Earth Science Informatics
https://doi.org/10.1007/s12145-023-01194-2

RESEARCH

# Enhanced Elliptic Curve- Diffie Hellman Technique with Bigdata Analytics for Satellite Image Security Enhancement in Internet of Things Systems

**N. Madhusudhana Reddy[1] · Anil Kumar Budati[2] · Shayla Islam[3] · Gajula Ramesh[4]**

Received: 11 October 2023 / Accepted: 11 December 2023


**Abstract**
With the emergence of cloud eco-system and technologies like Internet of Things (IoT), bit data analytics became essential to reap benefits of maintaining large volumes of data. As there is amalgamation of different devices, protocols, standard and use cases linked to IoT, there is increasing risk of security. IoT applications are vulnerable due to lack of security standards at global level. There is need for continuous efforts to provide end-to-end security in IoT applications. Sensor networks associated with IoT are resource constrained but produce large volumes of data or big data. In such environment, more light weight security primitives. Elliptic Curve Diffie Hellman (ECDH) is one such lightweight scheme for secure key exchange among connected devices. Nevertheless, ECDH is found vulnerable to attacks. To address this problem, we proposed a scheme known as E-ECDH (ECDH+SIGH) which is an enhanced version of ECDH. Our scheme is designed to enhance security level in IoT use cases. To evaluate our scheme, we used an IoT use case meant for anomaly detection in healthcare context. This application is in distributed environment where cloud infrastructure, IoT platform and Message Queue Telemetry Transport (MQTT) protocol are involved. Our experimental study showed that E-ECDH improves level of security in given IoT application and found to be better than existing security schemes.

**Keywords** Big data security · Internet of Things (IoT) · Diffie-Hellman · End to end security · IoT systems

## Introduction

With the emergence of novel technologies and distributed computing environments, there has been unprecedented growth in distributed cloud-assisted applications. Particularly Internet of Things (IoT) has enabled connectivity among physical and digital things leading to applications that were never possible earlier. Smart means of data collection and data dissemination are in place with IoT technology. IoT has led to applications like smart home, smart healthcare and smart city to mention few. This list of application is growing faster. Humans are exposed to unprecedented technology benefits and also possible risks. For instance, IoT technology could understand a thinking pattern of a human brain. Such sensitive problems also occur in addition to technology benefits. Nevertheless, technology cannot be blamed and it is the responsibility of people to use it for constructive purposes. An important use case of IoT is precision agriculture (Baranwal et al., 2016) which helps in making a technology driven farming beneficial to farmers. IoT has its influence on different industries. With wearable devices and

Communicated by: Dr S B Goyal

✉ Anil Kumar Budati
anilbudati@gmail.com

N. Madhusudhana Reddy
madhusudhan.nooka@gmail.com

Shayla Islam
shayla@ucsiuniversity.edu.my

Gajula Ramesh
ramesh680@gmail.com

[1] Computer Science & Engineering Department, R G M College Of Engineering &Technology, Nandyal, Andhra Pradesh, India

[2] ICSDI, UCSI University, Malaysia & Associate Professor, Department of ECE, Koneru Lakshmaiah Education Foundation, Hyderabad, India

[3] ICSDI UCSI University, Kuala Lumpur, Malaysia

[4] Department of CSE, Gokaraju Rangaraju Institute of Engineering & Technology, Hyderabad, India

Published online: 20 December 2023

health based sensors, healthcare industry is one such example where IoT has its splendid presence (Savola et al., 2015).

IoT applications do have security vulnerabilities apart from opportunities. Their security issues are classified into technical, methodological and organizational. The methodological category encompasses process models, protection of runtime, security control prioritization and assurance of security. With respect to organizational category, it involves security linked to human factors, organizational needs of security, security policies, standards, usage of third party components and security goals. Technical category involves IoT architectures, security to data, security to procedures, security to resources, physical constraints involved, distributed systems and data flows (Nguyen Duc et al., 2017). As explored in (Datta & Bonnet, 2016), there is lack of horizontal development linked to IoT use cases in terms of interoperability, network security, security standards and privacy issues. IoT security aspects include IoT security frameworks (Ammar et al., 2018; Kang et al., 2015) and privacy and security threats (Berkay Celik, 2018; Yashwant & Joshi, 2018). There are many existing security schemes such as RSA. However, as discussed in (Jonsson & Tornkvist, 2017), schemes like RSA cannot be directly used with IoT devices as it involves complexity. There is need for security schemes that are lightweight and compatible with resource constrained IoT devices. Moreover, it is important to propose schemes that are able to work in post quantum security scenarios also. To overcome the problems, we proposed a scheme known as E-ECDH which enables secure communications in an IoT case study application. Our contributions are as follows.

1. We proposed a scheme known as E-ECDH for secure end to end communications in IoT applications leading to robust communications.
2. Python based IoT application, a healthcare application for big data analytics, is used as case study to which proposed security scheme is integrated.
3. Experiments are made to find the utility of the proposed security scheme and its comparison with the existing ones.
4. ECDH and SIDH are combined to have higher level of security to meet PQ situations.

The remainder of the paper is organized as follows. "Related Work" section reviews literature on security to IoT applications. "Motivating Case Study and Problem Definition" section formulates the problem and describes a case study for security implementation.

"IOT case study application "section provides the case study implementation details. "Post quantum cryptography " section provides post quantum cryptography by combining SIDH and ECDH. "Proposed Method " section provides the proposed method. "Results & Discussion" section throws light on results of experiments with a case study IoT use case. "Conclusion" section concludes the research carried out in the paper and gives directions for future scope of the research.

## Related Work

This section reviews security concerns in IoT and also existing works. IoT applications are vulnerable to threats due to involvement of heterogeneous devices and environments. IoT security aspects are investigated in (Riahi et al., 2013) by analyzing may security schemes including asymmetric ones. Each IoT use case with underlying domain specific application has its security loopholes. The reasons for such security issues are plenty including lack of standards and use of diversified non-standard protocols and devices. IoT applications are also integrated with other technologies like blockchain to have secure communications and are maintained in a distributed ledger. Ethereum is one such blockchain platform that can be used with IoT applications. Moreover, IoT scenarios include M2M interactions that involve in data exchange and messaging (Pustišek & Kos, 2018; Datta et al., 2015). In such applications, it is very important to have secure end to end communications. M2M communications might be vulnerable to attacks and data integrity issues besides other possible attacks as discussed in (Tweneboah-Koduah et al., 2017). The vulnerabilities can be attributed to IoT integration and native domain applications. For instance, healthcare domain applications when integrated with IoT, it could be subjected to many kinds of privacy and security attacks. As the applications and environments are so complex with the presence of mobile devices also, it is not easy to control security aspects (Ahamed & Rajan, 2016).

