes an input message of variable length and produces a constant-length digest value as its output, which serves the purpose of verifying the authenticity of the original message. The MD5 hashing algorithm employs an intricate mathematical formula to generate a hash by dividing the data into fixed-size blocks and iteratively processing it, incorporating a distinctive value into the computation, and eventually transforming the outcome into a compact signature or hash. Using the MD5 hash is a more convenient method for verifying the integrity of a copy of a file compared to the laborious process of comparing each bit to ensure the two copies are identical.

A message is generated at the server by concatenating the server password and server id with uneven value v and then hashing function is applied to the concatenated result. Moreover, XOR operation is performed by considering hashed result and stored server key S_k^*. The generated message at the server is expressed as follows,

$$m_1 = H\left(J_{id} \| v \| J_{pwd}\right) \oplus S_k^* \quad (2)$$

The AC also generates a message by concatenating the stored id of server J_{id}^* with random number v and stored password of server J_{pwd}^* and then hashing operation is applied. Thereafter, server key S_k is XOR with the hashed result. If the message generated at the server and AC is same, then the server is registered at AC. The generated message at AC is represented as,

$$\tilde{m}_1 = H\left(J_{id}^* \| v \| J_{pwd}^*\right) \oplus S_k \quad (3)$$

The device id E_{id} and device password E_{pwd} is generated by an IoT device and it is then stored at the IoT server as E_{id}^* and E_{pwd}^*, respectively. The device id and password is also stored at AC as E_{id}^{**}, and E_{pwd}^{**}. A verification message is generated at AC using below expression,

$$V_1 = \left(H\left(E_{pwd}^{**}\right) \| u\right) \oplus v \quad (4)$$

Here, hashing function is applied to the stored password at AC E_{pwd}^{**} and then hashed result is concatenated with uneven number u. At last, the outcome is XOR with uneven value v. The verification alert is stored at the server and AC as V_1^* and V_1^{**}. Then, V_1^* is matched with V_1^{**}, device is registered at the server. Figure 2 illustrates the registration phase of proposed CHEK-based authentication approach.

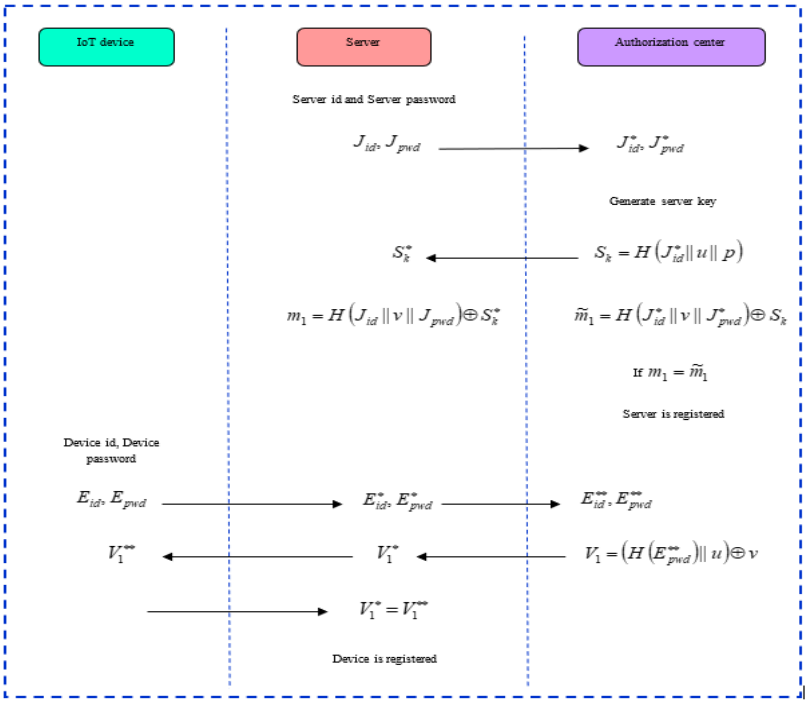


Figure 2: Registration Phase of Proposed CHEK-based Authentication Approach

Key Generation Stage

The third stage is the key generation stage in which the secret key pairs Y_k is generated using both public and private authorization key. Figure 3 shows the key generation phase of proposed CHEK-based authentication scheme. At first, private authorization key is generated at AC by performing the following process. The stored password E_{pwd}^{**} at AC is concatenated with security parameter p. Similarly, stored id E_{id}^{**} is multiplied with random number u. Both the function undergoes hashing function and hashed output is XOR with uneven number v. The expression is shown as below,

$$G_k = H\left(E_{pwd}^{**} \| p\right) \oplus H\left(E_{id}^{**} * u\right) \oplus v \tag{5}$$

Once the private authorization key is generated, public authorization key is generated using below expression,

$$P_k = H\left(E_{pwd}^{**} \| v\right) \oplus p * \mathrm{mod} u \tag{6}$$

where, p denotes the security parameter and mod is the mod function.

