Wireless Personal Communications
https://doi.org/10.1007/s11277-023-10708-6

Exploring the Challenges and Tensions of Privacy Using Internet of Things (IoT) and Cloud Technologies

Abdulaziz R. Alamro[1] · **Usama M. Ibrahem**[2,4] · **Talal M. Alsaif**[3]

Accepted: 11 August 2023

Abstract
The Internet of Things (IoT) is a global system of networked physical devices that will play a significant part in the next generation of the web (FI). More than 50 billion gadgets are predicted to be linked to the internet by 2023. As a result, a large number of Apps and services will be necessary to make these items readable, identifiable, locatable, accessible, and/or controlled through the web. Trust in the IoT security architecture is crucial for the IoT to be extensively accepted by both consumers and businesses. It is crucial to specify how data may be sent and received between devices in the IoT in a safe and reliable manner. We begin by developing a mechanism for establishing group keys, which will allow for secure multicast group communication in the Internet of Things. The second security aspect of our work is the design of a lightweight biometric user anonymity-preserving authentication protocol. "The third security aspect of our work is a technique for preserving the Source Location privacy. Improvements in accessibility are being made possible by the Internet of Things and the data it generates, in areas as diverse as smart homes and autonomous vehicles." As a result, Internet of Things gadgets and services are helping individuals with impairments become more independent and engaged in their daily lives.

Keywords Internet of Things (IoT) · Disabilities · Privacy tension

1 Introduction

This document grew out of a series of conversations with industry experts in 2017 and 2018, including two convening's co-hosted by the Future of Privacy Forum (FPF) and the American Association of People with Disabilities (AAPD) Technology Forum with

✉ Abdulaziz R. Alamro
DR.ALAMR@uoh.edu.sa

[1] Curriculum and Instruction, Faculty of Education, University of Ha'il, Ha'il, Kingdom of Saudi Arabia

[2] Applied College, University of Ha'il, Ha'il, Kingdom of Saudi Arabia

[3] College of Business Administration, Management & MIS Department, University of Ha'il, Ha'il, Kingdom of Saudi Arabia

[4] Faculty of Education, Suez Canal University, Ismailia, Egypt

Published online: 09 October 2023

funding from the Comcast Innovation Fund. “In order to discuss the potential benefits of the Internet of Things (IoT) for people with disabilities, as well as the data that may be generated and used by these devices and services, and the privacy challenges that may result, a number of industry professionals, consumer organisations, disability advocates, and other thought leaders have gathered for these discussions.”

People with disabilities stand to gain from the IoT, but there may be privacy issues that arise as a result. “Early discussion and action may help reduce the severity of these problems. We can gain a better understanding of the unique privacy considerations and tensions that people with disabilities may face when using IoT devices and services if we look at the issue through the lens of the Fair Information Practice Principles (FIPPs), which range from transparency, individual control, respect for context, focused collection, and security.” To better understand how persons with disabilities may be impacted by Internet of Things (IoT) devices and services, it is helpful to examine the FIPPs in this context, even if they apply to all users.

The exponential rise of Internet-enabled devices, from the simplest sensors to the most complex cloud servers, defines the Internet of Things. "Things in the context of the Internet of Things may refer to either electronic or non-electronic things. All items in the IoT have a common characteristic in that they may communicate with one another and other devices through the web. By enabling remote object control through pre-existing network infrastructure, network connection facilitates greater integration with the physical environment while reducing the need for human interaction. By using technologies like ubiquitous computing, communication capacities, Internet protocols, and apps, the IoT upgrades inanimate items from dumb to smart.” Adding intelligence and accessibility to everyday objects via the use of sensors, electronics, and connections has improved people’s lives by providing greater ease of use, safety, security, and resource conservation [3].

“The Internet of Things (IoT) crept up on us over the past decade, thanks to developments in wireless communication, embedded systems, and energy-efficient radio technologies that made it possible for tiny devices to react to and monitor their environments, thereby shaping a new networking paradigm able to act upon physical objects. Connecting “Anything” to “Anywhere” and "Anytime" allows the third dimension of the Internet of Things vision, which will lead to the development of new applications and services that will affect our ecological, medical, financial, and social well-being [4].”

Connecting everyday objects to the internet has the potential to revolutionise how we live and work. “Some of the many possible uses for the Internet of Things are: smart cities, health monitoring, home automation, smart transportation, smart agriculture, and smart grids. CISCO predicts that by 2020, there will be 50 billion Internet of Things (IoT) devices in use. It is because of this enormous potential that IoT is often heralded as the next wave of the Internet. The broad use of IoT technology and applications depends on their inherent security. Large-scale adoption of Internet of Things solutions is very improbable in the absence of assurances of privacy, authenticity, and secrecy at the system level. The heterogeneity of the IoT and the fact that the vast majority of IoT devices are resource-constrained when coupled with the robust nature of the Internet make it difficult to enable fully secure interactions between IoT entities.” Organizational and academic researchers continue to focus on security in the IoT [5].

It is based on the 3-layer design and uses components to organise the system. “The application layer is the topmost layer, followed by the service layer, the network layer, and the perception (or sensing) layer. Developing and maintaining services that end users and other programmes depend on falls within the purview of the Service layer. Service interfaces, service administration, service composition, and service discovery are all parts of the service layer. Here, service composition is used to interact with connected objects and divide or integrate services to efficiently meet service requests, service management is used to manage and determine trust mechanisms to meet service requests, and service interfaces are used to support interactions among all provided services [6].”

There are several technologies that are involved in IoT emergence. They are considered the main building blocks for the IoT existence today. Technologies for identification, localization, sensing, and provide IP addresses for the expected huge number of devices, and also technologies for enabling the small devices to communicate with other entities on the internet. In this section, we highlight some of the key enabling technologies for IoT [7].