There are different layers in IoT applications as discussed in (Liu & Yan, 2013). Therefore, at each layer security implementation is essential. Thus, it is indispensable to think about complete end to end security solution rather than making specific layer secure. IoT security challenges are plenty as discussed in prior works like (López et al., 2018; Diffie & Hellman, 1976; AL-mawee, 2012; Giuseppe et al., 2020; Li, 2020). The challenges include heterogeneity of hardware, mobility of nodes, use of resource constrained devices, usage of diversified protocols and platforms and lack of global standards (Nguyen et al., 2015). Existing security schemes such as RSA is found not suitable for lightweight connected devices in IoT. Security attacks in IoT use cases is the focus of (Tellez et al., 2016) where reverse engineering is used for making attacks. In (McEliece, 1978; Merkle, 1979) public key systems are studied for their complexity. In (Milne, 1986) two new kinds of asymmetric algorithms based on isomorphism of polynomials and Hidden Fields Equations

(HFE) respectively are defined. Big data and IoT scenarios and security aspects are investigated in (Montgomery, 1987; Sutjiatmo et al., 2019; Azmoodeh et al., 2019) while big data for sustainable industrialization (Al-Garadi et al., 2020), smart use cases (Suma, 2019), multimedia processing with privacy and security of big data (Ejaz & Anpalagan, 2019) are other significant contributions. IoT technology evolution and use of machine learning in IoT scenarios are two important studies (Alferidah & Jhanjhi, 2020; Ande et al., 2020) found. IoT has certain application level protocols such as CoAP as discussed in (Ukil et al., 2014). In (Sreeja et al., 2019) a lightweight symmetric scheme is defined for embedded IoT devices. Hasan et al. (Hasan et al., 2021a) exploited mining technique in IoT along with Quadratic and Fisher Linear discrimination analysis. Shayla et al. (Shayla et al., 2020) proposed a methodology for inter-technology handoff with multi-homing based approach. Hasan et al. (Hasan et al., 2021b) proposed a system for reliability analysis with the help of sensor cloud system and a measurement framework. Shami et al. (Shami et al., 2018) used PSO to achieve control and load balancing in heterogeneous 5G networks. Imran et al. (Imran et al., 2020) proposed a security scheme to protect mobile users' information using fuzzy logic based on sensitive region. In this paper, ECDH and SIDH are combined to have stronger security to meet PQ situations. To overcome the problems in the study we have proposed Enhanced Elliptic Curve Diffie-Hellman (E-ECDH) is an advanced cryptographic scheme that builds upon the foundational principles of the Elliptic Curve Diffie-Hellman (EC-DH) key exchange method. E-ECDH is designed to provide a higher level of security for secure communications in the context of Internet of Things (IoT) applications. This enhanced scheme addresses certain vulnerabilities present in EC-DH and aims to offer stronger protection for sensitive data exchanged between IoT devices and other components within IoT ecosystems.

## Motivating Case Study and Problem Definition

Figure 1 shows a motivating scenario showing the architecture of an IoT application leveraging the IBM Watson IoT Platform follows a structured flow to enable seamless connectivity, data processing, analysis, and integration. At its core are IoT devices equipped with sensors, collecting real-world data. These devices communicate using protocols like MQTT, transmitting data to the IBM Watson IoT Platform. Within the platform, a robust infrastructure manages device onboarding, authentication, and data ingestion. The Message Broker ensures reliable communication, while the Data Storage component securely stores the data for historical analysis. A powerful Rules Engine processes incoming data, triggering predefined actions or alerts based on predefined conditions. This processed data is further fed into analytics tools such as IBM Watson Studio, enabling businesses to gain deeper insights and predictive capabilities. Custom applications and user interfaces allow stakeholders

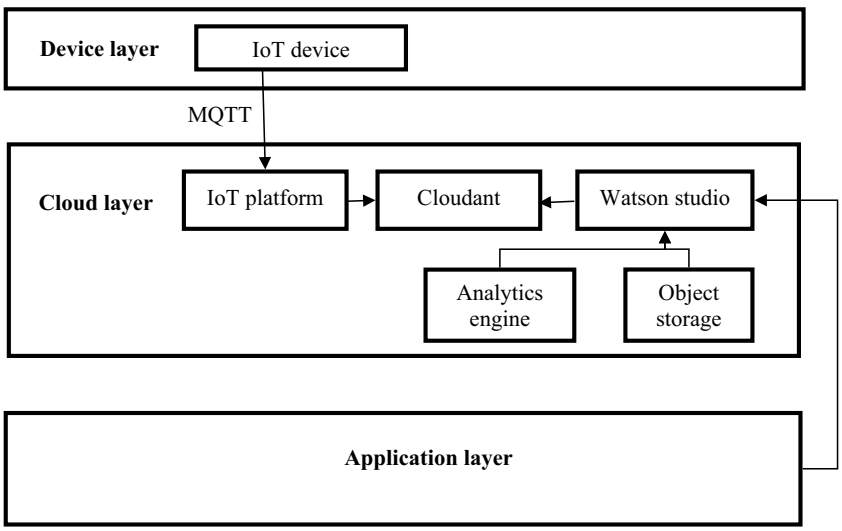


**Fig. 1** Architecture of an IoT application involving IoT device for sensing

IoT has revolutionized applications with unprecedented possibilities. However, it also brings increased security challenges. It is vulnerable to attacks at network level, service level, interface level, device level and even integrity level. IoT devices might be compromised to launch attack. An IoT application might be under the influence of attacker to disrupt services. Network level attacks disturb communications among connect devices. Interface attacks such SQL injection and XSS might cause problems with unwanted services injected. Attacks may also inject false data to pollute original data leading to integrity issues.

to monitor device status, visualize trends, and interact with the IoT ecosystem, while robust security measures safeguard data integrity, device authentication, and access control. Due to presence of increasing attacks, it is desired to have end to end secure communications in IoT use cases.

### RSA

RSA is one of the widely used scheme in different applications. It is asymmetric in nature. It needs two parties to have different key so as to avoid key exchange or key sharing. Each party involved in the communication can have two keys such as private and public. Each party knows the public key of the other party. Among the parties involved in communication, the scheme is made in such a way that each one has private key to decrypt the data sent by any sender because the sender uses public key of the receiver to encrypt data. However, RSA is found complex and not suitable for resource constrained devices in IoT applications. Then Diffie-Hellman is found to be lightweight technique as discussed in "Diffie-Hellman" section.

### Diffie-Hellman

DH is the scheme found to be lightweight when compared with PKI. DH helps in computation of secret key between parties to enable dynamic key exchange. Here is the procedure involved. Both communicating parties come to an agreement to use n and g as prime numbers. These numbers are made public. Then Alice uses X and secrete and performs computation such as A=g^(X )mod n and send the result to Bob. Similarly, Bob considered Y as his secret and performs computation such as Y=g^(Y )mod n and returns the result to Alice. Then K1=B^(X )mod n and K2=A^(Y ) mod n are computations made by Alice and Bob respectively to arrive at key exchange where K1=K2.

Figure 2 illustrates the Diffie-Hellman key exchange which is a cryptographic protocol that enables two parties, Alice and Bob, to establish a shared secret key over an insecure communication channel. This is achieved through a process where both parties independently select private keys and compute corresponding public keys using agreed-upon parameters. These public keys are then exchanged openly. By combining the other party's received public key with their own private key, both Alice and Bob compute the same shared secret key. The security of this scheme relies on the mathematical complexity of calculating discrete logarithms, ensuring that even if an eavesdropper intercepts the public keys, deriving the shared secret without the private keys is computationally infeasible. This elegant approach allows for secure key establishment without the need for secure channels or prior communication, making it a fundamental cornerstone of modern cryptography. This scheme is found to have its security vulnerabilities with replay, brute force and MITM attacks. Due to security vulnerabilities of DH, ECDH scheme is found to be more useful lightweight technique as discussed in "Elliptic Curve-Diffie Hellman" section.