Then, secret key pair is generated by performing XOR operation with private authorization key and public authorization key using the expression as follows,

$$Y_k = H\left(G_k \oplus P_k\right) \tag{7}$$

The secret key pair is stored at the server as Y_k^*. Thereafter, server generates a master key and it is stored in the IoT device as M_k^*. The expression for master key is computed as follows,

$$M_k = \left(Y_k^* \oplus \mathrm{mod} u\right) \| p \tag{8}$$

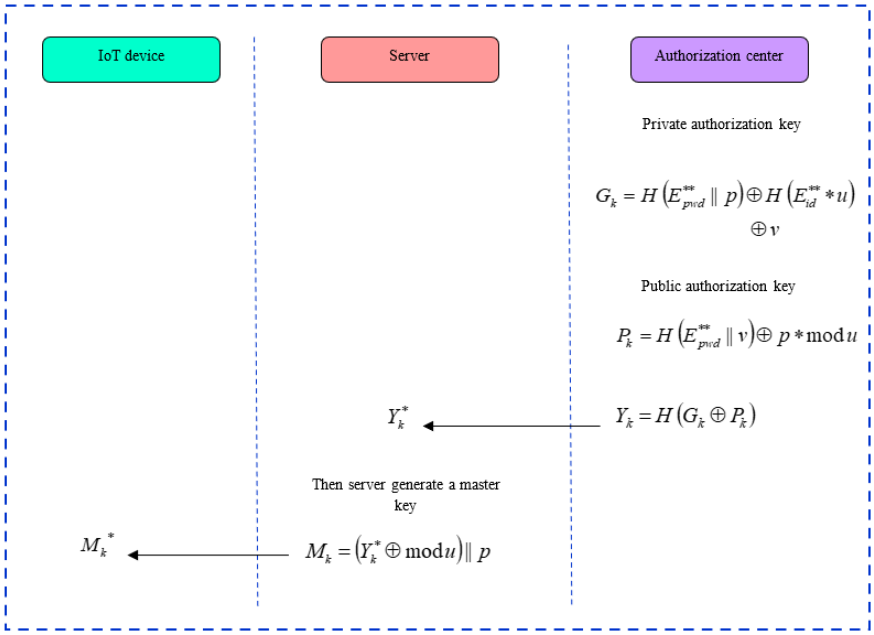


Figure 3: Key Generation Stage of Devised CHEK-based Authentication Method

Authentication Stage

The entities involve in authentication phase are IoT device, server, and AC. In authentication phase, AC verifies the authenticity of the IoT device who desired to access data. Here, IoT device sends a request to the server and an OTP is generated for verifying the authenticity of IoT device. Initially, an authentication request is sent to the server by concatenating device id and random number v and device password is concatenated with security parameter p. Then, XOR operation is carried out between the concatenated results. After that, encryption function is applied and finally, the encrypted result is multiplied with stored master key M_k^* using the following expression,

$$Q_1 = X\left(\left(E_{id} \| v\right) \oplus \left(E_{pwd} \| p\right)\right) * M_k^* \tag{9}$$

Similarly, a request is generated at the server using the following expression,

$$\tilde{Q}_1 = X\left(\left(E_{id}^* \| v\right) \oplus \left(E_{pwd}^*\right)\right) * M_k \tag{10}$$

Here, the stored id of device E_{id}^* is concatenated with a random number v and then concatenated result is XOR with the stored password of device E_{pwd}^*. Then, ECC encryption function is applied to such result and the encrypted result is multiplied with a master key M_k. The device is verified by matching Q_1 with $\tilde{Q}_1$. Elliptic curve cryptography (ECC) is a cryptographic algorithm in the public key domain that plays a pivotal role in various security operations, such as encryption. By leveraging the mathematical properties of elliptic curves, elliptic curve cryptography (ECC) establishes the security of key pairs, which is essential for public key encryption. ECC's approach to public key cryptography is rooted in the algebraic structure of elliptic curves over finite fields. Consequently, ECC generates keys that are significantly more challenging to break from a mathematical perspective. An elliptic curve is a two-dimensional curve represented by the equation y^2 = x^3 + ax + b, where 'a' and 'b' are constants,

while 'x' and 'y' are variables. These elliptic curves exhibit a range of compelling mathematical characteristics that render them highly suitable for cryptographic purposes.