“Although WSNs have advanced greatly in recent years, its basic component remains the same the sensor nodes that collect, analyse, and disseminate the data they collect (communicate with other entities using a wireless channel). Things with these sensor nodes installed in them may collect data about their surroundings, including temperature, motion, and other factors.” accordingly based on this information proper action can be taken, hence sensor nodes can make thing aware of their surroundings [8].

Integrating IoT technologies with medical devices help constant remote monitoring for patients and elderly people. Nevertheless, unauthorized access to an IoT health device may cause threatening to a person life for example in 2016 a successful hack on continuous glucose monitoring system (CGM) which cause a change to the insulin level given by the CGM, in such attack it may cause immediate death to the patient hence, attacks on IoT device go beyond information hacking it has a direct harm to human’s lives. Moreover, health reports given by the smart healthcare devices are considered highly personal and sensitive; any information leakage is a violation of individual privacy [9].

Standards for ensuring the safety of the Internet of Things are unique. The Internet of Things (IoT) links vast networks of heterogeneous smart devices, with an estimated number of linked devices in the billions, creating massive amounts of data and giving rise to new types of difficulties. Most IoT devices also have limited computing performance, tiny memory capacity, and restricted power supply, all of which prevent the implementation of conventional security measures [10]. This study is arranged as follows: in Sect. 2, a description of the literature review; in Sect. 3, a description of the research technique; in Sect. 4, an analysis of the results and discussion; and in Sect. 5, a description of the final conclusion and future work.

2 Literature Review

Literature review with respect to the study of Exploring the Benefits, Challenges and Privacy Tensions using Internet of Things (IoT) and People with Disabilities.

However, the protocol is designed for highly dynamic environments like vehicular networks, where the number of joining/leaving nodes is high, so a key distribution center (KDC) is used to handle the key distribution to the multicast group legitimate members in Catarinucci et al. [11] Proposed batch-based group key management protocol applied to the Internet of things.

The methodology is time-driven and relies on false predictions about when members would leave the organization, as shown by the author in Elijah et al. [12]. Additionally, the protocol is vulnerable to reply attacks, and the author does not provide a mechanism for authenticating group members.

A centralized group key establishment protocol using ECC was developed in smart home energy systems [13]. This protocol relies on a certificate authority (CA) to generate a public and private key pair for each node in the network. This approach uses a public key operation, which is computationally intensive.

Data security and patient privacy are issues that have received some attention; see, for example, [14]. This paper proposes a Key Management Protocol for usage in Body Area Networks, where sensors are implanted or worn by a patient, and where ECC and Hash functions are used for authentication and key creation. Even with the use of ECC to reduce computational and communication overheads, the protocol is vulnerable to reply attacks because it treats all sensors in a patient as a group and the patient controller (PC) controls key generation using the shared secret key already computed between the PC and each sensor.

A group key for networked smart objects was presented in Sha et al. [15]. The scheme is based on a global key generated through a cooperative effort by network nodes; however, it is a tree-based Key Management System (KMS) in which the key generation process is maintained in a bottom-up fashion, starting at the leaf node and working its way up to the tree's root. The author employs symmetric encryption, with each node having a pair-wise key shared with the base station to authenticate the global key distribution.

In Abdmeziem et al. [16] presented a continuous multicast authentication based on specific time intervals the scheme uses the secret sharing technique for the multicast group key distribution each member of the group holds a share.

In Naoui et al. [17] proposed a network deployment, entities run a distributed key generation protocol to generate session private/public keys for each entity in the network. These keys will be used in securing the communication between entities in the IoT network. Due to the use of polynomials, point multiplication, and point addition the scheme poses heavy computational and communication costs which consequently affect the energy consumed by the constrained- device.

Protocol1 in the proposed Group Key Establishment for Enabling Secure Multicast Communication in WSN for IoT Applications [18] used ECC, an improved version of as the author claims the protocol in Matsumoto [19] is susceptible to man in the middle attack and needs some enhancements to ensure data integrity and authenticity.

Conventional methods of identity verification use a shared secret key, as described by the symmetric authentication procedures in Bamasag and Toumi [20]. It just only a few moments to complete and can be run on a memory constrained microcontroller with less than 1 KB of ram, making it a good choice for embedded systems.

A novel authentication approach for hierarchical WSNs that allows for the insertion of nodes on the fly was presented in Dahshan [21]. This scheme is deemed lightweight since it makes use of simple cryptographic building blocks.

An ECC-based user authentication technique was presented in Porambage et al. [22], however it has significant computing requirements and is vulnerable to security flaws.

User identification and access control for IoT was suggested in Challa et al. [23]. Role-based access control is used in this approach.

Author [24] argues that the protocol of is problematic, and suggests improved protocols to address its shortcomings.

Xue et al. approach's was shown to be vulnerable to attacks like stolen-verifier attacks and off-line password guessing attacks in Amin and Biswas [25].

With the Internet of Things (IoT) in mind, [26] presented a minimal authentication mechanism for distributed wireless sensor networks (WSN). The paper's author claims his system is the first to offer an Internet of Things architecture in which distant users may bypass the gateway and communicate directly with the sensor node. The method was shown to be computationally efficient, as well as less resource- and memory-intensive.

Off-line password guessing attacks, as well as impersonation attacks on users and sensor nodes, were shown to be possible in Amin et al. [27].

A user authentication and key agreement technique in multi-gateway based on WSN was presented in Arasteh et al. [28], despite claims that the scheme is not energy efficient.

Some security flaws were discovered in Abbas et al. [29], including guessing passwords offline and man-in-the-middle attacks. After that, they suggested a better user authentication and key agreement technique for heterogeneous WSN to support the IoT idea.

