Complex & Intelligent Systems (2022) 8:3817–3832
https://doi.org/10.1007/s40747-021-00576-7

ORIGINAL ARTICLE

Secure transmission technique for data in IoT edge computing infrastructure

Rohit Sharma[1] · **Rajeev Arya**[1]

Received: 8 June 2021 / Accepted: 21 October 2021 / Published online: 23 November 2021

Abstract

Nowadays, the utilization of IoT technology has been rapidly increased in various applications such as smart city, smart banking, smart transport, etc. The internet of things allows the user to collect the data easily using the different sensors installed at various locations in the open environment. The data collection process by the IoT sensors is giving access to the various services. However, due to the open communication medium, it is difficult to provide secure access to these services. In this paper, a data transmission technique has been proposed, which will provide secure communication in IoT infrastructure for smart city applications. In this method, each IoT sensor have to prove their legitimacy to the reader and the base station before the transmission of data. Hence, the IoT sensors can transmit the required data in a secure and efficient way. In the proposed technique, the proof of correction shows that the required information is not supposed to send through an online medium, it is obtained at the receiver using the Euclidean parameters shared by the IoT sensors. The proposed technique is compatible to provide the security against most of the attacks performed by the attackers. Two random variables and complex mathematical calculation are making the proposed technique more reliable than others. This technique will significantly improve the security of different data transmission services which will be helpful to improve the smart city infrastructure.

Keywords Internet of things · Edge computing · Secure data transmission · Security and privacy · Authentication · Smart city

Introduction

The expansion of IoT services has developed a competitive environment by the introduction of new and innovative products launch for smart city applications. The frequently developed system imposed a new challenge towards system privacy and security [1]. Consequently, some of the products do not satisfy the privacy and security of the system which is the major concern of IoT as well as smart cities [2]. Most of the research work has been focusing on the possible applications and issues related to smart cities [3]. Earlier privacy and security are not taken as an important parameter until the ransomware threats have been developed like crypto wall [4], wannacry [5], crypto locker [6], etc. Due to these attacks, there is a sense of mistrust indulges for the IoT system. The system is criticized and said that it becomes the Internet of Vulnerabilities instead of the Internet of things [7]. There has been a wide wave of developing new applications for privacy and security within the IoT-based smart city implementation. There have been a variety of advertisements for secure products for smart cities [1]. In the proposed technique, three phases have been considered namely the Registration phase, Authentication phase, and Data transfer phase (Fig. 1). In the first phase, the IoT sensor has to perform the registration process by sending its Identity number along with the time stamp $[(S_{\text{iden}})\|T_1]$. In the authentication phase, sensor has to share $[\lambda_i = \in (R_g\|T_3)]$ and $[E_{\text{cp}}]$ to the receiver and in data transfer mode, the IoT sensor calculates the Euclidean parameter (x, y, z) and will send these parameters to the receiver. The operations of these three steps are elaborated in brief in the upcoming sections.

The important part of this research implies that it can give a deep understanding of cyberattacks so that the new policies can be made accordingly. The study posed an important question of the overall security of the system [8]. There have been various challenges in the non-technical implementa-

✉ Rohit Sharma
rohits.ph21.ec@nitp.ac.in

Rajeev Arya
rajeev.arya@nitp.ac.in

[1] Wireless Sensor Networks Lab, Department of Electronics and Communication Engineering, National Institute of Technology Patna, Patna, Bihar 800005, India

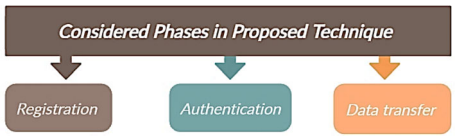

Fig. 1 Considered phases in proposed technique

tion of the system also, this is a major concern nowadays [9]. The reasons given by the study of "unsuccessful information technology projects" [10], for the failure of non-technical implementation are lack of support of top management, the business case is weak and project planning is poor. These kinds of problems are mostly possessed in the public sector. Several implications can be seen in the administrative history of the technological project in terms of technology adoption by government agencies [11]. Security is a tedious task in IoT, some of the concerns have arisen from the wireless sensor networks (WSNs) [12, 13]. The practical limitation in implementing IoT-based services in the security mechanism of smart cities is related to the IoT characteristics [14]. Smart cities show a dynamic behavior as they have a continuously changing environment due to the trade-off between CPS devices and citizens. The other complications arise due to the diverse architectures present in the smart city. Smart cities are also facing several economic problems in recent years. The challenges related to financing include declination of budget [15], descending order of state aid [16], and enhance budget uncertainty [17, 18]. In this paper, a secure data transmission technique has been introduced for IoT infrastructure. In this method, each IoT sensor (IOi) have to prove their legitimacy to the reader (Ri) and the base station (BSi) before the transmission of data. This technique will significantly improve the security of different data transmission services which will be helpful to improve the smart city infrastructure. The proposed technique resists many attacks such as Authentication attacks, User anonymity, forging attacks, and many more performed by the adversary.

The contribution of the paper is as follows:

1. A secure data transmission technique has been proposed, which includes three phases namely Registration, Authentication, and Data transfer.
2. Each IoT sensor (IOi) have to prove their legitimacy to the reader (Ri) and the base station (BSi) before the transmission of data.
3. The sensor node needs to send three Euclidean parameters to the receiver instead of recorded information.
4. The proposed technique resists many attacks such as Authentication attacks, User anonymity, forging attacks and many more attacks, which could be performed by the adversary.

In the first section, background related to smart cities and IoT security has been presented. The second section has the related literature and risks available in developing a smart city operation is described in the next section. The proposed secure data transmission technique has been discussed in the following section, also the analysis of the security has been investigated in the next section. The paper has been concluded in the next section with open issues.

Related works

It is necessary to authenticate as not to allow illegal participants into the network. There are so many conventional methods that are based on cryptography. The conventional method needs more time to process. One of the most common cryptography systems is RSA which requires a lot of time for its calculations. As there are so many limitations associated with conventional methods so, the researchers have proposed ECC (elliptic curve cryptosystem) for securing the network by doing the authentication [19]. The ECC is based on the Discrete Logarithm Problem (DLP) [20]. The proposed method is cost-effective but not secure as per individual users. The mobile users require a public key to access, it for authentication. There are several bilinear techniques propose to enhance the security level [21, 22] based on the Id system, these systems do not require to save every one another public key, so that memory space can also have minimized and credentials of every individual are safe. The different variant of ID-based systems is the grid security system for verification of atmospheric conditions based on clouds [23–25]. The other methods are given based on the client–server technique which authenticates by bilinear pairing [26–31]. As compared to the ECC technique cloud computing technique is more compatible. In the ECC technique, the managing key has to be in a secret form otherwise if the attacker got the major managing key of the service provider then the privacy of data will be gone. To resolve this issue cloud-based technique is used in which users can access resources on, on-demand basis. Also, to improve the security in cloud-based techniques, the position and history of the user should be known prior so that the privacy of the user is secured. The privacy of the users is secured by the verification method of information for 'n' times, the value of 'n' changes based on intended time provided by the cloud network [32–35]. The authors propose the Merkle tree method which has four types of network initialization, cloud captivity, verification, and secure computing [31, 36]. Recently, security policies and agreements are available for authentication like set up of the system, registration of the user, and authentication. These agreements provide security to all mobile users as they have a secret key that is only known to the individual user. The major weakness of this system is that an insider can take the master

Fig. 2 Risks available in developing a smart city operation

key of the network and can play with every user's credentials. The authors identify that there is no security between user and system [37, 38], the insider can identify the public key. In [39], the author proposes a collaborative task including security and energy-aware for D2D communication. This study measured the security workload by building a security model. The author has designed an authentication protocol using AI for real-time access to industrial medical. This authentication protocol can be overcome the various known attacks [40].

In the proposed method, each IoT sensor (IO*i*) have to prove their legitimacy to the reader (R*i*) and the base station (BS*i*) before the transmission of data. This technique will significantly improve the security of different data transmission services which will be helpful to improve the smart city infrastructure. The proposed technique resists many attacks such as Authentication attacks, User anonymity, forging attacks, and many more performed by the adversary.