Another authentication request is generated at the server and it is represented as follows,

$$Q_2 = X\left(J_{id} \| u\right) H\left(J_{pwd} \| Y_k^*\right) * C \tag{11}$$

where, C is a chebyshev polynomial and it is expressed as follows,

$$C = 32a^5 + 16a^3 + 8a^2 \tag{12}$$

$$a = H\left(J_{pwd} \| p\right) * u \tag{13}$$

The request is sent to the AC and it is given by,

$$\tilde{Q}_2 = X\left(J_{id} \| u\right) H\left(J_{pwd}^* \| Y_k\right) * C \tag{14}$$

An OTP is generated if $Q_2 = \tilde{Q}_2$ and it is computed using below expression as,

$$OTP = X\left(E_{id}^{**} \oplus G_k\right) * H\left(E_{pwd}^* \| Y_k\right) \tag{15}$$

Then, the OTP is stored at the IoT device as OTP^*. The AC verifies the OTP and then the device is authenticated. Figure 4 specifies the authentication phase of proposed CHEK-based authentication scheme.

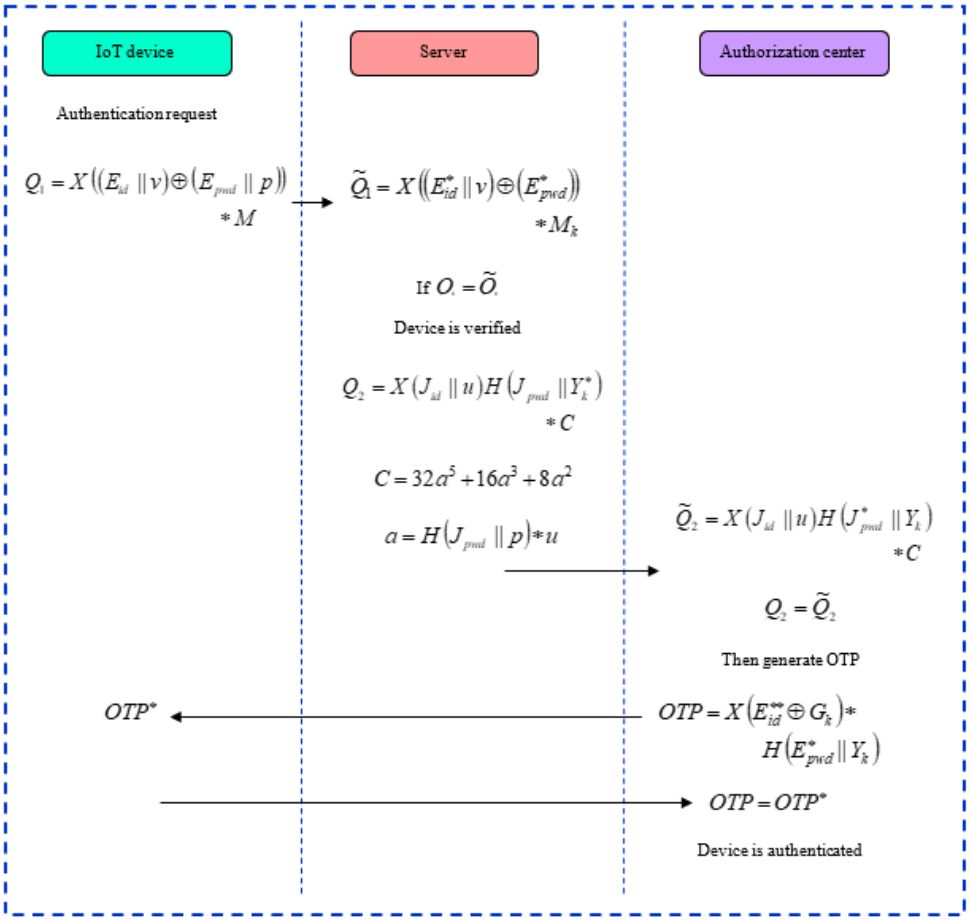


Figure 4: Authentication Step of Devised CHEK-based Authentication Scheme

4 Results and Discussion

This section explains the outcomes of devised CHEK-based authentication in regard to evaluation measures.

