A Lightweight Privacy-Preserving Communication Protocol for Heterogeneous IoT Environment

Irfan Nazir*

Arsalan Manzoor Zargar

Sharafat Majeed

Abstract: The accommodation of individuals' regular routines is enormously expanded by the Internet of Things (IoT), but the chance of touchy client information spillage is expanded when security methods aren't followed. Guaranteeing the security of information move between IoT gadgets is a fundamental element in different IoT situations, including Astute Associated Vehicles, Shrewd Homes, and Clever Urban areas. In any case, cryptographic correspondence approaches are tested by the confined assets of minimal expense IoT gadgets; even a little expansion in computer chip usage could prompt a huge decrease in battery duration for battery-controlled sensors. In this work, we propose a correspondence protocol that involves exclusively the symmetric key-based conspire to restrict the utilization of assets. This protocol offers very lightweight encryptions that are regardless profoundly successful in safeguarding information transmissions. The protocol creates symmetric keys that are conveyed by a tumultuous design, known as a strategic map, to battle off assaults, for example, gadget catch and key reset. We look at the security elements of the protocol by displaying it semantically. What's more, an appraisal is directed on asset utilization to guarantee runtime viability.

Index terms *- Internet of Things (IoT), key delegation, lightweight protocol, secure communication, symmetric encryption.*

1. INTRODUCTION

Smart homes [1], smart cities [2], and Intelligent Connected Vehicles (ICVs) [3] all prominently include Internet of Things (IoT) contraptions, which have turned into a fundamental piece of current residing. With a normal 25 billion connected IoT gadgets by 2020 and an expected $6 trillion in monetary effect by 2025, these contraptions are multiplying colossally [4]. These contraptions further develop comfort, proficiency, computerization, and versatility in a scope of settings.

Remote channels, which are intrinsically unsound and open delicate information to potential busybodies, are regularly used to associate IoT gadgets or sensors. For instance, on the grounds that car correspondence protocols need confirmation, Electronic Control Units (ECUs) in ICVs, which control vehicle rationale, are vulnerable to threatening controls [5]. A conspicuous method for safeguarding this delicate information and unstable discussions is to utilize start to finish encryption. To

start interchanges, protocolal IoT security protocols regularly utilize unbalanced key-based strategies, using calculations like Elliptic Curve Cryptography (ECC) [8], Diffie-Hellman Key Exchange (DHKE) [7], and RSA [6]. Be that as it may, these strategies are computationally requesting, and, surprisingly, a 5 percent expansion in computer chip usage can radically abbreviate IoT gadget battery duration [9].

Since symmetric cryptography requires less registering power, it is a more viable choice for Web of Things organizations. Nonetheless, there are various hardships in making a protected symmetric key-based correspondence framework. To begin with, it's critical to ensure the key pre-conveyance interaction's privacy. Gadgets are powerless against gadget catch assaults in light of the fact that to the necessity for gadgets to share keys for validation [10]. Third, an aggressor can tune in on any transmission without warning if long haul symmetric keys are compromised. The ongoing symmetric key-put together methods [11]-[18] concentrate with respect to making direct pairwise keys between neighboring hubs, but in view of their intricacy, they are either impossible for huge organizations or vulnerable to gadget catch endeavors. Certain symmetric key-based methods [1], [19] are just fitting for fundamental IoT settings, like brilliant homes, where access is restricted to individuals with the appropriate approval. By the by, in light of the fact that ICVs and other IoT frameworks are utilized outside, assailants can get to them. In this way, we want to give a general, symmetric key-based safe protocol that is reasonable for an assortment of IoT settings, particularly for low-fueled, effectively open gadgets like sensors in ICVs.

2. LITERATURE SURVEY

IoT gadgets are fundamental for savvy homes, urban communities, and ICVs. A review expected 25 billion connected IoT gadgets by 2020, influencing the worldwide economy by almost $6 trillion by 2025 [4]. These contraptions further develop computerization, versatility, productivity, and comfort in different settings.