Inferences for safety and security for censorious infrastructure in smart cities

There are several risks while developing an efficient and reliable smart city operation. This section represents various risk factors related to smart cities (Fig. 2).

Risk of infrastructure in smart city

The lifeline of any city is the infrastructure of the system [41]. There are various risk factors associated with the concept of the infrastructure of the city. There are two types of concepts regarding the cybersecurity of smart cities. The first one shows a huge enhancement in computing capability that rapidly increases the attack on the network which should be defended at a level. All the smart devices such as televisions, refrigerators, cameras, routers can become a source of malicious activity as it uses different software's. Urban areas show more effectiveness as compare to rural ones [42]. The second concept shows the presence of actuators in the system that affects the infrastructure of the smart city (such as filters, heating elements, switches, and valves). These actuators control things but at the same, there is a risk of physical damage as well. Therefore, when both the things are combined sensors and actuators the theft of security increases more [43].

Operational security and information security

Recently, major threat is ransomware and malware that encrypts files. These kinds of ransomware ask for ransom from the owner to unlock the files. These individual threats brought pathetic situations for user's computers and organizational cyber cells [44]. There is a huge loss of data with crypto locker, wannacry, and Reventon-type ransomware [45]. Ransomware affects personal files, work files everything in personal and professional computers [46]. Some of the enterprises depend upon data operation where this ransomware damages the whole system and made it the worst case [47]. There is the various reported case also which are pending trials or pending appeals [48]. In the healthcare sector, there are series of cases, like the case of a presbyterian hospital in California affected by ransomware. The data of the hospital are crippled by ransomware [49]. The effects of wannacry ransomware have been seen in early 2017 at the sites of the British Health Service (NHS) [50–52]. The data operations performed at payment machine, the computer to tackle traffic data, public transportation system also affected by some ransomware sometimes [53]. The ransom asked for these attacks is in several dollars and bitcoins [54]. A case of a transport system shows an extreme example of a ransomware attack which frees the travel cost and lost revenue [55]. The other way to cope up with the situation is to clean up all files from the system.

Safety and functional impacts vs. monetary impacts

The cyber-attack has serious consequences concerning financial access and confidential data. These are basic conceptual changes including physical impacts are present in smart cities, IoT, and other operational embedded networks [56]. There are structures like water waste control systems, transportation networks, and grid systems that are also computer-controlled networks [64–66]. The real-time analysis and changes towards urban structures like parking systems to traffic lights, the connection between different portals and networks will make the smart city implementation more complex and insecure. The most important part for policymakers is to understand that 'smart' can be taken in many ways [67]. As the smart city contains different types of sensors and computers are embedded in the system that is prone to deceive, deviation, malicious nodes, and outside attack [68–71].

Proposed secure data transmission technique

In the proposed technique, it is considered that the receivers are directly connected with the base stations. The notations used for the proposed techniques are elaborated in Table 1. In this study, three major nodes have been taken into consideration for the proposed technique, which are IoT sensor (IOi), Receiver (Ri), and Base station (BSi). The IoT sensors are denoted by (IOi) = {IO–IoT, $i = 1,..., n$}, receivers are denoted by (Ri) = {R Receiver, $i = 1,..., n$}, and Base station are denoted by (BSi) = {BS–Base station, $i = 1,..., n$}. At sensor end, data are classified in two categories namely Primary data [$P_{rd} = S_r||C_d||f_{rg}||I_{nf}$] and secondary data [$S_{cd} = N_{inf}||L_{att}||L_{ong}$]. Here, the meaning of the primary data is the data that are linked to the secret information of the node, such as the node serial number, node capacity, frequency range, and real-time recorded information. The recorded information is the information that is being recorded by the IoT sensor for real-time event monitoring. On the other side, the meaning of the secondary data is the data that is not linked to secret information and which can be used publicly such as the longitude and latitude of the node. For this technique, only secondary data are utilizing as the part of transmission between sensor and receiver.

A brief structure of the proposed technique is shown in Fig. 3. The architecture is showing the three major steps of the proposed technique, which are registration, authentication, and data transfer. In the first phase, the IoT sensor has to perform the registration process by sending its Identity number along with the time stamp [$(S_{iden})||T_1$]. In response to this, the receiver will revert a private prime key P_{ri} to the IoT sensor, which is useful in the upcoming steps at the sensor end. In parallel with P_{ri}, the receiver provides P_{rb} to the base station, where P_{ri} and P_{ri} contain the same prime values. In the authentication phase, the sensor has to share [$\lambda_i = \in (R_g||T_3)$] and [$E_{cp}$] to the receiver, and then, the receiver proceeds the λ_r along with a different timestamp to the base station for the calculation of $\phi'\left[\frac{P_r(x)}{S_{cd}(x)}\right]$. Base station has to reverts E'_{cp} to the receiver, which need to be matched with the E_{cp} received from the IoT sensor. If the condition satisfies, then authentication will be completed. In data transfer mode, the IoT sensor calculates the Euclidean parameter (x, y, z) and will send these parameters to the receiver. The receiver will forward these parameters to the base station for further processing. The values of α' will be calculated at the base station using the received Euclidean parameters and β'. The operations of these steps are elaborated in brief in the upcoming sections.

Here, it is avoiding to transmit primary data as it contains secret information. It is also considered that various IoT sensors are connected with a receiver and these sensors can send the data to the sensor on its request. For this technique, it is also considered that the base station stored all the needed information about the sensors such as S_{cd}, S_r, C_d, and f_{rg}. Following are the important expression to continue the technique:

Equation (1) represents the IoT sensor public key, which is the combination of prime value, random value and time stamp.

$$P_{ri} = (P_r + r_m)_2^t \tag{1}$$

$[R_{eq} = N_{inf}]$ (node information)
$[S_{cd} = N_{inf}||L_{att}||L_{ong}]$ (secondary data)

Table 1 Notations used for the proposed techniques

Symbols	Description
S_{iden}	Identity of IOT sensor
T_1	Time slot one
P_{ri}	IOT sensor public key
T_2	Time slot two
P_r	Prime number
r_m	Random number
P_{rb}	Base station public key
λ_i	Function of R_q & T_3
ε	A function parameter
R_q	Request from IOT sensor
T_3	Time slot three
λ_r	Function of R_q, T_3 & T_4
T_4	Time slot four
ϕ	Quotient function
$P_r(n)$	Polynomial function of prime number
$S_{cd}(n)$	Polynomial function of secondary information
N_{inf}	Node information
P_{rd}	Primary data
S_{cd}	Secondary data
C_d	Node capacity
f_{rg}	Frequency range
I_{nf}	Recorded information of IOT sensor
S_r	Node serial number
L_{att}	Node latitude
L_{ong}	Node longitude
P_{ack}	Positive acknowledgement
ψ	Polynomial function
H	Hash function
α	Function of information
β	Function of quotient
z	Euclidean parameter
G_c	GCD function
x	Euclidean parameter
y	Euclidean parameter