Experimental Setup

The execution of designed CHEK-based authentication is executed in PYTHON tool utilizing PC with 10 OS, 4GB RAM, and Intel core-i3 processor.

Evaluation Metrics

The performance of designed CHEK-based authentication is analyzed utilizing evaluation measures, like computational cost, and memory usage.

- ***(i) Computational Cost:*** Computational cost is the execution duration per time step during simulation.
- ***(ii) Memory Usage (MB):*** It is the memory space utilized by the model to perform the authentication framework.

Comparative Methods

The performance enhancement of devised CHEK-based authentication is compared with the traditional models, like ECC-based authentication method (Hammi, B., 2020) (Wei, F., 2020), EEDLAE (Sudhakaran, P., 2022), RESEAP (Safkhani, M., 2020), and OHE (Kalyani, G., 2020) (Vinoth, R., 2022).

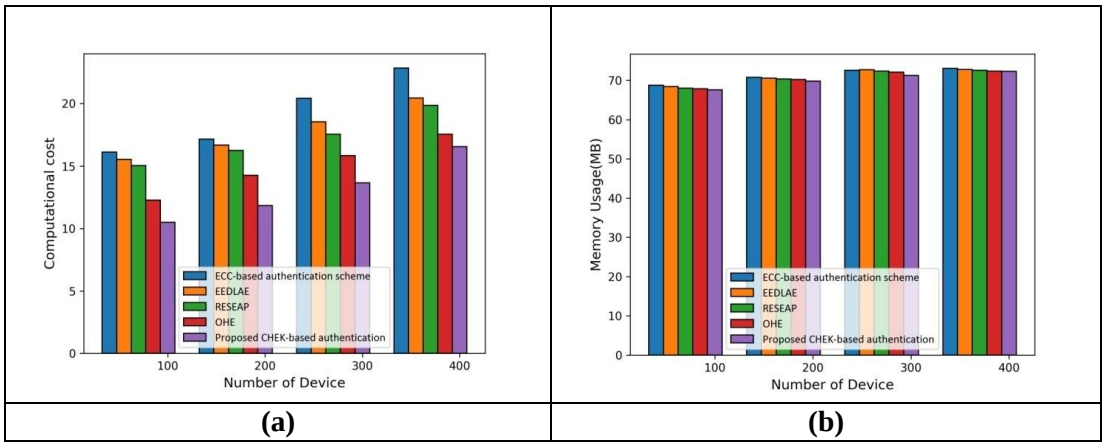
Comparative Analysis

This section shows the comparative evaluation of CHEK-based authentication in regard to performance measures using key length by increasing the number of devices.

(i) Analysis using Key Length=64

Figure 5 displays the analysis of CHEK-based authentication utilizing key length=64 by maximizing count of devices from 100 to 400. Figure 5 a) represents the comparative analysis of proposed CHEK-based authentication with respect to computational cost. When number of devices is 100, computational cost expensed by CHEK-based authentication is 10.482, while the existing methodologies yielded the computational cost of 16.115 for ECC-based authentication scheme, 15.537 for EEDLAE, 15.032 for RESEAP, and 12.253 for OHE. By increasing the number of devices to 400, the proposed CHEK-based authentication achieved the computational cost of 16.541. However, existing schemes attained the computational cost as 22.854, 20.448, 19.854, and 17.543 for ECC-based authentication scheme, EEDLAE, RESEAP, and OHE, respectively.

The assessment made by CHEK-based authentication utilizing memory usage is depicted in figure 5 b). By assuming number of devices as 100, devised CHEK-based authentication utilized the memory usage as 67.6MB and traditional methods yielded the memory usage of 68.8 MB for ECC-based authentication scheme, 68.4MB for EEDLAE, 68MB for RESEAP and 67.9MB for OHE. By varying the number of devices to 400, conventional techniques, such as ECC-based authentication scheme, EEDLAE, RESEAP, and OHE achieved the memory usage of 73.1MB, 72.8MB, 72.6MB, and 72.4MB, respectively.