As shown in Alhayani et al. [30], the method is not safe since it may be exploited via stolen-smartcard attacks, off-line password-guessing attacks, user-impersonation attacks, and because it does not protect users' anonymity.

The authors of Alomari et al. [31] argue that the security of the method provided in Sabri and Alhayani [32] is compromised by its susceptibility to Replay attacks and Denial-of-Service attacks, and they offer a more robust protocol to address these concerns.

To formally define the source location issue in sensor networks, the author of Alhayani et al. [33] proposed the Panda-Hunter model, which uses a directed random walk in which each node divides its neighbours into two sets according to their positions. If the source node randomly chooses a neighbour from the set to its left, the next neighbour will choose a neighbour from the set to its right, and so on (the sink node).

Phantom routing was suggested to increase source location anonymity in Bonino et al. [34]. When the source sends out a message, the message is uncased randomly for a total of h hops before it reaches the destination node. This is the first stage of phantom routing, in which a random walk is used to direct the packet to a phantom source. The second stage employs a different technique, in which the packet is routed to the destination node via single-path routing.

GROW is a two-way greedy random-walk algorithm developed in Buyya and Dastjerdi [35]. (Greedy Random Walk). A random walk is used here, and it comes from both the source and the sink. N-hop random walk is started by the sink, followed by M-hop random walk from the source. When a packet from the source reaches a node where these two pathways meet, the sink's path is used to send it on its way. Using local broadcasting, we can find the point where the two roads meet, cutting down on the need for any unnecessary backtracking during the random walk.

In Kumar et al. [36] whenever a source node delivers a packet to the sink, another node serves as a faked source node and transmits another packet attempting to mislead the adversary to discover the true source node.

3 Research Methodology

The Internet of Things (IoT) has the potential to revolutionise society and business, as well as the lives of people with disabilities. "Accessibility to Internet of Things (IoT) gadgets and services is on the rise in the modern day [36], with some IoT solutions being developed with people with disabilities in mind and others being repurposed by such people (see Fig. 1). Smart home technology and autonomous vehicles are just two examples of how the Internet of Things and the data it generates are improving accessibility [37]. By eliminating the need for certain types of human intermediates or adjustments, IoT-based services are also allowing people with disabilities to take an

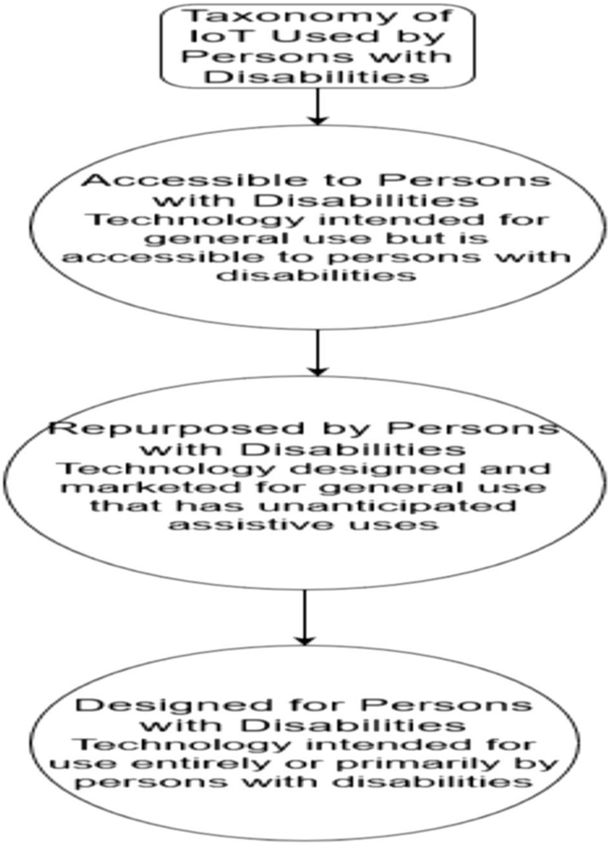
Taxonomy of IoT Used by Persons with Disabilities
Accessible to Persons with Disabilities Technology intended for general use but is accessible to persons with disabilities
Repurposed by Persons with Disabilities Technology designed and marketed for general use that has unanticipated assistive uses
Designed for Persons with Disabilities Technology intended for use entirely or primarily by persons with disabilities

Fig. 1 Architecture of Taxonomy of Internet of Things (IoT) Used by Persons with Disabilities

active role in daily life [38, 39]. Insights into the difficulties or advantages that people with disabilities face while utilising IoT devices may be gained by analysing the data generated by their usage of these tools." These learning's may be used into future or improved IoT product designs.

The collection, usage, and sharing of data on users may present particular privacy risks and problems, even while IoT devices and services may have advantages for people with disabilities. There is a dichotomy between the ways in which technology may either increase or decrease privacy, depending on the context [40]. Contextual factors, such as how the service or gadget is used, who is utilising it, and the tastes and values of the users themselves, all influence how people strike that balance. There may be differences in how people with disabilities weigh the potential advantages and privacy dangers of certain technologies. More nuanced thought and participation is necessary in assessing whether or not the benefits of using Internet of Things (IoT) devices and services for people with disabilities outweigh the hazards associated with data collecting.

In a forthcoming paper, we hope to do the following: identify a taxonomy of IoT devices and services used by people with disabilities; describe the benefits the IoT can offer to people with disabilities, communities, and businesses; and explore the privacy challenges faced by people with disabilities who use IoT services.

3.1 Smart Home Devices

“The same benefits that non-disabled people enjoy when using smart home gadgets also provide disabled people more freedom to do things on their own terms. For those who are blind or have mobility issues, the ability to use a Smart Home assistant to manage things like lighting, temperature, and security may be a game changer.

