Lightweight Multi Party Authorisation for IoT Device Access Using Bilinear Pairing and Shamir's Secret Sharing

Bikramjit CHOUDHURY [1], Amitava NAG [1], Dipankar RABHA [1], Sukumar NANDI [2]

[1] Dept. of CSE, Central Institute of Technology Kokrajhar, BTR, Assam-783370, India
[2] Dept. of CSE, Indian Institute of Technology Guwahati, Assam-781039, India

{b.choudhury, amitava.nag, b16it242}@cit.ac.in, sukumar@iitg.ac.in

Submitted April 30, 2025 / Accepted June 7, 2025 / Online first August 4, 2025

Abstract. *With the advancement of new hardware and software technologies, the Internet of Things (IoT) has become ubiquitous in our day-to-day life. Along with many diversified applications, IoT has made inroads into several sensitive areas like Healthcare, Industries (IIoT), Smart Cities, Real-time Systems and so on. With the exploding application of IoT, there is an exponential increase in the requirement for security and keeping in mind the constrained nature of IoT devices and networks, customized lightweight protocols and measures have been proposed in the literature.*

Multi-party authorisation is one of the key aspects of IoT security. Access to sensitive IoT devices should be allowed only after authorisation from trusted entities. In this work, we have proposed a novel Lightweight Multi Party Authorisation for IoT Device Access with key establishment using Bilinear Pairing and multi party authorisation through Shamir's Secret Sharing. All communications are protected by lightweight XOR-based encryption with pairwise session keys. Further, threshold based Shamir's Secret Sharing facilitates the provision of dynamic authorisation policy set by the Admin according to application requirement. A prototype is developed using Raspberry Pi3, DHT11 sensor and an Android Application and tested for satisfactory performance. The scheme is formally verified on AVISPA and an informal security analysis is performed to assess its resistance to various attacks. A feature based comparison of the proposed scheme with other state of the are works established the unique advantages of the system. The proposed scheme has potential applications including, but not limited to, IoMT, IIoT and Smarthome.

Keywords

Bilinear pairing, Shamir's Secret Sharing, Internet of Things, multi party authorisation, lightweight, IoT security

1. Introduction

IoT is all about M2M communication, but humans are inevitably entangled in its operation. Setup, authorisation, control parameter setting are some of the operations that require human intervention. As the Internet of Things (IoT) grows, more and more devices are connected to the Internet infrastructure, increasing the demand for ultra-low-power computing and communication. IoT devices are now pervasive in modern life, ranging from medical devices to critical infrastructures, and since these devices often need to cooperate to achieve the desired mission; security, trust, and privacy are new important design objectives for these devices [1]. Despite that, modern cryptography based solutions are computationally expensive and not suitable for IoT devices with limited resources [2], [3]. Thus, security and privacy have become the Achilles heel for IoT system design and implementation. For example, Industrial IoT, Security Cameras, Smart Lock and IoT in Healthcare (such as pacemakers and insulin pumps) communications are highly sensitive and device access should be controlled. Research on new low-power security primitives is therefore essential for the safe and secure implementation of IoT applications.

Applications of IoT are increasing by leaps and bounds in a wide spectrum of use cases. Along with exploded applications comes the increased risk as IoT devices are resource-constrained and often deployed in insecure environments. The involvement of IoT devices in many critical applications like Healthcare, Industry, and Smart cities makes it imperative to secure the IoT device access, failing which may lead to catastrophic consequences. Multi-party Authorisation (MPA) is the apt solution to this problem where IoT device access will be moderated by a group of supervisors [4]. Shamir's threshold-based Secret Sharing [5], a widely used proven technique that has the advantages of reliability, robustness, resistance to a single point of failure, and security, is perfectly suitable for MPA.

One sample use case of MPA in IoT is Industrial Control System. Modern Control Systems are automated and work based on the inputs of various sensors. Now, if there is a need to access any of the sensors or actuators for repair or param-

DOI: 10.13164/re.2025.0541

eter change, then it must be authorised by the concerned higher officials to prevent any malicious activity. Another use case may be access to sensitive IoT Healthcare devices like Insulin Pump or Pacemakers. Access to such devices must be protected by MPA as human lives are at stake.

In this paper, we have proposed a lightweight Bilinear Pairing and Shamir's Secret Sharing based Multi Party Authorisation scheme (MPA) for IoT device access. Initially Bilinear Pairing is used to set up session keys for secure communication, and then threshold based Shamir's Secret Sharing facilitates multi party authorisation. *Admin* has the flexibility to decide authorisation policy dynamically as per the application requirements. For some applications, authorisations from all the *Authorisers* may be compulsory, whereas in some cases minimum threshold t number of authorisations will be sufficient. Further, asymmetric authorisation, where permission from different *Authorisers* will carry different weight, can be configured by distributing a different number of shares to the *Authorisers* as per the access policy. As it is a threshold based scheme, availability of all the *Authorisers* are not compulsory, thus making the system more robust. Lightweight XOR based encryptions and Polynomial based Shamir's Secret Sharing are used in the scheme keeping in mind constrained IoT devices. Finally, a prototype of the system is developed in a testbed using Raspberry Pi3, DHT11 sensor and Android App for validation purpose.

Following are the key contributions of our work:

1) Novel scheme for Multi-Party Authorisation in IoT device access using Bilinear Pairing and Shamir's Secret Sharing.
2) Lightweight and low cost scheme for constrained IoT environment
3) Support for dynamic authorisation policy making it suitable to different IoT application contexts with varied authorisation requirements.
4) Development of a prototype with Raspberry Pi, Android App and DHT11 Sensor for validation.

The remainder of the paper is organised as follows. Section 2 presents the preliminary concepts related to the proposed system. Section 3 gives a brief discussion on existing works and open research issues, followed by Sec. 4, which sheds light on the proposed system. The implementation details along with the results and security analysis are presented in Sec. 5. Finally, the concluding remarks are recorded in Sec. 6.

2. Preliminaries

This section provides a brief introduction to the concept of Bilinear Pairing, Shamir's Secret Sharing and Multi Party Authorisation. Bilinear Pairing and Shamir's Secret Sharing form the basis of the set up and authorisation phases of the proposed Multi Party Authorisation system.

2.1 Bilinear Pairing

The bilinear map can be constructed on elliptic curves [6], [7]. Each computing operation is a pairing operation. Let G be a cyclic additive group, and let GT be a cyclic multiplicative group. Both groups G and GT have the same prime order q. Groups G and GT are called bilinear groups. The security of the bilinear pairing-based scheme relies on the difficulty of the Discrete Logarithm Problem (DLP); that is, given the point $Q = aP$, no efficient algorithm exists to obtain a given P and Q. The mapping $e : GxG- > GT$ is called a bilinear map if it satisfies the following properties:

i) Bilinear:

$$e(Q, P+R) = e(P+R, Q) = e(P, Q)e(R, Q), \forall P, Q, R \in G, \quad (1)$$

$$e(aP, bP) = e(P, bP)^a = e(aP, P)^b = e(P, P)^{ab}, \forall a, b \in Z. \quad (2)$$

ii) Nondegenerate:
$P, Q \in G$ exists such that $e(P, Q) \neq 1_{GT}$.

iii) Computable:
An efficient algorithm exists to compute $e(P, Q)$ for any $P, Q \in G$.

2.2 Shamir's Secret Sharing

In Shamir's Secret Sharing a Secret S is divided into n number of shares in such a way that combination of minimum t number of shares can only reconstruct the Secret S, where t is called the threshold [5]. It can be used to divide the key and distribute the shares among n number of participants, so that no single participant can use the key and if a participant lost its share still others can reconstruct the key.