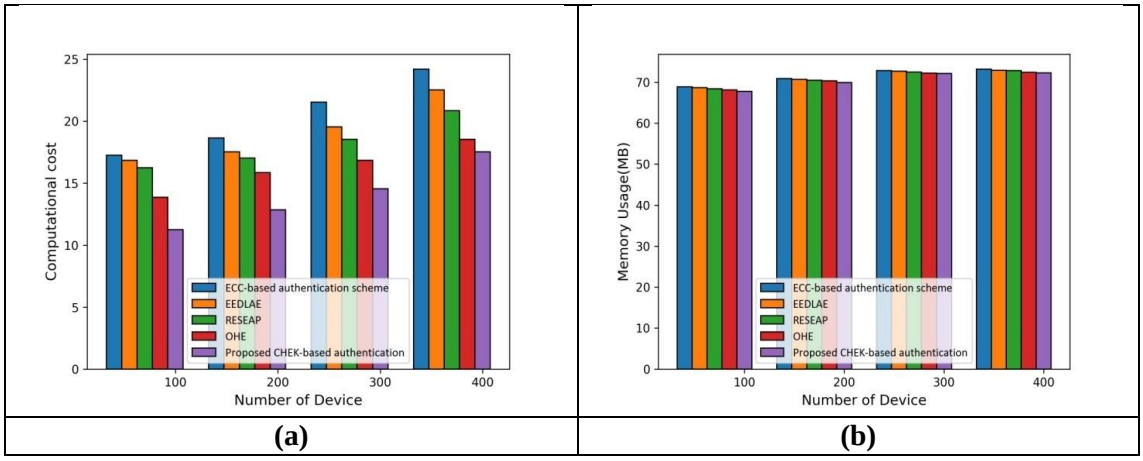
(a) **(b)**

Figure 5: Comparative Analysis Using Key Length=64, a) Computational Cost, b) Memory Usage

(ii) Analysis using Key Length=128

Figure 6 portrays the assessment of developed CHEK-based authentication utilizing key length=128 by varying number of devices with respect to evaluation metrics. Figure 6 a) illustrates the assessment of proposed approach with respect to computational cost. If the count of devices is 100, computational cost yielded by designed method is 11.255, whereas the existing schemes obtained the computational cost as 17.254 for ECC-based authentication scheme, 16.854 for EEDLAE, 16.254 for RESEAP, and 13.855 for OHE. Likewise, when number of devices is 400, computational cost attained by proposed CHEK-based authentication is 17.541 and existing methods attained computational cost as 24.215 for ECC-based authentication scheme, 22.541 for EEDLAE, 20.854 for RESEAP, and 18.541 for OHE.

Figure 6 b) depicts the evaluation of CHEK-based authentication in terms of memory usage. By considering number of devices as 400, memory usage utilized by proposed CHEK-based authentication is 72.3MB. However, the conventional methods obtained the memory usage of 73.2MB for ECC-based authentication scheme, 72.9MB for EEDLAE, 72.8MB for RESEAP and 72.4MB for OHE.



(a) **(b)**

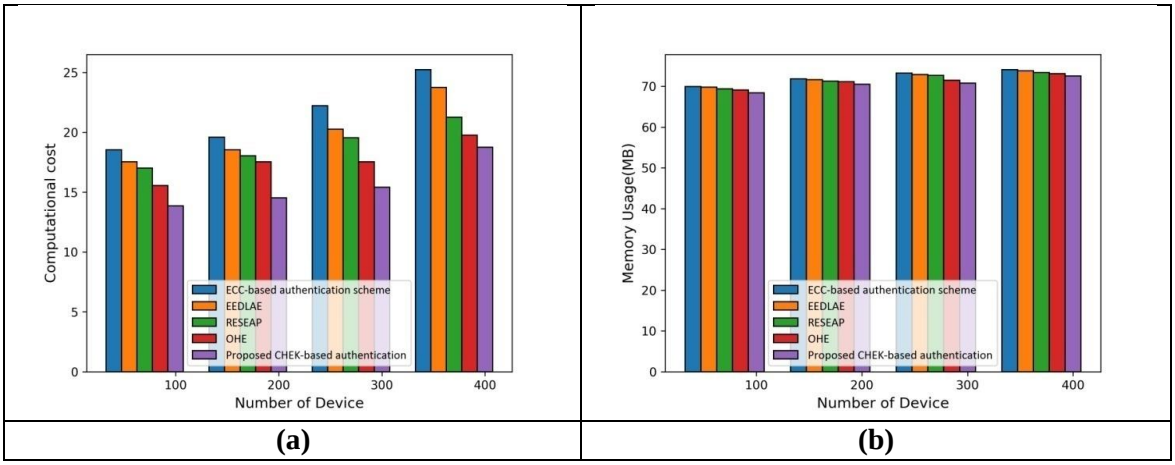
Figure 6: Comparative Analysis Using Key Length=128, a) Computational Cost, b) Memory Usage