Problems with Privacy: Some people with disabilities may be left out in the cold when transparency procedures like notice and consent are only made available in a single mode of communication. It’s possible that discriminatory ends might be served by misusing data.

Methods for Limiting Damage: To accommodate the wide range of demands within the disability population, it is important to provide notice and permission of data collection by a number of visual, aural, or tactile signals.”

3.2 Wearable’s and Tracking Devices

“Advantages: Wearable’s and other monitoring technologies allow for more user data collecting, which may help bridge the "data barrier" for people with disabilities in important ways. To lessen social and economic disparities, better information might influence legislation and resource allocation.

Problems with Privacy The disclosure and usage of IoT data may accidentally expose private information about people with impairments, which may then lead to prejudice or stereotyping.

As a mitigation strategy, it’s important to think about the range of possible sensitivity levels associated with IoT and to acknowledge the different privacy expectations users may have.”

3.3 Communications Technologies

“Text-to-speech programmes and teletypewriters are two examples of communication technology that may help people with disabilities gain autonomy and privacy by eliminating the need for a human translator in their interactions.

Problems with Privacy New Internet of Things (IoT) devices and services may be developed to replace or supplement existing ones, but they may not adhere to the same levels of privacy and security as the ones provided by conventional service providers.

Methods for Limiting Damage: It is important to include existing privacy protections into the design of assistive technologies when they are used to supplement and replace existing systems and services utilised by people with disabilities.”

3.4 Facial Recognition Technologies

“Facial recognition technology has the potential to greatly improve the lives of people with disabilities by facilitating communication and access to public settings. Disabled individuals may be made aware of surrounding people and picture subjects using these technologies.

Problems with Privacy: Third-party notification and opt-out methods might be challenging to establish. Recording and storing facial recognition data, capturing it in private or sensitive locations, or using it without people' knowledge or agreement raises serious privacy problems [41, 42]. Access to this information by law enforcement or its usage in a manner that violates individuals' right to privacy are additional potential sources of unease.

Strategies for Mitigation: Use Different Levels of Consent (Opt-in vs. Opt-out) Based on the Interaction Context and the User's Existing Positive Connection to the Subject of Facial Recognition."

3.5 Cloud Technologies

"Advantages Users with disabilities may save their preferred settings for various devices and applications in the cloud, ensuring that they always have access to the information and applications that best suit their requirements.

Problems With Privacy: Denial of service attacks, data breaches, and data loss are all threats that may affect cloud-based infrastructure [43]. To add insult to injury, cloud data is not as well protected from mandatory disclosure as on-premises information.

Methods for Limiting Damage: Use safe data communication methods and a thorough cloud data security programme to reduce the risk of sensitive information falling into the wrong hands."

3.6 Proposed Group Key Establishment Protocol

Smart agriculture is one of the application areas that IoT targets, in our network model of the smart watering system, for best utilization of water; the environmental monitoring unit collects data about soil moisture and temperature and delivers aggregated data to the gateway. Based on data received, the gateway can give commands to open/ close water flow to a group of the smart watering devices in a specific area of the farm. Model is presented in Fig. 2.

As the name implies, the network model relies on connections between nodes of varying capacities, both computationally and in terms of available energy. In a network, there are three basic categories of nodes to consider.

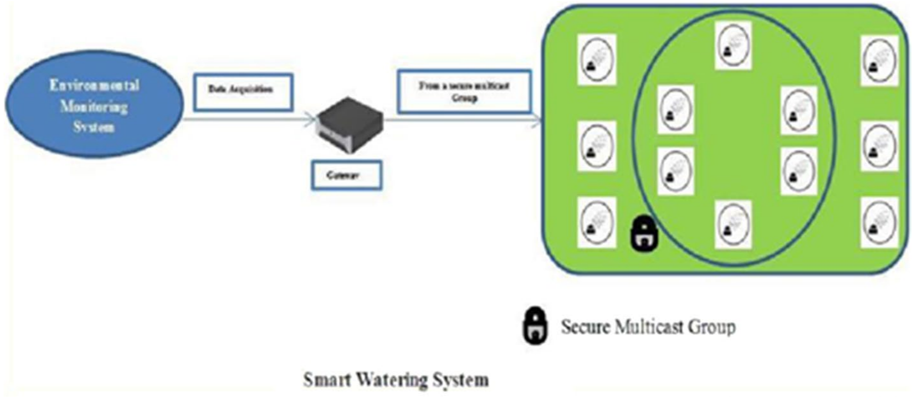

Fig. 2 Multicast group members of the smart watering system

1. Powerful node such as the gateway. It has a powerful computing capability and stable constant energy, belonging to the same structure of the network.
2. Proxy node is a less-constrained node able to implement cryptographic operations instead of neighbouring highly-constrained group nodes in the network it may have harvest energy capability.
3. Highly-constrained nodes not able to implement heavy cryptographic computations of the key exchange process such as sensor nodes.

In the proposed protocol base on our network model wherein one-to-many communication is required we propose an efficient multicast group key establishment scheme for IoT. The scheme consists of three phases. The first phase, pre-deployment phase in which the gateway, proxy, other constrained nodes in the network are configured the second phase, the group long-term secret key shares generation and distribution and the third phase, the Session key generation phase. The notations used in the protocol design are list below in Table 1.