### Elliptic Curve-Diffie Hellman

The Elliptic Curve Diffie-Hellman (ECDH) key exchange scheme is a cryptographic method that enables two parties, Alice and Bob, to establish a shared secret key over an insecure communication channel using elliptic curve cryptography. In this process, both Alice and Bob independently choose private keys and perform scalar multiplication on a predetermined elliptic curve point, resulting in their respective public keys. These public keys are then openly exchanged. By combining the received public key with their private key, both parties compute the same shared secret point. The security of ECDH hinges on the intractability of the elliptic curve discrete logarithm problem, ensuring that unauthorized third parties cannot easily derive the shared secret from the exchanged public keys. ECDH provides strong security with smaller key sizes compared to traditional methods, making it a vital component in modern secure communication protocols, such as SSL/TLS for web encryption. Through ECDH needs smaller key, its security strength is equivalent to that of RSA. Thus algorithms based on ECDH are lightweight and feasible for resource constrained IoT networks. ECDH exploits ECC and thus it is made lightweight as it needs smaller key size with negligible overhead. EC enables ease of computations due to its algebraic addition. As investigated in (Diffie & Hellman, 1976), provided two points like $P =$ (x_P, y_P) and $Q =$ (x_(Q ), y_Q), the slope can be computed as expressed in Eq. 1.

$$S = (y\_Q - y\_P)/(x\_(Q) - x\_P) \tag{1}$$

Then the points are subjected to summation as expressed in Eq. 2 and Eq. 3.

$$x\_R = S\hat{}2 - x\_p - x\_(Q) \tag{2}$$

$$y\_R = -y\_P + S * (x\_P - x\_R) \tag{3}$$

when y_P $/= 0$, the operation $P+P= 2P= R$ is known as doubling operation that is used to redefine Eq. 2 and Eq. 3 resulting in Eq. 4 and Eq. 5.

$$x\_R = (((3 * x\_P\hat{}2 + a))/(2 * y\_p\ ))\hat{}2 - 2 * x\_P \tag{4}$$

$$y\_R = (((3 * x\_P\hat{}2 + a))/(2 * y\_p\ )) * (x\_p - x\_R) - y\_P \tag{5}$$

Thus integration is achieved between EC and DB resulting in ECDH which is reused in the proposed E-ECDH scheme discussed in "IOT case study application" section.

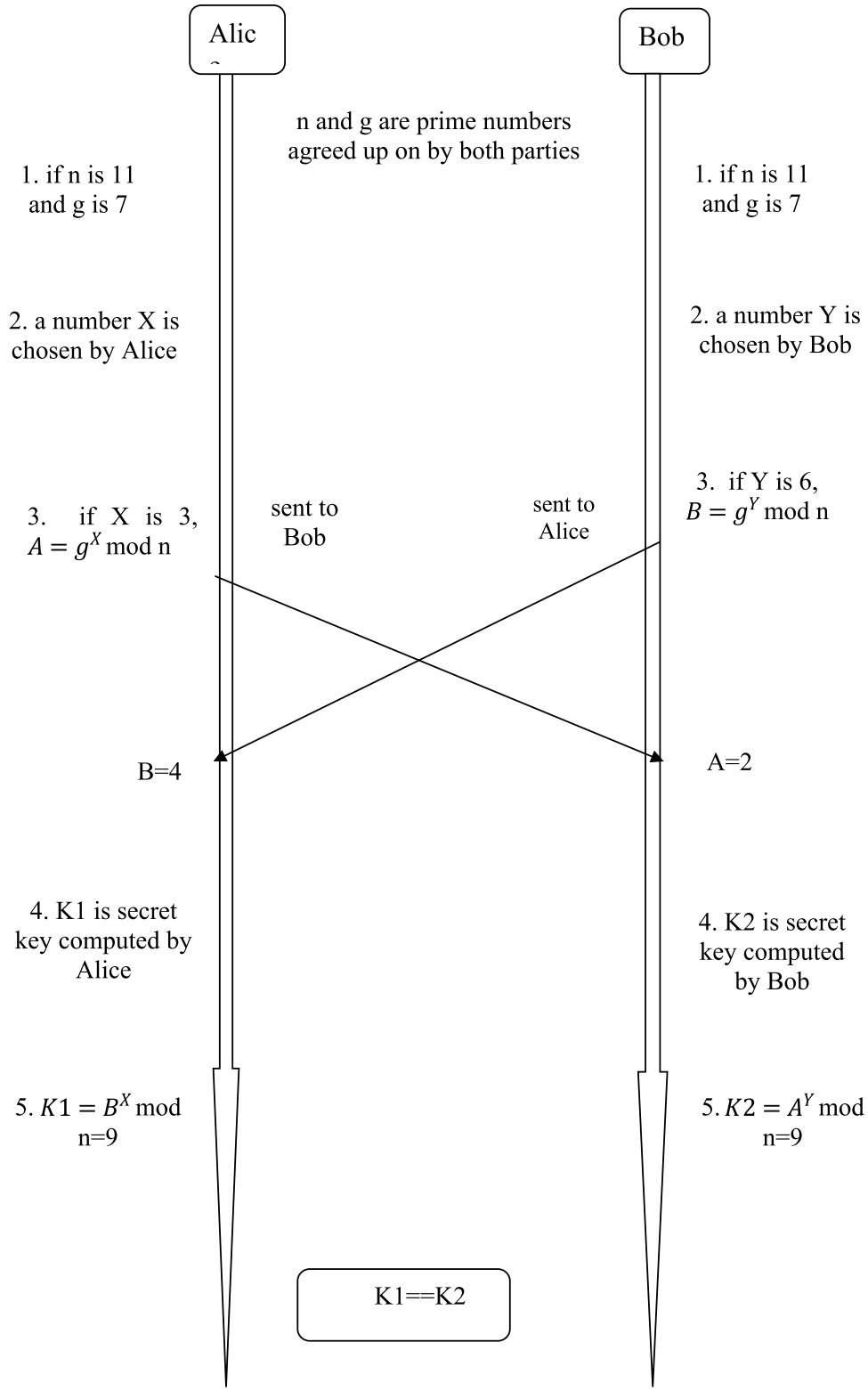


**Fig. 2** Shows key exchange with DH scheme

This kind of scheme is suitable for IoT use cases. The ECDH involves the following operations. Alice, initially, chooses n_A (an integer). This is nothing bit the user's private key. This key is chosen in such a way that it satisfies n_A<n. Then Alice generates public key which is denoted as P_A=n_A*G the base point is denoted as E_q(a, b). Similarly, Bob selects his private key such as n_B where n_B<n. Bob also computed public key denoted as P_B=n_B*G and the

base point is denoted as E_q(a, b). K=n_A*P_B is the secret key of Alice while Bob's secret key is K=n_B*P_A. The result associated with the two computations must be same such as $K = nA*PB = nA*(nB*G) = nB*(nA*G)$.

Figure 3 illustrates the fact that sharing secret key is made possible between two parties using ECDH. Both the parties are able to get same key such as K=(4,2). B= (2,4) is the base point used. The curve E is used to have y^2=x^3+x+6 over z_7. Alice and Bob α=4 and picks β=5 as their secret key respectively. One party computes P= αB=4(2,4)=(6,2) while the other party computes Q=βB=5(2,4)=(1,6) and they mutually exchange it to each other. K_A=αQ=4(1,6)=(4,2) and K_B=βP=5(6,2)=(4,2) are the computations involved with Alice and bob. Finally, they both will have a shared secret key such as (4,2) indicating successful key exchange. However, ECDH is found to be vulnerable to MITM attacks. Due to this SIDH is considered as candidate PQC scheme (as shown in "Supersingular-Isogeny Diffie-Hellman (SIDH)" section) and SIDH is combined with ECDH as the proposed PQC scheme (discussed in "Proposed Method" section).