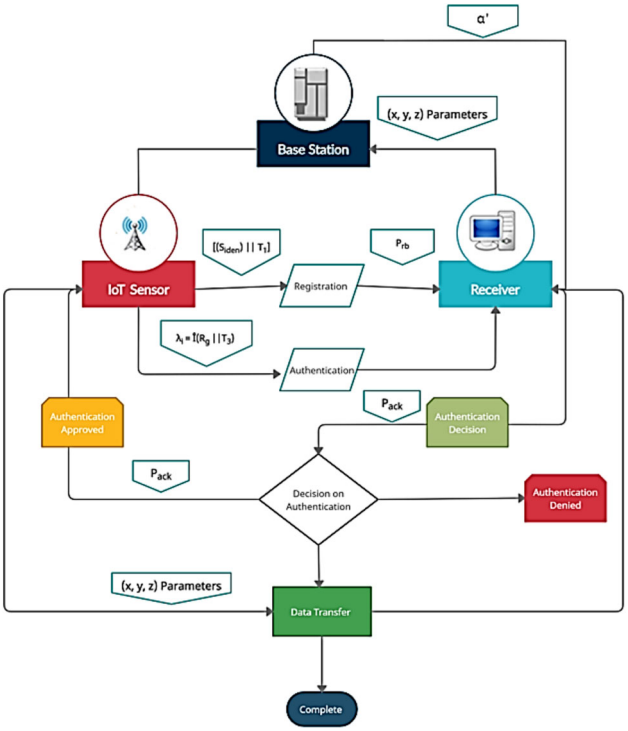

Fig. 3 Structure of the proposed technique

$$[P_{\mathrm{rd}} = S_{\mathrm{r}} \| C_{\mathrm{d}} \| f_{\mathrm{rg}} \| I_{\mathrm{nf}}] \text{ (primary data)}$$

$$\phi\left[\frac{P_{\mathrm{r}}(x)}{S_{\mathrm{cd}}(x)}\right] = \frac{\psi_{P_{\mathrm{r}}(x)}}{\psi_{S_{\mathrm{cd}}(x)}} \tag{2}$$

$$E_{\mathrm{cp}} = H\left[\phi\left(\frac{P_{\mathrm{r}}(x)}{S_{\mathrm{cd}}(x)}\right)\right]. \tag{3}$$

$[H = \mathrm{e}\,[P_{\mathrm{r}} \| r_{\mathrm{m}}]]$ (hash function)

Euclidean algorithm:

$$\alpha x + \beta y = z. \tag{4}$$

Equation (2) represents the value of quotient of the division between two functions namely $P_{\mathrm{r}}(x)$ and $S_{\mathrm{cd}}(x)$. Equations (3) and (4) represent the values of encryption function and the Euclidean algorithm. α and β are the functions of recorded information and secondary information. X, Y, and Z are known as Euclidean parameters. The timestamp is included in all the messages processed by sensors or receivers. In the time stamp process, the transmitting message has to be framed along with the exact transmitting timing of the message. Timestamp will also be verified at both the end for avoiding the replay attack.

Registration phase

In the proposed technique, three phases have been considered namely the Registration phase, Authentication phase, and Data transfer phase. The registration phase can be shown in Fig. 4. In the first phase, the IoT sensor have to perform the registration process by sending its Identity number along with the time stamp $[(S_{\mathrm{iden}}) \| T_1]$.

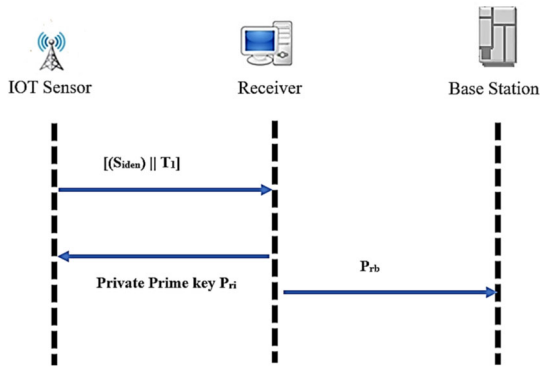

Fig. 4 Registration phase

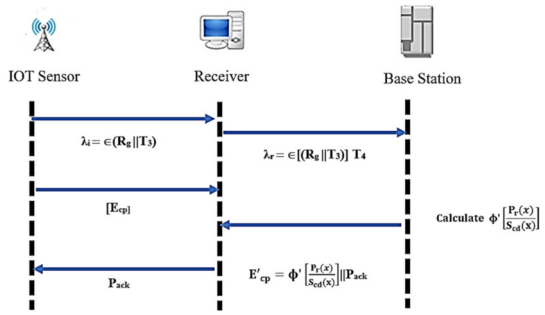

Fig. 5 Authentication phase

In response of this, receiver will revert a private prime key P_{ri} to the IoT sensor, which is useful in the upcoming steps at the sensor end. In parallel of P_{ri}, receiver provides P_{rb} to the base station, where P_{ri} and P_{ri} contains the same prime values.

Authentication phase

The authentication phase can be shown in Fig. 5. In the authentication phase, the IoT sensor has to prove its authenticity to the receiver. For this process, the sensor has to share $[\lambda_i = \in(R_{\mathrm{g}} \| T_3)]$ and $[E_{\mathrm{cp}}]$ to the receiver, which is nothing but the authentication request along with a timestamp and encrypted data. Then, the receiver proceeds the λ_{r} along with a different timestamp to the base station for the calculation of $\phi'\left[\frac{P_{\mathrm{r}}(x)}{S_{\mathrm{cd}}(x)}\right]$. In response of this, base station reverts E'_{cp} to the receiver, which need to be matched with the E_{cp} received from the IoT sensor. If condition satisfies, then authentication will be successfully completed.

The new sensor registration and authentication process are discussed in Algorithm 1, the algorithm for receiver and base station are also elaborated below.

Algorithm-1: *Registration and Authentication for IOT Sensor:*

Step 1:**Start**

Step 2: ***Registration →Read*** $[S_{iden}, T_1, P_r, r_m, t_2, Pr_i]$

Where S_{iden} *→server identity,*

T_1*→ time stamp,*

r_m *→random number,*

P_r *→Prime number,*

for $P_{ri} \rightarrow (P_r + r_m)\ t_2$

Step 3: ***Authentication→ Read*** $[\lambda_i, E_{cp}, T_3, R_s, \phi\left[\frac{P_r(x)}{S_{cd}(x)}\right]]$

for $\lambda_i \rightarrow \varepsilon[R_s, T_3]$

Send $\rightarrow E_{cp} \rightarrow \mathrm{H}\left[\phi\left(\frac{P_r(x)}{S_{cd}(x)}\right)\right]$ (*Apply polynomial division operation*)

{Let $P_r(x)$ *and* $S_{cd}(x)$ *are the two polynomials of degree n and m, then there will be two more polynomials namely quotient* $\phi\left(\frac{P_r(x)}{S_{cd}(x)}\right)$ *and remainder}*

{

If, T_i *= within limit*

then *accept the communication message*

Else

Dropped the communication message.

}

$P_r(x)$ *→ Polynomial Function of Prime*

$S_{cd}(x)$ *→ Polynomial Function of Secondary Data*

H *→ One Round Hash Function*

Step 4: ***Receive*** **[**P_{ack}**]**

P_{ack} *→ Positive Acknowledgment must be reached to the sensor for the completion of authentication.*

Step 5: ***End***

Algorithm-2: *Registration and Authentication for Receiver:*

Step 1: ***Start***

Step 2: ***Registration →Read*** *[S_{iden}, T_1]*

Step 3: ***for*** *[S_{iden}, T_1]*

S_{iden} → Server Identity

T_1 = Time One Slot

Step 4: ***Authentication→ Read*** ***[***P_{ri}, P_r, r_m, t_2, Pr_b, λ_i, λ_r, R_q, T_3, T_4, $E_{cp'}$***]***

$\lambda_i \rightarrow \varepsilon\ [R_q, T_3]$:

R_q – *Request from sensor to base station*

$\lambda_r \rightarrow \varepsilon\ [R_q, T_3]\ T_4$

Receive $\rightarrow E_{cp} \rightarrow \left[\phi\left(\frac{P_r(x)}{S_{cd}(x)}\right)\right]$(Apply polynomial division operation)

$T_3 \rightarrow T_4$ →*Time Function*

P_{ack} → *Positive Acknowledgment*

{

If, T_i = *within limit*

then

accept the communication message

else

dropped the communication message

}

Step 5: ***Send*** *[$E_{cp'}$, $P_{ack'}$]*

for $E_{cp'}$ → *Base Station Reaction*

$P_{ack'}$ → *Base Station acknowledgement to sensor*

Step 6: ***Compare*** *[E_{cp}, $E_{cp'}$]*

{

if, $E_{cp} = E_{cp'}$

then *authentication completed and can give the access to IoT sensor for entering into data transfer mode.*

else

authentication → denied (both values must be matched with each other)