In this stage, we start by setting up the devices used within the network, before deploying them a certain configuration have to be embedded to them. The field has a powerful device called the gateway (GWN) and less constrained nodes called the proxies (P) and other constrained sensor nodes (NJ). In this phase, the system administrator (SA) configures the network devices in offline mode as follows:

SA generates a unique identity Idi for each node in the network, where $\{1 \leq i \leq z\}$ and a randomly-generated secure password-key Xn uniquely for each node that is shared with the GWN. The value z represents the number of devices within the network. The values Idi and Xn will be stored in the corresponding node tamper-proof memory. Then SA also embeds the previous values (Idi, Xn) to the GWN memory. It should be noted GWN is more resource-rich having much more memory space and hence can store all the identities Idi and password-keys Xn of each device in the network.

When generating secret S, the gateway, which is a trustworthy and powerful node in the network, is used. Each node in the network will have a copy of the secret S, which has

Table 1 List of notations

Symbol	Description
GWN	Gateway
NJ	Constrained nodes
P	Proxy
n	Group members including the proxy
Idi	Unique identity for sensor nodes in the group n
IDg	The identity of the gateway
Xn	Unique Pre-Shared password between each member in (n) and the GWN
R	password between NJ-P to retrieve the SK
ci	Share stored in n
di	Metadata of ci (the number of „1‟ bits in si)
m	number of secret blocks
bi	secret block ($i \in \{0,\ldots,m-1\}$)
$\lvert b \rvert$	bit-size of a secret block ($\lvert b \rvert =$)
SK	Session key to encrypt communication between GWN and n
Ti	Timestamp used throughout the Scheme

been partitioned into m equal blocks, with each share consisting of a coded block ci and its metadata di for I in the range [0, n – 1]. The method 3.1 requires the secret S, the share count n, and the block count m as inputs. How the algorithm works is as follows:

Algorithm: 1 *Shares Generation*

```
“Input: m, n, S
Output: (c0, d0), (c n−1, d n−1)
$S = b0 \,||\, ... \,||\, b\ m-1$
$|b| = |S|/m$
$i \leftarrow 0$
for $j \leftarrow 0$ to $m - 3$ do
for $t \leftarrow j + 1$ to $m - 2$ do
for $z \leftarrow t + 1$ to $m - 1$ do
    $si \leftarrow bj \oplus bt \oplus bz$
    $di \leftarrow$ number of „1" bits in si
    $(ci, di) \leftarrow$ SWC. Encode (si, di)
    $i = i + 1$
    if ($i == n - 1$) then
    return (c0, d0), ..., (c n−1, d n−1)
end if
end for
end for
end for”
```

4 Results and Discussion

The communication costs depend on the length of the messages sent and received the smaller the message length the lower the communication cost. We conducted a comparison study for the resource-constrained nodes. The total communication cost of messages transmitted and received incurred by the resource-constrained nodes for session key establishment for the proposed scheme is 660 bytes wherein P. As a result, our protocol achieves the best optimization in network bandwidth and energy consumption among other schemes as shown in Fig. 3.

The key share pair (ci, di) represent the index of the share not the key itself hence, the size of ci = 5 bits and di = 6 bits where ci is $\log_2$ (32) = 5 and di represented by maximum of „1‟bits in a share, however, the storage cost is calculated according to the number of bytes stored in a node. The storage overhead of each node in our protocol is 53 bytes only which show that our protocol has the minimum storage cost among other protocols as shown in Fig. 4

Standard Crossbow TelosB sensor nodes are used for the calculation of energy costs; these nodes include a 4 MHz MSP430 micro processor, are IEEE 802.15.4 compliant, and can transmit data at 250 kbps. The proposed scheme consumed the lowest energy among other schemes as shown in Fig. 5.

"Analysis of the cost of storing data on sensors and smart phones reveals that the majority of the protocols shown in Fig. 6 have similar storage requirements for smart phones. We measured the cost of sensor storage during the time when the sensor was storing the most data (the moment of peak) and found that, contrary to the norm of 128,000 bits per sensor, the suggested protocol only requires a storage capacity of 256 bits see Fig. 7."

IoT and other constrained networks such as WSN use communication medium with small range and low bandwidth to meet the needs of their devices and to maintain low energy. IEEE and IETF shared the responsibility of standardizing technologies for IoT.

