A Lightweight Privacy Preservation Protocol for IOT

A Data and Metadata Protection Protocol

Ahmed Mahmoud Al-Badawy[1], Mohammed Belal[2], Hala Abbas[3]
Teaching Assistant, Computer Science Department-Faculty of Computers and Artificial Intelligence,
Helwan University, Cairo, Egypt[1]
Prof., Computer Science Department-Faculty of Computers and Artificial Intelligence, Helwan University, Cairo, Egypt[2]
Assist. Prof., Computer Science Department-Faculty of Computers and Artificial Intelligence, Helwan University[3]
Faculty of Computer Studies, Arab Open University, Cairo, Egypt[3]

***Abstract*—Due to rapid evolution of Internet of things (IOT) in terms of hardware, software and communication leads to widespread expansion across many domains and sectors. This expansion consequently results in sensitive data transfer increase for purposes of complex calculations and decision making which in turn leads to increase of data attacks and leakage which results in data privacy violation. Although, a lot of current solutions tried to fulfill data privacy via lightweight mechanisms but neither provided end to end protection nor gave a focus to metadata protection which can reveal valuable information about data it describes. This paper presents a lightweight complete data privacy protocol which manages the lifecycle of data starting from object registration till data transfer to cloud. The proposed protocol is a trusted third party free (TTP-Free) which adopts anonymization techniques, lightweight key agreement protocol, end to end encryption and message authentication code to fulfill identity and data protection which in turn fulfill complete data privacy.**

***Keywords*—IOT; data privacy; lightweight protocols; end to end protection; data and metadata protection**

I. Introduction

Internet of Things (IOT) is a physical network of resource constrained objects (ex. sensors, actuators, wearables, IIOT devices) connected together in order to rapidly exchange data to fulfill a specific job. IOT has three main visions [1] to focus on:

- Things vision which tends to focus on generic objects and integration of them into a framework (ex. RFID, NFC).
- Internet vision which tends to present IOT as a network-oriented (ex. IPO, communicating things).
- Semantic vision [2] which tends to view IOT as a worldwide network of interconnected things that can be uniquely identified (ex. reasoning over data, semantic technologies).

IOT in general aims to facilitate people's life and enhance countries' economies via introducing smart solutions capable of serving required needs which in turn leads to a better world. It can connect people, things, objects, and devices regardless of time and location with barrier free manner. With, the advances in IOT hardware and software started from enhancing communications networks, devices and reducing things sizes and cost reduction for constructing IOT networks led to invasion and domination of IOT in many domains due to benefits got from.

Healthcare [3][4] is one of domains that IOT tried to support to enhance people health and saves their life. Medical IOT aims to serve patients via presenting a lot of services started from monitoring services [5][6] where patients' health is tracked to avoid any health disaster till complex healthcare solutions for malignant diseases like cancer [7][8]. Moreover, IOT used to fight against pandemic diseases like Covid 19 [9][10].

Agriculture is another domain that IOT gave attention to enrich and support due to its economic importance to countries. IOT developed a special type of network [11] called agriculture IOT sensor monitoring networks (ASMN) in order to fully monitor farmland in (temperature, humidity, light and soil moisture) and take appropriate actions needed. These networks [12] aim to continuously monitor crops to protect crops' health.

Industry is the third domain that IOT tried to automate and support with industrial IOT (IIOT). IIOT [13][14] is a specialized network which manufacturers adopt to enhance production process started from supplying raw materials till customer services.

The advancement of IOT networks and increasing NO. of objects used led to increased exchange of sensitive data which in turn lead to a lot of security and privacy problems. Data privacy is one of the most important problems to be focused on due to sensitivity of data. Data here can be personal, healthcare, industrial or even militaria which needs to be protected while being transferred.

A lot of attacks aim to leak data to be abused, attacks can be categorized into two types:

- Active attacks which attacker tries to change the whole or part of data while being transferred.
- Passive attacks which attacker tries to read data only without any change.

In this paper, a lightweight trusted third-party free (TTP-Free) data privacy protocol is presented to build a secure communication channel for Device to cloud (D2C) which aims to protect IOT data and metadata as well. Although metadata might seem less important, it can reveal valuable information about the data it describes which in turn leads to privacy

compromise. The protocol depends mainly on four parts to fulfill privacy:

- Anonymization: regularly changing objects' identities in order to avoid tracking and impersonation attacks based on objects known IDs.
- Lightweight Key agreement Protocols: used between objects and cloud to construct session key without directly exchanging it which will be used later for data encryption/decryption.
- Lightweight End to End Encryption: designed especially for constrained devices to encrypt/decrypt data using already constructed key between object and cloud to make sure that no party can decrypt data transferred except cloud.
- Message Authentication Code: used to authenticate message via edge to ensure integrity and authenticity of data which in turn resist active attacks.

The paper is structured as follows: Section II gives an overview of the related work and the main differences between proposed work and existing research. Section III provides an overview of proposed protocol, all related algorithms and techniques used. Section IV discusses security analysis of proposed protocol via threat model and its analysis. Section V evaluates the proposed protocol against existing one to clarify strength and weakness of each one at predefined criterion. Section VI provides conclusion and future work.

II. Related Work

A lot of researches tried to provide solutions and mechanisms to IOT data privacy leakage due to its necessity. Many attacks include impersonation, injection, eavesdropping, data theft and reprogram attacks aims to track IOT networks for data leakage and abuse.

J. Andrew [15] proposed an anonymization clustering schema which aims to fulfill data privacy in medical IOT. This schema depends on two parts, client side which is responsible for anonymizing data generated by things using clustering K anonymity which fulfill privacy via clustering methodology, server side which uses cluster combination to reduce communication overhead which achieve privacy. This schema employs a trusted intermediate aggregation node to anonymize data got from client then send it to untrusted server to be sent to data collector. Usage of anonymization techniques with trusted third-party only fulfills data privacy partially due to a lot of attacks that can lead to original data restoring (ex. Re-identification attacks) besides relying on TTP -aggregation node- which can be attacked.