As presented in Table 1, elliptic curve points are provided. Elliptic curves are widely used in cryptographic

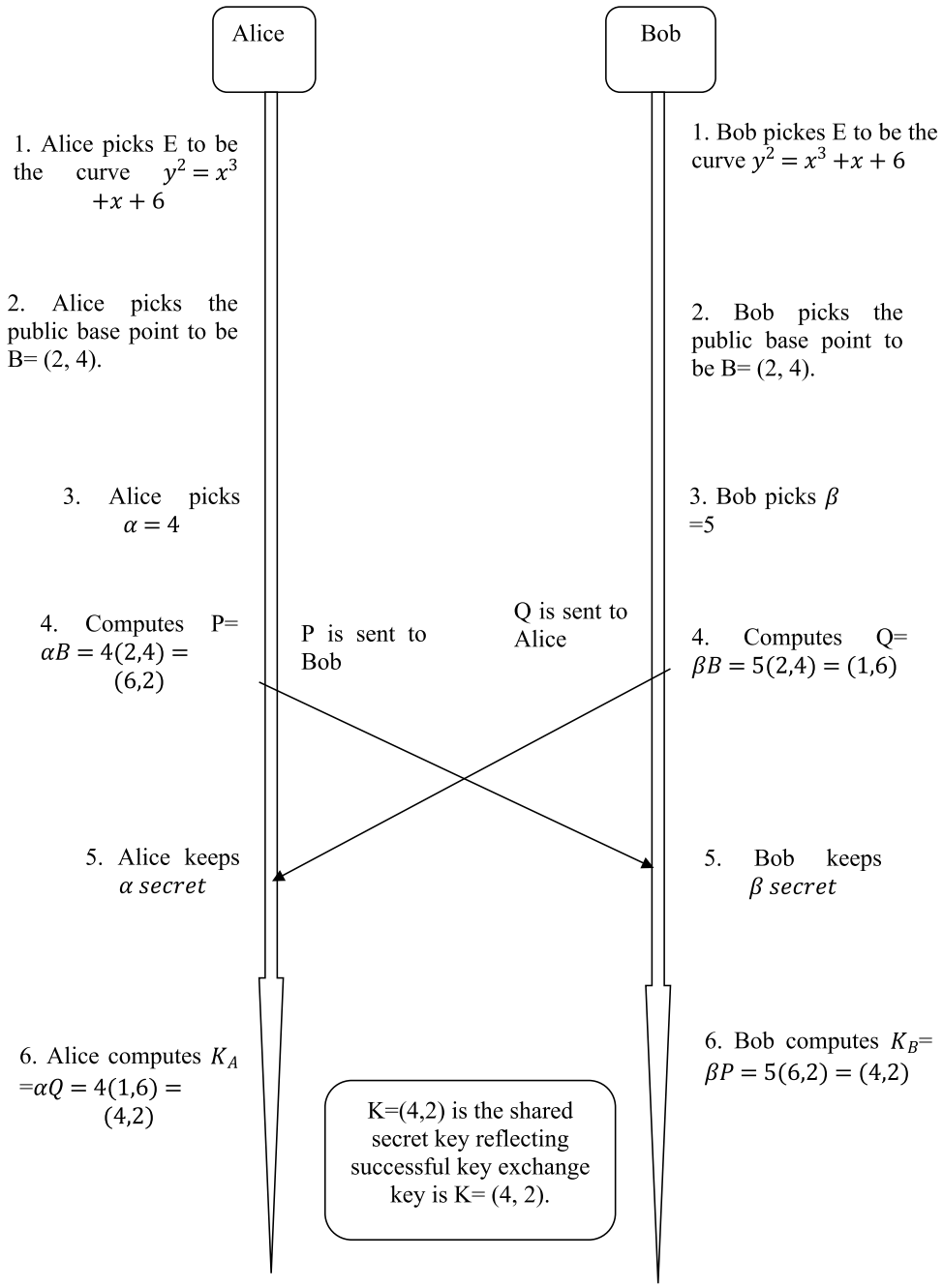


**Fig. 3** EC-DH scheme for key exchange

**Table 1** Shows elliptic curve points

| Finding all points over y^2 = x^3 + 1 ∈ F_{5^2}x + 1 ∈ F_{5^2} |
|---|
| The ideal generator is 1 + 1 t^1 + 1 t^2 |
| (0 ∈ F_{5^2}, 1 ∈ F_{5^2}) |
| (0 ∈ F_{5^2}, 4 ∈ F_{5^2}) |
| (0 + 3 t^1 ∈ F_{5^2}, 2 + 1 t^1 ∈ F_{5^2}) |
| (0 + 3 t^1 ∈ F_{5^2}, 3 + 4 t^1 ∈ F_{5^2}) |
| (0 + 4 t^1 ∈ F_{5^2}, 2 + 2 t^1 ∈ F_{5^2}) |
| (0 + 4 t^1 ∈ F_{5^2}, 3 + 3 t^1 ∈ F_{5^2}) |
| (1 ∈ F_{5^2}, 2 + 4 t^1 ∈ F_{5^2}) |
| (1 ∈ F_{5^2}, 3 + 1 t^1 ∈ F_{5^2}) |
| (1 + 1 t^1 ∈ F_{5^2}, 0 + 2 t^1 ∈ F_{5^2}) |
| (1 + 1 t^1 ∈ F_{5^2}, 0 + 3 t^1 ∈ F_{5^2}) |
| (1 + 3 t^1 ∈ F_{5^2}, 2 + 4 t^1 ∈ F_{5^2}) |
| (1 + 3 t^1 ∈ F_{5^2}, 3 + 1 t^1 ∈ F_{5^2}) |
| (2 ∈ F_{5^2}, 1 ∈ F_{5^2}) |
| (2 ∈ F_{5^2}, 4 ∈ F_{5^2}) |
| (2 + 2 t^1 ∈ F_{5^2}, 1 + 4 t^1 ∈ F_{5^2}) |
| (2 + 2 t^1 ∈ F_{5^2}, 4 + 1 t^1 ∈ F_{5^2}) |
| (2 + 3 t^1 ∈ F_{5^2}, 2 ∈ F_{5^2}) |
| (2 + 3 t^1 ∈ F_{5^2}, 3 ∈ F_{5^2}) |
| (3 ∈ F_{5^2}, 1 ∈ F_{5^2}) |
| (3 ∈ F_{5^2}, 4 ∈ F_{5^2}) |
| (3 + 2 t^1 ∈ F_{5^2}, 2 + 4 t^1 ∈ F_{5^2}) |
| (3 + 2 t^1 ∈ F_{5^2}, 3 + 1 t^1 ∈ F_{5^2}) |
| (4 ∈ F_{5^2}, 2 ∈ F_{5^2}) |
| (4 ∈ F_{5^2}, 3 ∈ F_{5^2}) |
| (4 + 2 t^1 ∈ F_{5^2}, 2 ∈ F_{5^2}) |
| (4 + 2 t^1 ∈ F_{5^2}, 3 ∈ F_{5^2}) |

primitives. In this paper, ECDH is combined with SIDH for stronger security to meet the requirements of PQC.