Web of Things gadgets and sensors are normally associated over remote channels, which are shaky and possibly open delicate information to snoops. ICV Electronic Control Units (ECUs), which control vehicle rationale, are dependent upon enemy control because of car correspondence norms' absence of confirmation [5]. Start to finish encryption normally gets delicate information and unstable discussions. Customary IoT security protocols introduce discussions with hilter kilter keys. These techniques use RSA [6], DHKE [7], and ECC [8]. These procedures take a ton of handling power, and, surprisingly, a 5% central processor increment will abbreviate IoT gadget battery duration [9].

Symmetric cryptography is more effective for IoT networks because of its low figuring necessities. Be that as it may, building a solid symmetric key-based correspondence protocol is troublesome. To begin with, stay quiet. Second, gadget catch assaults are conceivable in light of the fact that gadgets share confirmation keys [10]. Thirdly, compromising long haul symmetric keys permit assailants to snoop on any message. Current symmetric key-based arrangements lay out direct pairwise keys between encompassing hubs, yet they are either dependent upon gadget catch endeavors or excessively muddled for enormous organizations. Savvy homes utilize symmetric key-based approaches that are just appropriate for approved associations [1], [19]. ICVs and other IoT frameworks are outside, leaving them powerless against aggressors.

A few exploration have proposed symmetric key-based protocol changes to tackle these issues. Tune

et al. made a symmetric key-based security saving correspondence protocol for savvy home IoT applications [1]. Qiu et al. proposed a shrewd traffic time expectation approach for savvy urban areas in view of fine-grained street fragment time deduction [2], accentuating the need of safe metropolitan IoT network. Vcash, a standing structure for distinguishing disavowal of traffic administration in Web associated vehicles, by Tian et al. underscores the need areas of strength for IoT security [3].

These examinations give huge experiences, yet planning a nonexclusive, symmetric key-based secure protocol for heterogeneous IoT settings stays troublesome. Key pre-dispersion cycles can be gotten to ease this issue. Kumar et al. proposed JEDI, a many-to-many start to finish encryption and key designation system for IoT, to increment key administration security [9]. Regardless of whether a gadget is compromised, network security is kept up with this system.

Key administration techniques should be effective and versatile to get IoT interchanges. Das et al. analyzed Internet of Things security protocols and focused on the requirement for versatile key administration answers for handle the extending number of IoT gadgets [10]. Their exploration underlines the need for protocols that can adjust to changing organization geography and IoT gadget registering ability.

Also, IoT gadgets need lightweight cryptographic calculations to ration battery duration. Lara-Nino et al. overviewed elliptic bend lightweight encryption to find calculations that can be executed in asset compelled IoT gadgets [8]. Their discoveries show that lightweight cryptographic procedures like elliptic bend cryptography might get IoT interchanges without influencing gadget execution.

Van Bulck et al. created VulCAN, a powerful part verification and programming disconnection procedure for car control organizations, for car IoT [5]. ECUs in ICVs present novel security troubles, subsequently this strategy validates and secludes part correspondence. Designated security procedures can further develop IoT framework security in numerous applications.

Regardless of these advances, fostering a general, symmetric key-based safe protocol for heterogeneous IoT settings is troublesome. IoT applications like brilliant homes, urban areas, and ICVs require versatile and adaptable security arrangements. IoT gadgets fluctuate in availability, handling power, and security, consequently arrangements should consider that.

To conquer these issues, future exploration ought to assemble hybrid cryptographic protocols that incorporate symmetric and deviated encryption. IoT correspondence protocols can be secure and adaptable by utilizing symmetric and deviated cryptography. IoT network security might be improved by utilizing machine learning for anomaly detection and intrusion prevention.

Getting IoT correspondences has improved, yet fostering a protocolal, symmetric key-based secure protocol for heterogeneous IoT settings is as yet troublesome. Future examination can address key administration, versatility, and computational effectiveness difficulties to make secure security frameworks that safeguard IoT correspondences in shifted applications.