}

Step 7: **End**

Algorithm-3: *Registration and Authentication for Base station:*

Step 1:**Start**

Step 2: ***Registration →Read*** **[**P_{rb}**]**

for Pr_b *(Public key for base station forwarded by receiver)*

$P_{rb} \rightarrow (P_r + r_m)\ T_2$

$r_m \rightarrow$*random number*

$P_r \rightarrow$*Prime number*

$T_2 \rightarrow$ *time stamp,*

Check time stemp

{

If, $T_i =$ *within limit*

then *accept the communication message*

Else

Dropped the communication message

}

Step 3: ***Authentication→ Read*** $[\lambda_r, E'_{cp}]$

for $\lambda_r \rightarrow \varepsilon\ [R_q, T_3]\ T_4$*:*

$\varepsilon \rightarrow$*function for two assigned parameters*

$R_q \rightarrow$*Request from sensor to base station*

Send $\rightarrow E'_{cp} \rightarrow \left[\phi'\left(\frac{P_r(x)}{S_{cd}(x)}\right)\right]$ (Apply polynomial division operation *at base station email*)

{Let $P_r(x)$ *and* $S_{cd}(x)$ *are the two polynomials of degree n and m, then there will be two more polynomials namely quotient* $\phi\left(\frac{P_r(x)}{S_{cd}(x)}\right)$ *and remainder}*

$P_r(x) \rightarrow$ *Polynomial Function of Prime*

$S_{cd}(x) \rightarrow$ *Polynomial Function of Secondary Data*

Step 4: **End**

Proof of the authentication procedure In this section, the proof of the authentication procedure is discussed. For the completion of authentication, the following condition should be verified-

E_{CP} should be equal to the E'_{cp},

where E_{CP} is encrypted function of Quotient, which is obtained after the division operation between two functions namely $P_{\mathrm{r}}(x)$ and $S_{\mathrm{cd}}(x)$ at IoT sensor. E'_{cp} is the encrypted function of Quotient, which is obtained after the division operation between two functions namely $P_{\mathrm{r}}(x)$ and $S_{\mathrm{cd}}(x)$, and which is considered to be stored at the base station,

$$E_{\mathrm{CP}} = E'_{\mathrm{cp}}$$

$$\left[E_{\mathrm{CP}} = \left[\phi'\left[\frac{P_{\mathrm{r}}(x)}{S_{\mathrm{cd}}(x)}\right]\right]\right]$$

$$\left[H\left[\phi\left[\frac{P_{\mathrm{r}}(x)}{S_{\mathrm{cd}}(x)}\right]\right] = \left[\phi'\left[\frac{P_{\mathrm{r}}(x)}{S_{\mathrm{cd}}(x)}\right]\right]\right],$$

where $[H = \mathrm{e}\ [P_{\mathrm{r}} \| r_{\mathrm{m}}]]$, P_{r} and r_{m}, both values are already sent to the base station by the receiver, therefore the same hash function can be applied at base station end.

$$\left[H\left[\frac{\psi_{P_{\mathrm{r}}(x)}}{\psi_{S_{\mathrm{cd}}(x)}}\right] = H\left\{\phi'\left[\frac{P_{\mathrm{r}}(x)}{S_{\mathrm{cd}}(x)}\right]\right\}\right]$$

$$\left[\left[\frac{\psi_{P_{\mathrm{r}}(x)}}{\psi_{S_{\mathrm{cd}}(x)}}\right] - \left[\frac{\psi_{P_{\mathrm{r}}(x)}}{\psi_{S_{\mathrm{cd}}(x)}}\right]' = 0\right].$$

If the outcome of the procedure is equal to zero, then the authentication will be completed, else the operation will be denied. The Hash function is used to provide the fixed size enciphered data and then that enciphered data will be used for further processing [72, 73]. After the successful execution of the authentication process, a positive acknowledgment Pack will be transmitted to the IoT sensor from the receiver end.

Data transfer phase

The data transfer phase can be shown in Fig. 6. In data transfer mode, the IoT sensor calculates the Euclidean parameter (x, y, z) at their end and will send these parameters to the receiver. These parameters are calculated using the Euclidean Algo $\alpha x + \beta y = z$. Here, (x, y, z) parameters are not directly linked with the information part, so the transmission will take place without sharing the secret data. These parameters are calcu-

lated using the Greatest Common Divisor operation between I_{nf} and $\phi\left[\frac{P_{\text{r}}(x)}{S_{\text{cd}}(x)}\right]$.

Receiver will forward these parameters to the base station for further processing. The values of α' will be calculated at the base station using the received Euclidean parameters and β'. Here, β' is nothing but the Quotient, which is obtained after the division between two function namely $P_{\text{r}}(x)$ and $S_{\text{cd}}(x)$. β' must be equal to β for retracting the correct information at the receiver side.

Proof of the data transmission procedure At IOT sensor: The Euclidean parameters need to be calculated using Eq. (5).

$$\alpha x + \beta y = z = G_{\text{c}}\left[I_{\text{nf}} || \phi\left[\frac{P_{\text{r}}(x)}{S_{\text{cd}}(x)}\right]\right], \tag{5}$$

where α and β are the functions of recorded information and secondary information.

The algo for processing the data at IoT sensor is as follows

Algorithm-4: _*Data transmission at IoT sensor:*

Step 1:**Start**

Step 2: **Read** [α, β, z, x, y]
for α → *Information*
$\beta \rightarrow \left[\phi\left(\frac{P_r(x)}{S_{cd}(x)}\right)\right]$*(Apply polynomial division operation)*
$z \rightarrow G_c\left[I_{nf} || \beta\right]$

Step 3: ***find GCD (α, β)*** →*EUCLID (α, β)*
$\alpha \bmod \beta \rightarrow z$
While $z \neq 0$ ***do***
$\beta \rightarrow \alpha$
$z \rightarrow \beta$
$\alpha \bmod \beta \rightarrow z$
end while
return β
end

Step 4: ***find*** **(x, y)**

$$x \rightarrow \frac{G_c\left[I_{nf} || \phi\left[\frac{P_r(x)}{S_{cd}(x)}\right]\right] - \beta}{(I_{nf})}$$

$$y \rightarrow \frac{G_c\left[I_{nf} || \phi\left[\frac{P_r(x)}{S_{cd}(x)}\right]\right] - (I_{nf})}{\beta}$$

Step 5: ***End***

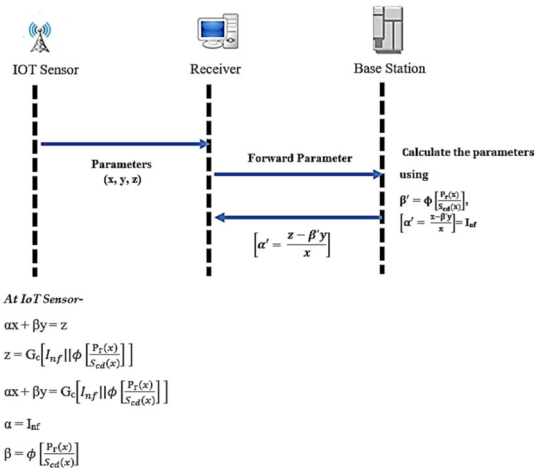

Fig. 6 Data transfer phase

X, Y and Z are known as Euclidean parameters. The value of z has been calculated using Eq. (6).

$$z = G_{\text{c}}\left[I_{\text{nf}} || \phi\left[\frac{P_{\text{r}}(x)}{S_{\text{cd}}(x)}\right]\right] \tag{6}$$

$$\beta = \phi\left[\frac{P_{\text{r}}(x)}{S_{\text{cd}}(x)}\right],$$

apply the value of α and β in equation number (5),

$$(I_{\text{nf}})x + \phi\left[\frac{P_{\text{r}}(x)}{S_{\text{cd}}(x)}\right] y = G_{\text{c}}\left[I_{\text{nf}} || \phi\left[\frac{P_{\text{r}}(x)}{S_{\text{cd}}(x)}\right]\right]$$

$$(I_{\text{nf}})x = G_{\text{c}}\left[I_{\text{nf}} || \phi\left[\frac{P_{\text{r}}(x)}{S_{\text{cd}}(x)}\right]\right] - \phi\left[\frac{P_{\text{r}}(x)}{S_{\text{cd}}(x)}\right] y,$$

after the analysis, the value of x and y will be as follows in Eq. (7)

$$\left[x = \frac{G_{\mathrm{c}}\left[I_{\mathrm{nf}}||\phi\frac{P_{\mathrm{r}}(x)}{S_{\mathrm{cd}}(x)}\right] - \phi\left[\frac{P_{\mathrm{r}}(x)}{S_{\mathrm{cd}}(x)}\right]y}{(I_{\mathrm{nf}})}\right] \tag{7}$$

$$\left[y = \frac{G_{\mathrm{c}}\left[I_{\mathrm{nf}}||\phi\left[\frac{P_{\mathrm{r}}(x)}{S_{\mathrm{cd}}(x)}\right]\right] - (I_{\mathrm{nf}})x}{\phi\left[\frac{P_{\mathrm{r}}(x)}{S_{\mathrm{cd}}(x)}\right]}\right]. \tag{8}$$

IoT sensor calculate the Euclidean parameter (x, y, z) at their end and will send these parameters to the receiver. Here, (x, y, z) parameters are not directly linked with the information part, so the transmission will take place without sharing the secret data.