(iii) Analysis using Key Length=256

Figure 7 shows the comparative evaluation of CHEK-based authentication with respect to performance measures. The assessment made by designed approach in terms of computational cost is specified in figure 7 a). When number of devices is 400, computational cost delivered by CHEK-based authentication

is 19.745, while the traditional methods attained the computational cost of 25.241 for ECC-based authentication scheme, 23.745 for EEDLAE, 21.254 for RESEAP, and 19.754 for OHE.

Figure 7 b) enumerates the comparative evaluation of devised CHEK-based authentication with respect to memory usage. By considering number of devices as 400, memory usage consumed by proposed CHEK-based authentication is 72.5MB. However, the memory usage yielded by traditional schemes, like ECC-based authentication method is 74.1MB, EEDLAE is 73.8MB, RESEAP is 73.4MB, and OHE is 73.1MB.



(a) **(b)**

Figure 7: Comparative Analysis Using Key Length=256, a) Computational Cost, b) Memory Usage

Comparative Discussion

Table 2 shows the comparative discussion of CHEK-based authentication. From the table, it is clear that the CHEK-based authentication has offered minimum computational cost of 16.541 and minimum memory usage of 72.3MB for analysis using key length=64.

Table 2: Comparative Discussion

Analysis using key length	Metrics/Methods	ECC-based authentication scheme	EEDLAE	RESEAP	OHE	Proposed CHEK-based authentication
Key length=64	*Computational cost*	22.854	20.448	19.854	17.543	**16.541**
	Memory usage (MB)	73.1	72.8	72.6	72.4	**72.3**
Key length=128	*Computational cost*	24.215	22.541	20.854	18.541	**17.541**
	Memory usage (MB)	73.2	72.9	72.8	72.4	**72.3**
Key length=256	*Computational cost*	25.241	23.745	21.254	19.754	**19.745**
	Memory usage (MB)	74.1	73.8	73.4	73.1	**72.5**

5 Conclusion

IoT is an immense technology and it has been considered as a promising solution and eases the burden of humans in day-to-day life. It enables communication effectively among humans and IoT devices.

Because of the scarcity of hardware for IoT objects, deployment of efficient security solutions for IoT environment is still remains as a major challenge. In this research, an effective strategy for authentication in IoT for secure communication is proposed using the CHEK-based authentication approach. The proposed approach includes four stages, like setup phase, registration, key generation, and authentication phase. In the setup phase, random numbers and security parameter are generated at the AC. In the registration phase, the device is registered by verifying the device authenticity and a secret key pair is generated at the key generation phase using private authorization key and public authorization key. Finally, the device is authenticated at the authentication phase. The authentication approach is designed by considering certain security operations, like hashing, encryption, secret key pairs, passwords, and so on. However, the proposed CHEK-based authentication has achieved a minimum computational cost of 16.541 and minimum memory usage of 72.3MB for analysis using key length=64. The suggested approach has yielded relatively superior results, and there is potential for further expansion by incorporating additional encryption techniques to enhance the system's security.

Funding

The authors affirm that they did not accept any grants, funding, or other forms of assistance in order to prepare this paper.

Competing Interests

There are no pertinent financial or non-financial interests that the authors need to disclose.

Author Contributions

The idea and methodology for the research project were contributed to by all authors. Each author prepared the materials and then carried out the data gathering and analysis. The first author wrote the first draft of the manuscript, while all other authors provided feedback on earlier drafts. The final manuscript was read and confirmed by every author.

Data Availability

The data used to support the findings of this study are included within the article.

References

[1] Ahmed, A. A., & Ahmed, W. A. (2019). An effective multifactor authentication mechanism based on combiners of hash function over internet of things. *Sensors*, *19*(17), 1-22.

[2] Anandkumar, M. (2020). Multicast routing in WSN using bat algorithm with genetic operators for IoT applications. *Journal of Networking and Communication Systems*, *3*(2), 1-8.