3. METHODOLOGY

i) Proposed Work:

We give a symmetric key-based protocol that is lightweight and safe. Key designation is carried out

utilizing Strategic Guide, a tumultuous framework. Disorder, which is capricious and unrepeatable, is many times utilized in cryptography. Before dispersion, Logistic Map boundaries and beginning qualities are arbitrarily made and allocated to every gadget as default design. This field and starting worth (the key) are utilized for confirmation when a gadget initially interfaces with a control place, like a cloud stage. Afterward, this control place can allocate one more boundary and introductory incentive for gadget to-gadget correspondence. Repeating the Strategic Guide with boundaries and beginning qualities refreshes all keys at the same time. Except if they catch the gadgets, adversaries can't compute the correspondence key on the grounds that the boundaries are kept mystery and never communicated openly. Aggressors can get to compromised gadget information on the grounds that the boundaries are arbitrary and not shared. This recommends our protocol opposes gadget capture.We test the protocol's security, adequacy, and protection from various dangers.

ii) System Architecture:

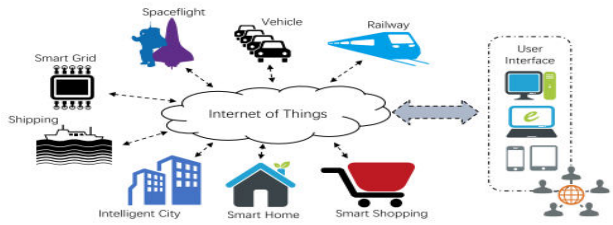


Fig 1 Proposed Architecture

The Internet of Things (IoT) is an organization of actual articles, vehicles, home machines, and different things outfitted with hardware, programming, sensors, actuators, and network that permit them to gather and exchange data. The graph has a few parts, including Smart Grid, Shipping, Intelligent City, Smart Home, and Smart Shopping. Each part is connected to a cloud, which stores and recovers data. There is likewise a UI part where customers can interface with the IoT gadgets. The graph's text marks incorporate spaceflight, vehicle, railway, and user interface.

iii) Modules:

In order to secure data transfer, a lightweight privacy-preserving communication protocol for heterogeneous IoT conditions has been introduced. This protocol gets rid of the need for key sharing systems or serious computational encryption, which are usually connected with existing cryptographic strategies. Four primary parts make up the methodology: Initialization, Establish Session Key, Generate IoT Network, and Communication. For safe and effective data transfer between IoT devices, each module is essential.

Generate IoT Network

This module mimics an IoT network with a Control Center and numerous gadgets. A tumultuous irregular number generator gives each IoT gadget a novel personality in the organization. Personality the board and secure correspondences are dealt with by the Control Center, a blue circle in the recreation.

The "Create IoT Network" button doles out secret characters to each IoT gadget to lay out the organization. The accompanying verification processes require these IDs. Users can check arrangement by survey delivered personalities and gadgets in the text box.

Initialization

The Introduction module confirms IoT gadgets imparting. Gadget A sends the Control Center its scrambled recognizable proof and Macintosh to convey information. The Control Center actually takes a look at distinguishing proof and Macintosh

against its data set. Gadget validation happens assuming the two checks succeed.

This forestalls unlawful access by permitting just endorsed gadgets to convey. The gadget's confirmation status shows assuming the Control Center checked it.

Establish Session Key

The Lay out Meeting Key module makes a protected correspondence meeting key after instatement. Information trades between verified gadgets and the Control Center require this meeting key. Gadget B sends its scrambled character and Macintosh to the Control Center for verification, similar to Gadget A.

When Gadget An and Gadget B are verified, the Control Center makes a meeting key. Encrypted communication between gadgets utilizing this meeting key permits data exchange without re-authentication.