The basic idea of the Shamir's scheme is based on Lagrange Interpolation Theorem which states that a polynomial of degree $t-1$ can be identified by minimum any t points on the polynomial curve. So if the threshold is t, then a polynomial of degree $t-1$ is constructed by selecting desired Secret S as a_0 and randomly choosing the coefficients $a_1, a_2, \ldots, a_{t-1}$. All the values are chosen over $GF(q)$.

$$f(x) = S + \sum_{l=1}^{t-1} a_l x^l. \quad (3)$$

Now, any n points on the polynomial curve can be chosen and distributed as shares $S_i = x_i, f(x_i)$ where $i = 1, 2, \ldots, n$. Secret S can be computed only after collection of at least t shares S_i using the following interpolation formula.

$$S = \sum_{i=0}^{t-1} f(x_i) \prod_{\substack{m=0 \\ m\neq i}}^{t-1} \frac{x_m}{x_m - x_i}. \quad (4)$$

2.3 Multi Party Authorisation

Multi Party Authorisation (MPA) demands the approval from multiple *Authorisers* before any activity [4], [8]. It is very much essential to protect critical and sensitive infrastructure, data, and devices from intended or unintended misuse. *Authorisers* are usually pre-assigned who held the responsibility of security of the system. One common example of MPA is the bank locker system in which both the owner and the banker together can only open the locker, one party alone can't access the locker.

MPA has wide ranging applications in Internet of Things deployed in many critical and sensitive use cases and consists of resource constrained nodes installed in vulnerable open environments having too many attack surfaces. As billions of smart Things from all spheres of our life are connected over the Internet, it has also become equally important to secure devices from unauthorised access.

3. Related Work

Over the last few years, IoT has emerged as a key technology having its application in many sensitive and critical areas. However, the unique characteristics of the IoT network have brought up novel challenges turning the traditional security approaches inapplicable. Resource constrained IoT devices are not capable of performing computationally intensive operations of traditional cryptography and deployment of IoT devices in open and vulnerable environments necessitates carefully crafted security policies [2], [3]. Thus novel security solutions to address the unique challenges of IoT network have been intensively explored resulting in many state of the art schemes [9], [10].

After its initial definition by Shamir, Secret Sharing has been used in diverse domains including secure multi party computation, multi party access control, multi party verification and multi-User authentication. From initial polynomial based secret sharing many new areas like image secret sharing, verifiable secret sharing, multi secret sharing, access structure based secret sharing and most recently post quantum secret sharing have been developed [11], [12]. Authors in [13], Demonstrated the design of a hardware dependent multi-User authentication scheme using RRAM and image secret sharing, where final resistance state of the RRAM will authenticate the Users. Group authentication and key agreement based on Shamir's secret sharing and group management by binary tree for machine type communication in LTE was proposed in [14].

Several multi party schemes are proposed in the literature to meet the security requirements of different applications. Authors in [15] have specified a multi party access control policy for online social network to restrict the use of shared data. In collaborative systems ownership may not always be homogeneous, resulting in the idea of symmetric and asymmetric authority over the resource [16]. Certificateless aggregation and authenticated encryption of data between Near Band IoT devices and Access and Mobility Management Framework in 5G network was devised in [17] where anonymity of devices are preserved. Kratos, a novel multi-User and multi-device aware access control mechanism that allows smart home users to flexibly specify their access control demands formulated in complex policies is proposed in [18]. Multi Authority Criteria based encryption for IoT where multiple authorities manage the global criterion universe and perform key generation to constitute attribute based access policy was proposed in [19]. Access control policies from multiple users are combined using privacy preserving techniques like homomorphic encryption and secure function evaluation for computation of multi party access control policies in [20]. In [21], authors have proposed a multi authority CP-ABE scheme for IoT devices. Lattice-based cryptographic construct such as Identity-Based Encryption (IBE) for multi party authentication and key agreement in IoT based e-healthcare services was explored in [22], [23]. A verifiable image secret sharing to detect and recognise fake shadow image was proposed in [24]. Privacy preserving aggregation of IIoT data was addressed in [25] where three types of aggregation i.e. sum, multiplication and variance operations were supported. Image secret sharing scheme for access and distribution of large scale visual data was proposed in [26].

Next we have discussed a few schemes about authorisation in the IoT domain. Oauth2.0 is widely used for authorisation in web and desktop applications and mobile devices [27]. But it is mainly for authorisation to third party applications on behalf of a user by an authorisation server, and can't deal with multi party authorisation. An inter cloud authorisation based on CP ABE was proposed in where access tokens for web applications were generated using ciphertext reencryption by the owners [28]. Decentralised solution for Multi Party Authorisation using Blockchain was explored in [8, 29, 30] for different applications. Smart contacts were used for implementing the authorisation policy for both public and private blockchain. But IoT security was not yet considered by these approaches. Risks associated with IoT authorisations were explored in [31] through ownership transfer attack and device sharing attack.

Although, multi party authentication, multi user access control, secure multi party computations and multi party verifications are explored in literature as discussed above, but so far the need of a lightweight multi party authorisation scheme to control IoT device access is yet to be addressed. There is a subtle difference in principle and objective of multi party authorisation with the other multi party schemes as explained in Sec. 2.

Taken together, these studies exhibit certain limitations: (a) limited focus on lightweight cryptographic techniques tailored for IoT devices with constrained resources, (b) a frequent absence of mechanisms for dynamic delegation or pre-authorized access control in multi-party contexts, (c) most solutions are domain-specific (e.g., healthcare, visual data), limiting general applicability to heterogeneous IoT environments, and (d) very few works offer a compositional solution integrating fine-grained access control, secure delegation, and multi-party trust models in one framework. Summary of the literature survey is provided in Tab. 1.

A novel multi party authorisation scheme is proposed that addresses the research gaps highlighted in Tab. 1. The proposed scheme is designed to be lightweight and low cost by using only XOR based encryption and low cost components in the prototype. Here, *Admin* can dynamically decide the authorisation policy for access control by selecting the right threshold value and share distribution scheme based on application requirements. The multi party authorisation policy proposed in this work is suitable for a wide array of IoT applications ranging from IIoT, IoMT to Smart Homes. A comprehensive scheme consisting of Bilinear Pairing based key establishment and Shamir's Secret Sharing based authorisation and dynamic secure delegation is devised for fine-grained access control in IoT applications enabling multi party trust model. Robustness of the system is established by the fact that it can function in the presence of only t out of n authorisers and can work independently without using any cloud service. Finally, a prototype is developed as a proof of concept of the proposed scheme.

4. Proposed System

In the proposed system, multiple *Authorisers* must authorise a request to access sensitive *IoT devices*. The system includes Bilinear Pairing for key exchange between *Admin* and other stakeholders and Shamir's Secret Sharing forms the basis of the authorisation phase where a *User's* request for device access depends on the permission from a threshold number of *Authorisers*.

4.1 System Model

The system has four main stakeholders *Admin*, *Authoriser*, *User* and *Gateway*; *IoT devices* participate via *Gateway*.

Admin: *Admin* is a trusted entity. *Admin* is responsible for system setup and initialisation of system parameters. In addition to that *Admin* verifies the identities of *Authorisers* and *Users* and performs periodic renewal of session keys by restarting the registration phase.

Authoriser: *Authorisers* verify *User's* credentials and decide on access permission. Number of *Authorisers* is determined during system set up. Proposed system can withstand up to n-t compromised *Authorisers* because of the (t, n) threshold secret sharing principle.

Ref.	Scheme / Approach	Target domain	MPA support	Lightweight	Secret sharing	Bilinear pairing	Dynamic delegation	Identified gaps
[4]	SSI + SMPC + Threshold Crypto	Healthcare EHR	Yes	Moderate (AES-GCM)	Yes	No	Yes	No bilinear pairing, centralized delegation
[8]	Blockchain-based MPA + Proxy Re-encryption	Decentralized (IPFS)	Yes	Heavy	No	Yes	Yes	Heavy infrastructure
[21]	RMA-CPABE	IoT / Fog	Yes	Moderate	No	Yes (CP-ABE)	No	No secret sharing or dynamic delegation
[22]	OTP-based Multi-Device Auth	General IoT	No	Yes	No	No	Yes	No multi-party control or cryptographic delegation
[23]	Lattice-based Multi-party Auth	E-healthcare	Yes	Yes	No	No	No	Lacks pairing and secret sharing
[24]	Multiparty Image Secret Sharing	Visual Crypto	Yes	Moderate	Yes	No	No	Image-focused; lacks dynamic auth
[25]	Secret Sharing for IIoT	Industrial IoT	Yes	Yes	Yes	No	No	No pairing-based crypto
[26]	Phase Wrapping Secret Sharing	Visual Data	Yes	Moderate	Yes	No	No	Visual-specific; lacks access control
[28]	ICAuth (CP-ABE)	Inter-cloud IoT	Partial (token based)	Yes	No	Yes	Yes	Lacks secret sharing; cloud-dependent
[29]	TANCS (MPA + Conflict Mediation)	Net Config Mgmt	Yes	Not IoT-specific	No	No	Yes	Not optimized for IoT
[30]	CP-ABE with Multi-Auth	General IoT	Yes	Yes (outsourced)	No	Yes	No	No secret sharing or MPA-specific design
[31]	Auth. Issues in 3rd-Party IoT	IoT Platforms	No	No	No	No	No	Only analysis, no solution

Tab. 1. Comparison of related works on secure multi-party authorization and access control in IoT.