Xuezhen [16] proposed a framework that aims to fulfill security and data privacy via cryptography and behavior pattern analysis. The framework is divided into levels according to IOT main entities:

- Objects: which is defined as sensors and actuators each of them has a security and privacy requirements.
- Communication networks: is responsible for communication between objects that needs to be protected to protect network from abuse.
- Users: who use the IOT, which is the most sensitive part as part of people in this context will be attackers themselves so users' behaviors must be carefully analyzed and stored to detect any malicious behavior.

In order to provide security and privacy to users and data. The framework used secured channel to fulfill required security but did not mention how to accomplish this. Moreover, the framework deals direct with object real identities which makes the system vulnerable to impersonation and tracking attacks.

Uzair Javaid [17] focused on data provenance and integrity by using BlockpPo framework which is a combination between PUFs which produces a unique response so data provenance is established with each IOT device, and blockchain which enforces data integrity to fulfill data privacy. Although, blockchain tried to fulfill data privacy across IOT networks, but still has a lot of challenges [18] which may affect that fulfillment starting from choosing blockchain platform (public, private) which will affect confidentiality and integrity of data. Moreover, the identity will be disclosed due to sharing transactions with their owners.

Othman [19] proposed a privacy preserving schema using homomorphic encryption in order to protect healthcare data privacy. Its main goal is to provide safe and secure aggregation for data with respect to energy consumption. The schema tried to protect data from active, passive, internal and external attacks. Although the proposed schema depends mainly on cryptography using homomorphic encryption which enables coordinator to work on without needs to decryption, it does take into consideration objects' identity protection which in turncan lead to tracking and impersonation attacks. Moreover, the schema does not state the data encryption decryption key mechanism used which is considered a very critical part to be covered due to diversity of attacks occurred on that part.

Prem Prakash [20] proposed a technique for data privacy preserving via introducing privacy preserving IOT architecture based on OpenIOT [21]. This architecture provides end to end privacy by giving ability to control access to sensitive IOT data via distributing and decomposing data into multiple data stores and then aggregated again when needed [22]. The technique composed of four communication parts (IOT device and gateway, gateway and data store, data store and data access finally, data access and user) which assumes that these communication channels are secured by applying cryptography and key sharing mechanisms only. Although this approach tried to fulfill data privacy by focusing on how to hide data that is transferred from between communication parties, this approach is not adequate to fulfill objective needed. Focusing on data only without paying attention to object identities can lead to data leakage which in turn leads to data privacy issues.

Mamun Abu-Tair [21] proposed a new architecture that aims to support IOT applications with a specified level of security and privacy. The architecture is bundled with new algorithm that is responsible for configuration of newly added sensors in terms of cryptographic suite to match target

applications. The architecture employs cryptography and anonymization to fulfill complete privacy but relying on trust management schema is considered a weak point. Moreover, key management schema is not stated which can lead to critical attacks.

Shancang Li [23] presents a lightweight privacy preserving protocol which aims to address privacy issues between objects, cloud and users using cryptography – homomorphic encryption-. The protocol depends on a key management schema which employs users' keys beside objects' keys to make sure that the data will be delivered to correct user. Although the protocol tried to fulfill data privacy but it has a major concern to be addressed, the protocol did not state in details key sharing mechanism which can be a weak point to the whole protocol moreover, the protocol deals with objects with their real identity which makes the system vulnerable to impersonation and tracking attacks.

Mohammed Ahmed [24] used remote patient monitoring as a case study in healthcare domain to fulfill security and data privacy via proposing a new system that provides mutual authentication and employed cryptography to protect data while being transferred. Although the proposed system tried to fulfill privacy via applying cryptography, the system does not pay attention to object identities which can be tracked and impersonated. Moreover, the registration phase for objects is not powerful to forbid injection attacks.

Xi lou [25] presented a lightweight security protocol which aims to fulfill data privacy via cryptography and symmetric key mechanism. This protocol tries to maximize symmetric keys generated via key delegation which uses chaotic system and logistic map to ensure unpredictability and unrepeatability of keys generated. The protocol depends mainly on control center as a trusted third party to be responsible for key management between communication parties which is considered a weak point if got controlled by attackers.

A lot of protocols and systems tried to fulfill data privacy by focusing on either protecting objects' identities or data which is considered a partially fulfillment. Some of them is trusted third party and others is trusted third party free. Up to our knowledge, all protocols focus mainly on objects' data as a protection level, but no one pay attention to metadata – like gateway id, manager id -. This gap is critical to be protected since leakage will lead to disclosure of much sensitive information (ex. Objects cluster, network location and sometimes object itself) will lead to data privacy violation. The proposed protocol is a trusted third party free which aims to fulfill full data privacy by protecting objects' identities and their data. Moreover, the proposed protocol has put into consideration the protection of metadata to avoid any privacy violation.

III. Proposed Protocol

The proposed protocol is considered a communication protocol with a set of defined rules that regulate exchange of data between parties in a secure manner to fulfill data privacy. The protocol focuses mainly on both:

- Data mainly reads from objects and needs to be transferred to the cloud.
- Metadata, which is data about data like timestamp, gateway id, edge id which needs to be protected as well.

The proposed protocol is trusted third party free that focuses on fulfilling data privacy via securing communication channels between objects and cloud by using lightweight key agreement protocol and end to end encryption to ensure that only cloudcan decrypt the data issued by objects. In addition, the protocol employs anonymization techniques for objects in order to prevent tracking and impersonation attacks for objects. Therefore, being trusted third party free and providing secure communication channel beside objects' identities anonymization will provide full data privacy.

Notations used are summarized in Table I.