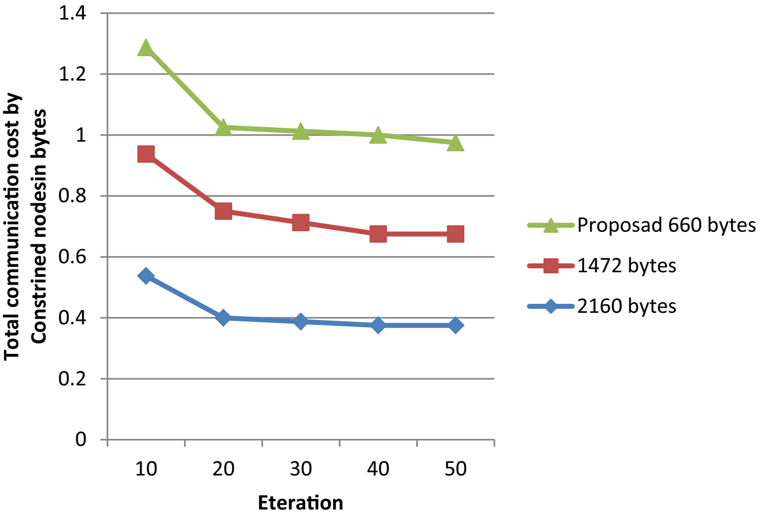

Fig. 3 Comparison of communication costs with other existing schemes

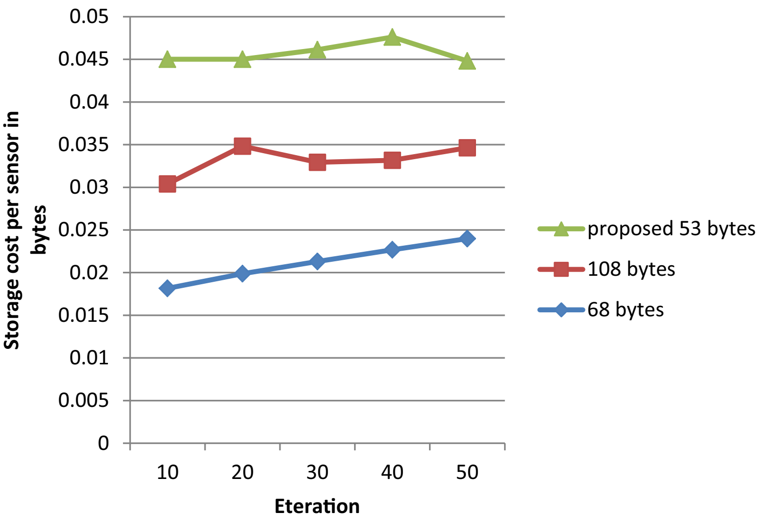

Fig. 4 Comparison of storage cost with existing schemes

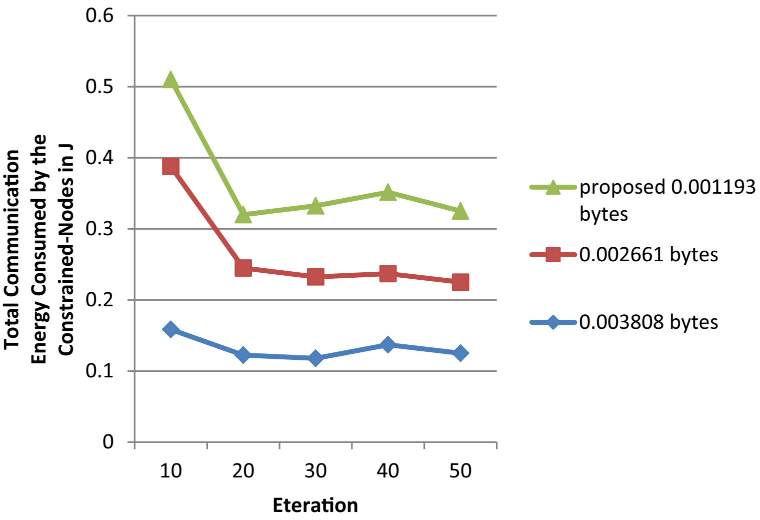

Fig. 5 Communication energy cost

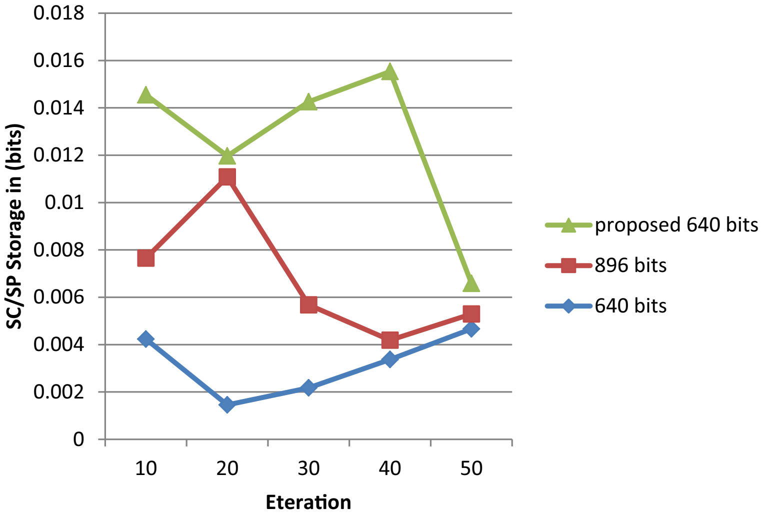

Fig. 6 Disability Storage cost of the proposed protocol and other related protocols

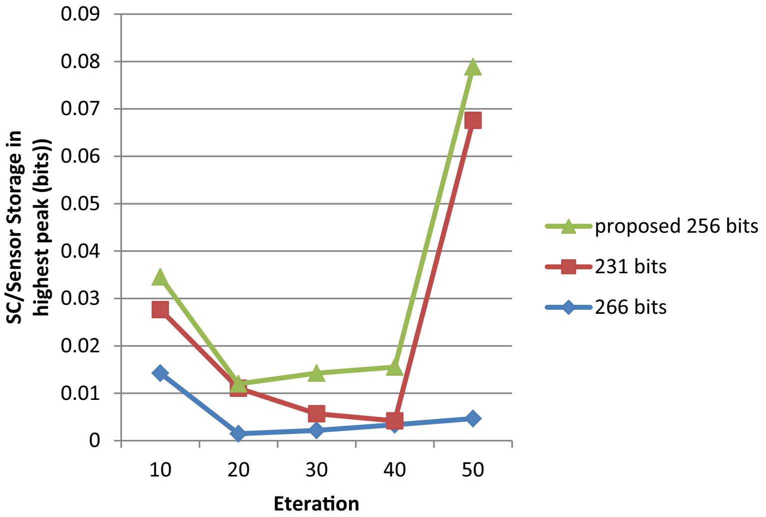

Fig. 7 Sensor storage cost of the proposed protocol and other related protocols

The IEEE 802.15.4 personal area network which was standardized for IoT comes with low bandwidth less than 256Kbps and a small packet size of 127 bytes.