User: *User* requests the *Admin* for device access thus starting the Authorisation phase. Access is granted for a session with a predetermined time limit.

Gateway: *Gateway* is a trusted entity controlling the access to *IoT devices*. A *User* after obtaining authorisation from sufficient numbers of *Authorisers* can establish device access over a secure channel through *Gateway*.

IoT Devices: *IoT devices* are under the purview of a *Gateway*. They have a secure communication channel with *Gateway*.

Admin, *Authorisers*, *User* are supposed to be resource rich (e.g. smartphone), *Gateway* is partially resource constrained (e.g. Raspberry Pi) and *IoT devices* are highly resource constrained.

4.2 System Architecture

Architecture of the system is explained in Fig. 1. The system is composed of two networks: A *User* network consisting of smartphones simulating *Admin*, *Authoriser* and *User*; and an IoT network consisting of *IoT devices*. Both the networks are bridged by a *Gateway* for example Raspberry Pi. MQTT is working at application layer to facilitate communication among Smartphones and Raspberry Pi over 4G LTE/WiFi. *IoT devices* are connected to *Gateway* over lightweight communication protocols like BLE, LoRa WAN etc.

It is assumed that *Admin* is fully trusted with impeccable security and *Gateway* Node is trusted or else device data is encrypted to withstand a compromised *Gateway*. *Gateway* to *IoT device* communication is protected by inherent security features of communication protocol. Also, *User* credentials are verified by *Admin* during registration and by *Authorisers* during authorisation phase. *Admin*, *Authoriser*, *User* and Gateway nodes are assumed to be powerful enough to thwart an attacker's threat.

As depicted in Fig. 2, an attacker may be a threat to all types of communication between *Admin*, *User*, *Authoriser* and *Gateway* node. An attacker may launch various attacks like impersonation attack, MIM, Replay Attack or eavesdrop or capture any communication message.

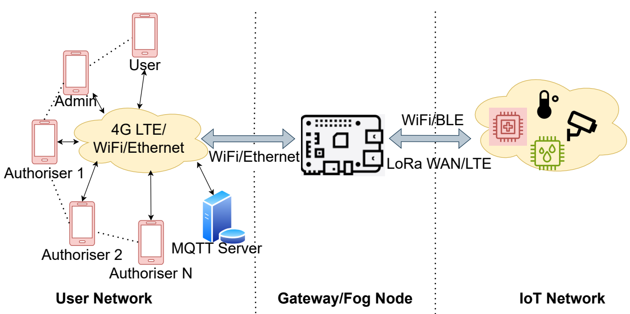

Fig. 1. System architecture.

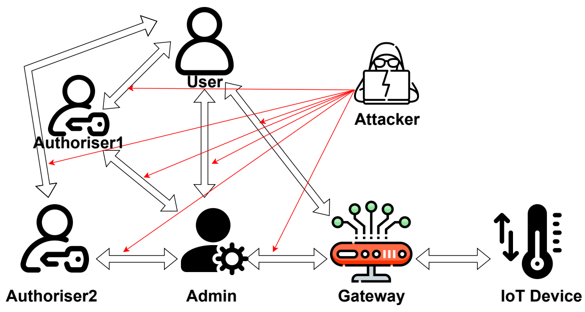

Fig. 2. Threat model.

4.3 System Setup

Admin set up the system by initiating the Login Phase. In the login phase, *Authorisers*, *Gateway* and *User* will register with *Admin* and establish a pairwise session key with *Admin* by using Bilinear Pairing. *Admin* further set the threshold t for Shamir's Secret Sharing based on access policy and decide periodic session key renewal interval.

Following are the assumptions related to public keys of the stakeholders:

- *Admin* stores its ECC public key (PU_{A}) and the private key (PR_{A}) : $PU_{\mathrm{A}} = PR_{\mathrm{A}}G$.
- Each *User's* smartphone stores its ECC public key (PU_i) and the private key (PR_i) : $PU_i = PR_iG$.
- The *Fog node* stores its ECC public key (PU_{F}) with the private key (PR_{F}) : $PU_{\mathrm{F}} = PR_{\mathrm{F}}G$.
- The *Admin* stores each *User's* ID (I_i) with its public key PU_i and *Fog node's* ID (I_{F}) with its public key PU_{F}.
- *Gateway* stores each *User's* ID (I_i) and each *IoT device's* ID (SD_j).
- The *Admin*, *User* and *Fog node* have agreed to a base point Q and a hash function H.

The proposed scheme consists of two phases, first phase for the establishment of session key using Bilinear Pairing and second phase for the multi party authorisation using Shamir's Secret Sharing.

4.3.1 Login Phase: Session Key Establishment Using Bilinear Pairing

In the login phase, as shown in Fig. 3 *User* will choose a random number with the ECC key and compute the session key using the public key of the *Admin* and then encapsulate it using the hash function $r_i \in 1, 2, \ldots, K-1$ compute $R_i = r_iG$ and $M_i = PR_i + r_i$ and compute session key $K_i = e(M_i + PU_{\mathrm{A}})$ Where PR_i is the private key of *User* and G is a point on ECC and sends the login request to *Admin*.

$$User \text{ -> } Admin: \; I_i, H(I_i||K_i), R_i.$$

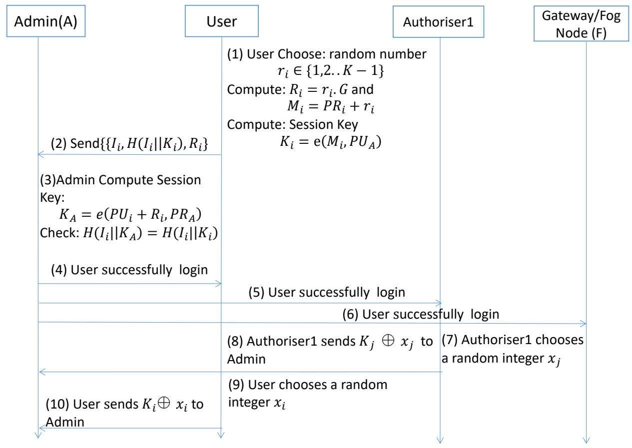

Fig. 3. Session key establishment using Bilinear Pairing.

The *Admin* computes the session key using the public key of the *User* and its own private key

$$K_A = e(PU_i + R_i, PR_A)$$

and verifies that

$$H(I_i||K_A) = H(I_i||K_i).$$

Then the *Admin* will intimate *User*, *Authoriser1* and *Gateway* about successful login of *User*.

Authoriser1 will choose a random integer and send to the *Admin* by encrypting with K_j.

$$\textit{Authoriser1 -> Admin :}\ K_j \oplus X_j$$

Similarly, *User* choose a random integer X_i and send to the *Admin* by encrypting with K_i.

$$\textit{User -> Admin :}\ K_i \oplus X_i$$

Session key thus established will be updated periodically.

4.3.2 Authorisation Phase: Multi-Party Authorisation using Shamir's Secret Sharing

Any *User* I_i requesting access to an *IoT device* SD_k must first send a request to the *Admin* aka MQTT server encrypted by session key K_i

$$\textit{User -> Admin:}\ K_i \oplus SD_k.$$

After verification of the request, the *Admin* will apply Shamir's Secret Sharing to generate shares from the secret S. The computed shares S_j, Device ID SD_k and hash of User Id and Device ID $H'(I_i||SD_k)$ will be distributed to all the *Authorisers* by encrypting with K_j

$$\textit{Admin -> Authoriser:}\ K_j \oplus S_j, K_j \oplus SD_k, H'(I_i||SD_k).$$

Admin also share the Secret S, SD_k and $H'(I_i||SD_k)$ to the *Gateway/Fog node* securely by XOR based encryption with K_F

$$\textit{Admin -> Gateway:}\ K_F \oplus S\ , K_F \oplus SD_k\ , H'(I_i||SD_k).$$

Then the *User* I_i submits its request for access to the *IoT device* SD_K from *Authorisers*. The *Authoriser* verify that $H'(I_i||SD_k) = H(I_i||SD_k)$ and may give permission by sending share S_j

$$\textit{Authoriser -> User:}\ S_j \oplus SD_k.$$

If the *User* manages threshold t numbers of authorisation, it computes S and sends $H(S)$ to the *Gateway*. After verifying that

$$H'(I_i||SD_k) = H(I_i||SD_k) \text{ and } H(S) = H'(S),$$

the *Gateway* allows the *User* access to *IoT device* SD_k. *User* can now access SD_k with secret S as the session key for secure communication. All the steps of the authorisation phase are depicted in Fig. 5 [on the next page]. Access permission will be time bound and after expiry fresh request is to be generated by the *User*.