TABLE I. Notations Summary

Notation	Description
O_i	$Object_i$
GT	Gateway
Mgr	Manager
IDS	Identity Server
Edg	Edge
Cld	Cloud
Fid_i	Fake ID_i
Id_i	ID_i
TS	Timestamp
Y-> Send(X,{Z})	Y Sends parameters Z to X
Y->Construct(X,Z)	Construct Part X With Z and store it in Y.
H(X)	Hashing X
Key	Session key between Object and cloud
O_i ->Enc(P, Key)	Encrypt plain text (P) with Key for O_i
O_i ->Dec(P, Key)	Decrypt cipher text (P) with Key for O_i
Read	Senor Captured Read
CldPubK	Cloud public Key
CldPrK	Cloud private Key
ChkElg	Check Eligibility
CAT(X,Y)	Concatenate X and Y

The proposed protocol consists of six main components as below:

- Object: is denoted by O_i which is responsible for gathering required data and do necessary functionality to it.
- Identity Server generators: is denoted by IDS, responsible for satisfying objects' requests to form fake identities.
- Manager: is denoted by Mgr which is responsible for managing objects lifecycle starting from object registration till data exchange. Each network cluster has its Mgr to do required jobs.

- Edge: is responsible for preparing object requests and adding necessary meta data.
- Gateway: is responsible for verifying eligibility for objects to send data or not and doing necessary functions to send data to cloud.
- Cloud: is responsible for mapping data to correct object identities, storing data and perform required analysis to take needed decisions.

Fig. 1 shows the key components of the proposed protocol.

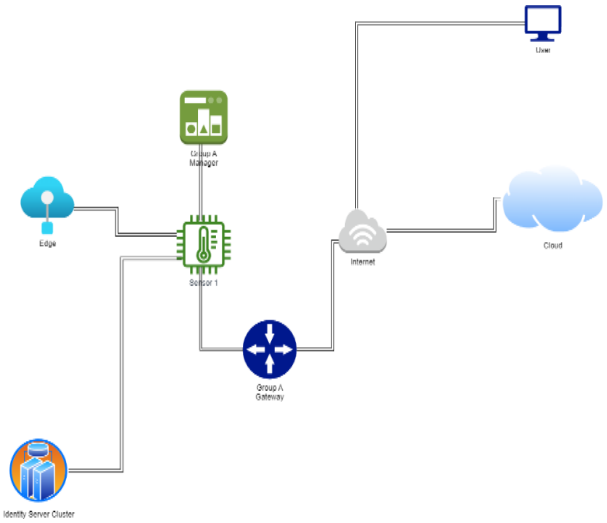

Fig. 1. Proposed Protocol.

The protocol consists of four phases according to below:

1) Registration Phase: Each object (Oi) to be added to IOT network must firstly send to it's Mgr to be registered and approved. Once got approval, Oi starts to request its fake identity to start communicating with.

2) Anonymization Phase: It is responsible for changing real object identity to fake one to resist any tracking attacks or impersonation for any object based on its real identity, as below:

- O_i sends a request with timestamp (T_1) for more than one IDS (n) where n >1 to form its fake identity if it is expired.
- IDS validate timestamp against timestamp threshold (T) via $|T_{IDS} - T_1| < \Delta T$ to determine if the request will be satisfied or rejected.
- Each server receive request generates part of identity uniquely and send it back to O_i with timestamp and expiry date.
- The severs send parts generated to cloud with other information required (server id, object id, timestamp).
- Cld concatenate parts received from servers based on received timestamps ascending, validate timestamp against timestamp threshold (T) via $|T_{cld} - T_i| < \Delta T$, hash the concatenation output to get fake identity, set expiry date for that fake identity based on system configuration and then store mapping for fake identity to real one in mapping tables.
- O_i prepares its fake identity as cloud did, validate timestamp and send it to cluster mgr to update its list.
- Cluster mgr updates its list and broadcast it to GT. Table II shows construction of fake identities.

TABLE II. FAKE IDENTITY GENERATION ALGORITHM

Algorithm 1: Fake Identity Generation by object Oi
1: O_i -> Send(IDS_1, { Id_i ,T_1 }). 2: IDS_1 -> Validate Timestamp if($\|T_{IDS1} - T_1\| > \Delta T$ then rejected 3: IDS_1 -> Send(O_i , { Fid_1‖ T_{s1} }) 4: IDS_1-> Send(Cld, {Fid_1 ‖ IDS_1 ‖ id_i ‖ T_{s1}}) . 5: O_i -> Send(IDS_2, { Id_i ,T_2 }). 6: IDS_2 -> Validate Timestamp if ($\|T_{IDS2} - T_2\| > \Delta T$) then rejected 7: IDS_2 -> Send(O_i , { Fid_2‖ T_{s2} }) 8: IDS_2 -> Send(Cld, {Fid_2 ‖ IDS_2 ‖ Id_i ‖ T_{s2}}) . 9: O_i -> Construct(CAT(Fid_1, Fid_2 , H(id_1, T_{s1}, T_{s2})), T_{f1}) and output Fid to be stored 10: Cld -> Construct(CAT(Fid_1, Fid_2 , H(id_1, T_{s1}, T_{s2}), T_{f1}))) and output Fid to be stored. 11: O_i -> Send(Mgr_i , { id_1 ‖ Fid_1}). 12: Mgr_i -> Update (List, {Fid_1}). 13: Mgr_i -> Send (GT, List).