At the Receiver Receiver will forward these parameters to the base station for further processing. The algo for processing the data at receiver is as follows.

The value of x, y, z is:

$$\left[x = \frac{G_{\mathrm{c}}\left[I_{\mathrm{nf}}||\phi\left[\frac{P_{\mathrm{r}}(x)}{S_{\mathrm{cd}}(x)}\right]\right] - \phi\left[\frac{P_{\mathrm{r}}(x)}{S_{\mathrm{cd}}(x)}\right]}{(I_{\mathrm{nf}})}\right]$$

$$\left[y = \frac{G_{\mathrm{c}}\left[I_{\mathrm{nf}}||\phi\left[\frac{P_{\mathrm{r}}(x)}{S_{\mathrm{cd}}(x)}\right]\right] - (I_{\mathrm{nf}})}{\phi\left[\frac{P_{\mathrm{r}}(x)}{S_{\mathrm{cd}}(x)}\right]}\right]$$

$$z = G_{\mathrm{c}}\left[I_{\mathrm{nf}}||\phi\left[\frac{P_{\mathrm{r}}(x)}{S_{\mathrm{cd}}(x)}\right]\right].$$

Algorithm-5: *Data transmission at receiver:*

Step 1: ***Start***

Step 2: ***Read*** [x, y, z, β] *(values received from IoT sensors)*

for $x \rightarrow \frac{G_{\mathrm{c}}\left[I_{nf}||\phi\left[\frac{P_{\mathrm{r}}(x)}{S_{cd}(x)}\right]\right] - \beta}{(I_{\mathrm{nf}})}$

$y \rightarrow \frac{G_{\mathrm{c}}\left[I_{nf}||\phi\left[\frac{P_{\mathrm{r}}(x)}{S_{cd}(x)}\right]\right] - (I_{\mathrm{nf}})}{\beta}$

$z \rightarrow G_{\mathrm{c}}\left[I_{nf}||\beta\right]$

Step 3: ***Read*** [α', β', x, y, z] *(values received from base station)*

for $\alpha' \rightarrow \frac{z-\beta' y}{x}$ *from Base Station*

$\beta' \rightarrow \phi\left(\frac{P_r(x)}{S_{cd}(x)}\right)$ *for Base Station*

{

If, $\beta = \beta'$

then *accept the information*

Else

Dropped the communication message

}

Step 4: ***End***

At the Base station The values of α' will be calculated at the base station using the received Euclidean parameters and β'. Here, β' is nothing but the Quotient, which is obtained after the division between two functions namely $P_{\mathrm{r}}(x)$ and $S_{\mathrm{cd}}(x)$. β' must be equal to β for retracting the correct information at the receiver side.

$$\alpha' x + \beta' y = z = G_{\mathrm{c}}\left[I_{\mathrm{nf}}||\phi\left[\frac{P_{\mathrm{r}}(x)}{S_{\mathrm{cd}}(x)}\right]\right]. \tag{9}$$

Put the value of x, y and z in Eq. (9):

$$\left[\alpha\left[\frac{G_c\left[I_{nf}||\phi\left[\frac{P_r(x)}{S_{cd}(x)}\right]\right]-\phi\left[\frac{P_r(x)}{S_{cd}(x)}\right]}{(I_{nf})}\right]+\phi\left[\frac{P_r(x)}{S_{cd}(x)}\right]\frac{G_c\left[I_{nf}||\phi\left[\frac{P_r(x)}{S_{cd}(x)}\right]\right]-(I_{nf})}{\phi\left[\frac{P_r(x)}{S_{cd}(x)}\right]}=G_c\left[I_{nf}||\phi\left[\frac{P_r(x)}{S_{cd}(x)}\right]\right]\right]$$

$$\alpha=\left[\frac{G_c\left[I_{nf}||\phi\left[\frac{P_r(x)}{S_{cd}(x)}\right]\right]-\phi\left[\frac{P_r(x)}{S_{cd}(x)}\right]\frac{G_c\left[I_{nf}||\phi\left[\frac{P_r(x)}{S_{cd}(x)}\right]\right]-(I_{nf})}{\phi\left[\frac{P_r(x)}{S_{cd}(x)}\right]}}{\frac{G_c\left[I_{nf}||\phi\left[\frac{P_r(x)}{S_{cd}(x)}\right]\right]-\phi\left[\frac{P_r(x)}{S_{cd}(x)}\right]}{I_{nf}}}\right].$$

The value of α can be calculated using the above mathematical expression, the final value of α is as follows:

$$\text{Assume}\begin{cases} a=G_c\left[I_{nf}||\phi\left[\frac{P_r(x)}{S_{cd}(x)}\right]\right] \\ b=\phi\left[\frac{P_r(x)}{S_{cd}(x)}\right]\end{cases}.$$

Then, the final expression will as follows:

$$\alpha=\frac{a-b\left[\frac{a-I_{nf}}{b}\right]}{\left[\frac{a-b}{I_{nf}}\right]} \quad\Rightarrow\quad \boldsymbol{\alpha=\frac{I_{nf}^2}{a-b}}$$

The algo for processing the data at base station is as follows

Where a and b are also the function of information I_{nf}. Hence, it is verified that the communication can be confirmed between the IoT sensor and receiver without sharing secret information. In the proposed technique, the significance of the Euclidean theorem is to create complexity in the calculation of different parameters, and confusion in the way of the adversary or attacker. The proposed technique will be very useful in many applications of IoT such as smart city, smart banking and smart transport, etc.

The analysis of security

In this section, we have analyzed the security of the proposed technique with various features such as replay attack resistance, authentication attack and resistance to forging attack.

Algorithm-6: _*Data transmission at base station:*

Step 1:**Start**

Step 2: **Read** [x, y, z, α', β'] *(values received from IoT sensors)*
[α', β'] *(values calculated at base station)*
for $\beta' \rightarrow \phi\left(\frac{P_r(x)}{S_{cd}(x)}\right)$ *(Apply polynomial division operation at base station)*
{Let $P_r(x)$ *and* $S_{cd}(x)$ *are the two polynomials of degree n and m, then there will be two more polynomials namely quotient* $\phi\left(\frac{P_r(x)}{S_{cd}(x)}\right)$ *and remainder}*
$P_r(x) \rightarrow$ *Polynomial of* P_r *at Base* Station
$S_{cd}(x) \rightarrow$ *Polynomial of Secondary Data at Base* Station

Step 3: ***find*** $\alpha' \rightarrow \{\alpha' x + \beta' y = z = G_c\left[I_{nf}||\phi\left[\frac{P_r(x)}{S_{cd}(x)}\right]\right]\} \rightarrow \frac{z-\beta' y}{x}$
put the value of x, y, z and $\beta' \rightarrow \phi\left(\frac{P_r(x)}{S_{cd}(x)}\right)$

$$\textit{assume}\begin{cases} a = G_c\left[I_{nf}||\phi\left[\frac{P_r(x)}{S_{cd}(x)}\right]\right] \\ b = \phi\left[\frac{P_r(x)}{S_{cd}(x)}\right]\end{cases}$$