## IOT case study application

We integrated the proposed security scheme to an IoT application. The application is meant for sensing patients health data and perform big data analytics to know abnormal readings or inconsistencies. The integration of the security scheme is meant for ensuring end to end secure communications across the IoT use case. The application has a simulator to mimic IoT device which senses data and sends it to IoT platform. The communication process is achieved using MQTT protocol which is found to be lightweight and efficient. MQTT is widely used in distributed applications where lightweight messaging is desired. Two sensors are associated with the IoT device. They are known as Accelerometer and Gyroscope. These sensors help in keeping track of patient's movements. The application also makes use of a reliable protocol named TCP/IP. The historical data that is with IoT middleware is exported to cloud based database for big data analytics. The data analytics is meant for identifying

**Table 2** Procedure to connect Cloudant database

```
cloudantdata=sqlContext.read.format("com.cloudant.spark").\
option("cloudant.host", host).\
option("cloudant.username", username).\
option("cloudant.password", password).\
option("view","_design/IoTp/_view/by-date").\
option("jsonstore.rdd.partitions", 4).\
load(dbName)
```

anomalies in patient's readings. The identified anomalies are visualized to help in making good decisions.

The piece of code in Table 2 helps in establishing connection to Cloudant database. This database is meant for storing data generated by sensors through IoT device. The data comes from the device to IoT platform. The code has provision to limit number of requests per second due to the use of free software version. If the limit is not set, it results in an error once the threshold is exceeded.

## Post quantum cryptography

As studied in (Craig et al., 2016) there is post quantum threats to security algorithms that rely on certain mathematical complexity. Therefore, it is essential to have key sharing schemes that are quantum-resistant. Towards this end, a hybrid algorithm based on Supersingular-Isogeny Diffie-Hellman (SIDH) and ECDH. Before discussing the hybrid method, the following subsection gives information about SIDH.

### Supersingular-Isogeny Diffie-Hellman (SIDH)

Luca De Feo and David Jao (David & De Feo, 2011) proposed SIDH in 2011 and it is regarded as quantum resistant DH (Diffie-Hellman) scheme that is based on elliptic curves. Instead of a single elliptic curve group, SIDH uses a set of elliptic curves that are "isogenous" in nature. The key sizes of SIDH are smaller than its PQC (Post Quantum Cryptography) counterparts such as the ones explored in (Jeffrey et al., 1998; Bernstein, 2006; Mike, 2015). Isogeny is a map of elliptic curves, denoted as phi: E_1 -> E_2, that send source curve identity to that of the target. Therefore, for every isogeny, there is dual isogeny with two isogenous curves. When an isogeny graph is considered, the edges are known as isogenies while the vertices are elliptic curves. Alice and Bob, instead of choosing secret multiplication by n, choose secret isogenies from isogenous curves and thus security is enhanced based on computational difficulty.

The starting curve is E_0 and points are P_A, Q_A, P_B, Q_B. These are set as system parameters. A kernel determines an isogeny uniquely. Alice needs secret scalars m_A and n_A, denoting a secret point such as [m_A]P_A + [n_A]Q_A, in order to have a secret isogeny phi_A. It results in kernel subgroup <[m_A]P_A + [n_A]Q_A> in order to determine the secret isogeny. Afterwards, Alice, at the points P_B and Q_B, evaluates phi_A. Then Alice sends E_A, phi_A(P_B) and phi_A(Q_B) to Bob. And Bob sends Alice the same with A and B values swapped. Then Alice constructs isogeny phi'_A, using E_B, phi_B(P_A) and phi_B(Q_A), with kernel such as <[m_A] phi_B(P_A) + [n_A] phi_B(Q_A)>. In the same fashion, Bob constructs an isogeny named phi'_B, using E_A, phi_A(P_B) and phi_A(Q_B), with kernel such as <[m_B] phi_A(P_B) + [n_B] phi_A(Q_B)>. Then there is mapping to curves such as phi'_A to E_AB and phi'_B to E_BA and both curves are isomorphic. The shared secret between them is j(E_AB) = j(E_BA) as elliptic curves are associated with j-invariant. More details on isogeny based cryptography are found in (Patarin, 1996; Weiqiang et al., 2019).

## Proposed Method

PQC community has been striving to improve security schemes further. The existing PQC compatible schemes also do not enjoy consensus among PQC community. However, the discussions found in (Bos & Friedberger, 2019) on PQC, there was recommendation to combine existing PQC schemes classical ones for further security until very robust PQC emerges in the efforts. In this paper, ECDH and SIDH are combined to achieve a PQC compatible security scheme. With the empirical study, we observed that there is little extra overhead caused when ECDH and SIDH are combined on standard elliptic curves. SIDH has its associated isogenous curves for p = 23723239 – 1. Curve like Ea/Fp2 : y2 = x3 + ax2 + x along with its #Ea = 2i · 3j result in formation of a quantum-secure SIDH variant. Considering Fp and its base field, it was observed that Fp and a are associated while Ea/Fp along with quadratic twist are found to be stronger besides being twist-secure (Bernstein, 2016). Thus the curve is considered similar to the one explored in (Bernstein, 2006). With respect to computations associatedwith Montgomery's ladder, (a + 2)/4 is the constant which is part of the computation. With empirical study it is observed that it is possible to obtain smallest absolute value linked to the constant such that #Ea and #E'a reflect a prime 4 times larger. Given an integer denoted as p containing a value as 624450, the resultant curve is as sown below.

$$Ma/Fp : y2 = x3 + ax2 + x$$

With respect to Ma, Frobenius endomorphism's tMa trace is as given below.

tMa=0x743FC8888E1D8916BAB6DD6500AD5265DF E2E04882877C 26BA8CD28BE24D10D3E729B0BD07B-C79699230B6BC69FEAC,

$$\#Ma = p + 1 - tMa = 4ra$$

and the other form is #Maj = p + 1 + tMa = 4raj where primes of 749-bit are ra and raj. Both Ma and Maj along

with Fp are somehow related a point's x-coordinate. As mentioned earlier with respect to twist-secure compatibility, Fp elements are considered to be valid public keys. Therefore, they are used to enhanced security of ECDH without considering point validation process. [0, ra) is a set of integers that are used as secret keys in ECDH. Then searching for $\alpha \in N$ to be smallest such that $(\alpha + 1)ra - 1$ and $\alpha ra$ consisting of same bit length to be in tune with LADDER function of constant time. Prior to performing multiplications (scalar) with the help of LADDAR, it is important to parse secret keys into [3ra, 4ra). Thus, when SIDH and ECDH are combined, there are benefits with respect to leveraging security. There is valid reason behind this as SIDH is bestowed with provisions to compute x([m]P ) = LADDER(x(P ), m, a). At the same time, speed related overhead on the proposed scheme is found to be less. Moreover, the integration of two schemes results in relatively larger public keys leading to enhanced security strength.

## Results & Discussion

This section presents experimental results. The IoT use case is implemented using PySpark as it could handle big data. The system implementation is based on the illustration provided in Fig. 1. IoT platform used is known as Watson IoT and Cloudant NoSQL is used for storing data. Watson Studio used in the proposed system is meant for pulling data from IoT middleware prior to performing data analytics. Cloud platform used in the study is from IBM. The protocol preferred for messaging is known as MQTT.

IoT integrated application pertaining to healthcare domain is used to evaluate our proposed scheme. The IoT application has sensors to capture health related information from sensors. As the sensors keep producing data from time to time, it is stored in IoT middleware before it is used for data analytics. Application keeps track of patients' activities linked to health. Thus the data acquired through this application plays vital role in rendering useful insights that benefit patients. The data analytics also provide actionable information to healthcare professionals to enable them planning medical interventions personalized. Therefore, the results provided in this section are related to healthcare application functionality and also our security scheme.