5 Conclusion and Future Work

Lightweight authentication and a key agreement system that protects users' anonymity was suggested in this research for use in the Internet of Things. "An individual's fingerprint is used in conjunction with a password in the proposed protocol. There are four stages to the proposed protocol: pre-deployment, registration, login and authentication, and password change/update. To guarantee the protocol's robustness and safety, a thorough security study was performed to identify and mitigate any security threats before it was put into place. The protocol's effectiveness in an IoT setting has also been confirmed by our performance evaluations. The results show that the suggested protocol can withstand the majority of common security threats while remaining low-overhead in terms of computing, storage, and communication. This makes it an excellent choice for the Internet of Things." For the future, we suggest Lightweight encryption for data confidentiality in IoT is a promising direction for future work. Key management with involvement of dynamic environment such as vehicular network should be investigated with consideration of scalability of involved participants.

Acknowledgements The authors extend their appreciation to the King Salman Center For Disability Research for funding this work through Research Group no KSRG-2022-057.

Authors' Contribution Both coauthors contributed significantly to the research and this paper, and the first author is the main contributor.

Funding This research has been funded by the King Salman Center For Disability Research, KSA Through project No. (KSRG-2022-057).

Data availability Enquiries about data availability should be directed to the authors.

Declarations

Conflict of interest The authors declare that they have no conflicts of interest to report regarding the present study.

References

1. Ammar, M., Russello, G., & Crispo, B. (2018). Internet of Things: A survey on the security of IoT frameworks. *Journal of Information Security and Applications, 38*, 8–27.
2. Jayakumar, H., Lee, K., Lee, W. S., Raha, A., Kim, Y., & Raghunathan, V. (2014). Powering the internet of things. In *Proceedings of the 2014 international symposium on Low power electronics and design*. ACM.
3. Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2017). A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. *IEEE Internet of Things Journal, 4*(5), 1125–1142.
4. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials, 17*(4), 2347–2376.
5. Ma, J. (2014). Internet-of-Things: Technology evolution and challenges. In *2014 IEEE MTT-S International Microwave Symposium (IMS2014)*. IEEE.

6. Fernandes, E., Jung, J., & Prakash, A. (2016). Security analysis of emerging smart home applications. In *2016 IEEE symposium on security and privacy (SP)*. IEEE.
7. Bude, C., & Kervefors Bergstrand, A. (2015). Internet of Things: Exploring and securing a future concept.
8. Li, S., Tryfonas, T., & Li, H. (2016). The Internet of Things: A security point of view. *Internet Research, 26*(2), 337–359.
9. Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of Things security: A survey. *Journal of Network and Computer Applications, 88*, 10–28.
10. Rose, K., Eldridge, S., & Chapin, L. (2015). The internet of things: An overview. *The Internet Society (ISOC), 80*, 1–50.
11. Catarinucci, L., De Donno, D., Mainetti, L., Palano, L., Patrono, L., Stefanizzi, M. L., & Tarricone, L. (2015). An IoT-Aware architecture for smart healthcare systems. *IEEE Internet of Things Journal, 2*(6), 515–526.
12. Elijah, O., Rahman, T. A., Orikumhi, I., Leow, C. Y., & Hindia, M. N. (2018). An overview of Internet of Things (IoT) and data analytics in agriculture: Benefits and challenges. *IEEE Internet of things Journal, 5*(5), 3758–3773.
13. Sherly, J., & Somasundareswari, D. (2015). Internet of Things based smart transportation systems. *International Research Journal of Engineering and Technology, 2*(7), 1207–1210.
14. Satyadevan, S., Kalarickal, B. S., & Jinesh, M. K. (2015). Security, trust and implementation limitations of prominent IoT platforms. In *Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014*. Springer, Cham.
15. Sha, K., Wei, W., Yang, T. A., Wang, Z., & Shi, W. (2018). On security challenges and open issues in Internet of Things. *Future Generation Computer Systems, 83*, 326–337.
16. Abdmeziem, M. R., Tandjaoui, D., & Romdhani, I. (2015). A decentralized batch-based group key management protocol for mobile internet of things (dbgk). In *Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (CIT/IUCC/DASC/PICOM), 2015 IEEE International Conference on*. IEEE.
17. Naoui, S., Elhdhili, M. E., & Saidane, L. A. (2016). Security analysis of existing IoT key management protocols. In *Computer Systems and Applications (AICCSA), 2016 IEEE/ACS 13th International Conference of*. IEEE.
18. Hendaoui, F., Eltaief, H., & Youssef, H. (2018). A collaborative key management scheme for distributed smart objects. *Transactions on Emerging Telecommunications Technologies, 29*(6), e3198.
19. Matsumoto, R. (2015). Strong security of the strongly multiplicative ramp secret sharing based on algebraic curves. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 98*(7), 1576–1578.
20. Bamasag, O., & Toumi, K. Y. (2016). Efficient multicast authentication in internet of things. In Information *and Communication Technology Convergence (ICTC), 2016 International Conference on*. IEEE
21. Dahshan, H. (2016). An elliptic curve key management scheme for Internet of Things. *International Journal of Applied Engineering Research, 11*(20), 10241–10246.
22. Porambage, P., Braeken, A., Schmitt, C., Gurtov, A., Ylianttila, M., & Stiller, B. (2015). Group key establishment for enabling secure multicast communication in wireless sensor networks deployed for IoT applications. *IEEE Access, 3*, 1503–1511.
23. Challa, S., Wazid, M., Das, A. K., Kumar, N., Reddy, A. G., Yoon, E. J., & Yoo, K. Y. (2017). Secure signature-based authenticated key establishment scheme for future IoT applications. *IEEE Access, 5*, 3028–3043.
24. He, D., Kumar, N., & Chilamkurti, N. (2015). A secure temporal-credential-based mutual authentication and key agreement scheme with pseudo identity for wireless sensor networks. *Information Sciences, 321*, 263–277.
25. Amin, R., & Biswas, G. P. (2016). A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks. *Ad Hoc Networks, 36*, 58–80.
26. Farash, M. S., Turkanović, M., Kumari, S., & Hölbl, M. (2016). An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment. *Ad Hoc Networks, 36*, 152–176.
27. Amin, R., Islam, S. H., Biswas, G. P., Khan, M. K., Leng, L., & Kumar, N. (2016). Design of an anonymity-preserving three-factor authenticated key exchange protocol for wireless sensor networks. *Computer Networks, 101*, 42–62.
28. Arasteh, S., Aghili, S.F., & Mala, H. (2016). A new lightweight authentication and key agreement protocol for Internet of Things. In *2016 13th International Iranian society of cryptology conference on information security and cryptology (ISCISC)*. IEEE.
29. Abbas, S. T., Mohammed, H. J., Ahmed, J. S., Rashid, A. S., Alhayani, B., & Alkhayyat, A. (2023). The optimization efficient energy cooperative communication image transmission over WSN. *Applied Nanoscience, 13*, 1665–1677.