3) Session Key Generation Phase: It is the phase responsible for constructing session key between object and cloud via lightweight key agreement protocol [26]. This protocol consists of two stages as below:

Registration stage: The object register itself on the cloud through the following:

- O_i chooses identity ID_i and password PW_i then two parameters a and b.
- O_i calculates $Mpw_i = h(PW_i \| a \| b \| ID_i)$, $HID_i = h(ID_i \| b)$ and $d_i = a \oplus b$.
- O_i sends { HID_i , Mpw_i , d_i , a} to Cld.
- Cld then calculates $v_i = h(HID_i \| Mpw_i)$ then chooses random numbers $c_i z_i$.
- Cld calculates both $B_i = h(HID_i \| x_s)$, $E_i = (B_i \oplus Mpw_i)$.
- Cld will store (z_i, HID_i) in its database.
- Cld will calculate $A_i = E_{xs}(c_i \| HID_i \| d \| a)$
- Cld will send { A_i , E_i , z_i , v_i , c_i , b, a}.
- O_i will calculate $T_i = A_i \oplus Mpw_i$
- O_i will store [T_i , E_i , z_i , v_i , c_i , b, a]

- Login and authentication stage: The object successfully logged in to authenticate itself and start information exchange as below:
  - O_i submit its ID_i and PW_i

- O_i calculates $Mpw_i = h(PW_i \| a \| b \| ID_i)$, $HID_i = h(ID_i \| b)$, $v_i = h(HID_i \| Mpw_i)$, $B_i = E_i \oplus Mpw_i$.
- After calculating new v_i , it compares it with old one.
- O_i calculates $d_i = a \oplus b$ and $cd_i = c_i \oplus d_i$.
- O_i chooses random number e_i and selects T_1 .
- O_i then calculates $A_i = T_i \oplus Mpw_i$, $M_i = E_{Bi} (T_1 \| e_i` \| A_i)$.
- O_i sends { cd_i , M_i , T_1 , HID_i } to Cld.
- Cld will select T_2 then check whether $| T_2 - T_1 | < \Delta T$.
- Cld will calculate $B_i = H(HID_i \| X_s \| z_i)$.
- Cld will $DEC(M_i)_{Bi} = (T_1, A_i, e_i)$ and $DEC(A_i)_{Xs} = (HID_i , a, c_i, d_i)$.
- Cld will then calculate $cd_i = c_i \oplus d_i$ and then check if new cd_i equals old one or not and the same for T_1 then chooses random number q_i.
- Cld finally will calculate $Q_i = H(A_i \| B_i)$, $s_i = q_i \oplus B_i$, $w_i = h(cd_i \| e_i)$, $N_i = E_{Ai} (s_i \| T_2 \| w_i)$.
- Cld will send N_i , T_2 back to object.
- O_i will select T_3 and check whether $| T_3 – T_2 | < \Delta T$.
- O_i will $DEC(N_i)_{Ai} = (s_i, T_2 , w_i)$.
- O_i will calculate $w_i` = H(cd_i \| e_i)$ and then checks whether $w_i` = w_i$ and $T_2 = T_2$.
- O_i will calculate $q_i = s_i \oplus B_i$, $Q_i = H(A_i \| B_i)$, $sk = H(e_i \| B_i \| Q_i \| q_i \| z_i \| s_i)$, $M N_i = H(Sk \| q_i \| s_i \| Q_i)$
- O_i will send M N_i and T_3 to cloud to finalize key construction.
- Cld will select T_4 and then checks $| T_3 – T_4 | < \Delta T$ and then calculates $sk = H(e_i \| B_i \| Q_i \| q_i \| z_i \| s_i)$ and M $N_i` = H(Sk \| q_i \| s_i \| Q_i)$ and then checks whether new and old M N_i are equal.

4) Transferring Data to Cloud Phase: It is the phase responsible for transferring data from objects to cloud to be processed and stored as below:

- O_i encrypts current read with lightweight Speck-R algorithm [27] using constructed session key on session key generation phase.
- O_i will send encrypted read with newly generated fake identity to Edg.
- Edg will prepare the request by adding needed meta data (timestamp, edge id, gateway id) to the request
- Edg will encrypt the whole data and metadata with cloud public key and send it to gateway in conjunction with message authentication code [28] to ensure data integrity and resist active attacks.
- GT will verify whether object has right to send data to cloud or not, if yes, the GT will forward data to cloud.
- Cld receives request then decrypts it using its private key and then go through verification in terms of timestamp and message authentication code [28] attached to ensure both data integrity and no reply attack took place.
- Cld will decrypt the data using previously constructed session key with O_i.
- Cld will get mapping for fake identity and check expiry date to validate if it is still used or not to avoid impersonation and identity theft attacks.
- Cld will store data with real identity.

IV. Security Analysis

This section provides a complete security analysis for proposed protocol by formulating threat model and threat model analysis with informal and formal analysis to prove correctness of designed protocol in terms of security and attacks resistance.

A. Threat Model

In IOT environments, integrity and confidentiality are considered critical part to be dealt with as stated in Dolev-Yao adversary [29].

According to proposed protocol, objects, gateways, managers, edges and identity servers are communicated to each other using internal IOT network. Objects before sending any data, must firstly acquire their fake identities to replace their real ones - in order to be protected from impersonation and identity tracking attacks - while sending data. Moreover, all communications to cloud must go through gateway which has ability to forward request or drop it due to any violation. Manager is responsible for managing authorization of objects in terms of sending data even though they got new fake identities. Edge is responsible for adding necessary metadata and providing a second layer of security to data by encrypting whole data by cloud public key to be sent to cloud which in turn fulfill data privacy. All parties (Manager, Gateway, Edge, identity) are assumed to be dishonest which means they are curious about data.

Attackers aim to reveal as much data as possible by trying to gain access to any IOT network party or sniffing communication network itself. Data is not only objects generated reads but its metadata as well due to its importance. Metadata can be used to extract valuable information about data itself (ex. object cluster, Location and object itself in many cases) to attackers which in turn causes data privacy leakage.

Our objective is to minimize the amount of information attackers can gain to protect data privacy through IOT networks via fulfilling confidentiality and integrity of data.

A lot of Assumptions to be considered:

- Attacker has ability to intercept any message between cloud and IOT network.

- Lightweight key agreement protocol [26] for key construction between objects and cloud and Speck-R [27] algorithm are secured.
- Cloud and object themselves are secured.

B. Threat Model Analysis

Recall that from our threat model, our objective is to minimize the amount of information attackers can gain to protect data privacy through IOT networks.

Attacks can be classified in to two main parts:

- Internal attacks which are carried out inside IOT network.
- External attacks which are carried out outside IOT network.