Result of data analytics reflecting anomalies visualized, as shown in Fig. 4, helps healthcare professionals to ascertain abnormalities in patient's condition. In the given time sequence, observations are made to know z-score dynamics that help in anomaly detection. The results show lower and upper bounds to know the spikes and their distribution over given time domain. The spikes indicate certain abnormalities in the patient data. Therefore, the visualization of outcome of data analytics has potential to understand abnormalities in the data acquired through IoT application. The data points plotted in the graph lying either below or upper threshold are abnormal in nature. The observations are also linked to time domain in order to understand when and what abnormalities are identified.

There are three sensors involved in the IoT application. Figure 5 shows the observations pertaining to each sensor. The three sensors are called as oa, ob and og respectively. The density plot for each sensor demonstrates the numeric

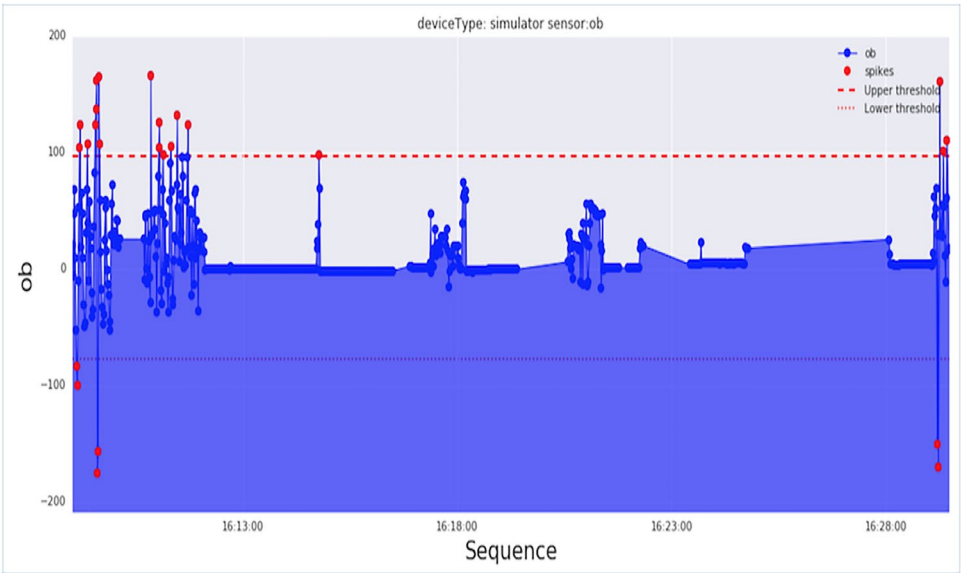


**Fig. 4** Result of data analytics reflecting anomalies visualized

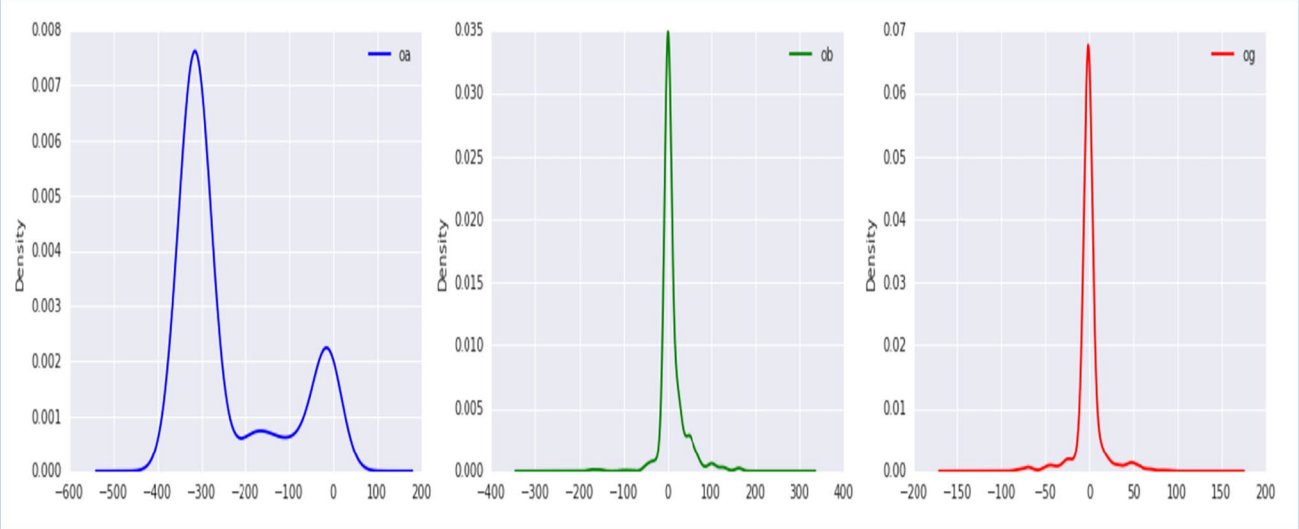


**Fig. 5** Shows density readings linked to the three sensors

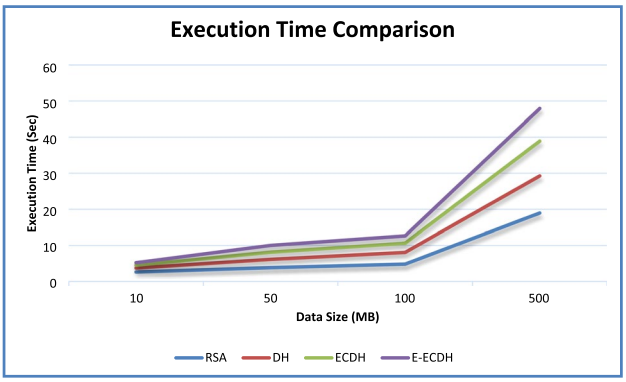


**Fig. 6** Execution time comparison among the security schemes against different workloads

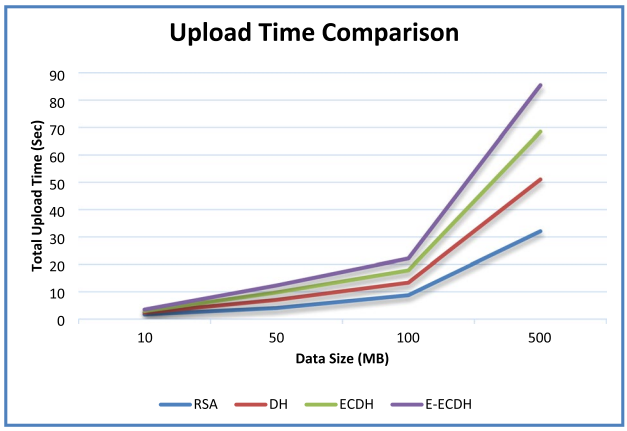


**Fig. 7** Upload time comparison of schemes against different workloads

variable (sensed reading) in terms of its smooth distribution over a time period. The peak of the curve associated with each graph reflects the numeric data with maximum concentration. It is observed that the smooth distribution of data points reflect concentration dynamics of numeric readings provided by respective sensors.

The experimental results, shown in Fig. 6, revealed that the time required for execution of each scheme against given workload varies. However, a common threat among all schemes is that the time required is increased as the workload increases. However, there is performance gain observed in case of the proposed scheme consistently among all workloads.