$\alpha=\frac{I_{nf}^2}{a-b}$ *{a and b are also the function of information* I_{nf}*}*

Step 4: ***End***

Table 2 Comparative analysis

	Dass et al. [57]	Fu et al. [58]	Chang et al. [59]	Li et al. [60]	Gui et al. [61]	Min et al. [62]	Ours
DoS attack resistance	N	N	N	Y	N	N	Y
Resistivity replay attack	Y	Y	Y	Y	Y	Y	Y
De synchronization resistance	Y	N	N	Y	N	N	Y
Mutual authentication	Y	N	Y	Y	Y	N	Y
Master key attack	N	Y	N	N	N	N	Y
Forward secrecy	Y	N	Y	N	Y	Y	Y
MITM attack resistance	Y	Y	Y	Y	Y	Y	Y
Traceability resistance	Y	N	Y	N	Y	Y	Y
Confidentiality and integrity	Y	Y	Y	Y	Y	Y	Y
Anonymity of tag	N	Y	Y	Y	Y	Y	Y

Y satisfy, *N* not satisfy

Resistance to replay attack In the replay attack, an attacker can delay or repeat the transmission of the valid message [74]. In this attack, the attacker intercepts the data and retransmit it. The adversary cannot perform this attack in the proposed technique, because the time stamp Ti is included in all the messages processed by the sensor or receiver. The timestamp will be verified at both the end for avoiding the replay attack. The communication message can be dropped if the timestamp is not acceptable.

Authentication attack In the proposed technique, the authentication procedure is very secured. Here, the IoT sensor sharing a secret message E_{cp} to the receiver for performing the authentication. The secret message E_{cp} is the function of two random variables which are P_r (Prime number) and r_m (random number) and these values are not fixed for each transaction. For the adversary, it is not possible to compute the exact value of $E_{cp.}$ Therefore, an attacker cannot perform an authentication attack.

Forging attack Forging is a dangerous attack performed by the attackers. In this attack, the adversary trying to forge the private key of the communication process [75]. In the proposed technique, IoT sensor sharing a secret message E_{cp} to the receiver for performing the authentication. The secret message E_{cp} is the function of two random variables which are P_r (Prime number) and r_m (random number) and these values are not fixed for each transaction. Therefore, it is not possible to find the exact values of P_r and $r_{m.}$

A comparative analysis in terms of adversary attacks can be shown in Table 2 and Fig. 7. In Table 2, various attacks have been shown over which the proposed technique is compatible to overcome the adversary action.

Computational cost and comparative analysis

In this section, the efficiency of the proposed technique is computed in terms of computational cost and comparative analysis. Previously published approaches have been considered for performing the comparative analysis.

Computational cost analysis

In the proposed technique, the computational cost has been computed using the time taken to authenticate one user or n number of users. The studies considered for the comparative analysis are Sun's et al. [31] scheme, Dass et al. [57] scheme, Chang et al. [59]. scheme, Fu et al. [58] scheme, Chen et al. [63] scheme and Gui et al. [61] scheme. Following parameters have been considered for the analysis of computational cost T_M: division operation, T_D: division operation, T_X: cost of XOR operation, T_F: cost of flip operation, T_S cost of circular shift operation, T_P: cost of paring operation, T_H: cost of hash function, T_A: division operation and T_R: cost of random number generation operation.

From Table 3, it can be seen that the computation cost of the proposed technique is comparatively very less. The computational cost of the proposed technique is $1T_H$, $2T_P$, and $1T_D$ only. Hence, the proposed algo is computationally efficient than the previous techniques.

The proposed approach is compatible to provide security against most of the attacks performed by the attackers. Two random variables and complex mathematical calculations are making the proposed technique more reliable than others.

Fig. 7 Comparative analysis

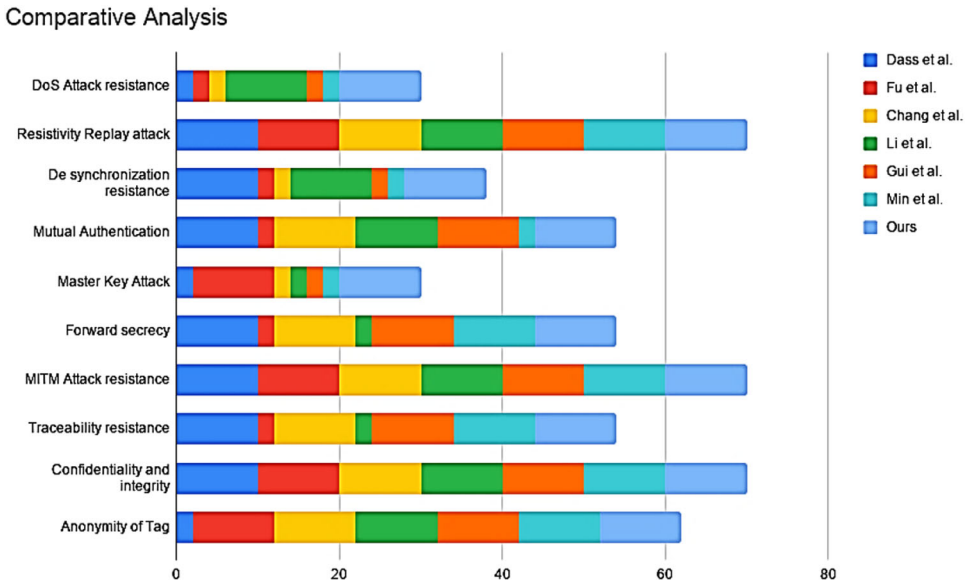

Table 3 Computational cost of authentication

	Computation cost for one user	Computational cost for n user
Sun's et al. [31] scheme	$2T_M + 1T_H + 2T_A$	$2nT_M + 1nT_H + 2nT_A$
Dass et al. [57] scheme	$1T_R + 1T_X + 3T_P + 2T_H$	$1nT_R + 1nT_X + 3nT_P + 2nT_H$
Chang et al. [59] scheme	$4T_H + 11T_X + 2T_R$	$4nT_H + 11nT_X + 2nT_R$
Fu et al. [58] scheme	$2T_R + 2T_X + 4T_H$	$2nT_R + 2nT_X + 4nT_H$
Chen et al. [63] scheme	$T_M + 2T_H + 2T_P + T_A$	$nT_M + 2nT_H + 2nT_P + nT_A$
Gui et al. [61] scheme	$2T_R + 1T_F + 2T_X + 3T_H$	$2nT_R + 1nT_F + 2nT_X + 3nT_H$
Ours	$1T_H + 2T_P + 1T_D$	$1nT_H + 2nT_P + 1nT_D$

Conclusion

In this paper, a secure data transmission technique has been introduced for IoT infrastructure. Each IoT sensor (IOi) have to prove their legitimacy to the reader (Ri) and the base station (BSi) before the transmission of data. The proposed technique includes three phases namely registration, authentication, and data transfer phase to complete communication between sensor and receiver. For security enhancements, the sensor node needs to send three Euclidean parameters to the receiver instead of recorded information. The proof of correction shows that the required information is not supposed to send through an online medium, it is obtained at the receiver using the Euclidean parameters shared by the IoT Sensors. This technique will significantly improve the security of data transmission services, which will lead to improving the smart city infrastructure. Figure 5 shows that the proposed technique resists many attacks such as Authentication attacks, User anonymity, forging attacks, and many more performed by the adversary. The authentication execution time for the proposed technique is very less in comparison with other techniques. Furthermore, a practical overview is needed for the proposed technique, which will have less execution time. An encrypted timestamp will be the next option to increase the complexity and confusion in the way of attackers. A more complex authentication approach for device-to-device communication in IoT infrastructure will be the next objective of this study.

Funding No funding.

Availability of data and materials Not applicable.

Code availability Not applicable.

Declarations

Conflict of interest There is no conflict of interest.