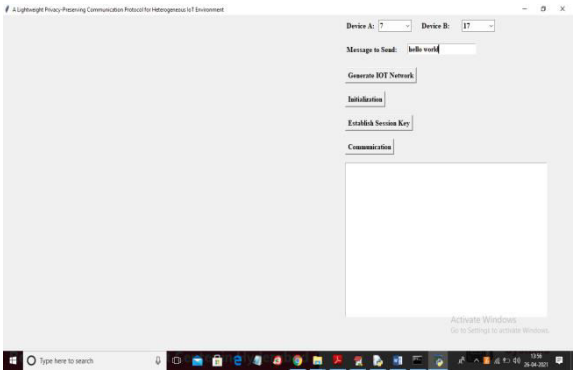
Communication

In the Communication module, verified gadgets devices encrypt and transfer data utilizing the meeting key. Gadget A sends information to the Control Center encoded with timestamps and symmetric encryption. Subsequent to confirming Gadget An and Gadget B, the Control Place sends scrambled information.

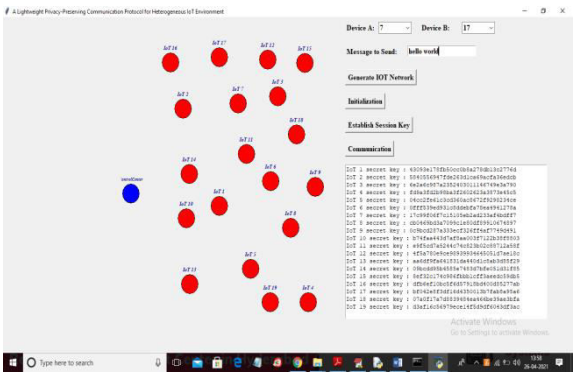
The Control Center safeguards information by permitting just confirmed gadgets to Communicate. Gadget B decodes the scrambled information with the meeting key to receive the first message. This guarantees secure and compelling IoT network availability.

4. EXPERIMENTAL RESULTS

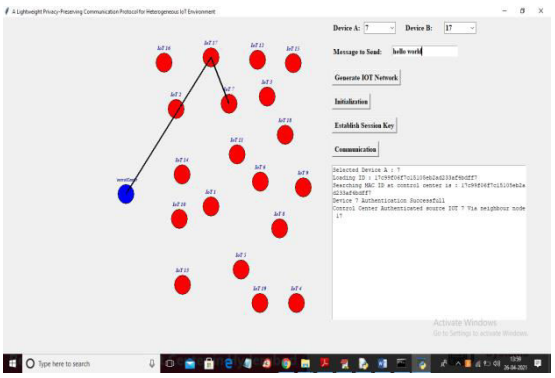
Double tap the "run.bat" document to send off the undertaking and see the screen below.



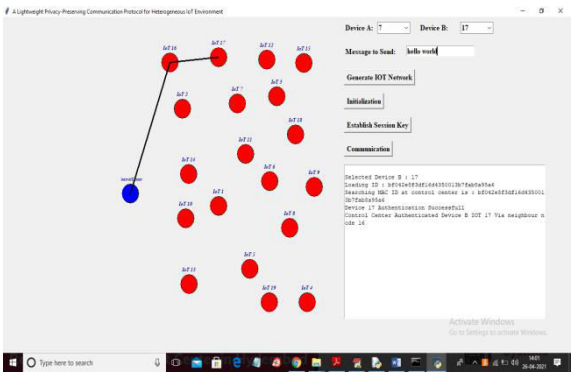
In the above screen, select device A and B from the drop-down box and type a message. I selected device A as 7 and device B as 17 and entered ‘hello world’. Click ‘Generate IOT Network’ to generate an IoT



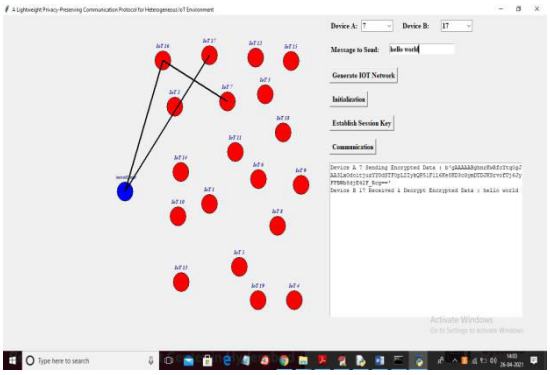
In the above screen, IoT network generated, red circles are standard IoT, blue circles are Control Center, and text area shows secret key generated for each IoT. Click ‘Initialization’ to authenticate device A and B.