Total upload time is measured and presented in Fig. 7. Each scheme is evaluated with the measure under different workloads. Two important observations are made in the results presented. The first observation is that, the workload

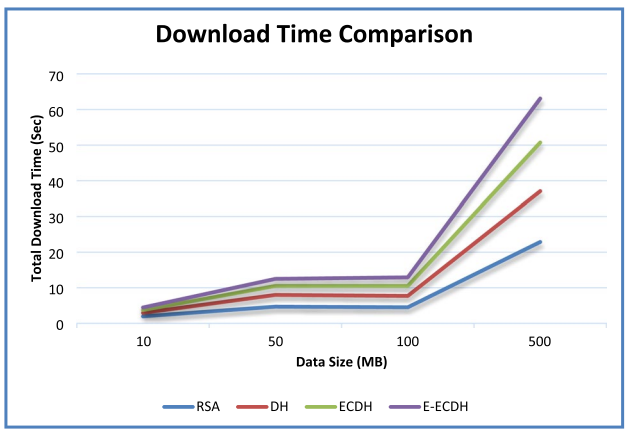


**Fig. 8** Download time comparison of schemes against different workloads

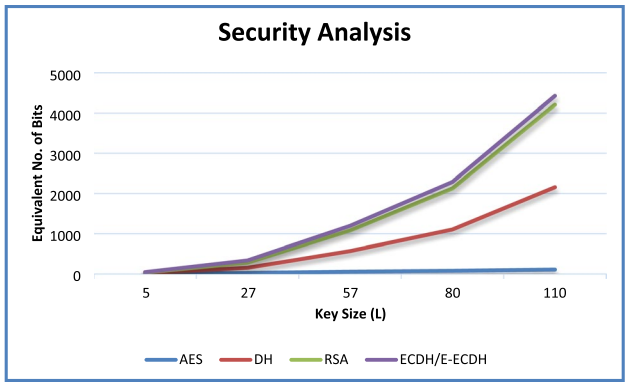


**Fig. 9** Security strength comparison of schemes

has its impact on the total upload time while the second one is that the proposed scheme is more light weight and required relatively less time when compared with the state of the art. When the workload is 500, there is significant difference found among the performance of the schemes. There is minimum of 5% and maximum of around 66% increase in performance shown by the proposed scheme.

Total download time is measured and presented in Fig. 8. Each scheme is evaluated with the measure under different workloads. Two important observations are made in the results presented. The first observation is that, the workload has its impact on the total download time while the second one is that the proposed scheme is more light weight and required relatively less time when compared with the state of the art. When the workload is 500, there is significant difference found among the performance of the schemes. There is minimum of 9% and maximum of around 50% increase in performance shown by the proposed system.

Security strength of schemes is provided in Fig. 9 in terms of key size versus equivalent number of bits. In the security analysis AES is the baseline considered whose security in terms of equivalent number of bits and the key length is same. This is the reason why AES is considered in this visualization unlike Figs. 7 and 8. With the observation considering equivalent number of bits, the proposed scheme shown better performance when compared with other schemes.

Table 3 shows comparison between the proposed scheme and existing SIDH scheme. The performance comparison results reveal that the proposed scheme security is enhanced to 384 bits from that of 192. It also reflects that the increased computation cost is less than 1.13x. At the same time, there is increase of public key size by less than 1.17x. Thus it is found that E-ECDH shows better performance over existing SIGH.

## Conclusion

In this paper we proposed a scheme for IoT use case for lightweight and secure communications among connected devices. Our scheme, named E-ECDH (ECDH+SIDH), enhances security of IoT application significantly as it enables secure end-to-end communications. We considered a healthcare application, as an IoT case study, for evaluation of E-ECDH. This scheme is designed to overcome the shortcomings of ECDH. E-ECDH is designed to safeguard communications in IoT integrated healthcare application. The healthcare IoT case study where big data analytics is involved is safeguarded with the help of the proposed scheme. The sensed data is stored in cloud platform. Our scheme is found lightweight and enable faster operations associated with E-ECDH. The enhanced ECDH with the help of SIDH combination has higher level of security. Since it is a hybrid for stronger security, it can be considered to be a PQC compatible scheme. However, it is still work in progress that needs further research. In our future work, we intend to apply our scheme to IoT use cases in other domains as well.

**Table 3** Performance comparison among PQC schemes

| Parameters | | SIDH Scheme | Proposed (SIDH+ECDH) |
|---|---|---|---|
| Equivalent bit security | Traditional schemes | 192 | 384 |
| | Quantum-Secure schemes | 128 | 128 |
| Public key size | | 564 | 658 |
| (cc $\times 10^6$) speed | Alice shared key | 44 | 50 |
| (cc $\times 10^6$) speed | Alice key generation | 46 | 52 |
| (cc $\times 10^6$) speed | Bob shared key | 50 | 57 |
| (cc $\times 10^6$) speed | Bob key generation | 52 | 58 |

**Acknowledgements** The authors would like to express their gratitude to the Ministry of Higher Education Malaysia for funding this research project through Fundamental Research Grant Scheme (FRGS) with Project Code: FRGS/1/2022/TK02/UCSI/02/1 and also to UCSI University, Malaysia.

**Author Contributions** N.Madhusudhan Reddy-Literature review, methodology
Budati Anil Kumar-Results development
Shayla Islam-Rough & Main draft preparation
Gajula Ramesh-Results validation

**Funding** Not Applicable

**Data availability** There is no third party of data is consider for this research work. Hence it doesn't required any permissions from third party.

## Declarations

**Ethical Approval** Not Applicable

**Competing interests** Personal Nature

## References

Ahamed J, Rajan AV (2016) Internet of Things (IoT): Application systems and security vulnerabilities. 2016 5th International Conference on Electronic Devices, Systems and Applications (ICEDSA), Ras Al Khaimah, United Arab Emirates, pp. 1-5

Alferidah DK, Jhanjhi NZ (2020) "A review on security and privacy issues and challenges in internet of things", IJCSNS International Journal of Computer Science and Network. Security 20(4)

Al-Garadi MA, Mohamed A, Al-Ali AK, Du X, Ali I, Guizani M (2020) A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security. In: IEEE Commun SurvTutor 22(3):1646–1685

AL-mawee W (2012) Privacy and Security Issues in IoT Healthcare Applications for the Disabled Users a Survey. Master's Theses. 651

Ammar M, Russello G, Crispo B (2018) Internet of Things: A survey on the security of IoT frameworks. J Inform Sec Appli 38:8–27

Ande R, Adebisi B, Hammoudeh M, Saleem J (2020) Internet of Things: Evolution and technologies from a security perspective. Sustain Cities Soc 54:101728

Azmoodeh A, Dehghantanha A, Raymond Choo KK (2019) Big data and internet of things security and forensics: Challenges and opportunities. Handbook Big Data IoT Sec:1–4

T. Baranwal, Nitika R, Pateriya PK (2016) Development of IoT based smart security and monitoring devices for agriculture. 2016 6th International Conference - Cloud System and Big Data Engineering (Confluence), Noida, India, pp. 597-602

Berkay Celik Z (2018) Program analysis of commodity iot applications for security and privacy: Challenges and opportunities. ACM Comput Surv 52(4):1–30