[3] Arafin, M.T., Gao, M., & Qu, G. (2017). VOLtA: Voltage over-scaling based lightweight authentication for IoT applications. *In IEEE 22nd Asia and South Pacific design automation conference (ASP-DAC)*, 336-341.

[4] Chen, Y., Wen, H., Song, H., Chen, S., Xie, F., Yang, Q., & Hu, L. (2018). Lightweight one-time password authentication scheme based on radio-frequency fingerprinting. *IET communications*, *12*(12), 1477-1484.

[5] Chou, W. (2002). Inside SSL: the secure sockets layer protocol. *IT professional*, *4*(4), 47-52.

[6] Garg, S., Kaur, K., Kaddoum, G., & Choo, K.K.R. (2019). Toward secure and provable authentication for Internet of Things: Realizing industry 4.0. *IEEE Internet of Things Journal*, *7*(5), 4598-4606.

[7] Hammi, B., Fayad, A., Khatoun, R., Zeadally, S., & Begriche, Y. (2020). A lightweight ECC-based authentication scheme for Internet of Things (IoT). *IEEE Systems Journal*, *14*(3), 3440-3450.

[8] Hammi, M.T., Livolant, E., Bellot, P., Serhrouchni, A., & Minet, P. (2018). A lightweight mutual authentication protocol for the IoT. *In Mobile and Wireless Technologies 2017: ICMWT, 4*, 3-12. Springer Singapore.

[9] Jan, M.A., Khan, F., Alam, M., & Usman, M. (2019). A payload-based mutual authentication scheme for Internet of Things. *Future Generation Computer Systems*, *92*, 1028-1039.

[10] Kalyani, G., & Chaudhari, S. (2020). An efficient approach for enhancing security in Internet of Things using the optimum authentication key. *International Journal of Computers and Applications*, *42*(3), 306-314.

[11] Kotenko, I.V., Saenko, I., & Kushnerevich, A. (2017). Parallel big data processing system for security monitoring in Internet of Things networks. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), 8*(4), 60-74.

[12] Liu, C.X., Liu, Y., Zhang, Z.J., & Cheng, Z.Y. (2013). The novel authentication scheme based on theory of quadratic residues for wireless sensor networks. *International Journal of Distributed Sensor Networks*, *9*(3), 1-9.

[13] Mahalle, P.N., Anggorojati, B., Prasad, N.R., & Prasad, R. (2013). Identity authentication and capability-based access control (iacac) for the internet of things. *Journal of Cyber Security and Mobility*, *1*(4), 309-348.

[14] Mandala, J., & SekharaRao, M.V.P.C. (2019). HDAPSO: Enhanced privacy preservation for health care data. *Journal of Networking and Communication Systems*, *2*(2), 10-19.

[15] Miranda, C., Kaddoum, G., Bou-Harb, E., Garg, S., & Kaur, K. (2020). A collaborative security framework for software-defined wireless sensor networks. *IEEE Transactions on Information Forensics and Security*, *15*, 2602-2615.

[16] Pakniat, N., Shiraly, D., & Eslami, Z. (2020). Certificateless authenticated encryption with keyword search: Enhanced security model and a concrete construction for industrial IoT. *Journal of Information Security and Applications*, *53*.

[17] Rostampour, S., Safkhani, M., Bendavid, Y., & Bagheri, N. (2020). ECCbAP: A secure ECC-based authentication protocol for IoT edge devices. *Pervasive and Mobile Computing*, *67*.

[18] Safkhani, M., Bagheri, N., Kumari, S., Tavakoli, H., Kumar, S., & Chen, J. (2020). RESEAP: An ECC-based authentication and key agreement scheme for IoT applications. *IEEE Access*, *8*, 200851-200862.

[19] Shah, T., & Venkatesan, S. (2018). Authentication of IoT device and IoT server using secure vaults. *In 17th IEEE international conference on trust, security and privacy in computing and communications/12th IEEE international conference on big data science and engineering (Trust Com/Big Data SE)*, 819-824.

[20] Shivraj, V.L., Rajan, M.A., Singh, M., & Balamuralidhar, P. (2015). One time password authentication scheme based on elliptic curves for Internet of Things (IoT). *In IEEE 5th National Symposium on Information Technology: Towards New Smart World (NSITNSW)*, 1-6.

[21] Sudhakaran, P. (2022). Energy efficient distributed lightweight authentication and encryption technique for IoT security. *International Journal of Communication Systems*, *35*(2).