And each part of them can be classified into:

- Active attacks which are considered unauthorized access aim to alter networks data or injecting data other than correct one.
- Passive attacks are considered unauthorized access to gain data without modifying it.

And according to our threat model assumptions, attacks on objects and cloud themselves are out of scope.

C. Informal Analysis:

The proposed protocol aims to fulfill the following:

- Confidentiality: The protocol aims to fulfill confidentiality via end-to-end encryption between object and cloud. Speck-R is used as a first layer encryption to protect data from unauthorized access and eavesdrop in conjunction with light key agreement protocol. Key agreement protocol is used to form encryption key without directly exchanging it which provides more security and prohibit key sniffing attacks. Therefore, any data to be transferred from objects will be in ciphertext form which in turn fulfills Confidentiality.
- Integrity: The protocol aims to fulfill integrity and authenticity of data via message authentication code which in turn resists active attacks. The edge before encrypting metadata will authenticate message by adding message tag to ensure that message is not tampered or altered through communication.
- Anonymization: The protocol aims to protect identity of objects by changing real identities of objects with other ones while sending reads to avoid tracking attacks and impersonation attacks which in turn preserve data privacy.

And the protocol has ability to resist the following:

- Man in the middle attack (MITM): The attacker position himself between two communication parties in order to intercept exchanged messages and modify the content. Even though, the attacker can store the message for a while and resend it later. The proposed protocol has ability to deal with this attack via fulfilling both Confidentiality and integrity by applying both E2E encryption and using message authentication code which in turn helps on defending against MITM attack.
- Eavesdropping and Interference: The attacker aims to eavesdrop on any part of the network to extract any valuable information. The proposed protocol has the ability to resist that by applying E2E encryption between object and cloud and adding a second layer of encryption between edge and cloud for metadata which in turn resists any eavesdropping attacks.
- False Data Injection attack: The attacker tries to inject false data instead of correct one which in turn leads to wrong decision on cloud. The proposed protocol has ability to resist that by firstly apply Anonymization for objects to anonymize objects' identities and register these identities on cloud. Secondly, two level encryption one with the session key using key agreement protocol between cloud and object, other with edge and cloud. Even though the attacker tried to inject a node into the network with the purpose of injecting false data, the gateway will not forward this data to cloud due to being unauthorized from network manager which in turn makes it difficult for any attacker to inject any false data to cloud.
- Advanced Persistent Threat: The attacker tries with many tactics and techniques to infiltrate IOT network and be silent and undetected for a long time with aim to steal and leak valuable information. The protocol has the ability to resist that via achieving Confidentiality and integrity.
- Reply attacks: The attacker tries to intercept network and retransmit a message between communication parties which in turn will lead to wrong timed message received. This wrong message can lead to disasters and wrong decisions due to being received correct at the wrong time. The proposed protocol has ability to resist this type of attack, by taking into consideration timestamp which message came with, if the difference between receivers' timestamp and message timestamp greater than threshold defined on protocol, the request will be rejected.

D. Formal Analysis

The proposed protocol had been verified by scyther tool [30], used to analyze and verify security protocols in terms of vulnerabilities and flaws in their design. According to our protocol implementation on scyther, seven roles are implemented to cover all protocol aspects.

The analysis will be for each protocol phase to make sure that the data and metadata are still protected while being transferred which in turn fulfills protocol goals in terms of data privacy. Fig. 2 states proposed protocol analysis results.

For registration and anonymization phase, the object sends to network manager to be added and approved. The manager checks eligibility for that object request to be approved or rejected. If the request is approved, the object starts to request

its fake identity via identity servers, minimum two servers to be requested as stated in Algorithm 1.

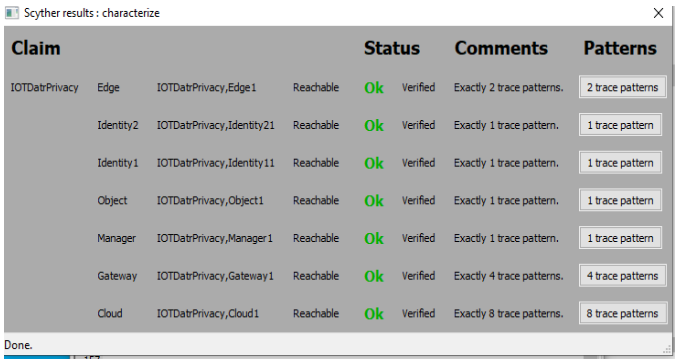

Fig. 2. Scyther tool results.

Once fake identity is got, the objects start to send collected data to cloud. Fig. 3 shows attack trace for registration and anonymization phase, the object is modeled as role Object and manager is modeled as role Manager.

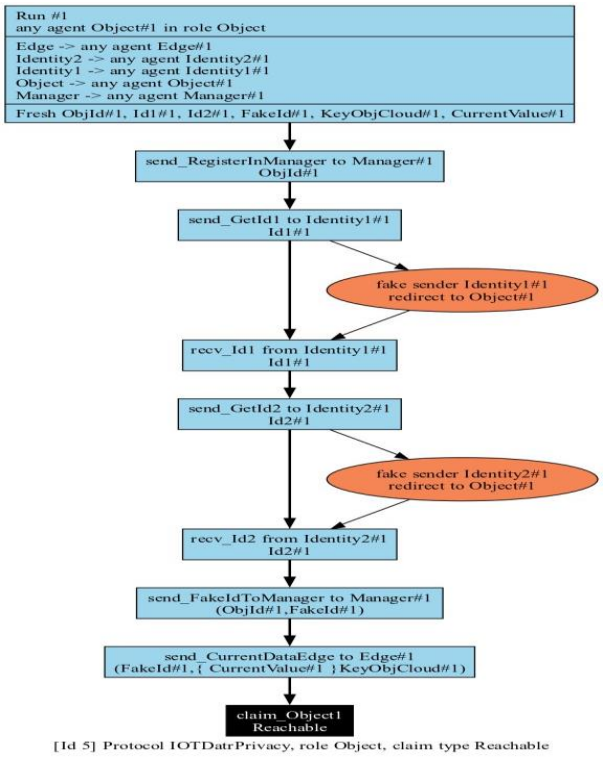

Fig. 3. Registeration and anonymization phase analysis.