References

1. Arias O, Wurm J, Hoang K, Jin Y (2015) Privacy and security in internet of things and wearable devices. IEEE Trans Multiscale Comput Syst 1(2):99–109. https://doi.org/10.1109/TMSCS.2015.2498605
2. Khatoun R, Zeadally S (2017) Cybersecurity and privacy solutions in smart cities. IEEE Commun Mag 55(3):51–59. https://doi.org/10.1109/MCOM.2017.1600297CM
3. Pouryazdan M, Kantarci B (2016) The smart citizen factor in trustworthy smart city crowdsensing. IT Prof 18(4):26–33
4. Cabaj K, Mazurczyk W (2016) Using software-defined networking for ransomware mitigation: the case of cryptowall. IEEE Netw 30(6):14–20. https://doi.org/10.1109/MNET.2016.1600110NM
5. Mohurle S, Patil M (2017) A brief study of Wannacry threat: Ransomware attack. Int J 8(5):1938–1940
6. Liao K, Zhao Z, Doupe A, Ahn GJ (2016) Behind closed doors: Measurement and analysis of cryptolocker ransoms in bitcoin. 2016 APWG symposium on electronic crime research (eCrime), 1–13. https://doi.org/10.1109/ECRIME.2016.7487938
7. Angrishi K (2017) Turning internet of things (IoT) into internet of vulnerabilities (IoV): IoT botnets. arXiv preprint arXiv:1702.03681
8. Smith KL (2017) The inconvenient truth about smart cities. https://blogs.scientificamerican.com/observations/the-inconvenient-truth-about-smartcities/. Accessed 16 Feb 19
9. Nam T, Pardo TA (2011) Smart city as urban innovation: focusing on management, policy, and context. Proceedings of the 5th international conference on theory and practice of electronic governance. ACM, pp 185–194
10. Whittaker B (1999) What went wrong? Unsuccessful information technology projects. Inf Manag Comput Secur 7(1):23–30
11. Goldfinch S (2007) Pessimism, computer failure, and information systems development in the public sector. Public Adm Rev 67(5):917–929
12. Shishvan OR, Zois D, Soyata T (2018) Machine intelligence in healthcare and medical cyber physical systems: a survey. IEEE Access. https://doi.org/10.1109/ACCESS.2018.2866049
13. Soyata T, Copeland L, Heinzelman W (2016) RF energy harvesting for embedded systems: a survey of tradeoffs and methodology. IEEE Circuits Syst Mag (MCAS) 16(1):22–57. https://doi.org/10.1109/MCAS.2015.2510198
14. Zhang ZK, Cho MCY, Wang CW, Hsu CW, Chen CK, Shieh S-P (2014) IoT security: ongoing challenges and research opportunities. In: Proceedings - IEEE 7th international conference on service-oriented computing and applications, SOCA 2014. Matsue, 17–19 Nov 2014, pp 230–234
15. Reuben, K. (2011). Municipal budget shortfalls. https://www.taxpolicycenter.org/taxvox/municipal-budget-shortfalls. Accessed 16 Feb 19
16. Maciag M, Wogan J (2017) With less state aid, localities look for ways to cope. Governing 30:32–37
17. Pagano MA, Hoene CW (2018) City budgets in an era of increased uncertainty: understanding the fiscal policy space of cities. Brookings Institution, Washington, DC. https://www.brookings.edu/wp-content/uploads/2018/07/20180718_BrookingsMetro_City-fiscal-policy-Pagano-Hoene-final.pdf
18. Sharma N, Sultana HP, Singh R, Patil S (2019) Secure hash authentication in IoT based applications. Procedia Comput Sci 165:328–335. https://doi.org/10.1016/j.procs.2020.01.042. ISSN 1877-0509
19. Koblitz N (1987) Elliptic curve cryptosystems. Math Comput 48(177):203–209
20. Recommendation for key management—Part 1: General (2005) Gaithersburg, MD, USA: Special Publication 800-57 Aug.
21. Advances in Cryptology-CRYPTO (2001) Identity-based encryption from the Weil pairing. Advances in cryptology-CRYPTO, vol. 2139. Springer, Berlin, pp 213–229 LNCS
22. Romdhani I (2017) Chapter 7—existing security scheme for IoT. In: Li S, Xu LD (eds) Securing the internet of things, Syngress. pp. 119–130. https://doi.org/10.1016/B978-0-12-804458-2.00007-X. ISBN 9780128044582
23. Lim HW, Robshaw MJB (2004) On identity-based cryptography and grid computing. In: Bubak M, van Albada GD, Sloot PMA, Dongarra J (eds) Computational science - ICCS 2004. Lecture notes in computer science, vol 3036. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-24685-5_69
24. Lim HW, Robshaw MJB (2005) A dynamic key infrastructure for grid. In: Sloot PMA, Hoekstra AG, Priol T, Reinefeld A, Bubak M (eds) Advances in grid computing - EGC 2005. Lecture notes in computer science, vol 3470. Springer, Berlin, Heidelberg. https://doi.org/10.1007/11508380_27
25. Mao W (2004) An identity-based non-interactive authentication framework for computational grids. Palo Alto, CA, USA: HP Labs Tech. Rep. HPL-2004-96, Jun
26. Ahmad A, Paul A, Khan M, Jabbar S, Rathore MMU, Chilamkurti N et al (2017) Energy efficient hierarchical resource management for mobile cloud computing. IEEE Trans Sustain Comput 2(2):100–112
27. Chen T, Yeh H, Shih W (2011) An advanced ecc dynamic id-based remote mutual authentication scheme for cloud computing. In: 2011 fifth FTRA international conference on multimedia and ubiquitous engineering. Loutraki, 28–30 June 2011, pp 155-159. https://doi.org/10.1109/MUE.2011.69
28. Goriparthia T, Das ML, Saxena A (2009) An improved bilinear pairing based remote user authentication scheme. Comput Stand Interfaces 31(January 1):181–185
29. Das ML, Saxena A, Gulati VP, Phafstak DB (2006) A novel remote user authentication scheme using bilinear pairings. Comput Secur 25(May 3):184–189
30. Khan Pathan S, Hong CS, Hee K (2009) Bilinear-pairing-based remote user authentication schemes using smart cards. In: Proceedings of 3rd international conference ubiquitous information management communication. New York, pp 356–361
31. Sun H, Wen Q, Zhang H, Jin Z (2013) A novel remote user authentication and key agreement scheme for mobile client–server environment. Appl Math Inf Sci Lett 7(4):1365–1374
32. Gope P, Das AK (2017) Robust anonymous mutual authentication scheme for ntimes ubiquitous mobile cloud computing services. IEEE Internet Things J 4(October 5):1764–1772. https://doi.org/10.1109/JIOT.2017.2723915
33. Roy S, Chatterjee S, Das AK, Chattopadhyay S, Kumar N, Vasilakos AV (2017) On the design of provably secure lightweight remote user authentication scheme for mobile cloud computing services. IEEE Access 5:25808–25825. https://doi.org/10.1109/ACCESS.2017.2764913
34. Zhang A, Wang L, Ye X, Lin X (2017) Light-weight and robust security-aware D2D-assist data transmission protocol for mobile-health systems. IEEE Trans Inf Forensics Secur 12(March 3):662–675. https://doi.org/10.1109/TIFS.2016.2631950
35. Moctar CBOME, Konaté K (2017) A survey of security challenges in cloud computing. International conference on wireless communications, signal processing and networking (WiSPNET). pp 843–849. https://doi.org/10.1109/WiSPNET.2017.8299880
36. Fotouhi M, Bayat M, Das AK, Far HAN, Pournaghi SM, Doostari MA (2020) A lightweight and secure two-factor authentication scheme for wireless body area networks in health-care IoT. Comput