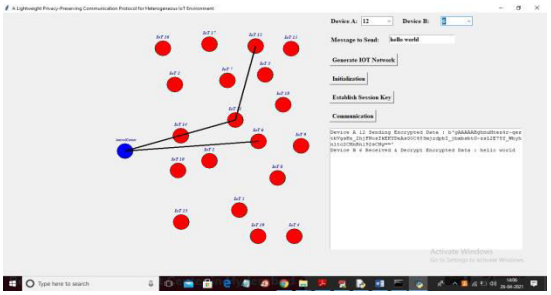
The preceding screen shows IoT 7 being authorized from Control Center by delivering a message. After authentication, device A dataset base ID and created ID match. To establish device A, Control Center, and device B session communication key, click 'Establish Session Key'.



Control Center authenticates Device B and establishes session key on above screen. Click 'Communication' to send data between Device A, Control Center, and Device B.



The following screen shows Device A transmitting data to neighbor IoT 16, IoT sending data to Control Center, and Control Center sending data to IoT17. Device A delivered encrypted data, which device B decrypted to get the original contents. Select any source or destination device and let Control Center authenticate and transfer data.



The accompanying screen shows IoT12 delivering data to IoT 6 via neighbor IoT and Control Center.

5. CONCLUSION

Our review presents a device-to-device security protocol that is inconceivably lightweight and simply depends on a symmetric key technique. We give assurance to assorted Internet of Things situations with our protocol. The chaotic system known as the Logistic Map is utilized in this protocol's synchronous key appointment component to guarantee that the symmetric keys' credits stay capricious, unrepeatable, and determinate. We evaluate the proposed convention's viability and security as well as its capacity to endure various unsafe blemishes. The outcome shows that our shrewd home framework protocol works better compared to before symmetric key-based examinations.

6. FUTURE SCOPE

Future examination could analyze how well the protocol scales in greater, more complicated IoT conditions, such brilliant urban areas and modern settings. Further developing security is the utilization of machine learning for anomaly detection. Looking at how well the protocol functions with various IoT equipment and how well it tends to be acclimated to new IoT norms would be useful too. At last, testing and certifiable application in different IoT biological systems can offer extra

bits of knowledge into its flexibility and viable viability.

REFERENCES

[1] T. Song, R. Li, B. Mei, J. Yu, X. Xing, and X. Cheng, ‘‘A privacy preserving communication protocol for IoT applications in smart homes,’’ IEEE Internet Things J., vol. 4, no. 6, pp. 1844–1852, Dec. 2017, doi: 10.1109/JIOT.2017.2707489.

[2] J. Qiu, L. Du, D. Zhang, S. Su, and Z. Tian, ‘‘Nei-TTE: Intelligent traffic time estimation based on fine-grained time derivation of road segments for smart city,’’ IEEE Trans Ind. Informat., vol. 16, no. 4, pp. 2659–2666, Apr. 2020.

[3] Z. Tian, X. Gao, S. Su, and J. Qiu, ‘‘Vcash: A novel reputation framework for identifying denial of traffic service in Internet of connected vehicles,’’ IEEE Internet Things J., to be published.

[4] Sumsung Smartthings Developers Documentation. [Online]. Available: https://smartthings.developer.samsung.com/blog/en-us/2019/ 01/17/Shape-the-Future-of-IoT-with-SmartThings

[5] J. Van Bulck, J. T. Mühlberg, and F. Piessens, ‘‘VulCAN: Efficient component authentication and software isolation for automotive control networks,’’ in Proc. 33rd Annu. Comput. Secur. Appl. Conf. (ACSAC), Orlando, FL, USA, Dec. 2017, pp. 225–237, doi: 10.1145/3134600.3134623.