For data transfer to cloud phase, this phase provides end to end secured channel between objects and cloud to safely transfer data from objects to cloud. Objects start communication by encrypting needed data by pre-established session key and then send encrypted data to edge with fake identity constructed. The edge will add needed metadata (timestamp, edge id, gateway id) to data received and then encrypt data and metadata with cloud public key and add message authentication code to the request to be verified in order to ensure data integrity. The protocol provides two levels of protection to fulfill data privacy:

- From object to cloud which mainly encrypts data using lightweight Speck-R due to nature of objects as being constrained devices. This level protects data from active/passive attacks.
- From edge to cloud which mainly encrypts previously encrypted data and metadata using public keys for cloud. This is considered a wrapper for the first level which means after encrypting object's data with speck-R, the edge adds necessary metadata and encrypt the whole data which already have encrypted read with public key for cloud which in turn gives more protection level.

The edge will send the whole request to GT to check whether the sent id is on list updated by managers or not. If yes, the request will be sent to cloud to be verified and stored.

V. Evaluation

In this section, a comprehensive evaluation of proposed protocol is presented by comparing it against xiluo [25] protocol. The criteria will be divided into two parts:

1) Strength of protocols to fulfill the following:

- Object Registration: The protocol must have the ability to make sure that no unauthorized object can be added to the network to avoid any injection and impersonation attack.
- Identity Protection: The protocol must have the ability to provide way to protect object identities to avoid impersonation and tracking attacks.
- Key Management: The protocol must have the ability to provide a way of constructing session keys without depending on trusted third parties or physically exchange it to make sure that the key will still be secured until changing it.
- Data Protection Level: The protocol must have the ability to protect data and metadata exposed from objects.
- Confidentiality: The protocol must have the ability to protect transferred data from eavesdropping and sniffing.
- Integrity: The protocol must have the ability to protect transferred data from tampering and modification
- Mutual Authentication: The protocol must have the ability to provide a way for communication parties to authenticate each other before starting communication.

Table III demonstrates the comparison in terms of protocol strength criteria.

TABLE III. COMPARISON BETWEEN XILOU AND PROPOSED PROTOCOL IN TERMS OF STRENGTH OF PROTOCOL

Criteria	XI LUO Protocol [25]	Proposed Protocol	Comment
Object Registration	Depends on Control Center which already had predefined records for objects (ID, Key) then after verification, the join request is accepted or rejected.	Depends mainly on cluster manager which already has a predefined records for objects (ID) then after validation, the join request is accepted or rejected	XI Luo Protocol is more powerful on registration phase since the verification is done through decryption of message using key that is already stored on control center. This operation is done once and may cost additional performance but fulfill more security against injection attacks
Identity Protection	Does not provide identity protection, in communication, it works directly with objects real identity	Provides identity protection via anonymization phase which depends on identity servers to change object real identity to another one	The proposed protocol is more powerful on identity protection. No communication is done unless object changed its real identity to another one to prevent identity tracking and impersonation attacks. The new identity must be frequently changed due to its expiration which in turn provide extra layer of security to prevent eavesdropping and inference attacks. The new identity is communicated to cloud to be able to receive information and correctly map it to correct object.
Key Management	Depends mainly on Control center to create the session key between communication parties. Therefore, in order to create a key between two objects, the first one will send a request to control center to create shared key then control center will back to requester and other party with needed key to start communication.	Depends mainly on lightweight key agreement protocol which aims to establish session key between communication parties only without need for any third parties. The communication parties only have the constructed session keys which provides more protection against key leakage	Proposed protocol employs a powerful key management approach via a lightweight key agreement protocol which ensures perfect secrecy and mutual authentication unlike Xi luo protocol, it depends on control center to provide that via persistent encryption keys stored on control center.
Data protection Level	Focuses mainly on objects' data	Focuses on objects' data and metadata related.	Proposed protocol focuses not only on data but metadata as well due to valuable information that can be revealed from.
Confidentiality	Partially fulfilled. Usage of cryptography to send and receive any message fulfill confidentiality but ability of control center to decrypt any sent message due to have access to all session keys is considered violation.	Fulfilled, being a TTP-Free and relying on End-to-end encryption starting from key construction which relies on lightweight key agreement protocol that is totally constructed between communication parties only then use of lightweight cryptography for any message sent or receive to ensure that no party whether internal or external network can read the message except authorized parties	Proposed protocol is considered more powerful in providing confidentiality. Xi luo protocol depends on key construction totally on control center which gives it ability to read any message sent due to have access to all keys used which in turn considered violation for confidentiality unlike proposed protocol which key construction is totally between communication parties only to forbid unauthorized access to data.
Integrity	Fulfilled via message authentication code used while exchanging messages	Fulfilled via message authentication code used while exchanging messages	Both fulfill integrity to make sure that any tampered message will be detected which in turn resist active attacks.
Mutual Authentication	Does not provided, communication parties does not have ability to securely authenticate each other due to being trusted to control center to authenticate each party before session key construction.	Fulfilled via key agreement protocol. Key agreement protocol aims to establish a session key between communication parties to securely exchange messages between each other. The first stage of adopted protocol is mutual authentication to make sure that each party authenticated each other before starting session key construction.	This is one of most critical part to be considered. Proposed protocol gives ability to communication parties to mutually authenticate each other before starting communication to resist any impersonate attacks and make sure that no one pretends to be other which in turn constitutes to confidentiality indirectly.