5. Result and Analysis

All our programs were executed on MacBook Pro (13 inch, M1, 2020) with 8.0 GB RAM and macOS Monterey. An Android application, developed using Android Studio Chipmunk (2021.2.1 Canary 1), Kotlin 1.4.32, JDK 1.8 and Gradle 6.5, has been installed on smartphones with the configuration of Android 10, 4 GB RAM and support for 4G LTE/WiFi 802.11 [32]. An IoT network with Raspberry Pi3 as a *Gateway* and DHT sensor as *IoT device* is configured which communicates with the traditional network over Wifi/4G LTE. MQTT3.1.1 facilitates communication between Raspberry Pi and smartphones. A glimpse of the testbed is provided in Fig. 4.

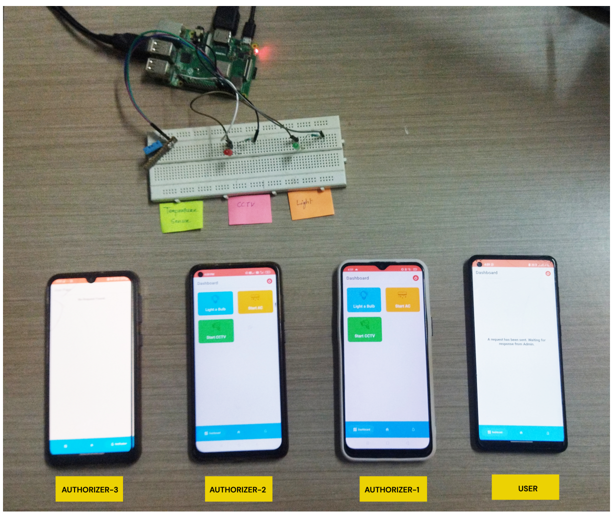

Fig. 4. Prototype setup.

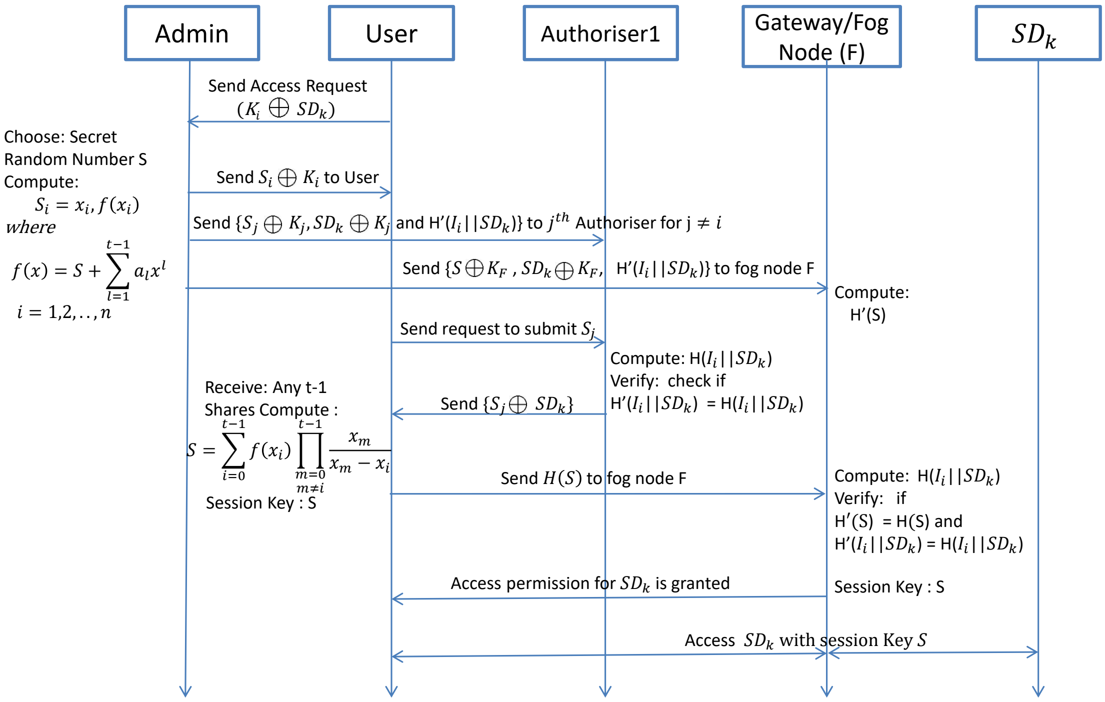

Fig. 5. Multi-party authorisation using Shamir's Secret Sharing.

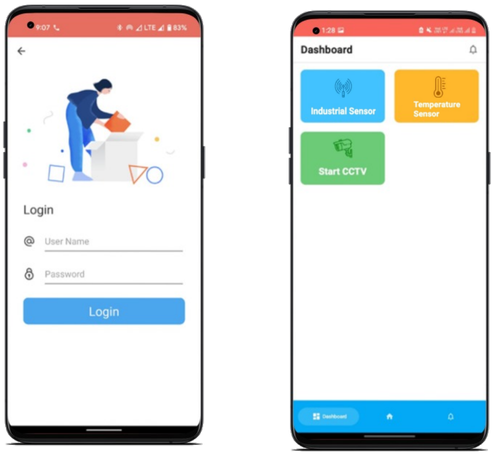

Fig. 6. Login interface.

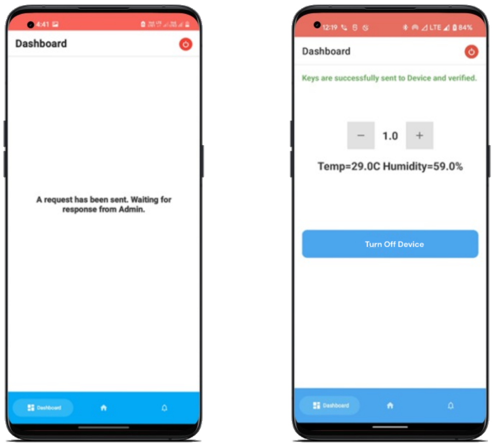

Fig. 8. Device control interface.

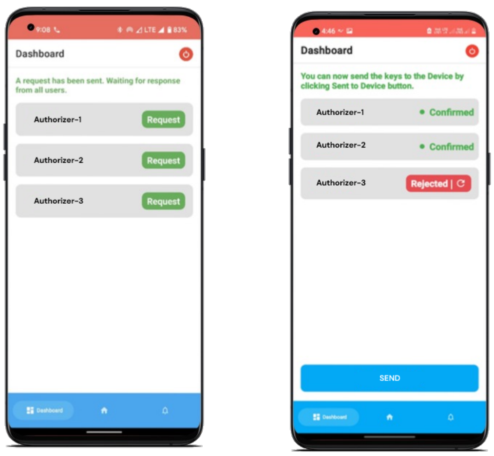

Fig. 7. User interface.

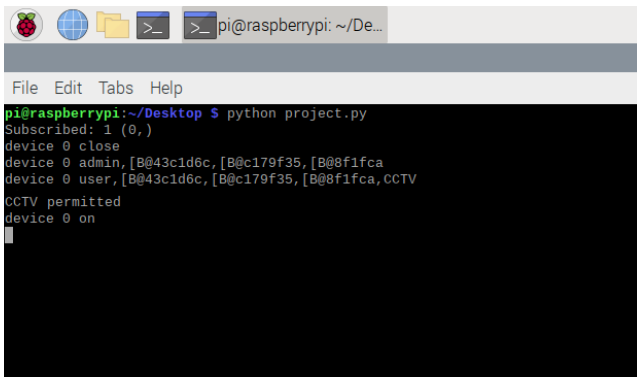

Fig. 9. Snapshot of Raspberry Pi interface.