[6] R. L. Rivest, A. Shamir, and L. Adleman, ‘‘A method for obtaining digital signatures and public-key cryptosystems,’’ Commun. ACM, vol. 21, no. 2, pp. 120–126, Feb. 1978, doi: 10.1145/359340.359342.

[7] W. Diffie and M. Hellman, ‘‘New directions in cryptography,’’ IEEE Trans. Inf. Theory, vol. IT-22, no. 6, pp. 644–654, Nov. 1976, doi: 10.1109/TIT.1976.1055638.

[8] C. A. Lara-Nino, A. Diaz-Perez, and M. Morales-Sandoval, ‘‘Elliptic curve lightweight cryptography: A survey,’’ IEEE Access, vol. 6, pp. 72514–72550, 2018, doi: 10.1109/ACCESS.2018.2881444.

[9] S. Kumar, Y. Hu, M. P. Andersen, R. A. Popa, and D. E. Culler, ‘‘JEDI: Many-to-many end-to-end encryption and key delegation for IoT,’’ in Proc. 28th USENIX Secur. Symp., USENIX Secur., Santa Clara, CA, USA, Aug. 2019, pp. 1519–1536. [Online]. Available: https://www.usenix.org/conference/usenixsecurity19/presentation/kumarsam

[10] A. K. Das, S. Zeadally, and D. He, ‘‘Taxonomy and analysis of security protocols for Internet of Things,’’ Future Gener. Comput. Syst., vol. 89, pp. 110–125, Dec. 2018, doi: 10.1016/j.future.2018.06.027.

[11] L. Eschenauer and V. D. Gligor, ‘‘A key-management scheme for distributed sensor networks,’’ in Proc. 9th ACM Conf. Comput. Commun. Secur. (CCS), Washington, DC, USA, Nov. 2002, pp. 41–47, doi: 10.1145/586110.586117.

[12] H. Chan, A. Perrig, and D. Song, ‘‘Random key predistribution schemes for sensor networks,’’ in Proc. Symp. Secur. Privacy, Berkeley, CA, USA, May 2003, pp. 197–213, doi: 10.1109/SECPRI.2003. 1199337.

[13] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, ‘‘Perfectly-secure key distribution for dynamic conferences,’’ in Proc. 12th Annu. Int. Cryptol. Conf., Adv. Cryptol. (CRYPTO), Santa Barbara, CA, USA, Aug. 1992, pp. 471–486, doi: 10.1007/ 3-540-48071-4_33.

[14] D. Liu, P. Ning, and R. Li, ‘‘Establishing pairwise keys in distributed sensor networks,’’ ACM Trans. Inf. Syst. Secur., vol. 8, no. 1, pp. 41–77, Feb. 2005, doi: 10.1145/1053283.1053287.

[15] A. K. Das, ‘‘A random key establishment scheme for multi-phase deployment in large-scale distributed sensor networks,’’ Int. J. Inf. Secur., vol. 11, no. 3, pp. 189–211, Apr. 2012, doi: 10.1007/s10207-012-0162-9.

[16] F. Hendaoui, H. Eltaief, and H. Youssef, ‘‘A collaborative key management scheme for distributed smart objects,’’ Trans. Emerg. Telecommun. Technol., vol. 29, no. 6, Jun. 2018, Art. no. e3198, doi: 10.1002/ ett.3198.

[17] A. K. Das, ‘‘ECPKS: An improved location-aware key management scheme in static sensor networks,’’ Int. J. Netw. Secur., vol. 7, no. 3, pp. 358–369, 2008. [Online]. Available: http://ijns.femto.com.tw/ contents/ijns-v7-n3/ijns-2008-v7-n3-p358-369.pdf

[18] I.-C. Tsai, C.-M. Yu, H. Yokota, and S.-Y. Kuo, ‘‘Key management in Internet of Things via kronecker product,’’ in Proc. IEEE 22nd Pacific Rim Int. Symp. Dependable Comput. (PRDC), Christchurch, South Island, Jan. 2017, pp. 118–124, doi: 10.1109/PRDC.2017.25.