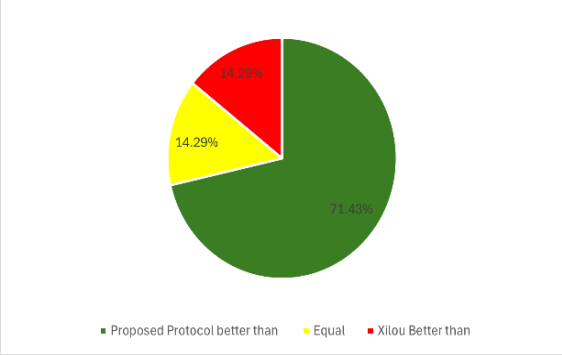

Fig. 4. Evaluation of proposed protocol in terms of protocol strength.

Although Xi Lou protocol tried to fulfill data privacy, it mainly depends on control center as a trusted third party to fulfill key exchange and object registration which in turn is considered security concern. If any attacker gain access to the control center, he will have access to all security keys for all individual objects and shared keys between objects. Fig. 4 summarizes results in terms of percentages with percentage of superiority of proposed protocol over XiLuo's one.

2) Attacks can resist which are the following:

- Man In the middle.
- Eavesdropping and Interference

- False Data Injection attack.
- Advanced Persistent Threat
- Active attacks.
- Reply attacks
- Tracking attacks.

Table IV demonstrates the comparison in terms of stated attacks.

Therefore, the proposed protocol has the ability to fully resist mentioned attacks and provide full data privacy. Fig. 5 summarizes the attacks resistance in terms of fully, partially and not resistant.

TABLE IV. COMPARISON BETWEEN XILOU AND PROPOSED PROTOCOL IN TERMS OF ATTACKS RESISTANCE

Attacks	XI LUO Protocol [25]	Proposed Protocol	Comment
Man in the middle attack (MiM)	Partially Protected	Fully Protected	For Xi lou protocol: dependency on control center as a trusted third party which makes the whole system vulnerable to MiM attack if attacker gain access to that. Proposed Protocol: provides end-to-end protection without relying on trusted third party. Objects try to establish their key via lightweight key agreement protocol instead of direct exchanging them which in turn provides fully protection against MiM.
Eavesdropping and Interference	Fully Protected	Fully Protected	Traffic on network is always encrypted which provide protection against Eavesdropping and inference
False Data Injection attack	Fully Protected	Fully Protected	Xi lou and proposed protocol fulfill protection against false data injection via encryption decryption used so no one can inject any data unless have a valid key on network. For Proposed Protocol: The protocol capable of resisting injection attacks by relying on end-to-end encryption which oblige all communication parties to establish session key before communication which ensures mutual authentication for communication parties. On the other side, on both protocols, registration phase works effectively against that attack as non-node can be injected on network without having a key registered already on control center in case of xi lou or have cluster manager approval in case of proposed protocol.
Advanced Persistent Threat	Partially Protected	Fully Protected	For Xi lou protocol: if attacker gain access to control center, attacker can be silent and has ability to extract all session keys constructed inside control center between communication parties. Proposed Protocol: it provides end to end security so gaining access to any part of network and stay silent will not reveal any information to attacker.
Active attacks	Fully Protected	Fully Protected	All messages sent are equipped with message authentication codes to resist any tampering to messages sent which in turn protect data from active attacks
Reply attacks	Fully Protected	Fully Protected	All messages sent are equipped with timestamps, these timestamps are validated against receiving party to make sure that no reply attack has been carried out.
Tracking attacks	Not protected	Fully Protected	For Xi lou protocol: the protocol deals with objects using their real identities without any masking or anonymization which in turn enables attacker to track any object inside network. Proposed Protocol: it provides anonymization for objects identities by replacing real object identities with fake one via identity servers which in turn change periodically object identities while data transfer which forbid and avoid any tracking attacks.

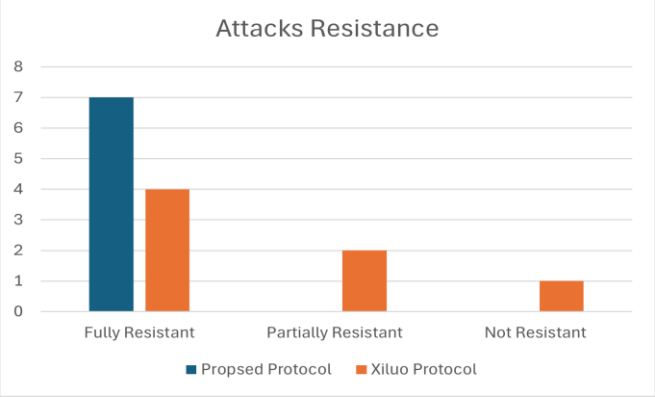

Fig. 5. Evaluation of proposed protocol in terms of attacks resistance.

VI. CONCLUSION

In this paper, a lightweight TTP-Free privacy preservation protocol is presented in order to provide complete data privacy via end to end protection for data and metadata while being transferred to cloud. The protocol depends on providing end to end encryption with a powerful lightweight key agreement protocol to fulfill full data privacy. The proposed protocol was analyzed using scyther tool to guarantee that no vulnerabilities are found. Furthermore, it was evaluated against others protocol in terms of protocol design criteria and attacks resistance. The results showed that the proposed protocol is well designed against the mentioned criteria and surpasses to other protocol by five out of seven which represents 71.4% of overall criteria and equalized in one criteria which is represented by 14.3% which makes the proposed protocol overall fulfillment is 85.7%

against 28.6% for others protocol. Moreover, the proposed protocol has ability to fully resist mentioned attacks which in turn makes it more suitable to fulfill data privacy objective.

In the future work, the proposed protocol will be extended to fulfill device to device (D2D) data privacy to affirm that all communications whether D2D or D2C are protected.

REFERENCES

[1] Atzori, Luigi, Antonio Iera, and Giacomo Morabito. "The internet of things: A survey." Computer networks 54.15 (2010): 2787-2805.

[2] INFSO, D. "Networked Enterprise & RFID INFSO G. 2 Micro & Nanosystems." Co-operation with the Working Group RFID of the ETP EPOSS, Internet of Things in (2020).