[22] Tawalbeh, L.A., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT Privacy and security: Challenges and solutions. *Applied Sciences*, *10*(12), 1-17.

[23] Vijayakumar, P., Pandiaraja, P., Karuppiah, M., & Deborah, L.J. (2017). An efficient secure communication for healthcare system using wearable devices. *Computers & Electrical Engineering*, *63*, 232-245.

[24] Vinoth, R., Deborah, L.J., Vijayakumar, P., & Gupta, B.B. (2022). An anonymous pre-authentication and post-authentication scheme assisted by cloud for medical IoT environments. *IEEE Transactions on Network Science and Engineering*, *9*(5), 3633-3642.

[25] Wei, F., Vijayakumar, P., Kumar, N., Zhang, R., & Cheng, Q. (2020). Privacy-preserving implicit authentication protocol using cosine similarity for Internet of Things. *IEEE Internet of Things Journal*, *8*(7), 5599-5606.
[26] Zhang, J., & Qu, G. (2019). Physical unclonable function-based key sharing via machine learning for IoT security. *IEEE Transactions on Industrial Electronics*, *67*(8), 7025-7033.
[27] Zhang, J., Shen, C., Su, H., Arafin, M.T., & Qu, G. (2021). Voltage over-scaling-based lightweight authentication for IoT security. *IEEE Transactions on Computers*, *71*(2), 323-336.
[28] Zhang, J.L., Qu, G., Lv, Y. Q., & Zhou, Q. (2014). A survey on silicon PUFs and recent advances in ring oscillator PUFs. *Journal of computer science and technology*, *29*(4), 664-678.
[29] Zhang, Y., He, D., Vijayakumar, P., Luo, M., & Huang, X. (2023). SAPFS: An Efficient Symmetric-Key Authentication Key Agreement Scheme with Perfect Forward Secrecy for Industrial Internet of Things. *IEEE Internet of Things Journal*, 1-1.
[30] Zhou, Y., Li, L., Obaidat, M.S., Liu, Y., Vijayakumar, P., & Hsiao, K.F. (2022). RAKI: A Robust ECC Based Three-party Authentication and Key Agreement Scheme for Medical IoT. *In GLOBECOM IEEE Global Communications Conference*, 1175-1180.

Authors Biography

Dr.S. Thanga Revathi is working as Assistant Professor in the Department of Computer Science and Engineering, SRM Institute of Science and Technology, Kattankulathur, Chennai, Tamil Nadu. She has 15 years of teaching experience in various Engineering College. She has obtained her PhD from Anna University, Master of Engineering from Bharath University and Bachelor of Engineering from Anna University. Her research area includes Data Security, Cloud Computing, Distributed Computing and Analytics. She has published papers in Referred National and International Journals. She has also presented many papers in International Conferences.

Dr.A. Gayathri, received the B. E degree in Electronics and Communication Engineering from Periyar Maniammai College of Technology for Women (Bharathidasan University, India) in 2001 and the M. Tech (CSE) degree in Computer Science and Engineering specialization from Bharath University, Chennai, India in 2005. She completed the Doctorate in the Department of Information and Communication Engineering at Anna University in 2017. Her commitment to excellence is exemplified by the recognition she has received, including the prestigious Best Faculty Award from Novel Research Academy, bestowed upon her by the Pondicherry Government. Her valuable insights and contributions have been documented in several papers published across SCI and Scopus indexed journals, solidifying her position as a respected figure in academia and research. She is currently working as Professor in Saveetha School of Engineering (Department of CSE), SIMATS, Chennai, Tamil Nadu.

Dr.A. Sathya, Associate Professor, Department of Artificial Intelligence and Data Analytics, Sri Ramachandra Faculty of Engineering and Technology. She has 17 Years of teaching experience. She has undertaken and guided many social relevant projects works. A patent has been filed in her name and authored book chapters in reputed publications like springer and Wiley. She published more than 25 papers in conferences and journals. Her area of interest includes Cloud security, Data Analytics. She worked in few consultancy projects in the area of machine vision, image processing, web application, mobile application and cloud computing.

M. Santhiya M.E (CSE), She has 6 years' experience in many reputed institutions and currently working as Assistant Professor in Rajalakshmi Engineering College, Sriperumbudur. A patent has been filed in her name and authored book chapters in reputed publications like springer and Wiley. She published more than 9 papers in conferences and journals.