The Bilinear Pairing and Shamir's Secret Sharing cryptosystem are implemented in using Python 3.6.5 [33]. The programs adopt the Pairing-Based Cryptography (PBC) library version-0.5.14 [34]. Pairing is over a 256-bit BN curve and provide 128-bit security. Shamir's Secret Sharing is working on GF(256) where shares are coded as a GF(256) polynomial and secret S is the aggregated value of those polynomials. The scheme used a lightweight version of the SHA-3 with 10*1 padding rule for message greater than 512, and its corresponding block size is 72 bytes.

The Android application supports three different types of login: *Admin*, *Authoriser* and *User*. Three smartphones are configured as *Authoriser1*, *Authoriser2* and *Authoriser3* and *User* is configured on a fourth smartphone. After login a *User* requests access to the *IoT device* as shown in Fig. 6. Figure 7 shows that *User* has got the permission from *Authoriser1* and *Authoriser2*, while *Authoriser3* rejected *User's* request. After getting threshold numbers of authorisations *User* has got access to DHT sensor data through *Gateway* as shown in Fig. 8 and Fig. 9.

Figure 12 [on the next page] describes the step by step working of the whole system as detailed below:

1) *User* sends *IoT device* access request to *Admin*.
2) *Admin* applies Shamir's Secret Sharing to computes n shares from Secret S, where n is number of *Authoriser*.
3) *Admin* distributes shares to all the *Authorisers*.
4) *Admin* sends secret S to *Gateway* (Raspberry Pi).
5) *User* request for authorisation from *Authoriser1*, *Authoriser2*, *Authoriser3*.
6) *Authoriser1* and *Authoriser2* give permission to *User* for *IoT device* access, but *Authoriser3* rejects.
7) *User* successfully computes secret S after getting threshold number of permissions and sends to *Gateway*.
8) *Gateway* grants access to *User* subject to verification of secret S.

5.1 Security Analysis

We have done the formal security verification of the proposed system using Automated Validation of Internet Security Protocols and Applications (AVISPA) tool [35]. We designed the system using high-level protocol specification language (HLPSL) which is a role-oriented language. Necessary roles are assigned to *Admin*, *Authoriser*, *Gateway* and *User* as shown in the Fig. 10. The proposed system is validated for its executability on the HLPSL specification. The result of verification by constraint logic-based attack searcher (CL- AtSe) backend confirms that proposed scheme is safe and resistant to replay attack and man in the middle attack under DY threat model as shown in Fig. 11.

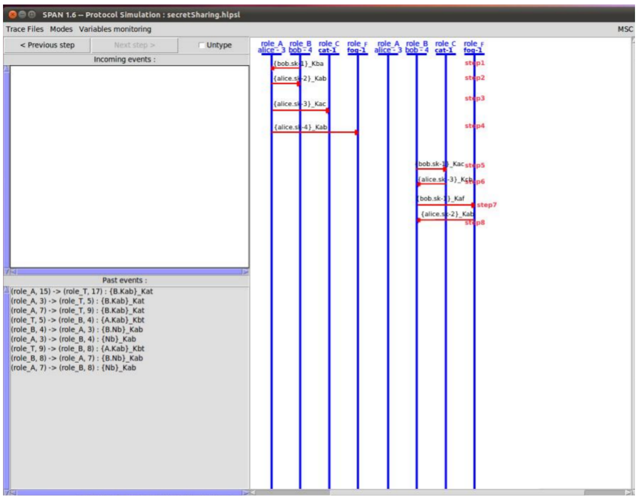

Fig. 10. Role assignment in HLPSL.

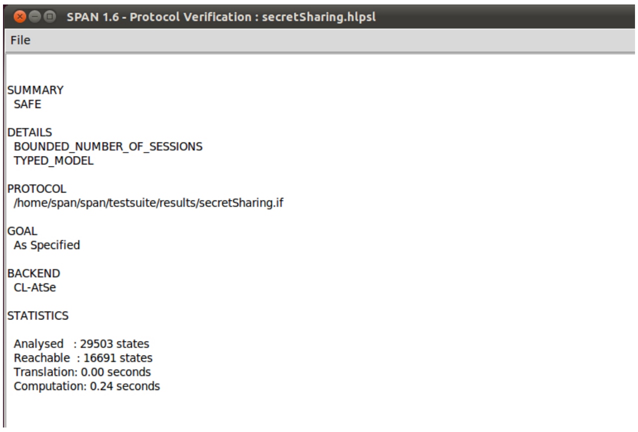

Fig. 11. Protocol status in CL-AtSE.

An informal security analysis of the robustness of the proposed scheme against various common attacks is provided below.

Spoofing Attack
Our proposed system is immune to spoofing as all stakeholders are identified to *Admin* by pairwise session keys K_i established using bilinear pairing during registration phase. Further *User* and *IoT device* identity are verified by *Authorisers* and *Fog node* against the stored hash $H(I_i||SD_k)$.

Man In the Middle Attack
An adversary trying to initiate a new session with *Gateway* parallel to an existing session must have to know secret S. But S is only known to *User* I_i after getting authorisation from t number of *Authorisers*. Also Hash of *User* and Device Id $H(I_i||SD_k)$ is used to verify every request for an *IoT device* access. Further, as all communications are encrypted using XOR based encryption, even if an attacker captures a message, it will not be able to decipher it. This establishes resistance to MitM attack.