[3] Naresh, Vankamamidi Srinivasa, et al. "Internet of Things in Healthcare: Architecture, Applications, Challenges, and Solutions." Comput. Syst. Sci. Eng. 35.6 (2020): 411-421.

[4] Kadhim, Kadhim Takleef, et al. "An Overview of Patient's Health Status Monitoring System Based on Internet of Things (IoT)." Wireless Personal Communications 114.3 (2020).

[5] Sangeethalakshmi, K., U. Preethi, and S. Pavithra. "Patient health monitoring system using IoT." *Materials Today: Proceedings* 80 (2023): 2228-2231.

[6] Kumar, Mohit, et al. "Healthcare Internet of Things (H-IoT): Current Trends, Future Prospects, Applications, Challenges, and Security Issues." *Electronics* 12.9 (2023): 2050.

[7] Onasanya, Adeniyi, and Maher Elshakankiri. "Smart integrated IoT healthcare system for cancer care." *Wireless Networks* 27 (2021): 4297-4312.

[8] Onasanya, Adeniyi, and Maher Elshakankiri. "Secured cancer care and cloud services in IoT/WSN based medical systems." Smart Grid and Internet of Things: Second EAI International Conference, SGIoT 2018, Niagara Falls, ON, Canada, July 11, 2018, Proceedings 2. Springer International Publishing, 2019.

[9] Singh, Ravi Pratap, et al. "Internet of things (IoT) applications to fight against COVID-19 pandemic." *Diabetes & Metabolic Syndrome: Clinical Research & Reviews* 14.4 (2020): 521-524.

[10] Bhardwaj, Vaneeta, Rajat Joshi, and Anshu Mli Gaur. "IoT-based smart health monitoring system for COVID-19." *SN Computer Science* 3.2 (2022): 137.

[11] Ruan, Junhu, et al. "Agriculture IoT: Emerging trends, cooperation networks, and outlook." *IEEE Wireless Communications* 26.6 (2019): 56-63.

[12] Kitpo, Nuttakarn, et al. "Internet of things for greenhouse monitoring system using deep learning and bot notification services." 2019 IEEE International Conference on Consumer Electronics (ICCE). IEEE, 2019.

[13] Santhosh, N., M. Srinivsan, and K. Ragupathy. "Internet of Things (IoT) in smart manufacturing." *IOP Conference Series: Materials Science and Engineering*. Vol. 764. No. 1. IOP Publishing, 2020.

[14] Serror, Martin, et al. "Challenges and opportunities in securing the industrial internet of things." IEEE Transactions on Industrial Informatics 17.5 (2020): 2985-2996.

[15] Onesimu, J. Andrew, J. Karthikeyan, and Yuichi Sei. "An efficient clustering-based anonymization scheme for privacy-preserving data collection in IoT based healthcare services." *Peer-to-Peer Networking and Applications* 14 (2021): 1629-1649.

[16] Zhen, X. U. E., and L. I. U. Xingyue. "Providing a Framework for Security Management in Internet of Things." International Journal of Advanced Computer Science and Applications 13.11 (2022).

[17] Javaid, Uzair, Muhammad Naveed Aman, and Biplab Sikdar. "Blockpro: Blockchain based data provenance and integrity for secure iot environments." *Proceedings of the 1st Workshop on Blockchain-enabled Networked Sensor Systems*. 2018.

[18] Alzoubi, Yehia Ibrahim, et al. "Internet of things and blockchain integration: security, privacy, technical, and design challenges." *Future Internet* 14.7 (2022): 216.

[19] Othman, Soufiene Ben, et al. "Privacy-preserving aware data aggregation for IoT-based healthcare with green computing technologies." *Computers and Electrical Engineering* 101 (2022): 108025.

[20] Jayaraman, Prem Prakash, et al. "Privacy preserving Internet of Things: From privacy techniques to a blueprint architecture and efficient implementation." Future Generation Computer Systems 76 (2017): 540-549.

[21] Soldatos, John, et al. "Openiot: Open source internet-of-things in the cloud." Interoperability and Open-Source Solutions for the Internet of Things: International Workshop, FP7 OpenIoT Project, Held in Conjunction with SoftCOM 2014, Split, Croatia, September 18, 2014, Invited Papers. Springer International Publishing, 2015.

[22] Abu-Tair, Mamun, et al. "Towards secure and privacy-preserving IoT enabled smart home: architecture and experimental study." *Sensors* 20.21 (2020): 6131

[23] Li, Shancang, et al. "Lightweight privacy-preserving scheme using homomorphic encryption in industrial Internet of Things." *IEEE Internet of Things Journal* 9.16 (2021): 14542-14550.

[24] Ahmed, Mohammed Imtyaz, and Govindaraj Kannan. "Secure and lightweight privacy preserving Internet of things integration for remote patient monitoring." *Journal of King Saud University-Computer and Information Sciences* 34.9 (2022): 6895-6908.

[25] Luo, Xi, et al. "A lightweight privacy-preserving communication protocol for heterogeneous IoT environment." IEEE Access 8 (2020): 67192-67204.

[26] Soni, Mukesh, and Dileep Kumar Singh. "LAKA: lightweight authentication and key agreement protocol for internet of things based wireless body area network." Wireless personal communications 127.2 (2022): 1067-1084.

[27] Sleem, Lama, and Raphael Couturier. "Speck-R: An ultra light-weight cryptographic scheme for Internet of Things." *Multimedia Tools and Applications* 80 (2021): 17067-17102.

[28] Van, Dang Hai, and Nguyen Dinh Thuc. "A privacy preserving message authentication code." IT Convergence and Security (ICITCS), 2015 5th International Conference on. IEEE, 2015.

[29] Herzog, Jonathan. "A computational interpretation of Dolev–Yao adversaries." *Theoretical Computer Science* 340.1 (2005): 57-81.

[30] Cremers, Cas JF. "Unbounded verification, falsification, and characterization of security protocols by pattern refinement." *Proceedings of the 15th ACM conference on Computer and communications security*. 2008.