[19] T. Song, R. Li, B. Mei, J. Yu, X. Xing, and X. Cheng, ‘‘A privacy preserving communication protocol for IoT applications in smart homes,’’ in Proc. Int. Conf. Identificat., Inf. Knowl. Internet Things (IIKI), Beijing, China, Oct. 2016, pp. 519–524, doi: 10.1109/IIKI.2016.3.

[20] W. S. Sayed, A. G. Radwan, and H. A. H. Fahmy, ‘‘Design of a generalized bidirectional tent map suitable for encryption applications,’’ in Proc. 11th Int. Comput. Eng. Conf. (ICENCO), Dec. 2015, pp. 207–211.

[21] T. S. Chaware and B. K. Mishra, ‘‘Secure communication using TPC and chaotic encryption,’’ in Proc. Int. Conf. Inf. Process. (ICIP), Dec. 2015, pp. 615–620.

[22] P. Tobin, L. Tobin, M. McKeever, and J. Blackledge, ‘‘Chaos-based cryptography for cloud computing,’’ in Proc. 27th Irish Signals Syst. Conf. (ISSC), Jun. 2016, pp. 1–6.

[23] C. Hu, A. Alhothaily, A. Alrawais, X. Cheng, C. Sturtivant, and H. Liu, ‘‘A secure and verifiable outsourcing scheme for matrix inverse computation,’’ in Proc. IEEE IEEE Conf. Comput. Commun. (INFOCOM), Atlanta, GA, USA, May 2017, pp. 1–9, doi: 10.1109/INFOCOM.2017. 8057199.

[24] S. A. Hirani, ‘‘Energy consumption of encryption schemes in wireless devices,’’ Ph.D. dissertation, Univ. Pittsburgh, Pittsburgh, PA, USA, 2003.

[25] W. Liao, C. Luo, S. Salinas, and P. Li, ‘‘Efficient secure outsourcing of large-scale convex separable programming for big data,’’ IEEE Trans. Big Data, vol. 5, no. 3, pp. 368–378, Sep. 2019, doi: 10.1109/TBDATA.2017.2787198.

[26] D. Dolev and A. Yao, ‘‘On the security of public key protocols,’’ IEEE Trans. Inf. Theory, vol. 29, no. 2, pp. 198–208, Mar. 1983, doi: 10.1109/TIT.1983.1056650.

[27] C. J. F. Cremers, S. Mauw, and E. P. de Vink, ‘‘Injective synchronisation: An extension of the authentication hierarchy,’’ Theor. Comput. Sci., vol. 367, nos. 1–2, pp. 139–161, Nov. 2006, doi: 10.1016/j.tcs.2006.08.034.

[28] S. Meier, C. Cremers, and D. Basin, ‘‘Strong invariants for the efficient construction of machine-checked protocol security proofs,’’ in Proc. 23rd IEEE Comput. Secur. Found. Symp., Edinburgh, U.K., Jul. 2010, pp. 231–245, doi: 10.1109/CSF.2010.23.

[29] J. Daemen and V. Rijmen, The Design of Rijndael: AES—The Advanced Encryption Standard (Information Security and Cryptography). Springer, 2002, doi: 10.1007/978-3-662-04722-4.

[30] D. Eastlake, III, and P. E. Jones, US Secure Hash Algorithm 1 (SHA1), document RFC 3174, 2001, pp. 1–22, doi: 10.17487/RFC3174.

[31] D. Eastlake, III, and T. Hansen, US Secure Hash Algorithms (SHA and HMAC-SHA), document RFC 4634, 2006, pp. 1–108, doi: 10.17487/RFC4634.

[32] D. Eastlake, III, and T. Hansen, US Secure Hash Algorithms (SHA and SHA-Based HMAC and HKDF), document RFC 6234, 2011, pp. 1–127, doi: 10.17487/RFC6234.