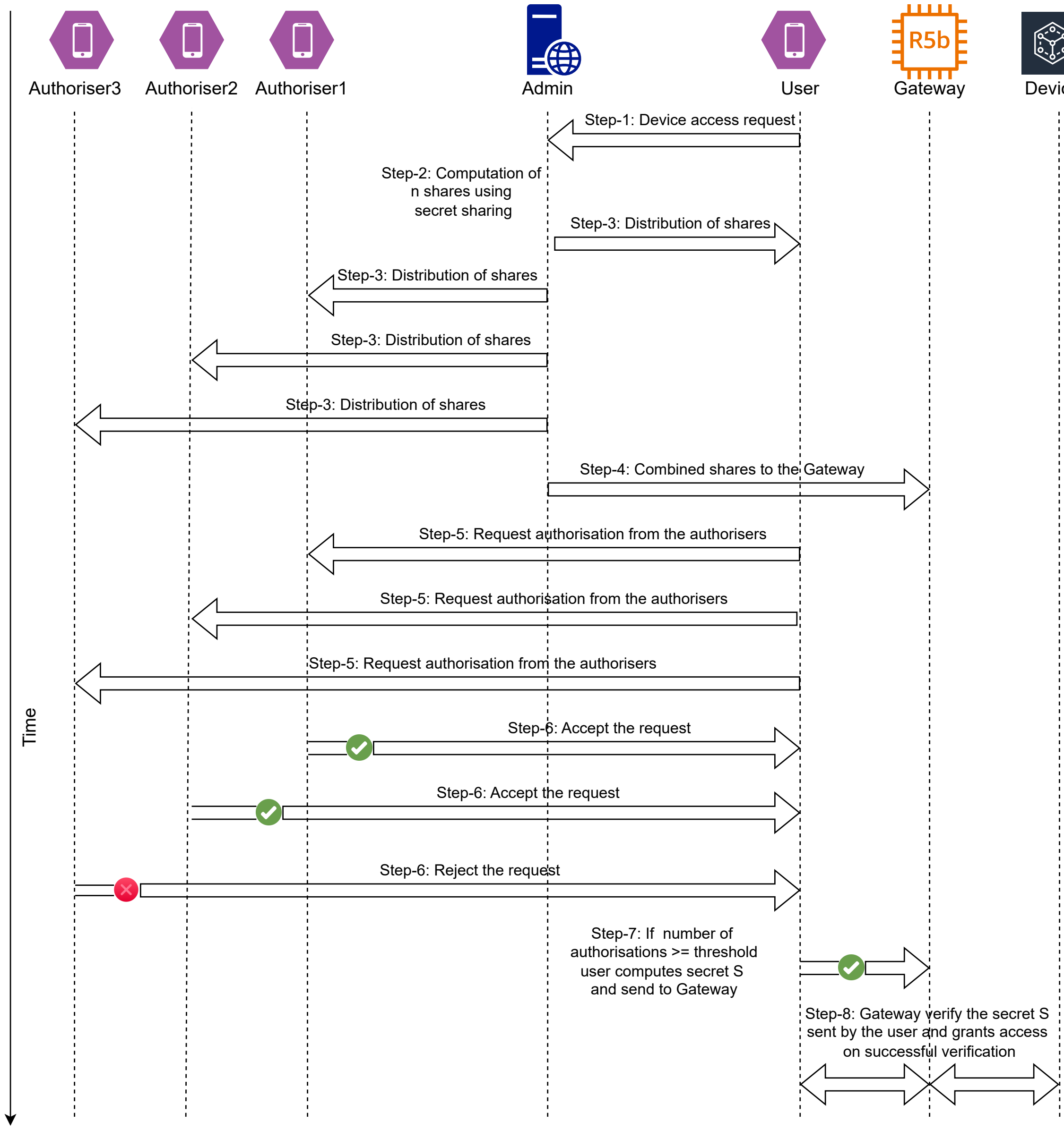

Fig. 12. Sequence diagram of the system in a three-authoriser and one user scenario.

Device Capture Attack
Even if an attacker captures the smartphone, still can't do any wrong without login credentials of the *User*, *Admin* or *Authorisers*. And chances of getting hold of the smartphone during an ongoing login session is very less.

Insider or Collusion Attack
Admin has to be fully secure, it can't be compromised. The system is resilient against $n - t$ *Authorisers* compromise because of inherent properties of (t, n) secret sharing scheme. Similarly, a compromised *User* will need permission from at least t *Authorisers* for getting data from *IoT device*. As mentioned above, spoofing the identity of a *User* or *Authoriser* is not possible in the proposed system.

Offline Password Crack
Session keys established during registrations are periodically renewed, so even if an attacker does crack the password after incurring huge cost in terms of time and computation power, periodic session key change will nullify the attack. Computational difficulty of Bilinear Pairing protects against brute force and guessing attempts of keys.

Replay and Preplay Attack
Every time a *User* requests access to a *IoT device*, fresh secret S and shares are generated by *Admin* for distribution to the *Authorisers*. Further, every request is associated with $H(I_i||SD_k)$, hash of *User* Id and Device Id, so an eavesdropper trying to reuse the previous secret, or pre use some random secret will fail.

Forward and Backward Secrecy
Session keys are pairwise and periodically renewed by running a fresh round of Bilinear Pairing. Again, every *IoT device* request is associated with a new Secret S and its corresponding shares leading to full forward and backward secrecy.

Ownership Transfer Attack [31]
Proposed scheme deals with authorisation at the *Gateway* level directly without the involvement of IoT clouds or Third Party Cloud. So it is resistant against this attack.

Device Sharing Attack [31]
For the same reason as above, device sharing attacks are not possible in the proposed scheme.

Denial of Service Attack
Every *User* must register with *Admin* to be a part of the system. A *User* trying to launch a DoS attack must spoof its identity. But as proved above, the system is resilient against spoofing attacks by authenticating *User* based on pairwise session key K_i. In addition to that if a *User* spoofs its identity to I'_i, then $H(I'_i||SD_k)$ will not match $H(I_i||SD_k)$, thus it proves resistance of the proposed scheme to DoS attack.

Anonymity and Untraceability
User and Device Ids not included in messages over public channels. Permissions are time bound and a fresh request initiates a new session of the multi party authorisation making it impossible to link two communications between the same *Users*.

It is evident from the above analysis that the proposed scheme is resistant to the most prominent threats to IoT applications. Combination of pairwise session keys, hashing, XOR based encryption, (t, n) secret sharing and login based access in Android application makes the system immune to the above attacks. Resilience and security of the proposed system are premised on the incorporation of these provably secure schemes.

5.2 Performance Evaluation

This section illustrates the performance evaluation of the proposed system focusing on computation cost, communication cost, storage cost and running time evaluations. Login time is primarily determined by the Bilinear Pairing operations between *Admin* and *Authoriser* or *User* for deciding pairwise session keys. Likewise, major components of Authorisation time include computation of the shares by Shamir's Secret Sharing, distribution of shares to the *Authorisers* and permission from *Authorisers* to *User*. Hence, both Login and Authorisation time are sensitive to the increasing number of *authorisers* as shown in Fig. 13. But as seen from the plot, the increase is linear and well within the acceptable limit confirming the scalability of the proposed system. We have assumed all the responses within a maximum delay of 1 ms. All experimental results are taken from the average value of 20 runs.

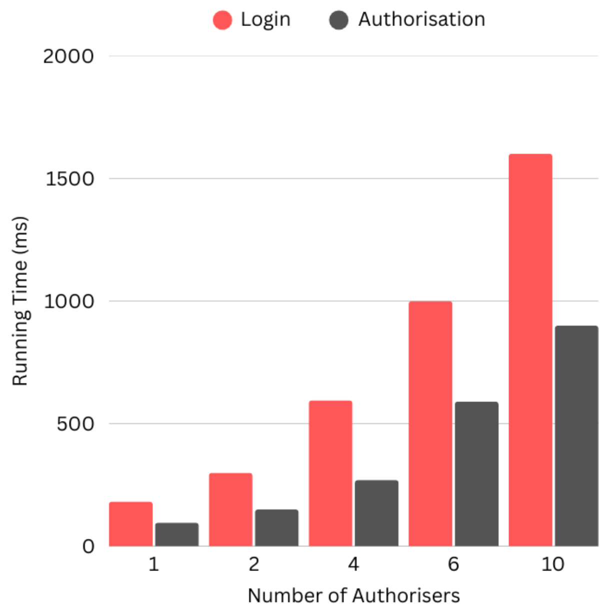

Fig. 13. Running time of login and authorisation phase.

The performance of our MPA protocol is measured in terms of computation cost, communication cost, storage cost and compared against state of the art protocols of Chaudhary et al. [21] and Sultan et al. [28]. Computation cost consists of the time required for the following basic operations T_{h} (Hash), $T_{G_{\mathrm{a}}}$ (A point addition on G elements), T_{bp} (Bilinear Pairing), $T_{G_{\mathrm{sm}}}$(A scalar multiplication on G elements), $T_{\mathrm{SS_D}}$(Secret Sharing share computation), $T_{\mathrm{SS_R}}$ (Secret sharing secret reconstruction), $T_{\mathrm{e/d}}$ (Symmetric encryption/decryption). Only computation intensive operation costs have been considered by ignoring XOR, concatenation costs and in Shamir's Secret Sharing threshold t is kept equal to n to simulate worst case upper bound. Experimental evaluations, over an average of 20 readings, have established the values of $T_{\mathrm{h}} = 0.0187$ ms, $T_{G_{\mathrm{a}}} = 0.0811$ ms, $T_{\mathrm{bp}} = 42$ ms, $T_{G_{\mathrm{sm}}} = 33.24$ ms, $T_{\mathrm{SS_D}} = 57.2$ ms, $T_{\mathrm{SS_R}} = 39.33$ ms and $T_{\mathrm{e/d}} = 0.032$ ms and total computation cost is reported in Tab. 2.

Similarly, communication and storage costs are measured by calculating the parameters, l_{pk_G} (length of a asymmetric key on elements of G (128 bits)), l_{k} (length of a session key (128 bits)), l_{id} (length of any identifier (32 bits)), l_{SS} (length of a secret or share (256 bits)), l_{hash} (length of a SHA3-512 hash digest (512 bits)), l_{rand} (length of a random number (128 bits)) and l_{m} (length of a general message (8 bits)), transmitted over the network and stored in each entity. Table 3 depicts the storage overhead at each entity i.e. *Admin*, *User*, *Authoriser* and *Gateway*. From Tab. 2 and Tab. 3 it is evident that the proposed system is performing better than the state of the art approaches in terms of computation, communication and storage overhead.