30. Alhayani, B., Kwekha-Rashid, A. S., Mahajan, H. B., Ilhan, H., Uke, N., Alkhayyat, A., & Mohammed, H. J. (2023). 5G standards for the Industry 4.0 enabled communication systems using artificial intelligence: Perspective of smart healthcare system. *Applied Nanoscience, 13*(3), 1807–1817. https://doi.org/10.1007/s13204-021-02152-4
31. Alomari, E. S., Nuiaa, R. R., Alyasseri, Z. A. A., Mohammed, H. J., Sani, N. S., Esa, M. I., & Musawi, B. A. (2023). Malware Detection using deep learning and correlation-based feature selection. *Symmetry, 15*(1), 123.
32. Sabri, B T., & Alhayani, B. (2022). Network page building methodical reviews using involuntary manuscript classification procedures founded on Deep Learning. In *2022 international conference on electrical, computer, communications and mechatronics engineering (ICECCME)*, Maldives, Maldives, 2022, pp. 1–8, doi: https://doi.org/10.1109/ICECCME55909.2022.9988457
33. Alhayani, B. S., Hamid, N., Almukhtar, F. H., Alkawak, O. A., Mahajan, H. B., Kwekha-Rashid, A. S., İlhan, H., Marhoon, H. A., Mohammed, H. J., Chaloob, I. Z., & Alkhayyat, A. (2022). Optimized video internet of things using elliptic curve cryptography based encryption and decryption. *Computers and Electrical Engineering, 101*, 108022.
34. Bonino, D., Alizo, M. T. D., Alapetite, A., Gilbert, T., Axling, M., Udsen, H., Soto, J. A. C. & Spirito, M. (2015). Almanac: Internet of things for smart cities. In *Future Internet of Things and Cloud (FiCloud), 2015 3rd* International *Conference on*. IEEE
35. Buyya, R., & Dastjerdi, A. V. (Eds.). (2016). *Internet of Things: Principles and paradigms*. Elsevier.
36. Kumar, P., Singh, J. P., Vishnoi, P., & Singh, M. P. (2015). Source location privacy using multiple-phantom nodes in WSN. In *TENCON 2015–2015 IEEE Region 10* Conference. IEEE.
37. Lopez, J., Rios, R., Bao, F., & Wang, G. (2017). Evolving privacy: From sensors to the internet of things. *Future Generation Computer Systems, 75*, 46–57.
38. Minch, R. P. (2015). Location privacy in the Era of the Internet of Things and Big Data analytics.
39. AlKawak, O. A., Ozturk, B. A., Jabbar, Z. S., & Mohammed, H. J. (2023). Quantum optics in visual sensors and adaptive optics by quantum vacillations of laser beams wave propagation apply in data mining. *Optik, 273*, 170396.
40. Sethi, P., & Sarangi, S. R. (2017). Internet of things: Architectures, protocols, and applications. *Journal of Electrical and Computer Engineering*. https://doi.org/10.1155/2017/9324035
41. Abdulrahman, S. A., & Alhayani, B. (2023). A comprehensive survey on the biometric systems based on physiological and behavioural characteristics. *Materials Today: Proceedings, 80*, 2642–2646.
42. Sun, G., Chang, V., Ramachandran, M., Sun, Z., Li, G., Yu, H., & Liao, D. (2017). Efficient location privacy algorithm for Internet of Things (IoT) services and applications. *Journal of Network and Computer Applications, 89*, 3–13.
43. Thao, T. P., Rahman, M. S., Bhuiyan, M. Z. A., Kubota, A., Kiyomoto, S., & Omote, K. (2017). Optimizing share size in efficient and robust secret sharing scheme for big data. *IEEE Transactions on Big Data, 7*, 703.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Pof. Abdulaziz R. Alamro The researcher has some researches and essays in the field of curricula, teaching methods and computer-assisted education, as well as training programs and the development of teaching skills. He has published two books in the field of teaching methods, and many publications related to the field of art education. He works as Curriculum and Instruction Professor, and Vice President of Hail University for Development and Business- KSA.

Prof. Usama M. Ibrahem The researcher has many researches and books in the field of educational design, e-learning, and educational design models, as well as distance training programs and the development of technological skills, and a publication has four books in the field of educational technology. He works As Professor of Educational Technology - College of Education, University of Hail and Professor of Educational Technology, Faculty of Education, Ismailia, Suez Canal University.

Dr. Talal M. Alsaif The researcher has an interest in the fields of management, business and development. He various works in business, Strategy, nonprofit organizations management, quality management, educational management, organizational and consumers behavior, need assessment and CSR. He works as an associate professor in the Management and MIS Department at the University of Hail, and the Dean of the Institute of Research and Consultations.