Bernstein DJ (2006) "Curve25519: New Di_e-Hellman speed records", In M. Yung, Y. Dodis, A. Kiayias, and T. Malkin, editors, Public Key Cryptography - PKC 2006, 9th International Conference on Theory and Practice of Public-Key Cryptography, New York, NY, USA, April 24-26, 2006, Proceedings, volume 3958 of Lecture Notes in Computer Science, pages 207-228. Springer

D. J. Bernstein The post-quantum internet. Invited talk at PQCrypto 2016: https://cr.yp.to/talks/2016.02.24/slides-djb-20160224-a4.pdf, Feb, 2016

Bos JW, Friedberger SJ (2019) Arithmetic considerations for isogeny-based cryptography. IEEE Trans Comput 68(7):979–990

Craig C, Longa P, Naehrig M (2016) Efficient algorithms for supersingular isogeny Diffie-Hellman. In" Advances in Cryptology–CRYPTO 2016: 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part I 36, pp. 572-601

S. K. Datta and C. Bonnet (2016) Easing IoT application development through DataTweet framework. 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), Reston, VA, USA, pp. 430-435

Datta SK, Gyrard A, Bonnet C, Boudaoud K (2015) oneM2M architecture based user centric IoT application development. 3rd International Conference on Future Internet of Things and Cloud, pp.1-8

David J, De Feo L (2011) Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In: Post-Quantum Cryptography: 4th International Workshop, PQCrypto 2011, Taipei, Taiwan, November 29–December 2, Proceedings 2011, 4, pp. 19-34

Diffie W, Hellman M (1976) New directions in cryptography. IEEE Trans Inf Theory 22(6):644–654

Ejaz W, Anpalagan A (2019) Internet of things for smart cities: technologies, big data and security. Springer International Publishing, Berlin/Heidelberg, Germany

Giuseppe A, Persico V, Pescapé A (2020) Industry 4.0 and health: Internet of things, big data, and cloud computing for healthcare 4.0. J Ind Inf Integr 18:100129

Hasan MK, Ahmed MM, Musa SS, Islam S, Abdullah SNHS, Hossain E, Nafi NS, Vo N. (2021b). An Improved Dynamic Thermal Current Rating Model for PMU-Based Wide Area Measurement Framework for Reliability Analysis Utilizing Sensor Cloud System . IEEE Access, pp.1–13. https://doi.org/10.1109/access.2021.3052368

Hasan MK, Ghazal TM, Alkhalifah A, Ab KA. (2021a). Fischer Linear Discrimination and Quadratic Discrimination Analysis–Based Data Mining Technique for Internet of Things. Front Public Health 9, pp.1-18.

Imran M, Ahmed SR, Kamrul HM, Rosilah H, Ul HA, Akram ZK, Sajjad S (2020) Protect Mobile Travelers Information in Sensitive Region Based on Fuzzy Logic in IoT Technology. Security and Communication. Networks:1–12. https://doi.org/10.1155/2020/8897098

Jeffrey H, Pipher J, Silverman JH (1998) NTRU: A ring-based public key cryptosystem. In: International algorithmic number theory symposium, pp. 267-288. Berlin, Heidelberg: Springer Berlin Heidelberg

F. Jonsson and M. Tornkvist (2017) RSA authentication in internet of things. Degree Project In Technology, First Cycle, 15 Credits Stockholm, Sweden

Kang Y-M, Han M-R, Han K-S, Kim J-B (2015) A study on the internet of things (IoT) applications. Int J Software Eng Appli 9(9):117–126

Li C (2020) Information processing in Internet of Things using big data analytics. Comput Commun 160:718–729

Liu Z, Yan T (2013) Study on multi-view video based on IOT and its application in intelligent security system," Proceedings 2013 International Conference on Mechatronic Sciences, Electric Engineering and Computer (MEC), Shenyang, China, pp. 1437-1440

López D, Daniel MBU, Cely CS, Murgueitio DT et al (2018) Developing secure IoT services: A security-oriented review of IoT platforms. Symmetry 10(12):669

McEliece RJ (1978) A public-key cryptosystem based on algebraic coding theory. Coding Thv 4244:114–116

Merkle RC (1979) Secrecy, authentication, and public key systems. PhD thesis, Stanford University

Mike H (2015) Ed448-Goldilocks, a new elliptic curve." Cryptology ePrint Archive

Milne JS (1986) Arithmetic Geometry, chapter Abelian Varieties, pp.103-150. Springer New York, New York, NY

Montgomery PL (1987) Speeding the Pollard and elliptic curve methods of factorization. Math Comput 48(177):243–264

Nguyen Duc A, Ronald J, Pangkaj P, Abrahamsson P (2017) Security challenges in IoT development: a software engineering perspective. pp.1-5

Nguyen XT, Tran HT, Baraki H, Geihs K (2015) FRASAD: A framework for model-driven IoT Application Development. In: 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT), Milan, Italy, pp 387–392

Patarin J (1996) Hidden _elds equations (HFE) and isomorphisms of polynomials (IP): two new families of asymmetric algorithms. In: U. M. Maurer, editor, EUROCRYPT '96, volume 1070 of LNCS, pp. 33-48

Pustišek M, Kos A (2018) "Approaches to front-end IoT application development for the ethereum blockchain", Science Direct. Procedia Comput Sci 129:410–419

Riahi A, Challal Y, Natalizio E, Chtourou Z, Bouabdallah A (2013) A aystemic approach for IoT security. DCOSS, Boston, United States. pp.351-355

Savola RM, Savolainen P, Evesti A, Abie H, Sihvonen M (2015) Risk-driven security metrics development for an e-health IoT application. 2015 Information Security for South Africa (ISSA), Johannesburg, South Africa, pp. 1-6

Shami TM, Grace D, Burr A (2018) Load balancing and control using particle swarm optimisation in 5G heterogeneous networks. IEEE:1–6

Shayla I, Khalifa OO, Abdalla HAH, Kamrul HM, Razzaque MA, Biswajeet P. (2020). Design and Evaluation of a Multihoming-Based Mobility Management Scheme to Support Inter Technology Handoff in PNEMO. Wireless Personal Communications, pp.1-21. https://doi.org/10.1007/s11277-020-07412-0

Sreeja R, Paul V, Menon VG, Khosravi MR (2019) A secure and efficient lightweight symmetric encryption scheme for transfer of text files between embedded iot devices. Symmetry 11(2):293

Suma DV (2019) Towards sustainable industrialization using big data and internet of things. J IoT in Social, Mobile, Analytics, Cloud 1(1):24–37

Sutjiatmo BP, Erwinsyah A, Lydia EL, Shankar K et al (2019) Empowering internet of things (IoT) through big data. Int J Eng Adv Technol 8, no. 6S2:938–942

Tellez M, El-Tawab S, Heydari MH (2016) IoT security attacks using reverse engineering methods on WSN applications. 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), Reston, VA, USA, pp. 182-187

Tweneboah-Koduah S, Skouby KE, Tadayoni R (2017) Cyber security threats to IoT applications and service domains. Wirel Pers Commun 95:169–185

Ukil A, Bandyopadhyay S, Bhattacharyya A, Pal A, Bose T (2014) Lightweight security scheme for IoT applications using CoAP. Int J Pervasive Comput Commun 10(4):372–392

Weiqiang L, Jian N, Zhe L, Chunyang L, O'Neill M (2019) Optimized modular multiplication for supersingular isogeny diffie-hellman. IEEE Trans Comput:1–1

Yashwant D, Joshi V (2018) "Some issues on architecture for secure services for IoT", Department of Electronics and Telecommunication. Engineering:1–13