Scheme	Computation cost			Communication cost		
	Login phase	Authorisation phase	Total	Login phase	Authorisation phase	Total
Proposed	$(2n+4)(T_h+T_{G_a}+T_{bp})+(2n+5)T_{G_{sm}}$ = **150.67*n*+334.59**	$(n+4)T_h+T_{SS_D}+T_{SS_R}+2T_{e/d}$ = **0.0187*n*+96.66**	**150.68*n* +431.25**	$(n+2)l_{rand}+l_{hash}+l_{id}+(n+2)l_m$ = **17*n*+102**	$(n+2)l_{hash}+(2n+2)l_{SS}+(n+2)l_{id}+(n+1)l_m$ = **133*n*+201**	**150*n*+303**
RMA-CPABE [21]	$(2n+23)T_{G_{sm}}$ = **66.48*n*+764.52**	$(5n+7)T_{G_{sm}}+3nT_{bp}+259n+520$ = **551.2*n*+750.68**	617.68*n* +1515.2	$(n+1)(l_G+l_{G_T})+nl_p+l_{id}+l_k+2l_m$ **28*n*+619**	$(2n+3)l_G+(n+2)l_{id}+nl_k+nl_p$ **309*n*+78**	337*n*+697
ICAuth [28]	$(n-1)T_{G_{sm}}$ = **33.24*n*–33.24**	$(3n+1)T_{G_{sm}}+(10n-9)T_{bp}+259$ = **519.72*n*–85.76**	552.96*n* –119	$(n+1)l_G+nl_p+nl_f+l_m$ **104*n*+57**	$(n+2)l_G+l_{id}+l_{G_T}+2l_m$ **32*n*+280**	136*n*+337

n is the number of *authorisers*

Tab. 2. Computation and communication cost comparison.

Scheme	Admin	User	Authoriser x n	Gateway
Proposed	$(n+4)l_{pk_G}+(n+2)l_k+(n+3)l_{id}+(n+1)l_{SS}+l_{hash}$ = **68*n*+204**	$2l_{pk_G}+l_k+l_{id}+(n+1)l_{SS}+l_{hash}$ = **32*n*+148**	$2l_{pk_G}+l_k+2l_{id}+l_{SS}+l_{hash}$ = **152**	$2l_{pk_G}+l_k+2l_{id}+l_{SS}+2l_{hash}$ = **216**
RMA-CPABE [21]	$(21n+1)l_G+l_{G_T}$ = **276*n*+768**	$3nl_G+4l_{G_T}$ = **768*n*+2048**	$4l_p$ = **1024**	$12nl_G$ = **3072*n***
ICAuth [28]	$(n+1)l_G+l_{G_T}$ = **256*n*+768**	$(n-1)l_G$ = **256*n*–256**	$(n+1)l_G+l_{G_T}$ = **256*n*+768**	——

n is the number of *authorisers*

Tab. 3. Storage cost comparison.

Scheme	Contribution	Lightweight, Low cost	Dynamic authorisation policy	Prototype	Formal security analysis	Key technology	Application
[4]	Multi party authorisation	×,×	×	×	✓	Self Sovereign Identity, SMPC, Threshold Cryptography	Electronic Health Record
[8]	Multi party authorisation	×,×	×	✓	✓	Blockchain	IPFS based
[17]	Multi party authenticated encryption	×,×	×	×	✓	Authenticated encryption, data aggregation	NB IoT 5G
[20]	Multi party access control	×,×	×	×	×	Homomorphic Encryption and Secure Function Evaluation	Social Network
[21]	Multi authority access control	✓,×	✓	×	✓	CP-ABE	IoT data access control
[23]	Multi party authentication	✓,×	×	×	✓	Lattice based IBE	E healthcare
[24]	Multi party verification	×,×	×	×	✓	Visual Secret Sharing, RSA, SHA-256	Multi Party Secure Computing
[25]	Secure multi party computation	✓,×	×	×	✓	Secret Sharing	Industrial IoT
[26]	Multi party secret sharing	✓,×	×	×	×	Image Secret Sharing, Optics based Image Cryptography	Large Scale Visual Data
[27]	Single user authorisation	×,×	×	✓	✓	Access Token	Web
Proposed	Multi party authorisation	✓,✓	✓	✓	✓	Bilinear Pairing and Shamir's Secret Sharing	IoT

Tab. 4. Comparison of the proposed scheme against state of the art schemes.

Feature comparison of the proposed multi party authorisation scheme with other similar schemes is provided in Tab. 4. As evident from the table, the proposed scheme stands out from the other state of the art approaches with its unique features of lightweight and low cost, dynamic authorisation policy and app based test bed design. Lightweight operations are ensured by the use of only XOR based encryptions, while computation intensive Bilinear Pairing and Shamir's Secret Sharing operations are performed only at the *Admin*, *Authorisers*, *User* and *Gateway*. As mentioned in Sec. 4.1, these devices are resource rich or partially resource rich, while resource constrained *IoT devices* are only engaged with lightweight operations. We have carefully chosen only low cost components while developing the prototype thus making it suitable for low cost application development. Under dynamic authorisation policy, *Admin* can control the number of permissions required by setting a suitable value of threshold t, whereas asymmetric authorisation, where different *Authorisers* have different weight of their permission, can be handled by distributing different number of shares in the Login phase.

6. Conclusion and Future Work

In this work we have developed a novel Bilinear Pairing and Shamir's Secret Sharing based multi party authorisation scheme for *IoT device* access. The proposed system can be applied in a wide array of application areas such as IIoT, Smart Home, IoMT etc where multi party authorisation can control access to sensitive devices. After establishing the session key using Bilinear Pairing, *Admin* uses Shamir's Secret Sharing to distribute shares to the *Authorisers*. Any *User* requesting access to an *IoT device* must generate the secret by receiving permissions from at least t number of *Authorisers*. The safety of the scheme is tested successfully with the formal protocol specification tool AVISPA and a prototype has been built using the Raspberry Pi-3, DHT sensors, and Smartphones installed with an android application. The system is found to be scalable in terms of registration and authorisation time against an increasing number of *Authorisers*. Advantage of the proposed scheme is established by comparing with other similar schemes in terms of key parameters. The proposed scheme stands out from the other similar schemes with its unique contribution of dynamic authorisation policy and prototype development. Attack analysis proves the resistance of the system to many common attacks.

In the future we are planning to deploy our system in a real IoT environment and validate its performance.

References

[1] SUN, P., SHEN, S., WAN, Y., et al. A survey of IoT privacy security: architecture, technology, challenges, and trends. *IEEE Internet of Things Journal*, 2024, vol. 11, no. 21, p. 34567–34591. DOI: 10.1109/JIOT.2024.3372518

[2] XIONG, Y., LUO, M. X. Searchable encryption scheme for large data sets in cloud storage environment. *Radioengineering*, 2024, vol. 33, no. 2, p. 223–235. DOI: 10.13164/re.2024.0223

[3] KARMOUS, N., HIZEM, M., BEN DHIAB, Y., et al. Hybrid cryptographic end-to-end encryption method for protecting IoT devices against MitM attacks. *Radioengineering*, 2024, vol. 33, no. 4, p. 583–592. DOI: 10.13164/re.2024.0583

[4] TAN, K. L., CHI, C. H., LAM, K. Y. Secure and privacy-preserving sharing of personal health records with multi-party pre-authorization verification. *Wireless Networks*, 2024, vol. 30, p. 4773–4795. DOI: 10.1007/s11276-022-03114-6

[5] SHAMIR, A. How to share a secret. *Communications of the ACM*, 2024, vol. 22, no. 11, p. 612–613. DOI: 10.1145/359168.359176

[6] CHEN, C., SHIH, T., TSAI, Y., et al. A bilinear pairing-based dynamic key management and authentication for wireless sensor networks. *Journal of Sensors*, 2015, vol. 2015, no. 1, p. 1–14. DOI: 10.1155/2015/534657

[7] AMIN, R., ISLAM, S. H., VIJAYAKUMAR, P., et al. A robust and efficient bilinear pairing based mutual authentication and session key verification over insecure communication. *Multimedia Tools and Applications*, 2018, vol. 77, p. 11041–11066. DOI: 10.1007/s11042-017-4996-z

[8] BATTAH, A. A., MADINE, M. M., ALZAABI, H., et al. Blockchain-based multi-party authorization for accessing IPFS encrypted data. *IEEE Access*, 2020, vol. 8, p. 196813–196825. DOI: 10.1109/ACCESS.2020.3034260