Netw 177: 107333. https://doi.org/10.1016/j.comnet.2020.107333. ISSN 1389-1286
37. Jegadeesan S, Azees M, Kumar PM, Manogaran G, Chilamkurti N, Varatharajan R, Hsu C-H (2019) An efficient anonymous mutual authentication technique for providing secure communication in mobile cloud computing for smart city applications. Sustain Cities Soc 49:101522. https://doi.org/10.1016/j.scs.2019.101522
38. Jose DV, Vijyalakshmi A (2018) An overview of security in internet of things. Procedia Comput Sci 143:744–748. https://doi.org/10.1016/j.procs.2018.10.439. ISSN 1877-0509
39. Li Z, Haiyang Hu, Hua Hu, Huang B, Ge J, Chang V (2021) Security and energy-aware collaborative task offloading in D2D communication. Future Gener Comput Syst 118:358–373
40. Qi R, Ji S, Shen J, Vijayakumar P, Kumar N (2021) Security preservation in industrial medical CPS using Chebyshev map: an AI approach. Future Gener Comput Syst 122:52–62
41. National Protection and Programs Directorate Office of Cyber and Infrastructure Analysis (2015) The future of smart cities: Cyber-physical infrastructure risk. https://ics-cert.us-cert.gov/sites/default/files/documents/OCIA%20-%20The%20Future%20of%20Smart%20Cities%20-%20Cyber-Physical%20Infrastructure%20Risk.pdf. Accessed 21 July 17
42. Al-Naji FH, Zagrouba R (2020) CAB-IoT: continuous authentication architecture based on blockchain for internet of things. J King Saud Univ Comput Inf Sci. https://doi.org/10.1016/j.jksuci.2020.11.023. ISSN 1319-1578
43. Baker AB, Eagan RJ, Falcone PK, Harris JM, Herrera GV, Hines WC et al (2019) A scalable systems approach for critical infrastructure security. Sandia National Laboratories, Albuquerque
44. Al-rimy BAS, Maarof MA, Shaid SZM (2018) Ransomware threat success factors, taxonomy, and countermeasures: a survey and research directions. Comput Secur 74:144–166
45. Hampton N, Baig ZA, He D, Chan S, Guizani M (2015) Ransomware: Emergence of the cyber-extortion menace. User privacy and data trustworthiness in mobile crowd sensing. IEEE Wirel Commun 22(1):28–34
46. O'Gorman G, McDonald G (2012) Ransomware: a growing menace. Symantec Corporation, Tempe
47. Francescani C (2016) Ransomware hackers blackmail US Police departments. https://www.nbcnews.com/news/us-news/ransomware-hackersblackmail-u-s-police-departments-n561746. Accessed 16 Feb 19
48. Mathews, L. (2018). Ransomware that hit Atlanta's computers destroyed police evidence https://www.forbes.com/sites/leemathews/2018/06/08/ransomware-that-hit-atlantas-computers-destroyed-police-evidence/#2143b552112d. Accessed 16 Feb 19
49. Wagstaff K (2013) Big paydays force hospitals to prepare for ransomware attacks https://www.nbcnews.com/tech/security/big-paydays-force-hospitalsprepare-ransomware-attacks-n557176. Accessed 16 Feb 19
50. Dwyer A (2018) The NHS cyber-attack: a look at the complex environmental conditions of WannaCry. RAD Mag 44(512):25–26
51. Ehrenfeld JM (2017) Wannacry, cybersecurity and health information technology: a time to act. J Med Syst 41(7):104
52. Martin G, Ghafur S, Kinross J, Hankin C, Darzi A (2018) WannaCry-a year on. BMJ 361:k2381. https://doi.org/10.1136/bmj.k2381
53. Gallagher S (2016) Ransomware locks up San Francisco public transportation ticket machines: some systems now restored; attacker demanded $73,000 https://arstechnica.com/security/2016/11/san-francisco-muni-hit-by-black-fridayransomware-attack/. Accessed 21 July 17
54. Stewart J (2016) San Franciscos transit hack couldve been way worse—and cities must prepare. https://www.wired.com/2016/11/sfs-transit-hackcouldve-way-worse-cities-must-prepare/. Accessed 21 July 17
55. Bay Area Rapid Transit (2017). About BART. https://www.bart.gov. Accessed 08 Oct 17. Beresford AR, Stajano F (2003) Location privacy in pervasive computing. IEEE Pervasive computing 2(1):46–55
56. Abendroth B, Kleiner A, Nicholas P (2017) A scalable systems approach for critical infrastructure security https://mscorpmedia.azureedge.net/mscorpmedia/2017/05/IoT_WhitePaper_5_15_17.pdf. Accessed 21 July 17
57. Dass P, Hari O (2016) A secure authentication scheme for RFID systems. International Conference on Information Security & Privacy (ICISP2015), 11–12 December 2015, Nagpur, INDIA; Procedia Computer Science, vol 78. pp. 100–106
58. Fu J, Wu C, Chen X, Fan R, Ping L (2010) Scalable pseudo random RFID private mutual authentication. 2nd IEEE International conference on computer engineering and technology (ICCET), vol 7. pp 497–500.
59. Chang AY, Dwen-Ren T, Chang-Lung T, Yong-Jiang L (2009) An improved certificate mechanism for transactions using radio frequency identification enabled mobile phone. Security Technology; 43rd Annual International Carnahan Conference. IEEE, pp 36–40
60. Li J, Wang Y, Jiao B, Xu Y (2010) An authentication protocol for secure and efficient RFID communication. In: 2010 international conference on logistics systems and intelligent management (ICLSIM). Harbin, pp 1648–1651. https://doi.org/10.1109/ICLSIM.2010.5461250
61. Gui Y-G, Zhang J (2013) A new authentication RFID protocol with ownership transfer. In: 2013 international conference on ICT convergence (ICTC). Jeju, Korea (South), pp 359–364. https://doi.org/10.1109/ICTC.2013.6675373
62. Chen M, Chen S (2015) An efficient anonymous authentication protocol for RFID systems using dynamic tokens. In: 2015 IEEE 35th international conference on distributed computing systems. Columbus, OH, pp 756–757. https://doi.org/10.1109/ICDCS.2015.94
63. Chen T, Yeh H, Shih W (2011) An advanced ECC dynamic ID-based remote mutual authentication scheme for cloud computing. In: 2011 fifth FTRA international conference on multimedia and ubiquitous engineering. Crete, pp 155–159. https://doi.org/10.1109/MUE.2011.69
64. Heeks R, Bhatnagar S (1999) Understanding success and failure in information age reform. Reinventing Gov Inf Age Int Pract IT Enabled Public Sect Reform 1:49–74
65. Mosenia A, Jha NK (2017) A comprehensive study of security of internet-of-things. IEEE Trans Emerg Top Comput 5(4):586–602. https://doi.org/10.1109/TETC.2016.2606384
66. Data Breach Investigations Report (2018) Executive summary. https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_execsummary_en_xg.pdf. Accessed 16 Feb 19
67. Bartoli A, Hernández-Serrano J, Soriano M, Dohler M, Kountouris A, Barthel D (2011) Security and privacy in your smart city. Proceedings of the Barcelona smart cities congress. pp 1–6
68. Cerrudo C (2015) An emerging us (and world) threat: cities wide open to cyberattacks. Securing Smart Cities
69. Logota E, Mantas G, Rodriguez J, Marques H (2014) Analysis of the impact of denial of service attacks on centralized control in smart cities. International wireless internet conference. Springer, pp 91–96
70. Conti G, Cross T, Raymond D (2015) Pen testing a city. https://www.blackhat.com/docs/us-15/materials/us-15-Conti-Pen-Testing-A-City.pdf
71. Kitchin R (2016) Getting smarter about smart cities: Improving data privacy and data security. Data Protection Unit, Department of the Taoiseach

72. Internet of things privacy and security in a connected world. https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-reportnovember-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf. Accessed 21 July 17
73. Lévy-Bencheton C, Darra E (2015) Cyber security for smart cities—an architecture model for public transport. https://doi.org/10.2824/846575
74. Ijaz S, Shah MA, Khan A, Ahmed M (2016) Smart cities: a survey on security concerns. Int J Adv Comput Sci Appl 7:612–625
75. Razzaq MA, Gill SH, Qureshi MA, Ullah S (2017) Security issues in the Internet of Things (IoT): a comprehensive study. Int J Adv Comput Sci Appl (IJACSA) 8(6):2017. https://doi.org/10.14569/IJACSA.2017.080650