[9] MANDAL, S., BERA, B., SUTRALA, A. K., et al. Certificateless signcryption based three factor user access control scheme for IoT environment. *IEEE Internet of Things Journal*, 2020, vol. 7, no. 4, p. 3184–3197. DOI: 10.1109/JIOT.2020.2966242

[10] LIN, C., HE, D., KUMAR, N., et al. HomeChain: A blockchain-based secure mutual authentication system for smart homes. *IEEE Internet of Things Journal*, 2019, vol. 7, no. 2, p. 818–829. DOI: 10.1109/JIOT.2019.2944400

[11] CHANDRAMOULI, A., CHOUDHURY, A., PATRA, A. A survey on perfectly secure verifiable secret-sharing. *ACM Computing Surveys (CSUR)*, 2022, vol. 54, no. 11, p. 1–36. DOI: 10.1145/3512344

[12] ZHAO, C., ZHAO, S., ZHAO, M., et al. Secure multi-party computation: Theory, practice and applications. *Information Sciences*, 2019, vol. 476, p. 357–372. DOI: 10.1016/j.ins.2018.10.024

[13] ARAFIN, M. T., QU, G. Secret sharing and multi-user authentication: From visual cryptography to RRAM circuits. In *Proceedings of the 26th edition on Great Lakes Symposium on VLSI*. Boston (USA). 2016, p. 169–174. DOI: 10.1145/2902961.2903039

[14] LOPES, A. P. G., HILGERT, L. O., GONDIM, P. R., et al. Secret sharing-based authentication and key agreement protocol for machine-type communications. *International Journal of Distributed Sensor Networks*, 2019, vol. 15, no. 4, p. 1–21. DOI: 10.1177/1550147719841003

[15] HU, H., AHN, G. J., JORGENSEN, J. Multiparty access control for online social networks: Model and mechanisms. *IEEE Transactions on Knowledge and Data Engineering*, 2012, vol. 25, no. 7, p. 1614–1627. DOI: 10.1109/TKDE.2012.97

[16] PACI, F., SQUICCIARINI, A., ZANNONE, N. Survey on access control for community-centered collaborative systems. *ACM Computing Surveys (CSUR)*, 2018, vol. 51, no. 1, p. 1–38. DOI: 10.1145/3146025

[17] ZHANG, Y., REN, F., WU, A., et al. Certificateless multi-party authenticated encryption for NB-IoT terminals in 5G networks. *IEEE Access*, 2019, vol. 7, p. 114721–114730. DOI: 10.1109/ACCESS.2019.2936123

[18] SIKDER, A. K., BABUN, L., CELIK, Z. B., et al. Kratos: Multi-user multi-device-aware access control system for the smart home. In *Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. Linz (Austria). 2020, p. 1–12. DOI: 10.1145/3395351.3399358

[19] SUN, J., YANG, Y., LIU, Z., et al. Multi authority criteria based encryption scheme for IoT. *Security and Communication Networks*, 2021, vol. 2021, p. 1–15. DOI: 10.1155/2021/9174630

[20] SHEIKHALISHAHI, M., STORK, I., ZANNONE, N. Privacy-preserving policy evaluation in multi-party access control. *Journal of Computer Security*, 2021, vol. 29, no. 6, p. 613–650. DOI: 10.3233/JCS-200007

[21] CHAUDHARY, C. K., SARMA, R., BARBHUIYA, F. A. RMA-CPABE: A multi-authority CPABE scheme with reduced ciphertext size for IoT devices. *Future Generation Computer Systems*, 2023, vol. 138, p. 226–242. DOI: 10.1016/j.future.2022.08.017

[22] EMAN, R. D., JAHAN, M., KABIR, U. A multi device user authentication mechanism for Internet of Things. *IET Networks*, 2023, vol. 12, no. 5, p. 229–249. DOI: 10.1049/ntw2.12088

[23] SAHU, A. K., SHARMA, S., PUTHAL, D. Lightweight multi-party authentication and key agreement protocol in IoT-based E-healthcare service. *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM)*, 2021, vol. 17, no. 2, p. 1–20. DOI: 10.1145/3398039

[24] YAN, X., LI, J., PAN, Z., et al. Multiparty verification in image secret sharing. *Information Sciences*, 2021, vol. 562, p. 475–490. DOI: 10.1016/j.ins.2021.03.029

[25] LIU, D., YU, G., ZHONG, Z., et al. Secure multi-party computation with secret sharing for real-time data aggregation in IIoT. *Computer Communications*, 2024, vol. 224, p. 159–168. DOI: 10.1016/j.comcom.2024.06.002

[26] KIM, Y., JEONG, O., MOON, I., et al. Multiparty random phase wrapping secret-sharing systems for visual data security. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2025, early access, p. 1–15. DOI: 10.1109/TSMC.2025.3541827

[27] *OAuth 2.0*. [Online] Accessed 2025-02-26. Available at: https://oauth.net/2/

[28] SULTAN, N. H., BARBHUIYA, F. A., LAURENT, M. ICAuth: A secure and scalable owner delegated inter-cloud authorization. *Future Generation Computer Systems*, 2018, vol. 88, p. 319–332. DOI: 10.1016/j.future.2018.05.066

[29] KINKELIN, H., NIEDERMAYER, H., MULLER, M., et al. Multi-party authorization and conflict mediation for decentralized configuration management processes. In *Proceedings of the IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*. Virginia (USA), 2019, p. 5–8. ISSN: 1573-0077

[30] XUE, Q., WANG, C., XUE, Z., et al. CP-ABE with multi-authorization centers and supporting outsourcing encryption and decryption. In *Proceedings of the 2nd International Conference on Electronic Information Technology and Smart Agriculture (ICEITSA)*. Huaihua (China), 2022, p. 275–281. DOI: 10.1109/ICEITSA57468.2022.00054

[31] CHEN, J., XU, F., DONG, S., et al. Authorisation inconsistency in IoT third party integration. *IET Information Security*, 2022, vol. 16, no. 2, p. 133–143. DOI: 10.1049/ise2.12043

[32] *Lightweight Multi Party Authorisation Android Application*. [Online] Accessed 2025-05-25. Available at: https://github.com/Dipankar-2018/LMPA-ANDROID-APPLICATION/

[33] *Charm: A Framework for Rapidly Prototyping Cryptosystems*. [Online] Accessed 2025-04-05. Available at: https://github.com/JHUISI/charm

[34] *PBC Library*. [Online] Accessed 2025-04-05. Available at: https://crypto.stanford.edu/pbc/

[35] *Automated Validation of Internet Security Protocols and Applications*. [Online] Accessed 2025-03-10. Available at: https://www.avispa-project.org/

About the Authors . . .

Bikramjit CHOUDHURY (Member, IEEE) is currently an Assistant Professor with the Department of Computer Science and Engineering, Central Institute of Technology Kokrajhar, Assam, India with more than 12 years of experience in teaching and research. He has published research articles in many international conferences and journals. His research interests include the Internet of Things security, Blockchain, AI and Network Security. He is a member of ACM and IEI.

Amitava NAG (Senior Member, IEEE) is currently a Professor in Computer Science and Engineering with the Central Institute of Technology Kokrajhar, Assam, India. He has more than 50 research publications in various international journals and conference proceedings. His research interests include the IoT, information security, advanced machine learning, deep learning, and computer vision. He is a fellow of IEI.

Dipankar RABHA got his B.Tech in Information Technology from Central Institute of Technology Kokrajhar. He is actively engaged with software development and has successfully established two startups in the IT field. Currently he is engaged as a team lead in the e-Office project of the Bodoland Territorial Council in Kokrajhar, Assam, India.

Sukumar NANDI (Senior Member, IEEE) received the Ph.D. degree in Computer Science and Engineering from the Indian Institute of Technology Kharagpur, India, in 1995. He was a Visiting Senior Fellow with NTU, Singapore, from 2002 to 2003. He is currently a Senior Professor with the Department of Computer Science and Engineering, Indian Institute of Technology Guwahati, India. He has more than 450 international journals and conference publications. His areas of research interests include computer networks, computer and network security, machine learning, VLSI, computer architecture, and computational linguistic. He is a Senior Member of ACM. He is also a fellow of the Indian National Academy of Engineering, the Asia-Pacific Artificial Intelligence Association, the Institution of Engineers (India), and the Institution of Electronics and Telecommunication Engineers (India).